



From: www.cio.com

Hacker Economics 3: MPACK and the Next Wave of Malware

– Scott Berinato, CSO

October 08, 2007

May: A Poor Re-emergence

The hackers known as 76 and Exoric weren't just the managers of 76service; they were also clients. Through his undercover work, [SecureWorks](#) researcher [Don Jackson](#) found that Exoric himself owned a project – a portfolio of trojan-infected machines – just like the ones the team sold. Only, since access was free to him, his was a much bigger project, with hundreds of bots focused exclusively on Gozi-infected machines in Mexico and Chile (.mx and .cl domains), and no 30-day expiration. For a while, Exoric also used his own storefront for the Latin and South American markets, called GucciService.

Special Report: The Hacking Economy
[Hacker Economics 1: Malware as a Service](#)
[Hacker Economics 2: The Conspiracy of Apathy](#)
[Hacker Economics 3: The Next Wave of Malware](#)
[Key Malware Terms](#)
[A Trojan's First Second](#)
[Death by iFrame](#)
[Inside a Hacker's Site: Screenshots](#)



But by May the business was strained by the constant pursuit of researchers writing signatures to detect Gozi and law enforcement working with them to find and take down the 76service servers.

Early in the month, Jackson was able to say “Gozi isn't working. No one is going to the site.” At this time, his personal site was also the victim of what he termed a poor DDoS attack that lasted 36 hours. Soon after that, when he visited 76service.com, he found it abandoned, with a simple message: “I choose shadow. Please, never come back again.”

It seemed that, finally, it was over. But it wasn't, of course. In fact even before Jackson found 76service.com abandoned, a new Gozi variant was already at work, and it would be learned that it had been infecting machines since at least April 14. This latest Gozi bot was better than ever. It had added keystroke logging as an alternative to form grabbing. And recognizing that researchers were their primary adversaries, the new version added features to stymie detection and reverse engineering. “Every copy of Gozi has a unique infection ID,” explains Jackson. “So when data comes into the server it can check against the ID to make sure it's a valid infection. This new version also checked to see what your bot had sent before. Basically it could shut you off if you kept logging in without delivering good data, which is what researchers do.” The new version also logged the bot's IP address so that it could be

blocked from communicating with the server.

But there were problems. A programming glitch caused the service to create huge files of redundant information, interrupting service to customers while the duo tried to fix it. "That's why QA testing is so important," deadpans Jackson. They had only nabbed about 500MB of data off of 200 infected PCs when their new ISP, which Jackson says was based in Panama, took them offline again.

It was a poor reemergence. Lurking on a discussion board with a colleague who could translate Russian, Jackson found a post by someone named 57, a hacker thought to be part of the HangUp Team. 57 wrote that 76 broke off work with Exoric because the two were spending more time on the lam than they did running the service.

The [FBI](#) had wound down on the case, according to Jackson (though in an official statement given to CSO from the press office, the FBI says it welcomes any leads on information related to Gozi and 76service, which it termed "unique"). While they continued to monitor some accounts they knew were connected to 76service, Jackson didn't think it would progress beyond that. 76service was officially defunct. By early June, 76 and Exoric had dissolved their partnership.

But 57 also seemed to indicate that 76 was back with HangUp Team and busy rewriting the Gozi form grabber. The new architecture would allow 76 to hide the drop servers from prying eyes, making it harder to interrupt or shut services down.

Jackson predicted at the time that a new 76service would follow in kind. After all, 76service didn't fail because of the service model. It failed because of a lack of manpower to secure and manage the service. It couldn't scale. "I think they cobbled together Gozi and 76service to see what it could do," says Jackson. "They realize what they need to do next. They spotted weaknesses. Torpig was the next step; it was better. Now what's next?" With the help of the HangUp Team, a 76service-like site capable of enduring its own success, will return using some descendant of Gozi or Torpig.

[*Next: A Radical New Strategy for Banks?*](#)

The Radical New Strategy?

If users are, as one bank CISO said, dumb; and if banks can just write off their losses; and if the Internet is fundamentally insecure; and if vendors defenses can't keep up; and if law enforcement is overmatched; what happens next?

Don Jackson thinks that the banks will simply transfer more of the risk. "The banks are worried but their answer is not to track these guys down or be more diligent about security," says Jackson, who says he remembers talking about this with bank security types at last year's Information Systems Security Association (ISSA) conference. "Their answer is to shift more responsibility on to their customers. They'll lower fraud limits, the amount of stolen funds they'll cover. They'll make it harder for consumers to prove they were defrauded—and easier to say it was the customer's fault.. You'll have to prove that you kept your end of the deal by patching your system and so forth. Watch the terms of use for online banking. I think you'll see changes."

Like Jackson, Chris Rouland of [IBM ISS](#) believes the days of acceptable loss at the banks are numbered, but he has a hard time seeing a "blame the customer" strategy succeed. "These write-offs, this thing about putting it on consumers, it will end. It has to," he says.

Rouland says that he is rethinking security at a fundamental level, and many others in the industry are as well. "We're basically telling banks that client security is your problem, not [your customers'] problem. We're saying all the awareness in the world can not adequately secure client machines. Telling customers to secure themselves will not work. We believe that in order to fix the problem, you have to protect customers' customers. You have no choice."

Notice Rouland did not say you have to secure the client. He never says the banks must figure out a way to protect that machine. That's careful and deliberate, because Rouland doesn't believe that's what banks have to do. When it comes to security PCs, Rouland's advice is radical: Give up.

"In the next generation," he says, "we will all do business with infected end points," he says.

He was asked to repeat what he said, just to be sure. So he did: "Our strategy is we have to figure out how you do business with an infected computer. How do you secure a transaction with an infected machine? Whoever figures out how to do that first will win."

[Next: June—disturbing developments](#)

June: Disturbing Developments

By mid-June, Gozi was practically forgotten, and the new thing was MPACK. This one even had some veteran researchers muttering pesdato!

A typical Trojan like Gozi might rely on one exploit to try and open up a connection with the target PC. MPACK, on the other hand, is a briefcase full of exploits, a dozen or more of them. Mostly they're old exploits, but the idea is that if you try 15 different lock picks, one is bound to get you in. What's more, MPACK then reports back to its server which exploits worked where and stores that information in a database, an intelligence function used to effectively pack the briefcases with the most successful lock picks. The practice seems to have vastly increased the successful infection rate of PCs that visit sites delivering MPACK.

MPACK is actually sold with malware such that once the briefcase of exploits gets access, a Trojan—often Torpig—will be delivered to the PC. Other Trojans, like Apophis (which steals digital certificates) and even the old Nuclear Grabber that Corpse was hocking more than a year ago are also available in conjunction with MPACK. It costs hundreds to thousands of dollars.

Researchers still trying to penetrate this service say that MPACK is being sold by sash, likely the same as "sash" who posted news of Corpse's semi-retirement on the Pinch3.net discussion board. (Sash sells Pinch, too). Sash in turn seems to be working with Step57, a group likely run by 57, the HangUp Team coder who Jackson had found who posted the news of 76service's demise. All of these players have connections to the Russian Business Network, according to several researchers, including Jackson.

MPACK's multiple-exploit technique was used before in an exploit called WebAttacker. But MPACK is more effective because of iFrames. Disturbingly, the iFramers seem to have come up with some automated exploit kit capable infecting a massive number of Web pages with illicit iFrames in a short period of time, "like a machine gun spraying holes in sites" says Lance James. The first round of iFrame injections created to deliver MPACK showed up, literally, overnight—more than 10,000 pages were infected, mostly on Italian sites. Since then the process has repeated itself, moving country to country. Thousands of infections all at once.

Researchers are still trying to understand what allows the deployment of so many iFrames so quickly. Mostly they're reporting on rumors and theories. Using a virtual host to infect many sites is one working theory. But no one knows yet for sure how it's done. What they do know is iFraming is officially pandemic. "The iFramers are making a killing," Jackson says. "They don't get their hands dirty with the actual malware. They just break into a server with scripts. It's a good business to be in right now."

[Next: The evolution of malware continues.](#)

Fraud 4ever

"The thing about MPACK," says James, "this is the start of the whole thing." By this he seems to mean that Golden Age of Internet Crime, that dawning era. "They're starting to think like architects instead of engineers." MPACK brings together the best iFrames, the best exploits and some state-of-the-art malware into a single package all of which is being improved constantly, and sold with a focus on customer service. In marketing parlance, it's not a product, it's a solution.

Special Report: The Hacking Economy

[Hacker Economics 1: Malware as a Service](#)

[Hacker Economics 2: The Conspiracy of Apathy](#)

[Hacker Economics 3: The Next Wave of Malware](#)

[Key Malware Terms](#)

[A Trojan's First Second](#)

[Death by iFrame](#)

[Inside a Hacker's Site: Screenshots](#)

Business is good. Internet criminals operate with de facto immunity. The pool of vulnerable computers to

exploit remains massive. The target financial institutions still treat their crime as acceptable loss. Law enforcement is otherwise occupied. And technical defenses are mere market conditions to adapt to. For example, when some clever banks came up with a way to beat keylogging by having users use "virtual keyboards" on the screen, criminal hackers just developed Briz, code that captures the pixels around the cursor, the pictures of the characters being typed. Problem solved.

The criminals innovate. Some tactics will make the hair on your neck prickle. Rumors persist of a nasty Brazilian banking Trojan that can change banking account numbers, routing numbers, balance, and payment/transfer values by injecting HTML or even whole, cloned HTTP requests into an online banking session on the fly, such that the person banking would see false information that reflected their intentions and not the actual transfer. Chris Rouland of IBM has seen similar functionality in a bot called Grams.

Prg, another form-grabbing Trojan discovered last October, makes researchers awfully nervous. New variants emerge every couple of months and managed to steal tens of GB of data before being detected. Its encryption is strong and well-designed, its ability to hide itself with anti-forensics deft.

In June, Don Jackson found a new Prg variant. It shipped with a development kit which allows anyone who buys it to adapt the code on the fly in order to evade anti-virus and anti-spyware. On the server where he found it, he also found a staging area where new variants were already developed and waiting to be released as soon as the defenses recognized and blocked the current variant. He also found a couple of drops for two different groups who had bought Prg and distributed it through both iFrames and some good old-fashioned "click-on-this-link" emails. The drops comprised 10,000 account credentials, including second factors of authentication and answers to those security check questions like your mother's maiden name meant to layer extra security into the online banking process.

"There's a consumer side of me that says, Be cautious but life must go on. Someone somehow will take care of this," says Christopher Hoff. "And the security side of me wants to curl up in the fetal position and not go out."

After Jackson discovered the Prg variant, he learned of two more Gozi variants found in the wild. The EXE inside these versions is called 76.exe, and is probably the product of 76's reunion with the HangUp Team. It's pesdato! It has vastly improved its server network and obfuscation techniques. It bounces traffic from country to country. It hides its drops well. In fact, Jackson's not sure what it even connects to. He's looking for the front end, the next 76service. He knows it's out there. But so far he can't find it.

2002-2007 CXO Media Inc. All rights reserved. Reproduction in whole or in part without permission is prohibited.