Defend Your Organization Against

Sean Heffley
Principal Sales Engineer
Ohio, WV, W.PA

October 2021

LogRhythm
Meet the Speaker

{
    "firstName": "Sean",
    "lastName": "Heffley",
    "company": "LogRhythm",
    "city": "Pittsburgh",
    "role": "Principal Sales Engineer",
    "TenureYears": "6.5",
    "ExperienceYears": "23",
    "bio": "23 years IT experience, background in networking and security",
    "linkedIn": "https://www.linkedin.com/in/sean-heffley-256a924/",
    "activities": "4 children, golf, mountain biking"
}

Company Confidential
## Global State of Ransomware 2021

Organizations that pay a ransom rarely recover all data

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Recovery Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>8%</td>
<td>Recovered all data after paying a ransom</td>
</tr>
<tr>
<td>29%</td>
<td>Recovered no more than half their data after paying a ransom</td>
</tr>
<tr>
<td>65%</td>
<td>Average amount of data recovered after paying a ransom</td>
</tr>
</tbody>
</table>

SOPHOS
Recent Attacks and the Kill Chain

Ransomware Technical Analysis

Detecting Ransomware

Q&A/Comments – If Mike doesn’t yank me.
Some recent examples...

Happy Blog

**KASEYA ATTACK INFO**

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70,000,000 in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.
Surface threats through centralized analysis of network traffic

Spectrum of Attacks

Known
- Indicators of Compromise (IOCs)
- Tactics, Techniques, and Procedures (TTPs)

Unknown
- Behavioral Profiling
Threats Haven’t Changed…

<table>
<thead>
<tr>
<th>Objective</th>
<th>Financial Gain</th>
<th>Revenge</th>
<th>Defamation</th>
<th>Fundraising</th>
<th>Financial Gain</th>
<th>Economic Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Financial Gain</td>
<td>Financial Gain</td>
<td>Notoriety</td>
<td>Communications</td>
<td>Propaganda</td>
<td>Financial Gain</td>
</tr>
<tr>
<td>Scareware</td>
<td>Spam/Phishing</td>
<td>Edward Snowden</td>
<td>WikiLeaks</td>
<td>ISIS/Taliban</td>
<td>Antifa Cyber Army</td>
<td>Credit</td>
</tr>
<tr>
<td></td>
<td>Ransomware</td>
<td>Chelsea Manning</td>
<td>Weev</td>
<td></td>
<td></td>
<td>Debit Card</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ohio Company</td>
<td></td>
<td></td>
<td></td>
<td>ACH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PHI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PCI Theft</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N. Korea</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>China</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Russia</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Iran</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>USA?</td>
</tr>
</tbody>
</table>

...nor has the way we protect and defend them
Anatomy of an Attack: Threat Kill Chain

Attackers are methodical and often predictable

- **Reconnaissance & Planning**
  - Spearphishing

- **Initial Compromise**
  - Malware

- **Command & Control**
  - Brute force and unauthorized account access

- **Lateral Movement**
  - VPN

- **Target Attainment**
  - Financial transfer

- **Exfiltration Corruption Disruption**
Detecting Ransomware

Technical Analysis
Ransomware Infection Timeline

- **T-00:00**: Exploitation and Infection
- **T-00:05**: Delivery and Execution
- **T-00:10**: Backup Spoliation
- **T-02:00**: File Encryption
- **~T-15:00**: User Notification and Cleanup
Initial Exploit and Infection

Unusual Activity Detected
We detected something unusual about recent activity to your Microsoft e-mail account. To ensure your security, we require an extra layer of protection. You will need to verify your Microsoft e-mail account by clicking the link below to confirm that the recent activity was yours and to regain access and enjoy your email service. Failure to verify will result in permanent suspension of your account.

What happened?

- Using a shared computer to access your account.
- Logging into your Microsoft account from a blocked device.
- Not logging off your account after usage.

Thank you for using your Microsoft account to bring the people you love closer together. For more information, visit https://account.live.com/services.

See you online,

The Microsoft team

---

FW: Account Limited

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

????????????

From: PayPal
PayPal <adm@mycom2k05ayy-41p8v8liogby78cimig@mail.com>
Sent: Friday, October 29, 2021 7:57 AM
To: jim.heffley@verizon.net
Subject: Account Limited
Importance: High

Hello, jim.heffley@verizon.net

Your PayPal account has been temporarily restricted

Your security is important to us.

If you did not attempt to access your account, you may have received this message in error. If you believe this is a legitimate request, you can click the link below to validate your account.


We will never ask you to provide your personal or financial information through email. If you have any questions, please contact us at 1-800-221-1168.

Sincerely,

PayPal Customer Service

---

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information: www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now: New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

---

©LogRhythm 2020. All rights reserved.
Initial Exploit and Infection

- Phishing
  - Links
  - Attachments
    > Especially with Macros

- Exploit kits
  - Favor Adobe Flash and IE vulnerabilities
Detecting Ransomware

Logging Requirements
Log Sources Required (for In-depth Detection)

• **Sysinternals: Sysmon or EDR Endpoint logs**
  - Extremely comprehensive and goes beyond command line logging.
  - Aside from windows command line logging, it also has the capability of looking registry changes, file access or modifications, Process Starting/Stopping network-based events.

• **Windows Security: XML – EVID 4688 (Process Start w/ Command Line)**
  - Simplest solution.
  - Deploys via GPO.
  - Appends command line into process start events (4688).

• **MS Windows PowerShell Logging**
  - Also easy to deploy. Logging is a bit more robust.
  - Deploys via GPO.
Ransomware Delivery and Execution (1 of 2)

- Delivered via SSL
  - Difficult to recover executable from wire
- Executable files in `%APPDATA%` and `%TEMP%`
- Auto-execution on restart
Ransomware Delivery and Execution (2 of 2)

- Registry keys for the persistence are added in various places, i.e:
  - HKEY_USERS -> [current user’s SID]:
    - “Software\Microsoft\Windows\CurrentVersion\Run”
    - “Software\Microsoft\Windows\CurrentVersion\RunOnce”
    - “Software\Microsoft\Windows\CurrentVersion\Policies\Explorer” -> “Run”
    - “Software\Microsoft\Command Processor” -> “AutoRun”
Propagating thru Network

- **Ryuk** will spread through the network using PsExec or Group Policy trying to infect as many endpoints and servers as possible.
- Hidden Admin shares
Suspicious Process Activity

- **Remove** Windows volume *shadow copies*
  - `vssadmin.exe delete shadows /all /quiet`
  - `WMIC.exe "shadowcopy delete"`
  - `powershell.exe -Command 'Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_._Delete()};'`

- **Boot Config Modification - BCDEdit.exe**
  - `C:\Windows\System32\bcdedit.exe" /set {current} safeboot network`
  - `Bcdedit.exe " /set {default} recoveryenabled no"`
New Process: Excessive File Access

- New Process: Usually a never seen before
- Excessive File Access
Your important files have been encrypted!
Most of your files are no longer accessible or usable due to them being encrypted.
You can only recover your files with our decryption service.
To decrypt your files send $ 400 USD in BITCOIN to

Address: 3MwjrwZaDyPY1eybS8dZrweEhQVwVCv1ye

Visit https://buy.bitcoin.com/ Register Buy Bitcoins Send $400
After payment contact manager@outlookpro.net
for the decryption KEY before YOUR DATA IS LEAKED ONLINE,
FBI YOU WILL END UP IN JAIL
THE EARLIER THE BETTER
YOU KNOW YOUR ACTIVITIES ARE PUNISHABLE BY LAW

Bad Gopher Ransomware Notification 3-9-21
You are Infected - What can you do?

1. Pay Ransom and HOPE you get the decryption key!

2. Wipe System & Restore from backup

THAT MOMENT YOU REALIZE IT’S GOING TO BE DIFFICULT TO EXPLAIN WHY YOU’RE LATE
Detecting Ransomware

Security Hygiene
Defend Against Ransomware (1 of 2)

- Maintain BACKUPS
- Educate yourselves and your users
  - Don’t open dubious attachments
  - Don’t click on dubious links
- Develop run books
  - Ransomware incident response & disaster recovery plans
- PATCH, PATCH, PATCH!
  - 75% of breaches are because of NO PATCHING.
- Disable macros
- Be cautious of small zipped files (.zip .rar .gz .7z)
Defend Against Ransomware (2 of 2)

- Invest in Security - Products and Personnel
  - NG Firewalls, IDS/IPS, email filter, AV/EDR, SIEM & UEBA
  - Pay the for Security Analysts
- LEAST PRIVILEGE – users have more rights than they need
- Correlate against Threat Lists
- Endpoint tools (EDR – Endpoint, Detection & Response)
  - Updated Anti-Virus signatures; App Whitelisting
  - Monitor for Ransomware behaviors
- Password complexity enforcement
- Insurance Policy
- MFA – Multi-Factor Authentication
- Vulnerability Scans
Detecting Ransomware

Detecting Behaviors
Command and Control (C2)

- Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.
- Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
- There are many ways an adversary can establish command and control with various levels of stealth depending on the victim’s network structure and defenses.

Source: https://attack.mitre.org/tactics/TA0011/
**Attacker Goal:** Gain access to a system on the inside

**Problem:** The attacker can't get through the firewall from the outside
Solution: The attacker will trick the user into installing a ‘C2 implant’ which will initiate an outbound connection from a user workstation. This will give the attacker access to the inside.
In a supply chain attack example, an attacker will breach an existing trust infrastructure to install multiple C2 implants.
Sunburst DGA

The dynamically generated component is based on:

- The physical address of the network interface
- The domain name of the device
- The content of the *MachineGuid* registry value
Connection to a C2 Server
Connection to a C&C Server

- Connect to a Command And Control (C2) node
Detonated two variants of Ransomware, Ryuk and Sodinokibi, both of which delete shadow copies. The following logs were picked up by (Sysinternals: Sysmon)

**Ryuk**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Message ID</td>
<td>1</td>
</tr>
<tr>
<td>Entity (Origin)</td>
<td>Primary Site</td>
</tr>
<tr>
<td>Entity (Impacted)</td>
<td>Primary Site</td>
</tr>
<tr>
<td>HostName (Impacted)</td>
<td>winde\1912eval</td>
</tr>
<tr>
<td>User (Origin)</td>
<td>user</td>
</tr>
<tr>
<td>User (Impacted)</td>
<td>user</td>
</tr>
<tr>
<td>Domain Impacted</td>
<td>WINDE\1912EVAL</td>
</tr>
<tr>
<td>Command</td>
<td>vsadmin.exe Delete Shadow /all /quiet</td>
</tr>
</tbody>
</table>

**Sodinokibi**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Message ID</td>
<td>1</td>
</tr>
<tr>
<td>Entity (Origin)</td>
<td>Primary Site</td>
</tr>
<tr>
<td>Entity (Impacted)</td>
<td>Primary Site</td>
</tr>
<tr>
<td>HostName (Impacted)</td>
<td>winde\1912eval</td>
</tr>
<tr>
<td>User (Origin)</td>
<td>user</td>
</tr>
<tr>
<td>User (Impacted)</td>
<td>user</td>
</tr>
<tr>
<td>Domain Impacted</td>
<td>WINDE\1912EVAL</td>
</tr>
<tr>
<td>Command</td>
<td>“C:\Windows\System32\cmd.exe” /c vsadmin.exe Delete Shadow /All /Guest &amp;bcdet /set {default} recoveryenabled No &amp;bcdet /set {default} bootstatuspolicy ignoreallfailures</td>
</tr>
</tbody>
</table>

Subject: C:\Windows\Sys\VOL\W4

Process Name: cmd.exe

Process ID: 10512

Severity: Information

Version: 10.0.18362.449

Session: 3bb69415-5-b8e2-5e23-0000-0010f6c49404
Let's build it out: AIE: Ransomware IoC (vssadmin.exe)

Verified Ransomware Matches: Phobos, WannaCry, Matrix, gigsaw, Locky, Cryptolocker, Bad Rabbit, Olymic Destroyer, NotPetya, Fantom, Shodinokibi, katyusha, GoldenEye, Ryuk, KUUB, stahp, HETS, .djvuu, 1HILDACRYPT, CrySIS.... And likely many more.
Sysmon - WARMIND Ransomware System Cripple
WARMIND Ransomware Burst Decrypt TXT Detection
Custom Rule Design - WastedLocker
Sysmon (Reg keys) CLOP Ransomware IOC
Sysmon - Malicious Office Document – Encoded Powershell (Emotet)
Detecting Ransomware: Suspicious Executables

- Ransomware delivery and execution
  - Network traffic rules
  - File execution from %APPDATA% and %TEMP%
Detecting Ransomware: Autorun Registry Keys

- Monitor Registry Run Keys

![Image of Registry Integrity Monitor Policy Manager]

- Registry Integrity Monitor Policy Manager
  - Policy Name: Monitor Registry Run Keys
  - Description: This policy monitors the standard LM Autorun keys on all machines.

<table>
<thead>
<tr>
<th>Monitored Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce</td>
</tr>
</tbody>
</table>

**AIE: Persistence: Registry RunKeys/Startup Folder**
- Global Entity
- 05/18/2020 12:28:29 pm
- Id: 456791

SmartResponse Not Set
Containment

• Kill processes
  - Endpoint protection system
• Remove host’s network connectivity
  - Switch port, WI-FI block
  - Disable host NICs

```powershell
#LocalHost
if($LocalHost -like $ImpactedHost)
{
  Get-WmiObject -Class Win32_NetworkAdapter -ComputerName $ImpactedHost -Filter ‘NetConnectionStatus = 2’ | %{ $_.disable() }
}
```

• Forcefully and quickly shut down host

```powershell
#LocalHost
if($LocalHost -like $ImpactedHost -OR $localIP)
{
  Stop-Computer -Force -ComputerName $ImpactedHost
}
```

#RemoteHost
Detecting Ransomware

Summary
Q & A

- Sean Heffley
  - Sean.Heffley@logrhythm.com