**Threat Landscapes**

**Stuxnet**

**Stuxnet Dossier**

Sophisticated malware attack targeting Iranian industrial control systems.

Included zero-day exploits, a windows rootkit, the first PLC rootkit, antivirus evasion techniques, complex process injection, and hooking code.

Self-replicates via removable drives exploiting LNK/PIF automatic file execution vulnerability.

Theoretically the attacker would need the target ICS’s schematics.

Attackers compromised two digital certificates.

Stuxnet would need to be introduced into the environment, via a willing or unwilling third party.

Once stuxnet had infected a computer in the organization, it began to spread in search of field PGs, typically windows computers used to program PLCs. Most are non-networked, so stuxnet would first try to spread over LAN to other computers using a zero day, a two-year-old vulnerability, infecting step 7 projects, and through removable drives.

Propagation over lan likely served as the first step of propagation, and used removable drives to hop any gaps to non-networked machines.

Attackers could control stuxnet through command and control server, but the target computer was unlikely to have network access, therefore the payload was built into the stuxnet executable. Updates to said executable would be propagated via a peer to peer method established by stuxnet.

When stuxnet found a target, it would modify the PLC code. These modifications sabotaged the systems, likely high value targets.

Victims attempting to verify the issue would not see any rogue PLC code as stuxnet hides its modifications.

Self-replication was effective but caused noticeable collateral damage.

**WannaCry**

**Enisa WannaCry Ransomware Outburst**

Malware that encrypts infected system and prompts for a payment in Bitcoin to decrypt files, after payment there is no guarantee that files will be decrypted.

Acts as a worm once in a system, self-propagating through the network in order to spread, this paired with the encrypting nature of the malware causes a lot of damage.

Affected 150 countries and over 230,000 systems.

Ransomware usually spreads via phishing emails. Method often uses social engineering to mislead recipient.

WannaCry exploits a Server Message Block vulnerability to propagate, this is often known as “EternalBlue”, allegedly developed by the NSA. It also installs the “DoublePulsar” backdoor incase of a failure in the EternalBlue exploit. The backdoor allows the attacker to access the infected computer system so that additional malware can be loaded on to the victim.

A few hours after the outbreak a researcher managed to constrain the rapid spread by registering the domain in the binary code of the malware, which was used as a killswitch. The use of this killswitch allowed for the slowing of the propagation. The malware was not proxy aware, and infection of machines not connected to the internet continued.

Notable infections include:

* NHS UK
* Telefonica
* Deutsche Bahn systems
* Renault
* Nissan
* Various Universities

If you’ve been hit by WannaCry:

* Isolate and take the infected hosts offline.
* Do not pay the ransom.
* Be aware of fake decryption tools.
* Files may be recoverable via the use of forensic techniques.

Methods to counteract WannaCry:

* Back up and protect your systems and files.
* Patch your system with the Microsoft patch which addresses the SMB vulnerability. Microsoft has even supplied patches for legacy systems to prevent the widespread propagation of the Ransomware.
* Update your antivirus signature database to the latest version. Antivirus firms are now detecting all the current variations of the ransomware.
* Consider adding a rule on your router for firewall to block incoming SMB traffic on port 445 from untrusted sources. Additionally, filter NETBIOS port 139 and RDP port 3389 in order to refrain from infecting other devices in the same network segment.
* CNN-CERT (Spanish CERT) has reportedly developed a vaccine, which prevent WannaCry from executing and encrypting a system if the system gets infected afterwards.
* If you are unable to patch your system disable SMBv1.

Follow best security practices:

Never use high privileged system / domain accounts for daily business.

Keep you operating system and installed software up to date.

Apply security patches and updates as soon as the become available.

Back up your systems following the 3-2-1 scheme. Verify operational capacity of backups.

Avoid opening suspicious email attachments.

Restrict access to network resources, block unnecessary ports, disable unnecessary services and segregate your network separating core operational systems from the rest of the network.#

**Ukrainian Power Grid Incident**

First publicly acknowledged incident that resulted in power outages.

225,000 customers in three different distribution level service territories, outages for several hours.

Attackers used spear phishing, variants of the BlackEnergy3 malware, and manipulation of the Microsoft office documents that contained the malware into the IT networks of the company.

Attackers had sophisticated knowledge of network connected infrastructure, such is Uninterruptable Power Supplies (UPSs) but also in ICSs through control systems, such as the HMI.

Attackers demonstrated ability to target field devices at substations, write custom malicious firmware, and render serial to ethernet convertors inoperable and unrecoverable.

In one case the attacks use a telephone system to generate thousands of phone calls to the support centre in order to block out customers reporting outages.

Capability to perform long term reconnaissance was great.

Consolidated list of technical components used by hackers:

* Spear phishing
* Identification of BlackEnergy3 at each of the impacted oblenergos.
* Theft of credentials from business networks.
* Use of VPNs to enter ICS network.
* Existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI.
* Serial to ethernet communications devices impacted at firmware level.
* Use of modified KillDisk to erase master boot record of impacted organisation systems as well as the targeted deletion of some logs.
* Utilising UPS systems to impact connected load with scheduled service outage.
* Telephone denial of service attack on call centre.

**Kill Chain Mapping**

*Stage 1 – Recon*

No prior reports of recon. Analysis of impacted organisations show interest may have been spurred from how the three affected orgs were using higher levels of automation, enabling remote opening of breakers in a number of substations. Coordination of final attack plan suggests recon took place at some point.

Weaponization or targeting. It does not appear that targeting was necessary. Attackers weaponized Microsoft office docs by embedding BlackEnergy3 within the docs.

During the intrusion phase, Delivery, Exploit, and install. The malicious documents were delivered via email to individuals in admin or IT network.

The documents opened and encouraged them to enable macros. Enabling the macros allowed the malware to exploit office functionality to install BlackEnergy3 on the victim system.

Upon install, BlackEnergy3 connected to command and control IP addresses to enable communication by the adversary. These pathways allowed the adversary to gain information from the environment.

First actions were to scrape credentials, escalate privileges, and move laterally through the network.

Attackers quickly moved away from the first foothold in order to blend in.

Using stolen credentials, adversary could pivot into network segments where Scada