Cybercrime Prevention Flyer

CPF 00002-2021-CID361-9H **1 February 2021**

Ransomware – A Virtual Hostage Situation

You likely have heard the term "ransomware" on the news or received an email letting you know your information has been compromised in a ransomware attack. According to Bitdefender, ransomware attacks increased significantly worldwide during the first six months of 2020 compared to the first six months of 2019. The increase in ransomware attacks is no surprise considering how commonplace remote working and distance learning has become in the COVID-19 environment. Individual users, businesses, hospitals, schools, and state and local governments have fallen victim to ransomware; the number of ransomware attacks in 2021 is expected to rise as a result.

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 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.

Ransomware is not a new method of attack for cybercriminals. 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.

How Ransomware is Downloaded

There are many methods used by cybercriminals to trick a user into downloading ransomware. However, the most common ransomware attack methods to look out for are:

- **Email** – Socially engineered phishing emails containing a malicious attachment or including a malicious link.
- **Internet** – Links in forums or search engines to compromised or copycat websites containing a malicious download.
- **Social media** – Cybercriminals impersonating someone you know and sending media or documents that require download.
- **Software vulnerabilities** – Unpatched and outdated software leave computer systems vulnerable to exploits while connected to the internet.

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

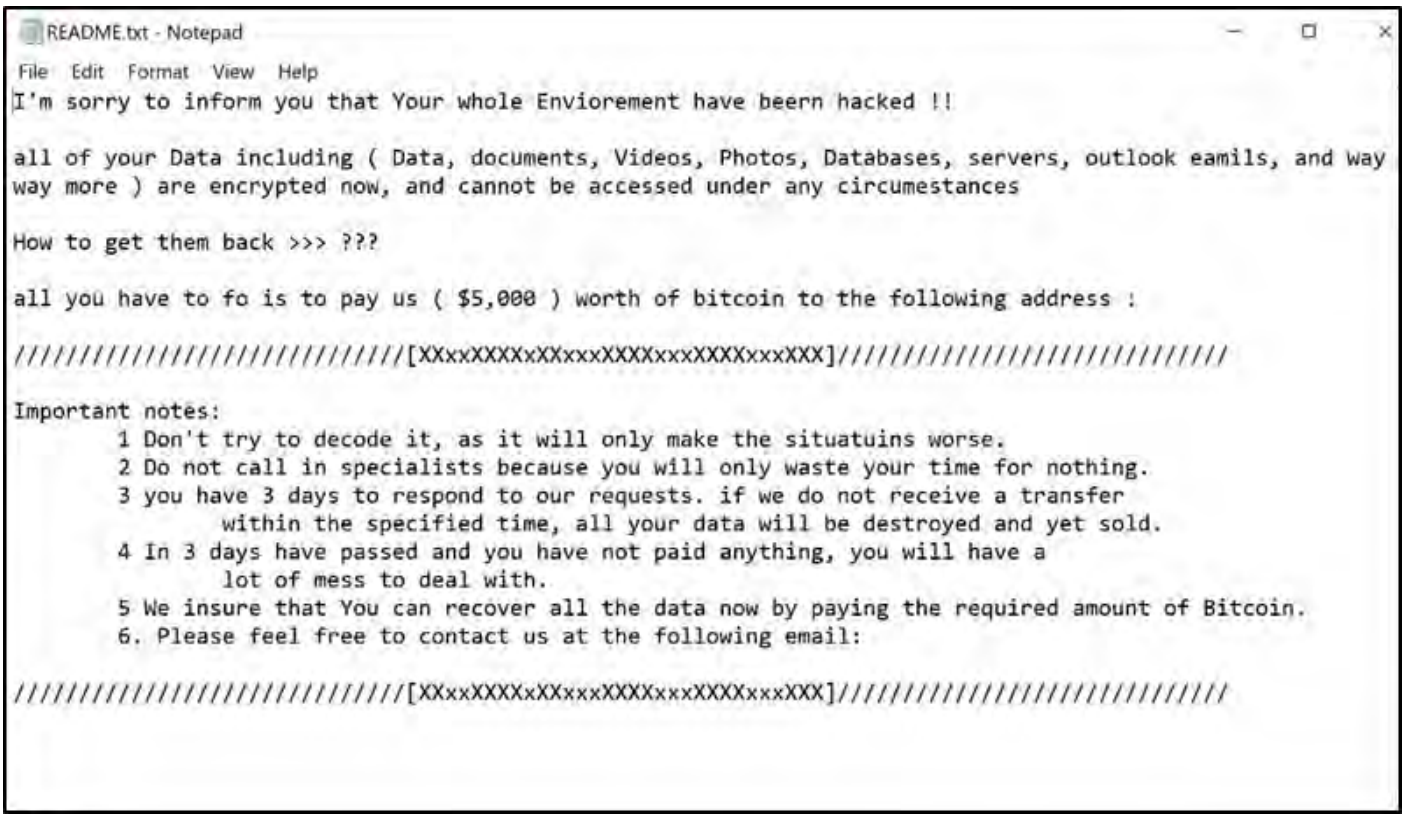
27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Cybercrime Prevention Flyer



Ransomware Message Text File Example

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 popups on websites and do not allow unsolicited downloads.
- **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.

Resources

Ransomware Guidance and Resources - Cybersecurity and Infrastructure Security Agency

Ransomware - FBI

A Guide to Ransomware – U.S. Secret Service

Ransomware: How to Prevent or Recover from an Attack - BackBlaze

Ransomware: Attacker's Top Choice for Cyber Extortion - FireEye

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF