Things to know about RANSOMWARE

WHAT IS IT?

Ransomware is a type of malware (malicious software) that locks up data to make it inaccessible until a sum of money is paid to cyber thieves by the computer or device's owner.

1 What it does

A computer or mobile device becomes infected with a ransomware program, commonly through a phishing email or a compromised web page.

Infection

Encryption

The ransomware program generates a "key" that encrypts, or locks, files - sometimes spreading to the network.

Extortion

A ransom note is left behind on the victim's screen that demands payment to decrypt or unlock the files. Instructions for payment typically require the user to purchase Bitcoins, a worldwide Internet currency.

Decryption ?

Attackers claim that once payment is verified, the victim will get a key to unlock data, but this doesn't always happen.

2 How it spreads

Infected websites

"Exploit kits" hidden on infected websites are programmed to find vulnerabilities - such as old, unpatched apps and software- on victims' machines and devices.

Phishing

By clicking on a link in email or downloading an infected attachment, users can inadvertently download ransomware programs.

Applications on mobile devices

Applications can be laced with ransomware.

Through the network

Malicious ransomware programs can migrate from a user's computer to a network and infect shared files.

3 Common methods of infection

Email attachments

Macroscripts in MS Office documents are a common way ransomware is downloaded onto a computer.

JavaScript can be disguised as a harmless-looking file, such as a text file, and it can be programmed to spread ransomware.

Exploit kits

Exploit kits are programmed to search for vulnerable applications. The popular "Nuclear" kit has been used to target Adobe Flash.

Types of ransomware

Variations of ransomware target different vulnerabilities, such as:

CryptoWall - spread via spam, infected websites and web ads

Locky- delivered in the form of infected MS Office documents or compressed attachments (e.g., .zip files) in phishing emails.

Ransomware may affect Windows, Macintosh, and Linux systems.

4 By the numbers

300%

Increase from 2015 to 2016

Attacks have risen from 1000 to 4000 per day since 2015

$679

Average payment

The average ransom demand has grown from $294 in 2015 to $679 in 2016.

600%

A growing trend

There has been a 600% growth in new ransomware variations since December 2015.

5 Consequences

Makes personal and University data inaccessible

Can cause reputational harm to the University

Paying ransom feeds the cyber crime chain

6 What to do

Detach computers from the network

Isolate infected computers from the network as soon as possible to prevent the spread of malicious programs to shared drives on the network.

Shut the computer or device down

Turning off the affected system may minimize the number of infected files.

Clean system & restore data from backup

Methods for cleaning an operating system (OS) or reverting to restore points vary between devices and machines, so seek advice as appropriate.
It is important to remember that data on your system may not be accessible after an attack so -

Back up data regularly!

Protect yourself and your data

Back up, Back up, Back up!

Back up all data that you are responsible for, using multiple methods or formats to back it up. Ensure that your sole backup is not connected to your computer, as it could also become infected.

Don't use an account with administrative privileges for every day use

Using an account with administrative privileges may allow the infection to spread further on a computer.

Disable macros in MS Office documents

A common method of infection is through macros in MS documents sent via email.

Never click on links in email or download attachments unless you can verify the source

Phishing emails are one of the most common ways that ransomware and other types of malware spread.

Update and patch

Out of date, unpatched operating systems and other types of software make it easy for cyber theives to know what vulnerabilities to target.

Use antivirus software and keep it updated

Antivirus can help defend against ransomware and other types of malware. Members of the UW community can download free antivirus here:

itconnect.uw.edu/wares/uware/sophos-anti-virus-software/

RESOURCES

Sophos, "How to Stay Protected Against Ransomware"
Cisco 2016 Midyear Cybersecurity Report
TrendMicro, "The Reign of Ransomware"
FBI, "How to Protect Your Networks from Ransomware"

UW Office of the Chief Information Security Officer
ciso.uw.edu

For more information, see our "Malware" online training:
https://ciso.uw.edu/education/online-training/#malware