U.S. ARMY
CYBER COMMAND
www.arcyber.army.mil | Follow @arcyber

Ransomware and Malware

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software, or malware, designed to deny a user access to a computer system or computer files until a ransom, typically cryptocurrency, has been paid. Ransomware uses encryption to hold the data hostage and requires a decryption key before a user is granted access.

Today ransomware is one of many methods used by cybercriminals to gain data from users for financial gain. Since it was first recorded in December 1989, ransomware has evolved from being a tool exclusively used by advanced cybercriminals to a service that can be implemented by any cybercriminal willing to purchase the necessary software. According to Edward LaBarge, director of the U.S. Army Criminal Investigation Command's Major Cybercrime Unit, ransomware attacks have been increasing and that trend is expected to continue.

HOW DOES RANSOMWARE WORK?

Cybercriminals use many methods to trick users into downloading ransomware. The most common ransomware attack methods to look out for are socially engineered phishing emails; links in forums or search engines to compromised or copycat websites containing a malicious download; social media impersonators; and software vulnerabilities.

A drive-by download occurs when a user unknowingly "downloads" a program without knowledge or by giving consent. Users may see an increase in system resources when a malware attack occurs; for example, an unexplained increase in CPU usage could be malware being loaded onto the computer.

HOW CAN RANSOMWARE BE AVOIDED?

To prevent ransomware from occurring or reoccurring, users should:

- Ensure their data is backed up regularly (manually or using automated backup software)
- Maintain the latest operating system updates
- Keep antivirus software installed and up to date
- Always use caution when opening email links or attachments
- Be mindful of pop-ups on websites and do not allow unsolicited downloads
- Stay informed on the latest ransomware trends and tactics used by cybercriminals

WHAT ARE SOME RECOMMENDATIONS FOR RANSOMWARE VICTIMS?

- **Isolate the infection.** Infected computers should be disconnected from the Internet (unplug the Ethernet cable or place the computer in airplane mode) as soon as possible to prevent ransomware from communicating with the attacker or spreading to other computers.
- **Identify the infection.** In most cases, it will be easy to determine if the system has been infected. However, determining how the ransomware was downloaded is not always as obvious. Identifying how the ransomware was downloaded can ensure other users do not make the same mistake.

- **Report it.** Ransomware victims are encouraged to report the incident to the Internet Crime Complaint Center at https://www.ic3.gov
- **Identify a solution.** It is recommended to wipe the system and restore it using a clean offline copy.
- **Prevent reoccurrence.** Evaluate how the infection occurred and put measures in places to ensure your system is not open to another infection.
- **Lastly, LaBarge recommends never paying the ransom.** "Paying doesn't guarantee you get your data back and it won't prevent the cybercriminals from hitting you again with another ransom," he says. Making the attack profitable also encourages further attacks, and paying does not guarantee that your data will not be sold by the attacker.

WHAT ARE MALWARE COMPUTER VIRUSES?

Malware and viruses are harmful computer programs that can be transmitted in a number of ways and differ in many ways, but are all designed to spread themselves from one computer to another through the Internet. Most commonly, they are designed to give the criminals access to the infected computers.

WHAT ARE "SPYWARE" AND "ADWARE"?

The terms "spyware" and "adware" apply to several different technologies. The two important things to know about them is that:

They can download themselves onto your computer without your permission (typically when you visit an unsafe website or open an unsafe attachment)

They can make your computer do things you don't want it to do. This might be as simple as opening an advertisement you didn't want to see, or as devastating as tracking your online movements, stealing your passwords, and compromising your accounts.

WHAT IS A "BOTNET"?

Botnets are networks of computers infected by malware (computer viruses, key loggers, and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks.

If your computer is infected with botnet malware, it communicates and receives instructions about what it's supposed to do from "command and control" computers located anywhere around the globe.

Many botnets are designed to harvest data such as passwords, Social Security numbers, credit card numbers, addresses, telephone numbers, and other personal information. The data is then used for identity theft, credit card fraud, spamming, website attacks, and malware distribution.

WHAT CAN I DO TO PROTECT MYSELF?

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it or mark it as junk email.
- **Protect all devices that connect to the Internet:** Along with computers, smartphones, gaming systems, and other web-enabled devices need protection from viruses and malware.
- **Plug and scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.