Volume 2 Issue 17

Date: 01.12.2025

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Stuxnet

Stuxnet is a highly sophisticated computer worm that became widely known in 2010. It exploited previously-unknown Windows zero-day vulnerabilities to infect target systems and spread to other systems. Stuxnet was mainly targeted at the centrifuges of Iran's uranium enrichment facilities, with the intention of covertly derailing Iran's then-emerging nuclear program. However, Stuxnet was modified over time to enable it to target other infrastructure such as gas pipes, power plants, and water treatment plants.

Whilst Stuxnet made global headlines in 2010, it's believed that development on it began in 2005. It is considered the world's first cyber weapon and for that reason, generated significant media attention. Reportedly, the worm destroyed almost one-fifth of

Iran's nuclear centrifuges, infected over 200,000 computers, and caused 1,000 machines to physically degrade.

Who created Stuxnet?

Whilst no-one officially claimed responsibility for Stuxnet, it is widely accepted that it was a joint creation between the intelligence agencies of the US and Israel. Reportedly, the classified program to develop the worm was code-named '**Olympic Games**' which began under President George W Bush and then continued under President Obama. The program's objective was to derail or at least delay Iran's emerging nuclear program.

Initially, agents planted the Stuxnet malware in four engineering firms associated with Natanz – a key location in Iran for its nuclear program – relying on careless use of USB thumb drives to transport the attack within the facility.

Is Stuxnet a virus?

Stuxnet is often referred to as a virus but in fact, it is a computer worm. Although viruses and worms are both types of malware, worms are more sophisticated because they don't require human interaction to activate – instead, they can self-propagate once they have entered a system.

Besides deleting data, a computer worm can overload networks, consume bandwidth, open a backdoor, diminish hard drive space, and deliver other dangerous malware like rootkits, spyware, and ransomware.

WhatsApp Screen Mirroring Fraud

In this type of scam, fraudsters trick a person into enabling screen-sharing via WhatsApp. This way, the fraudsters gain access to the person's sensitive information such as OTPs, bank details, passwords, personal messages, etc. As a result, the person can fall prey to financial losses, account takeovers and even identify theft.

How to stay Safe?

Verify the caller's identity through official channels before engaging.

Avoid screen-sharing unless absolutely necessary and only with trusted contacts.

Enable two-factor authentication on all financial and messaging apps.

Keep your phone's operating system and apps updated to close security gaps.

Notify your bank to freeze or secure your accounts.

Why is Stuxnet so famous?

Stuxnet generated extensive media interest and was the subject of documentaries and books. To this day, it remains one of the most advanced malware attacks in history. Stuxnet was significant for a number of reasons:

- It was the world's first digital weapon. Rather than just hijacking targeted computers or stealing information from them, Stuxnet escaped the digital realm to wreak physical destruction on equipment the computers controlled. It set a precedent that attacking another country's infrastructure through malware was possible.
- It was created at nation state level, and while Stuxnet was not the first cyberwar attack in history, it was considered the most sophisticated at the time.
- It was highly effective: Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.
- It used four different zero-day vulnerabilities to spread, which was very unusual in 2010 and is still uncommon today. Among those exploits was one so dangerous that it simply required having an icon visible on the screen – no interaction was necessary.
- Stuxnet highlighted the fact that air-gapped networks can be breached – in this case, via infected USB drives. Once Stuxnet was on a system, it spread rapidly, searching out computers with control over Siemens software and PLCs.

Cybersecurity for industrial/organizational networks

In the real world, advanced nation state attacks like Stuxnet are rare compared to common, opportunistic disruptions caused by things like ransomware. But Stuxnet highlights the importance of cyber security for any organization. Whether it's ransomware, computer worms, phishing, business email compromise (BEC), or other cyber threats, steps you can take to protect your organization include:

1. Apply a strict Bring Your Own Device (BYOD) policy that prevents employees and contractors from introducing potential threats onto your network.
2. Implement a strong and technically-enforced password policy with two-factor authentication that hinders brute force attacks and prevents stolen passwords from becoming threat vectors.
3. Secure computers and networks with the latest patches. Keeping up-to-date will ensure you benefit from the latest security fixes.
4. Apply easy backup and restore at every level to minimize disruption, especially for critical systems.
5. Constantly monitor processors and servers for anomalies.
6. Ensure all your devices are protected by comprehensive antivirus. A good antivirus will work 24/7 to protect you against hackers and the latest viruses, ransomware, and spyware.

Password change email from 'rnicrosoft.com' is a phishing scam

Heads up! There's a new phishing scheme targeting Microsoft users with fake password reset emails. Scammers have set up a website similar to Microsoft's, using 'rnicrosoft.com' to lure you in. This could lead to serious security breaches for your account. Make it a habit to scrutinize email addresses and links closely. For password resets, go straight to the Microsoft homepage.