RYUK RANSOMWARE

ALBANY INFRAGARD MEMBERS ALLIANCE

August 15, 2019

Participating Organizations

- New York State Intelligence Center (NYSIC)
- New York State Cyber Command Center (CYCOM)
- New York State Division of Homeland Security and Emergency Services (DHSES)
- Federal Bureau of Investigation (FBI)
- Albany InfraGard Members Alliance (Albany IMA)
- Coveware

Agenda

- Ransomware History
- Coveware
- Ryuk Ransomware
  - Ryuk Trends
  - Recommendations
  - Information for Law Enforcement
  - Reporting
- Technical Discussion
- Resources & References

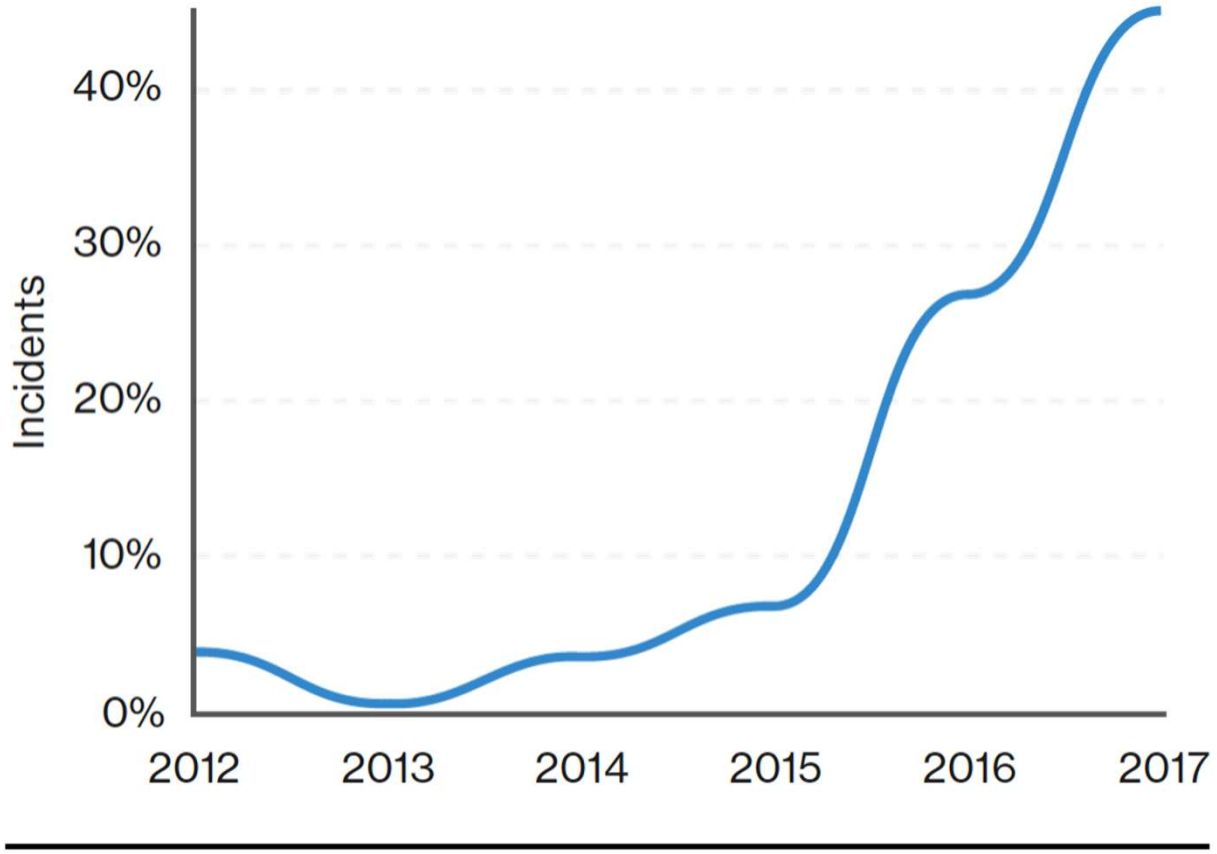
Ransomware History

Ransomware

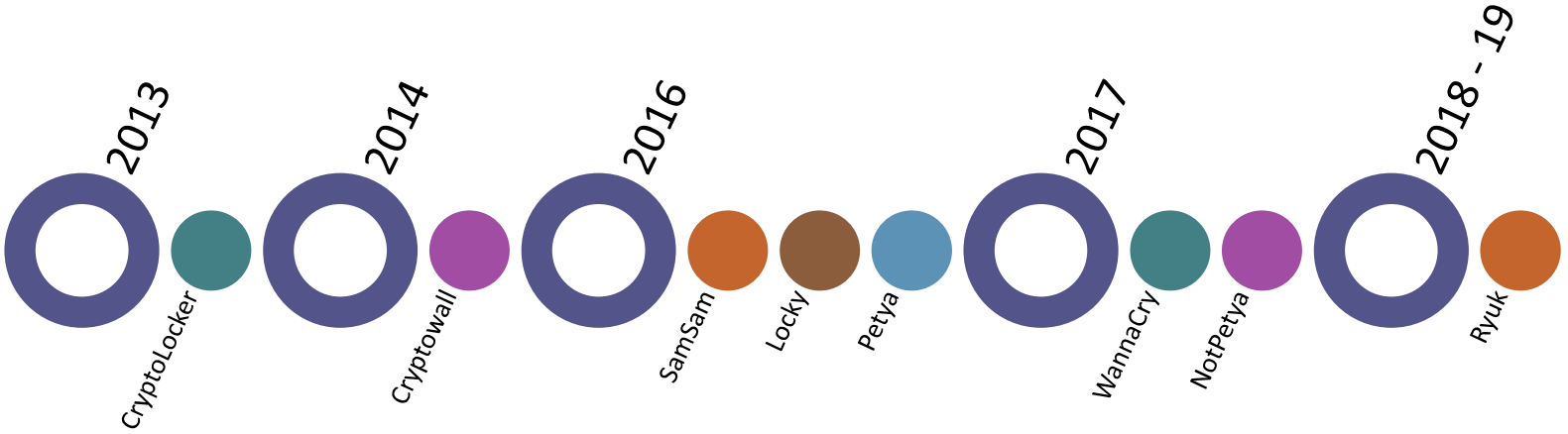
- A type of malware threat actors use to infect computers and encrypt computer files until a ransom is paid.
- Will attempt to spread to connected systems, including shared storage drives and other accessible computers.
- If the threat actor's ransom demands are not met (i.e., if the victim does not pay the ransom), the files or encrypted data will usually remain encrypted and unavailable to the victim.
- Even after a ransom has been paid to unlock encrypted files, threat actors will sometimes demand additional payments, delete a victim's data, refuse to decrypt the data, or decline to provide a working decryption key to restore the victim's access.
- The Federal Government does not support paying ransomware demands.

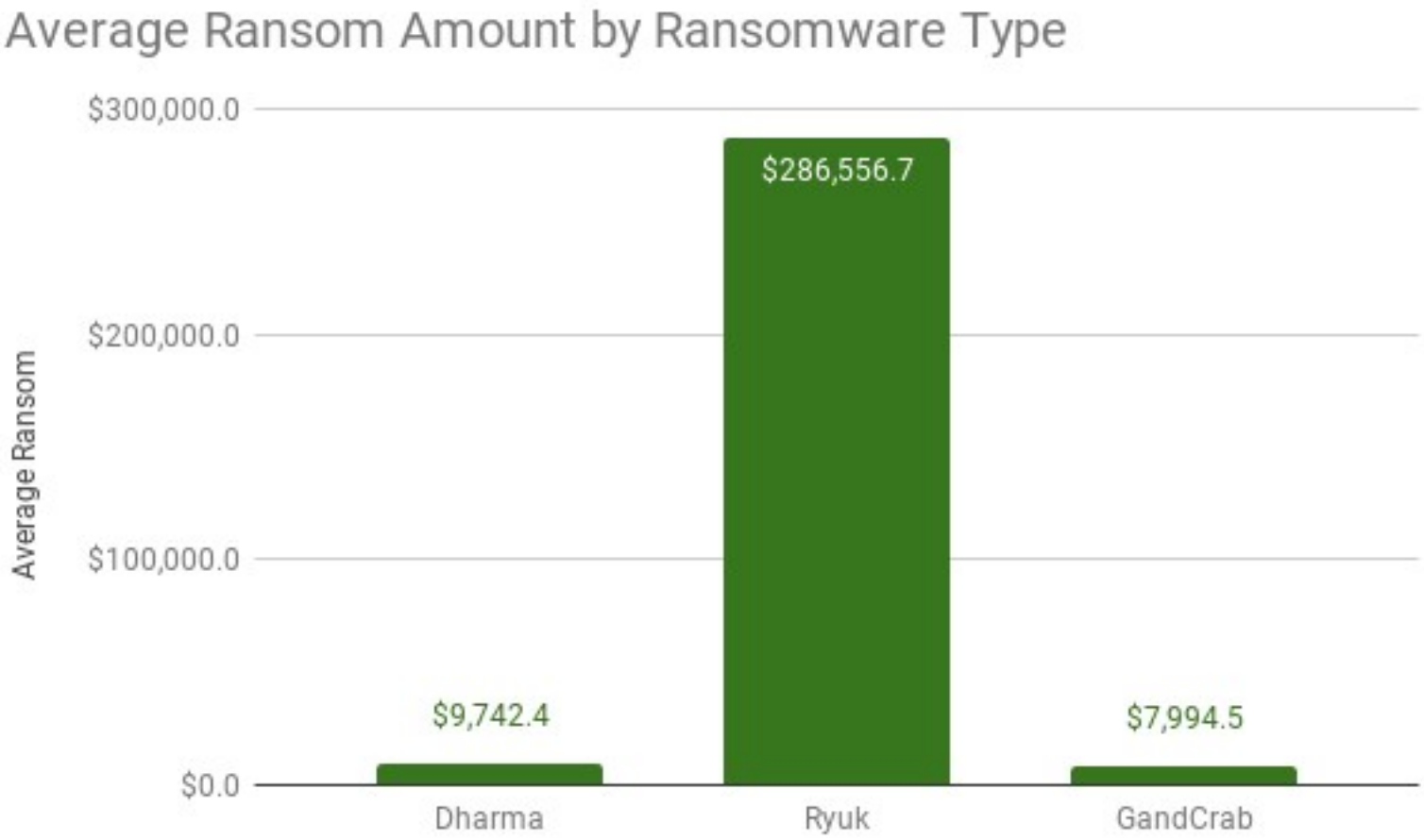
https://www.us-cert.gov/ncas/tips/ST19-001

Rise of Ransomware Within Malware



Evolution of Ransomware Variants





https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

7.3 days

Average number of days a ransomware incident lasts

$64,645

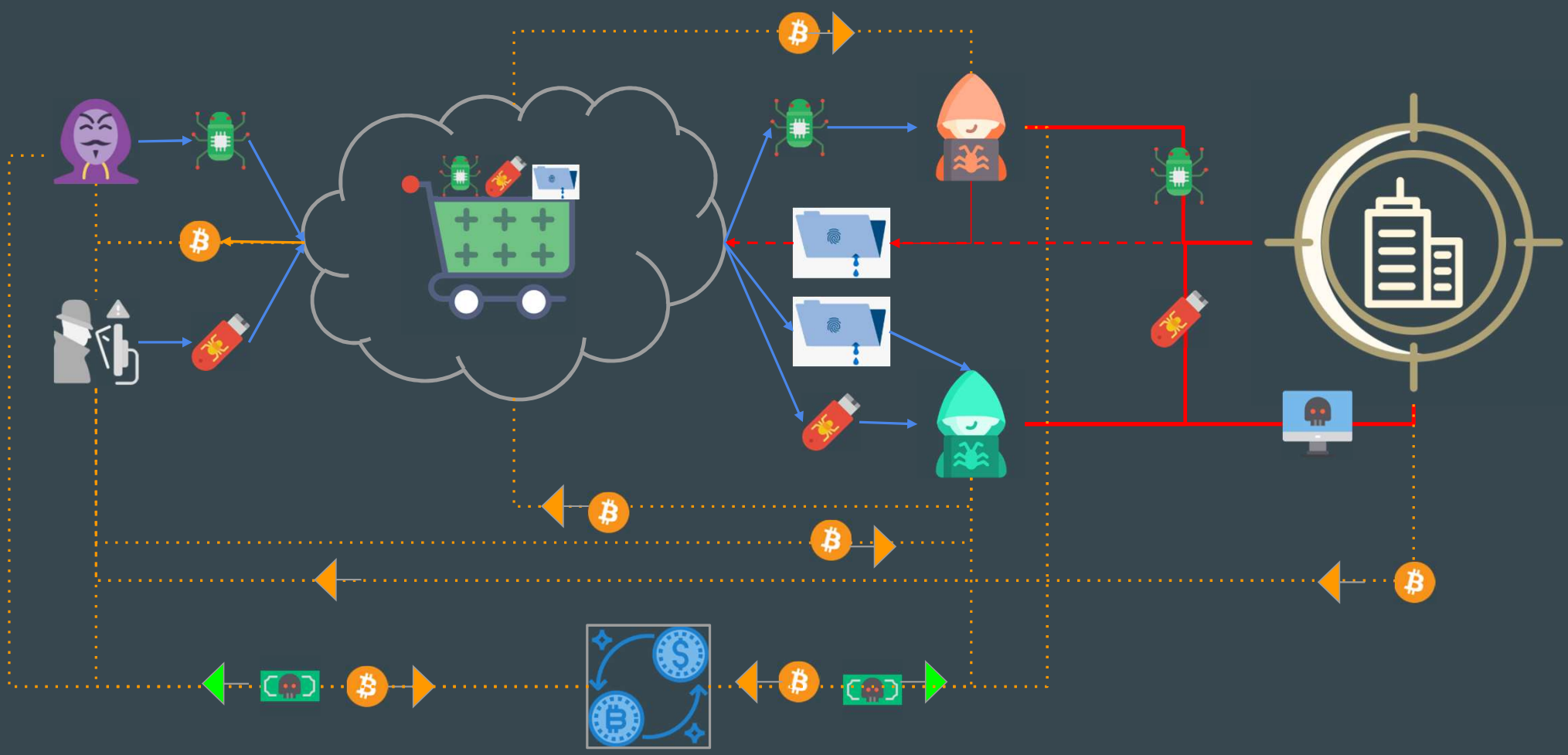
Average cost of ransomware incident related downtime

https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

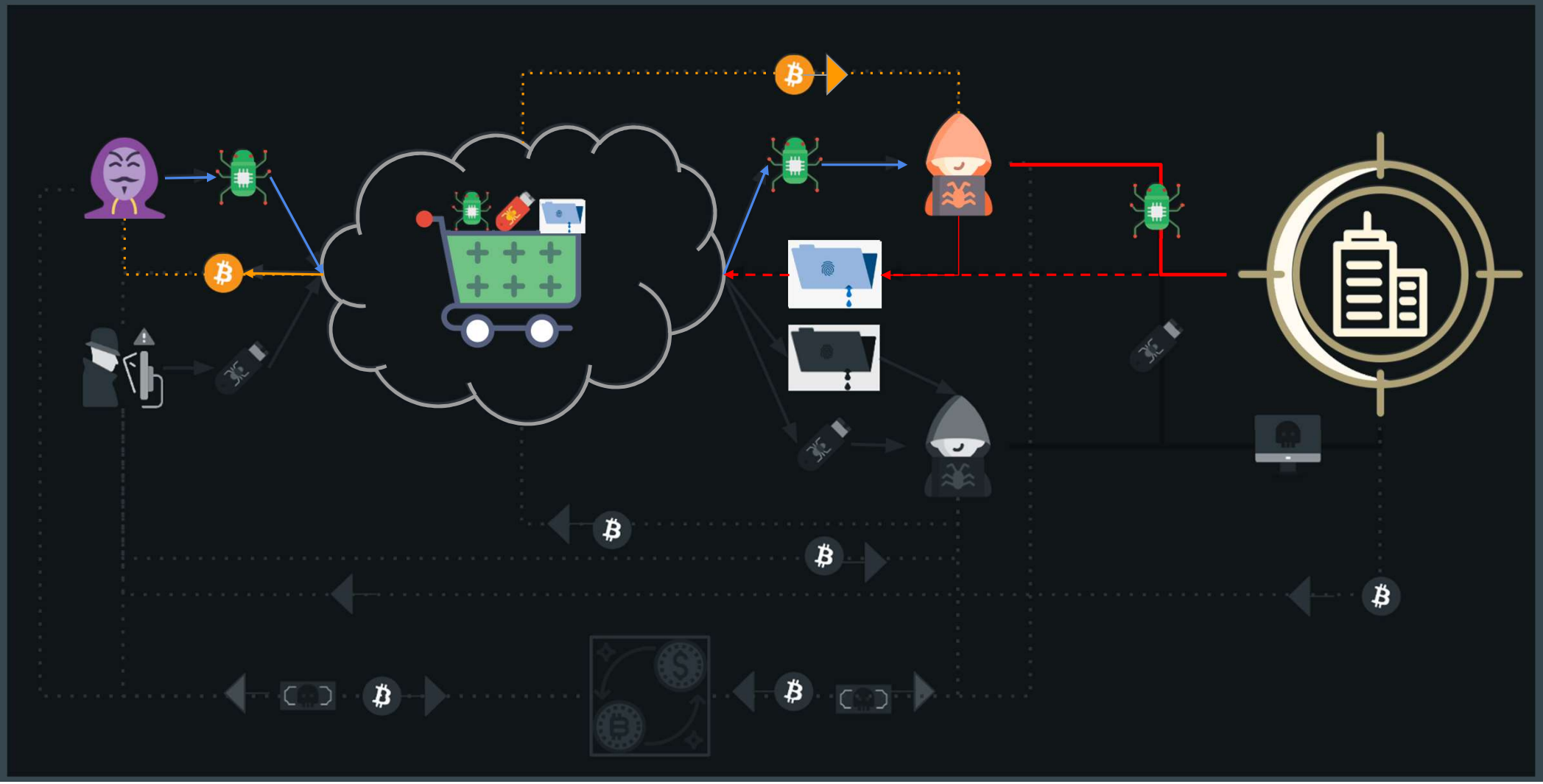
Coveware

Bill Siegel, CEO

Ransomware Supply Chain



Part 1: Exploit Kit Used to Breach Credentials



Part 1: IOC's and Mitigants

TRIAGE

Treat Trickbot / Emotet like EBOLA...assume the host is dead and contain its spread.

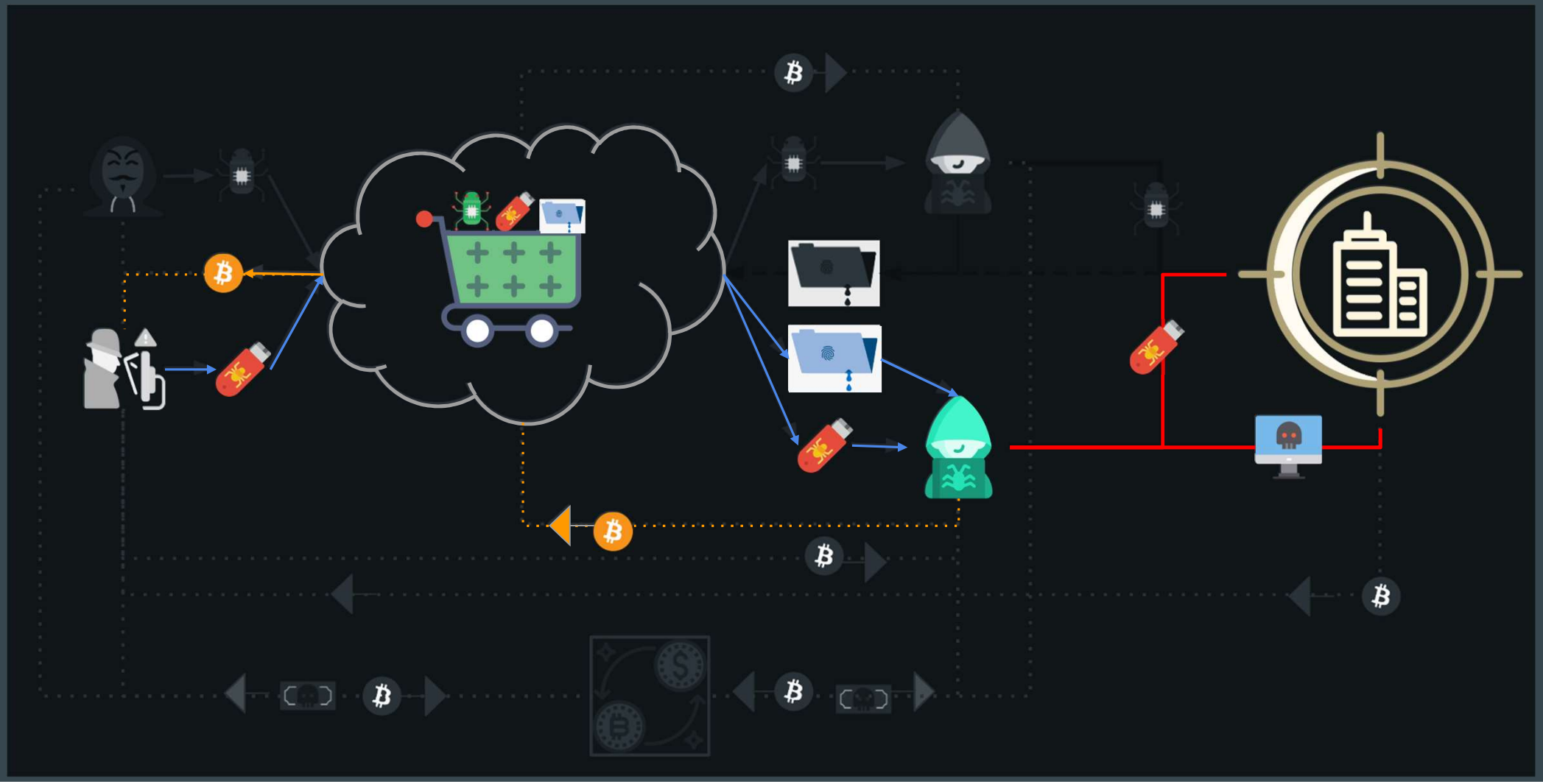
Non-Tech IOC's

"Glen from accounting had his personal bank account drained...so weird right...just a week or so after we all got those creepy phishing emails...."

Defense

+Security Awareness Training
+ATO counter measures
+Credential Monitoring
+MFA everything you care about

Part 2: Ransomware Supply / Distribution



Part 2: IOC's and Mitigants

Neuter Payloads before the drop

+Least Privilege applies to all users, not just admins
+Make it EXPENSIVE for the hackers

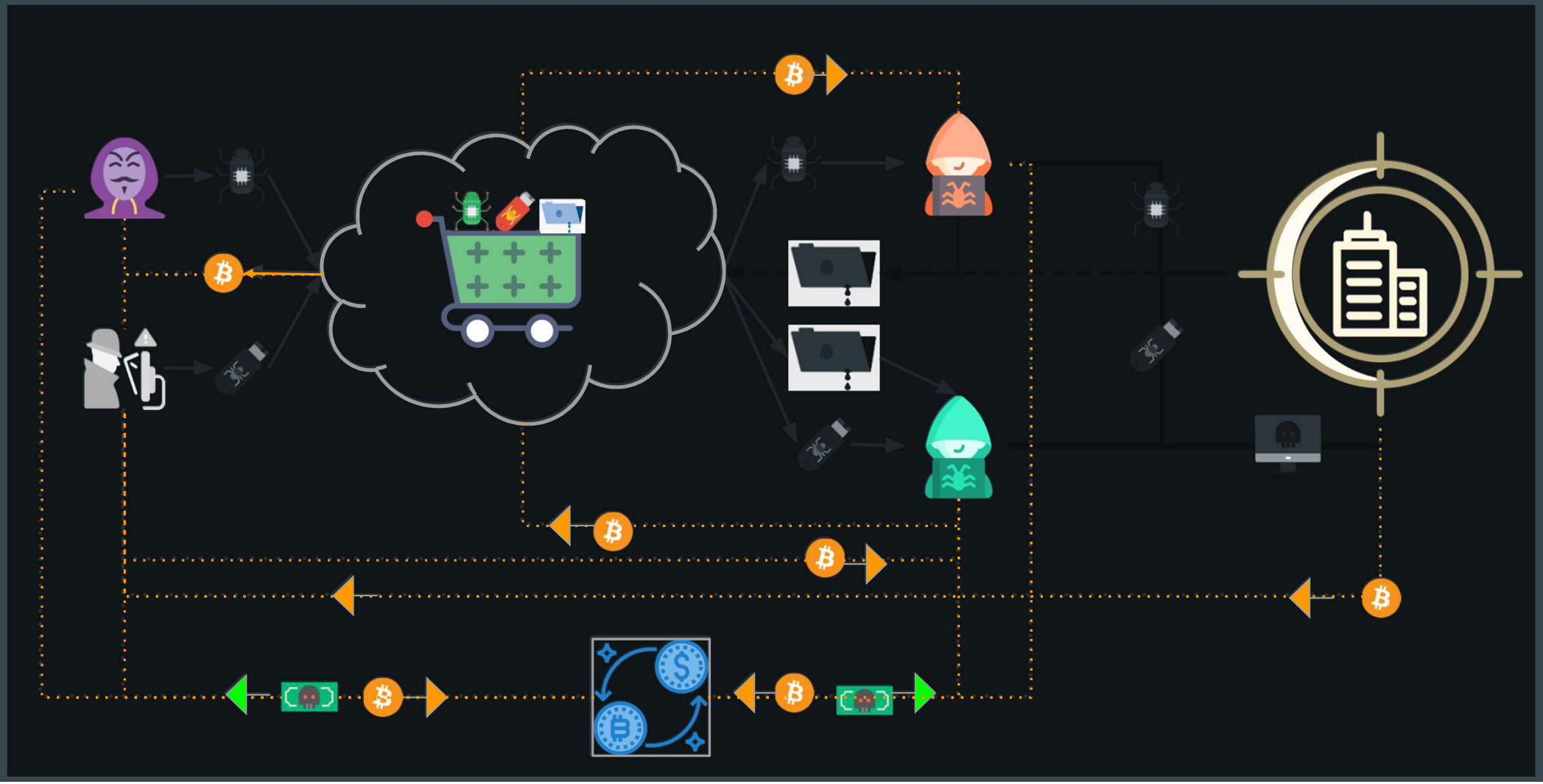
Non-Tech Mitigants

+Pay Security Admins well
+Run Background Checks on them regularly
+They will get approached

Defense

+MFA, MFA, MFA
+Properly partition your back up OFF your network.

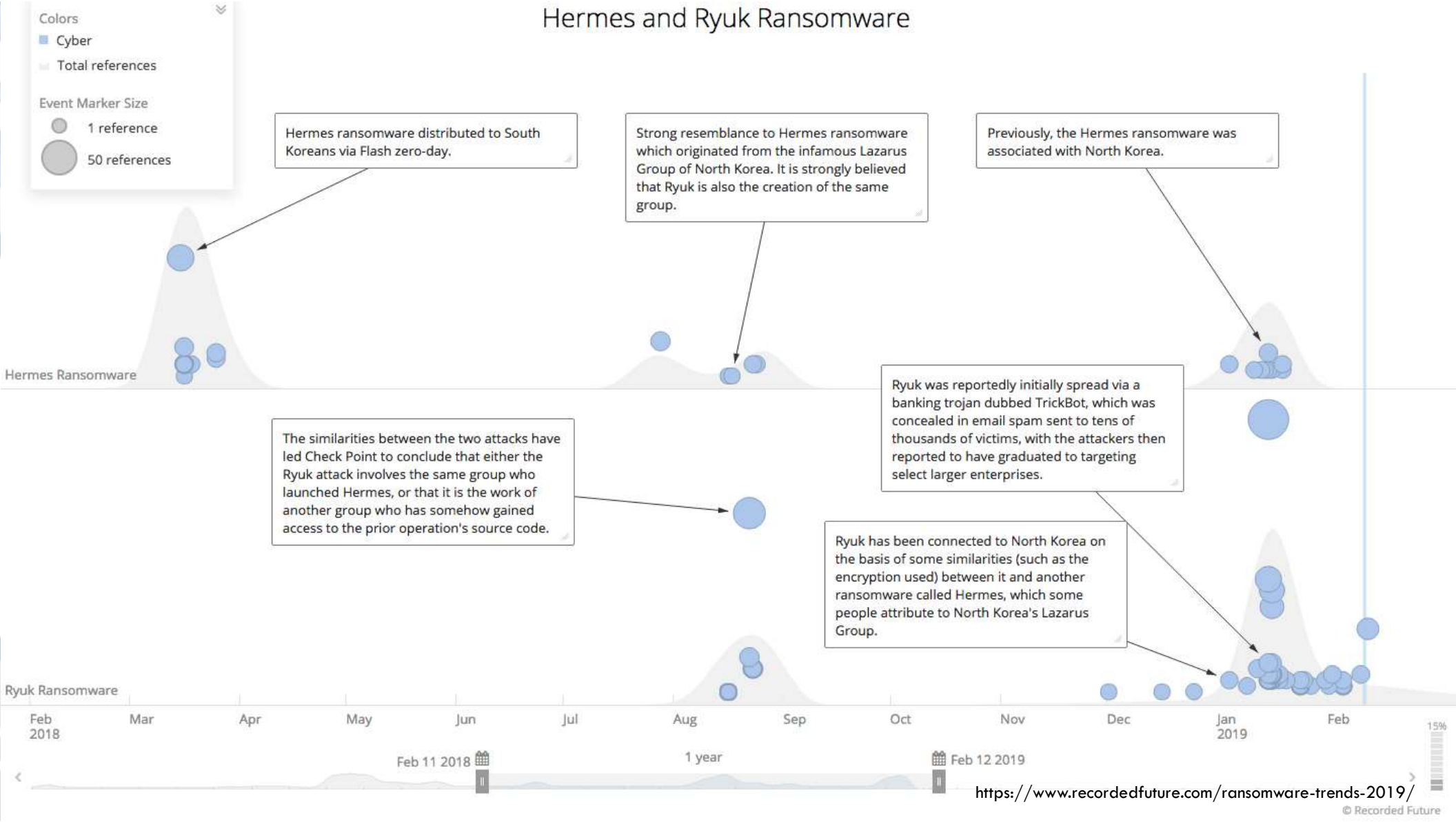
Part 3: Cashing Out



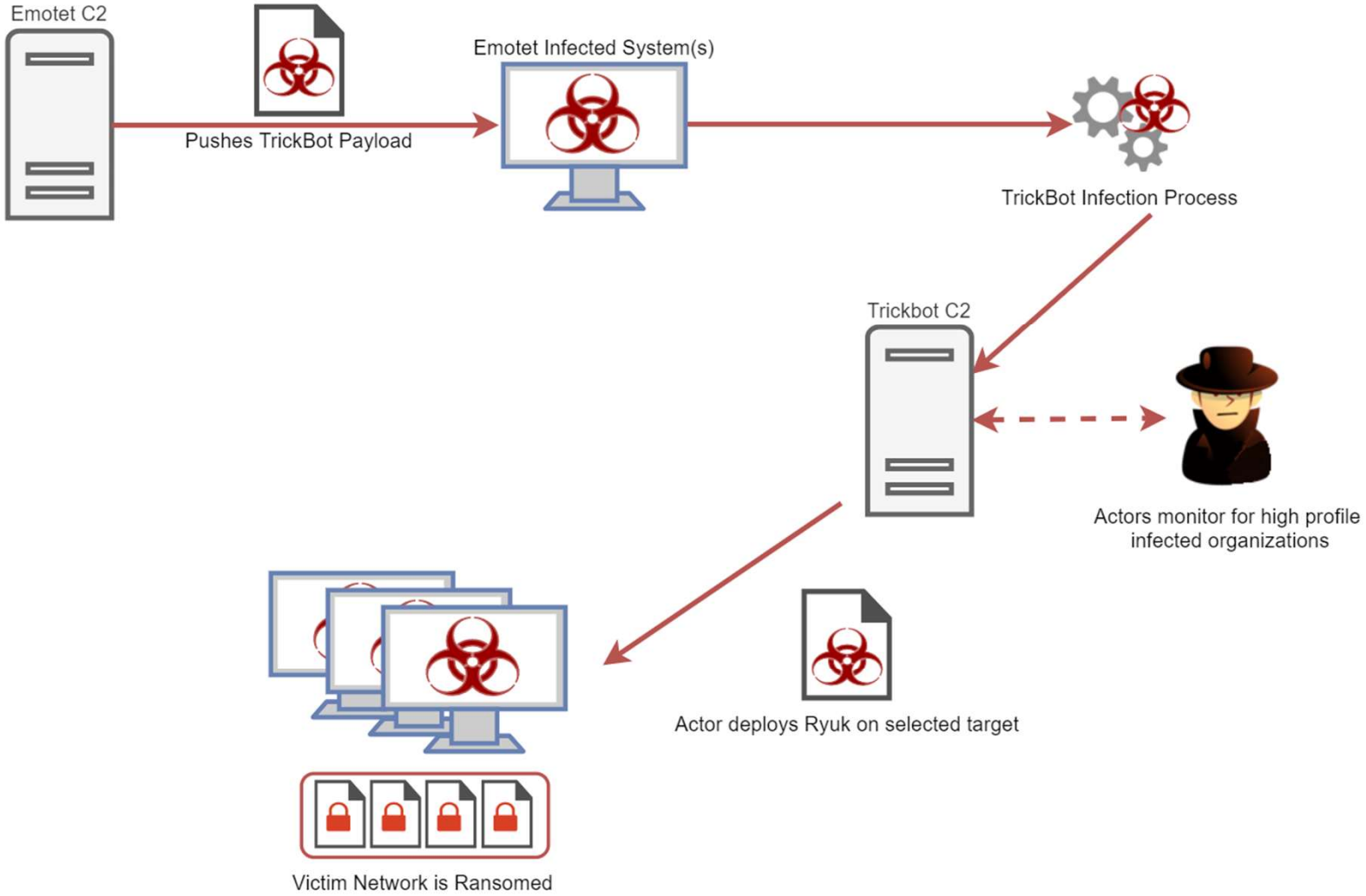
Ryuk Ransomware

2019 Ryuk Victims

- Georgia Judicial System
- Lake City, Florida
- Key Biscayne, Florida
- Riviera Beach, Florida
- Onondaga Library System – Syracuse, New York
- Other public and private organizations in New York



https://www.recordedfuture.com/ransomware-trends-2019/


Emotet C2
Pushes TrickBot Payload
Emotet Infected System(s)
TrickBot Infection Process
Trickbot C2
Actors monitor for high profile infected organizations
Actor deploys Ryuk on selected target
Victim Network is Ransomed

Compromise

- In many cases, Trickbot and Emotet infected systems are used to push Ryuk's dropper as a Stage 3 for the Ryuk payload
- Trickbot and Emotet rely on outdated SMB protocol vulnerabilities (EternalBlue) for compromise and lateral movement
- In some instances, internal AD server / DC staging is used
- The FBI has also observed compromise via RDP bruteforce, followed by non-malware methodology for lateral movement (PowerShell, psexec).

FBI Flash - MC-000103-MW - May 2, 2019

Execution

- Ryuk dropper runs a .bat file to delete Volume Shadows
  - Drops & Executes Ryuk
    - Deletes dropper
- Registry persistency
- Process injection
- Indexing network shares
- Encryption begins
- RyukReadMe files are dropped after encryption with payment info

FBI Flash - MC-000103-MW - May 2, 2019

Ryuk Trends

Ryuk Trends

- More than 100 major victims in 2018
- Focus was on high revenue victims
- Ransoms as high as $5 million
- Public sector Ryuk compromises as a percentage of victims more than tripled in 2019

FBI Flash - MC-000103-MW - May 2, 2019

Recommendations

Recommended Mitigations

- Scan system backups for registry persistence
- Scan system backups for other malware infections, particularly Trickbot and/or Emotet
- Execute a network-wide password reset
- Enact multifactor authentication
- Ensure network segmentation
- Ensure all file backups are located offline
- NIST / CIS Critical Security Controls

FBI Flash - MC-000103-MW - May 2, 2019

Information for Law Enforcement

Information for Law Enforcement

- Recovered executable files / Malware samples
- Copies of the "read me" file – DO NOT REMOVE the file or decryption may not be possible
- Copy of the ransom note
- Ransom amount and whether or not it was paid
- Live memory capture (RAM)
- Log files

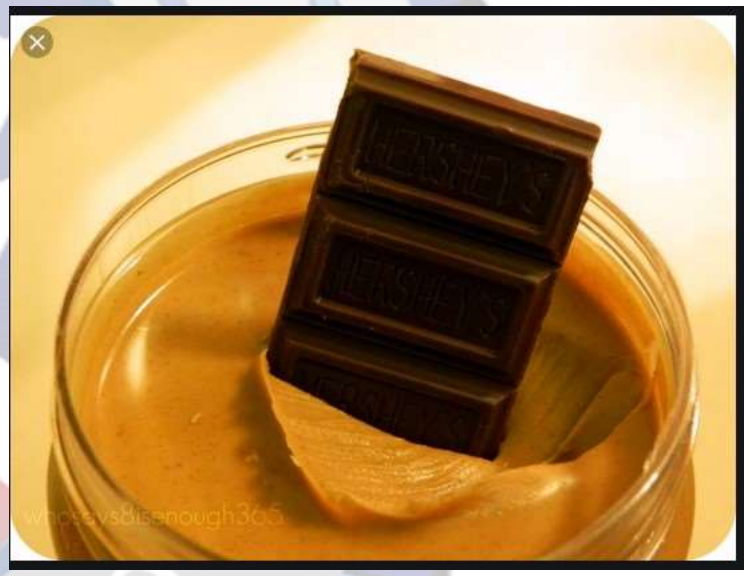
FBI Flash - MC-000103-MW - May 2, 2019

Reporting

Reporting

- FBI CyWatch (24/7) - CyWatch@fbi.gov - (855) 292-3937
- FBI Internet Crimes Complain Center – www.ic3.gov
- Your local FBI field office

TrickBot and Ryuk: Together



TrickBot and Ryuk: Together

TrickBot – Precedes Ryuk

Ryuk RansomWare Has Been Consistently Delivered By Leveraging An Existing TrickBot Infection.

Analysis From July / August TrickBot / Ryuk Incidents In NYS Reveal TrickBot Infections Going Back As Far

As January 2019 (or earlier).

TrickBot Will Disable AV, Windows Defender, Real-Time Monitoring.

TrickBot – Installed Service

ControlSet001\Services\zfpypypysw

Last Written Time	1/25/2019 17:42:45 UTC

Name	Type	Data
Type	REG_DWORD	0x00000010 (16)
Start	REG_DWORD	0x00000003 (3)
ErrorControl	REG_DWO[illegible]	0x00000001 (1)
ImagePath	REG_EXPAND_[illegible]Z	%SystemDrive%\mswvc.exe
DisplayName	REG_SZ	Tehno-ControlsService
ObjectName	REG_SZ	LocalSystem

TrickBot – Multiple Active Binaries

- **Analysts identified at least seventy one instances of Trickbot infections installed as Windows Services, with the earliest being 1/30/2019 13:26:27 UTC.**

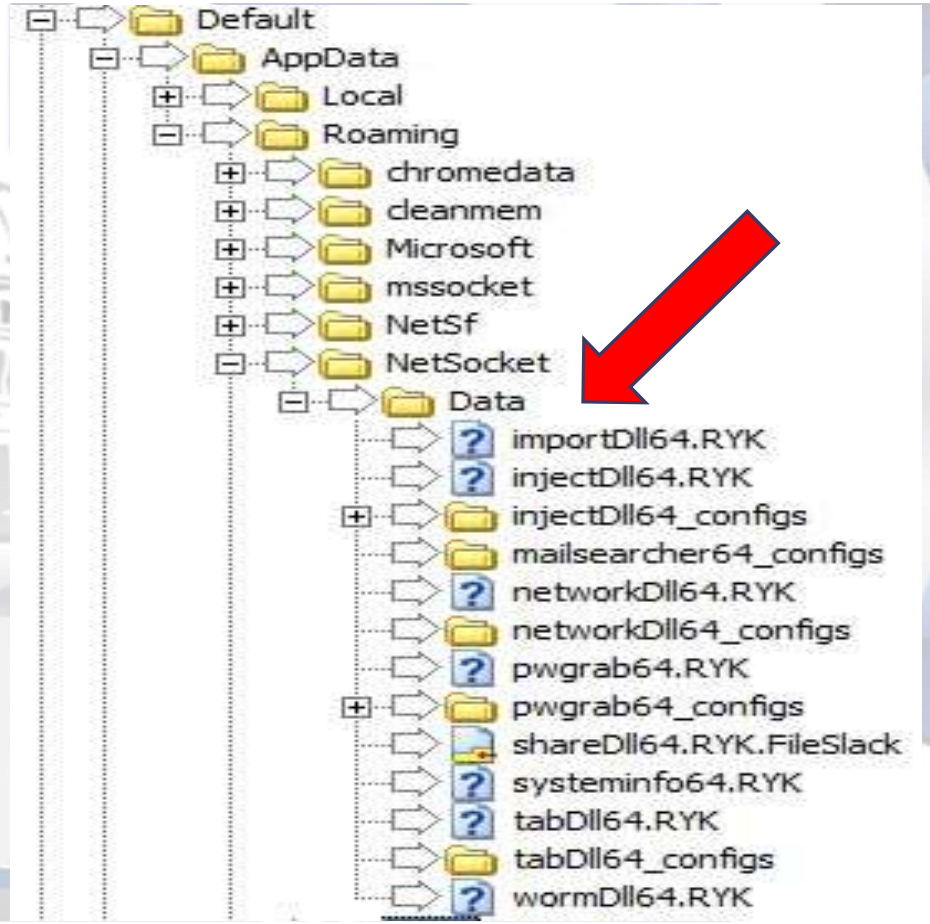
- **Analysts recovered 7 malicious binaries that were currently referenced by installed services.**

Name	Path	Created
swupd.exe	[root]/swupd.exe	4/15/2019 10:05:49 AM
swepe.exe	[root]/swepe.exe	4/8/2019 5:04:15 PM
swype.exe	[root]/swype.exe	4/12/2019 2:48:48 PM
widreh.exe	[root]/widreh.exe	3/28/2019 4:30:20 PM
rehary.exe	[root]/rehary.exe	4/4/2019 11:44:29 AM
windrh.exe	[root]/windrh.exe	3/18/2019 10:53:57 AM
windbh.exe	[root]/windbh.exe	3/13/2019 1:22:10 PM

TrickBot – Disbles AV / Defender

- **Powershell Event Log Example**
- <Events> <Name> **PowerShell** <TimeCreated> <SystemTime> **2019-07-27T23:50:49.959256Z** <EventRecordID> 170845 <Channel> Windows PowerShell <Computer> H-REDACTED.REDACTED.org <EventData> <Data> Stopped Available NewEngineState=Stopped PreviousEngineState=Available HostApplication=**powershell**
- **Set-MpPreference -DisableRealtimeMonitoring $true**
- <Binary>

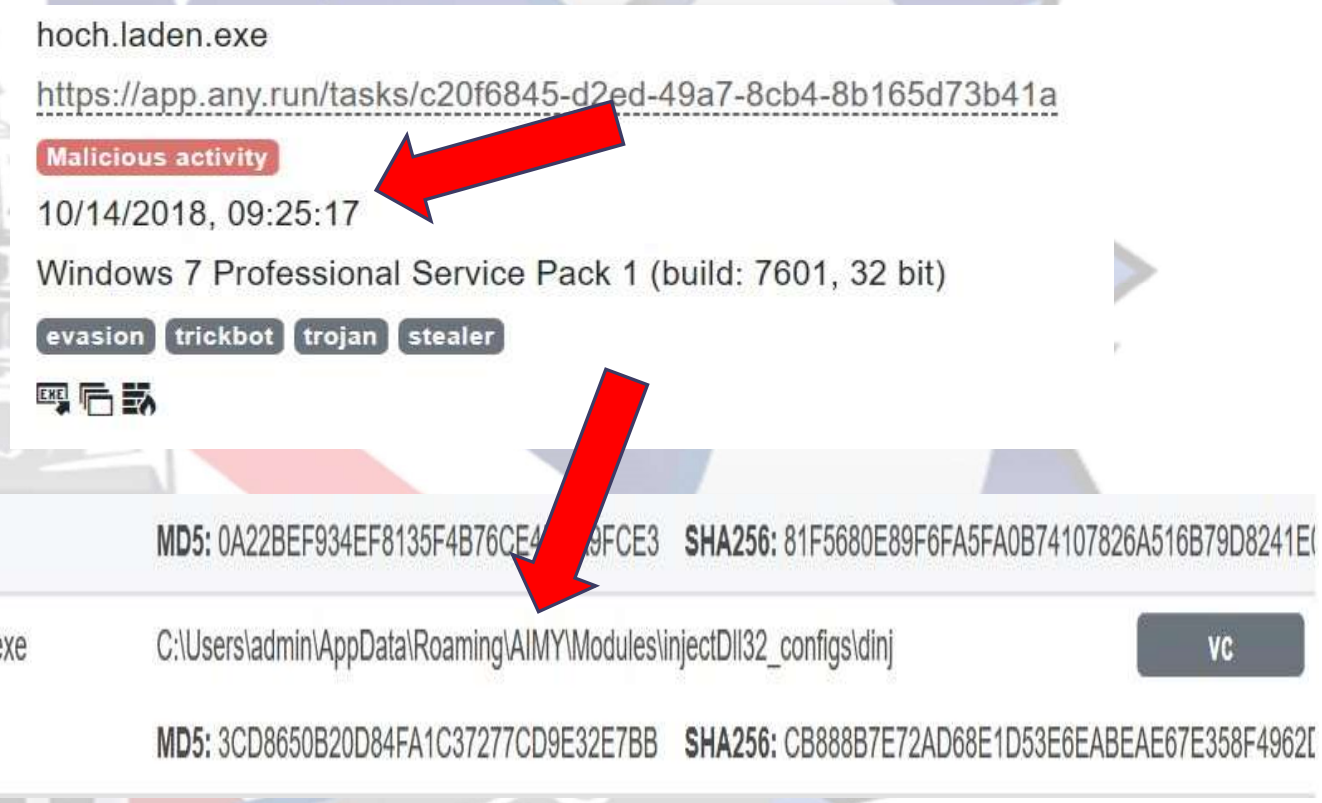
TrickBot – Domain Controller



TrickBot – Domain Controller

- **Files found on the system indicate infection may have occurred as early as 10/10/2018.**
- **A file creation date of 10/10/2018 2:33:53 PM was found for file: C:\Users\srvadmin\AppData\Roaming\AIMY\Modules\injectDll64_configs\dinj.RYK**
- **Note the file is Ryuk encrypted, and the .RYK extension was appended. All related TrickBot files in the Modules directory and modules are also encrypted.**
- **Earliest indication from the Windows Event Logs show evidence of infection dating back to 3/26/2019 4:09:13 PM. The event logs indicate PowerShell used to disable Windows Defender Real-Time monitoring by the command: "powershell Set-MpPreference -DisableRealtimeMonitoring $true".**

TrickBot – Domain Controller



Ryuk – Domain Controller

- Two Ryuk Binaries were found including a string within the binary of RyukReadMe.html:
- **C:\Users\Public\AbKZH.exe and C:\Users\Public\GNuRA.exe**
- Created Date7/28/2019 7:21:21 AM (2019-07-28 11:21:21 UTC)
- Modified Date7/28/2019 7:21:25 AM (2019-07-28 11:21:25 UTC)
-
- **RDP connections are listed in the event log at 7/27/2019 4:41:45 AM shortly before Ryuk encryption takes place. UserID='S-1-5-20' (NETWORK_SERVICE) was seen from the FP Server.**

Ruyk – Final Thoughts

- **The Ruyk ransomware encryption process for an analyzed workstation began on 07/28/2019 at 1:08 PM and was complete within 15 minutes.**

TrickBot - Ryuk

- If you are a system or network administrator, IT Director, ISO, etc. please take a moment when you get back the office to check for the indicators presented today. We have seen networks infected with TrickBot for six months and more before the Ryuk phase was triggered.

Contact

Johnny Griffin

New York State Cyber Command Center

Albany InfraGard

NYData518@outlook.com

John.Griffin2@its.ny.gov

Mobile: 518-275-2851

CYCOM Hotline: 518-242-5045

Resources and References

Resources and References

- FBI
  - Intelligence Bulletin – IB245 20190417 – April 17, 2019
  - Incidents of Ransomware on the Rise – April 29, 2016 – https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise
  - Flash – MC-000103-MW – May 2, 2019
    - https://1drv.ms/u/s!Agksp49o_Tp6t55l6ctlvheRbynRgw?e=dBv0hx
    - Password: infragard

Resources and References

- Cybersecurity and Infrastructure Security Agency (CISA)
  - ST18-004 – Protecting Against Malicious Code - https://www.us-cert.gov/ncas/tips/ST18-271
  - TA18-201A – Emotet Malware – https://www.us-cert.gov/ncas/alerts/TA18-201A
- Coveware - Ransom amounts rise 90% in Q1 as Ryuk increases - https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

Resources and References

- United Kingdom (UK) National Cyber Security Centre (NCSC) Advisory: Ryuk Ransomware Targeting Organisations Globally – NCSC-Ops/17-1922 – June 28, 2019
- Louisiana State Police Cyber Crime Unit – July 26, 2019
- Center for Internet Security
  - https://www.cisecurity.org/controls/
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - Security Primer – TrickBot – https://www.cisecurity.org/white-papers/security-primer-trickbot/

Questions

- Please send questions to Secretary@InfraGardAlbany.org
- https://www.infragardalbany.org/
- https://www.infragard.org/ Join Today

Evolution of Ransomware Variants

- 2013 CryptoLocker
- 2014 Cryptowall
- 2016 Locky
- 2016 Petya
- 2017 NotPetya
- 2017 WannaCry
- 2018 Ryuk