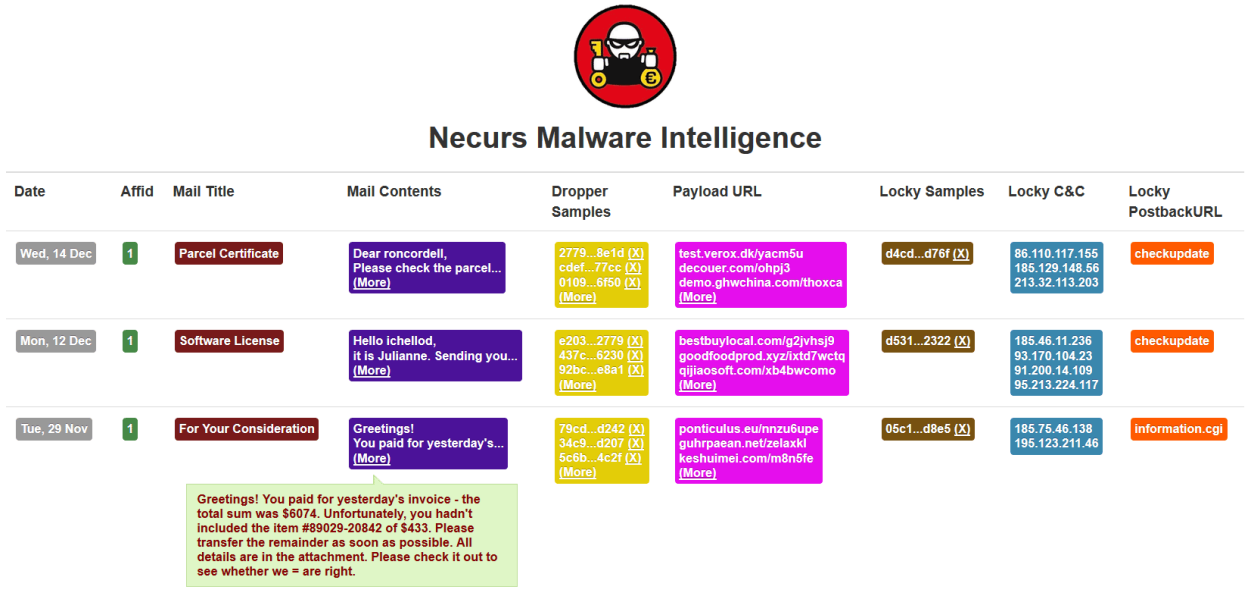
SCENARIO #6: **Hacking Group Thallium**

Scenario:

In 2019, the hacking group Thallium targeted Microsoft users such as Outlook emails by impersonating the company with the aim of stealing sensitive information [1]. After researching a potential target, Thallium identified individual employees of that organization or associated individuals. It uses publicly available information and social media interaction to do so. Next, the hackers create fake email addresses to launch phishing attacks. The hackers typically impersonate legitimate services, including Hotmail, Gmail, Yahoo or even the company's webmail service. In many other cases, the spoofed email appears to originate from a familiar contact known by the target. The spear-phishing emails include links or sophisticated redirects to fake websites set up and controlled by Thallium. It used malware to compromise over nine millions of systems to create Necurs, one of the world's largest botnets. The takedown of Necurs took eight years of planning and coordinated legal and technical endeavors by Microsoft and its partners across 35 countries, according to Tom Burt, Microsoft's VP for customer security and trust [2].



Dashboard with Necurs SPAM mail and Locky dropper/payload intelligence. Note that Locky is ransomware malware which is delivered by email with an attached Microsoft Word document that contains malicious macros. (From: https://www.uperesia.com/inside-the-necurs-botnet)

On one hand, engineers were able to hack Necurs “domain generation algorithm” by which the botnet generates random domain names, helping Necurs operators to register domains, to place management servers on them, and to connect bots (infected computers) to them to receive new commands. MS team were able to predict what domain names it would be using over the next 25 months and block them beforehand. On the other hand, a Microsoft law team _led a law suit in the US District Court for the Eastern District of Virginia and received a court order granting the company control over existing Necurs domains that are located in Virginia. Microsoft took down approximately 50 web domains used by Thallium to conduct its cybercrime operations [1].

In this scenario, students will experiment a social engineering technical called spear-phishing. Spear-Phishing attackers use victims' personal information on social media such as email address, friends list, geographical location, etc. and act as a friend or familiar entity and send a convincing but fraudulent message to their target. They will use Zphisher, a powerful open-source phishing attack tool, to see how victims' personal information is obtained (e.g., generates a fake pages to capture passwords, grabs victim's IP addresses to know its geographic location) and phishing attacks are conducted (e.g., sends SMS's using services like Facebook/Instagram/ Google, sends SPOOFED emails with the SMTP the victim provided) [3].

Students will also examine the legal bases Microsoft used to obtain an order seizing the servers used by these criminal actors and the creative process it developed for doing so. Microsoft's Digital Crimes Unit is a leader in developing creative approaches to address cyber crime and this was the fourth nation-state actor Microsoft had used similar tactics to shut down [4].

NICE Workforce Framework for Cybersecurity:

Scenario #5 & #6 will cover the following Knowledge areas.

K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0004 Knowledge of cybersecurity and privacy principles.
K0005 Knowledge of cyber threats and vulnerabilities.
K0007 Knowledge of authentication, authorization, and access control methods.
K0013 Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0046 Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0070 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0116 Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
K0131 Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.
K0135 Knowledge of web filtering technologies.
K0202 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0210 Knowledge of data backup and restoration concepts.
K0373 Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0392 Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0452 Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
K0624 Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

References:

[1] Microsoft Sues Hacking Group Thallium and Takes Control of 50 Domains, https://vpnoverview.com/news/microsoft-sues-hacking-group-thallium-and-takes-control-of-50-domains/
[2] New action to disrupt world's largest online criminal network, https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/
[3] https://github.com/rezaaksa/PhishX
[4] https://blogs.microsoft.com/on-the-issues/2019/12/30/microsoft-court-action-against-nation-state-cybercrime/