THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

August 2023

Cyber Security Awareness Newsletter

Protecting yourself and information from cybersecurity threats.

Cybersecurity attacks are known to be a serious threat to any organization. It is well known that colleges and universities carry large amounts of sensitive data such as academic records, personal information, research findings, intellectual property, etc. which makes us an attractive target for cybercriminals. So, where do threats start? This month I want to go over the cyber criminal threat, some threat intelligence information that has been reported worldwide, and discuss that activity with what we have seen internally.

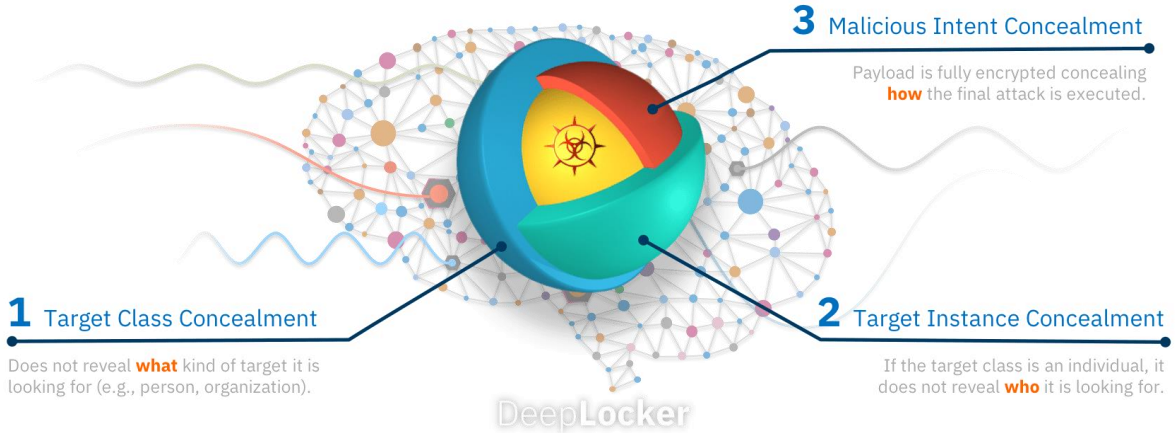
Cyberattack Example

Discovery –

Discussing the basics of any cyberattack: An attacker first starts with a discovery of assets. I've mentioned in a previous newsletter that: It must be worth the time to attack a target if they believe the payout is going to be worth the effort. Well… with the advent of AI, discovery has been made easier. Automating the reconnaissance of a target network and discovery of assets with vulnerable entry points can all be automated into a documented report for an attacker to review.

Evading -

AI has been learning to obfuscate the detection of malware to avoid detection by security tools. It is doing this by changing the code and/or behavior of malware dynamically. On the other side of the coin, detection tools are also using AI to combat evasive tactics. But let's say a compromise was successful, which can still happen.

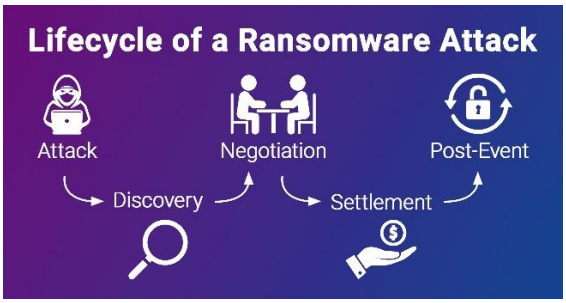


The Compromise -

Once a target has been compromised, attackers have been known to exfiltrate data (meaning they send compromised data to a location known to them) and encrypt the data that exists on the target system in preparation for requesting a ransom (assuming there is anything valuable found otherwise they may use other methods mentioned below). Weak encryption methods are no longer an option, so strong, more difficult to crack encryption methods are being used to ensure that data isn't recovered easily by a victim. Once that has been done, an attacker will sometimes communicate their compromise to the victim.

Communication of Ransomware -

The extortion aspect of ransomware can send anyone into a panic. Inciting a panic with an urge to pay a large amount of money is the ultimate goal of any ransomware. The United States government has always taken the stance to not pay a ransomware because there is no guarantee that your data will be returned to you in a viable state. But let's say that the ransom is paid, and you get your files back. The attacker probably has a copy of your data and might attempt to extort more money so that they don't release data to the public.



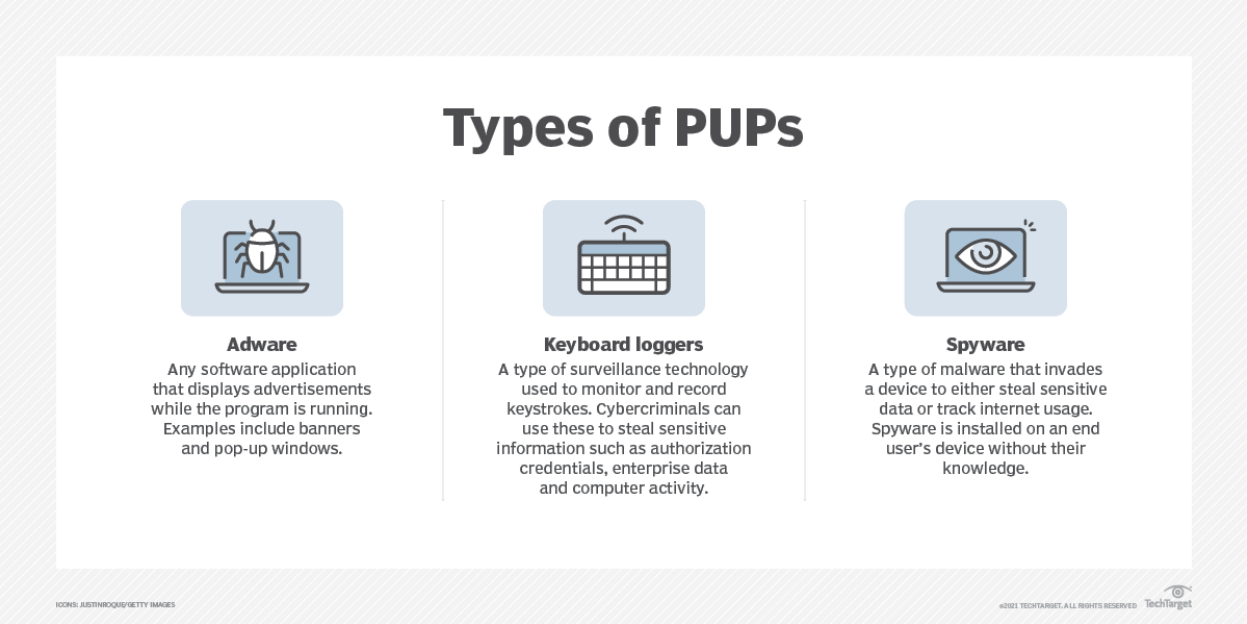
So now that you have seen an example compromise, what kind of scenarios are there in the industry where this plays out? A company called Splunk published a Global State of Security Report for 2023 stating percentages of respondents who reported incidents:

From this list, what have we seen on our end at the institution? System Compromise, Data Breach, Business Email Compromise, Ransomware Attack, Website impersonations, DDoS and account takeover/stolen credentials. So where do these kinds of items usually start? Most of the time, we observe many attempts to breach systems mainly through PUPs.

No, not like the picture above. **PUPs** is an acronym which stands for **potentially unwanted programs.**

But just like puppies there are several types of PUPS. They are sometimes introduced on purpose or by accident: Adware, Spyware, Browser Hijackers, and Rogue Software which can

slow down your computer, monitor your keystrokes, modify existing software on your computer, be very annoying and a potential security risk leading to any of the above incidents.



What tools do we use to combat PUPs before they become incidents?

Three of the tools that are widely used for our defenses are CrowdStrike, Malwarebytes and Windows Defender. CrowdStrike is a cloud-based platform that provides endpoint protection, threat intelligence, and incident response services. Malwarebytes, currently used on Macs, is a software-based solution that regularly scans and detects malware, ransomware, as well as other malicious programs and removes them from computers that may be lying dormant, waiting to attack. Windows Defender is a built-in antivirus program that comes with Windows 10 and 11. It provides real-time protection against malware, viruses, and other security threats. Together, these tools help our organization prevent, detect, and respond to cyberattacks in a timely and efficient manner.

As always, we welcome your feedback and any suggestions for topics that you would like us to cover in the next newsletter. Please send us an e-mail at security@bsd.uchicago.edu.