Experts Fear Trojan Proxy Server Virus

(10/13/99, 7:05 p.m. ET)
By Lee Kimber, TechWeb

Security experts are trying to track down the perpetrators of a huge Internet surveillance operation that they say could presage an attack on websites around the world.

Members of the Bethesda, Md.-based System Administration, Networking, and Security (SANS) Institute have already identified over 200 copies of a Trojan virus called RingZero that scans Web proxy servers and relays its findings back to remote computers across the Internet.

That means information, including credit card numbers, and other private transaction information could be stolen.

Since SANS warned its 64,000 members to check for the Trojan after the first was discovered two weeks ago, its researchers have slowly pieced together frightening evidence of a systematic attempt to gather information from commercial proxy servers. Proxy servers are widely used by business to handle Web access on office networks. They host intranet websites, let administrators restrict the websites staff may visit and cut bandwidth costs.

Once installed on a network, RingZero's pst.exe file randomly scans for proxy servers and makes them send their own Internet address and port number to what appears to be a data collection script running on a machine at www.rusftpsearch.net.

Crackers use IP addresses and port numbers as a starting point for breaking into computers.

"It's a quantum leap in distributed attack technology," said SANS security researcher John Green. "The proxy is being used to send its own IP address and proxy port home to the mother ship."

But SANS researchers think RingZero has other abilities too. They found the Trojan has a second part, called its.exe, that tries to retrieve files directly from Web-servers. Both parts seem able to work independently of each other. The researchers are currently trying to determine what the file-retrieving component does with its booty.

SANS is asking network administrators to check their systems for files called pst.exe and its.exe. It also wants to hear from any administrator who sees outgoing network traffic on port 8080 and 3128. Seeing such traffic on a network that doesn't have a proxy server is a strong sign that they have been infected by the RingZero
Zero Knowledge Systems: Hacking a Path to Net Privacy

By Lewis Perdue
VC Watch Editor  Stock Report Archives

There's no better example that one person's hack is another's privacy shelter than the fracas this past April between Intel Corp (INTC) and Zero Knowledge Systems.

Back then, ZeroK was an unknown Montreal start-up specializing in the development of Internet privacy software which had the temerity to announce that Intel's method of hiding the Pentium-III's infamous serial number was totally bogus and could be bypassed by any number of methods without the user's permission or knowledge.

Masterminded by crypto-cyberpunk Ian Goldberg who's broken more encryption keys than most Mafia enforcers have knee caps, the bypass was an Active-X applet that could secretly turn the serial number back on even if the PC owner had used Intel's utility to turn it off.

Goldberg, a Ph.D. candidate at the University of California at Berkeley is known for his part in cracking the 40-bit DES code in the RSA Challenge in three and a half hours; breaking the Netscape encryption system SSL; and breaking the cryptography in the GSM cellular phone standard. But when ZeroK announced the gaping hole in Intel's claims and posted the applet on its site, the embarrassed chip giant melted down. Intel declared the company a hacker site which was distributing malicious Trojan Horse code and immediately sicced Symantec and other virus software vendors on to the little company which quickly found itself branded as an online criminal.

"It's a typical 'shoot the messenger' approach," said ZeroK Founder and President Austin Hill who also pointed out that the company posted the applet only after it was clear that Intel did not intend to close the privacy gap.

Over the next couple of springtime weeks, Zero Knowledge Systems exchanged some pretty sharp public comments with Intel and Symantec that made the big guys look like back alley bullies ganging up on the class geek. And while the P-III chip still has privacy holes big enough to fly the Hindenburg through, ZeroK landed $12 million in venture capital on Sept. 30. thanks, in part, by the high profile it got from the controversy.

"The fracas did a lot of good raising both the issues and their profile," said Mike Santer, partner with Platinum Venture Partners which led the company's first round of venture along with Aragon Ventures and Strategic Acquisition Ventures. "Some big companies underestimate what happens when it looks like they are stomping the little guy."

ZeroK's new investment will allow it to roll-out its Freedom Network later this year. Users download free software form the company and then create pseudonyms (they call them "nyms") which cost $10 per year each. The software works alongside the user's existing browser, e-mail, chat, telnet or USENET software to encrypt the message into multiple layers of encryption and re-direct it through ZeroK's own server network.

According to the ZeroK Web site, "It's as if you were putting a scrambled letter into three or more envelopes, each with a different forwarding and return address. By creating one or more pseudonyms to use for different types of online activity - for instance, one for discussing health issues and a different one for job searching - you can prevent the two from being linked together and traced back to you in the real world. No one, not even Zero-Knowledge, will be able to connect your nyms to your true identity.

User cookies are stored on the user's computer in a "Cookie Jar" with a separate Jar for each nym.

According to ZeroK, "The fact that we don't store the cookies on our servers is one of the many distinctions between us and companies like Privada; we don't ask for, or hold, any of our users' personal information or cookies. Privada, Digitalme, Lumeria, Passport, Privacybank all act as gatekeepers for their users' information. You have to trust them with your privacy, whereas we don't ever ask for people's personal information. If they want to give it out, that's their business."

"I don't think this will upset user profiling," Santer said, "But it will allow the user to control their own privacy. Users have no faith in companies that promise to keep information private. This allows the user to determine the level of private they want."
Privacy Group Wants Users To Jam Spy Network

(10/11/99, 12:50 p.m. ET)
By Madeleine Acey, TechWeb
An Internet privacy group is planning a day of action against Echelon, the documented but officially secret intelligence services' electronic spying network.

Contributors to the Hacktivism mailing list have decreed October 21st "Jam Echelon Day" and are encouraging others to bombard the keywords-based listening network with provocative terms such as "revolution," "manifesto," and "revolt" in e-mails in the hope of overloading it.

Numerous books and a European Union study have detailed how the UKUSA alliance (comprising the intelligence services of the United Kingdom, United States, Australia, Canada, and New Zealand) has listening stations around the world scanning international phone, fax, and Internet transmissions for keywords mostly determined by the U.S. National Security Agency (NSA).

Other privacy groups welcomed the Hacktivism action as a symbolic gesture, but said they doubted it would have any great practical impact.

The organizers accepted that overloading the system might be an unattainable goal.

"Is it not better to signal displeasure at being monitored than passively allow it to happen? We believe so" the organizers said in a statement on their website. "Privacy should not be something that's considered only after it's been breached."

"I think a mass action is a brilliant idea, but from what we know, Echelon works on context analysis not just keywords," said Privacy International director Simon Davies. "If you look at the number-crunching power that would be necessary to do a straight keyword detection on mass communications, it's not hard to conclude that the manpower back-up would swamp the NSA. It seems to me a great symbolic step, but I don't think a keyword action itself is going to cripple the system. What would do it more readily is if there were particular themes followed and if they used keywords used in diplomatic and military contexts."

Nicholas Bohm of the London-based Foundation for Information Policy Research added that using low-level encryption would have a greater effect of clogging up message processing.

Bohm said what the Hacktivism group had planned could "damage the ability of the system to reach relevant messages."

"If everybody used trivial strength encryption, that would overload it," he said. "They've got to decrypt every message. This requirement would become unfeasible with huge volumes of processing."
Hotmail Still In Virus Hot Seat

(10/15/99, 2:34 p.m. ET)
By Lee Kimber, TechWeb
Hotmail still leaks up to 56 of the Internet's most virulent viruses, despite Microsoft's claim that it had patched security at the trouble-prone e-mail service, according to anti-virus experts. Those experts, who test every few days for viruses, said they successfully sent virus-infected e-mail through Hotmail's virus-scanning system earlier this week to prove that the hole is still open a week after Microsoft announced its combined audit with TRUSTe had left its system secure.

Anti-virus engineers at Star Internet, a Cirencester, England-based ISP, and other anti-virus experts said Microsoft engineers have known since last May that Hotmail's McAfee anti-virus scanning system leaked dangerous VBA-macro viruses such as Melissa.

Hotmail's engineers could not fix the problem because Hotmail runs on FreeBSD Unix, according to Star Internet. And Network Associates, which owns anti-virus software maker McAfee -- has produced a fourth version of McAfee anti-virus scanner that can detect Melissa-style macro viruses, but that version does not run on the FreeBSD Unix operating system used by Hotmail.

Anti-virus experts at Star Internet said they urged Hotmail to fix the problem after Hotmail became the biggest source of macro viruses in their business customers' networks.

"[Hotmail] confirmed the problem, then denied they had a problem," said Star anti-virus specialist Alex Shipp.

Shipp corresponded with Hotmail engineers via e-mail to alert them to the problem.

Microsoft refused to comment on whether it contracted Network Associates to write a Melissa-capable McAfee scanner for FreeBSD this summer. However, sources close to Network Associates' anti-virus development team confirmed that a beta version of the updated scanner was delivered to Microsoft for testing in mid-September.

Microsoft's slowness in dealing with security risks highlights a serious problem with free Internet services: They do not have enough money to fix problems, experts said. While Hotmail has substantial financial backing from parent Microsoft, many free

---

Intel's Hot Numbers Promise More Privacy

If you care a lot about keeping your data private, you should be concerned about your PC's ability to produce random numbers. A PC uses random numbers to generate encryption keys, which are used to secure much of the data sent over the Internet. But a truly random number is hard to find. Most PCs today generate pseudo-random numbers, using an algorithm seeded with a number that isn't quite random--the system's time of day. Eventually, a determined hacker can figure out the basis of the calculation and then grab the encrypted information--for example, data that's exchanged in the course of an online purchase.

Tough to Crack

Intel's 810, 810E, and 820 chip sets include hardware designed to foil even dedicated hackers. The so-called random number generator built into these chip sets derives a seed from the system's thermal noise: tiny, unpredictable variations in electrical current due to very slight changes in heat. Thermal noise-based seeds are hard for hackers to crack.

But there's one catch: For the RNG to work, encryption programs must tap into it--and today's apps don't know that it exists. Software and Web site support should begin late this year and gather steam throughout the year 2000, Intel says. (By then, all new Intel-based PCs will likely be shipping with hardware-based RNGs integrated on the motherboard.) As yet, AMD and Via do not incorporate an RNG in their system chip sets, but there's no reason they couldn't do this in the future. So while Intel deserves plaudits for its efforts to address long-standing security concerns, its RNG won't be an instant panacea for the many Internet security dangers. And you'll need a new PC to benefit from it at all.
Hotmail Still In Virus Hot Seat – Continued...

services run on the thin income streams they generate from banner ads and marketing surveys.

"Although we've contacted several free ISPs, none have shown much interest in offering e-mail virus scanning to free e-mail customers", Shipp said.

He said ISPs that sell to business customers were much more interested.

"I guess because it's just money off the bottom line to them," he said.

Graham Cluley, a senior technology consultant at anti-virus vendor Sophos, said anti-virus scanning is seen as a luxury.

"There's a lot of hype about ISP virus scanning at the moment because it's a nice feature to have," Cluley said. "It's also true that only a few ISPs are providing this kind of functionality."

Those ISPs tend to sell services to businesses rather than give them away to consumers. Cluley cites Star, intY, and LanSoft, who all use their extra security to promote their services to businesses. Yahoo and Excite do not virus-scan customers' free e-mail accounts.

But there's no evidence that security risks are damaging free Web services.

"The customer gets what they pay for," said Butler Group research analyst Carey Gray. "In the long term, I do not feel that these glitches in Hotmail security will reduce the [adoption] of e-commerce services."

SSG – Mission
The Student Systems Group's (SSG) purpose is to act as a link between the academic and business world through an affiliation with a professional information resource management association.

Newsletter – Mission
To disseminate information on current events and issues concerning the Information Technology field.

SSG Gears up for Tampa Florida!

Keep an eye out for us! We are shifting gears from competition to Fund Raising for our next endeavor in Tampa, Florida! We’re looking at raising approximately $20,000 by this spring. We need all the help we can get! If you see us out there, stop by and help us out by purchasing what ever it is we are selling at the moment. We thank you in advanced for your support.

Are you interested in Computers and Information Technology? Join the Student Systems Group Today!

“The Informant” Newsletter Team is looking for dedicated individuals to participate in this publication.