Midmarket IT Security News:

SecTor 2010: Researchers demonstrate malware samples used in targeted attacks

By Robert Westervelt, News Director
26 Oct 2010 | SearchMidmarketSecurity.com

TORONTO -- Security researchers demonstrated malware samples used in recent targeted attacks during a session Tuesday at the SecTor 2010 conference. These malware samples, through the use of simple, automated processes within the code, were able to evade antivirus detection and dupe computer forensics investigations.

Attackers are customizing the malware for each environment because they don't want to have malware that creates a lot of noise.
Jibran Ilyas, senior security consultant and forensics investigator, Spiderlabs

The researchers, members of Trustwave's Spiderlabs forensics and pen-testing teams, investigated more than 200 security incidents worldwide during the last year, collecting hundreds of malware samples; on Tuesday, they demonstrated a Windows credential stealer, a network rootkit and a client-side PDF attack.

But the depth and sophistication of malware used in targeted attacks includes many other techniques, the researchers said. Those include memory parsing to capture data, sometimes swiping credit card information in memory, before a payment system has a chance to apply encryption. The researchers also said keystroke loggers and network sniffers continue to cause trouble, and are often behind data breaches that aren't detected until long after the malware has completed its mission and attackers have moved on to another target.

Many of the firms targeted by the malware were using poor security processes. In some cases, the firms weren't properly vetting third-party IT firms or data-hosting providers, said Jibran Ilyas, a senior security consultant and forensics investigator for Spiderlabs incident response team. The organizations were smaller, cash-strapped firms who couldn't afford an onsite IT team, Ilyas said.

"In many cases [companies] have things like remote desktop, VNC and pcAnywhere, where there are ports open for third parties to come in," Ilyas said. "What they don't realize is that if they open it to integrators, they've opened it for the hackers."

Often, third-party IT services organizations are servicing hundreds of clients, increasing the likelihood that there isn't a unique password for each client, Ilyas said. Cybercriminals can easily crack the password to the remote access programs and gain a foothold, installing a rootkit and other malware without the client noticing. Even if the remote assistance programs are turned off, more malware is being coded with automated features to send back stolen data to cybercriminals using port 443, an SSL port, where communication is allowed by many businesses. The latest malware samples also use timing processes, often waiting until the early morning hours to upload the stolen data when fewer people are watching the systems. Cybercriminals are "going to get their data and they're going to get it every day," Ilyas said.

Ilyas demonstrated a memory rootkit malware sample that was found on a system at a Miami sports bar. The malware, which had three components, used a system file rather than an executable to get loaded into the kernel of the sports bar's Windows system. The rootkit immediately began capturing credit card data stored in memory, where it is unencrypted.

"One thing we'e learned is that customization is the key," Ilyas said. "Attackers are customizing the malware for each environment because they don't want to have malware that creates a lot of noise."

A Windows credential stealer, which targeted an adult toy store, had coding in it to modify time stamp files on the system in an attempt to dupe investigators by making the malware files blend in with other system files. After the attackers gained access, Ilyad said they discovered a database, which stored credit card transactions for 10 minutes. The attackers were able to code their own webpage to easily view and harvest the last 10 minutes of transactions, he said

An attack against an international VOIP provider with more than 80,000 customers used a network sniffer rootkit to steal system data, credit card numbers and other information. When the Spiderlabs team investigated the outsourced third-party hosting provider, the data center was located in a rickety barn, containing about 20 farm cats that lived among the equipment, said Nicholas J. Percoco, senior vice president of the Spiderlabs team. Attackers had an easy time gaining access, installing the rootkit and exporting the stolen data, streaming it out using a password-protected RAR file.

"The attackers aren't going away," Percoco said. "As organizations at the top are becoming more secure, the smaller organizations are not anywhere near using good security processes."

The team investigated an incident at a U.S. defense contractor, in which attackers targeted the firm's CEO, using his email address header and signature to send employees a phony message. The message contained a PDF attachment that if clicked, could execute the malware to steal data located in their documents folder. The cybercriminals used a compressed and encrypted file to receive the stolen data from the contractor via FTP.

Tags: Microsoft security threat management, Microsoft identity and access management, Antivirus, antispyware management, VIEW ALL TAGS

More on malware:

Enhanced Mitigation Experience Toolkit reduces buffer overflow attacks:
Microsoft Windows Enhanced Mititgation Experience Toolkit version 2 introduces six mitigations that reduce the risks posed by malware trying to cause an application buffer overflow.

How to find a keylogger on your computers:
If a hardware or software keylogger made it on to one of your organization's machines, it would be a security pro's worst nightmare. Learn how to detect and defend against the malware.

Using Windows software restriction policies to stop executable code:
Software restriction policies are one way to prevent known malware and file-sharing applications from taking control of your network.

Microsoft releases free regular expression patterns fuzzing tool
Midsized businesses not immune to attacks, data breaches, survey finds
Windows 7 backup tool: Three Windows 7 Backup and Restore use cases
Using Microsoft Security Essentials 2.0 for SMB antivirus protection
Windows 7 Backup and Restore Center a critical data protection tool
Enhanced Mitigation Experience Toolkit reduces buffer overflow attacks
Are virtual hard-disk defragment tools needed?
Windows 7 security guide: Best practices on security for Windows 7
How to use BitLocker To Go in Windows 7: A primer
How to use Windows Group Policy to secure and restrict USB devices

- **Microsoft identity and access management**

Are virtual hard-disk defragment tools needed?
Your BitLocker To Go Active Directory policy options
How to use Windows Group Policy to secure and restrict USB devices
RMS setup tips for multiple Active Directory domains
AD Rights Management Services: How to allow remote user access
Learn Active Directory security basics: How to configure the management tool
How to configure IIS authorization and manager permissions
Using Windows software restriction policies to stop executable code
Insurance company finds relief with Forefront user provisioning tool
How to perform an Active Directory health check

- **Antivirus, antispyware management**

Social engineering attack: How to remove rogue security software
SEO security: How to stop search engine optimization security attacks
How to find a keylogger on your computers
How to avoid attacks that exploit a Web browser vulnerability
What can the Khobe technique do to Windows antivirus software?
How to remove rootkits from your organization
McAfee launches SaaS antimalware, Web filtering service
Windows rootkit detection tools and tactics
Whitelisting applications vs. other antimalware defenses
Using HTTPS: How to encrypt and secure a website

RELATED GLOSSARY TERMS
Terms from Whatis.com – the technology online dictionary

- Back Orifice (SearchMidmarketSecurity.com)

RELATED RESOURCES

- 2020software.com, trial software downloads for accounting software, ERP software, CRM software and business software systems
- Search Bitpipe.com for the latest white papers and business webcasts
- Whatis.com, the online computer dictionary