Ransomware

Aamir Khan, CISSP, CISA, OCP, MCDBA, PMP, CHP, MBA, PHD
Chief Information Security Officer
California Community Colleges Technology Center
California Community Colleges Security Center
Why 2020 was a turning point for Cybersecurity

- As internet usage increased throughout the course of the global pandemic, cyber attacks against government organizations and infrastructure increased as well.

- More data and more data is collected everyday, policies to protect this data is more urgent than ever.

- Successful organizations need to create a strong culture of cyber hygiene.
Outlook

- 68 percent of business leaders are concerned about the cybersecurity risks their organization faces (Accenture Security)

- For chief auditors and corporate boards, data governance and cyber risks are now the top concern (Gartner)

- In 2020, a unique event took place. This was world’s largest Cyber Security Exercises. The theme was digital pandemic and how to prevent “Digital Pandemic” from all events.
The Experience of a Ransomware Attack

- Ransomware attack on last year
- Two different threat actors (from Romania IP’s)
- Files encrypted 3 different ways (Dharma variant)
- Servers (including email, web and emergency notification system)
- Backups
- Individual computer workstations
Recovery

• COD has cyber security insurance and rep helped to setup response team within hours (forensics team and legal counsel)
• Included negotiating for ransom with two threat actors (decryption tools do not work 100%)
• All servers older than 2012 were replaced/updated
• All servers were patched to current levels
• Restricted firewall traffic to US only (gradually opened up with additional monitoring/logging)
• Replaced rdp strategy with VPN over RDP (2-factor authentication)
• Installed EDR on all production servers and individual computers (using Sentinel One from Kivu); includes 24/7 real time monitoring
• Worked with CCC Tech Center to enable tenable security scanner
What is Ransomware?

- Category of malware that encrypts data on a computer or system until a ransom is paid to the attacker.

- A specific amount of payment is requested by the attacker or threat actor(s) to decrypt the victim's files.
  - Generally in Bitcoin
  - Decryption keys are provided to the victim to decrypt files

- In many cases, the victim does not receive the decryption keys after having paid the ransom to the threat actors.
Top industries for ransomware detections (May 2020, Trend Micro)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>1,870</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1,599</td>
</tr>
<tr>
<td>Healthcare</td>
<td>1,217</td>
</tr>
<tr>
<td>Financial</td>
<td>488</td>
</tr>
<tr>
<td>Oil and Gas</td>
<td>422</td>
</tr>
<tr>
<td>Technology</td>
<td>348</td>
</tr>
<tr>
<td>Insurance</td>
<td>272</td>
</tr>
<tr>
<td>Education</td>
<td>213</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>146</td>
</tr>
<tr>
<td>Energy</td>
<td>141</td>
</tr>
</tbody>
</table>
Financial Impact

- In 2020, average ransomware payment was up $200,000, compared to $100,000 in 2019

Ransomware is expected to attack a business every 11 seconds by the end of 2021 - Steve Morgan, Cybercrime Magazine
How does Ransomware target an organization?

- Often originates from a phishing email
  - Either has malicious document attached, or redirects end user to malicious website.

- Once installed:
  1) Manual Propagation
  2) Automated Propagation
Ransomware Workflow

**Malicious Software Download**
Infection originates from a phishing email, malware embedded on compromised web pages (watering-hole), or a compromised supply chain.

**Attack is Armed**
Depending on BIOS type, Malware replaces system files. Master Boot Record, or UEFI firmware is bypassed. More exploits are installed in the background.

**Infection Spreads**
Malware begins scans of internal networks for other points of ingress, steal credentials, and creates more vectors for lateral movement across the network.

**Malware Attacks**
Malware deploys final attack payload across the network. Payload will destroy files from the network leaving only encrypted copies and infected programs that perpetually reactive payload.

**Attack Success**
Files on infected systems are encrypted with AES or other encryption and victims are asked for ransom payment (usually bitcoin). After the payment is made, encryption keys are to be provided by the threat actor.

**Credential Theft**
Multi-Pronged Attacks
Files Encrypted
Attack Vectors

- Small and medium sized companies are becoming a common target for attacks utilizing RDP as an entry point.

- Large organizations are more likely to be targets for phishing as opposed to RDP.

RDP and VPN use skyrocketed since coronavirus onset

RDP use is up by 41%, enterprise VPN use is up by 33%.
## Ransomware Types

<table>
<thead>
<tr>
<th>Rank</th>
<th>Ransomware Type</th>
<th>Market Share %</th>
<th>Change in Ranking from Q1 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sodinokibi</td>
<td>15.4%</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Maze</td>
<td>7.7%</td>
<td>+7</td>
</tr>
<tr>
<td>2</td>
<td>Phobos</td>
<td>7.7%</td>
<td>+1</td>
</tr>
<tr>
<td>4</td>
<td>Netwalker</td>
<td>7.1%</td>
<td>+6</td>
</tr>
<tr>
<td>5</td>
<td>Dharma</td>
<td>6.4%</td>
<td>-2</td>
</tr>
<tr>
<td>6</td>
<td>Ryuk</td>
<td>5.1%</td>
<td>-4</td>
</tr>
<tr>
<td>7</td>
<td>Mamba</td>
<td>4.5%</td>
<td>-2</td>
</tr>
<tr>
<td>8</td>
<td>Snatch</td>
<td>4.2%</td>
<td>-1</td>
</tr>
<tr>
<td>9</td>
<td>Lockbit</td>
<td>4.2%</td>
<td>+4</td>
</tr>
<tr>
<td>10</td>
<td>DeathHiddenTear</td>
<td>3.9%</td>
<td>+4</td>
</tr>
</tbody>
</table>
Sodinokibi

Background:
Sodinikibi is authored by the creators of the GrandCrab ransomware, which was retired as of the summer of 2019.

Attack Vectors:
- Phishing email or website containing link to zip file. The file contains malicious JavaScript code.
- Initial access involves exploit of an Oracle WebLogic vulnerability (CVE-2019-2725)
  - Script executing exploit verifies if patch KB4457138 is installed
  - Script will not proceed if patch is found
  - Will run 32 or 64 bit shellcode depending on detected system architecture

Signs of Compromise:
- The infected system will have a ransom note appear on the desktop, opened in notepad.
- Desktop wallpaper changed (blue background)
- Targeted File Types:
  - .jpg, .jpeg, .raw, .tif, .png, .bmp, .3dm, .max, .accdb, .db, .mdb, .dwg, .dx, .cpp, .cs, .h, .php, .asp, .rb, .java, .aaf, .aep, .aepx, .plb, .prel, .aet, .ppj, .gif, and .psd.
Sodinokibi - Ransom Note
Sodinokibi - Encrypted Files
Sodinokibi - Sold as RaaS

Private Crypto Locker Affiliate Program
By UNKN, July 4, 2019 in (Software) - malware, exploits, bundles, crypts

UNKN
byte

Posted July 4, 2019

Due to the fact that we are expanding activity, we invite adverts by:

• Spam;
• Dediakm and networks;
• Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site and there are nothing for "learners" and "I will try / I will try". We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality "out of the box" according to the RaaS business model.
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact is in the PM.
Dharma

**Attack Vectors**
- Leaked or weak Windows AD Credentials
- Open RDP protocol (port 3389)
- Phishing emails
  - Malicious file attachments

**Signs of Compromise**
**Known File Extensions**
- .crysis, .dharma, wallet, java, .adobe, .viper1, .write, .bip, .zzzzz, .viper2, .arrow, .gif, .xtbl, .onion, .bip, .cezar, .combo, .cesar, .cmb, .AUF, .arena, .brrr, .btc, .cobra, .gamma, .heits, java, .monro, .USA, .bkp, .xlsx, .btc, .best, .bgtx, .boost, .heits, .waifu, .qwe, .gamma, .ETH, .bet, .ta, .air, .vanss, .888, .FUNNY, .amber, .gdb, .frend, .like, .KARLS, .xxxxx, .aqva, .lock, .korea, .plomb, .tron, .NWA, .AUDIT, .com, .cccmn, .azero, .Bear, .bk666, .fire, .stun, .myjob, .ms13, .war, .carcn, .risk, .btix, .bkpx, .he, .ets, .santa, .gate, .bizer, .LOVE, .LDPR, .MERS, .bat, .qbix, .aal, and .wal
Dharma

Known File Hashes:

- 0aaad9fd6d9de6a189e89709e052f06b
- bd3e58a09341d6f40bf9178940ef6603
- 38dd369ddf045d1b9e1bfbb15a463d4c

Ransom Notes:

- README.txt
- HOW TO DECRYPT YOUR DATA.txt
- Readme to restore your files.txt
- Decryption instructions.txt
- FILES ENCRYPTED.txt
- Files encrypted!!.txt
- Info.hta
DoppelPaymer

Background:
DoppelPaymer is named after BitPaymer because of similar code; it first appeared in June of 2019.

Attack Vectors:
- Downloadable temporary file primarily found on cryptocurrency websites
- Uses CVE-2019-19781 vulnerability as an entry point
  - Script executing exploit verifies if patch KB4457138 is installed
  - Elevates privilege using Netlogon Remote Protocol (CVE-2020-1472)

Signs of Compromise:
- The infected system will have a ransom note appear on the desktop, opened in notepad.
Known File Paths:

- \%LOCALAPPDATA\%random_filename.exe
- \%TEMP\%
- C:\Windows\j008.exe
- C:\windows\syswow64\mo5udwbb3pe:ZOdTr
- C:\windows\system32\msdtc.exe
- C:\windows\syswow64\intelcphecisvc.exe
- C:\windows\winsxs\amd64\microsoft-windows_com_dtc_runtime_31bf3856ad364e35_10.0.14393.0_none_46c76e6076b59fe9\msdtc.exe
- C:\install\PsExec.exe
- C:\install\id_M136_wp_enc_x32.exe
- C:\install\Eraser 6.2.0.2982.exe
- C:\install\svchost.exe
- C:\Windows\Prefetch\QZW0QEDFPMR.EXE-41AF8B09.pf
- \%LOCALAPPDATA\%random_filename.exe
- \%TEMP\%
- \%APPDATA\%msnet\QZW0QedfpmR.exe
- \%LOCALAPPDATA\%
- \%LOCALAPPDATA\%depthicon
DoppelPaymer - Ransom Note

File has been encrypted.

All files in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.

No exclusive have decryption software for your situation.

No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME or MOVE the encrypted and readme files.
DO NOT DELETE readme files.
DO NOT use any recovery software with restoring files overwriting encrypted.

This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at your personal page:

1. Download and install Tor Browser: https://www.torproject.org/download/
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar:

4. Follow the instructions on the site.
5. You should get in contact in 48 HOURS since your systems been infected.
6. The link above is valid for 7 days.
7. If email is not working - new one you can find on a tor page.

The faster you get in contact - the lower price you can expect.
DoppelPaymer - Encrypted Files
Ohio Gratings Inc. Your network has been penetrated.

This link and your decryption key will expire in 14 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
No any working decryption software is available from other sources.
Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files.
This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data.
So if you decide not to pay, we would share it.
It may harm your business reputation.

- Your reference ID: 135

[Online chat]
What is RDP and Why is it a popular attack vector?

- RDP = Remote Desktop Protocol
- Protocol developed by Microsoft. Released in the early 1990s as part of Windows NT platform. Enables end users to access a computer from another location.
- If left open to the internet, a hacker can gain direct access to the remote server. Attackers often scan for open port 3389.
How do attackers breach an organization through RDP?

- The attacker will run a port scan using Shodan, looking for open TCP port 3389 and then brute-force RDP credentials.

- Leaked credentials can be purchased on websites (ie. XDedic).

- The use of phishing to gain access inside of an organization. Once in, the attacker can brute force internal RDP access through the compromised device.
What happens after an attacker gains access through RDP?

- The attacker will use tools such as Mimikatz to harvest Windows AD credentials.
- With an administrator account, the threat actor will elevate privileges within the domain.
- Once within the network, the attacker will attempt to map out its topography.
Attack Vector: Managed Service Providers

- Organizations should consider the security practices and reputation of third party managed service providers.

- Threat actors often target MSP’s, with the objective of accessing client networks to propagate ransomware.

- Attackers may create spoof email accounts, or use compromised accounts belonging to the MSP, in order to phish clients.
What are best practices for RDP security from Ransomware?
Enforce a strong Windows AD password and administration policy

- This will make cracking obtained hashes of passwords difficult
  - Will Prevent direct access to campus resources should an attacker gain access to your network.
- Domain Admin accounts should be restricted and should not be used to administer low level systems.
Password Theft

- Once hashes are obtained, a password cracking tool is used to check a pre-compiled list of passwords against the available hashes of an account.

- DICTIONARY/WORDLIST ATTACK = Uses a precompiled list of words, phrases, and common/unique strings to attempt to match a password.

- BRUTE-FORCE ATTACK = attempts every possible combination of a given character set, usually up to a certain length.

- RULE ATTACK = generates permutations against a given wordlist by modifying, trimming, extending, expanding, combining, or skipping words.
# Password Length

<table>
<thead>
<tr>
<th>Password Length</th>
<th>Possible Combinations</th>
<th>Time To Crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>45697</td>
<td>&lt;1 s</td>
</tr>
<tr>
<td>5</td>
<td>11881376</td>
<td>&lt;1 s</td>
</tr>
<tr>
<td>6</td>
<td>308915776</td>
<td>&lt;1 s</td>
</tr>
<tr>
<td>7</td>
<td>8031810176</td>
<td>~4 s</td>
</tr>
<tr>
<td>8</td>
<td>208827064576</td>
<td>~1.5 M</td>
</tr>
<tr>
<td>9</td>
<td>5429503678976</td>
<td>~45 M</td>
</tr>
<tr>
<td>10</td>
<td>1411677095653376</td>
<td>~19 H</td>
</tr>
<tr>
<td>11</td>
<td>3670344486987780</td>
<td>~.1 Y</td>
</tr>
<tr>
<td>*12</td>
<td>95428956661682200</td>
<td>~1.5 Y</td>
</tr>
<tr>
<td>13</td>
<td>248115287320374E4</td>
<td>~39.3 Y</td>
</tr>
<tr>
<td>14</td>
<td>645099747032972E5</td>
<td>~1,022.8 Y</td>
</tr>
<tr>
<td>15</td>
<td>167725934228573E7</td>
<td>~26,592.8 Y</td>
</tr>
<tr>
<td>16</td>
<td>436087428994289E8</td>
<td>~691,412.1 Y</td>
</tr>
<tr>
<td>17</td>
<td>113382731538515E10</td>
<td>~17,976,714 Y</td>
</tr>
<tr>
<td>18</td>
<td>2947951020001390E10</td>
<td>~467,394,568 Y</td>
</tr>
</tbody>
</table>
Windows Group Policies

- Group Policies can be used to create security policy across a Windows network.
- The CCCTC Information Security Team can assist in developing and testing Group Policy.
- We will be doing presentations on Group Policy in the near future.
Restrict RDP Access Through Campus Networks Only

- Access to campus services (i.e. Windows machines) should only be done within the campus networks.
- Outside access should only be allowed through a VPN connection to your campus network.
- Ensure monitoring of RDP systems.
Require two-factor authentication to access campus services

- This should be configured when giving VPN access.
- RD Gateways can be configured to integrate with the Campus instance of DUO.
Only provide Windows RDP access to users who require it

- All Windows AD Administrators can log in via Remote Desktop by default. Default settings should be changed.
- Remote access for admin accounts should be limited to only those who strictly 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.
- If system administrators require RDP access, please only allow connection via VPN and 2FA as discussed previously.
Enable Network Level Authentication

- NLA requires an end-user to authenticate themselves before establishing a session with the server hosting RDP services.

- If RDP is required, then this should be enabled.
Prevent Phishing

- Staff should be trained to identify phishing emails and avoid downloading attachments or clicking hyperlink if the source seems untrustworthy.

- Always keep in mind, “Does the directly email relate to a matter that I am involved in?”

- Be wary of emails that imply urgency regarding passwords or account information:
  1) “Change password immediately”
  2) “Your mailbox is out of space”
  3) “There was a problem with your credit card information”
  4) “We have migrated to a new ……: Click Here”.
Cyber Hygiene Tips For Preventing a Ransomware Attack

1. Prevent Phishing
2. Disable Macros in Microsoft Office Documents
3. Enforce a Strong Password Policy & Require 2FA via VPN for Login
4. Consistently Monitor Network Traffic
5. Monitor Windows Events
6. Backup Assets Often
7. Patch Systems ASAP
8. Implement discussed RDP security practices.
This website is verified by Google Inc.

This website does not supply identity information.
Disable Microsoft Office Macros

- Macros are commands that help automate tasks related to Microsoft Office (i.e. Word, Excel).

- These can be abused to perform exploits on a system.

- Unless your organization requires Macros (cannot do every day tasks without it), it is strongly recommended for o365 admins to disable their use organization wide.
Enforce a Strong Password Policy & Require 2FA for Login

- Same concept as with RDP security.

- A strong password policy will make the cracking of obtained password hashes difficult.

- This will in turn make access to Windows AD accounts more difficult for attackers.
Backup Important Assets Often

- Backups of critical assets should be performed often.
- It is recommended to keep a copy of a backup in the cloud. On-premise backups can become infected as well during an attack.
Consistently Monitor Network Traffic

- Discovering unusual traffic on your networks can lead to the early detection of Ransomware.
- Monitor netflow and packet analysis.
Monitor Windows Events


- Splunk is available for all colleges as a free service.
Regularly Patch Software and Systems

- The latest software updates from vendors generally address known security vulnerabilities.

- Run vulnerability scans over your network to detect vulnerabilities, and find out what hosts need to be patched.

- Tenable.sc can help identify vulnerabilities over your networks.
Develop Comprehensive Network Diagram

- This can be useful during incident response
  - Enables responders to understand where efforts should be focused
Restrict Powershell Usage

- PowerShell is a tool for automating tasks and performing Windows Active Directory Administration.
- Restrict usage of Powershell on Windows systems via Group Policy
- Should be only available to system admins
- Enable transcription, module, and script block logging
Network Segmentation

- Physical or logical network segmentation can help separate various business or IT resources within your organization
- Can help contain the impact of intrusion affecting your organization
- Limits lateral movement on the part of malicious actors
Analyze Network Activity

- Behavioral patterns over a network should be analyzed over a period of several months.
- Determine how to distinguish between malicious and legitimate activity
Secure Domain Controllers

- Make sure DC’s are patched

- Recommended to have the latest version of Windows Server on Domain Controllers

- Ensure that unnecessary software are not installed, they can be vulnerable and be used for arbitrary code execution.
Recommended DC Group Policy Settings (CISA)

- The Kerberos default protocol is recommended for authentication.
- If Kerberos is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network.
- If possible, refuse LM and NTLM responses.
What to do if you are infected?

- Although it is usual to shut down an infected asset, the best action is to keep it turned on and isolate the system from your network.

- This is to “dump” RAM memory for analysis. There may be a chance of reaching the cryptographic keys in the RAM memory.

- This is also to collect and protect evidence, and ransomware encryption keys.
Phishing Testing Services

- The CCCTC Security Team will create campaigns to test security training effectiveness and awareness.

- This will be performed as part of a security assessment if requested.
Common Penetration Test Findings

**Critical unpatched systems**
- Windows Servers – Remote code execution
- Weblogic servers – Deserialization attacks

**Weak network security configurations**
- LLNMR enabled
- WPAD incorrectly configured
- RDP unpatched- open on Internet
- Open file shares with weak controls

**Windows Domains**
- Weak passwords
- Domain Admins
- Too many Domain Admins logged into high risk systems
  - Used inappropriately
CCCTC Information Security Center Services

- Penetration testing can reduce the impact of successful phishing attacks, find vulnerabilities and misconfigurations in your networks, and reduce excess and or damage from ransomware attacks.

- Tenable is an important tool to discover vulnerabilities within hosts on your network and take action to remediate them.

- Logging and monitoring Windows systems is critical for detecting infections. Our Splunk service can be used to do this.

- Attend security workshop, meetings, advisory, whitepapers, etc.
Thank You