Centre for Cyber Security, Audit, Forensics and Education
Visit: http://cms1.gre.ac.uk/research/csafe

School of Computing & Mathematical Sciences
UNIVERSITY of GREENWICH

Wednesday 26th March 2014, issue #5

In this issue:

C-SAFE Short Courses

Computer Forensic Evidence and the Law

Computer Forensic Evidence and the Law (Legal Aspects)

Computer Forensics for Lawyers

EnCase Computer Forensics 1 and 2 Certification (EnCE©)

Introduction to Computer Forensics

Penetration Testing and Vulnerability Assessment

For an updated list, click here.

Cyber-Security in Oil and Gas is more than just protecting intellectual properties and data!

AWARENESS OF CYBER-SECURITY

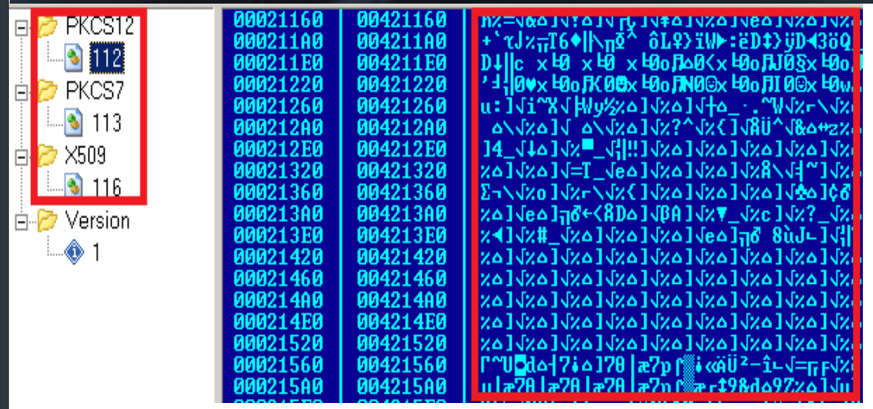
The profile of cyber-warfare and cyber-security has been raised and prioritised as a top national security threat in developed and developing countries such as the UK, US, China, Israel, Iran, South Korea and Singapore. All of the above mentioned countries having come under covert or targeted cyber-attacks from cybercriminals, other nation's government or organised hacktivists from around the globe.

Such countries have demonstrated the urgency to take action towards protecting their country's energy, telecommunications and wider infrastructures that are heavily relied upon and critical to a functioning society. It would also be wrong to assume to that it is only government infrastructure and departments that come under regular cyber-attacks, in fact cyber-attacks on the oil and gas industry in middle-eastern countries have been increasing since 2009 and continue to do so as this article is written. For example, the Singapore government is expected to invest USD $215Million (£130.3Million) by 2023 towards establishing a cyber-warfare unit to defend national assets and interests, and launch counter-attacks if need arises. Universities have received funding to promote cyber-security degree courses to close this specific skills gap and build a generation of cyber-troopers.
South Korea came under cyber-attacks from North Korea in 2009 and 2011, leading to South Korea investing $8.76 billion dollars to train 5,000 cyber-security experts by 2017 in response to North Korea's 3,000 strong cyber-warfare unit.

MOTIVES OF CYBER-ATTACKS?

Cyber-attacks on oil and gas is no longer just about pilferage of intellectual properties and sensitive data, but the increasing trend of causing visible damage that attracts public and media interest, in order to demonstrate cybercriminals' intentions and motives.

Motives to launch cyber-attacks towards oil and gas stem from revenge, envy, competitive advantage, political, racial and betrayal attacks; reasons for previous cyber-attacks include a perceived betrayal of Muslims by Saudi Arabia as Saudi bases oil prices in US currency and works with foreigners, adding pressures on local families with inflated oil price. Another accusation and justification is that the US created war for the purpose of stealing Gold, Oil and Opium (Afghanistan) but news broadcasts were heavily censored on mainstream media, hence the cyber-attacks to obtain public attention. Since 2009, Qatar's RasGas, Chevron, Saudi Aramco and Schlumberger in 2013 came under cyber-attacks, where they were infected by malwares, viruses, worms, back doors and trojans, at least one of the companies encountered physical attacks with potential for causing disruptions to supply chains. In 2013, a US oil company networks on several rigs and platforms were incapacitated due to malware downloaded by workers. Two months later, cyber-attack attempts from Iran failed to compromise industry IT networks, the aim being to destroy data and take control of critical Industrial Control Systems (ICS).



MODUS OPERANDI OF CYBER-ATTACKS?

Previously, the pattern of cyber-attacks on the oil and gas industry was to obtain proprietary information, strategic plans, investments, oil companies handbooks, bids tendered for new drilling acreage, geologic data and private negotiations with foreign officials. The success of the above pilferage includes the campaign '*Night Dragon*' launched by China based hackers to obtain confidential data from five major western energy companies during 2008 and 2011. The hack campaign stole away gigabytes worth of sensitive material, such as financial transactions, bid data and proprietary information on field operations and productions.

The trend now is to sabotage production and operational processes by introducing viruses, malware and worms through staff USB, laptops and browsers. The virus named 'Shamoon' also known as 'Simon' in Arabic, was programmed to swipe-and-wipe out the petroleum producer Saudi Aramco's network, the virus infected 30,000 PCs, where it corrupted files, including Master Boot Records (MBR) which rendered infected computers unusable. The virus further damages machines by preplacing stolen data with JPEG images, to prevent ultimate file recovery. With regards to the Schlumberger case, worm attacks replicating and DNS cache poisoning attacks were directing IP addresses to the attacker's site where attackers planted a backdoor onto the infected machines, on another occasion, viruses were introduced into network systems, causing connected PCs to infinitely loop reboot and never get to the start-up windows screen. According to Kaspersky Lab, targeted attacks cost US$2.4 million in damages with attacks via browsers being the primary method for spreading malware. Kaspersky further detected 1.2 million PCs in UAE infected by net-borne malware, which stands at 26.4% of users and 17.4 million PCs or 40% of users with the majority being infected by malware spread via USB and CD/ DVD.

RESIDUAL RISKS TOWARDS OIL AND GAS INDUSTRY?

Due to the increase integration of systems used in the oil and gas on and off-shore web communicative, production control and reporting systems, it is best practice to secure the following with the latest security features and industrial systems patched by vendors, as cyber-attacks targeting on RATs, SCADA and ICS systems are on the increase, oil and gas executives should consider raising security profiles and implement security preparation, as damages inflicted can be significant and substantial:-

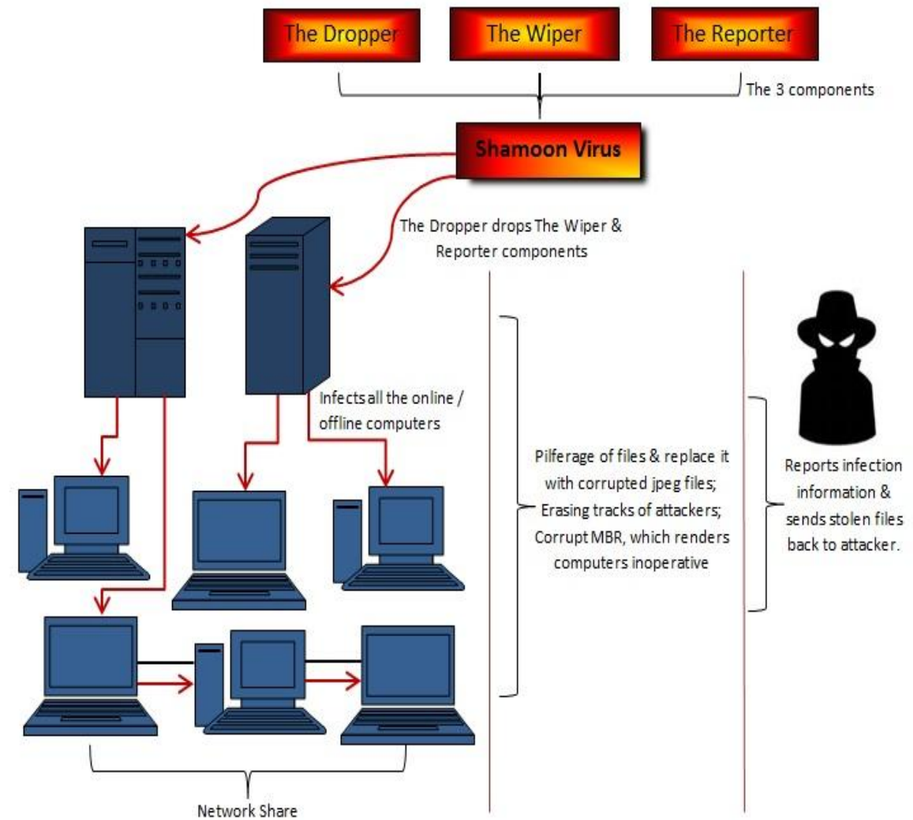
- Web Applications, Networks and Servers
- Windows OS Vulnerabilities
- RATs (Remote Admin Tools)
- SCADA (Supervisory Control & Data Acquisition)
- ICS (Industrials Control Systems)
- Stringent BYOD policy for employees
- Cyber-Security awareness training for employees i.e. identification of social engineering, spear-phishing, malwares, viruses, Trojans are introduced
- Physical protection for pipelines, refineries, rigs and platforms.

How 'Shamoon' Virus Attack Works?

The virus 'Shamoon' in Arabic means 'Simon' which follows the author's name, it has similar characteristic from the virus named 'Wiper' that swept through Iran in April 2012. However, the Shamoon virus has three separate components; they are known as - Dropper, Wiper and Reporter.

At each component stages, the virus gathers, destroys and retrieves information for the attacker. As shown in the following diagram, The Dropper initiates itself as services to be run on Windows startup, copies itself to network shares or servers and infects linked on/offline PCs that are connected to the infected hosts.

The Dropper component carries and drops the other two components (The Wiper and Reporter) onto infected PCs & networks to collect files, spread itself into file systems and hard disks, where the Wiper changes the Master Boot Record (MBR) to deem the hard disk unusable, it also collects, wipes and send the stolen files back to the attacker. The Wiper component also replaces all the stolen files with corrupted JPEG images to prevent any attempt of file recovery and erases tracks of the attacker. The Reporter sends information about the extent of the infection back to the attacker's computer.



Author's corner

Jane Teh is the CEO of Instinctus.org, a Cybersecurity & Corporate Training and Consultancy company based in South-East Asia.

E: Jane@Instinctus.org

SOFTWARE

To remove Shamoon virus, install and run each application in the order presented below:

1. First install FixNCR.reg from http://donwload.bleepingcomputer.com

2. Next, install RegCureProSetup.exe from http://awsdownload.regcure.com

3. Last, install SpyHunter-Installer.exe from http://www.enigmasoftware.com

or

for full instruction, visit http://www.cleanpcguide.com/download/

Click the left icon to find out more.