THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

May 2022

Cyber Security Awareness Newsletter

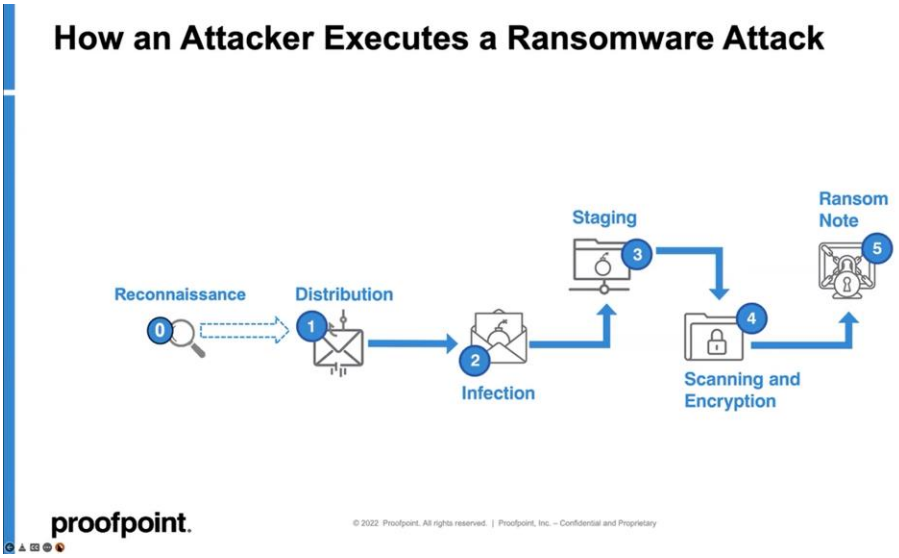
Protecting yourself and information from cyber security threats

Ransomware

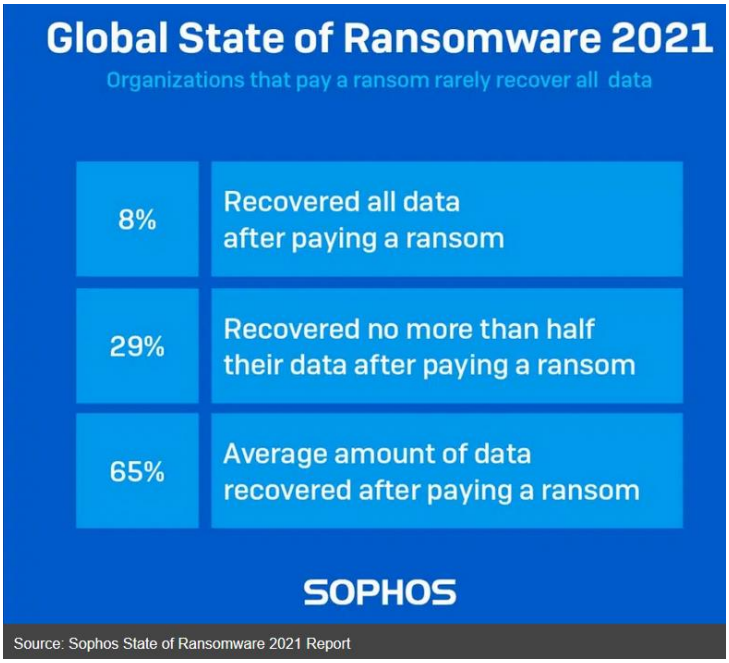
This month we wanted to focus on ransomware, due to the increase in its use this year.

So…. What is ransomware?

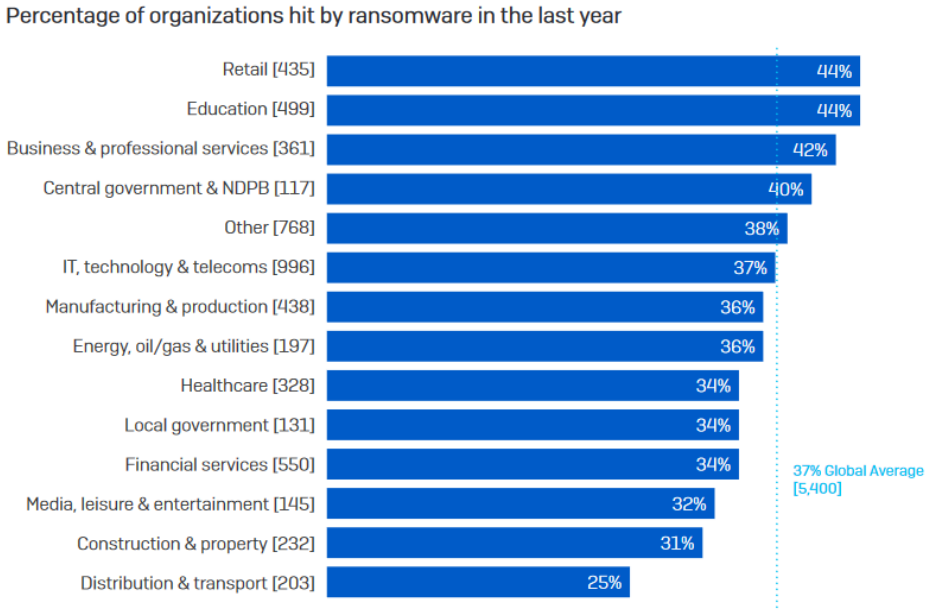
Crypto viral extortion, also known as "ransomware," was designed to hijack user files/systems and prevent a user from having access to them by encrypting them. Files and system can only be unencrypted by using a key that a malicious actor provides to the victim after demanding and receiving a digital currency fee.



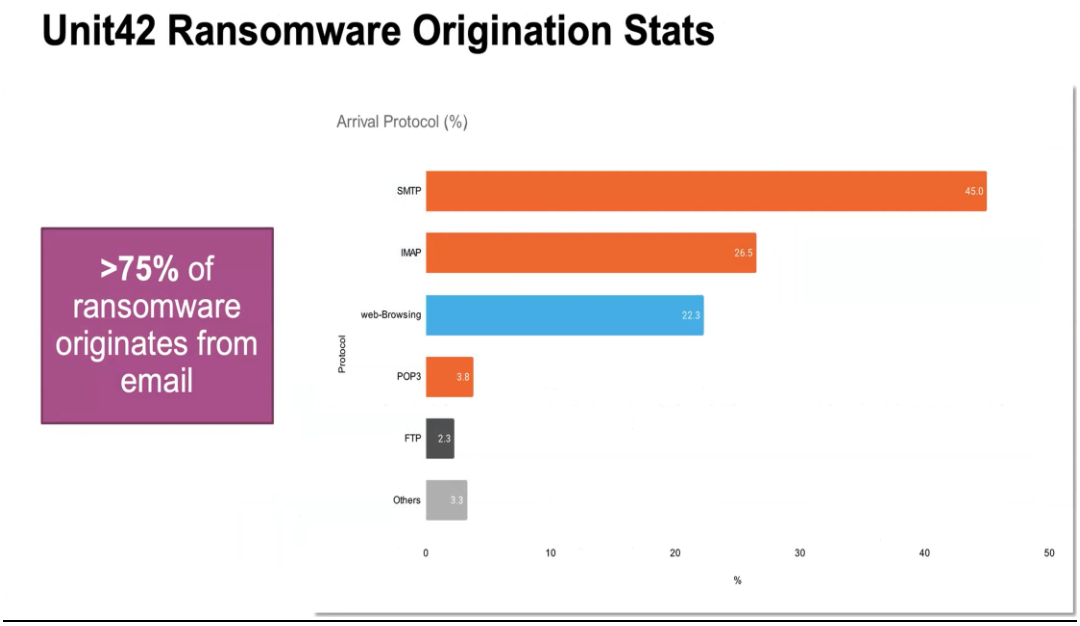
Unfortunately, a malicious actor may or may not release a key after payment, and even if a key is released, it might not work. Industry experts have also reported cases of data being exfiltrated (a copy of the data is made) before encryption occurs and used against the victim to extort more money, under the threat of publicly releasing the data if another payment is not made. Government agencies generally insist on never paying these ransoms, since doing so encourages and incentivizes a malicious actor to strike again.



Who have malicious actors been targeting? Everybody, and education is one of the top targets:



Where do most malicious attacks originate from? Mostly e-mail:



Ransomware Trends in 2022

Malicious actors have been taking sides in the Russia vs. Ukraine conflict, using the latest trends in attacks for ransomware. The type of attacks that are most prevalent now include:

- **Supply chain attacks.** Instead of attacking a single victim, supply chain attacks extended the blast radius. A prime example of a 2021 ransomware attack is the Kaseya attack, which affected at least 1,500 customers.

- **Double extortion.** As explained above, ransomware involves attackers encrypting information found on a system and then demanding a ransom in exchange for a decryption key. With double extortion, attackers also exfiltrate the data to a separate location. There, it can be used for other purposes, including leaking the information to a public website if a payment is not received.

- **Ransomware as a service (RaaS).** Gone are the days when every attacker had to write their own ransomware code and run a unique set of activities. RaaS is a pay-for-use malware, enabling attackers to use a platform that provides the necessary ransomware code and operational infrastructure to launch and maintain a ransomware campaign.

- **Attacking unpatched systems.** This was not a new trend for 2021, but it is one that continues to be an issue year after year. While there are ransomware attacks that do make use of novel zero-day vulnerabilities, most continue to abuse known vulnerabilities on unpatched systems.

- **Phishing.** While ransomware attacks can infect organizations in different ways, in 2021 some form of phishing email was more often than not a root cause.

- **TOAD. (**Telephone Oriented Attack Delivery) This method depends on calling a victim and having them follow instructions to click on a link to deliver malware onto the victim's system.

Ransomware Protections – Preventing and Defending

To protect against ransomware, the CyberSecurity and Infrastructure Security Agency (CISA) recommends the following actions:

1) Update your operating system and software. Updating your operating system keeps your system from being vulnerable to flaws in code that could have been fixed in the maintenance lifecycle of your operating system.
2) Implement user training and phishing exercises to raise awareness about the risk of suspicious links and attachments. We currently run user training and phishing attack exercises that are done every few months to raise awareness to these threats. E-mail is the #1 way malicious actors gain access to a system.
3) If you use Remote Desktop Protocol (RDP), secure, monitor it and use VPN. As you may or may not be aware the university has started locking RDP from sources outside the institution and ensured that systems that were visible on the public network had RDP removed or the system was move to an internal network. Use VPN to access resources internal to the institution.
4) Make an offline backup of your data. Making a backup of your system ensures you still have the data available in case of a need to recover. Although some cases of backups being tainted by malicious actors have been reported. Therefore, it is important to ensure that your backups are encrypted so that they can't be tampered with.

5) Use multifactor authentication (MFA). We encourage everyone to use Multifactor Authentication. The University even has MFA as a requirement to access some University resources. More information on MFA can be found here: https://its.uchicago.edu/2018/09/11/training-tip-cvpn/