Ransomware Considerations

Ransomware: Malicious software (malware) designed to encrypt local and network-based files and demand a ransom for decryption. Payment of the ransom is frequently requested in bitcoins (a relatively untraceable currency) via anonymous internet sites.

Online cyber-criminals and other nefarious attackers are constantly looking for new ways to access users' systems and then monetize this access. Common methods of breaking into systems are through interactions with a user, often with email attachments (phishing) or internet browsing (drive-bys). Once criminals have access, they can perform any number of activities.

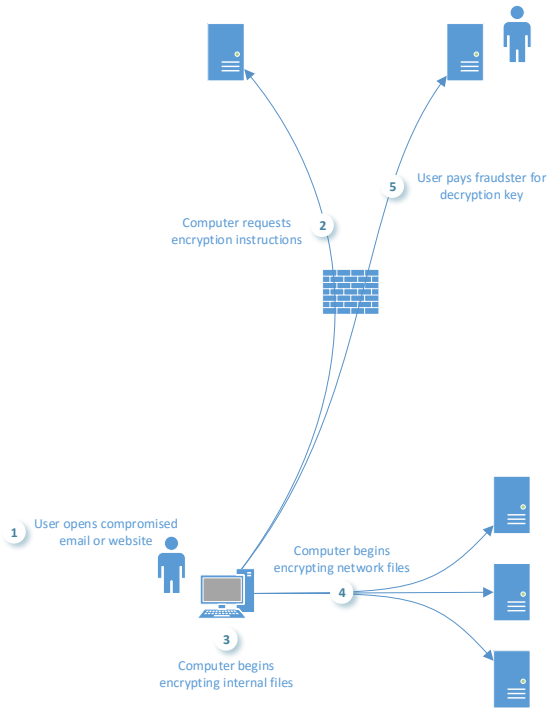
One of the more popular attacks by cyber-criminals is called a "ransomware" or "encrypting malware" attack, where the fraudster infects a computer with malicious software designed to encrypt user files and hold them hostage until payment of a ransom. From a criminal perspective, this is a relatively safe means of making money:

- the victim is 'happy' to pay for the return of their files
- there is little perceived harm if the files are returned
- the amount of money charged is frequently less than the cost to respond otherwise

However, these attacks can significantly damage operations, destroy critical systems and irreversibly corrupt data. In order to better prevent or respond to an attack, it is important to understand the basics behind an attack and the functionality of the malware.

Attack Methodology

An attack starts with a user accidentally executing a small file from an email or website that starts the infection and encryption process. These malicious files are resistant to detection by anti-virus because they change signatures rapidly and use common Windows® commands in their attacks.



Once the file is downloaded and executed on the system, it connects to the internet in order to get some needed components and then begins to encrypt files on the local computer and on network shares accessible from that computer. Files initially targeted for encryption are often the anti-virus definition files and similar preventative applications, which then prevents the system from defending itself against the malware.

After the files are encrypted, users are notified of the event and provided some means of contacting the attacker and getting the key, or 'decrypter'. While some older ransomware attacks used reversible encryption routines or left a trail on the system that could be used to decrypt the files, attackers have generally learned from their 'mistakes' and developed new ways of preventing any type of reverse engineering or unlocking.

Preparation & Response

When preparing for or responding to an attack, there are a number of important considerations that may lessen the likelihood or impact of an encrypting malware attack. There are different degrees of preparation and different techniques.

Preventative steps can prevent the attack in its entirety (e.g., removing mail and internet access), lessen the spread of the attack (e.g., limited access and connections between systems), warn of an ongoing attack (e.g., endpoint sensors) and blunt the effect of the attack (e.g., backups that can be restored).

Responsive steps can assist in controlling the damage and prevent subsequent re-infections or other collateral impact.

Before

1. Check Backups
2. Minimize access to network shares
3. Implement mail filters and web proxies
4. Use process monitoring and application whitelisting tools to supplement antivirus

After

1. Suspend backups to avoid overwriting good data
2. Stop network shares to prevent spread
3. Review logs to identify culprit

Preparation

There *are* effective ways to prevent, or at least significantly mitigate the risks from, encrypting malware attacks. Antivirus may have little effect at stopping the malware because the rapidly changing signatures and malicious tools tare difficult or impossible to distinguish from legitimate tools. While AV is still a necessary tool, better defenses include:

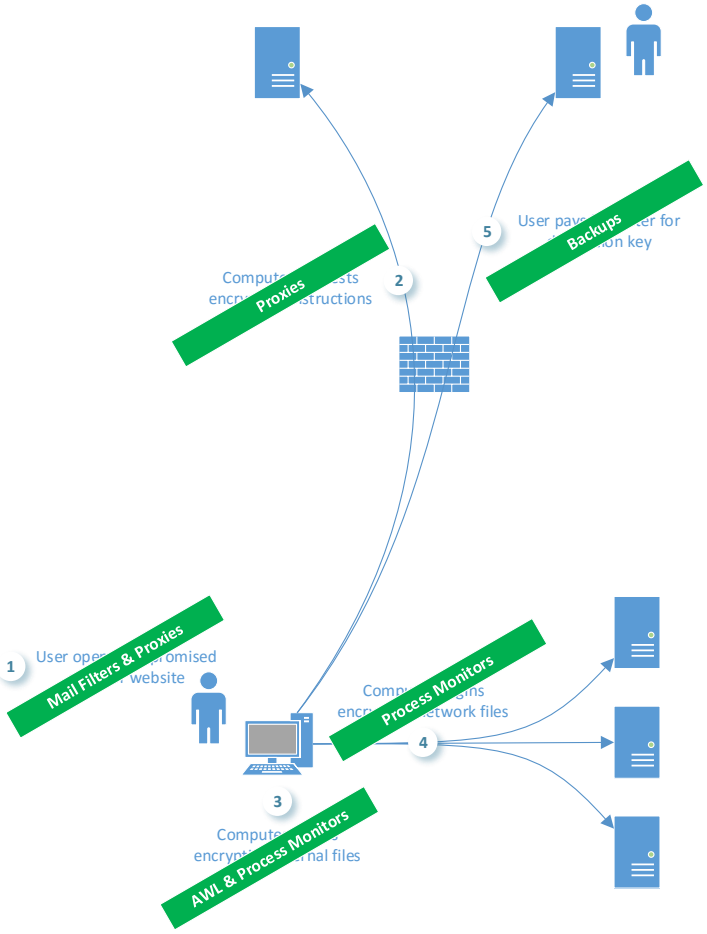
- *Proxies* (e.g., ZScaler, Websense) that monitor user connections to the internet and only allow connections to sites that are known good or have acceptable levels of risk. This can help prevent the initial malware download and can also disrupt the connectivity between the computer and the internet sites that have encryption instructions.
- *Incoming mail filters (e.g., Proofpoint)* that scan mail and attachments prior to arrival to remove high-threat attachments and identified phishing messages. This can help prevent infected messages from reaching the end-user.
- *Application white-listing* solutions (e.g., Bit9, McAfee FIM) that prevent programs from executing unless they are on a pre-defined list. This prevents the malware from running
- *Process monitoring* tools (e.g., CarbonBlack, Cylance) watch for suspicious applications and generate warnings when unexpected events occur.

Before an attack occurs, it is critical to have tested and verified backups of critical systems. This will blunt the attacker's strategic position in that files can be recovered with little data loss. Time can also be well-spent before an attack by reducing the number of mapped drives available to 'everyone', and limiting mappings and permissions to only the smallest population possible. If an infected computer and associated user does not have access to a network share or file, then the contents won't be maliciously encrypted. Network files are frequently over-shared to people that do not have a job requirement for access, which needlessly increases the exposure and risk of files being encrypted during an attack. For each of the steps in the attack process, there is an opportunity for successful defense, highlighted in the diagram below.

Response

Once an attack has begun, there are certain steps that can reduce the impact and assist in the remediation process. A summary of potential response steps includes

- Shut down shared connections to prevent continuing encryption
- Suspend backup jobs to prevent replacing clean files with encrypted copies that will not restore
- Identify endpoints running suspicious files:
    - Review network connections made to affected shares to identify endpoints
    - Deploy process-monitoring tools to endpoints to detect suspicious files and processes
- Review firewall log and endpoint activity to ensure no simultaneous attacker activity is occurring, as encrypting malware attacks are sometimes used as diversions



(1) Containing the malware, (2) identifying the infected system(s) and (3) suspending backups should be the response priority. Since the malware works by reaching out over the network to connected computers and shares, initial containment can be done by removing network shares and disconnecting mapped drives. While containing and identifying the affected systems, stopping backup processes is necessary to prevent backing up the encrypted files and overwriting older, unencrypted data. Since malware signatures may not be effective, other endpoint tools must be used to detect the malicious files and infected system(s). Sometimes, log files on file servers that were encrypted can be reviewed to look for indicators of systems connecting to large numbers of shares or files simultaneously. Systems

that have encrypted files in the root and system folders (e.g., c:\, c:\windows) are usually indicative of systems that are running the encrypting malware, since these folders are not otherwise available via the network. If the encryption process has completed, it is not uncommon for the malware to remove itself. If this is the case, it may be difficult or impossible to find the initial compromised systems unless sufficient logging and analysis solutions are in place prior to the attack.

Once infected systems have been identified, network shares can be brought back online and backups restored. If a ransom has been paid and decrypter provided, care should be taken that attackers do not introduce different malware or backdoors into the system through the decrypter. Additionally, system and access logs should be reviewed for any indictor that the attack was not a diversion from a more insidious attack.

Specific Action Items[1]

Identify Infected Machine via Log Analysis or Endpoint Agent Analysis

1. Create a list of servers with encrypted files. On these servers, check Security Event Logs (security.evtx) for users and machines that have connected to the shares with encrypted files.
2. If a process-tracking agent (e.g., CarbonBlack®) is installed, check for endpoints with large numbers of network connections (e.g., NetConn > 5000). This is indicative of the malware reaching out to various network locations and changing files. There are false-positives due to backup and antivirus jobs, but these should be easily filtered out by associated process.
3. Start reviewing machines identified in (1) for evidence of malware. Remember that antivirus may not detect the malware, but tools such as pslist[2] may show suspicious running files. Infected machines will also likely have encrypted files in local directories (e.g., c:\users\...) whereas machines reached over a network connection will only have shared directories encrypted.

Contain the Encryption Process until Endpoint is Identified

1. Forcibly disconnect file shares on the file server(s) to stop any currently connected devices.
2. Check share permissions *as well as* folder permissions and limit permissions to *specifically necessary* users (*not* groups). This will limit the potential impact/reach of an infected device.

Prevent Reoccurrences

1. Review Mail Filter settings to specifically block Office files with embedded macros and scripts.
2. Review Web Proxy settings to block known and suspicious malicious sites by reputation, and ensure all user browser activity runs through the proxy.
3. Configure watchlists in process monitoring tools to watch for (a) large number of network connections and (b) executables running from Temporary Internet and Outlook folders.

[1] Each case is different, and some of these may or may not apply.
[2] https://technet.microsoft.com/en-us/sysinternals/pslist