FRAUD Insights

CHICAGO TITLE®

TOP ten malware

Remember the "RANSOMWARE" article in the September 2019 issue of Fraud Insights? The cost from the attack to the city of Baltimore was estimated at $18.2 million — with the city transferring $6.5 million from a fund for parks and recreation to help pay for it.

That was just one example of many local governments being recently targeted and attacked. Ransomware remains an issue for not only governments but private businesses as well.

The Center for Information Security published a list of the top 10 malware types in 2019. Here they are:

1. TrickBot: Designed to steal financial login information; usually distributed via email asking a user to click or login through the email.
2. Emotet: Designed to steal financial login information through spam emails asking recipients to click to view, "Your Invoice" or "Payment Details." This malware can spread through systems and infect other computers.
3. ZeuS: Yet another variant designed to steal financial information. This incorporates key–logging malware. It was extremely successful in 2009 when it compromised more than 74,000 FTP website accounts. It is still around to this day.
4. Dridex: Again, designed to steal banking information via a system that utilizes macros in Microsoft® Word®. Be careful if you receive a Word file from an untrusted source asking to use macros.
5. Kovter: Is a file–less malware. Typically infiltrates a computer system through phishing emails, clicking on unsecure internet links or fake program updates.
6. CryptoWall: A ransomware distributed via spam emails with ZIP attachments. Remember, always look at the file type you are opening, as ZIP files may contain malicious PDF files.
7. Gh0st: A remote access Trojan (RAT) used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.
8. NanoCore: A Remote Access Trojan (RAT) sent via spam emails containing a Microsoft® Excel® spreadsheet. The malware can allow remote access by a cybercriminal and take full control of the infected computer.
9. Tinba (aka Tiny Banker): A type of Trojan malware designed to be a "man–in–the–middle" attack. The malware inserts itself between the user and the website they are accessing. The malware can see and steal the login information of the user.
10. Cerber: A ransomware Trojan on Microsoft® Windows® that can encrypt a user's files from a .docx file that is sent via email. Currently, a decryptor tool is only available for unencrypting the files.

Most of these malwares require a user to interact with an email or malicious file. It is important to remember to always look at who is sending you the file. Never open any file unless it is from a trusted source and you know that person is sending you a valid file.

Cybercriminals work hard to disguise malwares. They incorporate verbiage in emails they know will tempt us to click, "Your payment is past due," "Invoice," "Your SSN has been stolen," and so on. Their goal is to get you to click the link or download an attachment that launches the malware.

CONTINUED

Another important reminder is to always update your computer and virus protection software. There is a constant battle between criminals and security companies. Criminals introduce new malware, then security companies provide an update or a patch to stop it, then criminals update their malware to avoid detection, then security companies provide an update to detect it — and on and on. Having the latest version of security updates and patches is a must to protect against many of the known attacks.

In 2018, an Allentown, Pennsylvania city employee took his laptop while traveling and missed several software updates while not on the city's network. During his travels, the employee clicked on a phishing email and infected his computer. When he returned to the office, the infection spread to other computers.

The cleanup cost Allentown more than $1 million. If the updates or patches had been timely deployed, even though the employee clicked on the email, the virus protection software could have detected the attack before it spread.

We hope you enjoyed this year's cyber buzz articles concerning all things cyber related. Hopefully, you learned a bit about the cyber world and learned tips to keep safe while at home, work and even when traveling.

Article provided by contributing author:
Scott Cummins, Advisory Director
Fidelity National Title Group
National Escrow Administration