Rogue software

The plague of rogue anti-virus

ebook

An SC Magazine publication

Sponsored by

Web of deceit

Tainted JavaScript, indiscriminate surfing and forged ads have snared millions of computer users into a variety of scareware scams, reports Greg Masters.

There's a new monster loose and it doesn't care who its next victim is. Rogue security software, aka scareware or extortionware, pretends to be legitimate security software. Like a beast from a 1950's sci-fi movie, the fraud preys on victim's anxieties. There are more and more variants of this, but all do the same thing: display fake pop-up ads on the monitor that proclaim a computer system has been infected and can be fixed by downloading what turns out to be a phony anti-virus product. As well, this malware can cripple a computer's functionality, making it impossible, for example, to reach a website where legitimate AV cures are available.

This plight has been around for several years, but in 2009 reached new levels of havoc. According to the "Symantec Report on Rogue Security Software," released in October, from July 1, 2008 to June 30, 2009, the company received reports of 43 million rogue security software installation attempts. Cybercriminals are evolving their strategies and using increasingly persuasive online scare tactics to convince users to purchase rogue security software, according to the study.

There are two ways that rogue security software can end up on a user's computer. In this case, it's a pop-up screen on the computer that poses as a warning that a machine has been infected with malware. The warning looks genuine, but entices the nervous user to click-through to what they believe will provide an antidote, usually a fake anti-virus fix that costs anywhere from $30 to $100. But the consequences of this fraud don't stop there. Once a user is lured into this scheme and gives up credit card information and other personal details, this data can then be used in further identity fraud practices.

Exacerbating the contagion is the fact that the spread is being promulgated by the victims themselves. Most computer users surf without caution, clicking through to whatever catches their eye, whether it be the latest news report or a celebrity meltdown. By visiting a website and clicking on a link that seems genuine enough – promising a video, for instance – they become victims and transfer malware onto their computers.

As well, once a victim installs the fake software, they are given the false hope that their system is now safe, when in fact it may be corrupted to the point where it is open to new attacks. This is because the malware often prompts users to close down firewall settings and/or disable existing anti-virus programs.

Where did this monster come from? Researchers have traced the ISP trail to sites in Russia and the Ukraine, where sophisticated programmers, in one variation of the ploy, create web pages that have all the appearance of a legitimate Windows OS screen. In fact, one researcher at the SANS Internet Storm Center, commented that the code was "very elegant and clean." After being delivered to a computer via a trojan, these phony screens pop up onto a user's monitor and dupe them into believing that their machine has become infected by a virus. As the message has all the appearance of coming from the Windows Security Center, the user is duped into believing that clicking through will provide an anti-virus solution and fix the dilemma. Instead, a rogue AV program is installed and the user then has to pay to have it powered on or, in more blatant extortion models, uninstalled. But the underlying JavaScript code ensures that wherever on the image a user clicks, whether on the "Remove all" or "Cancel" buttons, the malware will load.

Some iterations of rogue security software contain keystroke loggers and backdoor functionality, according to Symantec. This allows the malware authors to siphon off personal

Rogue software

43m

installations of rogue security software were reported to Symantec in one 11-month period

information on an infected computer. And, like legitimate registered software, this establishes a connection between the computer and a server controlled by the scam artists linking what is now estimated to be millions of computers together into a botnet. Thus, updates can be pushed out to the network commanding the enlisted computers to perform any number of functions.

The many-headed beast

Rogue AV spreads via many channels. It is promoted on nefarious, as well as legitimate websites, including blogs, forums, social networking sites and adult sites. While legitimate sites are not in cahoots with these scams, they can become feeders when unscreened advertisements for rogue applications appear on the sites via third-party ad networks.

As well, scamsters can manipulate the placement of their listings to the top of search engine indexes by seeding the results. For example, when the Conficker worm made its way into the headlines at the end of 2008, the malware bad guys published website pages padded with SEO terms to make the pages more likely to appear in search results.

It can also be delivered via a drive-by download. This occurs when a user visits infected sites from which malicious code is downloaded without the user's knowledge.

The notorious Conficker worm, also known as Downup, Downandup, Conflicker, and Kido, has been revealed to be another delivery system. According to the Conficker Working Group, an assemblage of individuals and representatives from sveral dozen organizations, the worm spreads itself primarily through a buffer overflow vulnerability in the Server Service on Windows computers using a specially crafted RPC request to execute code on the target computer.

Conficker is believed to have linked million of machines worldwide into a botnet (estimates vary from 10 to 15 million), in effect creating a gigantic virtual computer capable of being operated remotely by its authors. For a long time, experts were unsure of Conficker's intention. Though detected as early as November 2008, the worm seemed to be laying dormant and not causing any harm. That uncertainty ended last April when it was reported by Kaspersky researchers to be using its peer-to-peer functionality to load a rogue AV application, called SpywareProtect2009, onto infected machines. This subsequently brought the typical scareware offer to "clean" the PC, for a price.

The popularity of social networking sites has opened new channels for the worm as well. Fake member profiles were recently used on Facebook in an attempt to push rogue anti-virus programs to unwitting users. The profiles enticed "friends" to click through to a home video, which then brought users the usual offers for malware scans, a report of infection, and then the grand finale, the request for victims to enter their credit card and other personal information so they could install an anti-virus product, which turns out to be fake.

While Facebook disabled the offending accounts, this scourge is not going away. Users of popular blogging platform Twitter fell victim to a similar scareware scam. The infestation began after a blast of tweets – brief text messages containing a hyperlink – enticed users to juste.ru, reportedly a Russian domain, to watch a "Best Video." The site seemingly presented content from YouTube, but in the background delivered a malformed PDF via an IFRAME on that site. This image file contained a number of exploits intended to infect users using unpatched versions of Adobe Reader. Twitter staff confirmed the "System Security" attacks and reportedly cleaned up the offending messages.

Pay to play

According to the Symantec report, cybercriminals are benefitting from a well-managed pay-for-performance business model. Scammers working as sales agents receive a commission each time a web surfer falls

$23k

per week earned in commissions by one sales affiliate selling rogue anti-virus

for the ploy of installing the phony security programs. In fact, the study reports that the top 10 sales partners for one such "affiliate program," TrafficConverter.biz, reportedly earned an average of $23,000 per week. Others place this figure much higher. That site was shuttered a year ago.

The report goes on to say that the creators of the distribution websites supply so-called affiliates with fake codec links, fake scanner links, malicious code executable files, as well as marketing materials. Their bundle may also include obfuscation tools, such as packers and binders, which aids in avoiding detection by creating variations of the code, sometimes as often as every five minutes.

The problem is compounded by the fact that the criminals are clever, says Ryan Olson, rapid response director, VeriSign iDefense,. "They trick people into doing what we've been training them to do." Namely, click on a link to install AV tools. Only in this guise, the links don't deliver what they promise. Further, he adds, they are using personal information that users don't suspect anyone else but trusted partners could know, such as their email address, title, where they work, etc.

Solutions are out there

The plague of rogue security applications is not going away anytime soon, despite a number of legal actions here in the United States and abroad to prosecute on charges of fraud and spam distribution. While some actions have led to prosecutions and fines at state levels and from actions brought by the Federal Trade Commission, the profits to be gained by perpetrators well-hidden behind a hard-to-trace computer trail is too much of an incentive to stop the business.

But there are tools and strategies to help in the battle. The first step, say many experts, is educating computer users to become alert to the dangers of clicking on suspect hyperlinks that will infect their machines. Most computer users are ill-informed or even oblivious to security precautions. For instance, when Microsoft released a security patch for Conficker, nearly a third of its users, according to estimates, didn't bother to install the update to their systems.

"We're definitely going to be tracing the money trail," says iDefense's Olson. But as far as mitigating the problem, he concurs that traditional AV products tend to be behind the ever-evolving threats out there. He says users must install trusted AV solutions and keep upgrading as soon as updates are released. But, he says, "I see no decline in rogue AV, it's only going to get better. It's a huge problem that's going to be difficult to fix."

Olson says that user education is essential to thwart this plight. "We've got to alert people to attacks," he says. Having intelligence in advance, training people to be aware that this is possible and to not open suspicious attachments are the first line of defense, he says.

Marc Fossi, manager, development security technology and response at Symantec, and executive editor of the Symantec report, agrees that education is key. "It's not just a matter of pointing out that this is a bad thing, using FUD strategies," he says. "It's more along the lines of explaining that this stuff is out there, and pointing out the tricks being used. It's vital to raise flags and make people think twice."

Brian Hazzard, vice president of product management at Waltham-Mass.-based Bit9, a company that offers whitelisting products and services, says that traditional anti-virus products can no longer keep up with all the new attacks. "Rogue software is designed to go around traditional technologies," he says. "We don't look for known bad software, as it's always changing. You have to change the paradigm." Whitelisting, he explains, allows only good software to run on a system, and it can be implemented in the enterprise so that IT can automatically manage use.

However, the fact is, the bad guys are outmaneuvering the security providers. Several vendors, including Microsoft, have released tools to remove Conficker. But the risk of re-

Rogue software

$250k

reward offered by Microsoft to catch author of Conficker remains unclaimed

infection remains high as systems are susceptible from USB sticks. Additionally, as soon as a patch is released, the malware authors evolve their attack to devise exploit new openings in the Windows environment. New security options in the just released Windows 7 operating environment may put a dent in the cat-and-mouse proceedings, but no one is holding their breath. In fact, Microsoft has offered a $250,000 reward to anyone who can nab the authors responsible for Conficker. The reward sits uncollected.

At the same time, technology offerings are struggling to keep up with the increasingly sophisticated code and methods used by smart criminals motivated by the promise of substantial monetary gain.

Shawn Eldridge, vice president of products and marketing at DeepNines, says that his company's Secure Web Gateway product filters every URL that users visit to inspect and compare that URL to a database of suspicious and known toxic sites. It then does content filtering to check for violations. "If the website manages to get past these two filters," he says, "when the page is downloaded it is scanned for content to make sure it doesn't violate policies."

Symantec's Fossi says one of the principal strategies the bad guys use is to take advantage of name recognition, naming one product Nortel Antivirus, for instance, a play on the actual Nortel telecom company and his company's Norton AntiVirus tool. "On some of the sites they put together, they make them look like legitimate vendor sites, using the same colors and layout," he says. "They're muddying the waters, using social engineering to make it look legitimate." Some of the sites grab testimonial quotes from a real AV product and tack it onto their sites, or even offer lifetime subscriptions to Norton AntiVirus with pictures of the actual boxes, though Symantec offers no such deal.

Marketplace effect

It's difficult to estimate the effect these rogue offerings are having on the legitimate marketplace. The sources we spoke to for this article had no hard evidence to quantify whether their sales were being cannibalized by the counterfeit offerings, or perhaps even harder to measure, whether their brand images were suffering a loss in consumer confidence.

"We have no way of knowing how many people are buying the stuff," says Symantec's Fossi. He says he hasn't heard whether his company is getting an increased number of support calls coming from customers who believe they've bought Symantec products, but in fact bought counterfeit goods. "Once they've been duped, oftentimes they don't like to admit it," he explains.

However, Fossi does say that it could potentially damage the reputation of legitimate vendors if people think they're purchasing legitimate software and it turns out to be phony. "A lot of these fake offerings tend to sound legitimate, so it makes it difficult for smaller, legitimate vendors," he says.

iDefense's Olson agrees that rogue software has been incredibly prevalent this year. But he too is unsure of what, if any, effect it is having on sales of legitimate products. "We did see Microsoft release its free AV product, so we might see a drop on the consumer side," he says. ■

20k

samples of rogue AV were identified in the first half of 2009

Sponsor

Thawte is a leading global Certification Authority. Our SSL and code signing digital certificates are used globally to secure servers, provide data encryption, authenticate users, protect privacy and assure online identifies through stringent authentication and verification processes. Our SSL certificates include Wildcard SSL Certificates, SGC SuperCerts and Extended Validation SSL Certificates.

Masthead

EDITORIAL

EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com

DEPUTY EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION

ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com

SENIOR PRODUCTION Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES

ASSOCIATE PUBLISHER, VP OF SALES Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*

EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*

WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*

NATIONAL INSIDE SALES EXEC. Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*