# THE CONFICKER MYSTERY

**Mikko Hypponen**
**Chief Research Officer**
**F-Secure Corporation**

Network worms were supposed to be dead. Turns out they aren't.

In 2009 we saw the largest outbreak in years: The Conficker aka Downadup worm, infecting Windows workstations and servers around the world.

This worm infected several million computers worldwide - most of them in corporate networks. Overnight, it became as large an infection as the historical outbreaks of worms such as the Loveletter, Melissa, Blaster or Sasser.

Conficker is clever. In fact, it uses several new techniques that have never been seen before. One of these techniques is using Windows ACLs to make disinfection hard or impossible. Another is infecting USB drives with a technique that works *even* if you have USB Autorun disabled. Yet another is using Windows domain rights to create a remote jobs to infect machines over corporate networks.

Possibly to most clever part is the communication structure Conficker uses. It has an algorithm to create a unique list of 250 random domain names every day. By precalcuting one of these domain names and registering it, the gang behind Conficker could take over any or all of the millions of computers they had infected.

## Case Conficker

The sustained growth of malicious software (malware) during the last few years has been driven by crime. Theft – whether it is of personal information or of computing resources – is obviously more successful when it is silent and therefore the majority of today's computer threats are designed to be stealthy. Network worms are relatively "noisy" in comparison to other threats, and they consume considerable amounts of bandwidth and other networking resources. Worms spread very aggressively and can be quite difficult to control. They are not generally the weapon of choice for today's eCriminal.

Infamous worms of the past such as Blaster, CodeRed, Melissa, and Nimda were authored more by hobbyists than by professional criminals. The Conficker worm, also known as Downadup, is quite different and may perhaps be an indication of threats to come. Analysis of its code reveals that it has in fact been authored by today's "professional" class of malware authors. While some of it is disorganized, the code is clearly not something that was written by an amateur.  It is complex code and demonstrates a sophisticated understanding of the security systems that must be circumvented for the worm to spread. Conficker utilizes server-side polymorphism and Access Control List (ACL) modifications to make network disinfection particularly difficult. When Conficker infiltrates a Local Area Network (LAN), removal can be a

very time consuming and possibly frustrating task.

Conficker exploits vulnerabilities (MS08-067) in the Windows Server service. (The Windows MS08-067 vulnerability was patched in an out-of-cycle update in October 2008.) It also does much more than this. Conficker uses autorun-worm techniques, spreading itself via removable USB thumb drives. Once it has infected a computer, it attempts to access Network Shares and also attempts to crack local account passwords. If Conficker compromises an administrator account, it uses the Windows Task Scheduler service to spread itself to non-infected computers. Those computers, having received the Scheduled Task from an "administrator" account, proceed to execute and run the worm without question.

Regarding the MS08-067 vulnerability, the Conficker worm needs to determine what language version of Windows it is attacking in order to exploit its victim. Earlier versions of Conficker were somewhat limited in their ability to make this distinction as they made a GeoIP location query via the Internet. The responding GeoIP database then converted the IP addresses, used by all computers, into a geographic location. When attacking a computer located in the USA, the worm attempts to exploit the English language version of Windows. If the IP address of the computer under attack is located in China, the worm then attempts to exploit the Chinese language version of Windows, and so on.

The providers of the GeoIP database being used by Conficker.A renamed and moved their database in order to deny Conficker the ability to locate its victims. Conficker.B responded to this change by integrating a small GeoIP database within its own code. Other small improvements in the worm's code lead to significant results.

The B variant of the Conficker worm spread rapidly during the months of January and February, infecting millions of computers worldwide. Countries such as China, Brazil, Russia, and India topped the list of infection counts. During the same period, there were many reported instances of European networks that were compromised. The out-of-band Windows MS08-067 vulnerability October update shortly before December's holidays helped contribute to a lack of testing resources, and many organizations failed to implement the necessary updates by the time variant B became a serious threat.

With a swiftly growing number of infections and the potential threat of the worm "calling home" to its authors, a number of companies within the antivirus industry, including F-Secure, banded together to form the "Conficker Working Group". The group has successfully worked together with Internet Domain Registars from many countries to block the domain address to which Conficker attempts to communicate. Blocking the worm's attempts to call home limits the worm's authors from using the infected computers for criminal purposes. This successful monitoring of the worm continues against the current variant, Conficker.C, which greatly increased the number of domains to which it attempts to call home.

**Conficker April 1st activation**

**Q:** I heard something **really bad** is going to happen on the Internet on April 1st! Will it?
**A:** No, not really.

**Q:** Seriously, the **Conficker worm** is going to do something bad on April 1st, right?
**A:** The Conficker aka **Downadup** worm is going to change it's operation a bit, but that's **unlikely to cause anything visible on April 1st**.

**Q:** So, what will it do on April 1st?
**A:** So far, Conficker has been polling 250 different domain names every day to download and run an update program. On April 1st, the latest version of Conficker will start to poll 500 out of **50,000** domains a day to do the same thing.

**Q:** The latest version? There are different versions out there?
**A:** Yes, and the **latest version is not the most common**. Most of the infected machines are infected with the B variant, which became widespread in early January. With B variant, nothing happens on April 1st.

**Q:** I just checked, and my Windows machine is clean. Is something going to happen to me on April 1st?
**A:** No.

**Q:** I'm running a Mac, is something going to happen to me?
**A:** No.

**Q:** So… this means that the attackers could use this download channel to run any program on all the machines?
**A:** On all the machines that are infected with the latest version of the worm, yes.

**Q:** But what's this peer-to-peer functionality I've heard about?
**A:** The worm has some peer-to-peer functionality which means that infected computers can communicate with each other without the need for a server. This enables the worm to update itself without the need for any of the 250 or 50,000 domains.

**Q:** But doesn't that mean that if the bad guys wanted to run something on those machines, they don't need to wait for April 1st?
**A:** Yes! Which is another reason why **it's unlikely anything major will happen on April 1st**.

**Q:** Is there going to be media hype?
**A:** Oh yes. Like there always is when a widespread worm has a date trigger. Think cases like Michelangelo (1992), CIH (1999), Sobig (2003), Mydoom (2004) and Blackworm (2006).

**Q:** But in those cases nothing much happened even though everybody expected something to happen!
**A:** Exactly.

**Q:** So, should I keep my PC shut down on April 1st?
**A:** No. You should make sure it's clean before April 1st.

**Q:** Can I change the date on my machine to protect me?
**A:** No. While the worm uses the local system time for certain parts of its update functionality it doesn't exclusively rely on that.

**Q:** I'm confused. How can you know beforehand that there will be a global virus attack on April 1st? There must be a conspiracy here!
**A:** Yes, you're confused. There is not going to be a "global virus attack". The machines that are **already infected** might do something new on April 1st. We know this because we have reverse engineered the worm code and can see that this is what it has been programmed to do.

**Q:** Would the downloaded program execute with admin privileges?
**A:** Yes, with local admin rights. Which is pretty bad.

**Q:** And they could download that program not just on April 1st but also on any day after that?
**A:** Correct. So there's no reason why they wouldn't do it on, say, **April 5th** instead of April 1st.

**Q:** Ok, they could run any program. To do what?
**A: We don't know what they are planning to do, if anything.** Of course, they could steal your data, send spam, do DDoS, et cetera. But we don't know.

**Q: They?** Who are they? Who's behind this worm?
**A:** We don't know that either. But they seem to be pretty professional in what they do.

**Q:** Professional? Is it true that Conficker is using the MD6 hash algorithm?
**A:** Yes. This was probably one of the first real-world cases where this new algorithm was used.

**Q:** Why can't you just infect a PC, set the clock to April 1st and see what happens?
**A:** That's not the way it works. The worm connects to certain websites to get the time-of-day.

**Q:** Oh yeah? Then shut down the websites where it gets the time-of-day and the problem will go away!
**A:** Can't. These are websites like google.com, yahoo.com and facebook.com.

**Q:** But surely you could spoof google.com in the lab to get a honeypot machine to connect to a download site today!
**A:** Sure. And the download sites **do not have anything to download**, today. They might, on April 1st. Or they might not.

**Q:** Now I'm worried. How do I know if I'm infected?
**A:** Try to surf to www.f-secure.com. If you can't reach our website you might be infected, as Conficker blocks access to security vendor's websites. Don't tell anybody, but users who can't access f-secure.com because of this can surf to www.fsecure.com instead.

**Q:** Where does the name "Conficker" come from?
**A:** Conficker is an anagram of sorts from **trafficconverter** – a website to which the first variant was connecting.

**Q:** Why does the worm have two names – Downadup and Conficker?
**A:** It was found at about the same time by multiple security companies and therefore got multiple names. Today most companies use the name Conficker. There's further confusion about the variant letters among vendors. We're all sorry for that.

**Q:** How many computers are currently infected with Conficker?
**A:** About 1-2 million. How many of those are infected with the latest version? We don't have an exact count.

**Q:** How is the industry reacting to all this?
**A:** We reacted by setting up the **Conficker Working Group**. Members include security vendors (including us), registrars, research units and so on.

**Q:** When was the first variant of Downadup/Conficker discovered?
**A:** It was found on November 20, 2008.

**Q:** Is this all just an April Fools joke?
**A:** No, it's not. And although we don't think anything will happen on this particular date, Conficker is nothing to laugh about. The gang behind this is serious and we should not underestimate them. The fact that we don't know for real what they are really after just makes it all a bigger mystery.

So, when exactly is Conficker activating?

It goes like this:

- Conficker checks the local clock every 90 minutes (in some cases even more frequently)
- The check is done with Windows **GetLocalTime** function
- GetLocalTime gives the local time, based on the local time zone
- Because of this, machines around the world are returning different times
- Clock skew affects this as well
- But not by much, as Windows machines will sync their local clock with time.windows.com **once a week**
- Once the local clock says it's April 1st, Conficker will collect a date from the net

This means that machines in Australia will already be collecting a date from the net when machines in Hawaii aren't.

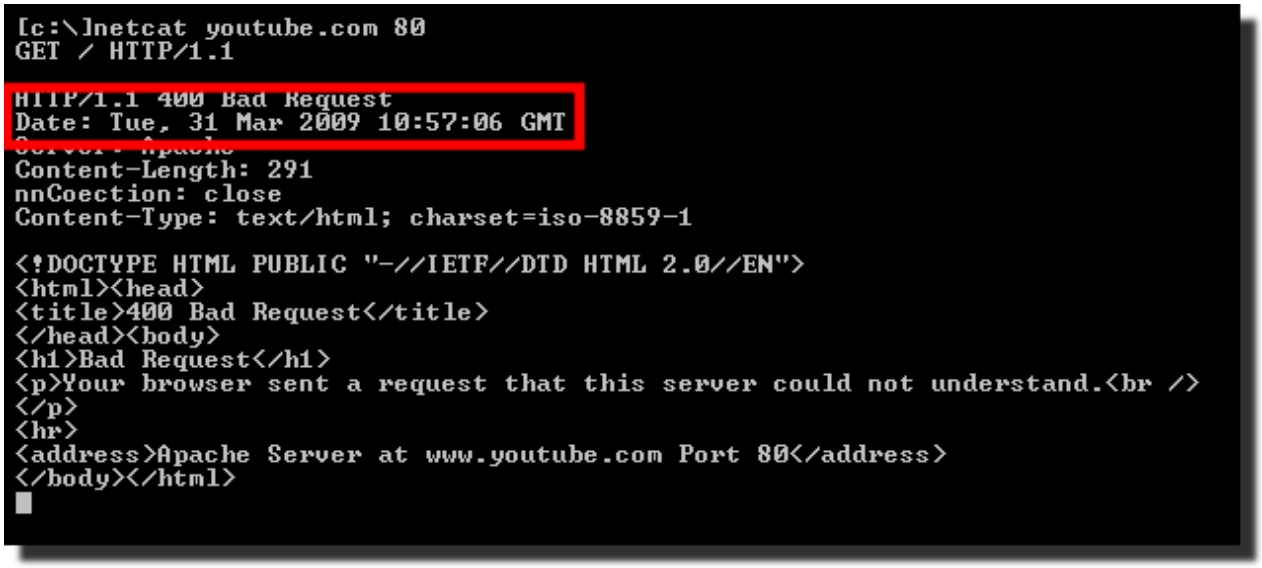
Conficker's net time collection uses several large websites to get the date. These are sites such as:

- adobe.com
- answers.com
- baidu.com
- bbc.co.uk
- comcast.net
- disney.go.com
- ebay.co.uk
- facebook.com
- imdb.com
- megaporn.com
- miniclip.com
- rapidshare.com

- torrentz.com
- typepad.com
- wikimedia.org
- yahoo.com
- youtube.com

The HTTP header time on these sites is very accurate and very close to each other.

You can check these yourself: simply connect to port 80 of any website with **netcat** or **telnet**. In Windows, simply run "telnet google.com 80". Once connected, type (blindly) "GET /" and hit enter a couple of times. You'll get a screenful of results, including a "Date:" field.




Here's some sample HTTP HEAD returns from websites that Conficker uses to check the date.

**Google.com**
Date: **Tue, 31 Mar 2009 06:27:42 GMT**
Client-Date: Tue, 31 Mar 2009 06:27:42 GMT
Client-Peer: 209.85.171.103:80

**Facebook.com**
Date: **Tue, 31 Mar 2009 06:28:24 GMT**
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Client-Date: Tue, 31 Mar 2009 06:28:24 GMT
Client-Peer: 69.63.184.143:80

**www.baidu.com**
Date: **Tue, 31 Mar 2009 06:31:47 GMT**

Expires: Tue, 31 Mar 2009 06:31:47 GMT
Client-Date: Tue, 31 Mar 2009 06:31:48 GMT
Client-Peer: 220.181.5.222:80

**www.youtube.com**
Date: **Tue, 31 Mar 2009 06:32:30 GMT**
Expires: Tue, 27 Apr 1971 19:44:06 EST
Client-Date: Tue, 31 Mar 2009 06:32:31 GMT
Client-Peer: 208.65.153.253:80

When the local clock says it's April 1st, Conficker will fetch the date values from the above sites and will use these values in an algorithm to generate 50,000 unique domain names. **Do note that even if the date from the web sites says it's March 31st, Conficker would still activate if the local clock says it's April 1st.**

The machines that are infected by Conficker.C and are turned on, will change modes between 00:00 and 01:30 on April 1st, based on machines own clock. The ones that are turned off, will change modes soon after they are booted up.

**Conficker.E**

On April 8th a new update was made available to Conficker.C infected machines via the P2P network. The new malware, Conficker.E, was executed and co-existed alongside the old infection.

It re-introduced spreading via the MS08-067 vulnerability. Spreading functionality was removed in Conficker.C and the gang behind this maybe realized they made a mistake and added it again.

The new variant does not have the domain generation algorithm like the previous variants have.

There's also a connection to rogue anti-virus products as we've seen it end up on Conficker.C infected machines. The rogue product was SpywareProtect2009.

Conficker.E deletes itself if the date is May 3, 2009 or later. It does not delete Conficker.C though so that will remain on an infected computer.

Additional technical details available at:
http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml