TEC WORKSHOP

Link: https://www.tecchannel.de/a/conficker-das-groesste-botnet-aller-zeiten,1986704

Grundlagen, Hintergrund und Information

Conficker - das größte Botnet aller Zeiten

Datum: 05.01.2010
Autor(en): Moritz Jäger

Der Conficker-Wurm hat innerhalb kürzester Zeit Millionen von Computer-Systemen infiziert - unbemerkt von Anwendern und Administratoren. TecChannel erklärt, warum die Malware so erfolgreich ist und wie Sie Conficker finden und entfernen.

In der IT-Industrie hatte sich die Meinung verbreitet, dass die Zeiten **der großen Infektionen**[1] wie „I Love you“ im Jahr 2000 vorbei seien. Dennoch tauchen immer wieder Malware-Produkte auf, die sehr erfolgreich und innerhalb kürzester Zeit eine unglaubliche Anzahl an Systemen infizieren. Ein solches Beispiel war der **Storm Wurm**[2]. Ein anderes Exemplar dieser Gattung ist der Wurm Conficker.

Seit **Ende 2008**[3], das erste Auftreten wurde am 21. November 2008 registriert, verbreitet sich diese Malware wie ein Lauffeuer. Inzwischen gibt es drei entdeckte Hauptvarianten und unzählige kleinere Modifikationen. Vorsichtigen Schätzungen zufolge hat der Wurm **bereits Millionen Systeme infiziert**[4] und seinem Botnet einverleibt. Allerdings ist immer noch unklar, wozu diese Armee an Zombie-Rechnern dienen soll. Derzeit hat noch keine Antivirenfirma eine Attacke auf das Botnet zurückführen können.

Was ist also so besonders an diesem Wurm, dass **Microsoft**[5] sogar eine **Prämie von 250.000 Dollar**[6] auf die Ergreifung der Hintermänner ausgesetzt hat?

[Hinweis auf Bildergalerie: **Bildergalerie: Conficker.**] gal1

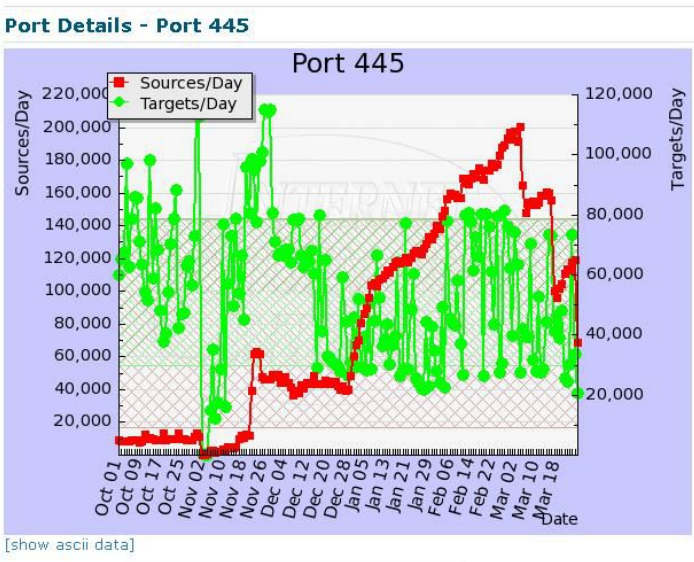
Dieser Artikel soll Ihnen die Hintergründe und Informationen rund um Conficker liefern. Im Beitrag werden wir für diese Malware durchgehend den Namen Conficker verwenden, auch wenn der Wurm von unterschiedlichen Antivirenherstellern anders getauft worden ist. Die folgende Tabelle zeigt Ihnen die Alias-Namen, unter denen der Wurm im Netz noch zu finden ist:

Andere Namen für Conficker

F-Secure	**Downadup.gen**[40]
Kaspersky	**Kido**[41]
Symantec	**Downadup**[42]
Trend Micro	**Downad**[43]

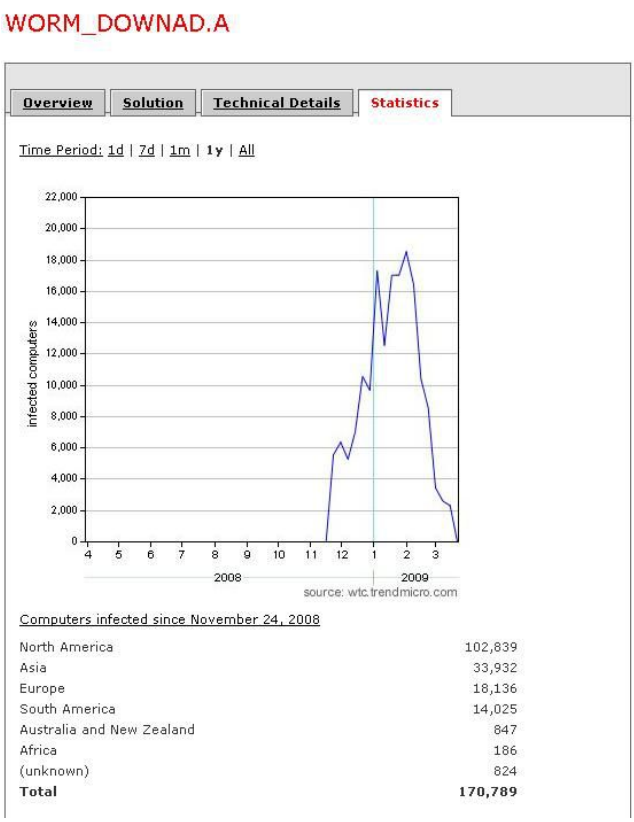
1. Wie konnte sich Conficker so schnell ausbreiten?

Die erste Version von Conficker wird am 21. November 2008 entdeckt. Der Wurm setzt auf **MS08-067**[7], eine ältere Schwachstelle im Windows-Server-Service. Conficker prüft über Port 445, ob das Zielsystem von der Schwachstelle betroffen ist. Trifft dies zu, dringt der Wurm in das System ein. Nach erfolgreicher Installation startete er einen HTTP-Server, der einen zufällig gewählten Port nutzt. Anschließend schickt sich der Wurm an neue Rechner.



Massiver Anstieg: der Traffic auf Port 445 seit Oktober 2008. (Quelle: SANS)
Foto: Firma

Ist ein neuer Rechner infiziert, verbindet sich dieser mit dem eben erstellten Webserver und lädt weitere Daten nach. So kann sich Conficker innerhalb kurzer Zeit massiv ausbreiten. Dieser verteilte Ansatz machte eine Unterbrechung der Infektionskette nahezu unmöglich, denn es erscheinen ständig neue Versionen des Wurms mit verändertem Hashwert, was viele signaturbasierte Sicherheitslösungen aushebelt.

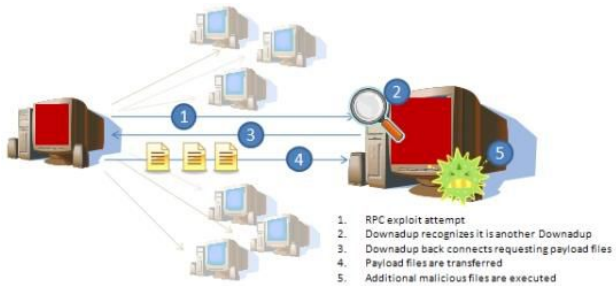


Infektion: die gefundenen Infektionen mit der ersten Version von Conficker. (Quelle: Trend Micro)
Foto: Firma

Ist ein System infiziert, generiert Conficker pro Tag 250 Web-Adressen. Der Wurm verbindet sich anschließend mit diesen Domains und sieht nach, ob dort neue Anweisungen vom Botmaster warten. Ist dies der Fall, lädt Conficker die zusätzlichen Informationen herunter und führt sie aus. Über diesen Mechanismus kann sich der Wurm beispielsweise aktualisieren.

Der Algorithmus, nach dem die Domains erstellt werden, konnte von Virenexperten relativ schnell ausgehebelt werden. F-Secure beispielsweise stellte r**egelmäßig aktualisierte Listen bereit**[8], in denen die entsprechenden Domains hinterlegt waren. Zusätzlich registrierte sich das Antivirenlabor einige dieser Domains und konnte so die Verbindungen zählen. Im Januar waren laut F-Secure etwa 2.395.000 Rechner infiziert, wobei das nur eine grobe Schätzung ist.

Doch der Download von Inhalten von zufällig erzeugten Domänen ist nur eine Methode, mit der Conficker an neue Inhalte kommt. Als zweiten Verbreitungsweg verfügt Conficker über ausgefeilte P2P-Funktionalitäten.



P2P: die Funktionsweise einer Peer-to-Peer-Infektion. (Quelle: Symantec)
Foto: Firma

Während der Wurm seine Instruktionen über P2P erhält, sichert er den befallenen PC zusätzlich ab. Conficker patcht MS08-067, die Schwachstelle, die der Wurm selbst zur Verbreitung nutzt. Künftig überwacht Conficker diesen Patch, um eingehende Angriffe zu analysieren. Ist der Code des Angriffs identisch mit dem von Conficker, kann der Wurm die angreifende Maschine auslesen und sich bei dieser anmelden. Das kontaktierte System wiederum antwortet mit zusätzlicher Payload, um die sich Conficker erweitert.

2. Mutation: Conficker.B nutzt USB-Speichermedien

Am 30. Dezember erscheint Conficker.B. Zunächst scheint es so, als hätten die Entwickler lediglich die Adressgenerierung verändert. Eine genauere Analyse offenbart aber einen völlig neuen Verbreitungsweg und zusätzliche Abwehrmechanismen. Statt nur noch auf anfällige Server zu zielen, kopiert sich Conficker.B nun auch auf angeschlossene USB-Speichergeräte und erstellt eine neue Startdatei „Autorun.inf“.

Gefälscht: der Autoplay-Bildschirm, wie ihn Conficker darstellt. (Quelle: Microsoft)
Foto: Firma

Diese ist von einem normalen Autostartdialog kaum zu unterscheiden. Klickt man allerdings auf „Open Folder to view Files“, wird der Wurm ausgeführt, der sich dann entsprechend im System einnisten kann.

Zusätzlich bringt das Wurm-Update eine weitere Gemeinheit mit: Conficker.B überprüft die DNS-Anfragen auf befallenen Rechnern und blockiert bestimmte Websites mit einem Timeout. Davon betroffen sind beispielsweise Webseiten und Patch-Dienste von Antivirenherstellern oder der Update-Service von Microsoft. Infizierte Rechner können dadurch keine Patche mehr herunterladen oder ihre Virensignaturen aktualisieren.

3. Unauffällige Netzwerk-Scans mit Blacklists

Im Verbreitungsweg gibt es noch eine Neuerung: Auf der Suche nach neuen Opfern setzt Conficker Netzwerk-Scan-Funktionen ein. Frühere Würmer haben diese Technik oft übertrieben, sodass es deutlich merkbare Einbußen bei der Geschwindigkeit gab. Conficker dagegen geht einen anderen Weg: Die Malware misst die durchschnittliche Netzwerkgeschwindigkeit des befallenen Systems, indem sie mehrere Webseiten kontaktiert und die Antwortzeiten misst.

Anschließend nutzt der Wurm die Werte, um die durchschnittliche Geschwindigkeit des befallenen Rechners im Netzwerk zu berechnen. Anschließend beginnt Conficker mit einem Netzwerk-Scan, um anfällige Rechner im lokalen Netz zu finden. Nach jedem Scan legt er dabei eine Pause zwischen 100 Millisekunden und zwei Sekunden ein. Durch diese Methode bemerken nur wenige Nutzer eine Verschlechterung der Geschwindigkeit. Conficker scannt auf diese Weise sämtliche Adressen aus dem aktuellen IP-Netz. Ist er damit fertig, greift er zufällige Adressen an. Reservierte Blocks, etwa 127.x.x.x, lässt die Malware aus.

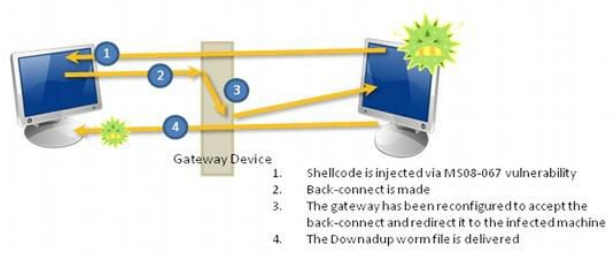
Die Entwickler beweisen zudem eine große Weitsicht. Jede Kopie des Wurms trägt eine Blacklist bei sich. Darauf sind die bekannten IP-Adressen von Anti-Malware-Organisationen eingetragen, etwa BitDefender, CERT, CA oder Symantec. Der Gedanke dahinter ist, dass sich der Wurm so verbreiten kann, ohne dass er in Honeypot-Netzen der Antivirenfirmen landet. Außerdem nutzt Conficker diese Listen, um Download-Anfragen von diesen IPs abzulehnen. Dadurch wird es für die Sicherheitsfirmen schwerer, an Code des Wurms zu kommen. Eine ähnliche Taktik nutzte bereits der **Storm Wurm**[9].

4. UPnP und Brute Force als Hilfsmittel

Router[10] stellen für viele Würmer ein nicht zu unterschätzendes Problem dar. Denn per **NAT**[11] teilen sie meist das private LAN von einem öffentlichen Netz. Dadurch können sich externe Systeme nicht ohne Weiteres mit lokalen Rechnern verbinden. Vor allem im Heimumfeld schafft das eine nicht zu unterschätzende Barriere. Conficker hat allerdings auch hier einen Weg gefunden: Der Wurm nutzt einfach den Standard Universal Plug and Play. Er ist heutzutage in den meisten Routern und Betriebssystemen vorhanden und aktiviert.

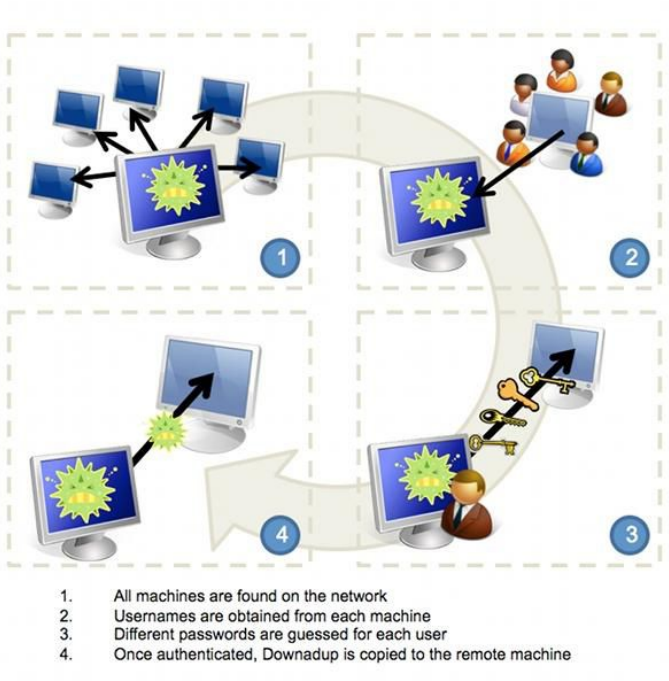
UPnP[12] ermöglicht es Geräten, andere Systeme im Netzwerk ohne einen zentralen Server zu finden. Außerdem kann ein System dadurch automatisch die benötigten Ports am Gateway öffnen lassen und Anfragen aus dem Netz an das entsprechende lokale System weiterleiten.

Per UPnP findet Conficker den lokalen Gateway. Diesem teilt der Wurm mit, dass er einen bestimmten Port öffnen und weiterleiten soll. Über diesen Port findet anschließend die komplette Kommunikation mit anderen infizierten Rechnern statt.



Umgebogen: Mittels UPnP kann Conficker nahezu unbemerkt mit der Außenwelt kommunizieren. (Quelle: Symantec)
Foto: Firma

Im LAN verwendet der Wurm noch eine weitere Technik, um sich fortzupflanzen. Dazu kopiert er sich über die administrative Netzwerkfreigabe „$ADMIN“ von Windows-PC zu Windows-PC. Meistens benötigt der Wurm dazu allerdings einen gültigen Benutzernamen samt Passwort. In einem ersten Versuch probiert Conficker die Zugangsdaten des aktuell angemeldeten Nutzers aus. Sind diese ungültig, weicht der Wurm auf einen **Brute-Force-Angriff**[13] aus.



Passwort-Brecher: Conficker versucht, in geschützte Netzwerkfreigeben einzudringen. (Quelle: Symantec) Foto: Firma

Dazu **testet Conficker**[14] mehr als 250 allgemeine Kombinationen, etwa „Admin Admin“, „password“ oder „1234“. Findet der Wurm eine passende Kombination, kopiert er sich über die administrativen Rechte in den Ordner System32. Anschließend erstellt er einen zeitgesteuerten Auftrag, der die soeben kopierte Datei ausführt. Diesen Vorgang wiederholt Conficker alle 40 Minuten.

5. Gesicherte Kontrolle durch Verschlüsselung und Signatur

Im Blog des **Symantec Security Response Teams**[15] tauchte eine interessante Frage auf: Wenn die Domains, von denen Conficker neue Instruktionen abruft, bekannt sind, was hindert andere Malware-Gangs oder die Sicherheitsindustrie daran, das Botnet zu übernehmen? Die Antwort ist einfach: ein passender Schlüssel samt Signatur.

Die Malware-Autoren haben diese Möglichkeit anscheinend seit Conficker.B in Betracht gezogen und entsprechende Gegenmaßnahmen ergriffen. Jede Payload, die Instruktionen für den Wurm enthält, ist mit der Technologie RC4 verschlüsselt. Der eigentliche Key ist dabei 64 Byte lang. Allerdings entschlüsselt Conficker die Daten nur, wenn sie mit einer passenden 4096 Bit langen Signatur gekennzeichnet sind.

Diese Signatur erinnert laut Symantec an den **RSA-Schlüssel**[16]. Die Analyse des entsprechenden Codes zeigte noch eine andere Besonderheit: Die Macher von Conficker sind sehr darauf bedacht, keinerlei Pufferüberläufe zu erzeugen, erlauben sich also keine Schwachstelle in ihrer verschlüsselten Übertragung.

6. Conficker.C – besser, härter, gemeiner

Die dritte aktuelle Variante von Conficker ist Version C. Erstmals entdeckt wurde diese Variante des Wurms im März 2009. Die neue Variante scheint weniger auf die Weiterverbreitung ausgerichtet zu sein, sondern soll das bestehende Botnetz anscheinend absichern. Unterstrichen wird diese Vermutung unter anderem durch die Tatsache, dass Conficker.C keinerlei zusätzliche Verbreitungsanstrengungen unternimmt. Um die befallenen Systeme zu sichern, bedient sich der Wurm mehrere Taktiken.

Conficker.C ist deutlich aggressiver im **Umgang mit Sicherheitstools**[17]. Die neue Variante sucht auf den befallenen Systemen aktiv Strings oder Prozesse, die auf ein Sicherheitstool hinweisen. Entdeckt der Wurm ein solches Programm, etwa Wireshark oder ein Anti-Virus-Tool, sendet Conficker.C ein Kill-Signal an den Prozess.

Zusätzlich haben die Entwickler auf die Entdeckung ihres Domain-Algorithmus reagiert. Die neue Conficker-Variante erzeugt keine 250 Domains mehr pro Tag, sondern 50.000 Domain-Namen. Aus diesen pickt sich der Wurm 500 Stück aus, die er dann zu kontaktieren versucht.

Die dritte Neuerung ist, dass die Conficker-Schreiber den Wurm gegen weitere Angriffe abhärten. Dazu wurden sowohl die HTTP-Infektionswege als auch die Verbindungen über P2P abgesichert und gegen Übernahmen geschützt. Die Tabelle zeigt die Unterschiede der drei Conficker-Varianten:

Wurm-Version	Conficker.A	Conficker.B	Conficker.B
Verbreitung	MS08-067	MS08-067 Brute-Force-Angriffe auf Netzwerk-Freigaben Verbreitung über USB-Medien	Verbreitungsmechanismen entfernt
Kontrolle	HTTP-Verbindungen 250 generierte Domains	HTTP-Verbindungen einfaches P2P 250 generierte Domains	verbesserte HTTP-Verbindungen verbessertes P2P 50.000 generierte Domains

Schutzfunktionen keine	einige DNS-Lookups werden unterbrochen, Auto-Update wird unterbrochen, HTTP- und P2P-Code signiert	einige DNS-Lookups werden unterbrochen, Auto-Update wird unterbrochen, Sicherheitsprozesse werden beendet, erweiterte Funktionen gegen Analyse-Maßnahmen, HTTP- und P2P-Code signiert

7. Neu: Conficker D und E

Die Entwickler der Malware waren 2009 nicht untätig. Nachdem Conficker.C verteilt war, folgten die Varianten Conficker.D und **Conficker.E**[18]. Beiden ist gemeinsam, dass sie deutlich mehr auf die Verteilung über P2P-Netzwerke setzen. Außerdem haben die Macher Maßnahmen gegen Anti-Viren-Programme deutlich verschärft. Beide Malware-Varianten prüfen die laufenden Prozesse auf Anti-Malware-Programme und schicken den jeweiligen Prozessen im Abstand von einer Sekunde einen Kill-Befehl. Die Befehle zielen dabei nicht nur Anti-Viren-Programme, sondern auch auf Patch- oder Diagnose-Programme. Wie schon zuvor manipuliert die Malware den DNS Lookup sowie die Auto-Update-Funktion von Windows. Conficker.E nutzte zur Verbreitung auch wieder die NetBIOS-Schwachstelle aus MS08-067, Conficker.D verzichtete darauf.

Im Video von **Symantec**[19] erklärt der Forscher Ben Nahorney wie die verschiedenen Versionen von Conficker zusammenarbeiten und wie der Update-Vorgang abläuft.

Wurm-Version	Conficker.D	Conficker.E
Verbreitung	Keine lokale Updates über P2P und HTTP	NetBIOS (MS08-067) Updates über P2P und HTTP
Update und Anweisungen	HTTP: Wurm prüft täglich 500 von 50000 generierten Domains P2P: Wurm scannt per UDP, erhält Anweisungen und Updates über TCP	NetBIOS-Push: Wurm prüft das lokale Netzwerk auf anfällige Hosts, patcht notfalls MS08-67 um eine erneute Infektion zu ermöglichen P2P: Wurm scannt per UDP, erhält Anweisungen und Updates über TCP
Schutzfunktionen	DNS-Lookups werden unterbrochen und im Speicher manipuliert, Auto-Update wird unterbrochen, Safe-Mode wird deaktiviert, Sicherheitsprozesse werden beendet	DNS-Lookups werden unterbrochen, Auto-Update wird unterbrochen, Sicherheitsprozesse werden beendet

8. Update: 1. April 2009 - Viel Hype um nichts

Wie bereits eingangs erwähnt, haben die drei Conficker-Varianten bislang wenig unternommen. Zuerst hat sich der Wurm massiv verbreitet, anschließend wurden die befallenen Systeme gesichert. Durch den Algorithmus konnten Malware-Analysten herausfinden, dass sich Conficker am 1. April 2009 neue Informationen holt. An diesem Datum erzeugte Conficker.C pro Tag 50.000 Domainnamen und prüfte anschließend bei 500 Domains, ob dort neue Anweisungen oder Programm-Updates vorlagen.

Tatsächlich erschienen neue Versionen von Conficker - allerdings erst Tage nach dem eigentlich angekündigten Termin. Außerdem unterschied sich die Verbreitung deutlich vom früheren Vorgehen. Vor allem die Verbreitung über P2P wurde von den Kriminellen genutzt.

Diverse Unternehmen haben versucht, die Reaktionen des Wurms nachzustellen. Allerdings war dies nicht so einfache, da Conficker die aktuelle Systemzeit mit mehreren Webseiten abgleicht. Zudem waren im Wurm selbst noch keine Payload oder Anweisungen vorhanden.

9. Neu: Geld verdienen mit Waldac und Scareware

Noch immer im unklaren ist, was die Hintermänner von Conficker eigentlich mit der enormen Anzahl von infizierten Zombie-PCs, im Dezember waren es mehr als sieben Millionen einzigartige IPs, anstellen möchten. Seit April 2009 wurde das Conficker-Netzwerk zweimal auffällig. Beide Male wurden die infizierten Rechner anscheinend an andere kriminelle Netzwerke ausgeliehen.

Das erste Mal arbeite das Conficker-Netzwerk anscheinend mit der Waledac-Gruppe zusammen. Conficker wurde dabei unter anderem Rechner nachgeladen, die mit Waledac infiziert waren. Anscheinend wurden beide Systeme für den Versand von Spam-Mails genutzt. Waledac steht übrigens im Verdacht, Verbindungen zur **Gang des Storm-Wurms**[20] zu haben.

Das zweite Mal sollte Conficker wahrscheinlich **direkt Geld verdienen**[21]. Dazu kooperierte die Malware mit den Hintermännern der Scareware „SpyProtect 2009“. Die Software arbeitet Rouge-AV-Programm, spiegelt dem Nutzer eines infizierten Systems also vor, dass er mit diversen Viren infiziert sei. Der erste Scan ist dabei kostenlos, will der Nutzer allerdings, dass sein System bereinigt wird, muss er dafür die Vollversion kaufen. Zu Beginn wurden diese Programme noch relativ günstig verkauft, inzwischen haben die Hintermänner die Preise deutlich erhöht.

[Hinweis auf Bildergalerie: **Bildergalerie: Scareware.**] gal2

10. Update: Gegenmaßnahmen und Reinigung

Neben dem Kopfgeld auf die Programmierer von Conficker hat Microsoft eine Reihe von Maßnahmen online gestellt. Erste und wichtigste Gegenmaßnahme ist die Installation des **Updates MS08-067**[22] auf jedem Rechner im Netzwerk. Wichtig ist auch, dass Sie die Autorun-Funktionen von USB-Geräten deaktivieren. Falls Sie keine passende Managementsoftware oder Gruppenrichtlinien verwenden, müssen Sie dazu den Registry-Schlüssel „NoDriveTypeAutoRun“ ändern. Die offizielle Anleitung dazu finden Sie **hier bei Microsoft**[23]. Zusätzlich empfiehlt sich das **Update der KB967940**[24]. Anschließend sollten Passwörter geändert werden, wobei starke Passwörter in jedem Fall vorzuziehen sind.

Die Entwickler der Sicherheitstools **Nmap**[25] und **Nessus**[26] können das überwachte Netzwerk ebenfalls auf eine Conficker-Infektion überprüfen. Bei Nessus geschieht das über das Plugin „**Conficker P2P Service Detection**[27]“, Nmap hat das passende Script namens „**smb-check-vulns.nse**[28]“ in der aktuellen Version bereits installiert.

Jeder Rechner sollte unbedingt mit einem aktuellen Virusscanner geprüft werden. Womöglich sollten Sie dabei Live-CDs nutzen, um eine Beeinflussung durch den Wurm zu verhindern. Ratsam ist in jedem Fall, auch die geplanten Tasks zu prüfen, ob sich dort auffällige Einträge finden.

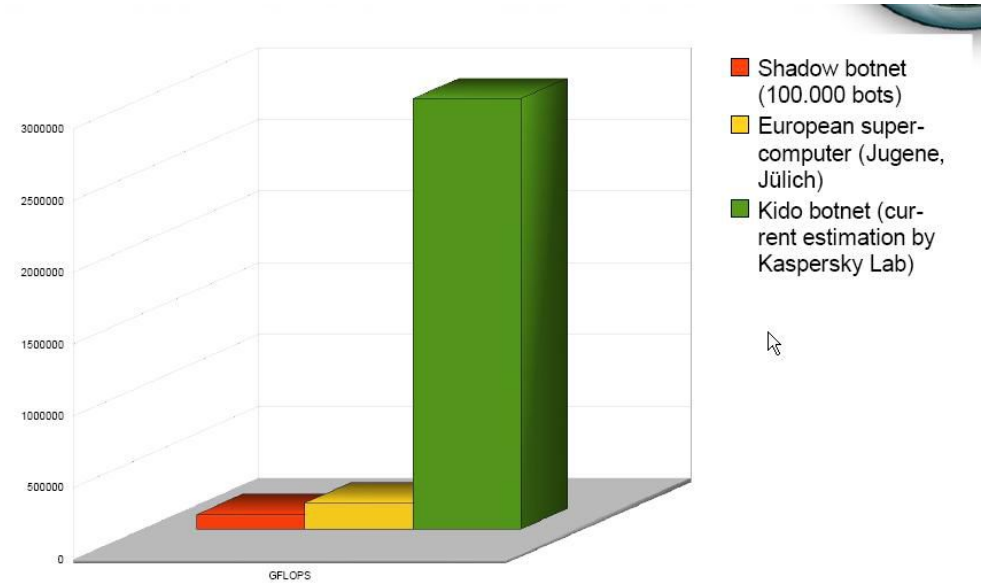
Sollten Sie eine Infektion feststellen, ist es wichtig, die jeweiligen Systeme vom Netzwerk zu trennen. Anschließend können Sie entweder einen Virenscanner oder dedizierte Programme der Anti-Malware-Forscher nutzen.

11. Neu: Fazit

Conficker bleibt ein Mysterium. Die Malware schlug hohe Wellen, sowohl bei den Medien wie auch bei den Viren-Analysten. Doch hinter den Kulissen arbeiten die Entwickler fleißig weiter an Verbesserungen der Malware. Dennoch ist noch immer unbekannt, was die Software eigentlich erreichen soll.

Möglich sind mehrere Szenarien. Conficker könnte lediglich als Proof-of-Concept oder Versuchsumgebung dienen, mit der neue Technologien, Infektionswege und Abwehrmaßnahmen gegen die Anti-Viren-Industrie getestet werden. Dafür würde sprechen, dass 2009 einige extrem erfolgreiche Malware-Familen, etwa Koobface oder **URLzone**[29] ihr Unwesen trieben.

Die Szenarien reichen von Distributed-Denial-of-Service-Angriffen auf ganze Länder bis hin zu einem Aprilscherz. Ein anderer Ansatz ist, dass das Botnetz für einen groß angelegten Betrug genutzt wird, indem die Bot-Armee **auf bestimmte Affiliate-Links**[30] angesetzt wird.



Supercomputer: Die geschätzte Rechenpower von Conficker (Quelle: Kaspersky)
Foto: Firma

Andererseits könnten die Hintermänner auch einfach nur abwarten, bis die Zeit gekommen ist. Oder sie nutzen die enorme Rechenkapazität bereits jetzt, um andere Dienste anzubieten. Denn ähnlich wie etwa beim SETI-Projekt würde sich diese Menge an Rechenzeit beispielsweise hervorragend rechenintensive Anwendungen wie etwa das Knacken von Passwörtern oder Codes eignen. Für Letzteres gibt es allerdings keinerlei Hinweise.

Andere Experten warnen vor Panikmache. Conficker habe eine Menge Aufsehen in den Medien weltweit erregt, daher würden die Besitzer des Botnets von einer Aktivierung abschrecken. Ziel von solchen Netzen sei, dass sie möglichst unauffällig agieren, um unerkannt ihre Aufgaben zu verrichten. (mje)

12. Anhang: Quellen und Lesehinweise

Von einem technischen Standpunkt aus betrachtet ist der Wurm so interessant, dass sich diverse Analytik-Teams mit ihm beschäftigen. Hier möchten wir Ihnen eine Linksammlung zur Verfügung stellen, in der Sie detaillierte Analysen und Kommentare von Firmen und IT-Experten zu Conficker finden:

Symantec: **Downadup Motivations**[31]; **The Downadup Codex (PDF)**[32]

Sophos: **Cleanup-Tool (Netzwerk-Version)**[33]; **Conficker Call-home Protocol v2**[34]

SANS: **Sammlung mit Links zu Removal Tools und Informationen**[35] (wird laufend aktualisiert)

SRI: **Tiefgehende Analyse von Conficker.C**[36] inklusive schematischem Aufbau

Bruce Schneier: **Balancing Security and Usability in Authentication**[37]

ICAN: **Microsoft und Sicherheitsfirmen kooperieren im Kampf gegen den Wurm**[38]

Honeynet Project: **Know Your Enemy – Containing Conficker**[39]

Links im Artikel:

[1] **https://www.tecchannel.de/sicherheit/news/2021957/top_10_der_internet_malware_aller_zeiten/**
[2] **https://www.tecchannel.de/sicherheit/spam/1748581/report_der_sturmwurm_die_evolution_der_malware/**
[3] **https://www.tecchannel.de/sicherheit/news/1778797/neuer_wurm_stopft_windows_luecke/**
[4] **https://www.tecchannel.de/sicherheit/news/2024827/conficker_infiziert_sieben_millionen_pcs/**
[5] **http://www.microsoft.com/de/de/default.aspx**
[6] **https://www.tecchannel.de/sicherheit/news/1818063**
[7] **http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-067.mspx**
[8] **https://www.tecchannel.de/sicherheit/news/1781818/f_secure_stellt_blockliste_fuer_downadup_bereit/**
[9] **https://www.tecchannel.de/sicherheit/spam/1748581/**
[10] **https://www.tecchannel.de/netzwerk/lan/2023795/kaufberatung_der_richtige_router_fuer_kmu_smb_firmen/**
[11] **http://www.openbsd.org/faq/pf/de/nat.html**
[12] **http://www.upnp.org/**
[13] **https://www.tecchannel.de/sicherheit/spam/431419/brute_force_attacken_passwoerter_tools_angreifer_router_hash_rainbow/**
[14] **https://forums2.symantec.com/t5/Malicious-Code/Downadup-Locking-Itself-Out/ba-p/389837**
[15] **http://www.symantec.com/connect/blogs**
[16] **https://www.tecchannel.de/ueberblick/archiv/401930/kryptographie_grundlagen/**
[17] **https://www.tecchannel.de/sicherheit/news/1833604/**
[18] **https://www.tecchannel.de/sicherheit/news/2006671/f_secure_entdeckt_confickere_neue_variante_verbreitet_sich/**
[19] **http://www.symantec.com/de/de/index.jsp**
[20] **https://www.tecchannel.de/sicherheit/spam/1748581/report_der_sturmwurm_die_evolution_der_malware/**
[21] **https://www.tecchannel.de/sicherheit/news/2013190/conficker_macht_sich_ans_geld_verdienen/**
[22] **http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx**
[23] **http://support.microsoft.com/kb/967715**
[24] **http://www.microsoft.com/technet/security/advisory/967940.mspx**
[25] **https://www.tecchannel.de/netzwerk/management/2019857/portscanner_nmap_zenmap_workshop_udp_tcp_well_kown_ports/**
[26] **https://www.tecchannel.de/pc_mobile/linux/431420/schwachstellen_aufspueren_mit_dem_nessus_scanner/**
[27] **http://www.nessus.org/plugins/index.php?view=single&id=36217**
[28] **http://nmap.org/nsedoc/scripts/smb-check-vulns.html**
[29] **https://www.tecchannel.de/sicherheit/spam/2023265/malware_urlzone_raeumt_online_konten_ab/**
[30] **https://forums2.symantec.com/t5/Malicious-Code/Downadup-Motivations/ba-p/393335;jsessionid=8C3E44D7F056ED6D7A3954189BDA8C9F#A254**
[31] **https://forums2.symantec.com/t5/Malicious-Code/Downadup-Motivations/ba-p/393335;jsessionid=8C3E44D7F056ED6D7A3954189BDA8C9F#A254**
[32] **http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_downadup_codex_ed1.pdf**
[33] **http://www.sophos.com/support/knowledgebase/article/51416.html**
[34] **http://www.sophos.com/security/blog/2009/03/3484.html?_log_from=rss**
[35] **http://isc.sans.org/diary.html?storyid=5860&rss**
[36] **http://mtc.sri.com/Conficker/addendumC/**
[37] **http://www.schneier.com/blog/archives/2009/02/balancing_secur.html**
[38] **http://www.icann.org/en/announcements/announcement-2-12feb09-en.htm**
[39] **http://www.honeynet.org/papers/conficker/**
[40] **http://www.f-secure.com/v-descs/worm_w32_downadup_gen.shtml**
[41] **http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782844**
[42] **http://www.symantec.com/norton/theme.jsp?themeid=conficker_worm**
[43] **http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_DOWNAD.A**

Bildergalerien im Artikel:

[gal1] **Bildergalerie: Conficker.**[gal2] **Bildergalerie: Scareware.**
