Cyber Threat Signal 2021

AusCERT, CERT-In, KrCERT/CC, Sri Lanka CERT|CC

AUSCERT

certin
Handling Computer Security Incidents

KrCERT/CC

SRI LANKA
CERT|CC

CONTENTS

Overview

Global Common Cyber Threat Outlook

National Cyber Threat Outlook

How to protect yourself from cyber threats

1 Overview

Global Common Cyber Threat Outlook
Targeted ransomware attacks becoming more common and more damaging
▪ Attacks targeting specific targets, such as governments and businesses. ▪ Surge of ransomware attacks in various industrial sectors such as service, manufacturing and healthcare. ▪ New aggressive methods to demand ransom, threatening to publish data and encrypting files.
National Cyber Threat Outlook
1. Transformation of Malspam to Masspearing (Australia, AusCERT)
▪ The introduction of 'masspearing' combining personalized emails and spam campaigns. ▪ Emotet malware on the rise through spam campaigns. ▪ Personalized attacks on specific targets within an organization using leaked data such as emails, contract information, etc.
2. Cyber-Attacks due to COVID-19 Pandemic Induced Work Culture (India, CERT-In)
▪ Attacks targeting teleworkers through malicious websites and emails containing malicious attachments. ▪ Growing risk of corporate data leakage from endpoint devices due to increased teleworking. ▪ Attempts to infiltrate corporate networks through remote network environments, such as vulnerable VPNs
3. Surge of second attacks using dark web data leaks (Republic of Korea, KrCERT/CC)
▪ As dark web markets expand, transactions of sensitive information grow. ▪ Surge in sales of network access authorization information such as VPN and RDP due to the recent teleworking trend. ▪ Attackers collaborate to lower threshold and expand scale of attack
4. Increasing sophisticated BEC(Business email compromises) (Sri Lanka, Sri Lanka CERT|CC)
▪ Attacks targeting export and import businesses. ▪ Use of phishing, spear phishing, etc., to attack corporate mail. ▪ Sophisticated attacks, such as sending spoofed or compromised payment information to partner accounts of companies.

2 Global Common Cyber Threat Outlook

1) Targeted ransomware attacks becoming more common and more damaging (common trend)

- Attacks targeting specific targets, such as governments and businesses.
- Surge of ransomware attacks in various industrial sectors such as service, manufacturing and healthcare.
- New aggressive methods to demand ransom, threatening to publish data and encrypting files.

Cyber Threat Outlook

In the wake of the COVID-19 pandemic, ransomware attacks were prevalent in 2020 using Trojans disguised as legitimate files, emails exploiting the remote working systems, and attacks on Remote Desktop Protocol(RDP).[1] With attackers now experimenting with different forms of ransomware for bigger scales of ransom, there has been a shift in the pattern of attacks. In 2021, both the scope of ransomware targets and the scale of damage inflicted by attacks are expected to increase.

A major trend in ransomware is the proliferation of targeted attacks in a variety of industries. Some of the recent ransomware victims have included the British foreign exchange company Travelex[2], the American GPS equipment manufacturer Garmin[3], the Japanese automaker Honda[4] and Dusseldorf University Hospital in Germany[5]. As seen from these examples, ransomware attacks have expanded in various sectors such as service, manufacturing, and healthcare. In particular, a new ransomware named Snake targeting industrial control systems has evolved into the cyber landscape, indicating that all industries will now potentially become ransomware targets.[6]

It is also expected that attackers will resort to stronger extortion methods for greater financial

---

[1] https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-trends-2020

[2] https://www.wsj.com/articles/travelex-outage-blamed-on-ransomware-attack-11578422140?page=2

[3] https://www.bbc.com/news/technology-53531178

[4] https://www.bbc.com/news/technology-52982427

[5] https://securityboulevard.com/2020/09/patient-dies-after-ransomware-attack-on-dusseldorf-hospital/

[6] https://ics-cert.kaspersky.com/alerts/2020/06/17/targeted-attacks-on-industrial-companies-using-snake-ransomware/

gain. The Maze ransomware is the first ransomware that introduced an extra way to create leverage against victims by stealing data while encrypting it. The attackers then threaten to publish the data if the victim decides not to pay. Recently, there has also been reports of a Sodinokibi ransomware variant which seeks out point of sale (PoS) systems and collect credit card information.[7] As such, attackers have been getting more aggressive in in their extortion methods, threatening to leak sensitive information and making various attempts to generate a second-stage payload, leading to growing damages by ransomware in the future.

[7] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sodinokibi-ransomware-cobalt-strike-pos

3 National Cyber Threat Outlook

1) Transformation of Malspam to Masspearing (Australia, AusCERT)

- The introduction of 'masspearing' combining personalized emails and spam campaigns.
- Emotet malware on the rise through spam campaigns.
- Personalized attacks on specific targets within an organization using leaked data such as emails, contract information, etc.

Cyber Threat Outlook

Spear phishing attempts are becoming increasingly sophisticated by the day. In recent years, there has been a proliferation of personalized attacks on specific targets and the attacks are likely to continue evolving further. Hackers obtain internal information on specific targets through the dark web, social networks, media, etc., and use such data to carry out precise and credible attacks. In addition, stolen corporate data such as financial information and contract details are then used to send out malware spam emails to the corporate accounts or clients in a new trend dubbed 'masspearing'. Against this backdrop, the growing use of Emotet malware attacks is accelerating the spread of malicious emails[8]. Emotet is a Trojan that first functioned as a banking trojan aimed at downloading additional payload through modules or malware after gaining access to a system. Once Emotet infects a system, it spreads itself by ransacking the contacts list and sending malspam to all the contacts. These attacks are often used as a springboard for secondary attacks such as ransomware and data theft and therefore require even further vigilance.

[8] https://www.malwarebytes.com/emotet/

2) Cyber-Attacks due to COVID-19 Pandemic Induced Work Culture (India, CERT-In)

- Attacks targeting teleworkers through malicious websites and emails containing malicious attachments.
- Growing risk of corporate data leakage from endpoint devices due to increased teleworking.
- Attempts to infiltrate corporate networks through remote network environments, such as vulnerable VPNs.

Cyber Threat Outlook

In 2020, the COVID-19 pandemic has resulted in a 600% increase in cybercrime worldwide[9]. As social distancing became essential and ushered in a 'non-contact' work culture, digitization has accelerated in all industries including sectors such as healthcare and education. This shift has also led to an expansion in the scope of cyberattacks. In particular, attacks exploiting vulnerable telecommuting environment are on the rise. Malware attacks have occurred in the form of sending email with malicious attachments to teleworkers or inducing them to access malicious websites. Because many teleworkers use their own personal devices to telework, these devices are relatively easy to attack. Because these personal devices would now hold corporate confidential information as well as personal account information, they have become tempting targets for hackers. Reports have also shown an increasing number of attempts to infiltrate corporate networks through remote access attacks such as exploiting weak VPN connections. In addition, because design of Security controls & monitoring systems may make it difficult to telework, it can be difficult to detect and respond to attacks in a timely manner, potentially causing significant damage. Therefore, greater efforts and measures are needed to enhance the security awareness of teleworkers and bolster the security of remote working environments.

[9] https://purplesec.us/resources/cyber-security-statistics/#:~:text=81%25%20of%20cyber%20security%20experts,losses%20could%20exceed%20%241%20billion

3) Surge of second attacks using dark web data leaks (Republic of Korea, KrCERT/CC)

- As dark web markets expand, transactions of sensitive information grow.
- Surge in sales of network access authorization information such as VPN and RDP due to the recent teleworking trend.
- Attackers collaborate to lower threshold and expand scale of attack.

Cyber Threat Outlook

As transactions in the dark web market increase[10] and the scale of cyber criminal organizations expands, attackers are taking to the darknets, with the aim of obtaining larger profits. In fact, on the dark web, individual cyber criminals can reportedly earn up to $2 million per year, and the total market size is said to reach $1.5 trillion[11]. A wide variety of sensitive information is currently sold and bought in the dark web including domain administration accounts, banking and financial accounts, as well as social media and online streaming service accounts[12]. In addition to ransomware attacks, this information can be exploited for credential stuffing and spear phishing, leading to even bigger attacks. Information collected through such attacks are then traded through the dark web again, leading to even more cyber crimes. With the recent increase in teleworking due to the COVID-19 pandemic, VPN (Virtual Private Network) and RDP (Remote Desktop) account information, which can exploited to penetrate corporate networks, are also becoming popular. In particular, these accounts are preferred by attackers because they are easy to collect by exploiting vulnerabilities of specific VPN products that have not been patched, or through brute force attacks, and can be used to completely control the system.[13] In addition, attackers are now collaborating to expand the scale of their attacks and to lower the threshold of attacks. They do so by selling network access rights rather than simply selling vulnerability execution codes or leaked information.[14] Such collaboration will further reinforce attack techniques and methods, and damage is expected to grow further.

[10] https://www.dailysecu.com/news/articleView.html?idxno=116411

[11] https://www.boannews.com/media/view.asp?idx=85536&page=7&kind=1

[12] https://www.boannews.com/media/view.asp?idx=89662

[13] https://www.itworld.co.kr/insight/110782

[14] https://www.boannews.com/media/view.asp?idx=91766

4) Increasing sophisticated BEC(Business email compromises) (Sri Lanka, Sri Lanka CERT|CC)

- Attacks targeting export and import businesses.
- Use of phishing, spear phishing, etc., to attack corporate mail.
- Sophisticated attacks, such as sending spoofed or compromised payment information to partner accounts of companies

Cyber Threat Outlook

This year, Sri Lanka has reported more than double the number of business email breaches (BEC) compared to last year. The number is expected to increase even further in 2021. In particular, import and export businesses, or international trade companies, were targeted due to the fact that many of them use email to conduct wire transfer payments. In recent years, hackers have refined their attack strategies, such as targeting the corporate mail through phishing or spear phishing in advance of an attack. Through a pre-attack, hackers change the settings for receiving and sending email, monitor the contents of the e-mail exchange with the account, and then intercept the payment information when the account sends the invoice. Because the invoice is outwardly a 'clean' email with no links or attachments, the company wires the fund as instructed without suspecting. These attacks are difficult to detect and require closer attention because of the potential scale of damage. In addition, even more sophisticated and intelligent attempts are expected in the future, such as impersonating a partner to change the details of a contract or to demand an urgent payment.

4 How to protect yourself from cyber threats

1) Ransomware

- Perform regular backup of all the critical information to minimize the loss.
- Check regularly for the integrity of the information stored in the databases.
- Maintain updated Antivirus/ End point protection software.

2) Masspearing

- Do not open suspicious attached files of mail and URL.
- Keep the operating system and third party applications up-to-date with the latest patches.
- Disable macros in Microsoft Office products such as Word, Excel, etc.

3) COVID-19 cyber threats

- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
- Change default passwords on your home Wi-Fi router to prevent hackers accessing your network.
- Use strong and unique passwords on every account and device.

4) Darkweb

- Use strong passwords and change them frequently.
- Use multi-factor authentication.
- Keep updated to the latest version.

5) BEC(Business email compromises)

- Use email authentication technology.
- Strengthen reporting mechanism for suspicious email and incidents detected by users.

AUSCERT

certfm
Handling Computer Security Incidents

KrCERT/CC

SRI LANKA
CERT|CC