

# Conficker: The Battle for Everyman

*What will control the soul of a machine—good code or evil?*

*“There are a thousand hacking at the branches of evil to one who is striking at the root.”*

—Henry David Thoreau

**N**ovember 21, 2008 wasn't a normal day at the Symantec Security Operations Center in Calgary, Canada.

The center is one of several world-wide that are staffed 24×7 by security analysts as a part of the Symantec Global Intelligence Network. This network is “the feedback loop of the intelligence put into 130 million Symantec product installations around the globe,” says Dean Turner, who is the network's director. “The Symantec Global Intelligence Network informs us of malware, phishing, spam, data leakage, data theft, backup—the entire spectrum of security concerns, and it helps us build better end-to-end solutions.”

Back in November, one of the 32,000 vulnerabilities that the center was tracking was in

By Alan Drummer

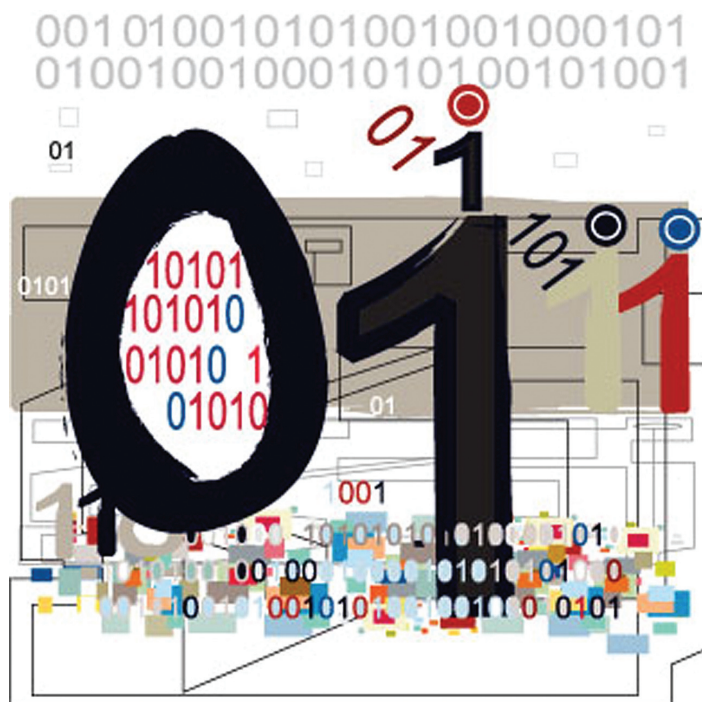
Microsoft's Remote Procedure Call (RPC) service. Microsoft had released a hot patch (MS08-067) for the vulnerability in October, but within weeks, Symantec DeepSight Early Warning Services—the monitoring system of the Global Intelligence Network—started to see increased TCP port activity on port 445. And on November 21, a DeepSight analyst in Calgary caught a piece of malware that was exploiting the vulnerability.

Symantec released a threat alert to its customers, checked with other security vendors, and sent the malware sample to the Microsoft Security Research Center for further analysis.

It turned out to be the variant A of Win32.Downadup, also known as the Conficker worm.

## Hacking at the Branches

Within a few months, Conficker.A, and its subsequent variants, had spread to what the Symantec team estimated was between two and three million computers,



becoming the most widespread network worm since Sasser in 2004. “The number of infections is difficult to estimate because we don't have visibility into how many machines may be behind network address translation or firewalls,” Turner comments. Behind a positive indication on a scan could be one, dozens, or hundreds of infected systems.

As analysts looked under the hood of Conficker, they found it remarkable for its sophistication. Said *The Downadup Codex*, a collection of postings on Conficker from Symantec Security Response Blogs, “this threat was able to jump certain network hurdles, hide in the shadows of network traffic, and defend itself against attack with a deftness not often seen in today's threat landscape. Yet it contained few previously unseen features. What set it apart was the sheer number of tricks it held up its sleeve.”

Among those tricks, the Symantec Security Response team notes, is the fact that Conficker

## Propagates itself expertly

- > It's polymorphic (its form changes), and it contains the ability to update itself or receive additional files for execution
- > Seeks to expand itself by checking daily for additional files from up to 50,000 possible DNS domains—a number big enough to make them difficult to block
- > Contains a peer-to-peer (P2P) updating mechanism, allowing one infected computer to update another. This has been used by Conficker to download other forms of malware such as the Waledac worm—which then attempts to spread itself by sending email with links to copies of itself
- > Attempts a brute-force attack of commonly used network passwords
- > Takes advantage of Universal Plug and Play to pass through routers and gateways
- > Uses AutoPlay to get users to execute it from removable drives

## Shields itself in a number of ways

- > Scans its network for vulnerable hosts, but selectively queries them to mask its traffic
- > Carries a large blacklist of IP ranges that belong to security vendors and does not attempt to exploit them, thereby avoiding “honeypot” systems
- > Encrypts transferred payload files, and only Conficker's authors have the key
- > Protects against buffer overflow exploitation—the technique it uses to attack—so that other malware authors can't exploit the Conficker botnet
- > Digitally signs an authentication for the command control channels of its bot networks
- > Contains a function to end security-related processes and blocks access to security sites to keep users from updating their security software

“This definitely wasn't the work

of script kiddies,” Turner says. “It's fairly complicated. The collection of skills required to not only help this thing propagate, but to armor it has been very sophisticated.”

## Collaboration Helps Both Attackers and Defenders

What's the objective of Conficker? “We don't know,” admits Turner. “Most likely the worm will be used to create a botnet that will be rented out to criminals who want to send spam, steal identities, and direct users to online scams and phishing sites.” The Conficker.E variant that was discovered on April 9 dropped a variant of W32.Waledac. This worm is one of the most active spam bots, stealing sensitive information, turning computers into spam zombies, and establishing a back door remote access to the infected computers.

Conficker could serve the vast Internet underground economy that Symantec researchers documented in a 2008 report,<sup>1</sup> where stolen information and illicit tools are bought and sold. Conficker itself could be the fruit of Internet collaboration. “I think that Conficker is probably not the work of one individual,” Turner explains. “Its source is probably a collection of individuals who are familiar with all the elements it represents.”

The threat it poses has triggered new collaboration among security companies. In February, 2009, Microsoft announced a \$250,000 reward for information leading to the arrest and conviction

Jeff Durfee, Director of IT Security, University of North Florida



## University of North Florida

**Founded:** 1972

**Headquarters:** Jacksonville, Florida

**Workforce:** Approximately 1,500 faculty and staff

**IT Staff:** Approximately 70

**Enrollment:** More than 15,000 students

**Website:** [www.unf.edu](http://www.unf.edu)

tion of Conficker's authors, and it also invited a group of Microsoft partners to work together in what has come to be called the Conficker Working Group ([www.conficker-workinggroup.com](http://www.conficker-workinggroup.com)).

Symantec was one of the invitees. “The group has since expanded to include all the major antivirus and security vendors, registrars, top-level domains, country top-level domains (CC TLDs)—just about everybody,” Turner says.

The collaboration is unprecedented. “Antivirus vendors are reverse engineering the malware itself and then providing their findings to everybody on the list,” Turner observes. “Samples were shared in the antivirus world

## “This definitely wasn’t the work of script kiddies.”

—Dean Turner, Director, Symantec Global Intelligence Network

before, of course, but generally not the actual analysis and the reverse engineering because that usually involves company intellectual property.”

While companies aren’t sharing their intellectual property now either, Turner notes, “the level of cooperation in trying to pull this thing apart has been pretty impressive. Companies are putting aside their competitive differences to work together and do something about this.”

### ▶ Witness to Malware: Symantec Global Intelligence Network

**130** million client, server, and gateway antivirus deployments

**240,000** sensors in 200+ countries

**6,000** monitored security devices

**2.5** million decoy addresses to capture spam, phishing, and security threats

Use the **Conficker Removal Tool** at [www.symantec.com](http://www.symantec.com) to get rid of the worm. If you can’t access [www.symantec.com](http://www.symantec.com), you may be infected.

An age-old battle has taken a new form: What code will control the soul of a machine—good or evil?

### The Fate of Everyman

Jeff Durfee is Everyman. His actual job title is director of IT security at the University of North Florida (UNF) in Jacksonville. There, his mission is to keep the infrastructure safe for more than 15,000 students and 1,500 faculty and staff.

Durfee became aware of Conficker by monitoring Internet security

sites. When he found out about it, he made sure that the 2,000 to 3,000 systems managed by the IT team at UNF were properly patched and protected. This wasn’t difficult, he explains, because “Altiris Client Management Suite from Symantec gives us insight into the software, processes, and patches that are running on our machines.”

But the school’s unmanaged endpoints—the laptops belonging to its 15,000 students—represent a bigger challenge. Durfee uses network access control software to ensure student laptops are up-to-date on their patching and antivirus protection before they can connect to the network. There is an approved list of antivirus solutions that students can choose from, and one of them—Symantec Endpoint Protection—has been purchased by UNF and made available to students free of charge.

“There has been a huge uptake of Symantec Endpoint Protection,” Durfee says. “We standardize on Symantec because it works very well in an enterprise setting, and it’s a very good client.”

There has been no disruption at UNF. “We have not seen much Conficker activity,” Durfee says. “We may have had one or two machines come in that were afflicted with something that looked like Conficker, but they were easily cleaned and corrected.”

The problem may not be over, however. “We’re not really off the hook yet. It could just be lying low. The biggest threat is malware that’s not as noisy,” Durfee notes. “That’s why we’re

very pleased with the way the players in the security industry have rallied so quickly to deal with Conficker.”

### Striking at the Root

Symantec’s Turner considers the talent behind Conficker. “I don’t have any respect for the effort that goes into creating malware like this,” he says. “Yes, the skill level and sophistication of these threats have increased over the past five to ten years. That’s driven in part by vendors building better and better security technologies. The bad guys have to create new variants and learn new tricks just to get their code out there.”

The ingenuity in the malware’s design doesn’t win any admiration either. “I think the problem is when people characterize this as a game,” Turner observes. “It’s not a game, because there are serious economic consequences. It’s no different than holding up somebody at gunpoint.”

Unfortunately, Turner adds, there will always be people inclined to make money the easy and illicit way. “And when you get down to the sociological question of why,” he concludes, “well, that’s a question we’ve been asking for 3,000 years.” ■

<sup>1</sup> “Symantec Report on the Underground Economy, July 2007 to June 2008,” Symantec Corporation, November 2008, [go.symantec.com/underground-eco](http://go.symantec.com/underground-eco).

*Alan Drummer is Creative Director for Content at NAVAJO Company. His work has appeared in the Los Angeles Times, San Francisco Examiner, Create Magazine, and on The History Channel.*

### ▶ Enhanced Security Against Malware

- > Altiris Client Management Suite
- > Symantec Critical System Protection
- > Symantec Endpoint Protection
- > Symantec DeepSight Early Warning Services
- > Symantec Managed Security Services