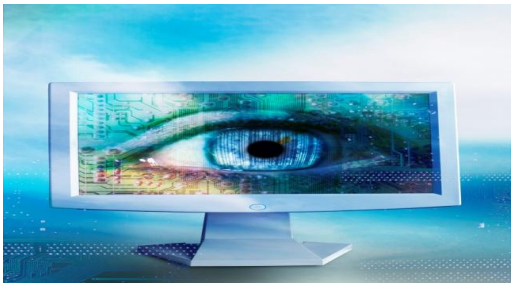
The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 16, April 2014

What is Malware?



Computer users of all ages have heard different terms such as virus, worm, or Trojan that describe malicious code or programs that can infect computers and mobile devices. In today's world, these different terms are now called ***malware***. Simply put, malware is a computer program used to perform malicious actions. In fact, the term malware is a combination of the words malicious and software.

Cyber criminals can use malware to infect a computing device, and then take control of the device functionality for malicious or illegal purposes to include stealing personal information, committing espionage, or launching denial of service attacks against businesses and government entities. Many users mistakenly believe that most malware targets Windows-based computer systems. This is a fallacy – malware can infect any computing device, including Smartphones and tablets. In fact, according to FCW.com, mobile malware is growing at an explosive rate, a trend that began in 2011 and continues today. According to recent industry reports from 2013, over 11.6 million mobile devices are infected by malware.

Who are the Attackers & Why

Cyber criminals develop malware for a variety of reasons. Some amateur hackers develop malicious code for a hobby, but many sophisticated cyber criminals have specific criminal motivations such as stealing business proprietary data, personal information, and passwords; sending spam emails; launching denial of service attacks; or engaging in identity theft.

According to the SANS Institute, cyber criminals who create, deploy, and benefit from malware can range from individuals acting on their own to well-organized criminal groups or government organizations. Further, the criminals that are creating today's sophisticated malware are often dedicated to that purpose as developing malware is their full-time job.

Protecting Yourself

The most critical security step you can take in the constant battle against cyber warfare is to install anti-virus (sometimes called anti-malware) software from trusted vendors on all computer systems to include ***all mobile devices***. And, you must keep your anti-virus software current. Cyber criminals are constantly inventing new malicious code to keep pace with technology advances in computing devices. For DOE EITS machines, software, operating system and anti-virus updates are done automatically. However, anti-virus cannot detect or remove all malware threats. You must take additional steps to protect yourself.

Beware of Social Engineering such as Phishing

A Phishing email will request personal information or request that you click on an embedded link. The email will appear as coming from a legitimate source, but in reality is nothing more than a malicious attempt to steal your information. Always attempt to verify the legitimacy of any information request by contacting the source using a telephone number (or other method) you are familiar with.

Beware of Malicious Code Embedded in Free Devices

Finally, be aware of unsolicited computing devices (e.g., thumb drives, CDs, etc.) that you receive at home or at work. Such devices may contain malicious code, and if connected to a network or personal computer, they can destroy files or disable computers or personal smart phones. If you receive a device in your official capacity as a "gift" from a reputable source or venue, do not use it; instead, retain any packaging along with the device and deliver it to your local security officer for evaluation.

Contributing source to this article: SANS Securing the Human Ouch! Security Newsletter.

Worst Password of 2013 is…

According to SplashData, the most commonly used and worst password of 2013 was **123456**. The term 'password' had held the top spot in previous years, but now there is a new winner! The list of top 25 common passwords below was compiled from files containing millions of stolen passwords posted online. This is a clear indication that many users do not take password security seriously.

We must always remember that passwords are the keys to your personal digital 'kingdom' at home and at work. Strong passwords are often your first line of defense against cyber attacks. Passwords should be long, strong, and unique. Passwords should be different for each account; have as many characters as allowed; and include numbers, letters (capital and lowercase), and special characters.

Most common BAD passwords of 2013

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. admin
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. 12345
21. password1
22. princess
23. azerty
24. trustno1
25. 000000

Flat Stanley & Stop.Think.Connect

Flat Stanley is joining the Stop.Think.Connect (STC) campaign! According to the Department of Homeland Security (DHS), the STC is joining the ***Flat Stanley Project*** to help kids learn about the importance of Cybersecurity. By downloading and using the Flat Stanley App, kids will be able to create their own "Flat Stanley" or "Flat Stella" character and send it on a tour of the Internet to learn about staying safer online and helping spread the word about cybersecurity.

The Flat Stanley App can be useful for kids, parents, and teachers to start a discussion about online safety. With kids spending more time than ever before on the Internet and social media, the partnership with the Flat Stanley Project allows DHS to further its efforts to raise Cybersecurity awareness among young Americans.

Here are a few simple tips kids will find on the app to help them remember to stay safer online:

- Be careful about what information you share online and always ask an adult first.
- Do not talk to strangers online and never agree to meet in person. Tell a parent or another adult you trust if a stranger contacts you in a chat room or through email or text message.
- Avoid sharing your passwords with anyone other than your parents.
- Don't open emails or download attachments from strangers.
- Keep your personal information private; if something seems too good to be true, then it probably is.
- Treat others online like you want to be treated.

For more information about how to access the Flat Stanly App visit http://www.flatstanley.com. To learn about what DHS is doing to keep kids safe online and for other cybersecurity tips, please visit http://www.dhs.gov/stopthinkconnect .

Information provided by Department of Homeland Security (DHS).

For questions regarding these articles or any Cybersecurity issue, search ***Cybersecurity*** *on Powerpedia or send an email to cybsectrn@hq.doe.gov.*