Cybersecurity Challenges in-light of the Coronavirus Epidemic

Executive Summary:

Over the past few weeks, CYE's researchers have been seeing a dramatic increase in the number of cybersecurity incidents reported by companies worldwide who have been affected by a wave of Coronavirus-driven cyberattacks (see graph below). Cybercriminals, looking to exploit the chaos and panic caused by the global pandemic, are leveraging the public's genuine fear and reduced caution, resulting in an increased likelihood of cybersecurity incidents. One example of a major security gap the attackers are exploiting is related to the influx of employees working from home. The new reality requires employees to work remotely, enabling a new and insecure gateway for retrieving sensitive information.

CYE is mitigating and resolving such issues daily, supporting numerous multinational corporation (MNCs) globally, and can assist with such concerns that may expose other members of Drive's ecosystem to risks of this nature.

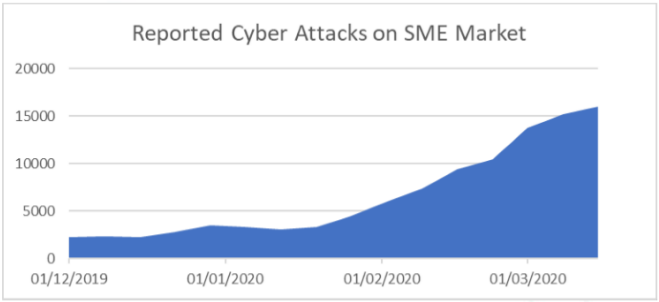

Figure-1: CYE global community reported cyber events

The Risk:

Phishing campaigns and ransomware attacks have seen the greatest increase over the past few weeks, with users clicking on attachments or links delivering a malicious communication, using the coronavirus theme as the lure. For example, a sophisticated attack took advantage of the trusted World Health Organisation (WHO), falsely claiming to be sent from WHO employees, asking the recipients for sensitive information, while exploiting the trust as an opportunity to distribute an attachment that steals personal information.

As the Coronavirus continues to spread, companies worldwide will be facing a far greater risk and a rapidly evolving threat landscape. As safe cyber-hygiene practices are neglected as a result of an organization's attention driven elsewhere, the exposure is on the rise. Higher reliance on remote work leads to numerous employees accessing data through unsecured and unsafe Wi-Fi networks, using personal devices to perform work, or potentially not following company's security protocols. This l puts companies and IT systems at greater risk of data breaches. Remote employees will not be connected via networks that are typically secured with protection layers such as firewalls, web filtering and data encryption and new threat scenarios will follow quickly.

Our Take and Suggestions:

As individuals are authorized to work remotely, including third-party providers (company supply-chain), cross-company protocols for maintaining proper security controls must be deployed as soon as possible. Beyond suggesting companies to tighten security controls and inform employees and

vendors regarding the greater risk, CYE would like to offer the following recommendations and training services for both companies and individuals, in order to reduce the risk of cyberattacks:

Expert Sessions - Online Training:

A session focusing on proactively addressing phishing campaigns, providing guidelines such as:

1. Key latest trends of phishing campaigns sent over emails and text messages, promising exclusive content, related or not to the Coronavirus. (Including Voice-Phishing)
2. Awareness – best practices & lessons learned from latest attack scenarios
3. Content Filtering configurations – reducing the potential attack surface

A session on internet connectivity strategy, internet perimeter and exposed services assessment

1. Organization authentication process review.
2. How to operate a secure communication architecture (VPV / Conf-call setup)
3. Authorization management process review.
4. Supply-chain remote connection & perimeter assessment.
5. Firewall configurations and enhanced monitoring review.

A session of auditing an Incident Response Readiness Program

1. Key process & procedures – best practices
2. Organization's readiness for addressing update various security attacks
3. Organization's End-Point protection mechanism – lessons learned
4. Organization's & personal backup process & procedures overview

For more information & further exploring how CYE's experts can help your organization's security to become more resilient in-light of the new threat landscape, please contact:
Ronen@cyesec.com