WIRED

<< Back to Article

Report: Cybercrime Stormed the Net in 2007

By Ryan Singel 12.07.07 | 6:30 PM

Security researchers say 2007 was the year online criminals showed off how smart and dangerous they can be.

Anti-virus vendor F-Secure added 250,000 new signatures to its malware database this year -- as many as the company added in its first 20 years combined.

"The driving force is that the malware is being done at a professional level," according to Patrik Runald, security response manager for F-Secure, speaking about the company's end-of-the-year report, released this week.

That explosion didn't come from hordes of hackers feverishly writing new programs to steal password and credit card numbers, though. Instead, hackers perfected automated tools that wrapped old exploits in new gift boxes -- sometimes changing the appearances of files offered as downloads as quickly as every five minutes.

That mighty morphing malware menace is one of many signs that individual fraud artists, organized crime and Eastern European hackers are transforming the face of online crime. Black-hat hackers increasingly infect legitimate sites with drive-by downloads and find clever ways to reap financial gain from malware. Online hijinks are no longer the province of curious teen hackers; 2007 made it clear it's all about the Benjamins.

Anti-virus programs that load new signatures every night can't compete with such sophistication and have to rely instead on examining downloads to figure out what they do, rather than what they are.

This was also the year criminals began perfecting botnets -- collections of compromised computers ordered by a hacker remotely to send spam, launch denial-of-service attacks or host phishing websites.

One botnet variant known as Rockphish used a technique known as fast flux DNS that let its owners create fake banking sites that were nearly immune to traditional website takedown techniques. Fast flux constantly rotated the location where a user would find a web page by changing which of the thousands of computers in the botnet was serving up the fake banking site at any moment.

The Storm botnet, which kicked off in January 2007, used e-mails about current events -- from a massive European storm to the beginning of NFL season -- to trick users into installing malware. Later, once anti-virus vendors figured out how to better block the attachments, the message began directing victims to websites packed with browser exploits that could install malware without any help from a clueless user.

Unlike most botnets which can be killed by disabling the master server that sends commands to the army, Storm uses peer-to-peer communication technology to render it immune to decapitation. Storm also noticed when researchers were poking around and launched reverse attacks on their computers, flooding them with torrents of useless traffic.

"It's pretty much impossible to close down," Runald said.

While researchers believe Storm is controlled by criminal elements in Eastern European countries, it seems to be attempting to steal mostly from Americans.

"It seems to have a U.S. focus -- the social engineering tricks have been things that attract Americans," Runald said. "That leads us to believe they have at least some sort of agent working inside the United States."

Now Storm's owners are segmenting the botnet, comprised of millions of computers, into smaller botnets, which security researchers think may be a prelude to renting out the smaller chunks to other spammers and phishers.

Meanwhile, Mark Gaffan, who works in security giant RSA's Identity and Access Assurance group, said traditional phishing attacks became less useful in 2007 -- though no less common.

Instead, the really malicious attacks are not lures to fake sites that try to steal your bank-account login and password, but sites that redirect you to log in at your real bank but piggyback in with you and make transactions while you are logged in, according to Gaffan.

Hackers are also increasingly turning to the phone to try to con their way into accounts, Gaffan said. Most online banks will let you pay bills, but don't let you transfer large sums of money to another person, something that can be done over the phone.

"You can typically social engineer and sweet talk your way through or brute force your way in," Gaffan said. "Once you get in, you are in (the equivalent) of a branch office."

These techniques are a reaction in part to extra security requirements that banks had to implement by the beginning of the year. Those measures, some obvious to customers and some hidden, complicated the work of breaking into online banks, even for bad

guys with user names and passwords.

Because of those measures, some online criminals are now breaking into sites that are "further away from the money" that nonetheless will eventually be profitable.

Examples from 2007 include hackers selling access to MySpace pages (which can later be used to spam or spread malware), and a targeted attack on Salesforce.com that let an attacker get at the company's customer database.

The year also saw a rise in the number of attempts to take over computers by seeding the web with videos that said users needed to install a special decoding plug-in known as a codec to watch it. Instead of installing a codec, however, the site would install malware that would later replace search queries with links that would profit the hackers.

In October, that attack was extended to users running Macs, something researchers says shows that Macs have enough of a mainstream user base to be worth attacking.

As for advice for individuals, Gaffan said little has changed: Use antivirus software. Don't download programs from sites you don't trust. Use bookmarks to log in to financial-services sites.

He also says to remain vigilant of any e-mails dealing with financial sites, and expect a flood of spam in January 2008 advertising a bank's "new products" for the new year. Such e-mails are customized, he said, and will use your name in the body of the message to make the story sound better.

Online crooks will wrap up the year with a scam that's become a holiday tradition, Gaffan predicts: fake Christmas e-cards that are actually keyboard-sniffing Trojan horses. Ho, ho, ho.