Things to know about MALWARE

WHAT IS IT?

Malware, short for malicious software, is a program or code that is used to disrupt a computer's normal operation.

Classification of Common Types

Virus

Software or code that infects other software when it is downloaded, activating or reproducing itself whenever the attacked software is run. A virus can be programmed to do any number of harmful things, including stealing data and disrupting systems.

Worm

Like a virus, a worm can destroy data and programs while replicating itself on a computer. Unlike a virus, which initially requires a human to download and activate it, a worm spreads automatically on a computer or throughout a network.

Trojan

Initially disguised as a legitimate file, it will search for data, such as financial information or browsing history, sending it to cyber criminals. It also may connect your computer to a botnet (see below).

Rootkit

Has the same capability as a virus or trojan, but it runs at a core level ("root" or "kernel") underlying the operating system in order to avoid detection and allow the intruder full access.

Keylogger

Records strokes on the keyboard and sends data such as passwords, financial account and other confidential or personal information to cyber criminals.

Adware & Spyware

Spyware steals data and/or tracks Internet activity to, among other things, send potentially relevant and typically intrusive advertising (Adware) to the user's computer.

Ransomware

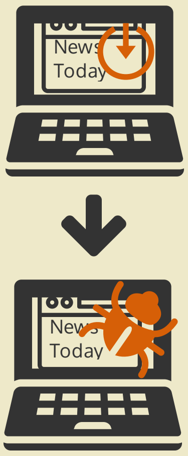
A relatively new type of malware that locks data and files using encryption, then demands payment to unlock the data, sometimes posing as FBI or other officials.

Bots

A computer that, unknown to its owner, has been compromised by an attacker through a virus or trojan and added to a botnet - a network of compromised machines that are then used for nefarious purposes, such as sending spam or launching denial-of-service attacks.

HOW DOES MALWARE INFECT A COMPUTER?

Through the web browser



While browsing, the user stumbles upon malware that an attacker has loaded onto a legitimate website. The malware downloads without the user's knowledge.

The malware redirects the user to a server with an "exploit kit" aimed at vulnerabilities in the operating system, browser, and applications.

85% of all malware comes from infected web pages

40% One exploit kit's compromise rate so far in 2015 (Angler)

30,000 new malicious URLS each day

Phishing

A user is tricked by an email designed to entice recipients into clicking on a link that leads to a web page or server loaded with malware.

A user is tricked into opening an attached file (e.g., .exe, .zip, .doc) that downloads malware onto the user's computer.

USB devices

Infected thumb drives and other USB devices also spread malware.

WHO IS RESPONSIBLE?

Cyber criminals use malware to steal data, such as personally identifiable information, credit card numbers and other financial data, as well as login passwords and credentials. They then convert it into cash in various ways, including selling it on sophisticated Internet marketplaces and forums.

The Offenders

All of us in the UW community share the responsibility to safeguard our personal data, passwords, and login credentials, and the University of Washington's institutional information.

The Defenders

WHAT CAN YOU DO?

Update and patch

Keep operating systems, software, browsers, and plug-ins updated and patched on all computers and devices.
Learn more:
ciso.washington.edu/update-and-patch

Use antivirus software on all computers and devices and keep it updated

Sophos Anti-Virus Software is available free of charge to all UW students, faculty, and staff. More info:
washington.edu/itconnect/wares/uware/sophos-anti-virus-software

Employ good password practices

Passwords online training:
ciso.washington.edu/online-training/#passwords

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

Phishing training and guidance:
ciso.washington.edu/resources/risk-advisories/phishing

Use encryption on files, devices, and communications when appropriate

Encryption guidance:
ciso.washington.edu/resources/privacy-briefs/encyption

Back up your data

Back up all data that you are responsible for in case of data corruption or loss due to malware.

RESOURCES

Sophos Five Stages of a Web Malware Attack
Cisco 2015 Midyear Security Report
McAfee Labs Threats Report: August 2015
How-to-Geek Not All "Viruses" Are Viruses: 10 Malware Terms Explained

Office of the Chief Information Security Officer
University of Washington

More info: http://ciso.washington.edu/online-training/#malware
Home page: ciso.uw.edu