Common Cyber Threats

Instructor: The importance of cybersecurity can be described with one word: information. Social security numbers, credit card numbers, trade secrets, classified and national security information are examples of information that malicious actors seek for financial, political or personal gain.

Protecting data is critical and understanding threats that may compromise it can help shape security measures. Threat actors use code, scripts, or other applications to breach systems in an attempt to obtain restricted information. This malicious software, or malware, is designed to damage or disrupt a computer system.

Common ways systems become infected with malware include a file attached to an email, a fraudulent link to or within a website, external media like a USB thumb drive or DVD, or an unpatched system.

There are several types of malware, each with its own purpose: A virus is a self-replicating program requiring a host file and action from a user in order to spread. In contrast, a worm self-replicates without the use of a host file and doesn't

require action from a user to spread copies of itself further infecting files, exploiting operating system vulnerabilities, and potentially consuming bandwidth.

A Trojan horse is a malicious code that masquerades as a normal file to get past security monitoring apparatuses. When executed, the trojan file creates a system backdoor that a hacker can access and steal information or attempt further infiltration. Spyware, as the name implies can capture user activities like applications active on the monitor, things in view of a webcam, or record keyboard strokes.

Rootkits are a collection of software - a kit - that seeks elevated privileges - root access of a system in order to gain full system control. Rootkits can hide running processes and files, including additional instances of itself. Ransomware has wreaked havoc on businesses and home users alike in recent years. Ransomware gives an attacker leverage for extortion. Data on a device may be encrypted with the attacker demanding payment by a deadline in exchange of the decryption key.

A website may be taken over, defaced, or the owner otherwise locked out until the timely ransom is paid. Attackers may

delete or share the data as a consequence for not meeting the ransom. Botnets are another threat commonly born of malware. Botnets are a collection of compromised systems that are remotely controlled by command and control- C2 - systems. A C2 can coordinate and manipulate a botnet of hundreds to millions of infected hosts. An infected system may be an unwitting participant bot known as a zombie. Botnets are used to further spread malware or perform denial-of-service attacks where bots work together to overwhelm a system's resources and render it unresponsive to legitimate users.

A common vector for a system intrusion is via a backdoor. Backdoor is a covert method of gaining system access by bypassing security controls. A backdoor isn't necessarily malicious; software developers many times include them as a method to access the software for legitimate administration purposes. But these holes should be closed or patched before the software is deployed to production.

Unpatched systems and applications are vulnerable to being exploited. Keeping applications up to date is vital to security but still not a catch all.

Anti-virus and anti-malware applications can have the latest signatures and still not detect malicious code. A small change to malware's code or behavior can help it evade detection. Zero-day exploits are malware that is unknown to the security community and doesn't have a mitigation solution. Similarly, a software application that has a weakness discovered, but a patch isn't available to address it, is known as a zero-day vulnerability.

Humans play a central role in protecting against these threats. While the first line of defense, unfortunately users are also the weakest link. Humans are vulnerable to manipulation.

Social engineering, for instance, is an attack where intruders attempt to appeal to or outwit a victim using persuasive language or triggers to convince the user to perform an action. Year after year data breach reports highlight the effectiveness of social engineering, specifically phishing - targeting via email. Social engineering is commonly the root of an intrusion: a user is duped into clicking a link, opening a locked door, or providing credentials.

These deceptive tactics are so effective that psychological manipulation has advanced to

target large groups of users for a more far-reaching impact. Social media platforms have become the vehicle for the campaigns. Anyone can post almost any information desired, leaving the onus to users digesting the information to scrutinize and fact-check. Virtual internet communities can have tremendous influence on one's opinions and views. When information is intentionally false to deceive and shape beliefs, it is weaponized disinformation.

Deep fakes is another threat and form of weaponized psychology. This manipulation technique leverages artificial intelligence or machine learning technologies to create realistic-looking alterations of videos. Debunking a false claim is difficult when the user saw and heard a message with no inkling the media they viewed was altered for deception.

Effective defenses for these threats are user training and awareness. The most stringent security controls can be bypassed by a user action. Another important measure is keeping systems and applications updated. There are numerous commercial solutions for managing patches and updates across an enterprise. To significantly decrease the threat of a compromise, compress the time between

release and installation of patches and ensure users understand their role in the organization's security.

Notices