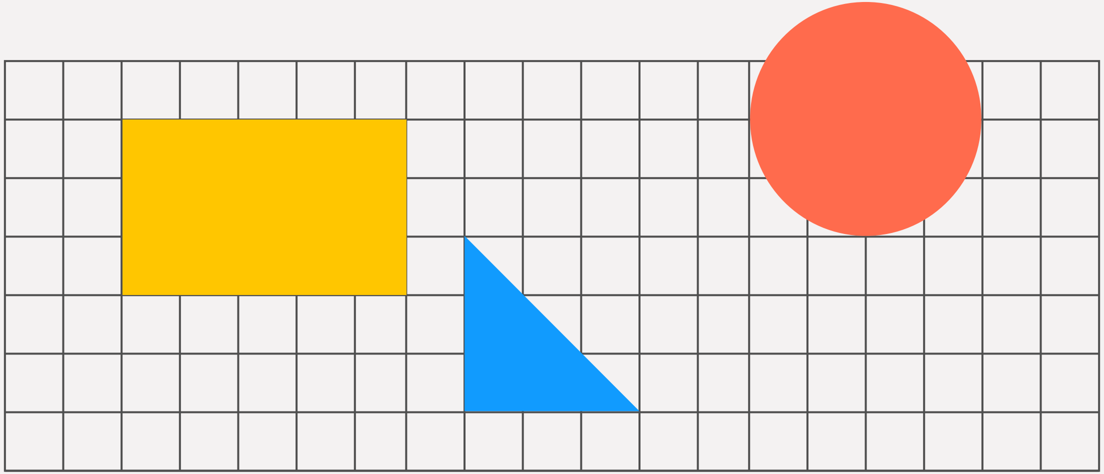
Ransomware Research And Simulation



📁 Lockbit

📁 Wannacry

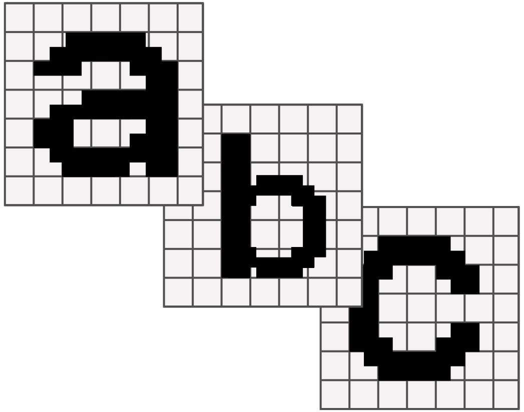
📁 Locky

📁 CryptoLocker

Learning Outcome

Outline

The learning outcome from ransomware research includes a comprehensive understanding of the operational mechanisms, propagation methods, and impacts of ransomware attacks. By studying specific ransomware such as WannaCry and LockBit, individuals gain insights into encryption techniques used by attackers, and the steps required for detection and prevention.



LockBit - Background

- **Evolution**: LockBit is a ransomware that was first identified in 2019 and operates as a Ransomware-as-a-Service **(RaaS) model**. This model allows even non-technical cyber-criminals carry out attacks. Lock It has went through multiple versions (2.0, 3.0, and 4.0), with each incorporating new advanced tactics like **double extortion**, **faster encryption**, and **evasion techniques**.
- **Notable Attacks**: High-profile victims include **Columbus McKinnon**(manufacturer of lifting and rigging equipment), **Accenture** (reportedly $50M ransom demand), and **hospitals**. Started a trend of targeting high-value organizations for large financial and operational damage.
- **Impact**: LockBit's success has **professionalized ransomware** which has lead to the the increase targeting of larger organizations. This has caused a shift of **enhanced cybersecurity** measures to be put in place such as **Zero Trust models**. This evolution of ransomware shows that corporations globally will need to put in more resources to keep up with evolving cyber-threats.
- **Key Features**: LockBit is known for its efficiency with its use of **automated encryption**, **"living off the land"** techniques where it uses legitimate tools and system resources to move within a network, and threatens victims with **data leak sites** to maximize pressure to pay ransom.

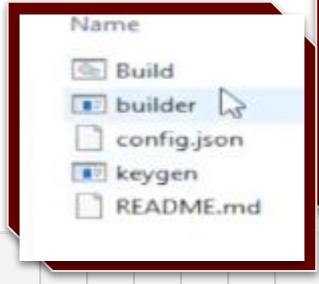
LockBit - Encryption

- **Build:** The **Build.bat** file will “automate the build” process which creates an “instance of ransomware”. “**keygen.exe** generates the public and private encryption keys”. The **config.json** file is used for additional configuration parameter for the attack. The **builder.exe** is “used to generate the different variations of the LockBit 3.0 ransomware by supplying different command line options”, **requires** existing config.json and pub.key/priv.key files generated.
- **Encryption**: Files are encrypted using a combination of **Salsa-20 algorithm** and **1024-bit RSA keys**. During the encryption threads, memory containing the private key is protected with **RtlEncryptMemory** and **RtlDecyptMemory**” so that they are only decrypted when needed.

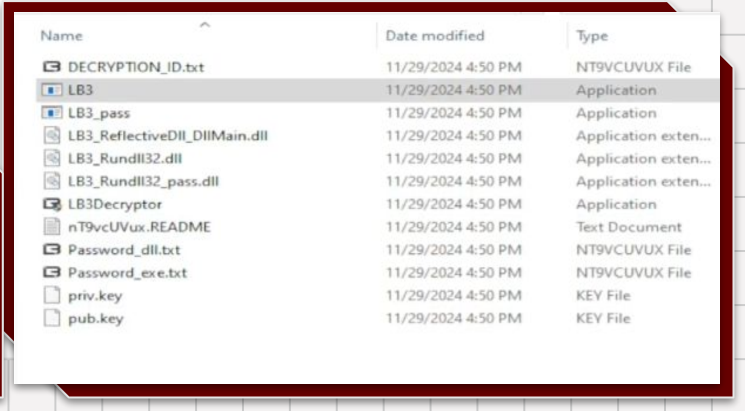
Additional Info:

priv.key – A private encryption key unique to this build that is used to encrypt victim files

pub.key – A public encryption key unique to this build that is used generate various strings that tie this instance of the ransomware to a victim.



Name
Build
builder
config.json
keygen
README.md



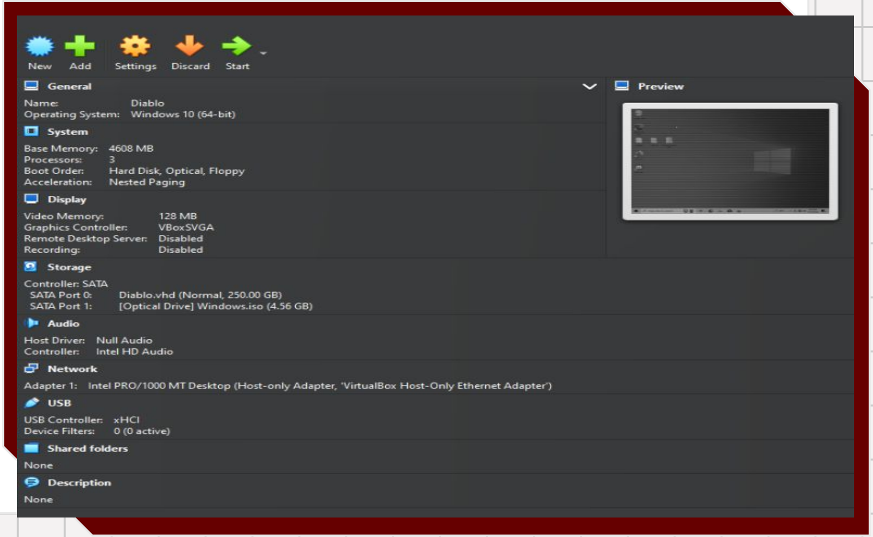
Name	Date modified	Type
DECRYPTION_ID.txt	11/29/2024 4:50 PM	NT9VCUVUX File
LB3	11/29/2024 4:50 PM	Application
LB3_pass	11/29/2024 4:50 PM	Application
LB3_ReflectiveDll_DllMain.dll	11/29/2024 4:50 PM	Application exten...
LB3_Rundll32.dll	11/29/2024 4:50 PM	Application exten...
LB3_Rundll32_pass.dll	11/29/2024 4:50 PM	Application exten...
LB3Decryptor	11/29/2024 4:50 PM	Application
nT9vcUVux.README	11/29/2024 4:50 PM	Text Document
Password_dll.txt	11/29/2024 4:50 PM	NT9VCUVUX File
Password_exe.txt	11/29/2024 4:50 PM	NT9VCUVUX File
priv.key	11/29/2024 4:50 PM	KEY File
pub.key	11/29/2024 4:50 PM	KEY File

LockBit - Delivery Methods

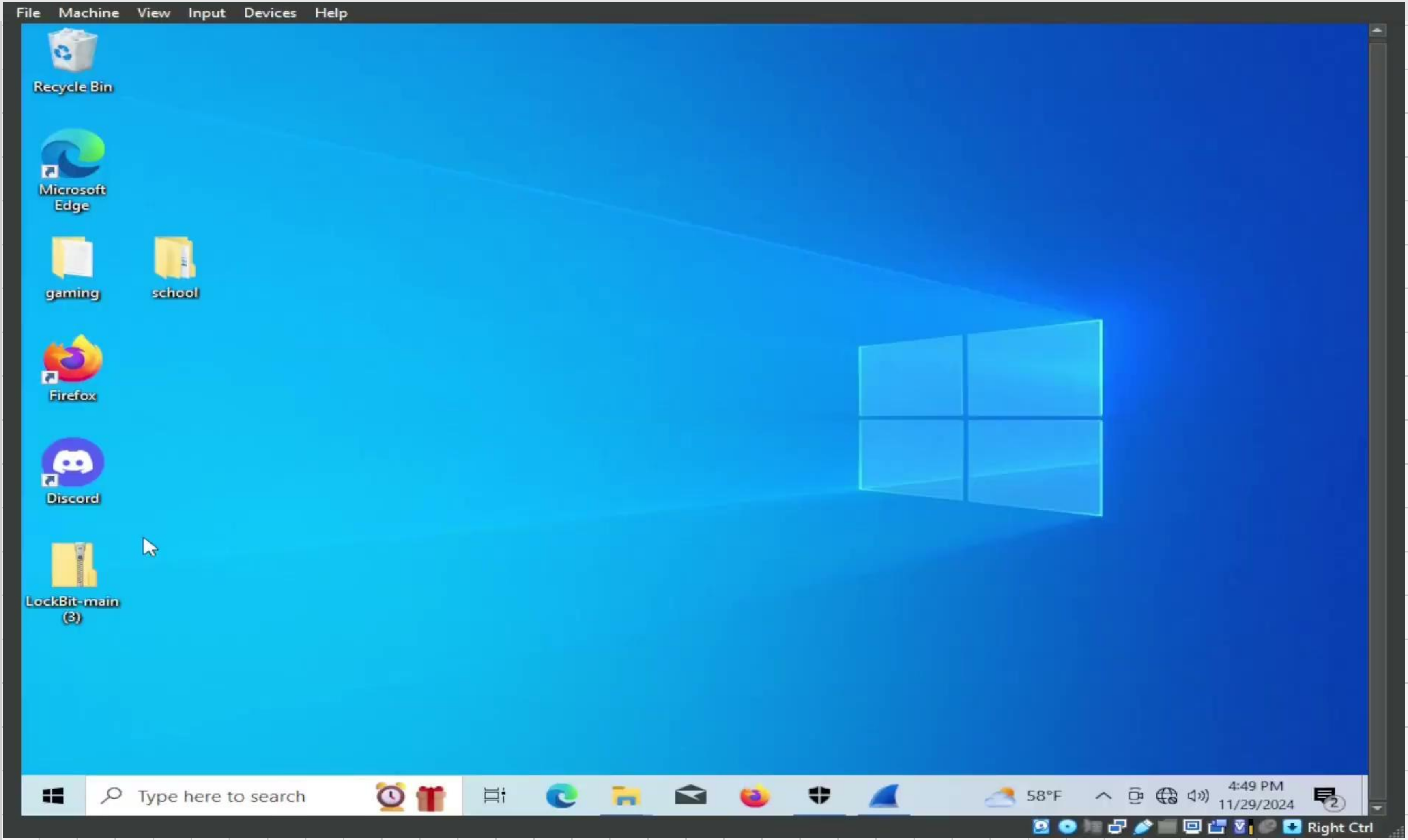
- **Attack Through Remote Desktop Protocol (RDP)**: Source: https://github.com/Tennessene/LockBit
  - *__Requires__ target system to have **RDP enabled** & **port forwarding** on the network
    - **Know the IP address** of your target or obtain it with NMAP
    - Make sure the **port 3389 is open** on the target's network with NMAP
    - Use a **brute force** tool such as Crowbar or Hydra
    - Connect using a client of your choice
    - **Copy the LockBit 3.0** files to the **remote machine** using your client, a cloud service, FTP, or any other method of your choice
    - **Execute Lockbit 3.0**
- **Attack Through Phishing Scheme**:
    - in Word, enter **dev mode** with `Alt+F8`
    - The macro in the guide works, but only for an executable already in the path. An easy way to copy and execute LockBit 3.0 is to **download and run the executable in the macro**.
    - **Send an email containing the document**, and when the **user opens and presses "Enable Editing"**, it should **execute LockBit 3.0**

LockBit - Methodology

- **Environment**: The test was conducted using the Virtualbox Hypervisor and a Windows 10 virtual machine.
- **Settings**: 3 Processors, ~4Gbs of memory, 250Gb of virtual storage, Host-only-Adapter (separates itself from the host network)
- **Setup/ Execution**:
  - ➢ Setup configurations of the virtual machine
  - ➢ Download lockbit and wireshark for further analysis
  - ➢ Configure lockbits settings,optional:
    - ■ Parameters & Keys
  - ➢ Run LB3 and analyze encryption process
  - ➢ Test the decryption executable provided

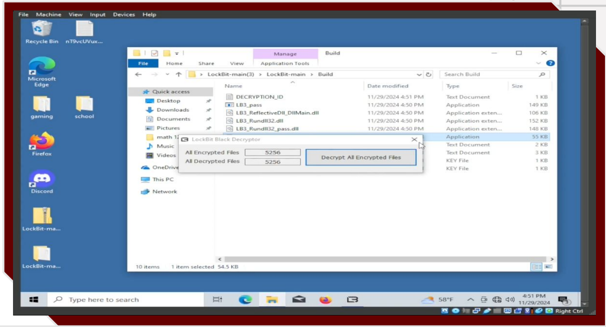


```
General
Name:               Diablo
Operating System:   Windows 10 (64-bit)
System
Base Memory:    4608 MB
Processors:     3
Boot Order:     Hard Disk, Optical, Floppy
Acceleration:   Nested Paging
Display
Video Memory:             128 MB
Graphics Controller:      VBoxSVGA
Remote Desktop Server:    Disabled
Recording:                Disabled
Storage
Controller: SATA
 SATA Port 0:     Diablo.vhd (Normal, 250.00 GB)
 SATA Port 1:     [Optical Drive] Windows.iso (4.56 GB)
Audio
Host Driver:   Null Audio
Controller:    Intel HD Audio
Network
Adapter 1:   Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')
USB
USB Controller:   xHCI
Device Filters:   0 (0 active)
Shared folders
None
Description
None
```


File
Machine
View
Input
Devices
Help
Recycle Bin
Microsoft Edge
gaming
school
Firefox
Discord
LockBit-main (3)
Type here to search
58°F
4:49 PM
11/29/2024
Right Ctrl

LockBit - Results

- The simulation was **successfully** able to show how **easily Lockbit** can be **set up and configured**.
- Executing the ransomware took **longer than anticipated** to encrypt files but is likely to do with it using **1024-bit RSA keys** which compared to other ransomware is not as efficient which you can see later this presentation.
- During encryption **programs are forced closed**, in my case wireshark. This seems to **persist until decryption**. Strange as I changed config file to disable program/service shutdown.
- The LB3Decryptor.exe did **successfully decrypt files** and on the surface level operations seemed to be resumed as normal such as wireshark.
- One notable change was that any files in the **recycle bin will be deleted** and won't be restored even after decryption.



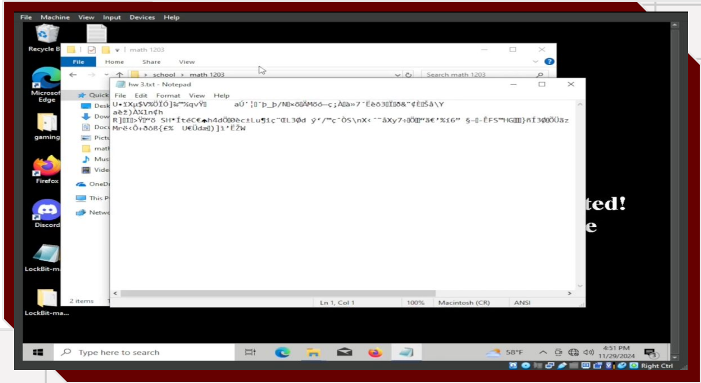
Name	Date modified	Type	Size
DECRYPTION_ID	11/29/2024 4:51 PM	Text Document	1 KB
LB3_pass	11/29/2024 4:50 PM	Application	149 KB
LB3_ReflectiveDll_DllMain.dll	11/29/2024 4:50 PM	Application exten...	106 KB
LB3_Rundll32.dll	11/29/2024 4:50 PM	Application exten...	152 KB
LB3_Rundll32_pass.dll	11/29/2024 4:50 PM	Application exten...	148 KB
		Application	55 KB
		Text Document	2 KB
		Text Document	3 KB
		KEY File	1 KB
		KEY File	1 KB

10 items 1 item selected 54.5 KB

LockBit Black Decryptor

All Encrypted Files: 5256
All Decrypted Files: 5256

Decrypt All Encrypted Files



hw 3.txt - Notepad

File Edit Format View Help

```
U•ĭXµ$V%ÖÏÓ]‰™%qvŸ       aÚ'¦´þ_þ/N×öÄMöó–ç;Àà»7´Ëèô3Ïð&"¢ÈŠâ\Y
aèž)À%1n¢h
R]I>Ÿ"ö SH*ÎtéC€h4dÖ0èc±Lu¶iç¨ŒL3Ød ý'/™ç˜ÒS\nX‹´˜âXy7÷Ö"ã€'%í6" §–-ÊFS™HG}ñÍ3ØÕÜãz
Mrë‹Ô+ðôß{£%  U€Üdæ)]ì'ËŽW
```

Ln 1, Col 1 100% Macintosh (CR) ANSI

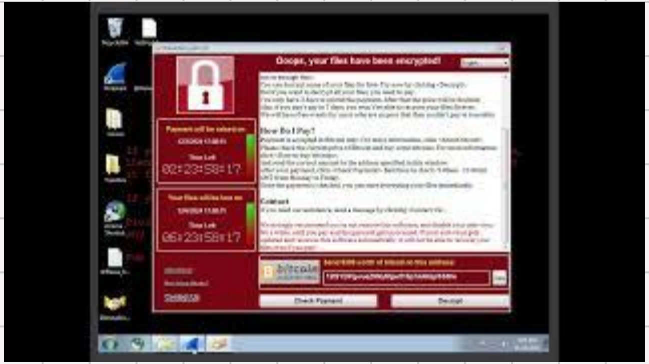
WannaCry - Background

- **Emergence**: WannaCry ransomware was first detected in May 2017 and caused a global outbreak within days.
- **Propagation**: It exploited a vulnerability in Microsoft Windows systems (EternalBlue) and included a worm component, enabling rapid self-propagation across networks.
- **Notable Attacks**: High-profile victims included the UK's National Health Service (NHS), Telefónica in Spain, and FedEx. The attack disrupted critical services, leading to significant operational and financial losses.
- **Impact**: WannaCry infected over 230,000 computers in more than 150 countries within its first week, with damages estimated to exceed $4 billion globally.
- **Key Features**: Utilized asymmetric encryption to lock files and demanded Bitcoin payments for decryption keys. A "kill switch" was discovered, slowing the spread but leaving lasting impacts on affected systems.

WannaCry - Encryption and Delivery

- **Encryption Methods**: Utilized a combination of AES-128 and RSA-2048 encryption to lock files. The AES key encrypts the data, and the RSA key encrypts the AES key, making decryption impossible without the private RSA key.
- **Targeted Files**: Scanned for files with specific extensions (.doc, .jpg, .mp4, etc.) to maximize impact and disrupt business operations.
- **Delivery Mechanism**: Exploited the **EternalBlue** vulnerability in Microsoft Windows systems, a leaked NSA exploit, to spread rapidly across unpatched machines.
- **Propagation**: Included a worm component, enabling it to spread autonomously to other devices on the same network, escalating its impact.
- **C2 Communication**: Sent encrypted data and ransom demands to its Command and Control (C2) server, awaiting Bitcoin payments for the decryption key.

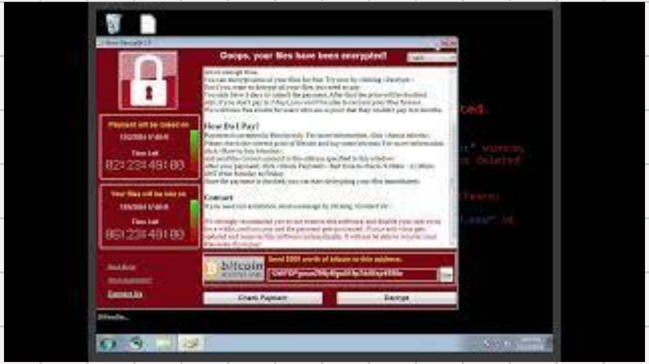
WannaCry - Simulation Process



Ooops, your files have been encrypted!

How Do I Pay?

Contact



Ooops, your files have been encrypted!

How Do I Pay?

Contact

WannaCry - Simulation Result

- **Setup and Execution**:
The ransomware was downloaded and executed in a Windows 7 VM environment set up using VMOracle. The setup included file transfers and basic network connectivity via a lightweight Chromium-based browser (Supermium). Execution required bypassing a typical “unverified publisher” warning.

- **File Encryption**:
The ransomware immediately encrypted a set of pre-loaded files on the VM. The encryption process targeted specific file types (e.g., .docx, .jpg) while leaving certain system files untouched, ensuring the system remained operational. Files were renamed with a `.WNCRY` extension, rendering them inaccessible without decryption.

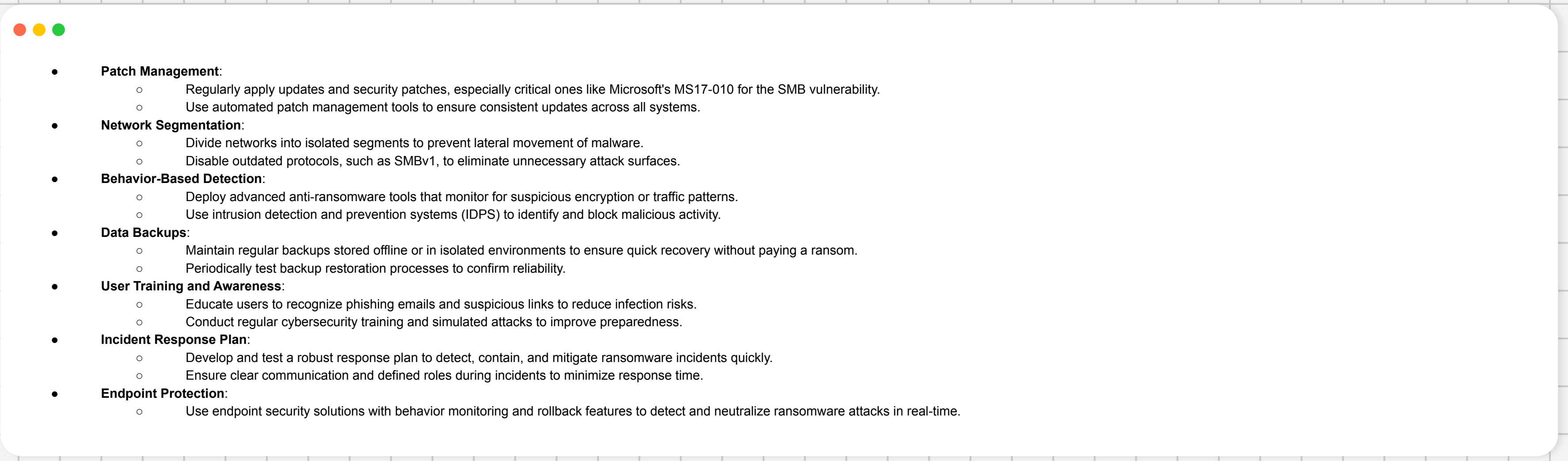
- **Network Traffic**:
Wireshark captured unusual SMB traffic during execution, including malformed commands like "TreeConnectAndX" and "WriteAndX". The ransomware also made repeated DNS queries to a hardcoded domain (`iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com`) and initiated TLSv1.3 traffic, indicating possible server communication attempts.

- **Impact on System**:
The desktop wallpaper was altered to display the ransom note, and a Bitcoin payment window popped up, guiding victims to purchase Bitcoin for decryption. The ransomware also generated “@Please_Read_Me@” files explaining the situation.

- **Extended Effects**:
Injecting a USB drive into the infected VM showed that WannaCry actively encrypted files on external devices, proving its ability to propagate beyond the initial infection point.

- **Anomalies Observed**:
While WannaCry attempted communication with external servers, no decryption process could be tested as this relied on actual ransomware server responses. Some files, such as `.JSON` and `.pcapng`, were left unencrypted, likely to maintain system functionality.

WannaCry - Prevention / Defense



- **Patch Management**:
  - Regularly apply updates and security patches, especially critical ones like Microsoft's MS17-010 for the SMB vulnerability.
  - Use automated patch management tools to ensure consistent updates across all systems.
- **Network Segmentation**:
  - Divide networks into isolated segments to prevent lateral movement of malware.
  - Disable outdated protocols, such as SMBv1, to eliminate unnecessary attack surfaces.
- **Behavior-Based Detection**:
  - Deploy advanced anti-ransomware tools that monitor for suspicious encryption or traffic patterns.
  - Use intrusion detection and prevention systems (IDPS) to identify and block malicious activity.
- **Data Backups**:
  - Maintain regular backups stored offline or in isolated environments to ensure quick recovery without paying a ransom.
  - Periodically test backup restoration processes to confirm reliability.
- **User Training and Awareness**:
  - Educate users to recognize phishing emails and suspicious links to reduce infection risks.
  - Conduct regular cybersecurity training and simulated attacks to improve preparedness.
- **Incident Response Plan**:
  - Develop and test a robust response plan to detect, contain, and mitigate ransomware incidents quickly.
  - Ensure clear communication and defined roles during incidents to minimize response time.
- **Endpoint Protection**:
  - Use endpoint security solutions with behavior monitoring and rollback features to detect and neutralize ransomware attacks in real-time.

Locky- Background

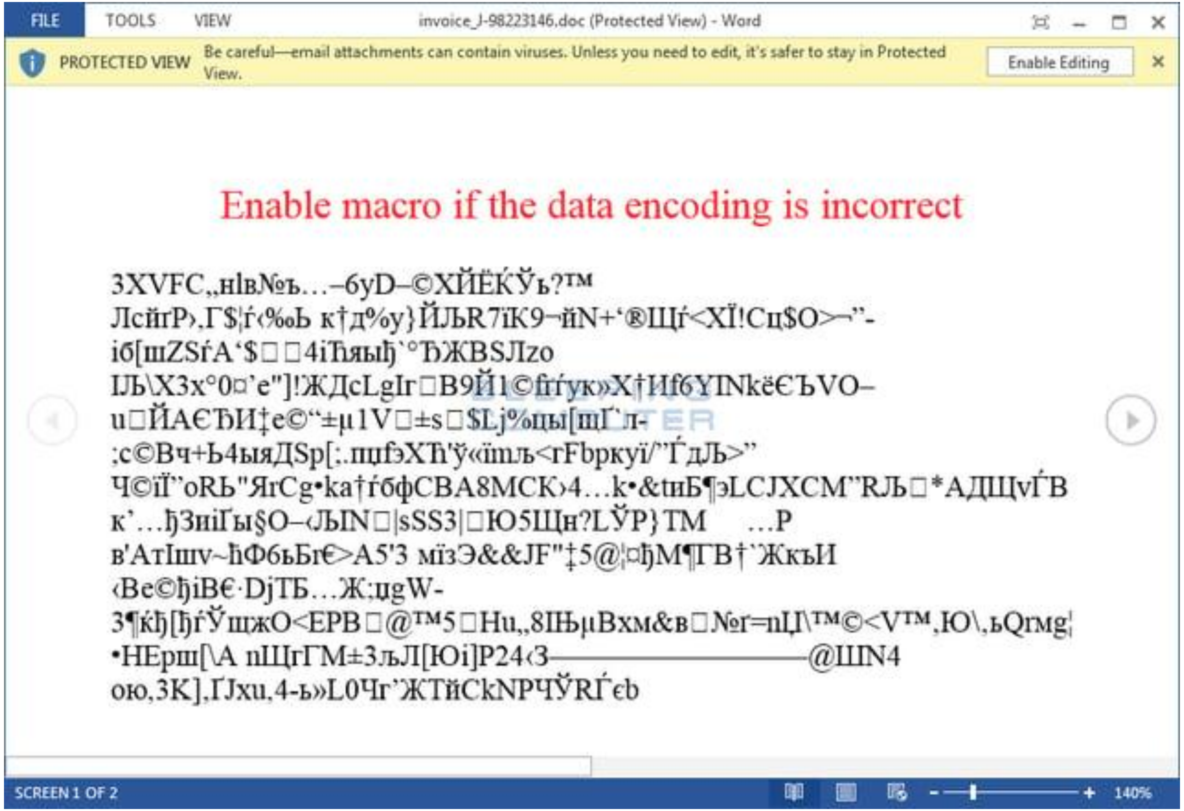
- Locky ransomware emerged in early 2016
- Locky was particularly notable for its rapid evolution, adding new features and obfuscation techniques to evade detection.
- It primarily targeted businesses and individuals globally, causing widespread disruption during its peak.
- It hit places such as Hollywood Presbyterian Medical Center, and Dartford Science & Technology College.

Locky - Encryption and Delivery

- The original version of Locky, appended the ".locky" extension to encrypted files and employed RSA-2048 and AES-128 encryption
- It first scans for any for files with certain extension to encrypt, such as .docx and .xlsx.
- It uses the AES-128 to encrypt these files and then the AES key is encrypted using RSA-2048's that are generated in every infection
- The private key that is required to decrypt the AES key is stored in the C2, Command and Control, Server which is a server ran by the attacker
- The Encrypted AES Key is then sent to the C2 Server and is only decrypted there where it waits for the ransom to be delivered before sending the decrypted key.

Locky - Encryption and Delivery

- Main method of Delivery for Locky was through social engineering, primary phishing emails.
- In these emails a document is attached which contains a macro which when macro is enabled it will execute the Locky encryption process.
- It kept evolving its delivery method and started using .docm and .js file disguised as .zip files and so on.
- Locky itself also kept evolving and had many variation created such as Zepto, Odin, Diablo6
- These variants were made for different reasons such as: evading detection, targeting new victims and adapting to defenses



Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

Enable macro if the data encoding is incorrect

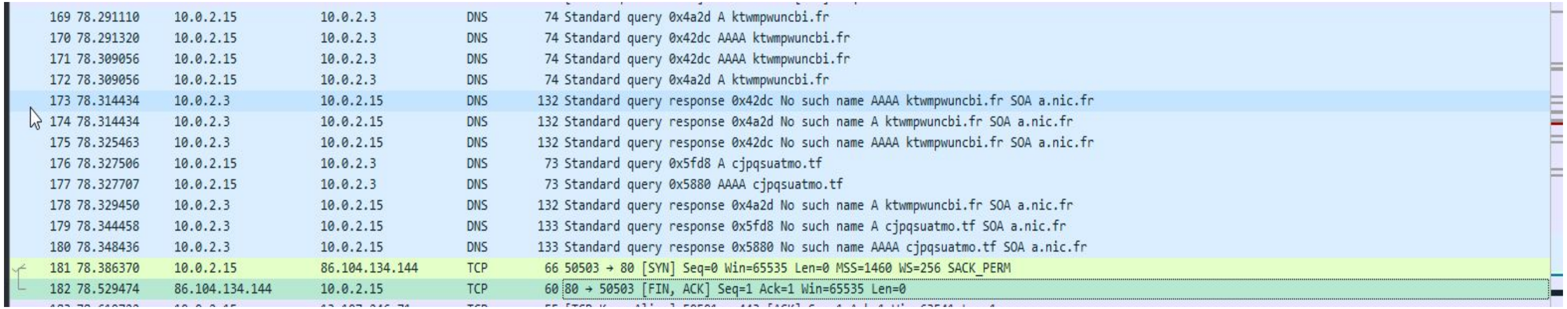
3XVFC„нlв№ъ…–6yD–©ХЙЁЌЎь?™
ЛсйгР›,Г$¦ѓ‹‰Ь к†д%у}ЙЉR7iK9¬йN+‘®Щѓ<XЇ!Сц$O>¬”-
iб[шZSѓА‘$□□4iЋяыђ`°ЂЖBSЛzo
ЏЉ\X3x°0¤’e"]!ЖДсLgІг□В9Й1©fгѓук»Х†Иf6YINkёЄЪVO–
u□ЙАЄЂИ‡е©“±µ1V□±s□$Lj%цы[шҐ`л-
;с©Вч+Ь4ыяДSp[;.пџfэXЋ'ў«imљ<гFbркуї/”ЃдЉ>”
Ч©ії”oRЬ"ЯгCg•ka†ѓбфCBA8MCK›4…k•&tиБ¶эLCJXCM”RЉ□*АДЩvЃВ
к’…ђЗиіҐы§O–‹ЉIN□|sSS3|□Ю5Щн?LЎР}ТМ …Р
в'АтІшv~ћФ6ьБгЄ>А5'3 мїзЭ&&JF"‡5@¦¤ђМ¶ГВ†`ЖкъИ
‹Ве©ђіВЄ·DjТБ…Ж;џgW-
3¶ќђ[ђѓЎщжО<ЕРВ□@™5□Hu„8IЊµВхм&в□№г=пЏ\™©<V™,Ю\,ьQгмg¦
•НЕрш[\А пЩгГМ±3љЛ[Юі]Р24‹З————————@ШN4
ою,3K],ҐJxu,4-ь»L0Чг’ЖТйCkNРЧЎRҐєb

Locky - Simulation Process

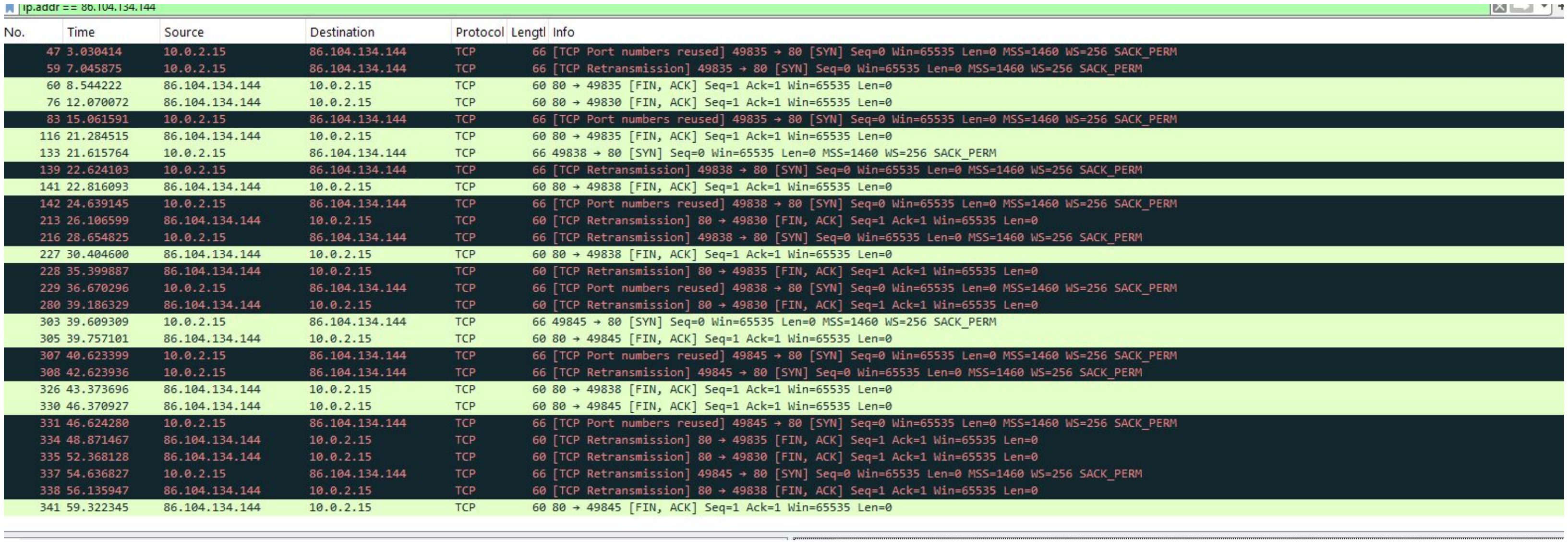
- Used VMware as the VM manager
- Tried two different Window images, 10 and 7
- Downloaded multiple different locky malware executables from the internet
- Took a snapshot of the VM for quick restoration after testing.
- Monitored network using Wireshark while the locky was running
- Monitored what the locky.exe process was attempting to do with sysmon

Locky- Simulation Result

- Locky was not be able to successfully be simulated in the VM environment,
- This was most likely due to not having a fully successful communication with the C2 Server it was trying to communicate with.
- It tried to communicate with a DNS using its built in DGA generator.
- It failed and tried its built in hard coded IP address ,
- It keeps trying to establish a connection with the IP address, but it refuses and FIN, ACK are sent by the server.
- Without a proper communication it seems like Locky did not attempt to encrypt any files in the VM.

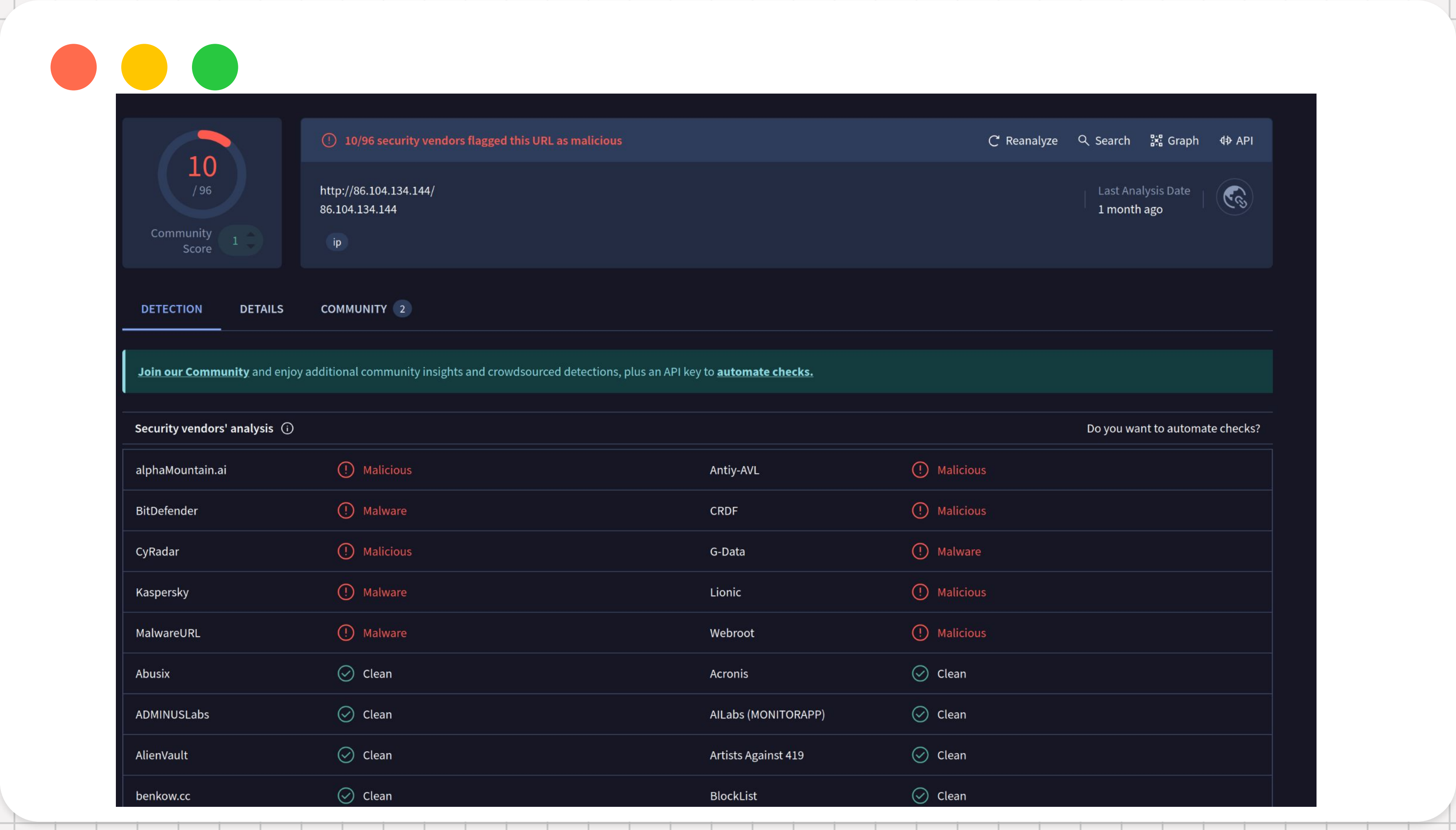


```
169 78.291110   10.0.2.15       10.0.2.3        DNS       74 Standard query 0x4a2d A ktwmpwuncbi.fr
170 78.291320   10.0.2.15       10.0.2.3        DNS       74 Standard query 0x42dc AAAA ktwmpwuncbi.fr
171 78.309056   10.0.2.15       10.0.2.3        DNS       74 Standard query 0x42dc AAAA ktwmpwuncbi.fr
172 78.309056   10.0.2.15       10.0.2.3        DNS       74 Standard query 0x4a2d A ktwmpwuncbi.fr
173 78.314434   10.0.2.3        10.0.2.15       DNS      132 Standard query response 0x42dc No such name AAAA ktwmpwuncbi.fr SOA a.nic.fr
174 78.314434   10.0.2.3        10.0.2.15       DNS      132 Standard query response 0x4a2d No such name A ktwmpwuncbi.fr SOA a.nic.fr
175 78.325463   10.0.2.3        10.0.2.15       DNS      132 Standard query response 0x42dc No such name AAAA ktwmpwuncbi.fr SOA a.nic.fr
176 78.327506   10.0.2.15       10.0.2.3        DNS       73 Standard query 0x5fd8 A cjpqsuatmo.tf
177 78.327707   10.0.2.15       10.0.2.3        DNS       73 Standard query 0x5880 AAAA cjpqsuatmo.tf
178 78.329450   10.0.2.3        10.0.2.15       DNS      132 Standard query response 0x4a2d No such name A ktwmpwuncbi.fr SOA a.nic.fr
179 78.344458   10.0.2.3        10.0.2.15       DNS      133 Standard query response 0x5fd8 No such name A cjpqsuatmo.tf SOA a.nic.fr
180 78.348436   10.0.2.3        10.0.2.15       DNS      133 Standard query response 0x5880 No such name AAAA cjpqsuatmo.tf SOA a.nic.fr
181 78.386370   10.0.2.15       86.104.134.144  TCP       66 50503 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
182 78.529474   86.104.134.144  10.0.2.15       TCP       60 80 → 50503 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
```



```
ip.addr == 86.104.134.144

No.  Time       Source          Destination     Protocol Lengtl Info
  47 3.030414   10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49835 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  59 7.045875   10.0.2.15       86.104.134.144  TCP        66 [TCP Retransmission] 49835 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  60 8.544222   86.104.134.144  10.0.2.15       TCP        60 80 → 49835 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
  76 12.070072  86.104.134.144  10.0.2.15       TCP        60 80 → 49830 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
  83 15.061591  10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49835 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 116 21.284515  86.104.134.144  10.0.2.15       TCP        60 80 → 49835 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 133 21.615764  10.0.2.15       86.104.134.144  TCP        66 49838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 139 22.624103  10.0.2.15       86.104.134.144  TCP        66 [TCP Retransmission] 49838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 141 22.816093  86.104.134.144  10.0.2.15       TCP        60 80 → 49838 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 142 24.639145  10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 213 26.106599  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49830 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 216 28.654825  10.0.2.15       86.104.134.144  TCP        66 [TCP Retransmission] 49838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 227 30.404600  86.104.134.144  10.0.2.15       TCP        60 80 → 49838 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 228 35.399887  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49835 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 229 36.670296  10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49838 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 280 39.186329  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49830 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 303 39.609309  10.0.2.15       86.104.134.144  TCP        66 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 305 39.757101  86.104.134.144  10.0.2.15       TCP        60 80 → 49845 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 307 40.623399  10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 308 42.623936  10.0.2.15       86.104.134.144  TCP        66 [TCP Retransmission] 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 326 43.373696  86.104.134.144  10.0.2.15       TCP        60 80 → 49838 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 330 46.370927  86.104.134.144  10.0.2.15       TCP        60 80 → 49845 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 331 46.624280  10.0.2.15       86.104.134.144  TCP        66 [TCP Port numbers reused] 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 334 48.871467  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49835 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 335 52.368128  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49830 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 337 54.636827  10.0.2.15       86.104.134.144  TCP        66 [TCP Retransmission] 49845 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 338 56.135947  86.104.134.144  10.0.2.15       TCP        60 [TCP Retransmission] 80 → 49838 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
 341 59.322345  86.104.134.144  10.0.2.15       TCP        60 80 → 49845 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
```



10/96 security vendors flagged this URL as malicious

http://86.104.134.144/
86.104.134.144

ip

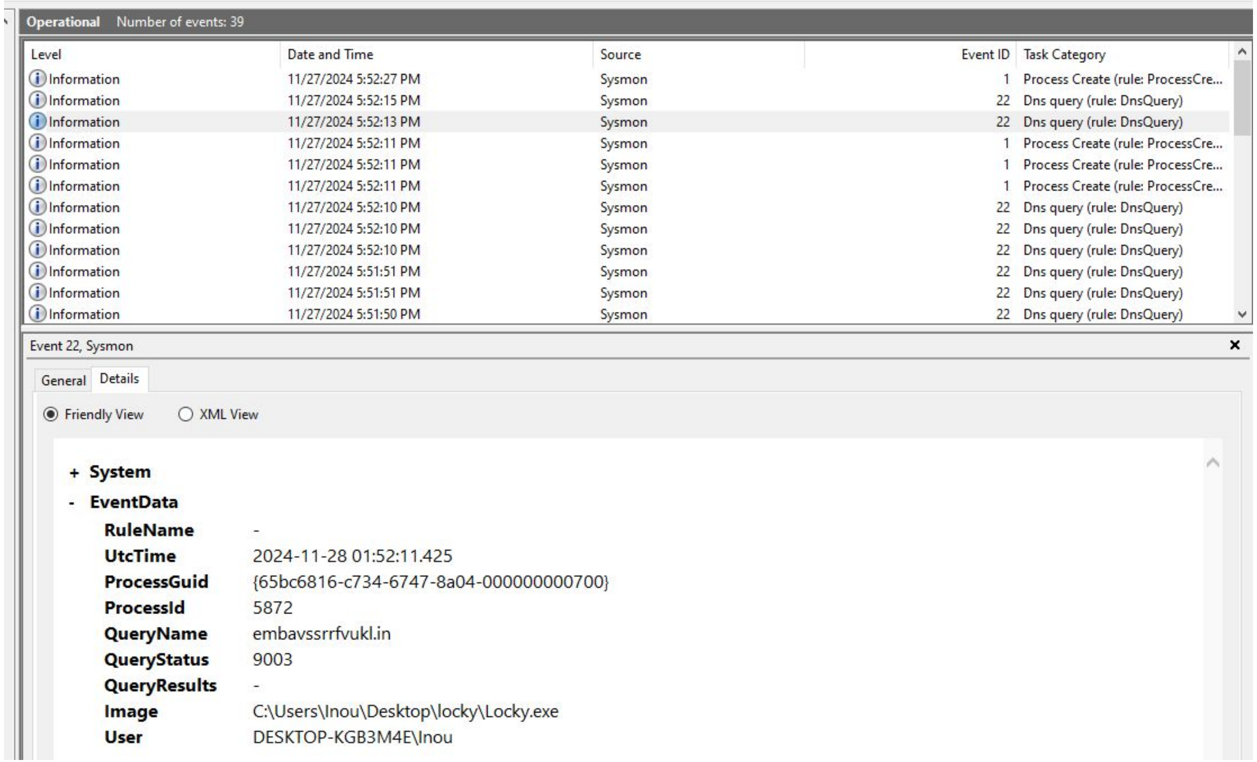
Last Analysis Date
1 month ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Malware	CRDF	Malicious
CyRadar	Malicious	G-Data	Malware
Kaspersky	Malware	Lionic	Malicious
MalwareURL	Malware	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Artists Against 419	Clean
benkow.cc	Clean	BlockList	Clean



Operational Number of events: 39

Level	Date and Time	Source	Event ID	Task Category
Information	11/27/2024 5:52:27 PM	Sysmon	1	Process Create (rule: ProcessCre...
Information	11/27/2024 5:52:15 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:52:13 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:52:11 PM	Sysmon	1	Process Create (rule: ProcessCre...
Information	11/27/2024 5:52:11 PM	Sysmon	1	Process Create (rule: ProcessCre...
Information	11/27/2024 5:52:11 PM	Sysmon	1	Process Create (rule: ProcessCre...
Information	11/27/2024 5:52:10 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:52:10 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:52:10 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:51:51 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:51:51 PM	Sysmon	22	Dns query (rule: DnsQuery)
Information	11/27/2024 5:51:50 PM	Sysmon	22	Dns query (rule: DnsQuery)

Event 22, Sysmon

● Friendly View ○ XML View

+ System

- EventData

RuleName	-
UtcTime	2024-11-28 01:52:11.425
ProcessGuid	{65bc6816-c734-6747-8a04-000000000700}
ProcessId	5872
QueryName	embavssrrfvukl.in
QueryStatus	9003
QueryResults	-
Image	C:\Users\Inou\Desktop\locky\Locky.exe
User	DESKTOP-KGB3M4E\Inou

Locky- Defense

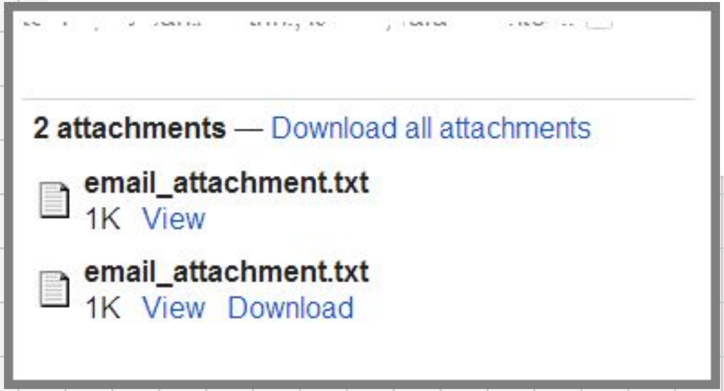
- Antivirus and Anti-Malware Updates
- Spam Filters, Attachment Scanning, Phishing Awareness
- Domain Blocking, Intrusion Detection and Prevention Systems (IDS/IPS)
- Regular Backups
- Running your system on a VM is also a good countermeasure.
  - **Snapshots**
  - **Natural protection against malware with VM detection**
  - **Controlled Network**

CryptoLocker- Background

- **Emergence**: First discovered September 2013
- **Impact**: The malware is capable of locating and encrypting files stored on shared network drives, USB drives, external hard drives, network file shares, and certain cloud storage systems. If a single computer on a network is infected, mapped network drives may also be compromised.

CryptoLocker- Encryption and Delivery

- **Encryption**: asymmetric encryption, only one party had the key, the HACKERS!!!
- **Delivery**: This malware was commonly sent through emails however it was also spread through USB flash drives.



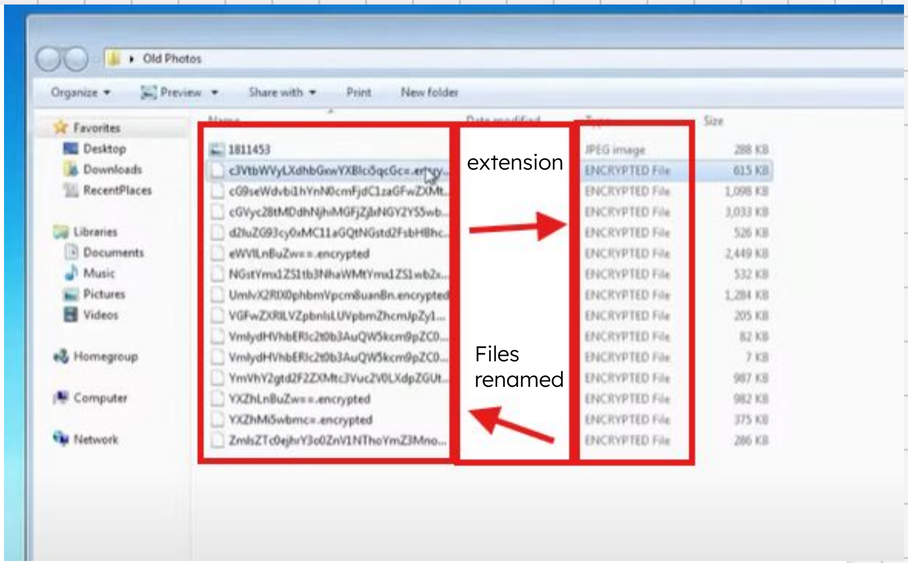
2 attachments — Download all attachments

email_attachment.txt
1K View

email_attachment.txt
1K View Download

CryptoLocker- Results

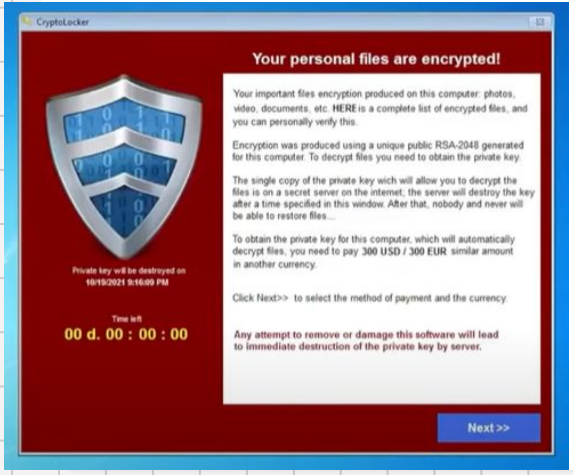
- CryptoLocker after executing the malware the files were shortly locked and given a new extension of “encrypted”
- Additionally the file names were changed. As seen in the picture to the left



Name	Type	Size
1811453	JPEG image	288 KB
c3VtbWVyLXdhbGxwYXBlc5qcGc=.encry...	ENCRYPTED File	615 KB
cG9seWdvbi1hYnN0cmFjdC1zaGFwZXMt...	ENCRYPTED File	1,098 KB
cGVyc28tMDdhNjhiMGFjZjljNGY2YS5wb...	ENCRYPTED File	3,033 KB
d2luZG93cy0xMC11aGQtNGstd2FsbHBhc...	ENCRYPTED File	526 KB
eWVlLnBuZw==.encrypted	ENCRYPTED File	2,449 KB
NGstYmx1ZS1tb3NhaWMtYmx1ZS1wb2x...	ENCRYPTED File	532 KB
UmlvX2RlX0phbmVpcm8uanBn.encrypted	ENCRYPTED File	1,284 KB
VGFwZXRlLVZpbnlsLUVpbmZhcmJpZy1...	ENCRYPTED File	205 KB
VmlydHVhbERlc2t0b3AuQW5kcm9pZC0...	ENCRYPTED File	82 KB
VmlydHVhbERlc2t0b3AuQW5kcm9pZC0...	ENCRYPTED File	7 KB
YmVhY2gtd2F2ZXMtc3Vuc2V0LXdpZGUt...	ENCRYPTED File	987 KB
YXZhLnBuZw==.encrypted	ENCRYPTED File	982 KB
YXZhMi5wbmc=.encrypted	ENCRYPTED File	375 KB
ZmlsZTc0ejhrY3o0ZnV1NThoYmZ3Mno...	ENCRYPTED File	286 KB

extension

Files renamed



Your personal files are encrypted!

Your important files encryption produced on this computer: photos, video, documents, etc. **HERE** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key wich will allow you to decrypt the files is on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** similar amount in another currency.

Click Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.

Private key will be destroyed on
10/19/2021 9:16:09 PM

Time left
00 d. 00 : 00 : 00

- In the picture to the left you can see the pop-up that informs you that your personal files have been encrypted and you have X amount of time to pay them to get the encryption key.

CryptoLocker- More thoughts

- Here is the task manager of the CryptoLocker files running, when trying to force stop these programs from running they immediately start right back up.

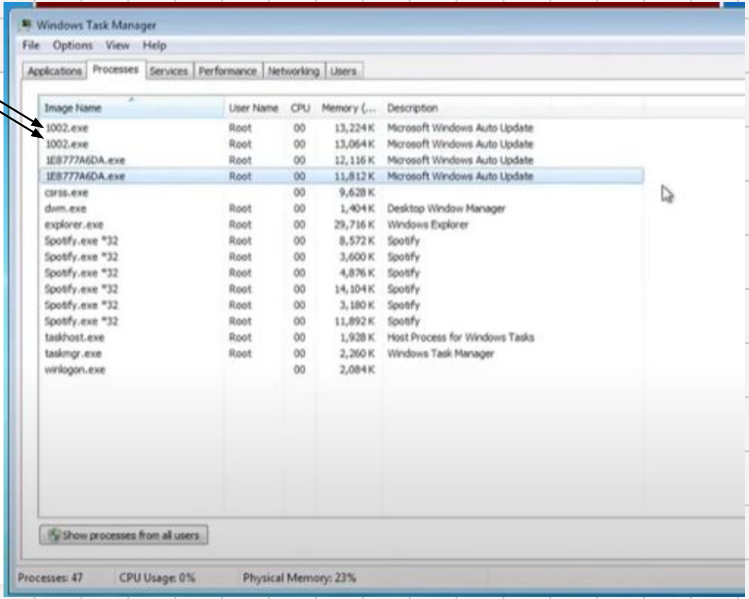

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Show processes from all users

Image Name	User Name	CPU	Memory (...	Description
1002.exe	Root	00	13,224 K	Microsoft Windows Auto Update
1002.exe	Root	00	13,064 K	Microsoft Windows Auto Update
1E8777A6DA.exe	Root	00	12,116 K	Microsoft Windows Auto Update
1E8777A6DA.exe	Root	00	11,812 K	Microsoft Windows Auto Update
csrss.exe		00	9,628 K	
dwm.exe	Root	00	1,404 K	Desktop Window Manager
explorer.exe	Root	00	29,716 K	Windows Explorer
Spotify.exe *32	Root	00	8,572 K	Spotify
Spotify.exe *32	Root	00	3,600 K	Spotify
Spotify.exe *32	Root	00	4,876 K	Spotify
Spotify.exe *32	Root	00	14,104 K	Spotify
Spotify.exe *32	Root	00	3,180 K	Spotify
Spotify.exe *32	Root	00	11,892 K	Spotify
taskhost.exe	Root	00	1,928 K	Host Process for Windows Tasks
taskmgr.exe	Root	00	2,260 K	Windows Task Manager
winlogon.exe		00	2,084 K	

Processes: 47 CPU Usage: 0% Physical Memory: 23%

CryptoLocker- Mitigation

These are the following recommendations US-CERT suggests users and administrators take the following preventative measures to protect their computer networks from a CryptoLocker infection:

- Conduct routine backups of important files, keeping the backups stored offline.
- Maintain up-to-date anti-virus software.
- Keep your operating system and software up-to-date with the latest patches.
- Do not follow unsolicited web links in email.
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

Work Cited

- Behling, D. (2022, October 15). *LockBit 3.0: Also known as LockBit Black*. VMware Security Blog. Retrieved from https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html
- https://github.com/Tennessene/LockBit
- https://www.youtube.com/watch?v=sS6_1r5hxi8
- https://www.youtube.com/watch?v=6PEA0nFyc0Q
- https://www.knowbe4.com/locky-ransomware
- https://blog.avast.com/a-closer-look-at-the-locky-ransomware
- https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections