The Washington Post

Cyber Security Community Joins Forces to Defeat Conficker Worm

By Brian Krebs
washingtonpost.com Staff Wrtier
Friday, February 13, 2009; 3:01 PM

Advertisement » Your Ad Here


The quarter-million dollar award Microsoft is offering for information that leads to the arrest and conviction of those responsibile for unleashing the "Conficker" worm may represent the culmination of what security experts say has been an unprecedented and collaborative response from industry, academia and Internet policy groups aimed at not just containing the spread of this worm, but also in creating a playbook for dealing with future digital pandemics.

Estimates of how many systems infected by Conficker, a contagion that has exploited Microsoft Windows PCs over the past few months, vary widely, from 2 million to more than 10 million machines. Microsoft estimates that at least 3 million PCs worldwide remain infected. Yet, PCs sickened by Conficker have not yet been observed in facilitaing the kind of illegal online activities typically spewed by computers infected with malicious software, such as sending spam or hosting scam Web sites.

Rather, security experts say the worm may be the first stage of a larger attack. By using a mathematical algorithm, Conficker can tell infected systems to regularly contact a list of 250 different domain names each day. If just one of those domains is registered by the virus writer, it could be used to download an as-yet unknown secondary component to all infected systems maliciously, such as malicious software.

"This worm would be a marvelous tool in hands of whoever can control it, but the real harm from it has yet to be felt, and we're trying to postpone that day," said Paul Vixie, founder of Internet Systems Consortium, a Redwood City, Calif., company whose open-source software powers millions of Internet servers around the globe.

For several weeks after Conficker first surfaced in November, the anti-virus community began studying and publishing their research online. Individual security researchers were then able to begin registering the 250 domains sought daily by Conficker-infected systems to ensure those machines would not receive its intended instructions. At least one researcher told washingtonpost.com that he registered a number of the domains in the names of the FBI and Microsoft.

But, the FBI already was investigating individuals who were found to have recently registered domains sought by Conficker-infected systems, according to Bill Woodcock, research director of Packet Clearing House, a San Francisco based non-profit organization that provides support and training to companies that manage critical Internet infrastructure.

"There have been law enforcement folks trying to figure out who the holders of these domains are," Woodcock said.

Officials for the FBI did not return calls seeking comment.

Phillip Porras, director of the computer security lab at SRI International, also began tracking Conficker domains in late November. Porras and his team learned they could determine sets of domains sought by Conficker host systems in the past or the future, merely by rolling back or forward the system date setting on Microsoft Windows systems that they had purposesly infected in their test lab.

As Porras's group began building lists of domains sought by Conficker that had already been registered, they found hundreds that traced back to security researchers and anti-virus companies that were hoping to glean intelligence about the number of systems infected with the worm.

"We found that lots of people had registered these domains to try and gather size estimates and to better understand the worm," Porras said. "Early on, various folks were sharing this data privately, but nothing was really that coordinated."

Yet, as December rolled around and the number of machines infected by the worm swelled into the millions, a consensus began to emerge within the security research community that they needed a broader coordination effort.

That community had only weeks before learned the consequences of inaction in the face of another mounting threat. In late November 2008, the "Srizbi botnet," a massive collection of compromised Microsoft PCs that sent billions of spam e-mails each day, was knocked offline after Internet providers shuttered the Web servers that were being used to control and update the botnet's activities.

Researchers knew that Srizbi had a built-in fallback mechanism similar to the updating capabilities in Conficker, a failsafe device that could resurrect the botnet by forcing infected systems to seek out a randomly generated set of four domains that changed every 72 hours.

For several weeks, FireEye, a private security company in Milpitas, Calif., took it upon itself to register each of the domains that Srizbi-infected systems were told to seek out in order to allow criminals to regain control over the wayward systems. But as the costs of registering those domains mounted, the company ceased reserving them. On Nov. 25, a day after FireEye quit registering the Web site names, unknown individuals took over that task, and the Srizbi botnet was back online and blasting out spam.

Woodcock said many in the security community, including the Internet Corporation for Assigned Names and Numbers (ICANN), which oversees the domain registration industry, were eager to avoid a repeat of the Srizbi fiasco.

"Nobody wanted to go through a big exercise to deal with the Conficker worm and not have a process in place to make it easier the next time this happens with a different worm," Woodcock said.

Still, coordinating a Conficker counterpunch would require some bending of the rules that govern domain name registrations, along with unprecedented level of cooperation from foreign governments.

For example, "top level domains" most sought after by Conficker-infested systems -- dot-com, dot-org and dot-net -- have explict contracts with ICANN that prohibit them from unilaterally reserving Web site names, even the seemingly gibberish domains that were known to be sought out by Conficker.

Also, some of the domains sought by Conficker would need to be registered through registrars controlled by soverign nations that are not beholden to ICANN, such as dot-ws (Western Samoa), and dot-cn (China).

Rodney Joffe, senior vice president of Sterling, Va., based Neustar Inc., which has an exclusive contract with ICANN to manage dot-biz and dot-us domain registrations, said ICANN recently took the unprecedented step of allowing registrars to set aside any domains sought by Conficker systems now or in the future.

Joffe said ICANN was instrumental in waving those restrictions for domestic registrars, but also in convincing the Chinese and other international registrars to agree to shelve the Conficker domains.

"People blame ICANN when anything having to do with domain names being used for abuse comes up," Joffe said. "But this is one of those interesting instances where ICANN has been very progressive in the kinds of help they've given the registry operators. There seems to be growing, global understanding that these kinds of things don't reflect well on anyone in the industry and actually cause damage to everyone."

For its part, ICANN will continue to work with the registry community to refine its policies on how to deal with future domain name-based threats, said Greg Rattray, chief Internet security advisor at ICANN.

"We agreed with the registries that we need to look at how to do this in a coordinated, coherent fashion that enables the community to respond in accordance with the contractual policy guidelines while at the same time being operationally effective and timely," Rattray said. "We hope this can become the model for more collaborative response in the face of future threats."

Rick Wesson, chief executive of Support Intelligence, a security firm in San Francisco, called the international effort to contain the worm "incredible."

"Here we have the Chinese cooperating with the Americans on a cyber threat when so much of the rhetoric [from the U.S. government] is about concerns around the cyber threat from China," said Wesson, who was also one of the researchers who began registering Conficker domains back in November.

But it's too soon for the community to declare victory, Wesson said. The next domain-based worm could significantly ratchet up the number of domains, and thereby sideline a large number of Web site names that might otherwise be commercially viable and sought after by legitimate Internet users.

"I think we're going to have successes and we're going to have failures, and this one clearly isn't a success until Microsoft has paid a quarter of million dollars and the individuals behind this worm are in jail," Wesson said.

Post a Comment

View all comments that have been posted about this article.

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies

You must be logged in to leave a comment. Login | Register

governing this site. Please review the full rules governing commentaries and discussions. You are fully responsible for the content that you post.

Submit

© 2009 Washingtonpost.Newsweek Interactive

Ads by Google

Computer Trojan Remover
Detect & Remove over 500,000 traces of Spyware & Trojans. Recommended.
www.pctools.com

Domain Names
Register names at NetworkSolutions® 24/7 award winning customer support
NetworkSolutions.com

Domain names
Register your Domain Name Now Great deals, 140$ in free extras
www.w-global.com