

German
Data
Security



G Data Whitepaper 2009

Wie kommt Schadcode auf Firmenrechner?

Ralf Benzmüller & Werner Klier
G Data Security Labs



Geschützt. Geschützter. G Data.

Inhalt

1. Wozu Malware?	2
2. Wie Cyber-Kriminelle mit Malware Geld verdienen	3
2.1 Botnetze.....	3
2.2 Spam	3
2.3 Erpressung.....	3
2.4 Datendiebstahl	4
2.5 Adware.....	5
3. Wie die Malware auf den PC kommt	6
3.1 Verbindung genügt.....	6
3.2 Per E-Mail	7
3.3 Per Instant Message	8
3.4 Per Tauschbörse.....	8
3.5 Per Datenträger	9
3.6 Über lokale Netzwerke.....	9
3.7 Per Webseite	10
4. Ablauf einer typischen Infektionswelle	13
4.1 Vorbereitung der Infektion	13
4.2 Durchführung.....	14
4.3 Den infizierten Rechner benutzen	14
5. Wie man sich schützen kann	15

1. Wozu Malware?

Die Beweggründe zur Erstellung und Verbreitung von Schadsoftware haben in den letzten Jahren einen bemerkenswerten Wandel vollzogen. Stand in den Anfangstagen der Computerviren noch ein beinahe sportlicher Ehrgeiz in Form eines Kräftemessens zwischen Computerspezialisten im Vordergrund, so sind Angreifer heute in erster Linie von handfesten finanziellen Interessen motiviert.

Im „digitalen Untergrund“ hat sich eine regelrechte Schattenwirtschaft etabliert, in der innerhalb straffer, tadellos durchorganisierter Strukturen professionell Malware erstellt, perfektioniert und verbreitet wird.

Innerhalb der Cybercrime-Ökonomie findet ein blühender Handel mit allen erdenklichen digitalen Gütern und Dienstleistungen statt. Auf entsprechenden Handelsplattformen sind Informationen über neu entdeckte Sicherheitslücken ebenso erhältlich wie die darauf maßgeschneiderte Malware, deren Urheber mitunter sogar eine Funktionsgarantie zusichern und ihre Abnehmer innerhalb des Garantiezeitraums kostenlos mit modifizierten Versionen versorgen.

Auch Armeen von infizierten Rechnern, die als sogenannte Zombies Teil eines Botnetzes geworden sind, werden auf Stunden- oder Tagesbasis zur Durchführung von Spam-Kampagnen oder gezielten Attacken gegen ungeliebte Webseiten oder Mailserver vermietet.

Und selbst das letzte Glied der kriminellen Wertschöpfungskette - die Umwandlung der erbeuteten Informationen, wie z.B. Kreditkartendaten in Bargeld - wird auf dem digitalen Marktplatz der Cyberkriminellen abgedeckt. Dazu heuern Scheinfirmen ahnungslose PC-Benutzer als „Finanzagenten“ an, die wiederum ihre privaten Bankkonten für dubiose Finanztransaktionen zur Verfügung stellen.

Längst ist das primäre Angriffsziel nicht mehr die Erstellung einer Schadsoftware, die ausschließlich auf Weiterverbreitung ausgelegt ist. Auch Firmennetze rücken zunehmend in das Blickfeld der Angreifer, um dort alle Arten von Informationen auszuspähen, die sich zu Geld machen lassen, oder um die Infrastruktur der attackierten Netzwerke zu kriminellen Zwecken zu missbrauchen.

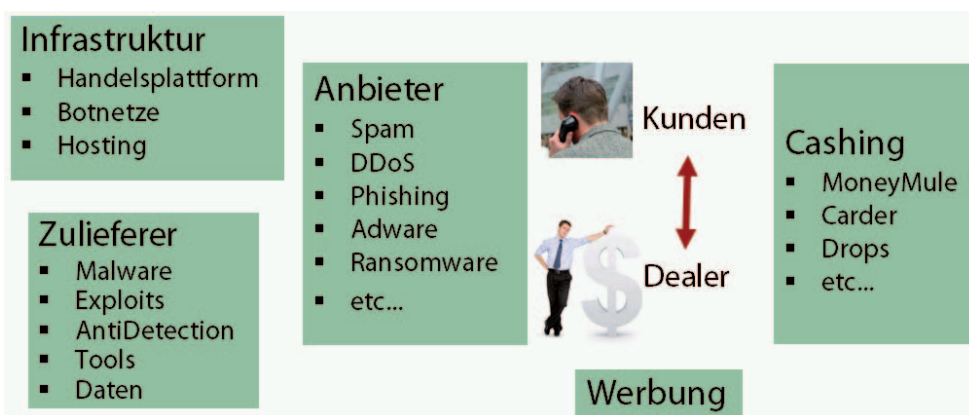


Abb.1: Übersicht über einzelnen Sparten der E-Crime-Ökonomie

Wie Abb. 1 zeigt, stellt sich die E-Crime-Ökonomie als eng vernetztes Geflecht vieler unterschiedlicher „Wirtschaftsbereiche“ dar. Im Hintergrund agieren die eigentlichen Akteure und liefern Malware, Wissen über neue Sicherheitslücken und verhökern gestohlene Daten. Diese werden durch Zwischenhändler auf spezialisierten Handelsplätzen an kriminelle „Kunden“ verkauft oder vermietet und letztendlich über angeheuerte, meist ahnungslose Mittelsmänner in bare Münze umgewandelt (sog. Cashing).

2. Wie Cyber-Kriminelle mit Malware Geld verdienen

Online-Ganoven erzielen auf unterschiedlichste Art und Weise finanziellen Profit. Eine wichtige Rolle spielt dabei der Einsatz von Armeen infizierter Rechner, die unter der Kontrolle der Angreifer stehen. Diese so genannten Botnetze können eine Reihe illegaler Aktivitäten durchführen, mit denen sich im digitalen Untergrund viel Geld verdienen lässt.

2.1 Botnetze

Botnetze sind Dreh- und Angelpunkt der eCrime-Infrastruktur. Sie dienen nicht nur dem Versenden von Spam oder Ausführen von Denial-of-Service-Angriffen. Zombie-Rechner werden auch dazu genutzt, Phishing- und Malwareseiten zu hosten - und um die Adressen von E-Mailservern auszukundschaften. Es ist daher nicht verwunderlich, dass die Zahl der Botnetz-Rechner bis heute stark zugenommen hat. Da die Botnetze in kleinere Einheiten mit wenigen Tausend Zombies segmentiert wurden, ist auch die Zahl der Botnetze deutlich gewachsen.

Erfolgte die Steuerung ursprünglich fast ausschließlich per IRC (Internet Relay Chat; textbasiertes Chat-System), so entstanden in der nächsten Entwicklungsstufe mehr Botnetze, die andere Protokolle zur Steuerung nutzen. Modernere Botnetze, wie etwa das berühmte Sturm-Botnetz, sind als Peer-to-Peer-Netz (P2P) angelegt. Das ebenso mächtige Zunker-Botnetz kommuniziert per HTTP. Nach dem Shutdown des dubiosen Internet Service Providers McColo verloren einige Botnetze ihre Kommandorechner und waren damit handlungsunfähig. In der Folge sind die Botnetze Srizbi und Storm verschwunden. Neuere Botnetze, wie z.B. Waledac oder Conficker, generieren nun viele verschiedene Kontaktmöglichkeiten, um jederzeit über die Botnetze verfügen zu können. Die Tarnmechanismen werden zudem immer ausgefeilter und mit häufigen Updates und Rootkits werden die Backdoors effizient getarnt. Die Programme und Daten für einen Auftrag werden erst unmittelbar zuvor übertragen und anschließend wieder gelöscht.

2.2 Spam

Spam ist ein großes Geschäft. Daran verdienen nicht nur die Anbieter der beworbenen Produkte. Der Versand der Spam-Mails erfolgt meist über Botnetze. Für den Versand von 2 Millionen E-Mails über 14 Tage zahlte der Spammer Solomon 195\$. 20 Millionen E-Mails kosteten 495\$. Der Handel mit wirkungslosen Pillen, gestohlener Software und minderwertigen Replikatoren ist so selbst bei geringsten Rücklaufquoten lukrativ, wobei die Rücklaufquoten alles andere als spärlich ausfallen. Die halblegalen Produkte, die dort beworben werden, haben ihre Klientel, die größer ist, als man gemeinhin vermutet. Und es gibt hier nicht nur betrügerische Händler, die ihre Kunden um die bezahlte Ware prellen. Jeremy Jaynes, seinerzeit der achtgrößte Spammer der Welt, brachte es auf ein Monatsgehalt von bis zu 750.000\$.

2.3 Erpressung

Wenn der Webshop einer Firma sehr einträglich ist oder ein Unternehmen davon abhängig ist, dass E-Mails zeitnah verarbeitet werden, dann ist das Unternehmen durch Angriffe auf diese Dienste erpressbar. Die zusammengeschalteten Zombie-PCs eines Botnetzes können eine Webseite oder einen Mailserver mit sinnlosen Anfragen bombardieren. Mit den massenhaften Server-Anfragen wird ein System so überlastet, dass ein normaler Betrieb nicht mehr möglich ist.

Mit diesen verteilten Überlastangriffen (engl. Distributed-Denial-of-Service, DDoS-attack) können nicht nur Wettbüros und Online-Casinos erpresst werden. Wer stündlich fünf- und

sechsstellige Beträge umsetzt oder eine Spiele-Community mit Dienstleistungen versorgen muss, ist mitunter bereit das Lösegeld zu zahlen, das oft nur einen Bruchteil der Umsatzeinbußen beträgt. Meist geht es um 4-stellige Beträge. Die Dunkelziffer ist sehr hoch.

DDoS-Attacken werden aber auch zu politischen Zwecken eingesetzt. In Estland wurden Ende April und Anfang Mai 2007 die Server von Ministerien, Regierungsbehörden, Banken, Zeitungen und Unternehmen lahmgelegt. Die Entfernung eines russischen Soldatendenkmals hatte den Unmut der russischen Bevölkerung hervorgerufen. Als die Demonstrationen gewalt- sam niedergeschlagen wurden, kamen Botnetze als politisches Mittel zum Einsatz.

Abgesehen von der bereits erwähnten Erpressung durch verteilte Überlastangriffe, gibt es noch weitere Möglichkeiten, von Opfern Geld zu erpressen. Ransomware; wie z.B. GPCoder, verschlüsselt bestimmte Dateien eines Rechners. Wer auf die Inhalte seiner Dateien wieder zugreifen möchte, muss ein Entschlüsselungsprogramm erstellen, das je nach Fall zwischen \$12 und \$200 kostet.

In Unternehmen gibt es aber noch andere Modelle. Ein Trojanisches Pferd könnte kinderpor- nografische Bilder, illegale Software und/oder kopiergeschützte Video- und Audiodateien auf den infizierten Rechner eines Mitarbeiters übertragen. Der Angreifer kann nun den Mitarbeiter gegenüber seinen Vorgesetzten erpressen oder dem Unternehmen mit einer Anzeige bei der Polizei drohen.

2.4 Datendiebstahl

Der Handel mit gestohlenen Daten beschränkt sich nicht nur auf gestohlene Kreditkarten- und Bankzugangsdaten. Durch Phishing-Angriffe werden mittlerweile auch Zugangsdaten für eBay, Soziale Netzwerke, Online-Shops, E-Mail-Accounts uvm. gestohlen. Mit Keyloggern - das sind Schadprogramme, die Tastatureingaben aufzeichnen - können sogar noch mehr Daten gestoh- len werden. Etwa die Zugangsdaten zu Firmen-Servern, Online-Rollenspielen, die Inhalte (ver- traulicher) E-Mails und Dokumente oder die Zugangsdaten zu Servern, Foren und VPNs. Wenn ein gerade bereinigter Webserver nach wenigen Tagen erneut infiziert ist, dann könnte es daran liegen, dass der Systemadministrator seine Passwörter an einen Keylogger verloren hat. Die Logfiles solcher Keylogger werden in Untergrundforen zu Preisen von wenigen Hundert Euro für Dutzende von Gigabytes gehandelt. Diese Informationen werden dann von anderen Gruppen ausgewertet und weiter vermarktet.

Die gestohlenen Daten werden vielfältig eingesetzt:

- Kreditkartendaten werden dazu verwendet gefälschte Kreditkarten zu „drucken“ oder in Online-Shops einzukaufen.
- Bankdaten werden genutzt, um unautorisierte Überweisungen durchzuführen. Da bei privaten Bankkonten die Überweisungssumme limitiert ist (ab 5000 EUR gelten besondere Sicherheitsmaßnahmen), ist auch die Beute limitiert. Diese Begrenzungen gelten für viele Bankkonten von Unternehmen nicht. Darum verstärken die Online-Bankräuber ihre Aktivi- täten, um an solche Zugangsdaten zu kommen.
- Gestohlene eBay-Accounts werden genutzt, um mit dem Kauf von Waren gestohlenes Geld zu waschen.
- Der Zugang zu Online-Rollenspielen wird genutzt, um die Online-Währungen und Utensili- en zu stehlen.
- Mit den Zugangsdaten von E-Mail-Accounts und Social Networks wird im Namen der Opfer Spam versendet.

- Gestohlene persönliche Daten werden genutzt, um im Internet Konten in bestimmten Foren zu eröffnen. Diese Konten werden dann für illegale Aktivitäten und Betrugsszenarien genutzt.

2.5 Adware

Adware. zeichnet mitunter das Surfverhalten des Nutzers auf, blendet beim Aufruf bestimmter Seiten Werbung ein oder manipuliert Suchabfragen. Die Bezahlung der Adware erfolgt entweder nach Anzahl der erzeugten Clicks (dann wird z.B. die Startseite des Browsers von befallenen Rechnern manipuliert) oder pro installierter Version. Entsprechende Partner-Programme finden sich in einschlägigen Onlineforen. Obwohl im vergangenen Jahr auch große Firmen der Adware-Branche juristische Niederlagen verkraften mussten, hat sich die Anzahl der Werbemalware und der potenziell unerwünschten Programme in den letzten beiden Jahren mehr als verfünffacht.

Fazit: Dies sind keinesfalls alle Geschäftsmodelle der Online-Kriminellen. Aber es sollte nun klar sein, dass Online-Kriminalität ein großes Geschäft ist, dessen jährliche Schäden im zwei- bis dreistelligen Milliardenbereich angegeben werden - das ist mehr als im Drogengeschäft. Die genannten Geschäftsbereiche zeigen die Schwerpunkte der Malwareverbreiter auf. Das wichtigste Instrument sind die Botnetze. Sie sind die Basis von Spamversand und Phishing-Attacken. Erpressung, der Diebstahl von Daten und die Einblendung von passender Werbung sind weitere Schwerpunkte.

3. Wie die Malware auf den PC kommt

Nachdem die Motivation der Malware-Verbreiter beleuchtet wurde, können wir uns dem eigentlichen Thema dieser Studie widmen. Es gibt zahlreiche Wege, wie Malware auf den Firmen-PC gelangen kann. In bestimmten Fällen kann es schon ausreichen, den Rechner mit dem Internet oder einem lokalen Netzwerk zu verbinden. Aber auch E-Mail, Tauschbörsen, Instant Messages und sogar Datenträger können Schadcode enthalten. Am gefährlichsten sind derzeit aber präparierte Webseiten, die entweder direkt eine Datei herunterladen oder unbemerkt im Hintergrund als sogenannte Drive-By-Downloads den Rechner infizieren.

3.1 Verbindung genügt

Die zahllosen Internet-Würmer und Bots, die ständig autonom im Internet kursieren, stellen eine ständige Bedrohung für mit dem Internet verbundene Rechner dar. Pausenlos generieren sie mehr oder weniger zufällig IP-Adressen und prüfen, ob die dazugehörigen Rechner anfällig für Sicherheitslücken sind. Die Auswahl der IP-Adressen ist häufig eingeschränkt, so dass nur bestimmte Netzbereiche - z.B. eines bestimmten Internet Providers oder einer bestimmten Region - ausgewählt werden. Welche Sicherheitslücken genutzt werden, variiert mit der Zeit. Selbst schon längst geschlossene Sicherheitslücken werden noch abgefragt, etwa die von Blaster (2003) und Sasser (2004). Häufige Angriffsziele sind in der folgenden Liste aufgeführt:

- Plug'n'Play (MS05-039) über TCP/445, TCP/139
- RPC-DCOM (MS03-026/MS03-039) über TCP/135, TCP/445, TCP/1025
- LSASS (MS04-011) über TCP/445
- MySQL über TCP/3306
- Arkeia über TCP/617
- Veritas über TCP/6101
- Veritas über TCP/10000
- WINS über TCP/42
- Arcserve über TCP/41523
- NetBackup über TCP/13701
- Workstation Service (MS03-049) über TCP/135, TCP/445
- WebDaV über TCP/80
- DameWare über TCP/6129
- MyDoom-Backdoor über TCP/3127
- Bagle-Backdoor über TCP/2745
- IIS 5.x SSL PCT (MS04-011) über TCP/443
- Accounts mit Trivialpasswörtern (Verbindung über TCP/139 bzw. TCP/445)
- MSSQL-Server mit Trivialpasswort (z.B. „SA“-Account mit Leerpasswort) über TCP/1433

In einer Studie wurden über einen Zeitraum von drei Monaten Attacken auf verschiedene Rechnerarchitekturen gemessen. Windows-Rechner wurden dabei im Durchschnitt alle 38 Sekunden angegriffen. So mancher Systemadministrator hat bereits erlebt, wie ein neu aufgesetzter Rechner während des Downloads der Patches nach wenigen Sekunden angegriffen und übernommen wurde. In Netzen mit vielen Endkunden (z.B. T-Online) liegt die Angriffsdich-

te deutlich unter dem Mittelwert von 38 Sekunden. Dazu kommt, dass in den letzten Jahren die Erstellung von Exploit-Codes professionalisiert wurde. Manchmal erscheinen Exploit-Codes für Sicherheitslücken schon wenige Tage nach den ersten Berichten darüber. Auch die Anzahl der Exploits, die entdeckt werden, weil sie von Malware genutzt werden (sog. Zero-Day-Exploits), nimmt ständig zu. Das jüngste Beispiel hierfür war der Wurm Conficker, der neben der automatischen Verbreitung auch lokale Freigaben mit schwachem Passwortschutz und den Autostart-Mechanismus von USB-Datenträgern zur Verbreitung nutzt.

Diese Art des Angriffs funktioniert ohne Zutun des PC-Nutzers und in den meisten Fällen auch ohne das Wissen des Nutzers. Eine gut konfigurierte Firewall bzw. ein Router schützen vor solchen Angriffen.

3.2 Per E-Mail

Nach wie vor verbreiten sich viele Schädlinge per E-Mail. Die großen Ausbrüche von Loveletter, Melissa oder Sobig und Netsky, die teilweise die Mailserver in die Knie zwangen, werden immer seltener und sind auch von den Verbreitern der Würmer nicht beabsichtigt. Sober, Nyxem und WarezoV waren die letzten E-Mail-Würmer, die in den Medien große Beachtung gefunden haben. Stattdessen werden viele kleinere Wellen gestartet, die zeitlich und lokal begrenzt sind. Im Gegensatz zu den vollautomatisch ablaufenden Infektionen von Internet-Würmern werden E-Mail-Würmer erst gefährlich, wenn der Empfänger den Dateianhang öffnet. Alleine das Eintreffen einer schädlichen Mail stellt noch keine Gefahr dar und nur in wenigen Fällen reicht es aus, die E-Mail im Client anzeigen zu lassen (z.B. Bubbleboy und Klez). Das Gros der E-Mails bedarf der Mithilfe des Empfängers, der wird mit vielfältigen Social-Engineering-Tricks zum Öffnen des Anhangs verleitet wird. Dazu können alle möglichen Angaben des E-Mail-Headers gefälscht werden. Besonders gerne genommen wird hier die Absenderadresse. Nur die erste Generation der E-Mail-Würmer leitete sich unter dem Namen des Opfers weiter. Heute sind fast alle Absenderadressen von E-Mail-Würmern gefälscht.

Da mittlerweile ausführbare Dateien in E-Mails weggefiltert werden (entweder am Gateway oder im Client) und auch das Gefahrenbewusstsein der E-Mail-Nutzer gestiegen ist, haben die Malwareautoren die Strategie gewechselt. Anstelle der Dateianhänge werden die E-Mails mit Links auf die Dateien im Internet versendet. Diese E-Mails wurden zunächst nicht als schädlich erkannt. Allenfalls der Spamfilter kann sie ausfiltern. Das Handling für den Benutzer ist aber sehr ähnlich. Er klickt auf den Link, der Browser fragt, was er tun soll und bietet normalerweise an, die Datei auszuführen. Es dauerte aber nicht lange, bis direkte Links auf Malware ebenfalls als schädlich erkannt wurden. Die Malwareautoren verweisen daher nun auf eine Webseite, wo der Empfänger entweder einen Download neu starten muss oder der Download durch mitunter zahlreiche Weiterleitung automatisch startet.

Als Lockvogel, mit denen die Opfer zum Ausführen der Datei bzw. zum Aufrufen von Webseiten verleitet werden (das sog. Social Engineering), fungiert entweder der Absender, die Betreffzeile und/oder der Inhalt der Mail. Aber auch der Name des Dateianhangs, doppelte Dateieindungen, populäre Icons oder der Domainname des Links können zur Schlüssigkeit eines solchen Betrugsversuchs genutzt werden. Jordan und Goudey (2005) nennen die folgenden zwölf psychischen Faktoren, auf denen die erfolgreichsten Würmer zwischen 2001 und 2004 beruhen:

- Unerfahrenheit (inexperience)
- Neugier (curiosity)
- Gier (greed)
- Zaghaftheit (diffidence)

- Höflichkeit (courtesy)
- Eigenliebe (self-love)
- Leichtgläubigkeit (credulity)
- Wunschdenken (desire)
- Lust und Liebe (lust)
- Drohung (dread)
- Gegenseitigkeit (reciprocity)
- Freundlichkeit (friendliness)

M. Braverman ergänzte:

- Allgemeine Konversation (generic conversation): Kurze Aussagen, wie „Cool“ etc.
- Virenwarnungen und Software-Patches
- Malware-Fund auf dem PC
- Virenprüfberichte am Ende der Mail
- Informationen oder Meldungen zu Accounts: z.B. der Telekom-Trojaner, der sich als überhöhte Telefonrechnung ausgibt
- Fehlermeldungen der Mailzustellung
- Körperliche Anziehung (Physical attraction) (überlappt sich mit dem Punkt Lust und Liebe von Jordan & Goudey)
- Anklagen (Accusatory): z.B. der BKA-Trojaner, der angeblich illegale Dateien gefunden haben will
- Aktuelle Ereignisse
- Free stuff: Manche Menschen lassen alle Vorsicht außer Acht, sobald es etwas kostenlos gibt

Die Täuschungsversuche hören aber noch nicht auf, wenn der Schädling sein Ziel erreicht hat und ausgeführt wurde. Nach der erfolgreichen Attacke gilt es zu verhindern, dass ein Opfer merkt, dass es infiziert wurde. Dazu werden Fehlermeldungen, Bilder oder (manchmal leere) Dokumente geöffnet. Einige Würmer wie Sircam und Magistr hängen sich an eine Datei an und wenn der Schadcode gestartet wurde, wird auch die Originaldatei geöffnet. So bleibt die Infektion unbemerkt.

3.3 Per Instant Message

Die meisten Instant-Message-Würmer senden Nachrichten mit Links auf Webseiten. Die Möglichkeit, direkt Dateien zu übertragen, wird kaum noch genutzt. Auch hier beruhen die Angriffe wie bei E-Mails auf Social Engineering. Einige Instant-Message-Würmer besitzen sogar Chat-Engines und sind in der Lage, kurze Gespräche zu führen und so Vertrauen aufzubauen.

Wer Instant Messaging im Unternehmen nutzt, sollte einen Client wählen, der es erlaubt eingehende Dateien zu prüfen. Einige Clients bieten dazu die Möglichkeit, einen Virens scanner per Kommandozeile aufzurufen.

3.4 Per Tauschbörse

In einer von G Data durchgeführten Studie haben wir in P2P-Tauschbörsen nach Begriffen gesucht, die mit den aktuellen Top-20-Online-Games in Zusammenhang stehen. Zu Beginn der

Studie waren von den knapp 1000 heruntergeladenen Dateien 33% von Schädlingen befallen. Etwas mehr als zwei Drittel (68%) der Schädlinge waren als Adware zu identifizieren, 23% waren Trojanische Pferde und 5% Backdoors.

Im Verlauf der über sechs Monate durchgeführten Studie waren bereits mehr als die Hälfte der geprüften Dateien aus P2P-Tauschbörsen mit Schadcode präpariert. Dieser Anteil gipfelte gegen Ende des Untersuchungszeitraums in einem Spitzenwert von über 65% infizierter Dateien.

Diese Zahlen belegen, dass P2P-Tauschbörsen nach wie vor bei Malwareautoren äußerst beliebt sind. Wer sie im Unternehmen nutzt, sollte sich auf jeden Fall wappnen.

3.5 Per Datenträger

Immer wieder kommt es vor, dass Datenträger wie Festplatten, DVDs oder MP3-Player bei der Auslieferung ab Werk mit Malware verseucht sind. Es wird auch von Fällen berichtet, in denen auf dem Parkplatz vor einem Unternehmen USB-Sticks mit Spyware gezielt „verloren“ wurden. Einige Mitarbeiter wollten wissen, was auf dem Stick drauf ist und verseuchten so ihren PC mit Spyware.

Der Anfang 2009 in den Medien überaus präsente Wurm Conficker nutzte unter anderem die Autorun-Funktion von Windows-Betriebssystemen, um sich per Wechseldatenträger zu verbreiten. Die Würmer aus der Familie Autorun nutzen ebenfalls diese „Funktion“ von Windows und sorgten seit dem zweiten Halbjahr 2008 für ein Revival der Würmer. Ratschläge, die Autorun-Funktion einfach zu deaktivieren, liefen zunächst ins Leere, da dies nachträglich über einen entsprechenden Microsoft-Patch überhaupt erst möglich wurde.

Diese Fälle zeigen, dass Unternehmen, insbesondere wenn sie wertvolle Daten beherbergen, auch auf ungewöhnlicheren Wegen angegriffen werden und dass man nicht vorsichtig genug sein kann.

3.6 Über lokale Netzwerke

Ein weiterer Verbreitungsweg sind Freigaben in lokalen Netzwerken. Einige Würmer kopieren sich auf alle frei zugänglichen Bereiche. In vielen Fällen nutzen sie dabei Listen mit gängigen Passwörtern. Auch Conficker setzte unter anderem auf diese Schwachstelle. Daher sollten in Unternehmen starke Passwörter verwendet werden und die Freigaben sollten regelmäßig, am besten täglich, auf Schadcode geprüft werden. Einige Varianten von Rbot und Conficker verwenden u.a. die folgenden Logins:

„ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „COMPUTER“, „DATABASE“, „DB2“, „DBA“, „DEFAULT“, „GUEST“, „NET“, „NETWORK“, „ORACLE“, „OWNER“, „ROOT“, „STAFF“, „STUDENT“, „TEACHER“, „USER“, „VIRUS“, „WWWADMIN“

und Passwörter:

„0“, „000“, „007“, „1“, „12“, „123“, „1234“, „12345“, „123456“, „1234567“, „12345678“, „123456789“, „1234567890“, „12345678910“, „2000“, „2001“, „2002“, „2003“, „2004“, „ACCESS“, „ACCOUNTING“, „ACCOUNTS“, „ADM“, „ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „BASD“, „BACKUP“, „BILL“, „BITCH“, „BLANK“, „BOB“, „BRIAN“, „CHANGEME“, „CHRIS“, „CISCO“, „COMPAQ“, „COMPUTER“, „CONTROL“, „DATA“, „DATABASE“, „DATABASEPASS“, „DATABASEPASSWORD“, „DB1“, „DB1234“, „DB2“, „DBA“, „DBPASS“, „DBPASSWORD“, „DEFAULT“, „DELL“, „DEMO“, „DOMAIN“, „DOMAINPASS“, „DOMAINPASSWORD“, „ERIC“, „EXCHANGE“, „FRED“, „FUCK“, „GEORGE“, „GOD“, „GUEST“, „HELL“, „HELLO“, „HOME“, „HOMEUSER“, „HP“, „IAN“, „IBM“, „INTERNET“, „INTRANET“, „JEN“, „JOE“, „JOHN“, „KATE“, „KATIE“, „LAN“, „LEE“, „LINUX“, „LOGIN“, „LOGINPASS“, „LUKE“, „MAIL“, „MAIN“, „MARY“, „MIKE“, „NEIL“, „NET“, „NETWORK“, „NOKIA“, „NONE“, „NULL“, „OAINSTALL“, „OEM“, „OEMINSTALL“, „OEMUSER“, „OFFICE“, „ORACLE“, „ORAINSTALL“, „OUTLOOK“,

„OWNER“, „PASS“, „PASS1234“, „PASSWD“, „PASSWORD“, „PASSWORD1“, „PETER“, „PWD“, „QAZ“, „QWE“, „QWERTY“, „ROOT“, „SA“, „SAM“, „SERVER“, „SEX“, „SIEMENS“, „SLUT“, „SQL“, „SQLPASS“, „STAFF“, „STUDENT“, „SUE“, „SUSAN“, „SYSTEM“, „TEACHER“, „TECHNICAL“, „TEST“, „UNIX“, „USER“, „VIRUS“, „WEB“, „WIN2000“, „WIN2K“, „WIN98“, „WINDOWS“, „WINNT“, „WINPASS“, „WINXP“, „WWW“, „WWWADMIN“, „XP“, „ZXC“

Auf diese und ähnliche Passwörter - auch in deutscher Übersetzung - sollten User in ihrem Netzwerk daher verzichten.

3.7 Per Webseite

Das momentan wichtigste Einfallstor für neue Schädlinge sind Webseiten. Sie nutzen eine strukturelle Schwachstelle in der Arbeitsweise von Virenscannern. Virenscanner prüfen Dateien entweder, sobald eine Systemkomponente darauf zugreifen will (OnAccess) oder auf Anfrage (OnDemand). Die Prüfung des Virenscanners findet also erst statt, wenn der Schadcode bereits als Datei vorliegt. Wenn nun per HTTP die Daten der Webseite zum Browser übertragen werden, werden die darin enthaltenen HTML-Codes und Skriptbefehle zunächst im Arbeitsspeicher des Browsers interpretiert und ausgeführt. Irgendwann entscheidet der Browser dann, dass die Inhalte auf der Festplatte gespeichert werden sollen. Möglicherweise schlägt nun der Virenscanner Alarm. Die Schadcodes sind dann aber bereits ausgeführt. Damit ein Virenscanner vor schädlichen Webseiten wirkungsvoll schützen kann, muss der Inhalt des HTTP-Datenstroms geprüft werden, bevor er in den Browser gelangt.

Im Zusammenhang mit E-Mails wurde schon darauf eingegangen, dass Schaddateien von Webseiten heruntergeladen werden können. Dies geschieht entweder durch einen direkten Link auf die Schaddatei, durch Weiterleitungen oder indem der Nutzer durch Tricks dazu gebracht wird, die Datei per Klick auf einen Button bzw. Link auf den Rechner zu laden und auszuführen.

Zwei typische Maschen, mit denen Nutzer zum Download und zur Installation von Malware verleitet werden sollen, seien kurz vorgestellt. Sogenannte Scareware gaukelt dem Opfer durch gefälschte Warnmeldungen vor, dass das System mit Malware infiziert sei. Zur Entfernung der Infektion soll das Opfer seine Kreditkarten-Informationen preisgeben und etwa 50 Dollar für eine angebliche „Vollversion“ eines Schummel-Scanners bezahlen.

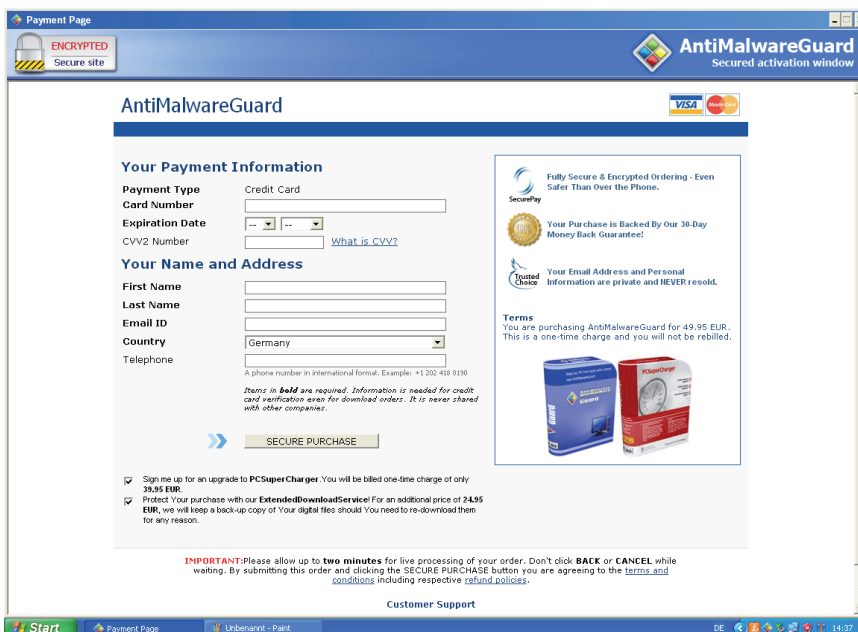


Abb. 2: Eine Scareware-Webseite fragt nach den Kreditkarten-Informationen des Opfers

Gerne wird auch eine Masche benutzt, bei der die Opfer auf eine Webseite gelockt werden, auf der sich angeblich ein Video befindet. Dieses kann einen angeblich erotischen Inhalt oder aber auch einen Bezug zu einem tagesaktuellen Ereignis haben, das momentan in den Medien präsent ist (Naturkatastrophe, Flugzeugunglück, Präsidentschaftswahl, Sportereignis). Um das angepriesene Video zu betrachten, muss der Besucher angeblich zunächst einen speziellen Video-Codec oder eine neuere Version des Flash-Players installieren, in dem die Schadsoftware versteckt ist. Hinter diesem Link verbirgt sich dann immer wieder Malware, die anstelle des Flash-Players auf dem Rechner installiert wird.

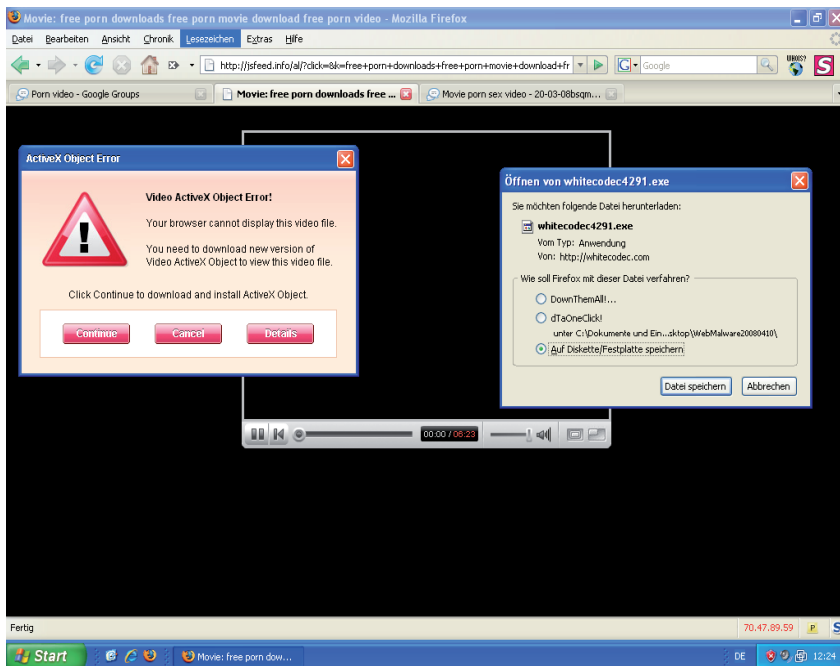


Abb. 3: Angewandte Video-Webseite, die zum Download eines infizierten Codecs auffordert

Es gibt aber noch eine weitere Angriffstechnik, bei der das Opfer nicht eingreifen muss: sogenannte Drive-By-Downloads. Während Downloads vom Besucher der Webseite initiiert werden müssen, geschehen Drive-By-Downloads - wie die Name schon sagt - unbemerkt im Vorbeisurfen. Dazu werden auf einem Server-Rechner, der vom Malware-Verbreiter kontrolliert wird, Skripte hinterlegt, die zunächst prüfen, auf welchem Browser und welchem Betriebssystem der PC des Webseiten-Besuchers basiert. Passend zugeschnitten auf die jeweilige Kombination wird dann Schadcode nachgeladen, der den Browser und seine Komponenten auf Sicherheitslücken prüft. Wenn die Suche positiv ausfällt, wird Schadcode übertragen, der diese Sicherheitslücke ausnutzt, um den Rechner zu übernehmen. Solche Schadcodes heißen Exploits. Für Windows-Rechner mit Internet Explorer kursieren die meisten Exploits. Aber auch die Schwachstellen von Firefox, Opera und Safari werden genutzt. Für die Installation der Skripte gibt es Tools wie MPack IcePack oder FirePack, die dafür sorgen, dass die Skripte korrekt installiert werden. Momentan bedienen sich Malware-Autoren der folgenden Sicherheitslücken am häufigsten:

- CVE 2007-0071 Adobe Flash
- CVE 2008-1309 RealPlayer
- ourgame_GLIEDown2 Internet Explorer
- CVE 2006-0003 MS06-01, MDAC
- CVE 2007-5601 RealPlayer

Wenn der Server vorbereitet ist, muss der Malware-Verbreiter nur noch Besucher auf seine Seite locken. Das geschieht einerseits durch Spam-Mails, die mit interessanten Nachrichten, besonderen Angeboten oder Lotteriegewinnen auf die Seite locken. Immer öfter werden auch Anfragen bei bekannten Suchmaschinen wie Google, Yahoo und Bing so manipuliert, dass schädliche Webseiten in den Suchergebnissen weit oben erscheinen. Auch ein Vertipper bei der Eingabe des Links im Browser kann auf schädliche Seiten führen. Zwei Beispiele: „microsoft.com“, „goggle.com“ oder „mcaffede“ sowie viele andere Domains, deren Schreibweise der von bekannten Webseiten ähnelt, werden schon seit Jahren registriert, um darauf Werbung anzuzeigen. Nun kann mit der Verbreitung von Adware oder Malware zusätzlich Geld verdient werden.

Viel effektiver ist es aber, wenn der Schadcode in die Webseiten einer bekannten Domain integriert werden kann. Gelingt es einem Angreifer den Webserver unter seine Kontrolle zu bringen, wird mit den oben erwähnten Web-Exploit-Toolkits in jede Webseite eine Zeile eingefügt, die Schadcode von einem anderen Server nachlädt (z.B. per IFRAME oder SCRIPT). Auch für Angriffe auf Webserver gibt es mittlerweile Tools, die mit Wörterbuchattacken versuchen das Passwort des Administrator-Zugangs zu knacken. Ebenso werden Sicherheitslücken in gängiger Web-Software wie Content Management Systeme, Blog- und Forensoftware und Administrationstools ausgenutzt, um Webserver zu übernehmen. In der Mehrheit der Fälle werden diese Angriffe nicht auf einzelne Webserver beschränkt, sondern massenhaft und automatisiert durchgeführt. Die Folge: Schadcode lauert nicht nur in den dunklen Bezirken des Internets, sondern kann sich auf jeder Domain verstecken.

Eine andere Möglichkeit bieten Werbeeinblendungen auf beliebten Webseiten. Fast alle populären Domains nutzen die Möglichkeit per Werbung mit der Webseite Geld zu verdienen. Die Werbebanner werden normalerweise per IFRAME in die Seite eingeblendet, sodass der Betreiber keinen Einfluss auf die dort dargestellten Inhalte hat. Es obliegt dem Werbetreibenden, die Inhalte der ausgelieferten Werbeinhalte zu prüfen. Das ist aber leichter gesagt als getan. Die Schadskripte, die mit MPack oder ähnlichen Tools erstellt werden, sind hochgradig verschleiert und verschlüsselt (die Erstellung polymorphen Schadcodes ist auch mit Skriptsprachen machbar). Auf diese Weise gelingt es, Schadcode in legitime Webseiten einzubinden. Circa 80% aller Drive-By-Infektionen erfolgen auf legitimen Webseiten.

Aber man kann Schadcode auch übertragen, ohne einen Webserver zu cracken. Links in Foren, Blogs oder E-Mails können den Schadcode enthalten, der dann in der aufgerufenen Seite ausgeführt wird. Das interaktive Mitmach-Internet bietet zahllose Diskussionsforen und Wikis, in denen die Teilnehmer eigene Beiträge schreiben und Dateien hinterlegen können. Dort kann manchmal auch Malware hochgeladen werden oder es wird ein Link auf eine schädliche Webseite hinterlegt. Einmal ist es einem Autor in Wikipedia gelungen, im Artikel über den Blaster-Wurm einen Link auf ein Removal-Tool zu setzen, das sich später als Trojanisches Pferd herausstellte. In solchen Foren sind auch Menschen (bzw. deren Maschinen) aktiv, die keine guten Absichten hegen. Und mit den zahllosen gestohlenen Identitäten finden sie zu den meisten Plätzen leicht Zugang und sind dabei sogar getarnt.

Aber es ist nicht unbedingt notwendig den Schadcode auf einem Server zu platzieren. Schon der Link auf beliebige Webseite kann den Schadcode enthalten, der dann auf der Zielseite ausgeführt wird. Diesen Angriff bezeichnet man als Cross Site Scripting (XSS). XSS ist immer dann möglich, wenn die Eingaben eines Nutzers auf einer Folgeseite wieder angezeigt werden und die Eingabe nicht auf ausführbare Inhalte geprüft wird. Wenn z.B. der Name aus einem Formular in der folgenden Bestellung wieder angezeigt wird, ist das durchaus nützlich. Wenn ein Angreifer anstelle seines Namens aber JavaScript-Code eingibt, so wird der - sofern er nicht ausgefiltert wird - vom Browser ausgeführt. Ein Beispiel für Cross Site Scripting: Ein Formular

verlangt nach einem Namen. Anstelle seines Namens gibt der Angreifer folgenden Code ein:

```
<SCRIPT>alert(„You're pwned“)</SCRIPT>
```

Nach dem Abschicken des Formulars wird dieser Code auf der Folgeseite nicht dargestellt, sondern ausgeführt. Im vorliegenden Fall erscheint eine Warnmeldung. Ein echter Angriff enthält gefährlicheren Code.

Aber selbst wenn die Formulareingaben gefiltert werden, kann man den Schadcode direkt in den Link der aufgerufenen Seite schreiben. Etwa so:

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert(“You're pwned“)</SCRIPT>
```

Ein solcher Link kann sich hinter jedem Text verstecken, der in einem Forum oder Blog hinterlegt wurde. Noch perfider ist es aber, wenn solche XSS-Links in den Suchergebnissen von Google erscheinen. Die Malwareautoren optimieren korruptierte Blogeinträge für die Suchroboter von Google und mit ein paar Verschleierungstricks gelingt dies auch immer wieder, obwohl Google mit viel Aufwand versucht solche XSS-Links aufzuspüren und aus den Suchergebnissen zu eliminieren.

Ähnlich ist es auch mit den vielen neuen Möglichkeiten, die Web 2.0 bietet. Wer angesichts der Bedrohungslage auf die Idee kommt, dass es nützlich sein könnte, aktive Inhalte oder Skriptsprachen im Browser nicht mehr zuzulassen, sperrt sich damit aus der schönen neuen Welt des Web 2.0 mit seinen unzähligen Möglichkeiten aus. Eine Vielzahl dieser neuen Funktionen bietet aber auch Potenzial für Missbrauch und erhöht die Menge möglicher Sicherheitslücken. Der XSS-Wurm von Samy verschaffte sich Ende 2005 bei Myspace per Cross-Site-Scripting (XSS) innerhalb von 18 Stunden mehr als eine Million Freunde. Cross-Site-Scripting als Gefahr wird aber nach wie vor unterschätzt.

Schadcode verbreitende Domains findet man also nicht nur in den düsteren Ecken des Internets, in beliebten Download-Portalen (z.B. Rapidshare) und auf gecrackten Internet-Pages, sondern auch auf legitimen Webseiten und in Google-Suchergebnissen. Fazit: Im Prinzip kann auf jeder Webseite Schadcode lauern.

4. Ablauf einer typischen Infektionswelle

Die Durchführung einer Attacke durch Cyber-Kriminelle erfolgt in der Regel nach einem charakteristischen Muster. Eine typische Infektion hat sich im Laufe der letzten Jahre stark gewandelt. Würmer wie NetSky und MyDoom hatten große Dateianhänge, die monolithische Schadsoftware mit vielen integrierten Funktionen enthielten. Daraus sind in den letzten Jahren viele kleine, kompakte und hochspezialisierte Module geworden, die je nach Bedarf flexibel nachgeladen werden. Die Infektion läuft in mehreren Phasen ab. Nachdem der jeweilige Schädling vorbereitet und die potenziellen Opfer ausgewählt wurden, erfolgt der eigentliche Angriff. Anschließend können die infizierten Systeme, die fortan unter der Kontrolle des Angreifers stehen, für nahezu beliebige kriminelle Aktivitäten missbraucht werden.

4.1 Vorbereitung der Infektion

Zunächst muss der Schädling, den man verbreiten will, entwickelt werden. Das muss aber nicht bei jeder Infektionswelle aufs Neue geschehen. Hat der Malware-Autor einmal einen Schadcode entwickelt, kann er von dieser Vorlage mit Hilfe von Laufzeitpackern, anderen Compilern und Tools zur Verschleierung von Code für verschiedene Wellen so lange neue Varianten erstel-

len, bis sie von den gängigsten AntiViren-Programmen nicht mehr erkannt werden. Wenn der Schadcode vorsieht, dass der Virenschanner auf infizierten Rechnern erkannt wird, dann reicht es aus sicher zu stellen, dass für die gängigsten Virenschanner eine nicht erkannte Version des Schädling vorliegt. Wer dies nicht selber tun möchte, findet in entsprechenden Untergrundforen Leute, die entsprechende Dienstleistungen mit Garantie zu lukrativen Preisen anbieten.

Liegt der Schädling dann vor, muss sich der Angreifer für einen (oder mehrere) Verbreitungswege entscheiden. Beispielsweise kann er den Schädling durch einen automatisch durchgeführten Angriff auf eine Sicherheitslücke durchführen. In diesem Fall bemerkt das Opfer nichts von dem Angriff bzw. der Infektion. Er kann aber auch eine der üblichen Betrugsmaschen wählen, um den Nutzer selbst dazu zu bringen, den Schädling zu starten. Im ersten Fall braucht der Angreifer dann einen Exploit, der den Rechner kapert, im zweiten Fall eine Webseite und/oder eine verführerische E-Mail beziehungsweise Instant Message, die den Nutzer zum Download und zur Ausführung der Datei veranlassen. Wenn der Schädling auf einer Webseite gehostet werden soll, müssen die Domains registriert werden und die passenden Dateien dort hinterlegt werden. Für die meisten dieser Aktivitäten gibt es einfach zu bedienende Tools.

4.2 Durchführung

Nach der Übernahme des Rechners wird meist ein Trojan-Downloader gestartet. Dieser sorgt dafür, dass die schädlichen Dateien auf den Rechner gelangen und gestartet werden. Zunächst wird der Urheber der Attacke über den Erfolg der Infektion und über das gekaperte System informiert. Dann werden die Sicherheitseinstellungen des infizierten PCs heruntergefahren. Der Rechner ist somit den weiteren Aktivitäten der Malware schutzlos ausgeliefert. Im nächsten Schritt wird dann weitere Malware auf den Rechner geladen. Für die Ausführung dieser Schritte können mehrere Schaddateien genutzt werden.

In vielen Fällen ist die erste Schaddatei, die nachgeladen wird, eine Backdoor, die z.B. mit einem Rootkit versteckt wird und daher unbemerkt im Hintergrund läuft. Durch diese Hintertür bekommt der infizierte Rechner einen neuen Besitzer, der nun nach Belieben mit dem Rechner agieren kann. Die Backdoor erlaubt es unter anderem, den Rechner per IRC, P2P oder HTTP mit vielen anderen PCs weltweit zu koordinieren. So wird der Computer Teil einer mitunter riesigen Zombie-Armee. Nach der Installation der Backdoor wird das infizierte System genauer inspiziert und der Angreifer entscheidet, was er mit dem Rechner anfangen will. Die gecrackten Rechner werden mit Spyware nach verwertbaren Daten durchsucht und/oder mit Adware ausgestattet. Wenn der Rechner über eine gute Anbindung ins Internet verfügt, kann er zum Versand von Spam verwendet werden, illegale Dateien zum Download anbieten oder Phishing- bzw. Malware-Webseiten hosten.

4.3 Den infizierten Rechner benutzen

Wenn die Zombie-Rechner eines Botnetzes zum Versand von Spam genutzt werden sollen, spielt der Botnetz-Betreiber per Backdoor ein Malware-Paket auf dem infizierten Rechner auf, das unter anderem die Mail-Vorlage, eine Liste mit Mailadressen und die Software zum Versand der Mails enthält. Wenn diese Datei eingerichtet ist, wird sie gestartet und der Versand beginnt. Nachdem alle Mails verschickt sind, löscht sich die Software mit allen Daten vom Rechner. Nur die Backdoor bleibt - gut versteckt - zurück und wartet auf weitere Befehle.

5. Wie man sich schützen kann

Der Schutz von Firmenrechnern vor Malware ist nur ein Bereich der IT-Sicherheit, den man immer zur gesamten IT-Sicherheit eines Betriebs in Relation setzen muss. IT-Sicherheit ist kein Zustand, sondern ein Prozess. In jedem Unternehmen sind bestimmte Benutzergruppen oder Bereiche besonders gefährdet und brauchen speziellen Schutz. In diesem Prozess muss jedes einzelne Unternehmen in vielerlei Hinsicht Entscheidungen treffen, die zu ganz individuellen Lösungen führen.

Zunächst verbindet man mit Schutz vor Malware den Einsatz von technischen Verfahren, die gegen die definierten Gefährdungen schützen (sollen). Die wichtigsten technischen Maßnahmen sind:

- **Virenschutz**
Sollte sowohl auf Servern als auch auf Clients installiert werden. Dieser sollte zudem den HTTP-Datenstrom und gegebenenfalls die Daten aus Chats (ICQ, IRC) auf Schadcode prüfen.
- **Spamschutz**
Da E-Mails anstelle der Dateianhänge nur noch Links auf schädliche Webseiten enthalten, wird der Spamschutz gleichzeitig zum Malwareschutz.
- **Firewall, Intrusion Detection/ Prevention**
Daten aus dem Netzwerk-Traffic können dazu genutzt werden, gängige Angriffe von Internet-Würmern zu entdecken und zu verhindern.

Aber auch andere technische Maßnahmen tragen zum Virenschutz bei. Patch Management, Virtualisierung von Software, Nutzerrechte auf Firmenrechnern, Zugangskontrollen für Dateien und Netzwerkbereiche sowie viele weitere Vorkehrungen ergänzen die offenkundigen Sicherheitsmaßnahmen. Auf die einzelnen Möglichkeiten kann und soll hier nicht näher eingegangen werden. Das IT-Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bildet hier eine umfassende Quelle.

Leider reichen technische Maßnahmen nicht aus, um das Netzwerk eines Unternehmens wirkungsvoll zu schützen. Die Sicherheitsmaßnahmen müssen von den Mitarbeitern akzeptiert und getragen werden. Den Rahmen hierfür liefern mit der Geschäftsleitung abgestimmte Richtlinien für den Umgang mit Computern, Datenträgern und anderen sicherheitsrelevanten Informationen. Dabei sind rechtliche und ethische Rahmenbedingungen zu berücksichtigen. Die Schutzmaßnahmen müssen sich in der Struktur der Organisation widerspiegeln. Beispielsweise sollten Verstöße gegen die Richtlinien auch mit Sanktionen belegt sein. Last not least sollten alle Mitarbeiter über Gefahrenquellen im Internet und im Berufsalltag informiert werden. Wenn aufmerksame Mitarbeiter die technischen Maßnahmen ergänzen, kann es gelingen die Rechner eines Unternehmens frei von Malware zu halten.