UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

CID LOOKOUT
ON POINT FOR THE ARMY

Ransomware: A Virtual Hostage Situation

QUANTICO, VA (Feb. 17, 2021) – The U.S. Army Criminal Investigation Command's Major Cybercrime Unit (MCU) is warning the Army community about an increase in ransomware attacks.

According to Edward LaBarge, director of CID's Major Cybercrime Unit, there was a rise in ransomware cyberattacks in 2020 and the trend is expected to continue this year.

Ransomware is a type of malicious software, or malware, designed to deny a user access to a computer system or computer files until the 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.

Similar to other types of malware, ransomware is one of many methods used by cybercriminals to gain data from users and to attempt financial gain. The first recorded ransomware attack was in December 1989 using floppy discs. As ransomware evolved, it moved away from being a tool exclusively used by advanced cybercriminals and became a service that can be implemented by any cybercriminal willing to purchase the software.

Today, there are many methods used by cybercriminals to trick a user into downloading ransomware. The most common ransomware attack methods to look out for are from socially engineered phishing emails, links in forums or search engines to compromised or copycat websites containing a malicious download, fake social media impersonators, and through software vulnerabilities.

-MORE-

LaBarge said the two most common ways MCU is seeing ransomware executed is by "infecting ones computer through phishing emails or visiting a malicious website via a drive-by download."

A drive-by download occurs when users unknowingly "download" a program without knowledge or by giving consent. LaBarge said users typically 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.

To prevent ransomware from occurring or reoccurring, users should ensure data is backed up regularly, maintain the latest operating system updates, keep antivirus software installed and up-to-date, and always use caution when opening email links or attachments.

"It is important to always ensure your data is backed up," said LaBarge. "It is recommended that you back up your data monthly. If possible, you should have your backups automated so you don't have to worry about it. Whether it's using the iCloud, Time Machine or the Windows 10 backup feature, having it automated will help ensure your data is protected against tragedy."

He also 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."

Ransomware Victim Recommendations

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 – Ransomware attacks on Army issued computers must be reported to your system administrator or security representative. If a personally owned computer becomes infected, you are strongly encouraged to report the incident to the Internet Crime Complaint Center.
Identify a solution – How data gets recovered on Army issued computers is determined by your unit's system administrator. For personally owned computers, it is recommended to wipe the system and restore it using a clean offline copy. While it may be tempting to pay the ransom, there is no guarantee that your data will not be sold by the attacker. Furthermore, paying the ransom, making it profitable for the cybercriminals, only encourages future ransomware attacks.
Prevent reoccurrence – Evaluate how the infection occurred and put measures in places to ensure your system is not open to another infection.

Tips to Avoid Becoming a Ransomware Victim

Education – Stay updated on ransomware trends and the evolving methods used by cybercriminals in ransomware attacks.
Cyber best practices – Avoid opening attachments or clicking on links in suspicious emails. Be mindful of pop-ups on websites and do not allow unsolicited downloads.

-MORE-

Regular updates – Ensure your computer's operating system and antivirus software are updated. As ransomware variants are identified, updates and patches are created and released to prevent infection.

Backups – Maintaining valuable information offline, such as an external hard drive, provides an alternative method of recovering data lost in a ransomware attack.

-30-

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil