CYBERMINUTE

Alberta Cybersecurity Insights

TLP: WHITE

Operation Endgame: A Global Strike Against Cybercrime's Backbone

In late May 2024, law enforcement groups from Denmark, France, Germany, the Netherlands, the UK, and the USA, supported by numerous other European countries, worked to take down dozens of servers. These servers were being used as part of botnets in an international manoeuvre codenamed Operation Endgame. A botnet is a collection of internet-connected devices infected by malware. It enables threat actors to control the devices for malicious activities, including sending phishing emails and conducting digital espionage.

Operation Endgame was specifically directed at the operations of prolific malware groups—such as IceID, Smokeloader, Pikabot, and Bumblebee—responsible for targeting critical systems worldwide and impacting untold numbers of victims. In affecting these groups, the operation had a global impact on the malware dropper ecosystem, significantly affecting the delivery of ransomware and other malicious software attacks.

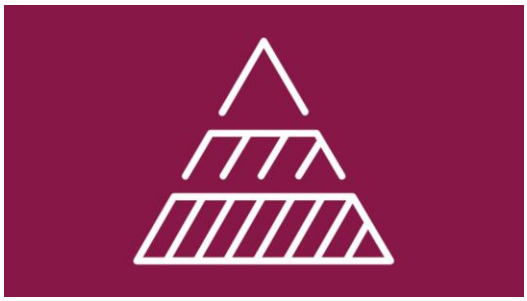
In addition to the server takedowns, Operation Endgame resulted in the search of 16 locations, the arrest of four individuals, and the seizure of over 2,000 domains previously controlled by the threat actors, now in the hands of law enforcement. According to a Europol post, this is merely the start. A dedicated website has been launched to keep the public informed about the forthcoming actions.

Operation Endgame was a significant step taken this month to enhance the digital ecosystem. However, it wasn't the only action. Throughout June 2024, several cybercriminals were arrested, including the alleged leader of the hacking group known as Scattered Spider. Additionally, three people were apprehended for purportedly hacking into websites and accounts linked to the Philippines government. Moreover, authorities caught a hacker believed to have worked for the Conti and LockBit ransomware groups.

A further legal step that has been taken this month is the sanctioning of 12 senior leaders of the anti-virus company Kaspersky Lab by the US government, coinciding with the USA's move to ban the use of Kaspersky products nation-wide within the next year. These moves were made with the express goal of better protecting American critical infrastructure, in addition to addressing security and privacy concerns which the USA feels are implicit with the organization being based in Russia.

These are precedent setting times, as cybercrimes face increasingly stringent measures, highlighting the increased understanding of just how much digital crimes impact people, organizations, and countries in the world.

Click Here to Read More!



Flowing Up the Pyramid of Pain: Unmasking China's Cyberespionage

On June 6th, 2024, the Canadian Centre for Cybersecurity (CCCS) issued a warning to

Ransomware Groups Increasingly Attacking Healthcare Sector

This year has seen an increase in attacks against the healthcare sector, indicating a

Canadians and Canadian organizations regarding the threat posed by the People's Republic of China (PRC). This warning aligns with the National Cyber Threat Assessment (NCTA), which concluded that the threat from China is the most substantial by "volume, capability, and assessed intent."

China-centric threat activity is oriented towards the objectives of the PRC, with a focus on cyberespionage. The PRC strategically targets entities whose compromise yields diplomatic leverage, economic advantage, and a strategic foothold in the networks of North American critical infrastructure. While network prepositioning is a more direct threat to the US than to Canada, Canadian operators will likely feel the impact of such a cyber-attack due to their interoperability with the US.

The CCCS has observed the widespread targeting of Canadian entities by the PRC across:

- **Government**: At all levels, from local municipalities to provincial and federal agencies.
- **Critical Infrastructure:** Energy, telecommunications networks, and transportation systems.
- **Research and Development:** Universities, labs, and innovation hubs.

realistic possibility that healthcare service providers are becoming a preferred target for threat actors, and further confirms that the healthcare sector is no longer off-limits. Multiple organizations that provide critical services to the healthcare sector have been under attack by ransomware groups, affecting hospital's ability to deliver treatment and patient care in multiple countries. In some cases, the attacks have led to theft of Protected Health Information (PHI) and Personally Identifiable Information (PII).

In June, the ransomware group known as Qilin compromised the UK-based pathology services provider Synnovis. Multiple hospitals in London were impacted, resulting in appointments such as blood transfusions and surgeries to either be postponed, cancelled, or redirected to unaffected hospitals. However, the UK's National Health Service (NHS) provided assurance that all emergency services were still able to be performed.

In May, Ascension healthcare was the victim of a ransomware attack that disrupted electronic health record systems, forcing healthcare staff to resort to pen and paper. Several file servers had signs of compromise, leading to the assessment that

- **Government-Affiliated Entities:** Any organization with close ties to the Canadian government.
- **Advocacy Groups:** Individuals and organizations championing Taiwan or Hong Kong.

To counter China-base cyberespionage, the CCCS and Mandiant recommend that defenders shift away from indicators of compromise (IoC) and focus on tactics, techniques, and procedures (TTPs). This is crucial for several reasons:

- **Operational Relay Box Networks:** These are a form of mesh network comprised of virtual private servers, IoT devices, and compromised routers. Effectively they are a shared botnet that is being used by multiple China-based cyberespionage groups. Their usage has complicated attribution and reduced the shelf-life of network IoCs to approximately a month.
- **Living Off the Land:** China-based threats are notorious for using legitimate tooling to achieve various goals, a technique known as living off the land. In doing so, they hide in plain sight and evade signature-based detection.
- **Trusted Third-Party Services:** By leveraging trusted third-party

some patient data was stolen. CNN reported that the ransomware group BlackBasta conducted the attack, a group that has previously targeted multiple Alberta-based organizations.

In February, Change Healthcare Group (a subsidiary of UnitedHealth) was compromised by the ransomware group BlackCat (aka ALPHV). The attack was severely damaging and led to the theft of 6TB of patient data. UnitedHealth also paid the ransom of 22 million USD worth of Bitcoin to BlackCat. Furthermore, the attack also disrupted the provision of healthcare, and processing of financial subsidies to prescriptions across many facilities in the US.

Recently, the FBI and Department of Health and Human Services (HHS) released a joint advisory on a widespread phishing campaign. They observed threat actors leveraging personal information stolen from previous breaches to socially engineer targets and fraudulently transfer money to attacker-controlled bank accounts.

It's highly likely that data stolen from the attacks on healthcare service providers could also be leveraged to launch further sophisticated attacks. Organizations can

services for command and control, China-based threat actors cloak their activities in legitimacy.

In the words of Bruce Lee, “be formless, shapeless, like water.” Cyber defenders must embody this fluidity, adapting to the ever-evolving threat landscape. For China-centric threats, the path lies upward—up the pyramid of pain—toward understanding and countering their elusive techniques.

Click Here to Read More!

better defend their networks from attacks by implementing MFA on all accounts to mitigate threat actors using stolen credentials to authenticate into target environments. Monitoring logins to detect any anomalous characteristics associated with each account such as geolocation and user agent strings can also help detect malicious activity. Networks should also be segmented to restrict lateral movement opportunities for any threat actors.

Click Here to Read More!

CYBER ALBERTA