FACT SHEET

U.S. Army Cyber Command

The Nation's Army in Cyberspace

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: RANSOMWARE

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.

Source: U.S. Army Criminal Investigation Command
For more information about computer security, other computer-related scams, and other cybercrime alert notices and prevention flyers visit the Army CID Major Cybercrime Unit website at https://www.cid.army.mil/mcu-advisories.html

Follow ARCYBER on
(click the images to visit our pages)

Cyber

ABOUT US: Army Cyber Command integrates and conducts cyberspace, electronic warfare and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. As of 16 Feb 2021