CYLANCE
CONSULTING

10 THINGS YOU NEED TO KNOW ABOUT RANSOMWARE

Some cybersecurity experts call ransomware attacks an epidemic. In 2016, the FBI estimated that ransomware attacks resulted in over $1 billion in income for cybercriminals (Source: CNN). Experts attribute the ransomware epidemic to people's carelessness in clicking on phishing emails and infected advertisements. Here are 10 things organizations should know about ransomware:

01

Ransomware was first reported in 1989

...and since then, a number of different variants have evolved — MSIL/Samas is designed to encrypt entire networks rather than single devices

02

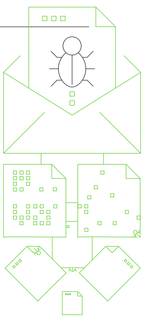
Ransomware doesn't discriminate when it comes to platforms and devices

Any device that can connect to the Internet is at risk

03

Ransomware can be distributed through various channels, such as:

- Spam email campaigns that contain malicious links or attachments
- Security exploits in vulnerable software
- Internet traffic re-directs to malicious websites
- Legitimate websites that have malicious code injected into the website
- Malicious advertisements (malvertising)
- Phishing emails with malicious links or attachments
- Social engineering
  (coercing users into breaking security protocols to introduce malware into their systems)
- SMS messages
- Botnets
- Self-propagation
  (spreading from one infected computer to another)
- Ransomware-as-a-service



04

Ransomware often goes undetected

by traditional detect-and-respond antivirus solutions, because they lack the ability to spot and remove second-generation malware

05

Organizations should change their mindset from a reactive-based model to a prevention-oriented one

Prevention includes:

- Keeping software up-to-date, including operating systems
- Avoiding dangerous web locations
- Educating users to detect potential cyberattacks delivered *via* phishing emails, infected banners, spam emails, social engineering attempts, and more
- Using machine learning based cybersecurity tools

06

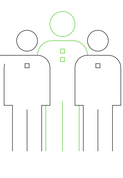
Organizations should develop a prevention and response plan

- Prepare in advance of an attack
- Find and address vulnerabilities
- Review and test your plan

07

Organizations should identify a prevention and response team

- Choose an appropriate service level agreement
- Ensure the team possesses specialized expertise
- Vet and validate the team's expertise



08

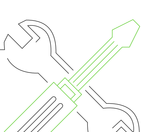
Organizations should perform a compromise assessment

- Detect current and previously compromised systems
- Collect evidence and analyze adversary tactics
- Remediate across the enterprise

09

Organizations should complete a security tools assessment

- Evaluate existing security tools
- Execute a gap analysis
- Remediate findings and outline opportunities for improvement



10

Organizations should respond and future-proof

- Contain discovered incidents immediately
- Perform complete remediation activities
- Carry out sustainable prevention

As threatening as ransomware sounds, damage can be avoided with increased user awareness coupled with the right security practices. Businesses need to be aware of the risks and take adequate precautions to minimize the impact in the event of an attack. Contact **Network Utilities** to learn more about how **Cylance** can help you prevent and remediate ransomware.

networkutilities
t: 02087833800
e: sales@netutils.com
www.netutils.com

CYLANCE
www.cylance.com