California Community Colleges | Information Security Center

WHITE PAPER: Ransomware Defense & Response

A Guide for California Community Colleges | October 2020

Table of Contents

What is Ransomware?

Ransomware is a type of malware that infects a computer or system and encrypts its data until a ransom is paid to the attacker. After encryption, an on-screen alert is displayed to the affected system(s). This contains a message demanding a specific amount of payment — generally in bitcoin — to decrypt the user's files. In theory, decryption keys are intended to be provided to the victim once they have paid the ransom. In many cases, however, the victim may not receive the decryption keys even if they have paid the ransom to the threat actors.

What is the Financial Impact of Ransomware?

In Q2 2020, the number of ransomware attacks decreased while the average payment increased. According to Covware, the average ransom payment is $178,254.

How Does a Computer System Become Infected?

Attackers often install ransomware onto a system through a phishing email. This email either contains a malicious attachment or a hyperlink that redirects a user to an infected website, where the malware is installed onto the user's system without their knowledge.

Phishing emails intended for a ransomware attack usually contain an attached Microsoft Office document containing a malicious macro. When the user opens the file, the malicious macro is enabled. The macro then runs a script which downloads the malware's executable file. The file is installed on the victim's computer, scans for files on the system, and eventually encrypts them.

Ransomware installed through malware from a malicious website is commonly referred to as "drive-by malware." The infected websites, known as "watering holes," are designed to attract as much traffic as possible.

On a lower level, ransomware has two ways of propagating through a system once it is installed:

1. **Manual propagation**
   This requires the threat actor having access to your environment with administrator-level privileges. Once this is achieved, they will perform the following:
   - Run file encryptor scripts on your systems.
   - These are commonly deployed using Windows batch files (.bat), Microsoft Group Policy Objects (GPO's), and/or vulnerable software on the victim's system.

2. **Automated propagation**
   - Certification or Windows token extraction from filesystem or RAM.
   - Utilizing Windows frameworks, for example, Windows Management Instrumentation (WMI), SMB, or PsExec to tie to execute payloads.
   - Unpatched vulnerabilities leading to exploitation (e.g., EternalBlue, which can be patched with the Microsoft Security Bulletin MS17-010 security update).

An Example Command Run by WannaCry

WannaCry was a 2017 worldwide ransomware attack that targeted computer systems running the Microsoft Windows operating system. It spread using EternalBlue, an exploit for older Windows systems. Although a patch for this exploit was readily available, many systems had not applied the patch.

To illustrate how systems became infected, let us look at a command that was used to execute WannaCry on a given computer system. The command is: **"cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet"**.

In order to join several sequences of commands in a single shot from the command line, separate command lines are connected using the "&" character. In the above example, we have five command lines launched at one time.

Let us enumerate these to better understand the ransomware actions:

1. **cmd.exe /c vssadmin delete shadows /all /quiet**
   Cmd.exe is the Windows command line interface which, when used with the "/c" clause, instructs to carry out the command specified by the string and then terminates.

   Vssadmin2 is the command line used to administer Microsoft Windows shadow copy volumes. In this command line, the system is ordered to delete all volumes (delete shadows / all), and in a silent way (/quiet).

2. **wmic shadowcopy delete**
   The wmic command is used to manipulate WMI3 information within an interactive command shell. Here, the WMI is instructed to delete the shadow copy volume.

3. **bcdedit /set {default} bootstatuspolicy ignoreallfailures**
   BCDEdit is a command-line tool for managing Boot Configuration Data (BCD). BCDEdit used with the "/set" clause is used to configure specific boot entry elements, such as kernel debugger settings, memory options, or options that enable test-signed kernel-mode code or load alternate hardware abstraction layer (HAL) and kernel files.

   The statement "{default} bootstatuspolicy ignoreallfailures" is used to disable Windows Error Recovery on startup.

4. **bcdedit /set {default} recoveryenabled no**
   Utilizing the same BCDEdit command-line tool, this instruction prevents the attached asset from attempting to repair the reboot.

5. **wbadmin delete catalog -quiet**
   WBadmin is a command line oriented to backup and restore Windows operating systems, volumes, files, folders, and applications. This command line (wbadmin delete catalog) deletes the backup catalog stored on the local machine in a silent way (-quiet).

Tips for Preventing a Ransomware Attack

1. **Avoid getting phished.**
   Deploy email spam filters and educate end-users on good cyber hygiene practices. Employees should be trained to identify phishing emails and avoid downloading attachments if the source seems untrustworthy. They should also be able to identify fake web pages.

   Be wary if you receive phone calls asking for company information. It may be a criminal using the technique of social engineering to prepare for a future attack.

2. **Avoid the use of macros in Microsoft Office documents.**
   Macros are commands and instructions to help automate tasks involving Microsoft Office. If your organization does not require the use of Macros in your workflows, Office 365 admins should disable and block them from running.
   - Intel Insight: How to Disable Macros

3. **Backup important assets often.**
   Backups of critical assets should be done regularly. It is recommended to store backups "offsite," preferably in the cloud as on-premise backups can become infected as well.

4. **Enforce a strong password policy and require two-factor authentication for login.**
   This should be done for Windows Active Directory accounts as well as other services.

5. **Consistently monitor network traffic.**
   Discovering unusual traffic on your networks can lead to the early detection of ransomware.

6. **Regularly patch software and systems.**
   The latest software updates are generally used to address known security vulnerabilities.

Remote Desktop Protocol Best Practices

Insecure Remote Desktop Protocol (RDP) services are a common means to install ransomware onto an organization's assets (e.g., Dharma, Phobos, etc.). Colleges are considered small/medium sized businesses that are at larger risk for RDP-based attacks, according to the Covware Q2 2020 Ransomware Report.

Following are recommended practices to avoid RDP-based attacks:

1. **Enforce a strong Windows Active Directory password policy.**
   This will make cracking hashes of passwords difficult and should prevent direct access to campus resources should an attacker gain access to your network.
   - Password must meet complexity requirements (Windows 10) — Windows security

2. **Restrict RDP access through campus networks only.**
   Access to campus services (i.e., Windows machines) should only be enabled within the campus networks. Outside access can be allowed through a VPN.

3. **Require two-factor authentication to access campus services.**
   This should be configured when giving VPN access to students and faculty.

Remote Desktop Gateways can be configured to integrate with the campus instance of Duo Authentication.

- Two-Factor Authentication on VPN Connection
- Two-Factor Authentication for Microsoft RD Gateway on Windows 2012 and Later

4. **Only provide Windows RDP access to users who require it.**
   All Windows Active Directory Administrators can log in via Remote Desktop under default configuration. Remote access for administrator accounts should be limited to only those who require it.

   If Remote Desktop is not necessary for system administration, you should remove all admin-level access through RDP, and restrict it to user accounts only.

5. **Enable Network Level Authentication (NLA).**
   NLA requires an end-user to authenticate themselves before establishing a session with the server hosting RDP services.

6. **Change the listening port from 3389.**
   Attackers often scan networks for devices listening on the default Remote Desktop TCP port 3389. Although this approach is helpful, this is considered "security by obscurity," which is not the most reliable security approach. You should ensure that you are also using other methods to tighten down access as described in this article:
   - Change the listening port in Remote Desktop

What to Do After Infection?

After an asset has been infected, a typical response is to shut it down for fear of spreading the infection. **This is not recommended.**

The correct action is to isolate the asset from the network and keep the asset turned on so that it is possible to "dump" the RAM memory to analyze. If there is a chance of reaching cryptographic keys, the opportunity is to look for information in RAM memory.

Typically, in a device with RAM capture software, such as FTK Imager portable, the Lite version is used. The ransomware will try to encrypt the data also on the external device where the capture software resides. Being that FTK Imager is a compact software, we can load it into memory and monitor the files that the ransomware tries to create on the external device, excluding each one as the ransomware tries to create it. This slows down the encryption process on the external device, enough to dump the RAM.

Summary

Ransomware attacks can be highly disruptive and costly to an organization. Infection can be avoided — or its impacts minimized — using proper security practices. As a general rule of thumb:

- Avoid opening links or other types of files from suspicious emails.
- Be wary if you receive phone calls asking for company or organizational information. It may be a criminal using the technique of social engineering preparing for a future attack.
- Avoid using ports for remote access, such as 3389, among others. These have been the main vectors of ransomware infection. Consider the use of VPN for this need.
- If you or your organization are the victim of a ransomware attack, never turn off the affected asset without first doing a complete RAM memory dump.

For more information on the contents of this guide, please contact:

Omer Usmani
Security Analyst
Information Security Center
California Community Colleges Technology Center
ousmani@ccctechcenter.org

About the Information Security Center

The CCC Information Security Center offers an extensive array of services and resources to help colleges maintain the integrity of information systems, and more effectively enforce regulatory and district security policies.

We are funded under the Shared Infrastructure Program grant by the CCC Chancellor's Office in order to provide these services free of charge to every California community college.

Visit the Information Security Center to learn more.