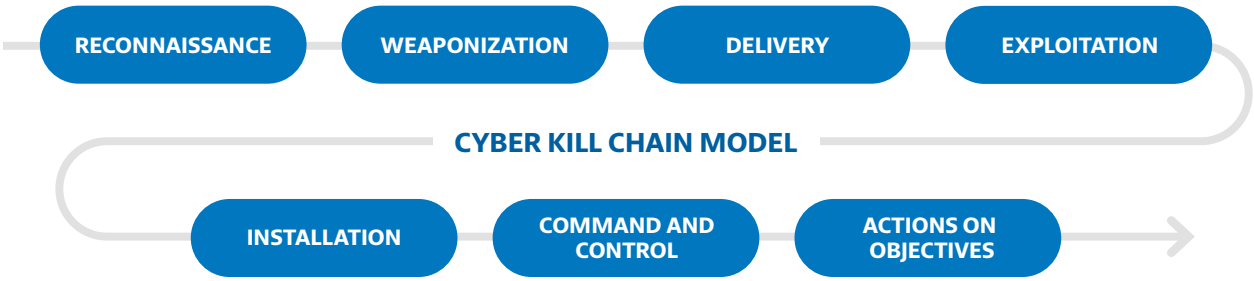
Insperity
HR that Makes a Difference™

Are you prepared to defend yourself against a ransomware attack?

Dr. Tim Proffitt, Managing director technology security

Ransomware is a type of malware (computer virus) that removes users' access to their data by means of forced encryption. Encryption is the method by which usable data is converted into unreadable data as a means of privacy. Encrypted data can be converted back into usable data by the owner with a known, private key. Access to the encrypted files returns only after making the payment (ransom) to the attacker. After the victims pay the ransom, the attacker provides the necessary decryption key and can even go so far as to assist in the decryption process. The ransom costs can range from a few hundred to a million dollars, depending on the situation. There is always a debate on the merits of paying or not paying the ransom to recover the files. Paying the ransom can be a crime and a company should consult with their legal advisors. Here are some tips to help you avoid the stress of an attack like this.



CYBER KILL CHAIN AND INSPERITY REMEDIATION

An organization's best defense against ransomware would be to use the Lockheed Martin Cyber Kill Chain (CKC) taxonomy model. Using this famous seven-step naming system, each defense can be described along with its strength. The Cyber Kill Chain model was developed to identify the order an attacker must follow to be able to to complete an attack against a victim.

RECONNAISSANCE PHASE

In this phase, the attacker collects as much information about the organization as possible. This information is vital for devising a powerful attack. Attackers will often search and pull any data they can find on your organization (such as key management team members, technology administrators, stakeholders and critical users who would have access to technology systems) from social media sites. Systems (computers and servers) that are directly connected to the internet are assessed for vulnerabilities and attackers will formulate a game plan to gain entry into those systems using this collected information.

Your defense against the Reconnaissance Phase

- Perform frequent vulnerability scans to understand known vulnerabilities and open communication channels. Vulnerability scanning can be conducted by your IT staff or by a third party.

- Use a firewall with specific inbound and outbound rules to minimize approved traffic. Open firewall rule will allow more conversations.
- Create social media guidelines to help minimize the amount of data found on sites like LinkedIn, Facebook and Twitter. This can help users understand the importance of keeping sensitive information about the company from being publicly posted.
- Perform routine penetration tests against your external systems and remediate any findings. Penetration testing assists in shrinking the known information technology risks to the organization. These tests are often conducted by third parties and should be executed when new technology is deployed or systems are deprecated.

WEAPONIZATION PHASE

Attackers will build a malicious payload (a file that may look benign, such as a PDF or Microsoft Office document, but will instead infect the computer) with the means of bypassing security controls that they learned during the Reconnaissance Phase. They will use a range of techniques to disguise the malware into a benign-looking payload. A more advanced attack will exploit a remote-access zero-day vulnerability to disable security controls and provide a privilege elevation in the target environment. The goal of the weaponized malware is to infect the technology asset and have the ability to talk back home to the attacker's infrastructure. The phone home feature is desirable for the attackers to execute the entire attack.

Your defense against the Weaponization Phase

- Use vulnerability management, which is key in identifying known attacks against endpoints (personal computers or servers) and should be used to close those gaps in your systems.
- Make weaponization difficult for attackers by making your security controls hard to overcome. Following strong security guidance like the CIS 20 critical controls is a great start.
- Be consistent with patch management to close known technical risks. Monthly patching of all technology systems is a great way to reduce the attack vector in weaponization.

DELIVERY PHASE

In the Delivery Phase, attackers are figuring out the best way to sneak their malware into the hands of an organization's userbase. This can often be through malicious email attachments or USB flash drives. For example, a user will receive a legitimate-looking email (i.e. from a vendor or billing company), which contains a URL to a website that hosts an attacker's malicious payload. Because the user recognizes this sender, the user will click the link and download the malicious payload without thinking twice.

Your defense against the Delivery Phase

- Deploy endpoint detection and response (EDR) technologies to combat malware. This includes running products like Symantec, McAfee, Palo Alto Cortex, Microsoft Defender and Sophos AV.
- Ensure you have a properly configured firewalls to block many attacks from malware attack sources. Executables (programs or applications that can run on the computer) should not be permitted to cross a firewall.
- Block known malware domains with a web filter.
- Having files that come into the organization be detonated in a sandbox (an isolated, protected environment that can be used to test programs without the risk of impacting other parts of the computer) will identify malicious payloads. Microsoft ATP, Forcepoint, Joe Sandbox, Malwarebytes, and others are designed to solve this.
- Set up email filtering techniques to block known phishing and malware domains. Links and attachments should be vetted and removed from any email that is found risky.
- Train users in phishing techniques so they know how to avoid them. Phishing emails should be deleted by users and reported to the email administrator.

EXPLOITATION PHASE

The attacker's payload downloads the ransomware (Delivery Phase), launches the virus and scans the victim's machine for possible vulnerabilities. An unpatched operating system or a vulnerable application can be exploited to achieve the required

privilege (admin) to run the ransomware. The malicious payload exploits the vulnerability on the target environment and executes. This step provides the attacker with the minimum required access to the target environment.

Your defense against the Exploitation Phase

- Deploy intrusion prevention sensors and/or next-generation firewall appliances to block and alarm on known ransomware exploits.
- Employees should not be administrators of their computers. Administrator rights should be a second user account that is used only when needed to install software or to conduct configuration changes. Users that must retain administrative rights should have additional controls installed for monitoring these activities in case these computers are compromised.

INSTALLATION PHASE

In this phase, the malicious software will install itself on the computer and reach out to other systems to infect those as well. The attack will replicate through the entire technology environment. This generally involves propagating the malware throughout the network and installing additional remote administration tools. These malicious administrative backdoors are used to persist in the infrastructure even when systems reset. The ransomware will often delete a user's local backup files, such as the Windows Shadow Volume.

Your defense against the Installation Phase

- Deploy endpoint detection and response (EDR) technologies to combat the installation of malware. This includes running products like Symantec, McAfee, Palo Alto Cortex, Microsoft Defender and Sophos AV.
- Ensure users don't have administrative rights. Accounts with administrative privileges should be minimal. By default, most Microsoft operating system users are administrative by default. Organizations should undertake a project to remove these rights and have users run the systems as users. If the malware cannot install because it does not have the proper rights, it has been prevented.
- Configure computers according to a security standard. There are several MS websites and Apple websites dedicated to listing the setting needed to "harden" an operating system to attack.
- Ensure computers are sending their logs to a centralized location for review. Log review with an event manager can quickly identify when an attack is underway. Early identification of an attack will greatly reduce the damage to the organization. Security event management (SEM) can come in many shapes and sizes, with some free and others under a commercial license. Organizations should pick the appropriate SEM and allocate time to review security logs. Splunk, Alienvault, Elastic, McAfee, RSA NetWitness, LogRhythm, Exabeam and Mandiant all have products.
- Patch management should be utilized to keep the number of vulnerabilities under control. Critical and high-risk vulnerabilities should be patched with urgency.

COMMAND AND CONTROL PHASE

After being installed on a technology asset, it is time for attackers to act in the environment by setting up a remote command and control (C&C). The C&C channel will be used to deliver attackers' commands to the malware and/or exfiltrate data from the target environment.

Your defense in the C&C phase

- Configure a firewall to block known C&C channels and alarm on this activity.
- Create a barrier to C&C conversations with local firewall rules from the hardening process (configuring the system so that it is more difficult to attack).
- Endpoints should log to the centralized SEM for C&C alerting and response from administrators.
- More mature organizations can deploy additional tools such as cloud access security brokers (CASB), user behavioral analytics (UBA), and process monitors to better identify when command and control activities are occurring in the environment.

ACTIONS ON OBJECTIVES PHASE

Once there has been a successful C&C establishment, the malware will perform the desired action. The attack may have varying objectives, but in this example, exfiltrating or extracting private information and encrypting files is the most common result. Once the files are encrypted by the attackers, this data will be unusable until the victim obtains the private key that encrypted the data.

Your defense against the Actions on Objectives Phase

- Process monitoring can watch for the appearance of ransomware and will be used to place infected machines into an isolated state. Tools like Microsoft process monitor, Carbon Black, Tripwire, PaloAlto XDR and Nagios will meet this need.
- EDR technologies can block and identify actions.
- User behavior analytics (UBA) technologies can alert the propagation of the infection between machines.
- Backups are used as a last resort to obtain unencrypted data. Backups should be created on a daily (or more frequent) basis and be stored offline or in a segmented area on the network that is tightly controlled.

In summary, there is an in-depth defense strategy that an organization can use at each level of the kill chain to reduce the threats from ransomware. In some cases, the mitigation will happen in the delivery phase. Other attacks may be blocked at the action on objectives phase. Regardless of where the attack is mitigated, the defense worked, and the ransomware attack was stopped.

REFERENCES

https://www.cisa.gov/ransomware

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

https://www.cisecurity.org/controls/cis-controls-list/

https://www.comparitech.com/net-admin/process-monitoring-tools/

https://www.paloaltonetworks.com/cortex/cortex-xdr

https://link.springer.com/article/10.1007/s11416-019-00338-7