HOW DOES RANSOMWARE ATTACK AN ORGANIZATION'S DATABASE?

Ransomware is malicious software, which can be installed onto your devices by clicking on a link that contains a virus.

This will grant the attackers control of the organization's system and machines to eventually access and encrypt important files. Attackers will then demand a ransom for these stolen files.

HOW DOES RANSOMWARE ATTACK?

1. DELIVERY

The attackers send an email to the targeted organizations and businesses by attaching the link of the virus.

2. INFECT

When the receiver clicks on the link, the dropper starts to download the virus into the machine.

3. CONTROL

Attackers then gain access to the devices and system, which as a result, allows them to control the hacked system.

4. DISCOVER

After controlling the system, the ransomware will search for important data to encrypt.

5. STEAL

Once found, important data is stolen from the system.

6. ENCRYPT

The stolen files are encrypted and the screen is locked displaying the ransomware to the victim.

7. DEMAND

Attacker will demand money in order to give the passcodes to unlock the system

CONCLUDE

- Paying the demanded ransom does not equal to gaining back access to your data.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key
- Some victims who paid the ransom have reported being targeted again by cyber criminals
- Paying the ransom will encourage this criminal business model

TIPS TO PREVEN RANSOMWARE

- Avoid clicking on suspicious and unusual links
- Do not disclose personal information
- Do not use unknown USB sticks
- Do not open suspicious email and attachments
- Keep your programs and operating system up-to-date
- Use only known download sources
- Use VPN services on public Wi-Fi networks

References

- Ransomware attacks, a growing threat that needs to be countered. (n.d.) Www.unodc.org. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- Cybersecurity Infographic: 7 Stages of a Ransomware Attack. (2021, July 7). Securance Consulting. https://www.securanceconsulting.com/7-stages-of-a-ransomware-attack/
- ProofPoint. (2016, August 15). What Is Ransomware, How to Prevent Attacks, Remove, & More | Proofpoint. Proofpoint. https://www.proofpoint.com/us/threat-reference/ransomware

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

HOW DOES RANSOMWARE ATTACK

AN INDIVIDUAL'S DATABASE

Ransomware is a type of malware that can attack an individual's database.

If a computer or network has been infected with ransomware, it will start to encrypt the data and cybercriminals will demand ransom money in exchange for releasing the data.

The process of such an attack is shown below:

1

PHISHING

Meticulous entity sends a phishing email.

2

RECEIVING

If users receive a phishing email and click on the link, the malware will exploit the user's device and begin its execution.

3

CONTROLLING

The malware gains control of the public key, accounts, and passwords.

4

ENCRYPTING

Files get encrypted and the screen displays the ransomware to the user.

5

EXTORTING

The user is demanded to pay a ransom in order to retrieve the stolen files.

6

DECRYPTING

After the ransom is paid, attacker will or will not send the private key, which is required for the decryption of the stolen files

WRAPPING UP

- Paying the demanded ransom does not equal to gaining back access to your data.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key
- Some victims who paid the ransom have reported being targeted again by cyber criminals
- Paying the ransom will encourage this criminal business model

TIPS TO PREVENT RANSOMWARE

- Avoid clicking on suspicious and unusual links
- Do not disclose personal information
- Do not use unknown USB sticks
- Do not open suspicious email and attachments
- Keep your programs and operating system up-to-date
- Use only known download sources
- Use VPN services on public Wi-Fi networks

References

- Ransomware protection: How to keep your data safe in 2021. (2021, June 15). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware
- Akara.umapornsakula. (n.d.). Ransomware attacks, a growing threat that needs to be countered. United Nations Office on Drugs and Crime. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- The real cost of a ransomware attack, and how to mitigate ransom threats. (n.d.). Global Security Mag Online. https://www.globalsecuritymag.fr/The-Real-Cost-of-a-Ransomware,20201019,103952.html

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

IMPORTANT ACTIONS

TO TAKE AS AN INDIVIDUAL

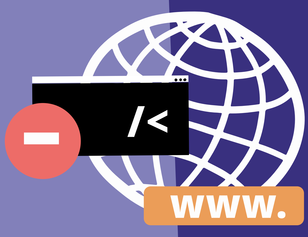
Falling victim to ransomware could put your vital business or personal data at risk of being lost forever.
These steps can help individual prevents ransomware from stealing their valuable data.

ACTION 1

MAKE REGULAR BACKUPS

Up-to-date backups are the most effective way of recovering from a ransomware attack.

ACTION 2



PREVENT MALWARE FROM BEING DELIVERED AND SPREADING TO DEVICES BY NOT CLICKING ON SUSPICIOUS LINKS

It is possible to reduce the likelihood of malicious content reaching your devices through a combination of filtering, blocking websites that are known to be malicious, actively inspecting content, and using signatures to block known malicious codes.

ACTION 3

PREVENT MALWARE FROM RUNNING ON DEVICES

A 'defense in depth' approach assumes that malware will reach your devices. You should therefore, take steps to prevent malware from running.

The measures required will vary for each device, but in general you should aim to use device-level security features.

ACTION 4

PREPARE FOR AN INCIDENT

Ransomware attacks can be devastating for various reasons such as operation halts and brand reputation damages.

Thus, it is important to perform the following preventive measures:

1. Evaluate the levels of risk ransomware could pose to operations ahead of time.
2. Develop a business continuity plan
3. Lay out your payment plan
4. Focus on prevention

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

DIFFERENT FORMS OF RANSOMWARE

Cyber criminals are getting more ambitious with their ransomware. Here are some of the most common forms of ransomware.

1 CRYPTO RANSOMWARE OR ENCRYPTORS

Crypto ransomware is designed to encrypt the victim's important data, but does not to interfere with basic computer functions.

Crypto developers often add a countdown to their ransom demand, such as "If you don't pay the ransom by the deadline, all your files will be deleted."

LOCKER RANSOMWARE 2

Locker ransomware interferes with the basic computer functions, where victims are only allowed to interactwith the ransom demand.

Locker ransomware does not target specific files, but simply locks you out of your devices altogether.

3 SCAREWARE

Scareware acts as a security program that pretends to have detected a virus or other issue on your computer, in which it directs you to pay to resolve the problem.

Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts without actually damaging files.

DOXWARE OR LEAKWARE 4

Doxware threatens to distribute sensitive personal or company information online.

Victims are forced to pay the ransom to prevent private data from falling into the wrong hands or entering the public domain.

5 RaaS (Ransomware as a Service)

RaaS creators host their ransomware on dark net sites as a market place and allows criminals to purchase it as a subscription.

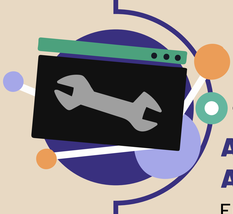
Once members infect computers and collect ransom payments, a portion of the ransom is paid to the RaaS creator under previously agreed-upon terms.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

10 PRINCIPLES OF ORGANIZATIONAL CYBERSECURITY TO RANSOMWARE PREVENTION

RISK MANAGEMENT

Ensure that the technology, systems, and information in your organization are assessed for risks in the most appropriate way.



ARCHITECTURE AND CONFIGURATION

Ensure that good cybersecurity is integrated into systems and services from the outset, and ensure that those systems and services can be maintained and updated regularly.

LOGGING AND MONITORING

Design your systems to be able to detect log in activities and investigate incidents of ransomware.

ASSET MANAGEMENT

Know and understand the data and systems that your organization needs to manage.

DATA SECURITY

Protect data where it is vulnerable in accordance with the risks. Back up your data and perform regular checks.

ENGAGEMENT AND TRAINING

Engage and support staff members to develop the skills and knowledge of cybersecurity and ransomware.

INCIDENT MANAGEMENT

Plan your response to cyber incidents and ransomware in advance by ensuring that you have the right personnel involved.

VULNERABILITY MANAGEMENT

Keep your systems protected throughout their lifecycle by keeping them updated. Additionally, develop a vulnerability management process.

SUPPLY CHAIN SECURITY

Collaborate with your suppliers and partners by embedding security within the contracting process.

It's essential to support organizations in your supply chain to practice ransomware prevention.

IDENTITY AND ACCESS MANAGEMENT

Control who can access to organization systems and data.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

IMPLEMENTING
EMPLOYEE TRAINING ON RANSOMEWARE
FOR SMALL BUSINESSES

Ransomware criminals do not differentiate small or large businesses. Everyone is a potential victim.

Hence, conducting training and educating your staff are some of the best preventive measures to protect your business.

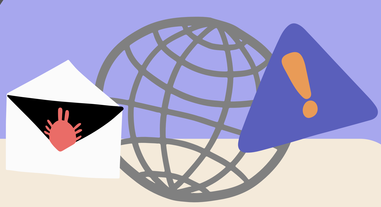
Here are some tips in implementing employee training on ransomware.

CONSIDERATIONS

CONDUCT SECURITY AWARENESS TRAINING

Having security awareness training in place for your staff is one of the best preventive measures for protecting your business.

Not only is your team informed about different types of cyber threats, but they also understand their roles in protecting company's networks and data.



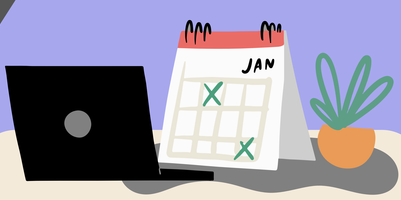
FOCUS ON SPECIFIC CYBERATTACKS

Training your staff on the tricks or methods that cybercriminals are likely to use, including some of the common ways computers and devices become infected, is essential.

TRAINING PROGRAM FOR NON-TECHNICAL AUDIENCES

Getting all of your team on board for comprehensive cybersecurity practices and making the contents easy to understand has been proven to be effective.

It is important to keep in mind that ransomware and cyberattacks are not just for IT professionals.



REGULAR TRAINING SESSIONS

Refreshing your employees' knowledge, encouraging them to report suspicious activities, and reminding them on the importance of cybersecurity practices and preventive measures, are ultimately some of the most optimum ways to protect a small business from cybercrime.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

IMPLEMENTING EMPLOYEE TRAINING ON RANSOMEWARE

FOR LARGE BUSINESSES

Large companies consist of many departments and employees. Conducting regular training exercises is the best preventive measure for protecting large businesses.

Here are some tips in implementing employee training on ransomware.

CONSIDERATIONS

REGULARLY UPDATED TRAINING

Regularly updated training programs cultivates healthy routines in the workplace.

On average, a training program can last for 2 months.

EDUCATION ON CYBERCRIME

Security awareness training helps your employees identify their precarious actions and better adopt cyber hygiene.

HANDS-ON APPROACH

Simulation drills will allow your team to track the progress of employees and identify any individuals who may require additional training.

SPECIFIC SECURITY TRAINING

As ransomware and phishing attacks are rising dramatically, specific prevention training programs are highly recommended.

CUSTOMIZED TRAINING BASED ON DEPARTMENTS

Companies should customize the cybersecurity's contents according to different employees' roles.

For instance, non-IT teams should concentrate on prevention, cybersecurity awareness, and reporting suspicious actions, while the IT teams are tasked to immediately combat infections.

EDUCATION ON REPORTING

All employees should train on how to report activities of ransomware.

The guidelines should include who to report to, how to report, and other relevant information.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

IMPORTANCE OF EMAILS

INTERNET AND SOCIAL MEDIA POLICIES

The internet provides the perfect ingredients for cybercriminals attacks.

Below are 5 tips to strengthen the security of your social media, internet, and other online platforms.

OFFLINE BACKUPS

The best policy to secure data is to have it backed up in several locations.

This reduces the loss of any encrypted information and restores system function in the case of ransomware attacks.

SPAM FILTER

More than 99% of emails threats may be avoided by using an efficient spam filter that can adjust itself in conjunction with a cloud-based threat intelligence center.

EMAIL SECURITY INSIDE AND OUTSIDE THE GATEWAY

Secure Email gateway solutions utilizes URL defenses and attachment sandboxing to identify risks and

prevent them from being sent to users. This prevents ransomware from infiltrating endpoint systems and users from unintentionally installing malware onto their devices.

SANDBOX TESTING

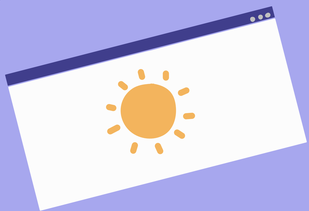
A sandbox is a typical tool used by security experts to test new or unknown files.

Sandboxes facilitate a secure environment for testing suspicious files while isolating it from the rest of the network.

WEB FILTERING

Web filtering technologies can prevent users from visiting risky websites and downloading malicious files.

This can prevent viruses such as ransomware from being downloaded via the internet.



UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

ESTABLISHING A SYSTEM SECURITY PLAN

A system security plan (SSP) is a document that outlines how an organization implements its security requirements.

An SSP outlines the roles and responsibilities of security personnel. It details the different security standards and guidelines that the organization follows.

For most firms, 4 basic steps are followed to create an SSP.

1

GATHER ALL SECURITY INFORMATION

Gather all documentations, policies, and procedures that describes the current security position for your system that is "in scope" for a Cybersecurity Maturity Model Certification (CMMC) or NIST 800-171 compliance assessment.

2

CONSULT CYBER SECURITY EXPERTS

Get inputs from the people responsible for system security, such as the system managers, system operators, and data owners, to ensure the documentation matches your environment's current state.

3

FILL UP THE GAPS

If there are gaps in your documentation, you will need to supplement those based on interviews, research, and other credible sources.

4

ORGANIZE AND COMPLETE YOUR SYSTEM SECURITY PLAN

Per the recommendations of the Department of defense (DoD), put all components of your SSP into a template to make sure it is correct, complete, and well organized.

There is no "official" or required SSP template, so create one that is easy to use.

RECOMMENDATIONS

If you have an internal security team, your in-house IT/security staff can fill in your SSP template.

A disadvantage with that approach can be a lack of objectivity to identify gaps that an auditor might later find.

Another option is to outsource a third-party expert to help with the process. This not only takes less time and money than a DIY approach, but also ensures the result complies with requirements and is useful to auditors.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

THE IMPORTANCE OF USING LICENSED, UP-TO-DATE SOFTWARE

Keeping software up to date and using the licensed version may not seem important, but this is a mistake that keeps the door open for hackers to access your private information, putting you at risk for identity theft, loss of money, credit fraud, and more.

Here are the benefits of using up-to-date software and legal software.

IMPROVED SECURITY

Hackers can use vulnerabilities within outdated software to exploit and harm your computer system and steal personal data.

Old software can become gateways into your network for hackers.

BETTER PROTECTION

Reports have shown that people and organizations who use unlicensed PC software generally encounter more malware than those who do.

This is because cybercriminals can pre-install or embed malware in the software and use it to gain unauthorized access to your information.

ROUND-THE-CLOCK SUPPORT

Licensed software generally comes with 24/7 tech support.

Whenever you face a problem, you can rest assured knowing that assistance will come quickly.

PROTECT OTHERS

If your device is infected by a virus due to vulnerabilities in outdated software, it can easily be passed on to your friends, family, and business associates.

IMPROVE PERFORMANCE

Old software can often eat up more computing power than it needs to. If the software is taking up a lot of extra time or it is just not running like it used to, then it could be time to update the software to the latest version.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

ENFORCING SECURE PASSWORD POLICIES

Enforcing strong passwords can become a proactive measure to protect you from ransomware attacks.

HERE ARE SOME TIPS:

PASSWORD LENGTH

A minimum of eight characters on all systems with a mix of special characters and numbers make it difficult to hack passwords.

For example: Donald-Mouse49!

PASSWORD HISTORY

Do not use the same password for every site as hackers will be able to steal all of your online accounts if they manage to hack into one of them.

PERSONAL INFORMATION

Avoid using birthdates, names, or phone numbers since it will be easy to guess the password.

EMAIL NOTIFICATIONS

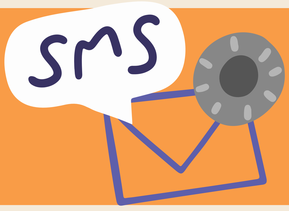
Use "Email Alert" every time for login in order to look out for any unusual activities.

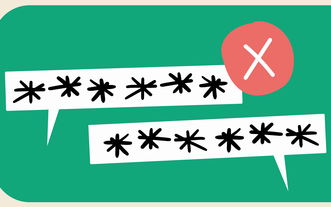
PASSWORD AGE

Password changes are recommended every 30, 60 or 90 days

MANAGER

Use an encrypted application to manage your passwords. This prevents hackers from easily accessing this encrypted information.



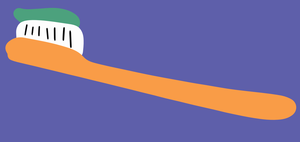


TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is an effective method of adding another layer of security to your account.

LOGIN-SHARING

Within the organization, do not share or passwords or use accounts together.



"Treat your password like your toothbrush.
Don't let anybody else use it and get a new one every six months."

-Clifford Stoll-

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

3 WAYS TO IDENTIFY RANSOMWARE THREATS

When it comes to malware detection strategies, both businesses and individuals have several options.
Each technique falls into one of 3 types:

1. SIGNATURE-BASED METHOD

Signature-based ransomware involves a static examination of files in a short period of time.

Data from executable files can be treated by security platforms as either ransomware or an authorized executable.

2. BEHAVIOR-BASED METHODS

Behavior-based detection involves the use of a tool to compare recent with past behavior.

For example, remote access to the company desktop from another state on the same day the employee checked in from the office.

3. DECEPTION-BASED DETECTION

Deception-based detection involves detection, analysis, and defense against zero-day and advanced attacks, often in real time. This process provides insight into malicious activities within internal networks.

WHAT TO INCLUDE IN YOUR REPORT

When reporting a ransomware incident, each country may have different requirements.

In order to provide useful information to the relevant law enforcement or forensics department, please be ready to provide the following information in your report.

1. THE FILE EXTENSION OF THE ENCRYPTED FILES
2. THE DATE AND TIME OF THE RANSOMWARE ATTACK
3. THE PHOTO OR A COPY OF THE RANSOM DEMAND NOTE
4. THE RANSOMWARE'S FULL NAME, WHICH IS USUALLY INCLUDED IN THE RANSOM NOTE OR ENCRYPTED FILE
5. ANY IP ADDRESSES CONNECTED TO THE NETWORK THAT YOU ARE UNFAMILIAR WITH
6. YOUR ORGANIZATION'S INFORMATION; ITS SECTOR, BUSINESS TYPE, AND SIZE, AND THE APPROPRIATE CONTACT PERSON.
7. THE METHOD OF THE ATTACK, WHETHER IT IS FROM AN EMAIL LINK OR ATTACHMENT, INTERNET BROWSING, OR OTHER MEANS OF INFECTIONS.
8. THE THREAT ACTOR'S EMAIL ADDRESS, URL, OR ANY OTHER WAY OF COMMUNICATION
9. THE ELECTRONIC COPIES OF CORRESPONDENCE WITH THE PERPETRATOR, IF APPLICABLE
10. THE BITCOIN WALLET ADDRESS OF THE CYBERCRIMINALS, USUALLY IDENTIFIED ON THE RANSOM PAGE.
11. THE AMOUNT REQUESTED FOR RANSOM AND THE AMOUNT PAID FOR RANSOM
12. THE OVERALL LOSSES ASSOCIATED WITH THE RANSOMWARE ATTACK INCLUDING, BUT NOT LIMITED TO, THE RANSOM AMOUNT.

References

1.eJohnson, K. (2021, September 7). 3 ransomware detection techniques to catch an attack. SearchSecurity. Retrieved November 22, 2021, from https://www.techtarget.com/searchsecurity/feature/3-ransomware-detection-techniques-to-catch-an-attack.

2.Report Ransomware Crime. (n.d.). Retrieved November 22, 2021, from https://www.provendatarecovery.com/report-ransomware-crime/

3.Ransomware detection. Unitrends. (2021, July 1). Retrieved November 22, 2021, from https://www.unitrends.com/solutions/ransomware-detection.

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

BENEFITS OF OUTSOURCING CYBERSECURITY

Insurance helps recover, but not stop a cyber-attack. It is best to implement preventive measures using cybersecurity services managed by certified specialists.

POTENTIAL TO SAVE MONEY

Having an in-house cybersecurity team can be costly. Outsourcing saves the cost of hiring IT staff or creating a new department.

AROUND THE CLOCK SERVICE

Ransomware attacks can occur at any time. Being monitored by specialists 24/7 is a safer choice.

ACCESS TO A BROADER RANGE OF SKILLS AND EXPERIENCE

As ransomware attacks evolve, experts can remove threats with up-to-date tactics, techniques, and procedures.

DEDICATED AND SKILLED SECURITY SERVICE PROVIDERS

Outsourcing cybersecurity services equips your specific needs from dedicated professionals skilled in solving technical issues.

GREATER FLEXIBILITY

It is critical to be proactive in upscaling security operations to respond to the rapidly changing business and threat landscapes.

GREATER VALUE FROM DETECTION TECHNOLOGY

By assuring the most up-to-date tools, cybersecurity can assist you to prevent threats and ease technological management.

References
Loyer, S. (2021). 6 Reasons/Benefits of Outsourcing Cyber Security Services. TGVT. https://tgvt.net/reasons-why-outsourcing-cyber-security-services/
Team, T. R. (2020). Five reasons to consider outsourcing your organisation's cyber security. Redscan. https://www.redscan.com/news/five-reasons-to-consider-outsourcing-your-organisations-cyber-security/
Cybriant. (n.d.). 9 unique reasons to outsource cyber security monitoring. https://cybriant.com/outsource-cyber-security-monitoring/

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

WHY IS CYBERSECURITY NOT THAT COMPLICATED?

WHAT IS RANSOMWARE?

Ransomware is a type of malware that encrypts a victim's files. This allows the attacker to demand a ransom to access this data

HOW DOES YOUR DEVICE GET INFECTED WITH RANSOMWARE?

One of the most common delivery systems is a Phishing spam - e-mail attachments disguised as a file you trust.

Other ways include downloading files from phishing sites or social media applications and clicking on 'infected' links.

HOW TO PREVENT RANSOMWARE?

There are many ways to prevent ransomware. A few tips include:

- Never click on suspicious links
- Avoid disclosing personal information
- Do not open suspicious email attachments
- Never use unknown USB sticks
- Keep your programs and operating system up to date
- Use only known download sources

WHAT TO DO IF YOU ARE A VICTIM OF RANSOMWARE?

Report the ransomware attack to the appropriate authority.
Anticipate the aftermath of the ransomware attack. Note that paying ransom does not equal getting back your data!
Seek advice or support from an experienced cyber security expert.

Please note that these are just some of the many personal safety measures you can take to keep yourself safe from ransomware and cybersecurity threats.

For more advanced issues, it is recommended you seek advice from an IT professional.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

HOW TO STAY SAFE AS A NON-DIGITAL NATIVE

There are simple things non-digital natives can do to stay safe on the internet and protect their personal information.

DO'S

KEEP YOUR PROGRAMS AND OPERATING SYSTEM UP TO DATE

KEEP YOUR PRIVACY SETTING ON

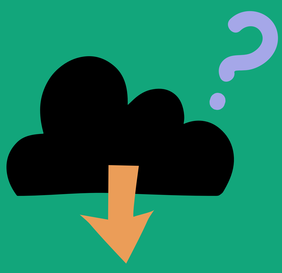
MAKE SURE YOUR INTERNET CONNECTION IS SECURE

CHOOSE STRONG PASSWORDS

DONT'S

AVOID DISCLOSING PERSONAL INFORMATION ONLINE

AVOID CLICKING ON LINKS IN SPAM MESSAGES OR ON UNKNOWN WEBSITES



DO NOT USE UNKNOWN DOWNLOAD SOURCES

DO NOT OPEN SUSPICIOUS EMAIL AND ATTACHMENTS

READY?

WITH THE RIGHT E-SAFETY KNOWLEDGE, YOU CAN PREVENT FUTURE PROBLEMS. IT IS IMPORTANT TO REMEMBER THAT ANYONE CAN BE TARGETED IF THEY STAY NEGLIGENT.

REFERENCES

HTTPS://WWW.MCAFEE.COM/BLOGS/INTERNET-SECURITY/8-TIPS-FOR-STAYING-SAFE-FROM-RANSOMWARE-ATTACKS/ HTTPS://WWW.ESECURITYPLANET.COM/THREATS/RANSOMWARE-PROTECTION/ HTTPS://USA.KASPERSKY.COM/RESOURCE-CENTER/THREATS/HOW-TO-PREVENT-RANSOMWARE

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

WHAT TO DO IF YOUR ORGANIZATION FACES RANSOMWARE THREATS?

A SIMPLE PROCESS OF HOW TO HANDLE RANSOMWARE

DETECTION

Ransomware is detected through either technology or personnel

Good detection technology raises a red flag that something is wrong

All employees must know how to report incidents.

ANALYSIS

Sufficient analysis must be made to take subsequent action

Confirm the incident is real

Determine the scope of ransomware

ESCALATION

If deemed severe, escalate the incident, and pass it to the Computer Security Incident Response Team (CSIRT), the disaster response team, or the business community.

CONTAINMENT

With proper authorization, disconnect the system from the organization's site network.

This is a business decision, not a technical decision.

Detachment must be approved by proper authorities withinthe organization.

RECOVERY

Reparation

- Data can be restored from backup tapes
- Manual Software reinstallation

APOLOGY

Explain the potential threat and damage in detail and actions to compensate victims, if any.

PUNISHMENT

•Identify the personnel responsible for the download of ransomware. Put into consider-ation that malware can be accidentally downloaded without any prior knowledge.

•Make the decision whether criminal prosecution is needed.

•Collect and manage evidence.

POST-MORTEM EVALUATION

•Reflect and create a follow-up plan.

•Ask what the organization can do differently next time?

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

HOW KNOWLEDGE-SHARING COMMUNITIES CAN HELP PREVENT RANSOMWARE

Knowledge sharing communities play a big role in raising public awareness and sharing best practices to prevent ransomware.

1 RAISING AWARENESS

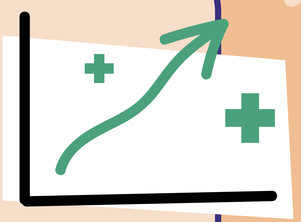
Public awareness of ransomware is increased within a community through the sharing of knowledge.

PROVIDING RELEVANT INFORMATION 2

If there are experts and enthusiasts within the community, these people can provide information and solutions that tailor to the specific needs of individuals.

3 CONTRIBUTING TO IMPROVEMENTS

Information sharing within communities can play a big role in improving security practices. As a result, advice is personalized and more relevant to the individual.

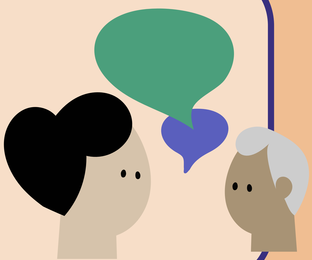


UPDATING INFORMATION 4

By sharing the most recent incidents of ransomware attacks, knowledge-sharing communities can inform the public and engage effective preventative measures.

5 STRENGTHENING ORGANIZATIONAL SECURITY

By sharing knowledge on the best cybersecurity practices and solutions with members, the overall security of the member's organization is strengthened.



UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

ANYONE CAN BE A VICTIM OF RANSOMWARE

With the development of technology and digital advancement, ransomware attacks have also grown tremendously. This cybercrime attack targets people of all sectors and anyone can fall victim.

HEALTHCARE SECTOR

Healthcare institutions perceive ransomware attacks as a serious threat that may unfortunately lead to life-threatening incidents for clients and patients. These organizations and hospitals store important data that are critical not only for their patients, but also for their own staff.

Small and Medium-Sized Enterprises (SMEs)

SMEs allocate fewer resources to cyber defense due to their tight budget and misconceptions that small businesses will not be targeted by cybercriminals.

FINANCIAL SECTOR

The nature of the financial sectors which normally involves the handling of their clients' personal information, such as their credit card details, social security number, contact information, makes them a perfect target for cybercriminals.

EDUCATION SECTOR

Due to budgetary constraints, most educational institutions have to settle for smaller IT departments. This makes them prone to ransomware attacks, as the small teams have to manage high incidences of online file sharing.

THE LEGAL SECTOR

Legal bodies are extremely appealing targets of ransomware as they are home to countless amounts of classified data, including those that might concern national and international security.

And many more!

References

1. Martin, J. A. (2017, July 14). Who is a target for ransomware attacks? CSO Online. Retrieved November 22, 2021, from https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html.
2. Who is a target for ransomware attacks? Cyber Security Solutions, Compliance, and Consulting Services - IT Security. (2019, October 21). Retrieved November 22, 2021, from https://www.infoguardsecurity.com/who-is-a-target-for-ransomware-attacks/.
3. Irei, A. (2021, September 29). Top 10 ransomware targets in 2021 and Beyond. SearchSecurity. Retrieved November 22, 2021, from https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond.

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

PERSONAL SAFETY CHECKLIST

TO PROTECT YOURSELF FROM RANSOMWARE AND ONLINE SECURITY THREATS

Ransomware is a form of malware where access to a computer is blocked until a ransom is paid. The recent pandemic has prompted an increase in remote work, which has led to a 148% increase in ransomware attacks. (AFCEA, 2021)

Here are a few must-dos to protect yourself from ransomware and cybersecurity threats in the era of social distancing.

KEEP DATA PRIVATE

Being selective when it comes to sharing personal information, such as names, ID numbers, and bank details, online is crucial.

BE SECURE

Adding many layers of security is another way to keep yourself secure. These may include enabling two-factor authentication, generating a strong password, installing a firewall, and downloading anti-virus programs.

BACK-UP REGULARLY

Backing up mainly refers to making a copy of your data on an external hard drive or in the cloud. Remember to do this regularly to ensure that you will always have your essential data in store.

UPDATE SOFTWARE

Looking out for any software updates for your operating system and programs is also essential. These updates often give your device protection against newer cybersecurity threats.

CREATE STRONG PASSCODES

A strong password should be eight-character long, have symbols, numbers, and capital letters, and should not include personal information such as birthday and email. Using different passwords for each account is also highly recommended.

AVOID SUSPICIOUS SITES

Clicking on suspicious-looking websites, files, or email is one of the most common ways to trigger ransomware attacks. Avoid clicking these unusual links to prevent yourself from falling victims to these cybercriminals.

References

- Security National Bank of South Dakota. (n.d.). Internet Safety Tips For Everyone Who Spends Time Online. Blue Compass, Des Moines, Iowa, www.Bluecompass.Com. https://www.snbsd.com/about/online-safety-guide
- Datto's 2019 State of the MSP Report. (2021, October 25). Datto. https://www.datto.com/resources/dattos-2019-state-of-the-msp-report
- Kaspersky. (2021, July 12). Ransomware protection: how to keep your data safe in 2021. Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

CHECKLIST OF ORGANIZATION SAFETY PROTOCOLS

Malware infections can be devastating to an organization, and recovering your valuable data can be a difficult process. The recovery itself also often requires the service of experts.

Hence, it's recommended that users and administrators take the following preventive measures to protect their computer networks from ransomware infections.

1 IDENTIFY ASSETS

Identify organization's assets such as important devices, data, and applications that may become targets of ransomware attacks.

2 BACKUP & RECOVERY

Perform and test backups regularly to mitigate the damage of data or system loss and to speed up future recovery processes.

Network-connected backups can also be affected by ransomware. Therefore, critical backups should be isolated from the network for best protection.

3 OPERATING SYSTEM AND SOFTWARE

Keep your operating system and software up-to-date with the latest patches. Having vulnerable applications and operating systems increase the risk of malware infection.

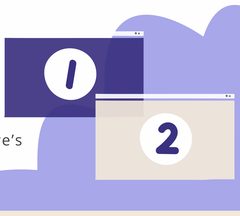
4 ANTI-VIRUS SOFTWARE

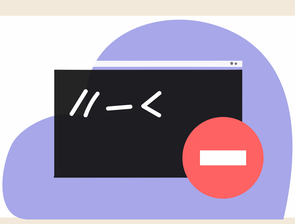
Maintain the latest anti-virus software and check all software downloaded from the internet before running and using them.

5 LIMIT USER ACTIVITY

Restrict users' ability to install and run unwanted software applications within machines.

Apply the principle of "Least Privilege" to all systems and services to prevent or limit malware's destructive impact.





6 DISABLE MACROS

Avoid enabling macros, a special code that gets replaced with specific information, from email attachments. Opening attachments and enabling macros will ause embedded codes to execute malware on the machine.

7 UNSOLICITED LINKS

Do not follow unsolicited web links in emails. Refer to phishing resources online to prevent unintentional harm to the organization.

Please note that these are just some of the many protocols your organization can follow to keep your important data safe from ransomware and cybersecurity threats.

For more advanced issues, it is highly recommended that you seek advice from IT professionals.

References

- National Institute of Standards and Technology (NIST). (2020b, October 1). Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides. NIST. https://miro.com/app/board/o9J_lOAZb0=/?moveToWidget=3074457388175839345&cot=14
- National Institute of Standards and Technology (NIST). (n.d.). Ransomware Protection and Response. NIST Computer Security Resource Center | CSRC. Retrieved October 20, 2021, from https://csrc.nist.gov/projects/ransomware-protection-and-response
- Australian Government. (n.d.). What to do if you're held to ransom: Step 6: Notify and report. ACSC. https://www.cyber.gov.au/ransomware/step-6-notify-and-report
- What Do I Do To Protect Against Ransomware? https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

CHECKLIST ON INTER-ORGANIZATIONAL SAFETY PROTOCOLS

As businesses transcend diverse cultural boundaries, online security has become more challenging.

Thus, inter-organizational safety protocols should be implemented to ensure cybersecurity attacks do not occur during inter-organizational exchanges.

It is recommended to take the following preventive measures to avoid ransomware attacks while attending to these inter-organizational processes:

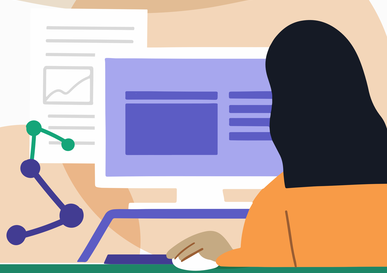
ESTABLISH COMMON ORGANIZATION PROTOCOLS

It is essential for organizations that share or exchange information regularly to establish some common organizational protocols.

These include, but not limited to, having common individual and organizational safety protocols, sharing internet and email policies, and consolidating coherent security and reporting systems.

MONITOR THE NETWORK

Regardless of the network arrangement methods chosen, prior to their establishments, organizations should have decided which of them should watch out for suspicious activities that might indicate a ransomware assault.



APPLY THREAT INTELLIGENCE

All organizations involved in the exchanges are recommended to update their staffs on the latest information about cyber threats and risk forecasts which could affect themselves or their counterparts in the same region or industry.

AVOID SHARING PERSONAL INFORMATION

To prevent data leakage, organizations should still be selective in handing out personal information or sharing accounts despite their mutual agreements.

CYBER AWARENESS TRAINING AND EDUCATION

All organizations should conduct co-organizational training and education to ensure everyone has the same level of awareness on cybersecurity threats and prevention practices.

Please note that these are just some protocols your organization can take to keep yourself safe from ransomware and cybersecurity threats.

For more advanced issues, it is recommended that you seek advice from IT professionals.

References

- Bisson, D. (2020, October 5). 30 Ransomware Prevention Tips. The State of Security. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/
- Check Point software technologies LTD. (n.d.). Why Anti-Ransomware? : Sophisticated, Evasive, Disruptive. Check Point. https://www.checkpoint.com/harmony/anti-ransomware/
- Kaspersky. (2021). Ransomware protection: how to keep your data safe in 2021. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

ROLE OF GOVERNMENT IN DEVELOPING STRONG CYBERSECURITY FRAMEWORKS

CONSTRUCT SOLID FOUNDATIONS

Governments play a major role in creating and maintaining a comprehensive, legal cybersecurity framework which is based on the national cyber security policies.

This framework should be built upon the following key principles.

Risk-based and prioritized

Cyber threats constantly mutate. Establishing a hierarchy of priorities with critical assets/sectors at the top is an effective starting point.

Technology-neutral

A technology-neutral approach is vital to ensure access to the most effective solutions in the marketplace.

Policies that require the use of certain technology can restrict the development of best practices.

Practicable

Any strategy is only as effective as it is implementable across a broad scope.

Government over supervision of private operators can prove to be counterproductive leading to an over-focus on compliance.

Flexible

When managing cyber risk, no "one-size-fits-all" approach exists. Each business faces distinct challenges, and requires the flexibility to address their unique needs.

Respectful of privacy and civil liberties

Security requirements should be balanced with the need for protecting privacy and civil liberties.

Ensuring that requirements do not intrude the fundamental rights of actors.

ESTABLISH OPERATIONAL ENTITIES WITH KEY RESPONSIBILITIES FOR SECURITY

Governments should set up operational entities to prevent cybercrime with ensured response, such as computer security response teams.

2 1 3

ENGENDER TRUST AND WORK IN PARTNERSHIP

No country or government can address cybersecurity risk alone.

Collaboration with non-governmental entities and international partners are crucial components for an effective cybersecurity.

Partnering with the private sector

Most infrastructure is owned by the private sector, making effective public-private cooperation essential.

Partnering improves the effectiveness of risk management, fostering trust and avoiding legal obstacles.

Global rather than isolated

Effective cybersecurity policies and strategies need to maintain global partnerships.

Frameworks should maintain international, voluntary and market-driven standards in order to maximize global information sharing and protection.

FOSTER EDUCATION AND AWARENESS ABOUT CYBERSECURITY RISK

People, process and technology are essential in ensuring cybersecurity. Governments should include awareness-raising, education and training on cybersecurity priorities, policies and programs as important components of any cybersecurity strategy.

Citation

- National Institute of Standards and Technology. (2021, May 13). NIST Releases Tips and Tactics for Dealing With Ransomware. NIST. https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware
- United States Secret Service. (n.d.). Preparing for a Cyber Incident. Secretservice.Gov. https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident
- Asia-pacific Cybersecurity Dashboard: Summary: Bsa: The Software Alliance BSA Alliance - https://cybersecurity.bsa.org/2015/apac/

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

OVERVIEW

OF MAJOR RANSOMWARE ATTACKS ACROSS THE ASIA-PACIFIC REGION

A report[1] disclosed the Asia Pacific region has 1.7 times the average encounter rate for ransomware attacks than the rest of the world.

Below are some of the major incidents from 2020 to 2021.

[1] Microsoft

2020

INDIA

74% of Indian businesses were targeted by ransomware attacks; with a third paying ransoms ranging from US$ 1 million to US$ 2.5 million to hackers.

SEPTEMBER 5, 2020

THAILAND

A hospital in Thailand[2] was unable to access its data due to ransomware attacks, but no demand for payment was sent.

However, some organizations were forced to pay ransoms up to 1 million Baht (US$32,000) to retrieve data.

[2] Saraburi Hospital

APRIL-DECEMBER 2020

JAPAN

Japan faced numerous ransomware attacks described as "very serious" by the National Police Agency last year.

Corporations in Japan reported 93 ransomware infections in 2020, an increase of 80% over the previous year.

OCTOBER 31, 2020

INDONESIA

2.9 million members' information of, a Fintech startup company[3] had been stolen and sold on a hacker forum.

This information included full names, email addresses, phone numbers, bank accounts, and tax and national ID numbers.

[3] Cermati-the fintech startup company

SEPTEMBER, 2020

MALAYSIA

A Malaysian web-hosting service became the target of a ransomware attack.

Perpetrators demanded US$ 900,000 in cryptocurrency.

MAY,2020

HONG KONG

A subsidiary of an international insurance company in Hong Kong was hit with a ransomware attack, in which the hackers demanded a payment of US$ 20 million.

MAY, 2020

THE PHILIPPINES

A daughter company of an international insurance corporation operating in the Philippines was requested to pay US$20 million in ransom by the cybercriminals.

References

- Ransomware attacks, a growing threat that needs to be countered. (n.d.). Www.unodc.org. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- Timeline of Cyber Incidents Involving Financial Institutions. (2016). Carnegie Endowment for International Peace. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
- Asia Pacific cyber incidents in 2020 hold big implications for this year's cyber insurance market | Munich Re Topics Online. (n.d.). Munichre.com. https://www.munichre.com/topics-online/en/digitalisation cyber/asia-pacific-cyber-incidents-in-2020.html ;
- Thai hospitals and companies hit by ransomware attacks. (2020, September 10). Reuters. https://www.reuters.com/article/us-thailand-hospital-ransomware/thai-hospitals-and-companies-hit-by-ransomware-attacks-idUSKBN2611WV ;
- Huge rise in ransomware cyberattacks on Japan firms an extreme threat: police. (2021, March 4). Mainichi Daily News. https://mainichi.jp/english/articles/20210304/p2a/00m/0na/020000c

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

CASE STUDY ON PUBLIC & PRIVATE SECTORS

THAILAND
SEPTEMBER 2020

HOSPITAL, PUBLIC SECTOR

CASE STUDY 1

HOSPITALS IN THAILAND ATTACKED BY HACKERS, UNABLE TO ACCESS DATA

Summary:

Hospitals in Thailand have been attacked and demanded a ransom with a "ransomware" code.

On September 5, one such attack resulted in a hospital[3] unable to access its data which led to life-threatening damages and was forced to slow down operations using only manual functions.

[3] Saraburi Hospital

CASE STUDY 2

ACER FACED WITH RANSOM UP TO $100 MILLION AFTER HACKERS BREACH NETWORK

Summary:

The REvil ransomware group stole a large amount of sensitive information from Acer's network. The information was auctioned on the dark web until Acer agreed to pay the demanded ransom.

TAIWAN
MARCH 2021

PC MANUFACTURER, PRIVATE SECTOR

CASE STUDY 3

JBS, WORLD'S LARGEST MEAT PROCESSOR SHUT DOWN

AUSTRALIA
JUNE 2021

FOOD PROCESSOR, PRIVATE SECTOR

Summary:

The world's largest meat processing company[4] shut down operations on multiple continents until hackers received the ransom of $11 million (£7.8m).

[4] JBS

Comments by stakeholders:

The company[4] said it was necessary to pay to protect customers, and it paid the money because of the sophistication of the attack, even though the "vast majority" of its plants remained operational.

[4] JBS

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

CASE STUDIES ON INDIVIDUALS & SMALL BUSINESSES

SINGAPORE, AUGUST 2020

● FOOD AND BEVERAGE

Summary:
An F&B business found its servers infected with NetWalker and directed the company to a site on the dark web to view the ransom amount.

All data was lost since backups were stored on their affected servers resulting in rebuilding its IT system from scratch.

Conclusion:
Based on this case, we can conclude that small businesses often lack the security or training to prevent and mitigate the effects of ransomware attacks.

THAILAND, JULY 2019

● INDIVIDUAL

Section Type:
Individual

Summary:
A Thai Facebook user reported that his computer was infected with ransomware. A letter from the hacker revealed that half of the company's data had been encrypted and demanded $6,500 in Bitcoin to retrieve the stolen files.

Conclusion:
This case demonstrated that anyone can fall victim to cyberattack. Any organization and individual who uses computers to manage their data is at risk.

VIETNAM, APRIL 2018

● IT COMPANY

Section Type:
Small business sectors

Summary:
An IT employee[5] in Ho Chi Minh City, received the Vietnam Computer Emergency Responses Teams' announcement detailing spread of a ransomware virus called GandCrab from the company's IT department.

Fortunately, the company suffered no damages because they were notified of the ransomware in advance.

[5] Kim Ngoc

Conclusion:
This case[5] proved that having effective prevention mechanisms decreases the risk as well as damage of ransomware attacks.

[5] Kim Ngoc

References

- How ransomware is a big problem for small business – and what to do about it. (n.d.). Insureon. https://www.insureon.com/blog/how-ransomware-is-a-big-problem-for-small-business
- T. (2019, July 13). โจรไซเบอร์ส่ง "ไวรัสเรียกค่าไถ่" ป่วนออฟฟิศ บีบเหยื่อจ่ายเงินแลกปลดล็อก. www.thairath.co.th. https://www.thairath.co.th/news/society/1614458
- Van Anh Vietnam Investment Review. (2018, April 7). Ransomware GandCrab attacks Vietnam. Vietnam Investment Review - VIR. https://vir.com.vn/ransomware-gandcrab-attacks-vietnam-58065.html
- Yu, E. (2021, July 8). Singapore sees spikes in ransomware, botnet attacks. ZDNet. https://www.zdnet.com/article/singapore-sees-spikes-in-ransomware-botnet-attacks/

UNODC United Nations Office on Drugs and Crime | CYBERCRIME | From the People of Japan | RansomAware

BREAKDOWN OF RANSOMWARE TARGET INDUSTRIES

HEALTHCARE

Due to the emergence of the COVID-19 pandemic, the healthcare institutions have become tempting targets of cybercriminals.

Healthcare industries include hospitals and testing centers that treat COVID-19 patients and save lives.

INFORMATION TECHNOLOGY

The pandemic also affects the IT industries as many companies have to resolve to remote working.

This new setting makes it easier for attackers to exploit IT gaps and find vulnerable ransomware targets.

In 2020, IBM Security X-Force analyzed that 41% of the cyberattacks targeted organizations with operational technology (OT) networks.

RETAIL

The growth in online shopping has increased the existing security challenges faced by the retail sector.

The nature of retail organizations typically involves holding a lot of sensitive data, including customers' names, their addresses, and even their financial information.

EDUCATION

Schools worldwide were forced to operate online in the wake of the COVID-19 pandemic. Due to the pressures on ensuring the continuity of learning, the education industry is the sector most likely to pay the demanded ransom should they be attacked by cybercriminals.

The education sector usually has tight budgets for both IT and cybersecurity, with stretched IT teams battling to secure an outdated infrastructure with limited tools and resources; such as downloading pirated software.

GOVERNMENT AGENCIES

Government agencies and infrastructures are vulnerable to ransomware attacks as the nature of their works are time-sensitive and crucial to the region.

These agencies are required to respond quickly to emergency and in the recovery of their data are more willing to pay the ransom amount and will fulfill the payment faster.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

ASIA PACIFIC CYBERSECURITY TRENDS

Cybersecurity solutions help individuals and organizations to monitor, detect, report, and handle cyber threats in order to maintain data confidentiality.

Here is an overview of cybersecurity trends from the year 2000 to 2021.

ADOPTION OF CYBERSECURITY SOLUTIONS

The adoption of cybersecurity solutions is likely to grow with the rapid penetration of the internet into developing and developed countries.

INCREASE OF CYBERSECURITY-RELATED ISSUES

Many countries in Asia are facing more cybersecurity-related issues.

According to an international security company[1] report, India accounts for 37% of the global breaches in terms of records compromised or stolen.

[1]Gemalto

APAC CYBERSECURITY MARKET IS EXPECTED TO SIGNIFICANTLY GROW

Cyberattacks have increased through ransomware during this pandemic, as organizations shifted to working remotely.

A study[2] reveled approximately 19 million COVID-19 ransomware and phishing attacks were noticed in Asia in 2020 alone.

[2]Microsoft

INCREASE USE OF CLOUD-BASED SERVICES

Increased usage of cloud-based services became a hotspot for cyberattacks as people work in unfamiliar, less secure circumstances.

Thus, a cloud-based cybersecurity solution is vital to security.

EVOLVING RANSOMWARE

With rapidly changing technology comes rapidly advancing threats. Cyber security solutions have become ever more prominent as they not only help an organization to detect cyberattacks, but also help to counter them.

Citation

- Lynett, M. (2015, November 25). A history of information security from past to present. Document Management | MES. https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present?hs_amp=true
- Asia-pacific Cybersecurity Market: 2021 - 26: Industry Share, Size, Growth - Mordor Intelligence https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
- The history of cyber security — Everything you ever wanted to know. (2021, June 10). SentinelOne. https://www.sentinelone.com/blog/history-of-cyber-security/
- A history of information security. (2019, June 27). IFSEC Global | Security and Fire News and Resources. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

ARE BUSINESSES IN ASIA PACIFIC PREPARED TO DEAL WITH RANSOMWARE ATTACKS?

WHAT THE EXPERTS SAY:

DELL TECHNOLOGIES 2021 GLOBAL DATA PROTECTION INDEX (GDPI) FINDINGS

Organizations face data protection challenges through newly-developed technologies such as cloud-native applications, Kubernetes containers, and AI.

In the Asia Pacific region, 82% of IT decision-makers are concerned their current data protection solutions ***will not*** meet all future business challenges.

REPORT BY LEADING IT SECURITY OGANIZATION SOPHOS

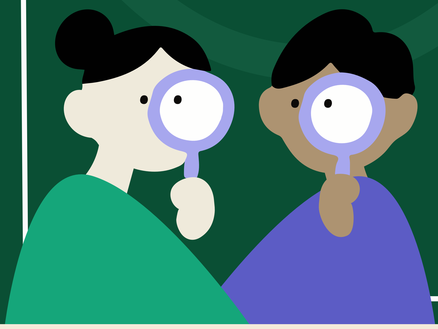
COVID-19 pandemic accelerated the rise of ransomware attacks on retail organizations as merchants shifted to selling their products and services online.

A retail survey[1] revealed that they were vulnerable to a growing new trend: extortion-only attacks.

Ransomware attackers don't encrypt files but threaten to leak stolen information online if a ransom demand ***is not*** paid.

[1] Sophos' State of Ransomware in Retail survey

DIRECTOR OF SECURITY ENGINEERING APJ AT VECTRA AI



The evolution of ransomware is a top concern in the Asia Pacific. In 2021, cyber-criminal groups modified their tactics to no longer rely on automated malware alone.

Users have adopted cloud services which allows attackers access to ransom at even faster rates than the normal 8-30 days. In fact, these attacks can be completed within a day.

KEY TAKEAWAYS

APAC Organizations must constantly train their staff members on cybersecurity.

Executive members need to be aware of potential damages by ransomware attacks.

A ransomware-incident-drill is an effective method which emphasizes the individual role people need to play to secure their businesses.

References

1. Accidental hero' halts ransomware attack and warns: This is not over. (2017, May 15). the Guardian. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack
2. Ransomware To Ransomops: Why Apac Enterprises Are Increasingly Vulnerable Cyber read-2021 Chris Fisher-November 18 - https://www.cpomagazine.com/cyber-security/ransomware-to-ransomops-why-apac-enterprises-are-increasingly-vulnerable/
3. Feiner, L. (n.d.). Amazon, Google and other tech companies join government effort to fight ransomware. CNBC. https://www.cnbc.com/2021/08/05/amazon-google-join-government-effort-to-fight-ransomware.html
4. Raj. (2021, September 16). Are Asian businesses really prepared to deal with ransomware attacks? Techwire Asia. https://techwireasia.com/2021/09/are-asian-businesses-really-prepared-to-deal-with-ransomware-attacks/

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

IMPORTANT MILESTONES OF UNODC

REGARDING RANSOMWARE AND CYBER SECURITY

INTRODUCTION

UNODC has been actively participating in the promotion of Asia Pacific's ransomware and cybersecurity awareness.

Cybercrime continues to grow in the region and is quickly evolving from an emerging threat to a criminal enterprise.

THAILAND

- **Bangkok (Thailand), July 31, 2017**
  Thailand strengthened its capacity to trace and investigate cryptocurrencies.
- **Bangkok (Thailand), March 26, 2018**
  UNODC and The Kingdom of Thailand joined together to fight Cybercrime in Southeast Asia.
- **Bangkok (Thailand), February 25, 2021**
  UNODC launched the report "Darknet Cybercrime Threats to Southeast Asia," a first of its kind analysis of darknet-enabled threats in the region.
- **Bangkok (Thailand), July 5, 2021**
  UNODC and the private sectors partnered together to train cybersecurity professionals.
- **Bangkok (Thailand), October 18, 2021**
  Ransomware attacks identified as a growing threat that needs to be countered.

VIETNAM

- **Dong Ha, Quang Tri Province (VietNam), June 5, 2015**
  Training of frontline officers went high tech in Viet Nam.
  Fifty front-line officers representing Border Liaison Offices (BLO) and related customs agencies, border guards and police counter-narcotics, environmental and economic units successfully completed two intensive five-day training courses

LAOS

- **Vientiane (Lao PDR), August 20, 2018**
  Lao PDR and UNODC held first roundtable discussions on cybercrime.
- **Vientiane (Lao PDR), August 23, 2019**
  UNODC opened the first specialized Forensics Laboratory in Laos for analyzing digital evidence.

MALAYSIA

- **Langkawi (Malaysia), February 26, 2019**
  UNODC engaged ASEAN in regional exercise on cyber threat intelligence collaboration for joint cybercrime and counter terrorism response.

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

TOP 5 INDUSTRIES AFFECTED BY RANSOMWARE ATTACKS IN ASIA PACIFIC

During the COVID-19 pandemic, cybercrimes have increased by 600% in the Asia Pacific region.

Within the series of cyberattacks, ransomware was the most prominent malware threat across the various sectors.

RANKING	1.	2.	3.	4.	5.
INDUSTRY TYPE	**EDUCATION**	**DISTRIBUTION & TRANSPORT**	**FINANCIAL INSTITUTIONS**	**BUSINESS & PROFESSIONAL SERVICES**	**RETAIL**
RANSOMWARE RECOVERY COST (UNIT: million US dollars)	**USD$ 2.73**	**USD$ 2.44**	**USD$ 2.10**	**USD$ 2.00**	**USD$ 1.97**
EXAMPLE OF MAJOR INCIDENT WITHIN THE REGION	***Korea*** - In May 2017, a cybercriminal group called WannaCry, suspected to have originated from North Korea, infected South Korean Universities. This incident was devastating as the South Korean cybersecurity agency[2] has just reported approximately 130,000 ransomware attacks last year, costing KRW300 billion (US$268 million). ***Korea*** - In May 2017, ransomware[2] in North Korea attacked South Korean universities. In addition, a South Korean cybersecurity agency[3] reported the nation faced 130,000 ransomware attacks last year, costing KRW300 billion (US$268 million). [2] RanCERT	***India*** - In June 2017, the nation's largest container port[4] was infected by ransomware[5] The incident caused the computer system to be locked down delaying all shipments. [4] Jawaharlal Nehru Port (JNPT) [5] Petya ransomware	***Asia Pacific -*** In November 2021, branches of an insurance giant[6] based in Thailand, Malaysia, Hong Kong, and the Philippines were attacked by a ransomware group, "Avaddon." 3 TB of sensitive data was stolen. [6] JAXA Asian	***Singapore -*** In August 2021, Asia's leading merchant commerce platform services[1] was hit by BlackMatter, a ransomware group. They obtained important services and private agreements between an Indian merchant platform company[7] and multiple Indian banks, and personal information of 500,000 records [7] Pine Labs	***Thailand -*** In July 2020, Maze ransomware attacked a beverage company[8] and made claims over the dark web. Hackers have not yet released the stolen data, so it appears that the company is yet to accept or reject the ransom. [8] Thai Beverage Public Company

References

1. The State of Ransomware in Education 2021. (n.d.). https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf
2. Insurer AXA hit by ransomware after dropping support for ransom payments. (n.d.). BleepingComputer. Retrieved November 22, 2021, from https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/
3. Ransomware attacks, a growing threat that needs to be countered. (n.d.). https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware