624TH OPERATIONS CENTER
INTELLIGENCE SURVEILLANCE & RECONNAISSANCE DIVISION

Cyber Threat Bulletin

9 January 2012 (Issue 101)

Prepared/edited by 624 OC/ISRD (AFCYBER)

The Cyber Threat Bulletin is designed to keep Air Force members knowledgeable of user & network threats. It is located on the AF Portal. It's against our policy to send out this bulletin or request personal data via email.

2012 Top Ten Cyber Threats

Every year as technology grows and advances thus do the threats that surround it. Predicting what new cyber threats to look for may not always be an easy task. By keeping up with the past trends and ever changing current environment, may help to give us a good handle on how to prepare for what may be to come.

Last year we saw great changes in Hacktivism, mobile threats, social-media exploitation, client-side exploitation, and targeted attacks. As many of these will only continue to evolve as we step in to 2012, there are many more to be added to the list and not ignored. According to McAfee, the top ten threats for 2012 are:

1. **Attacking Mobile Devices –** Over the last two years mobile devices and smartphones have experienced a huge increase in attacks with 2011 showing the largest levels in mobile malware history. As they did on PCs, rootkits and botnets deliver ads and make money off of their mobile victims the same way. The installation of software or spyware, ad clicks or premium-rate text messages, as well as a shift toward mobile banking attacks is just a few threats facing mobile device users. As more users handle their finances on mobile devices, techniques previously dedicated for online banking will now focus on mobile banking users, bypassing PCs and going straight for mobile banking apps.

2. **Embedded Hardware -** GPS, routers, network bridges, and recently many consumer electronic devices use embedded functions and designs. Malware that attacks at the hardware layer will be required for exploiting embedded systems. Attackers will often try to

"root" a system at its lowest level. If code can be inserted that alters the boot order or loading order of the operating system, greater control is gained and can maintain long-term access to the system and its data. The consequence of this trend is that other systems that use embedded hardware, for example, automotive systems, medical systems, or utility systems will become susceptible to these types of attacks. These proofs-of-concept code are expected to become even more effective in 2012.

3. **"Legalized" Spam –** Since the drop in global spamming volumes from the peak in 2009 and the increased black market cost of sending spam through botnets, "legitimate" advertising agencies. The United States' CAN-SPAM Act was watered down so much that advertisers are not required to receive consent for sending advertising. "Legal" spams, and the technique known as "snowshoe spamming," are expected to continue to grow at a faster rate than illegal phishing and confidence scams.

4. **Industrial Attacks -** Gaining more attention every day, the cyber threat potential is one of few that pose real loss of property and life. Water, electricity, oil and gas are essential to people's everyday lives, Many industrial systems are not prepared for cyber attacks, yet many such as water, electricity, oil and gas are essential to everyday living. As with recent incidents directed at water utilities in the U.S., attackers will continue to leverage this lack of preparedness.

5. **Hacktivism –** One thing is certain, when a target was identified, hacktivists are a credible force. The problem in 2011 was the undefined structure, differentiating between rogue script kiddies and a politically motivated campaign was a task. McAfee Labs predicts that in 2012, either the "true" Anonymous group will re-invent itself, or die out. The other piece to look for in 2012, digital and physical demonstrations becoming more engaged and targeting public figures more than ever before.

6. **Virtual Currency –** Also commonly referred to as cyber-currency, a popular means to exchange money online which is not backed by tangible assets or legal tender laws. Many use services such as Bitcoin, which allows users to make transactions through a decentralized, peer-to-peer network using an online wallet to receive "coins" and make direct online payments. Users need a wallet address to be able to send and receive coins, the wallets however are not encrypted and the transactions are public. This boosts opportunity for cybercriminals, not to mention Trojan malware.

7. **Rogue Certificates –** We often tend to trust digitally-signed certificates without a second thought believing the digital signature or certificate authority they came from to be legit. Recent threats such as Stuxnet and Duqu used rogue certificates to evade detection and investigations have shown that as many as 531 fraudulent certificates were issued from DigiNotar, a troubled Dutch authority that recently declared bankruptcy. Increased targeting of certificate authorities and the broader use of fraudulent digital certificates will only increase, giving attackers an even greater advantage.

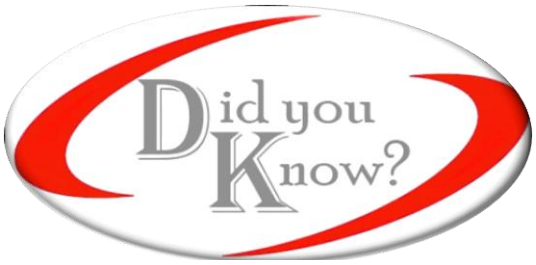
8. **Cyber War –** As more and more countries are realizing the harmful outcomes cyber attacks pose, industrial attacks for example, that carry crippling potential, the need for defense is

more apparent than ever. McAfee Labs expects to see countries demonstrate their cyber war capabilities in 2012, in order to send a message.

9. **Domain Name System Security Extensions -** A technology to protect name-resolution services from spoofing and cache poisoning by using a "web of trust" based on public-key cryptography; meant to protect a client computer from inadvertently communicating with a host as a result of a "man-in-the-middle" attack. Unfortunately it would also protect from spoofing and redirection of any attempts by authorities who seek to reroute Internet traffic destined to websites that are trafficking in illegal software or images. With governing bodies around the globe taking a greater interest in establishing "rules of the road" for Internet traffic, McAfee Labs expects to see more and more instances in which future solutions are hampered by legislative issues.

10. **Advances in Operating Systems** - Recent versions of Windows have included data-execution protection as well as address-space layout randomization. These security methods make it harder for attackers to compromise a victim's machine. Encryption technologies have also boosted OS protection in recent years. As with most internal OS security measures, attackers very quickly found ways to evade them. Advances by the information security industry and operating system will continue to advance, but will that push malware writers to focus on directly attacking hardware? McAfee Labs expects to see more effort put into hardware and firmware exploits and their related real-world attacks through 2012.

(Source: http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf)



WATCH OUT FOR TAX SCAMS

With the holidays behind us and the new year beginning, that means tax season. New scams emerge every year and while not being able to identify them all, there are a few things you can do you better protect yourself.

- Always check on the legitimacy of the tax preparation service you are going to use, always use a licensed and established preparer or company

- If you receive an email from any tax preparation software company, do not open them or click on any link. If you actually need an upgrade, go directly to the company's secure site

- Try never to leave any mail in your mailbox for an extended period of time. Use a locking mail box or a P.O. Box to ensure your mail is secure

(Source: http://www.vvdailypress.com/news/scams-32130-tax-irs.html)

For any security related questions, issues, or concerns, contact your Unit Information Assurance Officer, Wing IA and/or the Information Protection Office.

Do you have a question, comment, or concern? Have a topic you would like to see in a future bulletin? Feel free to call us at DSN: 969-9612, or e-mail us at 624oc.isrd@lackland.af.mil. The use or omission of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

To receive automatic notification of each new Cyber Threat Bulletin loaded to the AF Portal, select the "Set an Alert" button at the top of the Cyber Threat Bulletins Archive page.