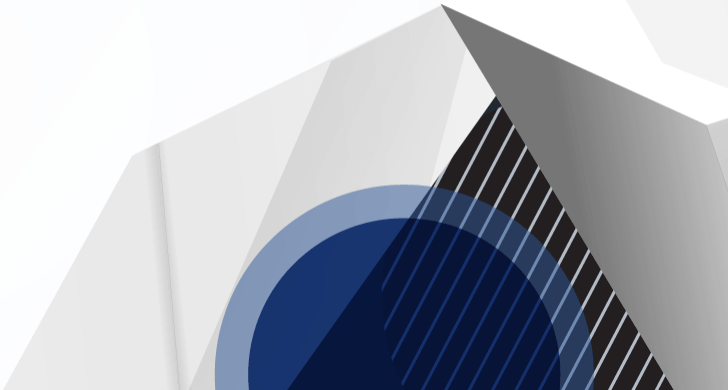
FIREEYE™

AaaStronomically Profitable

A guide to detecting and defending against ransomware

Kirstie Failey

October 26, 2019



➜ ~ whoami

- Kirstie Failey, Consultant
  - @gigs_security
  - Mandiant Professional Services
  - Incident response, digital forensics, threat hunting
  - Previously: PCI and HIPPA compliance
- I've done a lot of ransomware investigations…

What This Talk IS:

An overview of what ransomware is - specifically RYUK.

How ransomware is commonly deployed through networks

Common detections to work into your security model

Introduction to tools I love using during ransomware investigations.

What This Talk is NOT

- A custom development of detections for YOUR network
- The golden key to stopping ransomware incidents across the board

Let’s Get Started!

Case studies and examples are drawn from our experiences and activities, but do not represent our work for any one customer or set of customers.
In many cases, facts have been changed to obscure the identity of our customers and the associated individuals.

Why Ransomware?

… But why ransomware?

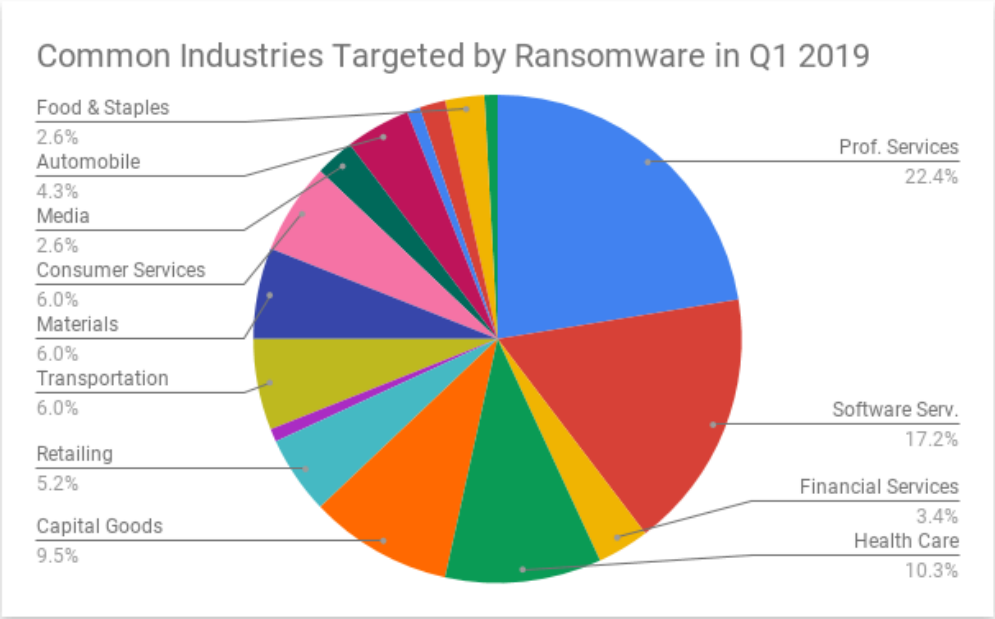
- No zero days.
- It's super successful.
- It's Easy.

What is ransomware?

What is ransomware?

- Ransomware is a type of malware designed to deny access to a computer system or data until a ransom is paid.
- It typically spreads through phishing emails or by unknowingly visiting an infected website.
- Can be commodity variants or targeted events.

How Are These Targeted Attacks Different?



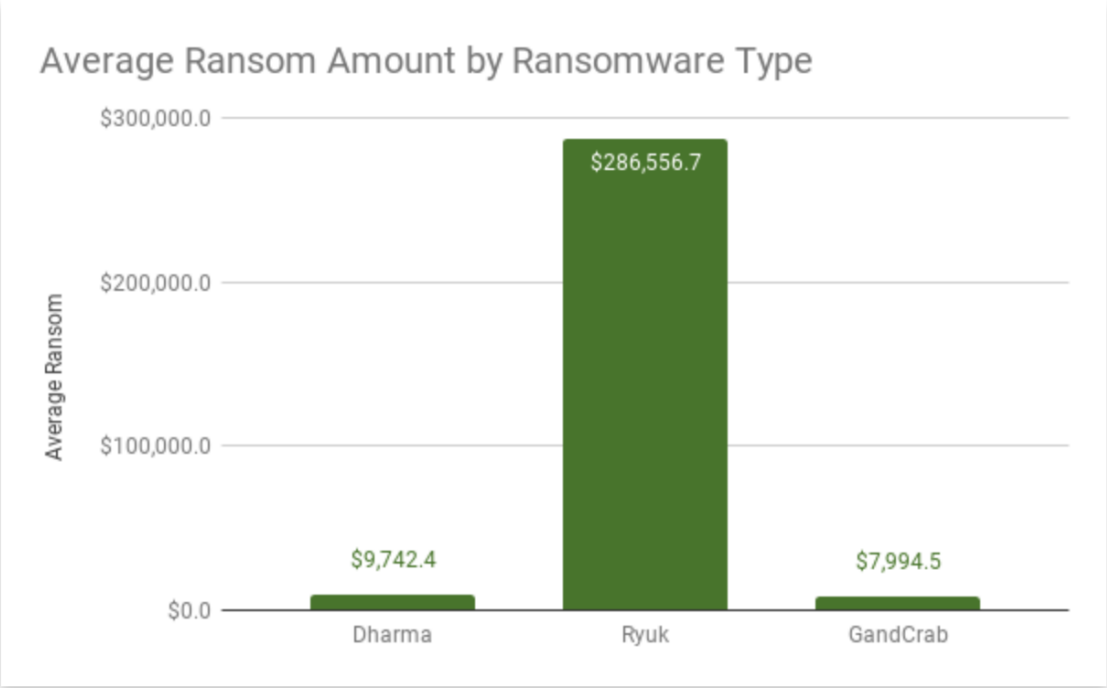
Source: https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

"In Q1 of 2019, the average ransom increased by 89% to $12,762, as compared to $6,733 in Q4 of 2018. The ransom increase reflects increased infections of more expensive types of ransomware such as Ryuk, Bitpaymer, and Ienc rypt. These types of ransomware are predominantly used in bespoke targeted attacks on larger enterprise targets."

-CoveWare

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

Let's talk RYUK



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

To Pay or Not to Pay.

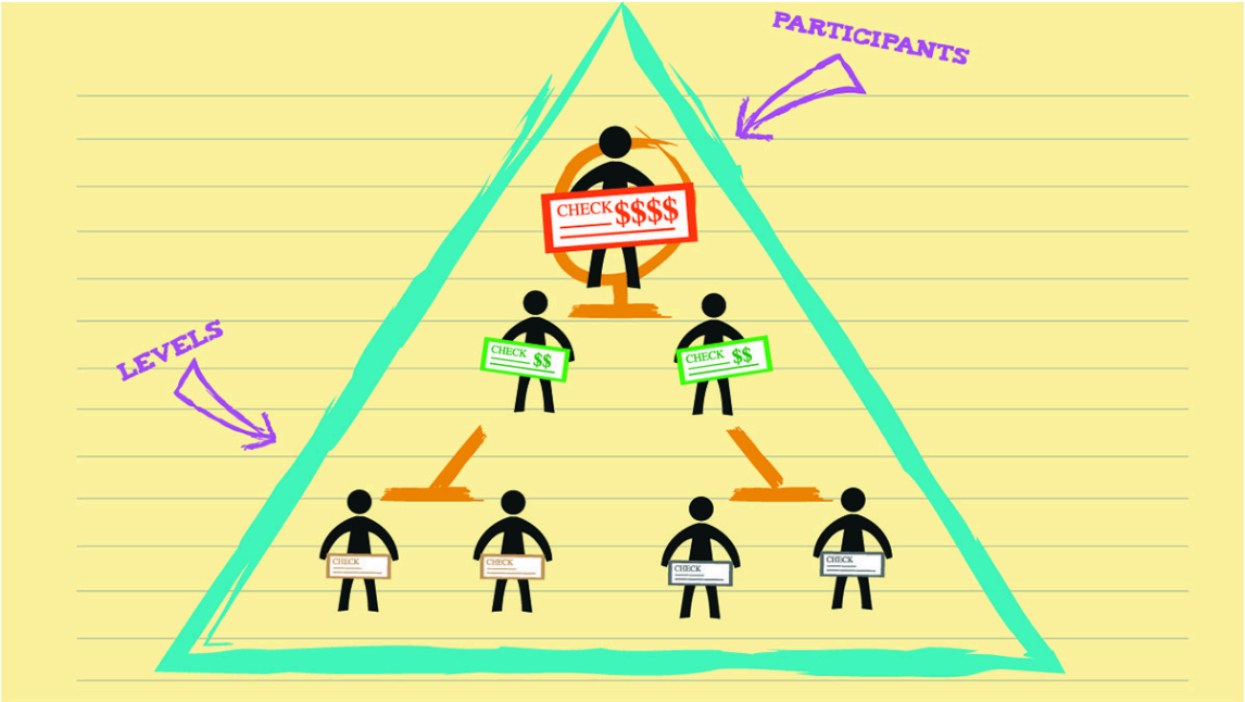
Ransomware Payments

It's a business risk decision.

Questions to consider:

Are there backups to revert to?	Can the environment be rebuilt?	Do we have the ability to pay?

Ransomware Business Model

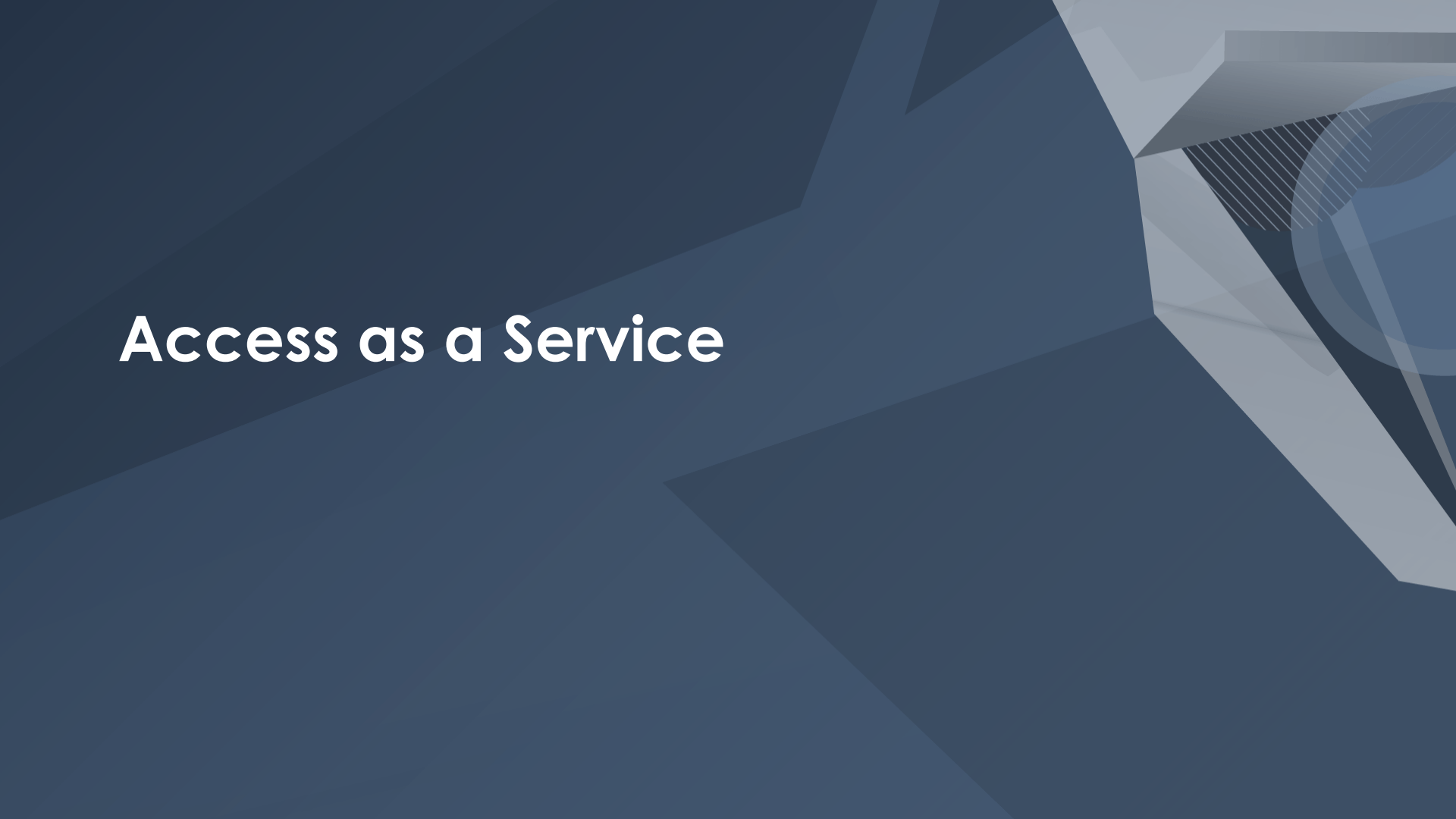


Source: https://abaforlawstudents.com/2015/12/29/aftermath-of-a-ponzi-scheme-collapse/

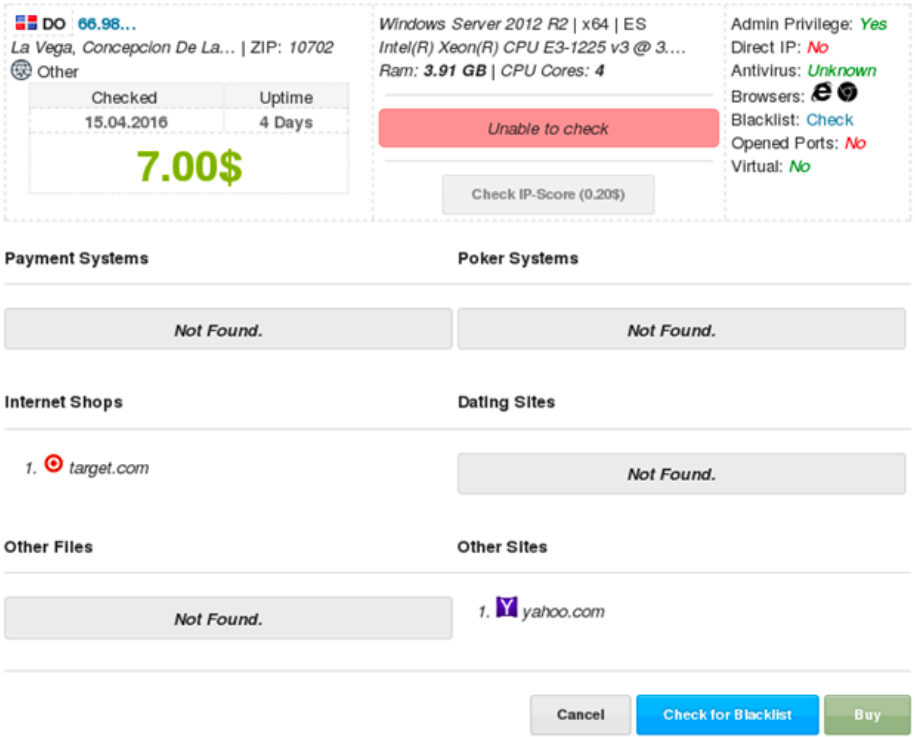
It’s never just ransomware

1. How did they deploy?
2. What accounts were used?
3. How did they get access to that account?
4. What were they able to do with that account?

Access as a Service



Buying access



Source: https://securelist.com/xdedic-the-shady-world-of-hacked-servers-for-sale/75027/

Trick[or treat]bot

- TRICKBOT capabilities
  - Persistent
  - Evades detection
  - Moves laterally
- Without a threat actor “in the environment”
- Deployed through phishing Emails

Take the ~~lazy~~ easy path

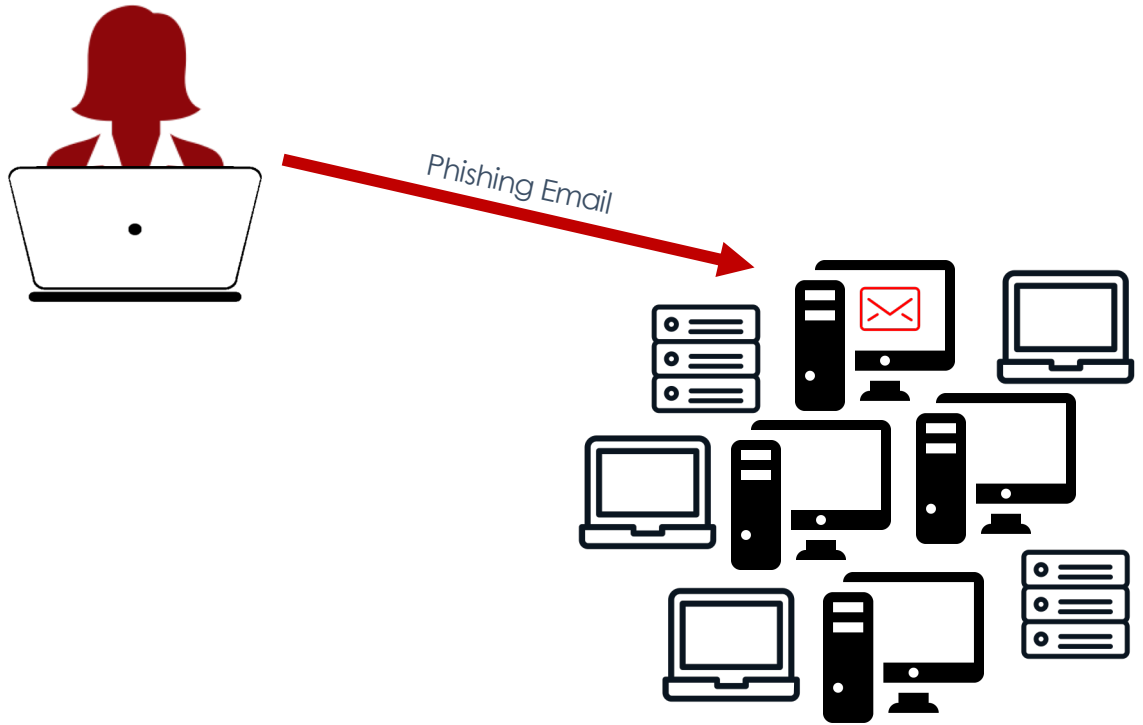
Module	Capability
importDll	Browser Data Stealer Module
InjectDll	Browser Injects Module
mailsearcherDll	Email Address Collection Module
networkDll	Network Reconnaissance Module
NewBCtestDll	Arbitrary Code Execution Module
psfin	Point-of-Sale (POS) Discovery Module
pwgrab	Password Stealer Module
shareDll	Lateral Movement Module
squlDLL	SQL Server Data Collection Module
systeminfo	System Information Gathering Module
tabDll	Lateral Movement Module
vncDll	VNC Remote Desktop Module
wormDll	Monero Miner Module

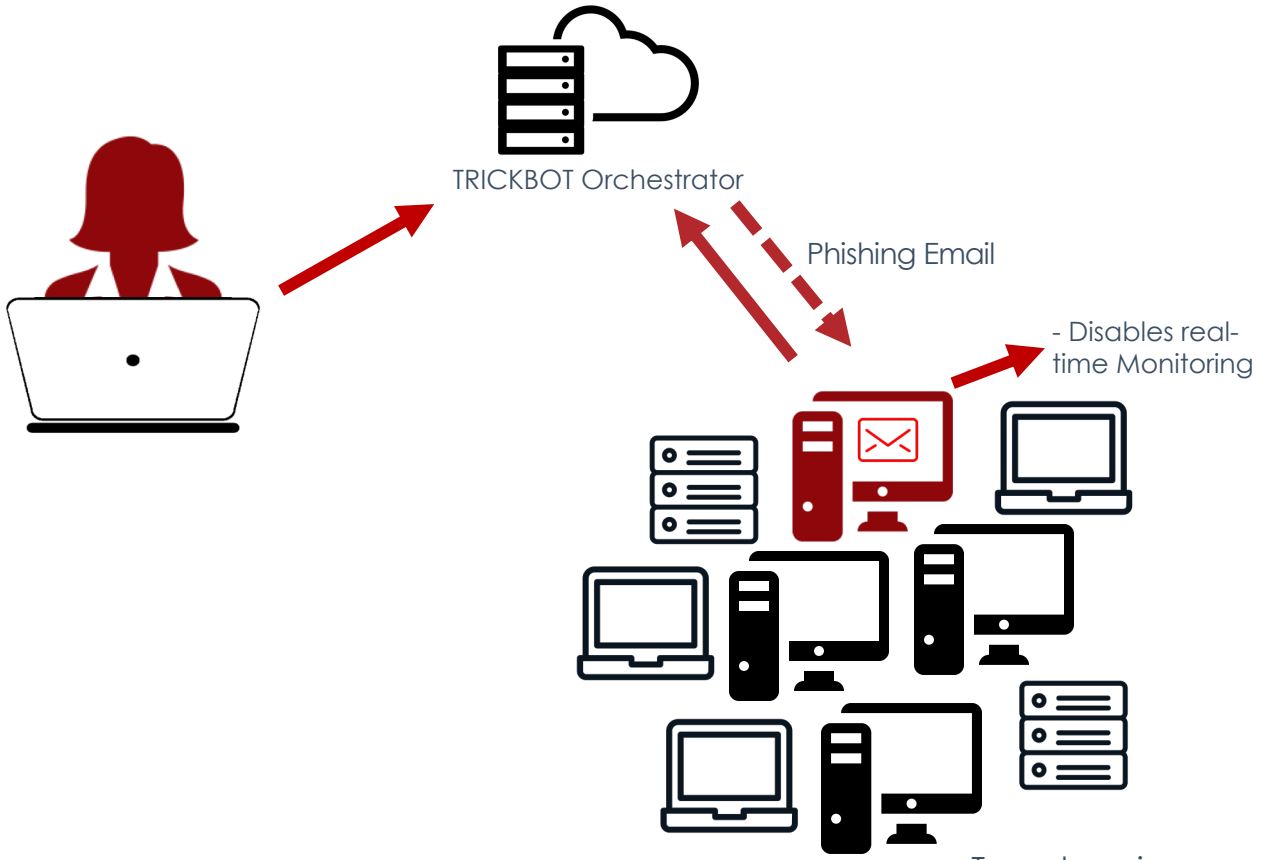
Take the ~~lazy~~ easy path

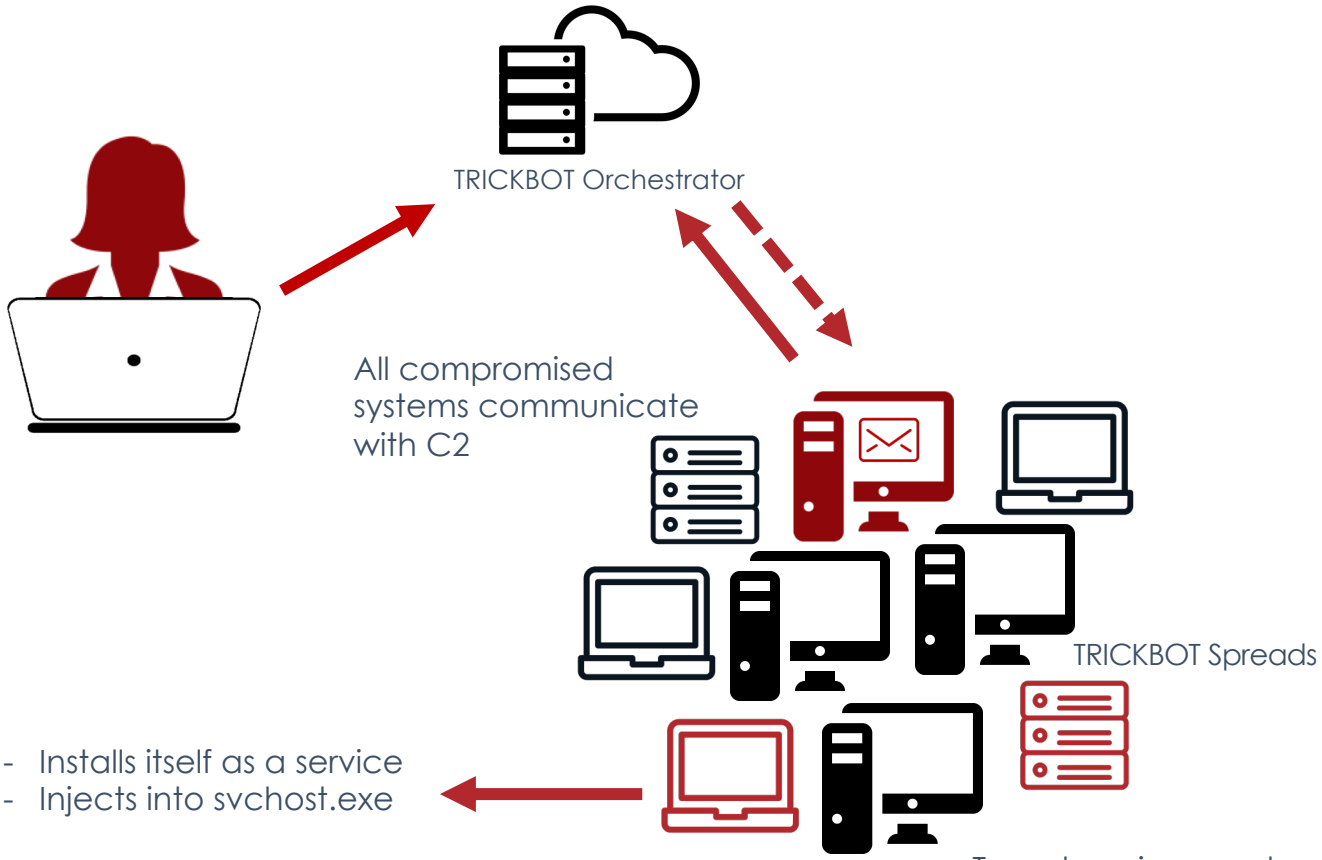
Module	Capability
importDll	Browser Data Stealer Module
InjectDll	Browser Injects Module
mailsearcherDll	Email Address Collection Module
networkDll	Network Reconnaissance Module
NewBCtestDll	**Arbitrary Code Execution Module**
psfin	Point-of-Sale (POS) Discovery Module
pwgrab	Password Stealer Module
shareDll	Lateral Movement Module
squlDLL	SQL Server Data Collection Module
systeminfo	System Information Gathering Module
tabDll	Lateral Movement Module
vncDll	VNC Remote Desktop Module
wormDll	Monero Miner Module

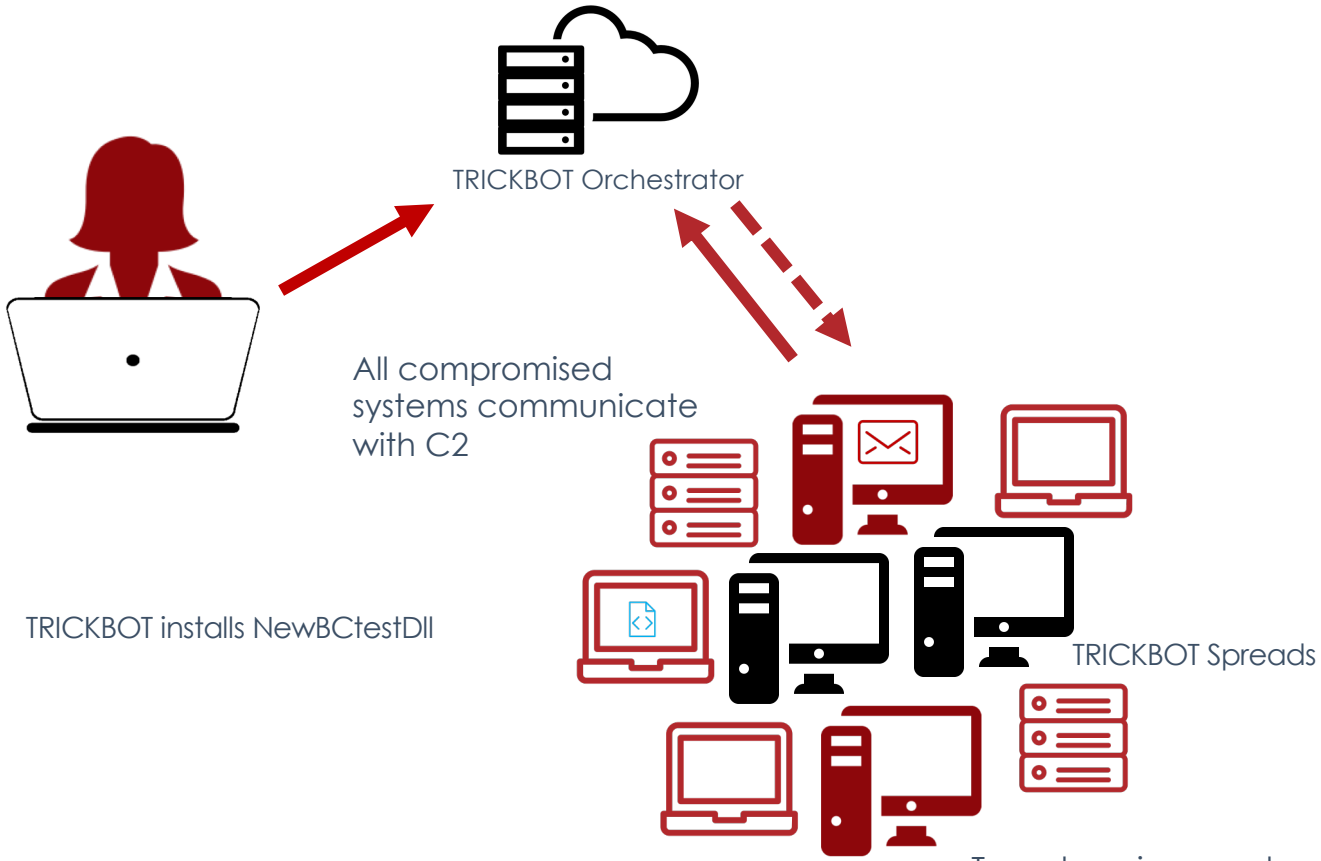
TRICKBOT Used to Provide Continuous Access

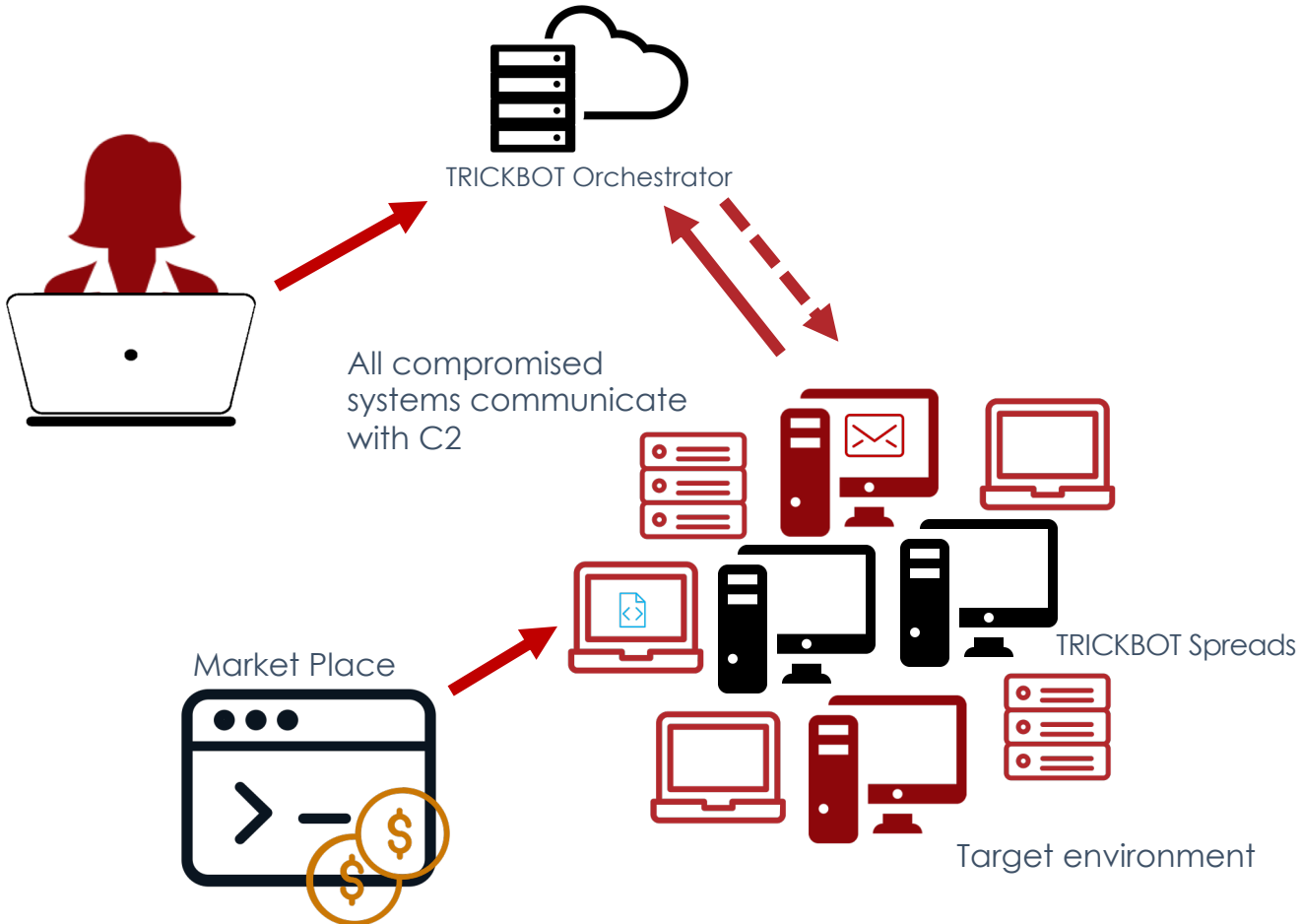
- Threat actors leverage TRICKBOT to download post exploitation frameworks to install additional backdoors.
  - EMPIRE
  - COBALT STRIKE
- Threat actors leverage backdoor access to deploy ransomware

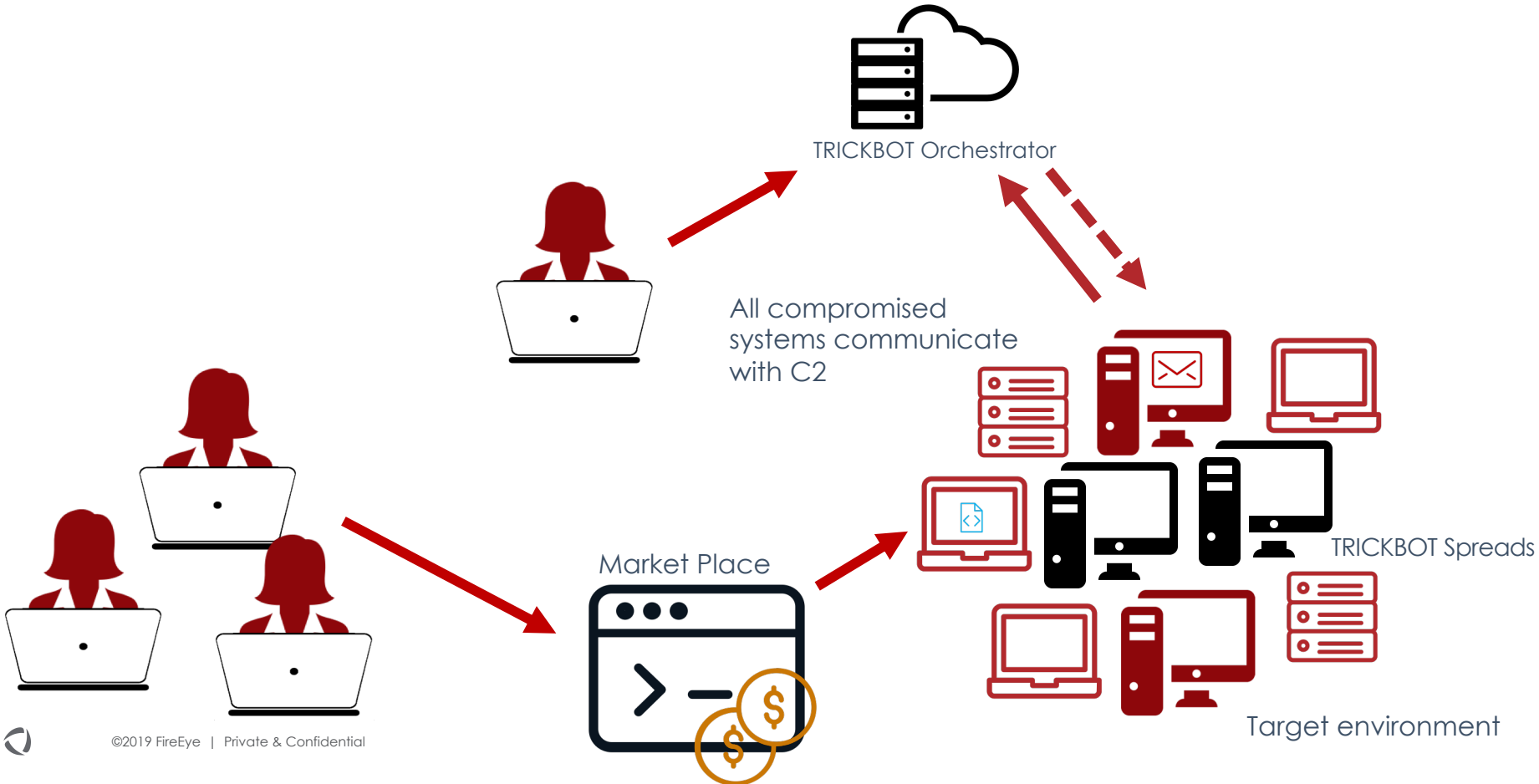


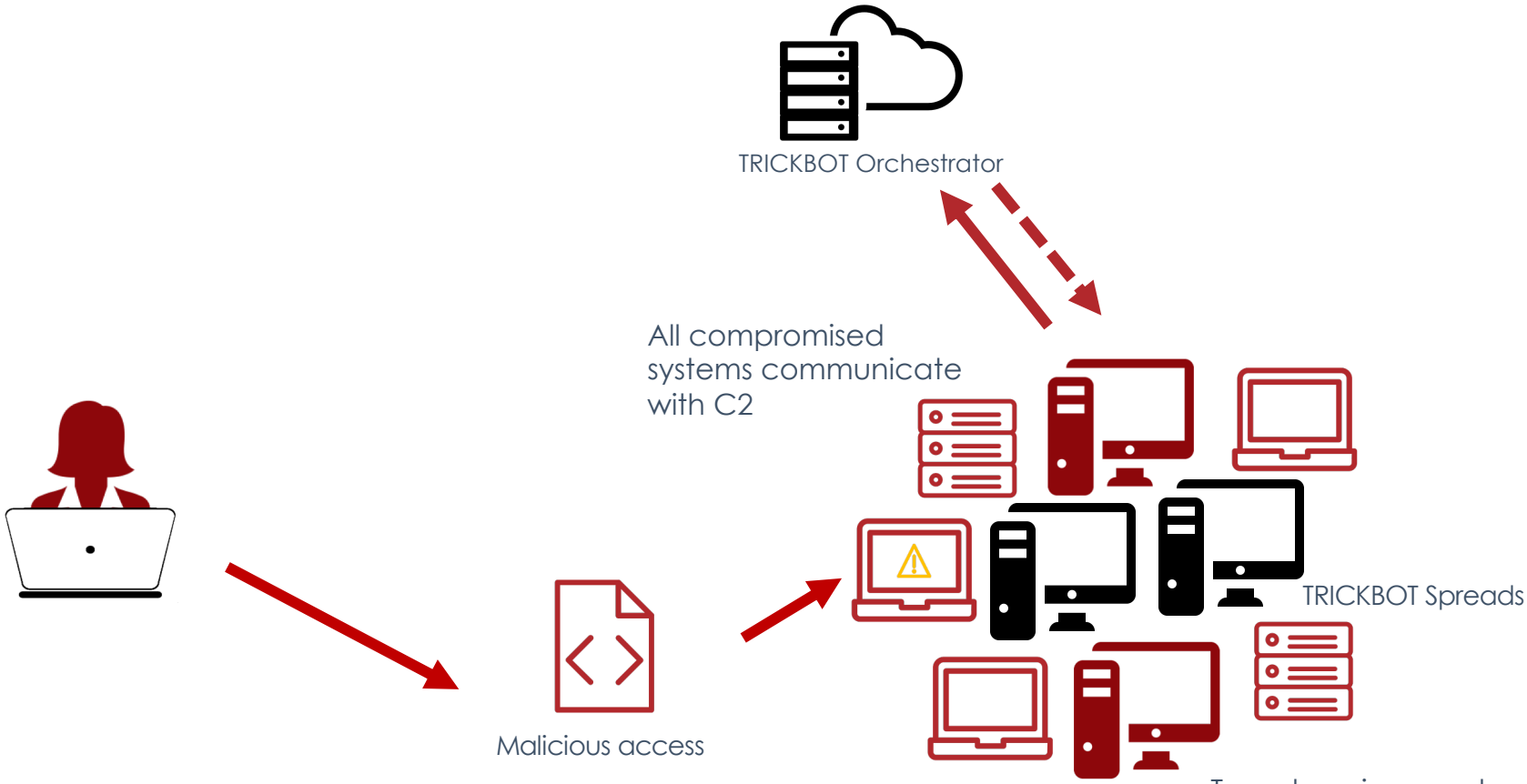


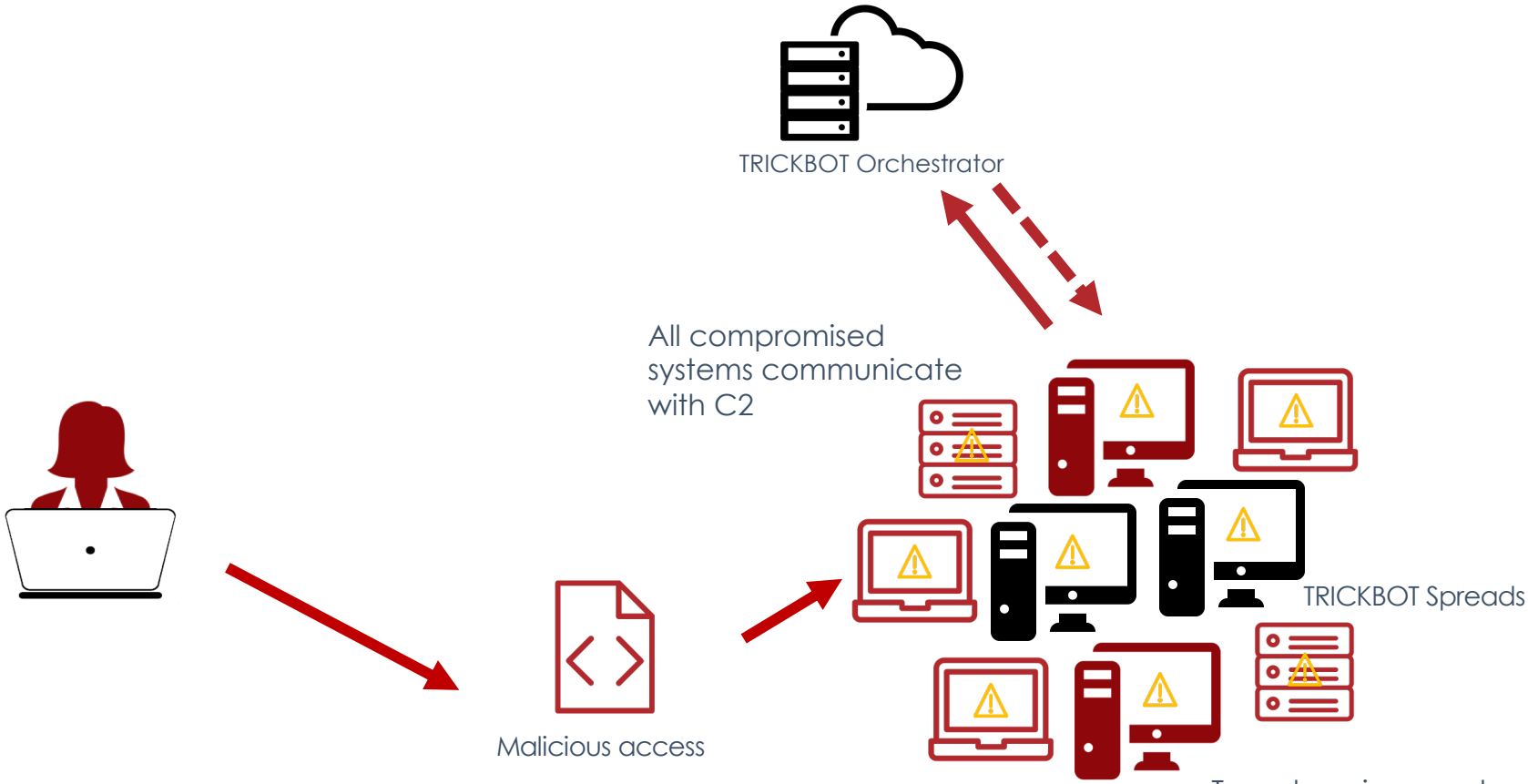












Ransomware

Your network has been penetrated.

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

Backups were either encrypted
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation.
More than a year ago, world experts recognized the impossibility of deciphering by any means except the original decoder.
No decryption software is available in the public.
Antiviruse companies, researchers, IT specialists, and no other persons cant help you encrypt the data.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT DELETE readme files.

To confirm our honest intentions.Send 2 different random files and you will get it decrypted.
It can be from different computers on your network to be sure that one key decrypts everything.
2 files we unlock for free

To get info (decrypt your files) contact us at
<REDACTED><at>protonmail[.]com
or
<REDACTED><at>tutanota[.]com

BTC wallet:
<REDACTED>

Ryuk
No system is safe

#RYuKIDDINGME

```
$ 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\"
```

#RYuKIDDINGME

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

RYuKIDDINGME

```
C:\Users\<USER>\AppData\Local\GroupPolicy\DataStore\0\SysVol\<DOMAIN>\Policies\{122D51C9-1337-41BB-7331-87A9B7984122}\User\Scripts\Logon\<RANSOMWARE>.exe
```

@BlueTeam - It’s preventable

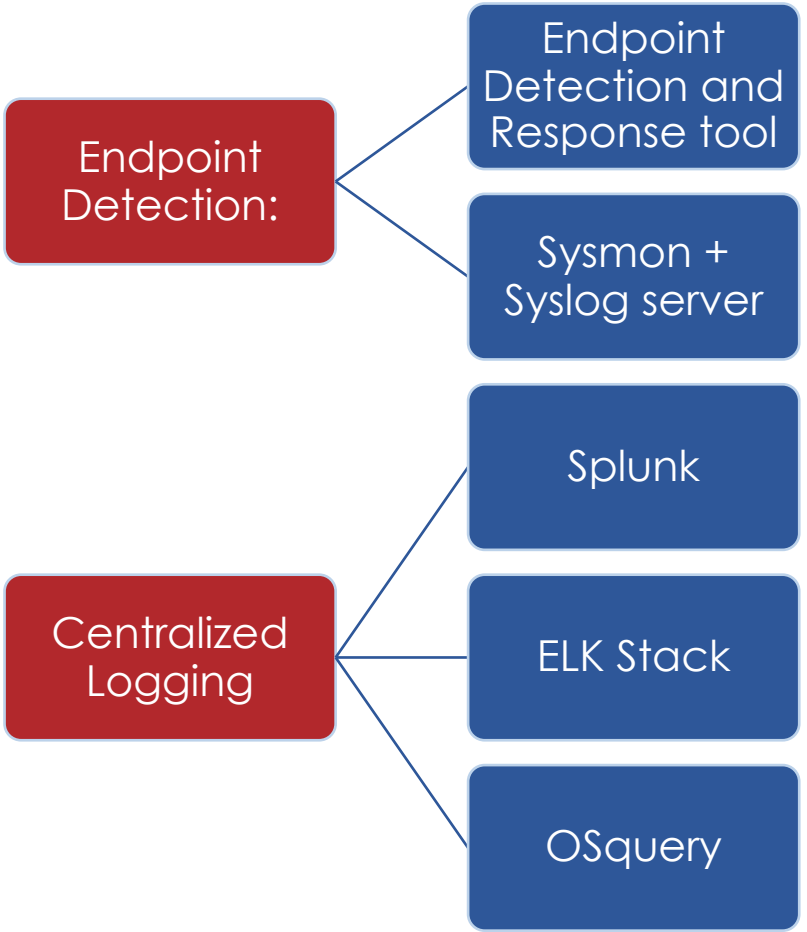
Ransomware Events are Detectable

- Ransomware events are loud.
- TRICKBOT is Loud

DETECTIONS!

- Monitor Event Logs for Services/Tasks created
- Monitor for users created
  - Added to groups (specifically added to admin groups)
- POWERSHELL LOGGING
- Monitor for AV Alerts
  - Users disabling AV
  - “Detection”
  - “Taken Action on”
- TRICKBOT Communication
  - Monitor Ports (TCP) 447 or 449 and/OR (TCP) 443

TOOL ALERT!



Prevention is much easier

- Limit the use of Domain Admin
- Disable Windows "service" accounts
  - "Public" and "Default"
- Disable shares on computers if possible

Key Takeaways

RANSOMWARE IS NOISY, BUT SO IS THE DEPLOYMENT.

RANSOMWARE INCIDENTS ARE HARD TO ATTRIBUTE.

IDENTIFYING THESE FRAMEWORKS IS EASY. CLEANING THEM UP IS HARDER.

OUTSOURCING IT IS HAPPENING MORE AND MORE, HOWEVER THERE IS A HUGE RISK IN DOING SO.

The end.

Contact me: @gigs_security

Check out these tools!

- CyberChef - use the offline mode - https://gchq.github.io/CyberChef/
- Cyber Chef Cheat Sheet - https://gist.github.com/Neo23x0/6af876ee72b51676c82a2db8d2cd3639
- SysMon Config - https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml
- Decode TRICKBOT: https://github.com/hasherezade/malware_analysis/tree/master/trickbot
- Installing ELK: https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04

Additional Resources

- TRICKBOT Modules: https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-shows-off-new-trick-password-grabber-module/
- Awesome Research by the Swiss CERT team: (https://www.govcert.admin.ch/downloads/whitepapers/govcertch_trickbot_analysis.pdf)
- PowerShell Logging: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Ransomware Protection and Containment Strategies: https://www.fireeye.com/blog/threat-research/2019/09/ransomware-protection-and-containment-strategies.html
- EmiSoft: https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/