Computerwürmer

am Beispiel des Conficker Wurms

Autor:
Rüdiger Trost

Presales Consultant
Ruediger.Trost@F-Secure.com

Zielstattstrasse 44
D-81379 München

FOM Fachhochschule für Oekonomie & Management
University of Applied Sciences

Hausarbeit, Berufsbegleitender Studiengang zum
Diplom-Wirtschaftsinformatiker (FH)

Inhaltsverzeichnis

Abkürzungsverzeichnis

CERT	**C**omputer **E**mergency **R**esponse **T**eam
DARPA	**D**efence **A**dvanced **R**esearch **P**rojects **A**gency
DLL	**D**ynamic **L**ink **L**ibrary
IRC	**I**nternet **R**elay **C**hat
MD-6	**M**essage **D**igest Algorithm **6**
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NAT	**N**etwork **A**ddress **T**ransaltion
P2P	**P**eer-**to**-**P**eer
SHA-1	**S**ecure **H**ash **A**lgorithm Version **1**

Abbildungsverzeichnis

1. Einführung in das Thema

1.1 Aufgabenstellung

Im Rahmen einer Seminararbeit im Fach Betriebsinformatik 2 wird im folgenden Dokument auf das Thema Computerwürmer im Allgemeinen und einige Beispiele eingegangen. Das Ziel der Arbeit ist es, einen Überblick zu verschaffen und Fakten zu Verhaltensweisen von Malware der Kategorie „Wurm“ zu bieten. Hierbei wird im Speziellen auf den Conficker Wurm eingegangen. Beim Conficker Wurm handelt es sich um einen aktuellen Fall, daher überwiegen in diesem Teil die Internetquellen den Literaturquellen.

1.2 Eingrenzung

Der Begriff Computerwurm wird oft in Verbindung mit anderer Malware, also Viren, Trojanern und Rootkits, verwendet. In dieser Arbeit wird nur am Rande auf diese anderen Arten von Malware eingegangen. Um vor allem die Funktionsweise von Würmern zu erläutern wird auch der Begriff Botnetz erklärt, welcher nicht zwingend nur mit dem Thema Wurm einhergeht, sondern durchaus auch im Kontext Virus und Trojaner zu finden ist.

2. Grundlagen

2.1 Was ist ein Wurm?

Dem RFC 4949 nach wird der Wurm als Computerprogramm, welches sich selbst vollständig auf einen anderen PC im Netzwerk verteilen kann, und dort Systemressourcen verbraucht definiert.[1] Der Wurm benötigt keinen Wirt wie z.B. ein Programm, sondern bringt alle Voraussetzungen für die Verbreitung selbst mit.
Erstmals aufgetaucht ist ein Wurm im Jahr 1988. Der Morris-Wurm legte durch Überlastung 10% des Internets lahm (6.000 von 60.000 Knoten). [2]
Obwohl der Morris-Wurm anfangs als Virus angesehen wurde[3], gilt er heute als der erste Wurm.[4] Als Reaktion auf diesen ersten globalen Teilausfall wurde das Computer Emergency Response Team (CERT)[5] vom U.S. Defence Advanced Research Projects Agency (DARPA) gegründet.[6]

2.2 Verschiedene Arten von Würmern

2.2.1 Netzwerkwurm

Ein Wurm kann über Schwachstellen im Betriebssystem ein System infizieren. Diese Schwachstellen findet ein Wurm selbstständig und nutzt sie mit Hilfe eines Exploits aus. Ein Exploit ist ein Programmcode, welcher gezielt Schwachstellen ausnutzt um Code einzuschleusen. Nach dem Ausnutzen des Exploits wird eine Kopie des Wurms auf den verwundbaren Rechner gespeichert, von wo aus der Wurm nach dem nächsten verwundbaren Rechner sucht.[7] Nicht nur verwundbare Systeme können mit einem Wurm infiziert werden, auch eine fehlerhafte Konfiguration der Netzwerkfreigaben kann dazu führen, dass der Wurm darauf gespeichert wird. Führt ihn dann jemand aus, kommt es zu einer Infektion trotz eingespielter Sicherheitsupdates.

---

[1] Vgl http://www.rfc-editor.org/rfc/rfc4949.txt, Stand 30.05.2009
[2] Busch C. / Wolthusen S. (2002), S. 11
[3] Vgl. ftp://athena-dist.mit.edu/pub/virus/mit.PS , S.2, Stand 10.06.2009
[4] Nazario, J. (2003), S. 39
[5] vgl. http://www.cert.org/meet_cert/, Stand 07.07.2009
[6] Eckert, C. (2008), S.65
[7] Kaspersky, E. (2008), S. 55

2.2.2 Email-Wurm

Alternativ werden Würmer per Email verteilt. Bei dieser Form der Verbreitung verwendet der Wurm manipulierte Emails, welche versuchen den Benutzer dazu zu bringen, den Anhang, also den Wurm, auszuführen. Alternativ beinhaltet die Email einen Link, welcher den Benutzer auf eine infizierte Website locken soll. Zum Versenden der Emails bedient sich der Wurm verschiedener Methoden[8]:

- Direkte SMTP Verbindung, d.h. der Wurm bringt eine Email Bibliothek mit
- Nutzen von Microsoft Outlook
- Nutzen der MAPI-Funktion von Windows.

2.2.3 Bluetooth-Wurm

Eine nicht so häufige Variante ist der Bluetooth-Wurm, welcher sich unter mobilen Endgeräten, sog. Smartphones verbreitet. Ist ein solcher Wurm auf einem Smartphone installiert, so sucht er permanent nach sämtlichen Bluetooth Empfängern und verschickt sich selbst als Information, oder als Programm an solche Empfänger. Der erste bekannte Wurm dieser Art ist der Wurm Cabir, welcher das Handybetriebssystem Symbian Series 60 angegriffen hat.[9] Cabir hat keine Sicherheitslücke im System ausgenutzt, sondern muss aktiv vom Benutzer installiert werden, um sich zu aktivieren. Führt der Benutzer die nötigen Schritte aus, verbreitet sich der Wurm automatisch auf alle sichtbaren Bluetooth-Geräte in Reichweite.

---

[8] Kaspersky, E. (2008), S. 53

[9] Vgl. http://www.f-secure.com/v-descs/cabir.shtml, Stand 30.05.2009

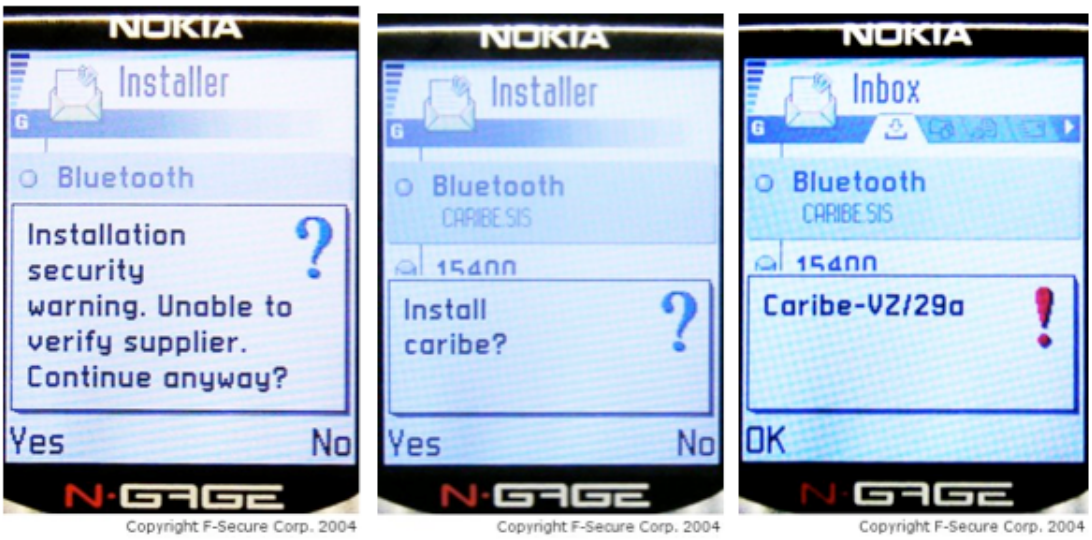

Abbildung 1: Infektion mit Caribe
Quelle: http://www.f-secure.com/v-descs/cabir.shtml, Stand 30.05.2009

2.3 Abgrenzung zum Virus

Verschiedene Autoren sehen im Wurm eine Unterart eines Virus, da sich beide reproduzieren.[10] Im Großteil der Literatur stellt der Wurm jedoch eine eigene Unterart der Kategorie Malware dar, da der Wurm andere Verbreitungsarten verwendet wie der Virus. Ein Virus ist eine Befehlsabfolge, welche zwingend ein anderes Programm als Wirt benötigt.[11]

2.4 Was ist ein Botnetz?

Die mit einem Wurm infizierten Rechner bilden in der Regel ein sog. Botnetz. Auch mit Viren und Trojanern infizierte Rechner können Mitglieder eines Botnetzes sein. Als Teil eines Botnetzes kann der Rechner von einer zentralen Stelle aus Befehle empfangen, um von dort gezielte Angriffe zu starten. Zur zentralen Koordination der Bots wird zumeist ein Internet Relay Chat (IRC) verwendet. Diese zentrale Stelle ist der erste Ausgangspunkt für Maßnahmen gegen ein Botnetz.

[10] Harley, D./Slade, R./Gattiker, U. (2002), S. 42
[11] Eckert, C. (2008), S. 51

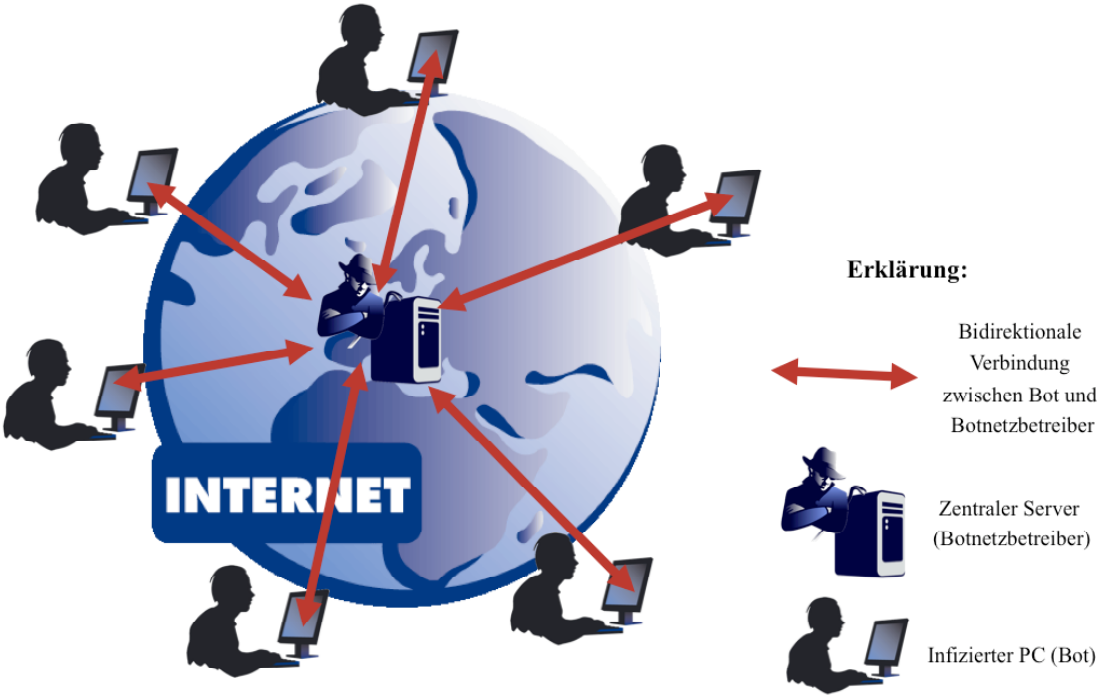

Abbildung 2: Aufbau eines Botnetzes

Neuere Botnetze verzichten auf einen zentralen Server und arbeiten Peer-to-Peer. Ein solches Peer-to-Peer Botnetz wurde zum Beispiel vom Storm Worm verwendet.

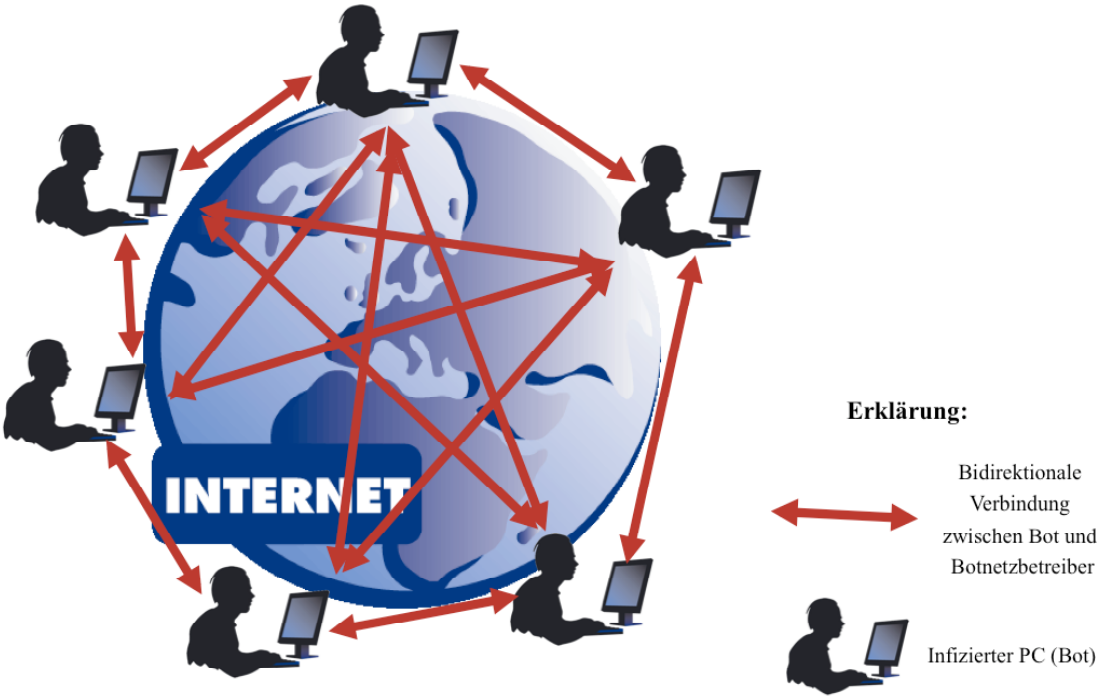

Abbildung 3: Peer-to-Peer Botnetz

Ein Botnetz besteht in der Regel aus mehreren tausend infizierten PCs. Kriminelle können ein bereits bestehendes Botnetz mieten, um eigene Angriffe (zum Beispiel Distributed Denial of Service Attacken) von dort zu starten.[12]

Solche Angebote findet man in Internetforen, welche sich auf den Austausch von Malware und Botnetzen spezialisiert haben.

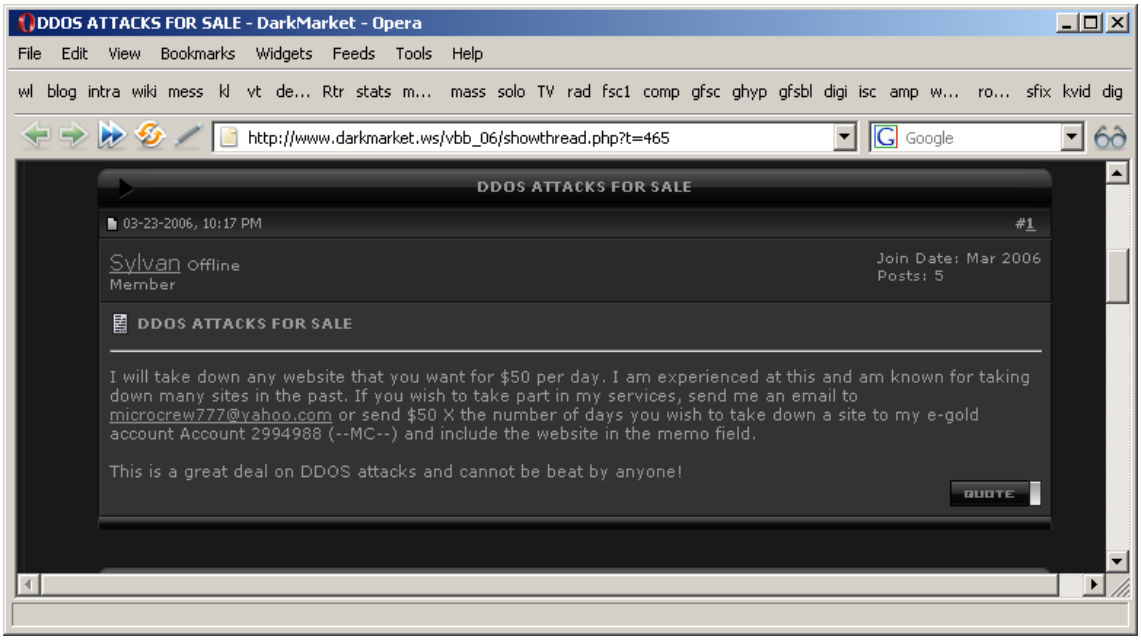

Abbildung 4: Mietangebot für ein Botnetz
Quelle: http://www.f-secure.com/weblog/archives/00001679.html

3. Fallstudie: Conficker

3.1 Verbreitung

Der Conficker-Wurm wurde erstmals im November 2008 entdeckt.[13] Er wird auch unter den Namen Downadup oder Kido geführt.[14] Über eine Sicherheitslücke im Server Dienst von Microsoft Windows, kann mit einem manipulierten RPC –Paket Code eingeschleust werden.[15] Diese Sicherheitslücke verwendet Conficker um sich zu verbreiten. Als Dynamic Link Library (DLL) kommend, kann der Conficker nicht direkt ausgeführt werden, sondern muss von einer anderen Applikation gestartet werden. Bei

[12] Eckert, C. (2008), S. 21
[13] Vgl. http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker, Stand 04.06.2009
[14] Vgl. http://www.f-secure.com/weblog/archives/00001553.html, Stand 04.06.2009
[15] Vgl. http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx, Stand 04.06.2009

der Infektion über die Sicherheitslücke MS08-067[16] wurde ein Expolit verwendet, um die DLL in den Server Service von Microsoft Windows einzuschleusen.[17] Alternativ kopiert sich Conficker auf USB-Sticks oder Netzwerkfreigaben um dann via rundll32.exe aufgerufen zu werden. Abbildung 5 zeigt eine reguläre autorun.inf, welche von Microsoft Windows standardmäßig automatisch interpretiert wird.

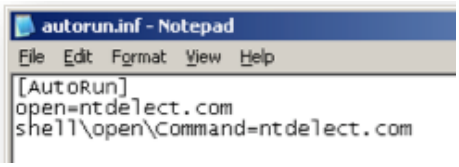

Abbildung 5: normale autorun.inf
Quelle: http://www.f-secure.com/weblog/archives/00001575.html

Steckt man einen USB-Stick an einen mit Conficker infizierten Rechner, so wird der Wurm auch auf diesen kopiert. Conficker verwendet eine autorun.inf, welche durch nutzlosen Code aufgefüllt ist, um die eigentliche Aktion zu verbergen (Abbildung 6).

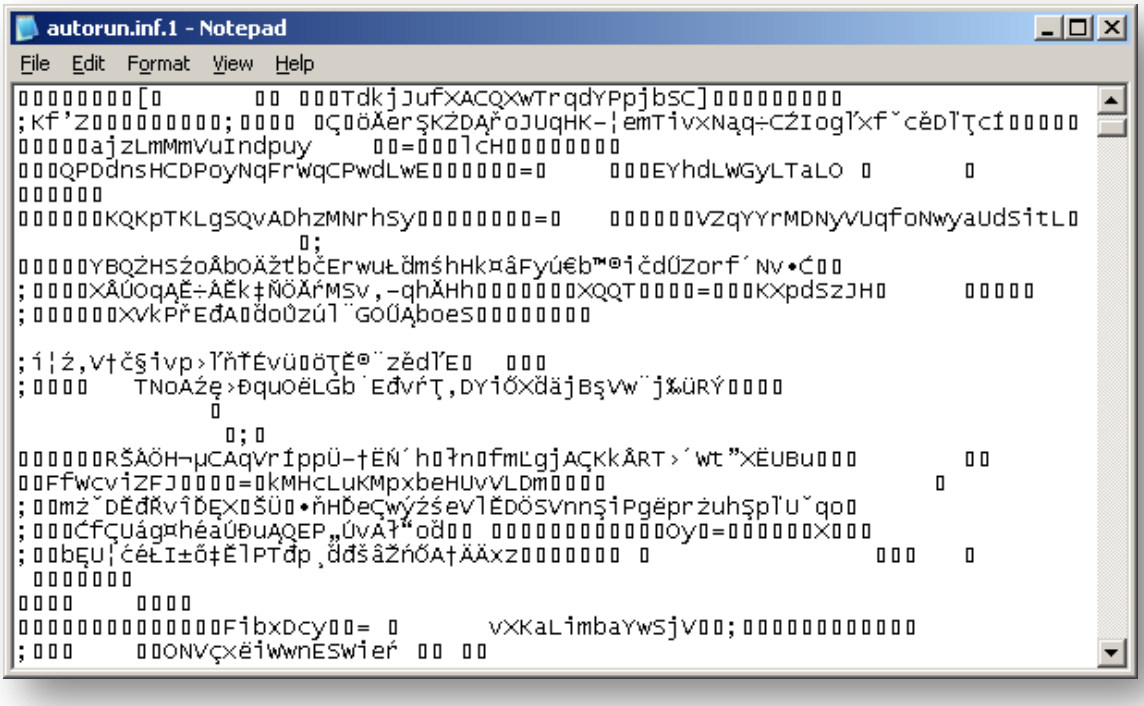

Abbildung 6: Conficker autorun.inf 1
Quelle: http://www.f-secure.com/weblog/archives/00001575.html

[16] Vgl. http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx, Stand 04.06.2009
[17] Vgl. https://www.honeynet.org/files/KYE-Conficker.pdf, S.2, Stand 07.04.2009

Weiter unten im Quelltext der autorun.inf findet man den Syntax einer normalen autorun.inf (Abbildung 7).

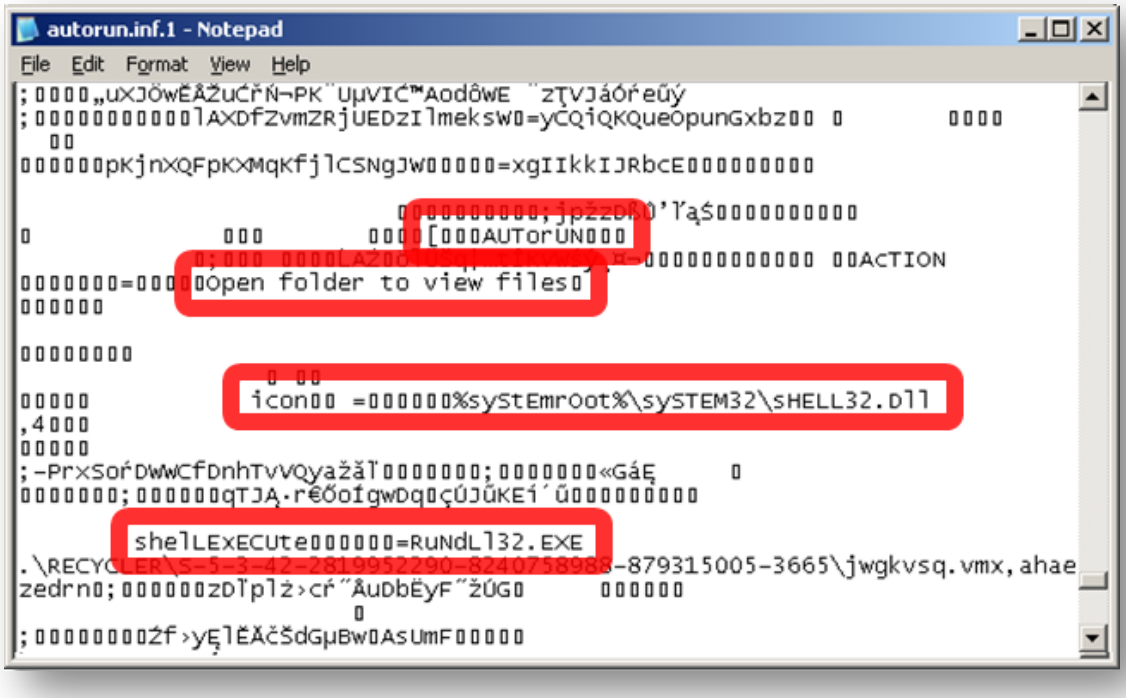

Abbildung 7: Conficker autorun.inf 2
Quelle: http://www.f-secure.com/weblog/archives/00001575.html

Die verborgene autorun.inf öffnet einen Userdialog, welcher den User dazu bewegen soll den Wurm zu starten. Da das geöffnete Fenster genau so aussieht wie ein reguläres Windows-Fenster ist eine Erkennung durch den Benutzer schwierig. (Abbildung 8)

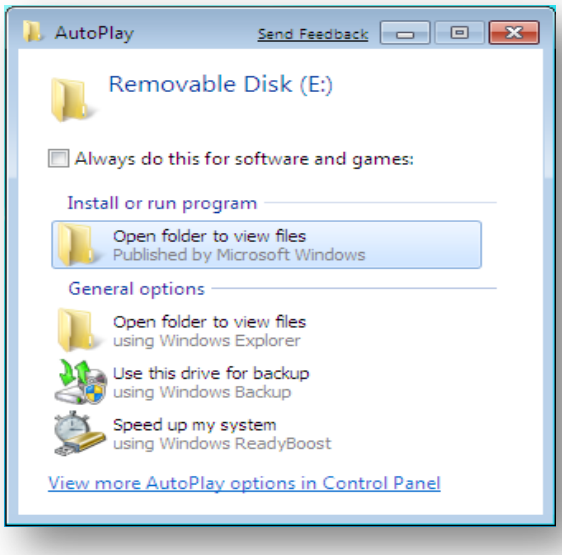

Abbildung 8: Dialogfenster, welches von Conficker autorun.inf geöffnet wird
Quelle: http://www.f-secure.com/weblog/archives/00001575.html

Eine weitere Verbreitungsmöglichkeit des Conficker-Wurms ist die Verbreitung über Netzwerkfreigaben. Hier verwendet Conficker eine reguläre Windows Funktion, um sich die angemeldeten Benutzer eines PCs anzeigen zu lassen. Ausgehend von diesen Benutzernamen versucht der Wurm ein Netzwerklaufwerk mit dem entfernten PC zu verbinden. Als Passwort verwendet Conficker eine Liste mit den gängigen Passwörtern:

abc123	customer	money	qqqqq	xxxxx
academia	database	monitor	qweasd	zxccxz
access	default	mypass	qweasdzxc	zxcvb
account	desktop	mypassword	qweewq	zxcvbn
Admin	domain	mypc123	qwerty	zxcxz
admin	example	nimda	qwewq	zzzzz
admin1	exchange	nobody	root123	
admin12	explorer	nopass	rootroot	
admin123	files	nopassword	sample	
adminadmin	foobar	nothing	secret	
administrator	foofoo	office	secure	
anything	forever	oracle	security	
asddsa	freedom	owner	server	
asdfgh	games	pass1	shadow	
asdsa	home123	pass12	share	
asdzxc	ihavenopass	pass123	student	
backup	Internet	passwd	super	
boss123	internet	Password	superuser	
business	intranet	password	supervisor	
campus	killer	password1	system	
changeme	letitbe	password12	temp123	
cluster	letmein	password123	temporary	
codename	Login	private	temptemp	
codeword	login	public	test123	
coffee	lotus	pw123	testtest	
computer	love123	q1w2e3	unknown	
controller	manager	qazwsx	windows	
cookie	market	qazwsxedc	work123	

Abbildung 9: Conficker Passwortliste
Quelle: http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml

Ist der Wurm auf einem PC aktiv, bei dem ein Benutzer mit administrativen Rechten angemeldet ist, verwendet Conficker diesen Account anstatt der Liste.

3.2 Conficker Zeitleiste

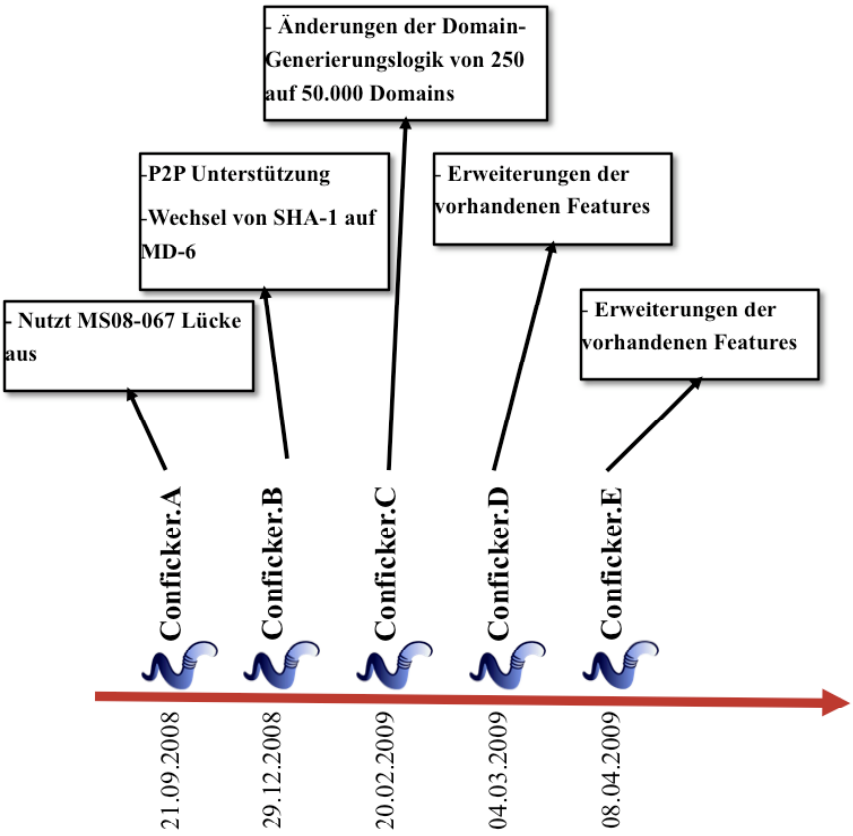

Abbildung 10: Zeitleiste der Verschiedenen Conficker Versionen
Quelle: in Anlehnung an: http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline

3.3 Conficker Botnetz

Conficker besitzt eine aufwendige Logik um ein Botnetz zu bilden. Anstatt einen festen zentralen Server oder IRC zu nutzen, generiert Conficker.A jeden Tag nach einem festen Algorithmus 250 Domainnamen aus 6 Top-Level-Domains, zu denen er sich verbinden kann. Durch das Herausfinden dieses Algorithmus konnten die Schätzungen über die Verbreitung bereitgestellt werden. Das Anti-Viren-Labor von F-Secure konnte durch Reverse Engineering des Conficker-Wurms genau bestimmen, wann der Wurm eine Verbindung an welche Domain initiieren würde und hat diese Domains vorab registriert und dort einen Webserver mit Verbindungsprotokollierung installiert. Da es sich um Domainnamen handelt, die ein normaler Internet-Surfer zufällig eingibt, kann

man davon ausgehen, dass alle Verbindungen zu der Domain ausschließlich von infizierten Rechnern stammen. Im Protokoll des Webservers steht die Quelle der IP Verbindung, welche keine Information über die Anzahl der Rechner hinter der IP-Adresse bietet, da eine Network-Adress-Translation (NAT) im Internet weit verbreitet ist. Bei einer Netzwerkadressübersetzung werden Rechner mit privaten IP Adressen hinter einer oder mehreren offiziellen IP Adressen versteckt. Im Weblog der Firma F-Secure geht man davon aus, dass hinter jeder IP Adresse im Schnitt 9 PCs stehen, was im Januar eine Anzahl von ca. 2.400.000 infizierten PCs bedeutet hätte.[18]

Damit der Conficker Wurm daran gehindert wird, Aktualisierungen über einer der generierten Domains herunterzuladen, wurde die Conficker Working Group[19] gegründet. Dieser Arbeitsgruppe gehören neben einigen Anti-Viren Software Herstellern auch unter anderem Firmen wie Cisco, Microsoft, AOL und Facebook an.[20]
Mit dieser übergeordneten Instanz in Form der Arbeitsgruppe werden Top-Level-Domain Betreiber mit den Domainlisten des Conficker Wurms versorgt, damit eine Registrierung der Domain unterbunden werden kann. Der Conficker Wurm hat darauf reagiert, indem er mit der Variante Conficker.B einen P2P Mechanismus und mit Conficker.C[21] die Anzahl der genutzten Top-Level-Domains auf 116 erweiterte.[22]

Conficker.B wurde am 29. Dezember 2008 erstmals erkannt und bringt neben der Peer-to-Peer Funktionalität auch eine Veränderung des Signierungsalgorithmus mit.[23]
Damit der Conficker Wurm nur vom Botnetzbetreiber Aktualisierungen und Payloads empfangen kann, werden diese Daten digital signiert. Conficker.A nutzt hierzu SHA-1[24], eine kryptologische Hash-Funktion., welche als Teil des Secure Hash Standards vom amerikanischen National Institute of Standards and Technology (NIST) im Jahr 1993 entwickelt wurde.[25] SHA-1 gilt seit dem Jahr 2005 als unsicher.[26]

---

[18] Vgl. http://www.f-secure.com/weblog/archives/00001579.html, Stand 09.06.2009

[19] Vgl. http://www.confickerworkinggroup.org, Stand 09.06.2009

[20] Vgl. http://www.confickerworkinggroup.org/wiki/pmwiki.php, Stand 09.06.2009

[21] Vgl. http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.c, Stand 09.06.2009

[22] Vgl. http://www.confickerworkinggroup.org/wiki/pmwiki.php/TLD/TLDOperators, Stand 09.06.2009

[23] Vgl. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, Stand 09.06.2009

[24] Vgl. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, Stand 09.06.2009

[25] Eckert C. (2008), S. 352

[26] Vgl. http://www.schneier.com/blog/archives/2005/02/sha1_broken.html, Stand 09.06.2009

Conficker.B verwendet MD-6, einem Hashfunktion welche erst im September 2008 vorgestellt wurde.[27] Die Verwendung von Md-6 ist ungewöhnlich, da es sich zu diesem Zeitpunkt um die neueste Hashfunktion handelte.[28]

Die Variante Conficker.C wurde am 20.Februar erkannt.[29] Der Algorithmus zum generieren der Domainnamen wurde in Version C erweitert. Wo vorher 250 Domainnamen generiert wurden, erzeugt Conficker.C eine Domainliste mit 50.000 Domains, von denen er sich zu 500 verbindet, um Aktualisierungen und eine Payload herunterzuladen. Auch veränderte sich die Frequenz der Abfragen, Conficker.A und Conficker.B haben sich mehrfach am Tag zu den erzeugten Domainnamen verbunden, Variante C nur einmal pro Tag.

Zusätzlich filtert Conficker.C die DNS-Antworten vor dem Verbinden zu einer der generierten Domains.
Die Verbindung wird nicht aufgebaut wenn...

- ... der DNS Server mehrere IP Adressen zurückliefert.
- ... die IP Adresse 127.0.0.1 zurückgeliefert wird.
- ... die IP Adresse auf einer eingebauten Blacklist steht.
- ... die gleiche IP Adresse bei einer vorherigen DNS-Abfrage zurückgeliefert wurde.
-

Erreicht Conficker.C keine der Domains, startet er nach 24 Stunden mit der Generierung einer neuen Liste von 50.000 Domains. Die Domainnamen bestehen aus 4 bis 10 Zeichen plus einer der 116 zufällig ausgewählten Top-Level-Domains.[30]
Conficker.D und Conficker.E, welche im März bzw. April erkannt wurden brachten keine neuen, sondern nur Erweiterungen der bereits bekannten Funktionen.

[27] Vgl. http://groups.csail.mit.edu/cis/md6/, Stand 09.06.2009
[28] Vgl. http://mtc.sri.com/Conficker/addendumC/index.html, Stand 10.06.2009
[29] Vgl. http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, Stand 10.06.2009
[30] Vgl. http://mtc.sri.com/Conficker/addendumC/index.html, Stand 10.06.2009

4. Abwehrmaßnahmen

Gegen Würmer im Allgemeinen sollte man einen aktuellen Virenscanner in Verbindung mit einer Personal Firewall einsetzen. Der Virenscanner schützt den PC mit aktiviertem Echtzeitschutz vor jeder Art von Malware, welche auf die Festplatte oder in den Arbeitsspeicher geschrieben wird.

Um Netzwerkwürmer zu blockieren, bevor sie auf die Festplatte geschrieben werden, sollte man eine Personal Firewall einsetzen, welche eingehenden Netzwerkverkehr blockiert. Alternativ konfiguriert man die Netzwerkdienste möglichst eingeschränkt.[31]

Da Würmer in der Regel eine Schwachstelle im Betriebssystem ausnutzen, sollten Sicherheitsupdates zeitnah eingespielt werden.[32] Im speziellen Fall Conficker handelt es sich um das Microsoft Update MS08-067, welches die Schwachstelle im Server Dienst behebt.

Wenn ein Wurm bereits einen Rechner im Netzwerk infiziert hat, sollte man diesen schnellstmöglich vom Netzwerk trennen, damit von ihm keine weiteren Infektionen ausgehen.[33] Einige Würmer sind in der Lage die vorhandene Sicherheitssoftware zu deaktivieren, eine Bereiningung des Systems kann in einem solchen Fall von einer Boot-CD durchgeführt werden.

Eine spezielle Abwehr gegen den Conficker Wurm hat das Institute of Computer Science in Bonn[34] entwickelt, basierend auf der Tatsache, dass der Conficker.A keine IP Adressen aus der Ukraine angreift[35]. Bevor Conficker.A eine Verbindung zu einer fremden IP aufbaut, fragt er bei einem Geo-IP Dienst an, ob sich die IP Adresse in der Ukraine befindet, und verschont diese Adresse dann gegebenenfalls. Die Adresse zum Geo-IP Dienst ist fest einprogrammiert, was den Anbieter des Dienstes nach dem Ausbruch des Wurms dazu gezwungen hat, den Service umzuziehen.

Das Institute of Computer Science bietet nun den Service für den Conficker Wurm wieder an, mit dem Unterschied, dass für alle angefragten IP Adressen das Land

---

[31] Eckert, C. (2008), S.68
[32] Eckert, C. (2008), S. 67
[33] Vgl. http://technet.microsoft.com/en-us/security/dd452420.aspx, Stand 10.06.2009
[34] Vgl. http://iv.cs.uni-bonn.de/, Stand 07.07.2009
[35] Vgl. http://mtc.sri.com/Conficker/addendumC/index.html, Stand 10.06.2009

Ukraine zurückgeliefert wird und somit der infizierte Rechner keine Verbindung zu dieser IP Adresse aufbaut.[36]

5. Zusammenfassung

Die Ausbreitung des Conficker Wurm macht es deutlich: auch wenn ein Wurm heutzutage keine 10% des Internets lahmlegen kann, wie es im Jahr 1988 mit dem Morris Wurm der Fall war, kann er doch eine beträchtliche Anzahl an Rechnern infizieren. Bricht ein Wurm aus, ist das durch Zunahme bestimmter Verbindungen erkennbar. Auf Abbildung 11 sieht man deutlich, wie zum Beispiel beim Ausbruch des Conficker Wurms Verbindungen auf Port 445 sprunghaft angestiegen sind.

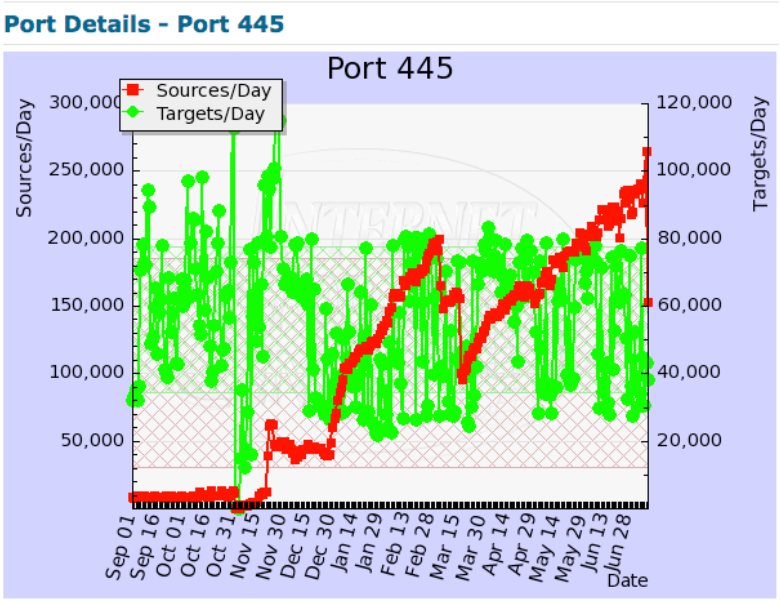

Abbildung 11: Verbindungen auf Port 445
Quelle: http://isc.sans.org/port.html, Stand 07.07.2009

Auch größere Netzwerke waren von Conficker betroffen, so musste beispielsweise die Bundeswehr wochenlang gegen den internen Wurmbefall vorgehen.[37]

Am 30.06.2009 zählt die Conficker Working Group 5.217.862 eindeutige IP Adressen, welche mit dem Conficker Wurm infiziert sind. Das Problem Conficker ist also noch

---

[36] Vgl. http://four.cs.uni-bonn.de/wg/cs/applications/containing-conficker/

[37] Vgl. http://www.bundeswehr.de/portal/a/bwde/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd443DgwBSUGYAfqR6GIBIQixoJRUfW99X4_83FT9AP2C3NCIckdHRQAlYgRn/delta/base64xml/L2dJQSEvUUt3QS80SVVFLzZfQ18zUkU!?yw_contentURL=/C1256EF4002AED30/W27PED65714INFODE/content.jsp

nicht beseitigt, obwohl die Sicherheitsupdates für die ursprüngliche Verwundbarkeit im Server Dienst von Microsoft Windows, sowie eine Erkennungssignatur für nahezu jeden Virenscanner längst zur Verfügung stehen.

Microsoft hat ein Kopfgeld von 250.000 USD auf Hinweise, die zu einer Verhaftung von Urhebern der Conficker Varianten führen, ausgesetzt.[38] Für Microsoft ist ein Kopfgeld seit dem Jahr 2003 in einem Fall von Malware gängige Praxis.[39] Trotzdem wird es weiterhin Computerwürmer wie den Conficker geben, die durch neue Techniken ein Botznetz bilden und das Internet in bestimmten Maßen belasten.

[38] Vgl. http://technet.microsoft.com/en-us/security/dd452420.aspx, Stand 10.06.2009

[39] Vgl. http://www.microsoft.com/presspass/press/2003/nov03/11-05AntiVirusRewardsPR.mspx, Stand 10.06.2009

6. Literaturverzeichnis

Bush C. / Wolthusen S. (2002): Netzwerksicherheit, ISBN 3-8274-1373-7, Spektrum Akademischer Verlag Gmbh, Heidelberg 2002

Eckert, C. (2008): IT-Sicherheit, 5. Aufl., ISBN 978-3-486-58270-3, Oldenbourg Wissenschaftsverlag GmbH, München 2008

Harley, D./Slade, R./Gattiker, U. (2002): Das Anti-Viren-Buch, 1. Aufl., ISBN 3-8266-0846-1, mitp Verlag, Bonn 2002

Kaspersky, E. (2008): Malware, 1. Aufl., ISBN 978-3-446-41500-3, Carl Hanser Verlag, München 2008

Nazario J. (2003): Defense and Detection Strategies against Internet Worms, ISBN 1-58053-5372, Artech House Inc, Boston 2003

Conficker Working Group (2009): Home Page, http://www.confickerworkinggroup.org, Stand 09.06.2009

Conficker Working Group (2009): Home Page, http://www.confickerworkinggroup.org/wiki/pmwiki.php, Stand 09.06.2009

Conficker Working Group (2009): TLD Operators, http://www.confickerworkinggroup.org/wiki/pmwiki.php/TLD/TLDOperators, Stand 09.06.2009

Conficker Working Group (2009): Timeline, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, Stand 09.06.2009

Conficker Working Group (2009): Timeline, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline, Stand 10.06.2009

Computer Emergency Response Team (2009): Meet CERT, http://www.cert.org/meet_cert/, Stand 07.07.2009

Eichin M. / Rochlis J. (1989): With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988, ftp://athena-dist.mit.edu/pub/virus/mit.PS, S.2, Stand 10.06.2009

F-Secure Corporation (2004): Virus Description of Cabir, http://www.f-secure.com/v-descs/cabir.shtml, Stand 30.05.2009

F-Secure Corporation (2008): Creating MS08-067 Exploits, http://www.f-secure.com/weblog/archives/00001553.html, Stand 04.06.2009

F-Secure Corporation (2009): When is AUTORUN.INF really an AUTORUN.INF?, http://www.f-secure.com/weblog/archives/00001575.html, Stand 04.06.2009

F-Secure Corporation (2009): How Big is Downadup? Very Big., http://www.f-secure.com/weblog/archives/00001579.html, Stand 09.06.2009

Leder, F. / Werner T. (2009): Know Your Enemy: Containing Conficker, https://www.honeynet.org/files/KYE-Conficker.pdf, S.2, Stand 07.04.2009

Microsoft Corporation (2003): Microsoft Announces Anti-Virus Reward Program, http://www.microsoft.com/presspass/press/2003/nov03/11-05AntiVirusRewardsPR.mspx, Stand 10.06.2009

Microsoft Corporation (2008): Microsoft Security Bulletin MS08-067 , http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx, Stand 04.06.2009

Microsoft Corporation (2008): Win32/Conficker, http://www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker, Stand 04.06.2009

Microsoft Corporation (2008): Worm:Win32/Conficker.C, http://www.microsoft.com/security/portal/Entry.aspx?Name=Worm:Win32/Conficker.c, Stand 09.06.2009

Microsoft Corporation (2009): Conficker Worm: Help Protect Windows from Conficker, http://technet.microsoft.com/en-us/security/dd452420.aspx, Stand 10.06.2009

Network Working Group (2007): Internet Security Glossary Version 2 / RFC 4949, http://www.rfc-editor.org/rfc/rfc4949.txt, Stand 30.05.2009

Porras, P. / Saidi, H. / Yegneswaran, V. (2009): Conficker C Analysis, http://mtc.sri.com/Conficker/addendumC/index.html, Stand 10.06.2009

Rivest R. (2008): The MD6 Hash Algorithm, http://groups.csail.mit.edu/cis/md6/index.html, Stand 09.06.2009

Schneier B. (2005): SHA-1 broken, http://www.schneier.com/blog/archives/2005/02/sha1_broken.html, Stand 09.06.2009