Conficker – One Year After

A Short Overview

Disclaimer

The information and data asserted in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post -release information.

This document and the data contained herein are for information purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorses the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide. Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

Table of Contents

About This Document

This document is primarily intended for IT&C System's Security Managers, System and Network Administrators, Security Technology Developers, Analysts, and Researchers, but it also addresses issues pertaining to a broader audience, like small organizations or individual users concerned about the safety and integrity of their networks and systems.

We Would Like to Hear from You

As the reader of this document, you are our most important critic and commentator. We value your opinion and want to know what you like about our work, what you dislike, what we could do better, what topics you would like to see us cover, but also any other comments and suggestions you wish to share with BitDefender's Team.

You can e-mail or write us directly to let us know what you did or did not find useful and interesting about this document, as well as what elements and details we should add to make our work stronger.

When you write, please be sure to include this document's title and author, as well as your name and phone or e-mail address. We will carefully review your comments and share them with the authors and contributors who worked on this document.

E-mail:

documentation@bitdefender.com

Mail:

BitDefender Headquarters

West Gate Park

24th, Preciziei Street

Building H2, Ground Floor

6th district, 062204, Bucharest

ROMANIA

Conficker – One Year After

Răzvan Livintz
Communication Specialist

By far, *Conficker* (a.k.a. *Downadup* or *Kido*) was not the cleverest e-threat ever, nor the most dangerous. It is though one of the most intriguing well-written pieces of malware, with a great damaging potential and an intricately smart manner of update.

Since its egression in late October 2008, rumors and scientific data mingled into a cornucopia of facts, while mass-media enjoyed feeding their readers with terrifying figures and apocalyptic scenarios tattling the death of the Internet as we know it on April Fool's Day.

In what security context did Conficker appear?

At the beginning of 2009 Internet users have had to cope with approximately 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits, Trojans and other malware. The reason behind 95% of all these e-threats remains profit, both financial and technological.

Malware production followed an ascending trend, exploiting the same Web based capabilities of Trojans, spyware and rootkits. Early days of 2009 already saw a 460% increase in Web-based infections and a 400% augmentation of e-mail spam distributing Trojans. It is certain that many of the existing e-threat families will suffer significant upgrades and mutations, in terms of stealth and automation of spreading mechanisms.

As the latest issue of BitDefender E-Threats Landscape Report showed, between January and June 2009, the most active countries in the realm of malware propagation were China (33%), France (24%) and the United States (14%), followed by Romania and Spain (6%), Australia and Germany (4%), India and Canada (3%), UK and Mexico (below 1.8%).

What is Conficker?

Conficker is a network worm[1] that takes advantage of vulnerabilities in Microsoft® Windows® to spread. The worm by itself does not produce any damage. As far as we know it, none of the five existing variants corrupt files or steal data. It first appeared in November 2008 and ever since continued to spread and compromise systems around the globe.

Conficker always comes wrapped in an obfuscated layer which aims at deterring analysis. The real malware is contained inside in an encrypted form. It is packed with a standard open-source packer for executables, but to prevent unpacking it is never written on disk and hides under the appearance of an invalid executable. This has the side effect of being undetectable when injected into another process, looking as a standard memory allocated page.

[1] A *network worm* can be defined as a computer program that replicates itself and is self-propagating. Worms, as opposed to viruses, are meant to spawn in network environments. Being self-contained programs, they do not infect other applications. They can carry instead a malicious payload, just like viruses.

A computer can get infected in three possible ways:

a) if not patched with the latest security updates and not protected by a security solution

b) if the administrator account on the attacked system has a week password

c) if the computer has the Autoplay feature enabled and an infected mapped/removable disk is attached.

Upon execution, Conficker injects itself into several processes – such as explorer.exe, svchost.exe – and modifies some parameters in the system registries to hide its presence. It produces multiple copies, which it stores in different .DLL files within the most important system folders (Program Files, Documents and Settings, Temp and System32).

It monitors and blocks access to Web sites and update services related to security companies, while it also disables Windows Automatic Update Service.

Subsequently, it tries to connect and infect other available network resources that it can access using a list of weak passwords, while newer versions also exploit Microsoft® Windows® Autorun feature for the spreading purposes.

Conficker also possesses a communication mechanism which is employed for update and further instructions, as detailed in the following section.

What damage did Conficker do?

As previously described, the malware creators behind Conficker engineered it with a lot of craft and succeeded in producing an illustrious heir for its precursors, namely Welchia, Blaster, Sobig, Sasser and Storm.

First and foremost, Conficker's purpose is to spread and compromise as many machines as possible. It achieved this goal using a vulnerability in Microsoft® Windows® RPC Server Service, described in the Microsoft Security Bulletin MS08-067. The flaw is to be held accountable for allowing an attacker to remotely execute code onto an unprotected machine. Early 2009 estimations confirmed Conficker's success in spreading – by the end of Q1, the total number of compromised machines around the globe almost equaled Belgium's or Netherlands' population. Variants B and C also included into the spreading mechanism the exploitation of Autorun function for removable drives and media (such as USB portable storage devices), and the possibility to access by brute force the insufficiently protected network shares (namely those with weak passwords).

The second mission of Conficker is to set up, deploy and maintain a viable stealth communication system between the compromise machines for updating and command purposes. The communication mechanism suffered the most elaborate development from one variant to another and it is responsible for the allegations related to the Internet Apocalypse. Conficker's initial three versions connected to a limited number of domains – around 250 – in order to update. The enhancements introduced in the last two variants are to be held accountable for the generation of 50,000 random domains, Conficker C and D being able to select 500 URLs and randomly check them for updates.

The third purpose of Conficker is to paralyze defensive systems. From its second variant, the worm began to disable Windows Update and block the access to the majority of antimalware Web sites. The consequence translated as the total failure in getting automatic or manual updates for the installed security suites or products. Moreover, any attempt to connect to vendors' or third-parties' Web sites in order to get disinfection tools becomes futile, as malware creators behind Conficker update almost instantaneously the list of URLs to be blocked.

To summarize, Conficker's mission until now was to create a worldwide army of yet-dormant machines, able to communicate, update and receive orders, while also neutralizing any defense system in place.

Was Conficker defeated or eradicated?

Although Microsoft offered a $250,000 bounty to catch the people behind the worm, the quarterly evolution of Conficker infections reveals at least three alarming aspects, both for security community and computer/Internet users:

Malware creators do not sleep nor do they take vacation. The ingeniosity and skillfulness used to create the five breeds of Conficker are the strongest evidence that malware authors are always innovative when it comes to profit.

The high rate of infections also tells that the level of awareness is still low among users. Not only when it comes to (constantly) update an OS with the latest fixes against security flaws, but even in terms of (good sense) removable media scanning against malware (even if it comes from a trusted sources).

Last but not least, it also shows that many users do not know that removal tools are available and they could employ them to disinfect their systems (until is not too late).

Top 10 most infected countries in Q1 2009

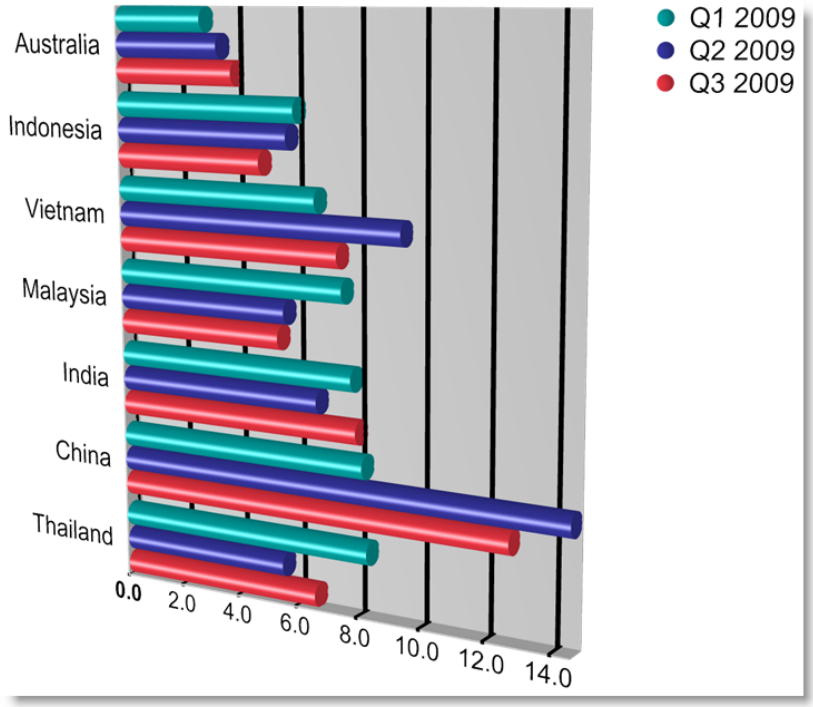
Thailand	8.35 %
China	8.20 %
India	7.85 %
Malaysia	7.56 %
Vietnam	6.70 %
Indonesia	6.03 %
Philippines	4.53 %
Australia	2.94 %
France	2.42 %
Italy	2.17 %
Other countries	43.26 %

Top 10 most infected countries in Q2 2009

China	14.59 %
Vietnam	9.44 %
Romania	7.48 %
India	6.72 %
Indonesia	5.78 %
Malaysia	5.66 %
Thailand	5.57 %
Australia	3.49 %
Philippines	2.74 %
Mexico	2.58 %
Other countries	35.94 %

Top 10 most infected countries in Q3 2009

China	12.76 %
India	8.00 %
Vietnam	7.41 %
Thailand	6.65 %
Romania	6.13 %
Malaysia	5.45 %
Indonesia	4.88 %
Australia	3.98 %
Mexico	2.72 %
Colombia	2.71 %
Other countries	39.32 %



Top 10 most infected countries between Q1 and Q3 2009

China	12.96 %
Romania	8.02 %
Vietnam	7.75 %
India	7.48 %
Thailand	6.30 %
Malaysia	5.64 %
Indonesia	5.05 %
Australia	3.63 %
Philippines	2.91 %
Mexico	2.49 %
Other countries	37.76 %

What we expect from Conficker?

Ultimately, Conficker acts as any botnet. *Botnet* is a coined term derived from *robot network*. A botnet might be understood as a collection of *malicious software robots* (abbreviated *bots*), whose purpose is to run different kind of computer applications controlled by the owner or the disseminator of the software robot source, on a group of compromised computers, usually connected to the Internet.

From this point of view we can only expect for worse, as described below:

Corruption of Defensive System

The most dangerous aspect related to Conficker infection is that it completely neutralizes defensive systems. In other words, any infected machine holds a huge security breach that can be exploited anytime from now on. It is like having a house with a door wide open all the time, even when you sleep or go to work or in vacation.

Distributed Denial of Service

A botnet can be used as a tool to completely paralyze other computers over the Internet through what is known as *Distributed Denial of Service* (DDoS). The botnet attacks a network or a computer system to disrupt service via the loss of connectivity or consumption of the victim network's bandwidth and to overload the resources of the victim's computer system. This can prevent the access to a particular Web site for a long period of time, which, in case of Web-operating companies, but not only, might lead to total isolation.

Pay-per-Click Systems Abuses and Frauds

Botnets can be used to engage in click abuses and frauds. The bot is used to visit a specific Web page and/or automatically "click" on the advertisement banners. The purpose is to obtain financial gain by automating visiting and/or clicking on a pay-per-view or pay-per-click system (to actually cheat the online advertising companies that pay a sum of money for each visit or click on that page, like Gooogle Adsense).

Key Logging, Traffic Monitoring and Mass Identity Theft

Many bots watch the keyboard activity and report the keystrokes stream to their owner. Some bots have features to look for visits to particular Web sites where passwords or bank account information is entered. With a filter program, the bot owner can extract only the keyboard sequence typed before or after words like "PayPal" or "Credit Card". This allows cybercriminals to gain access to personal information and accounts belonging to thousands of people.

Spamming

The drones from a botnet can be used to harvest e-mail addresses and/or send/forward a huge amount of messages to other computers. For instance, this was the case of a mass-mailing spam campaign at the end of 2007, pleading for Ron Paul candidature at the 2008 US presidential elections.

How can we protect?

The following five simple rules should be enough to keep you away from any upcoming disaster:

- Check with your operating system provider on a regular basis – download and install the latest security updates, malware removal tools, as well as other patches or fixes.
- Install and activate a reliable password protected antimalware, firewall, spam filter and parental control solution, like those provided by BitDefender.
- Update your antimalware, firewall and spam filter as frequent as possible, with the latest virus definitions and suspicious applications/files signatures.
- Scan your system frequently.
- Stay informed about e-threats and security.

If your system has been infected, there is still hope. Check http://www.bdtools.net/, download the Downadup Removal Tool, follow the instructions and clean your system. Ideally, once you eliminated Downadup from your machine, you should patch your OS with the latest updates, install and activate an antimalware suite.