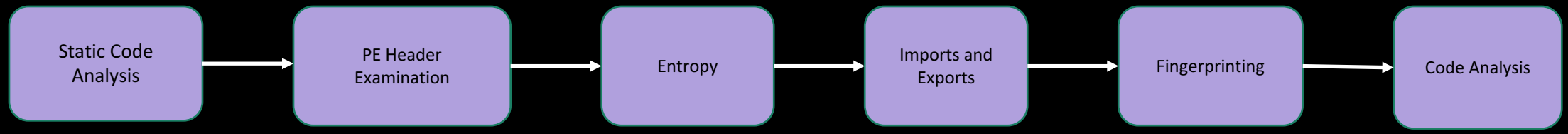
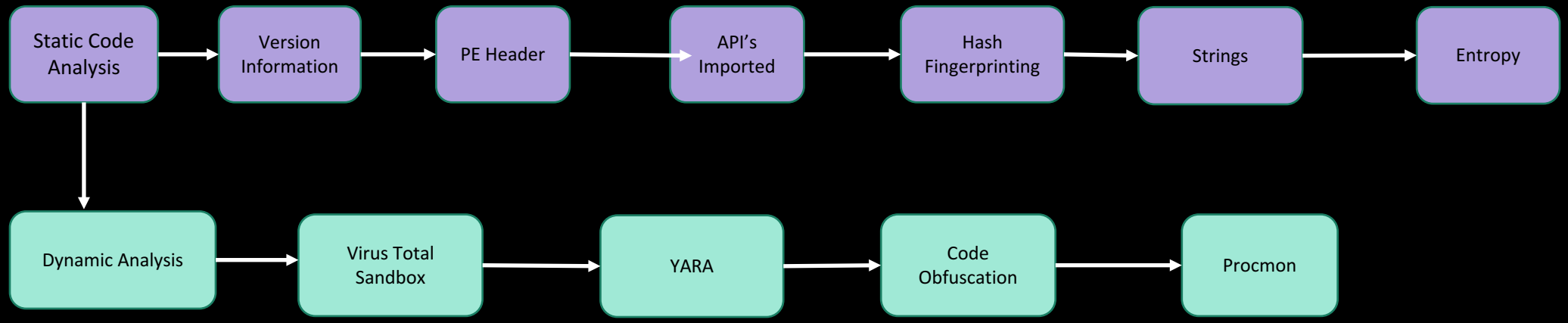
Forensic Post Mortem
CERBER, MAKTUB , LOCKY

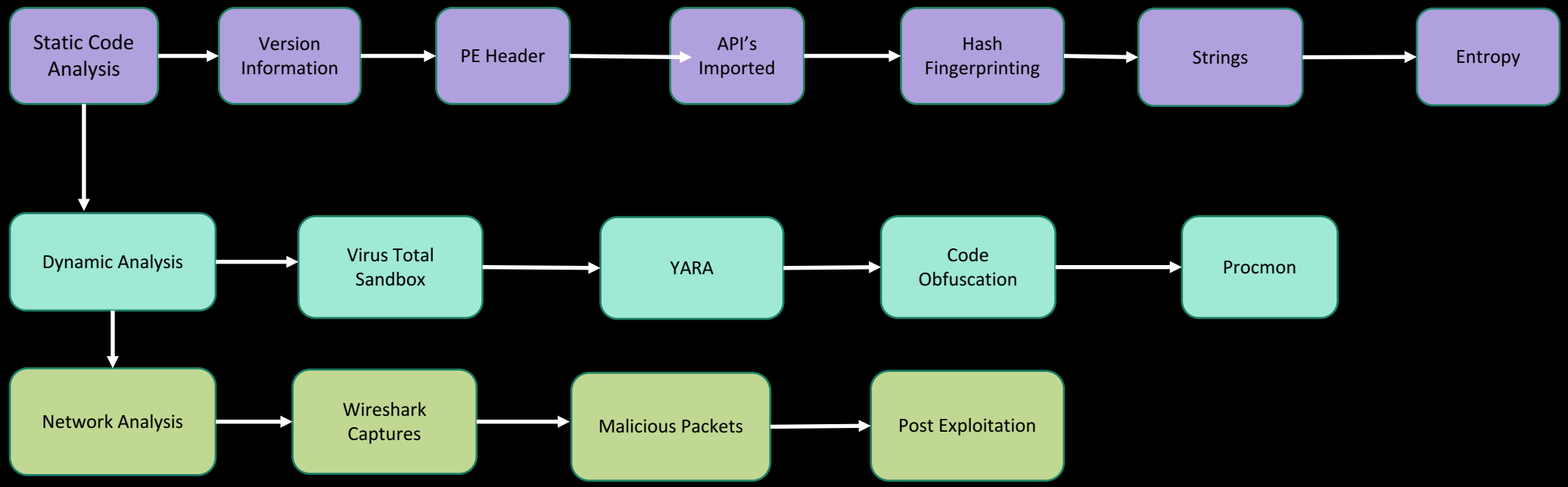
VERONICA SCHMITT
https://medium.com/@veronica_66606
VERONICA@DFIRLABS.COM

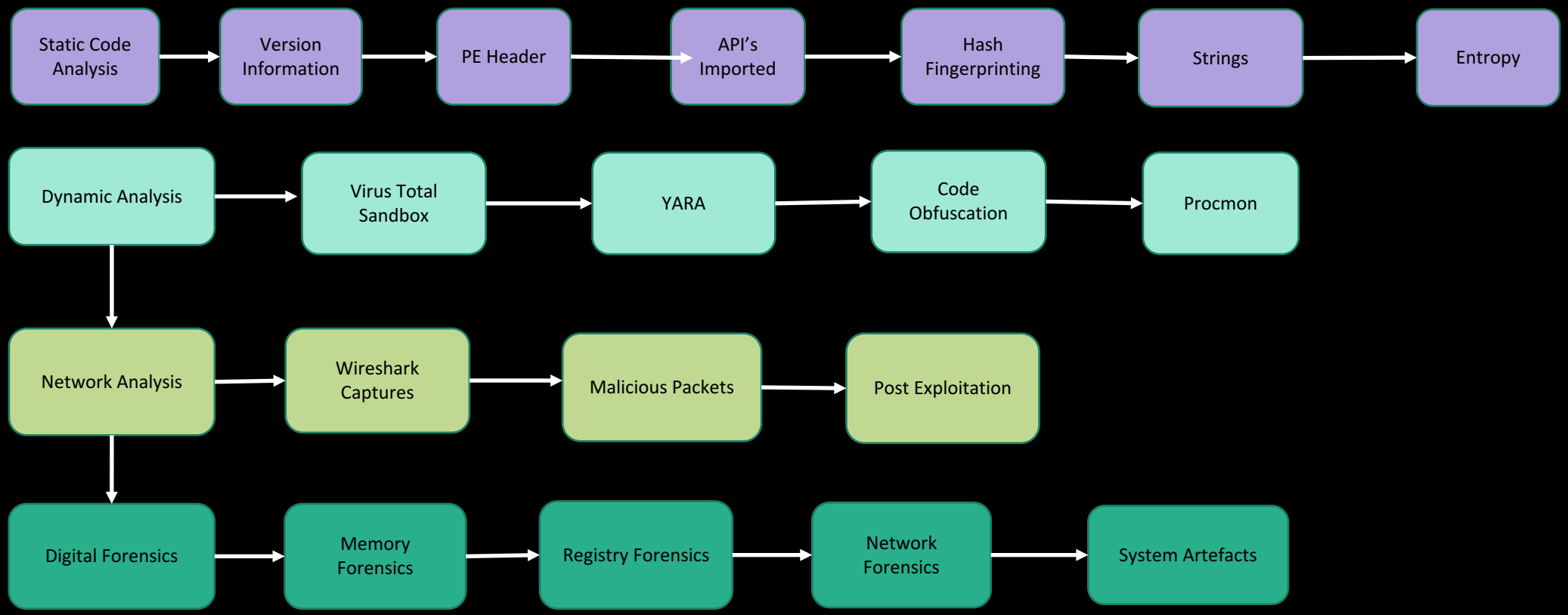
SAMPLES LOOKED @

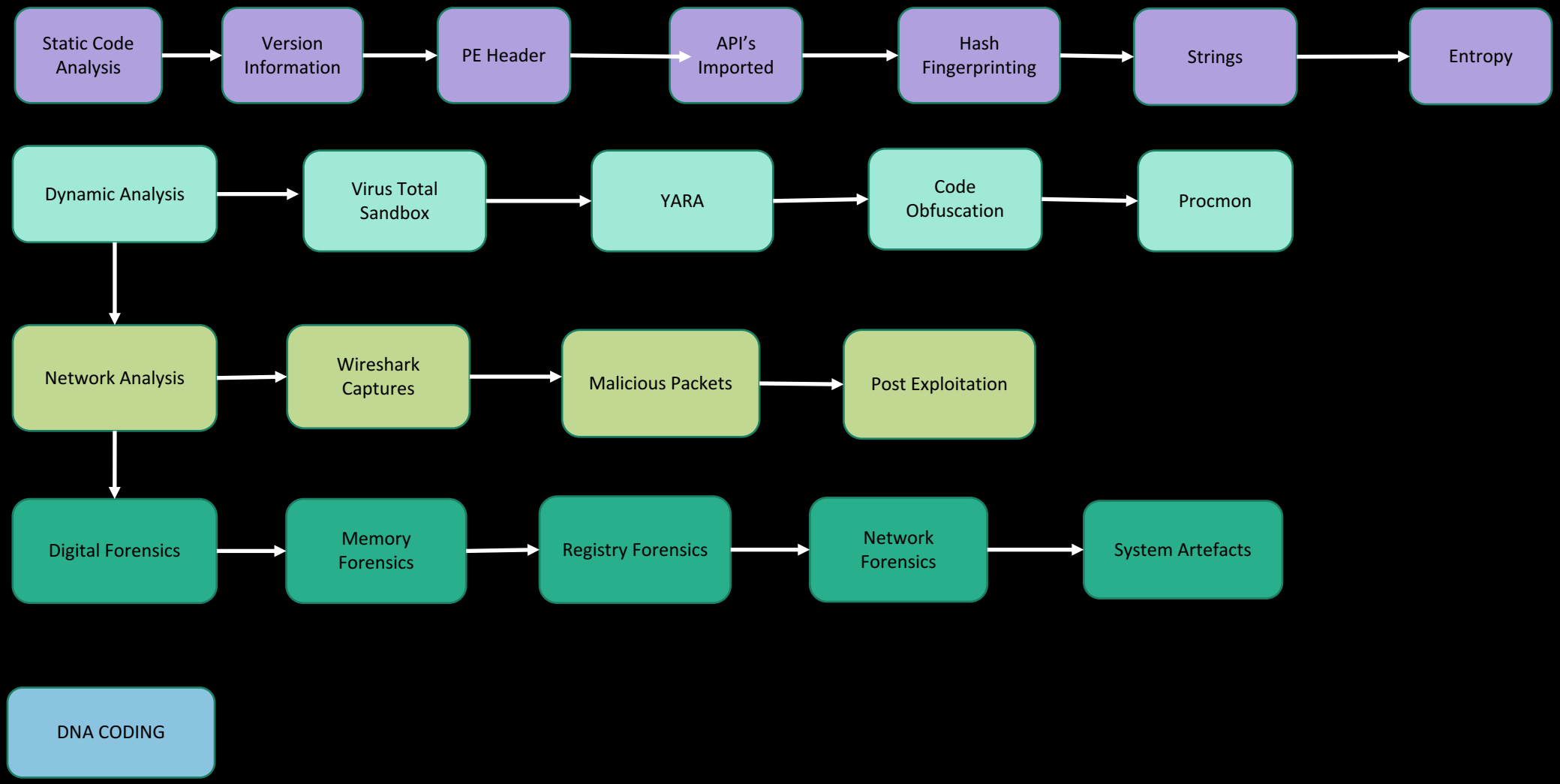
NEW APPROACH TO MALWARE


Static Code Analysis
PE Header Examination
Entropy
Imports and Exports
Fingerprinting
Code Analysis

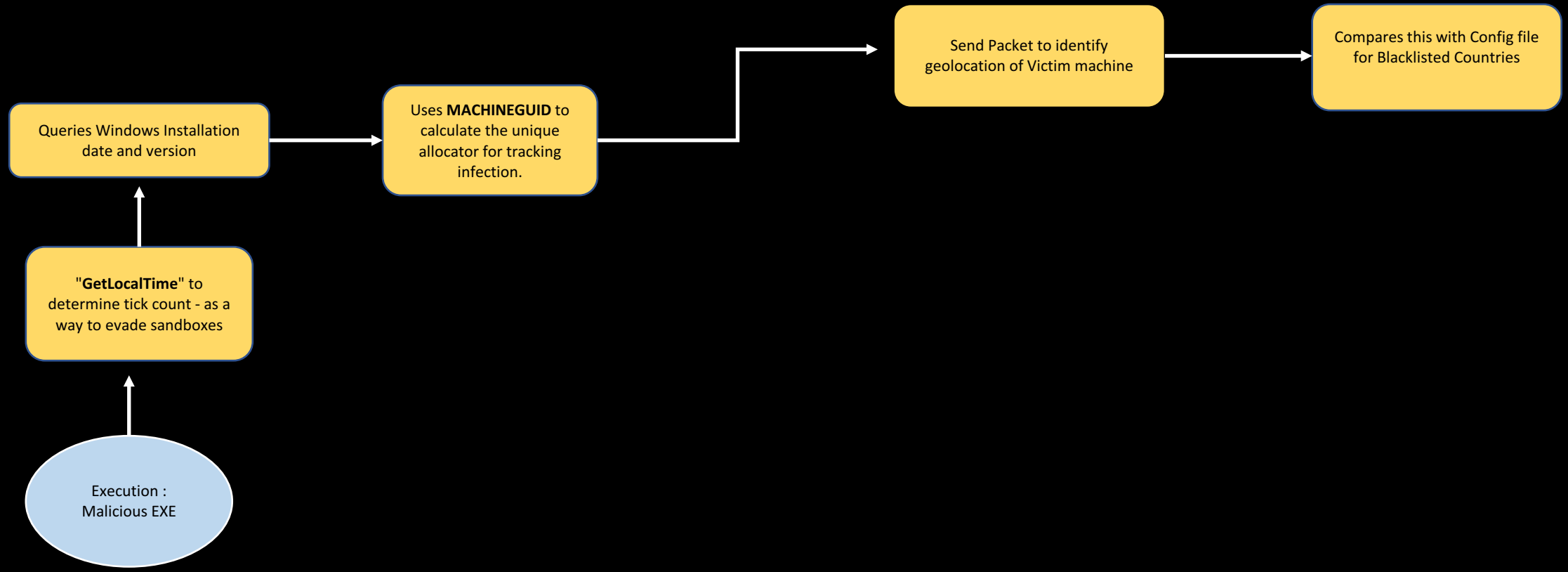

Static Code Analysis
Version Information
PE Header
API's Imported
Hash Fingerprinting
Strings
Entropy
Dynamic Analysis
Virus Total Sandbox
YARA
Code Obfuscation
Procmon

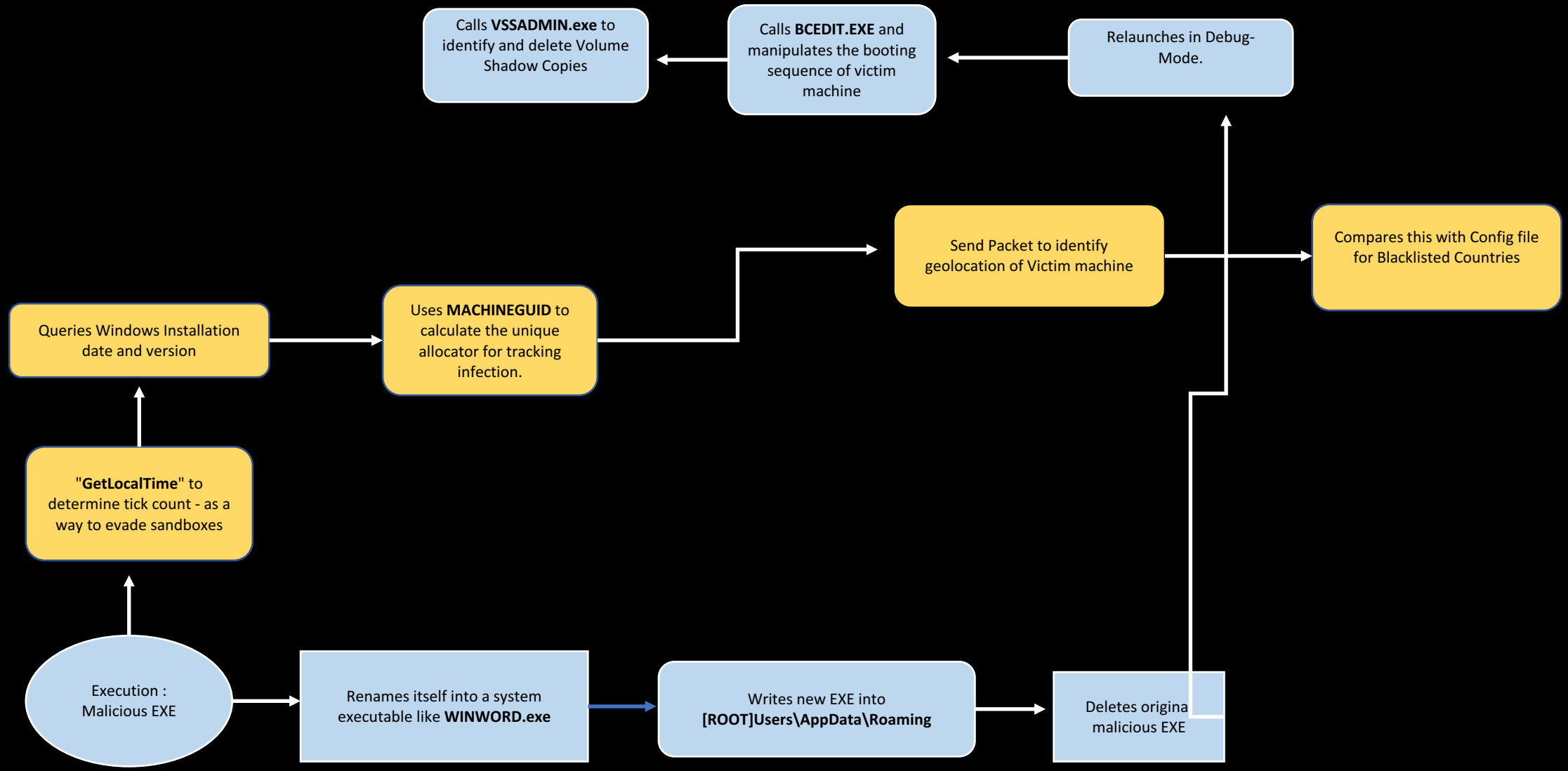

Static Code Analysis
Version Information
PE Header
API's Imported
Hash Fingerprinting
Strings
Entropy
Dynamic Analysis
Virus Total Sandbox
YARA
Code Obfuscation
Procmon
Network Analysis
Wireshark Captures
Malicious Packets
Post Exploitation

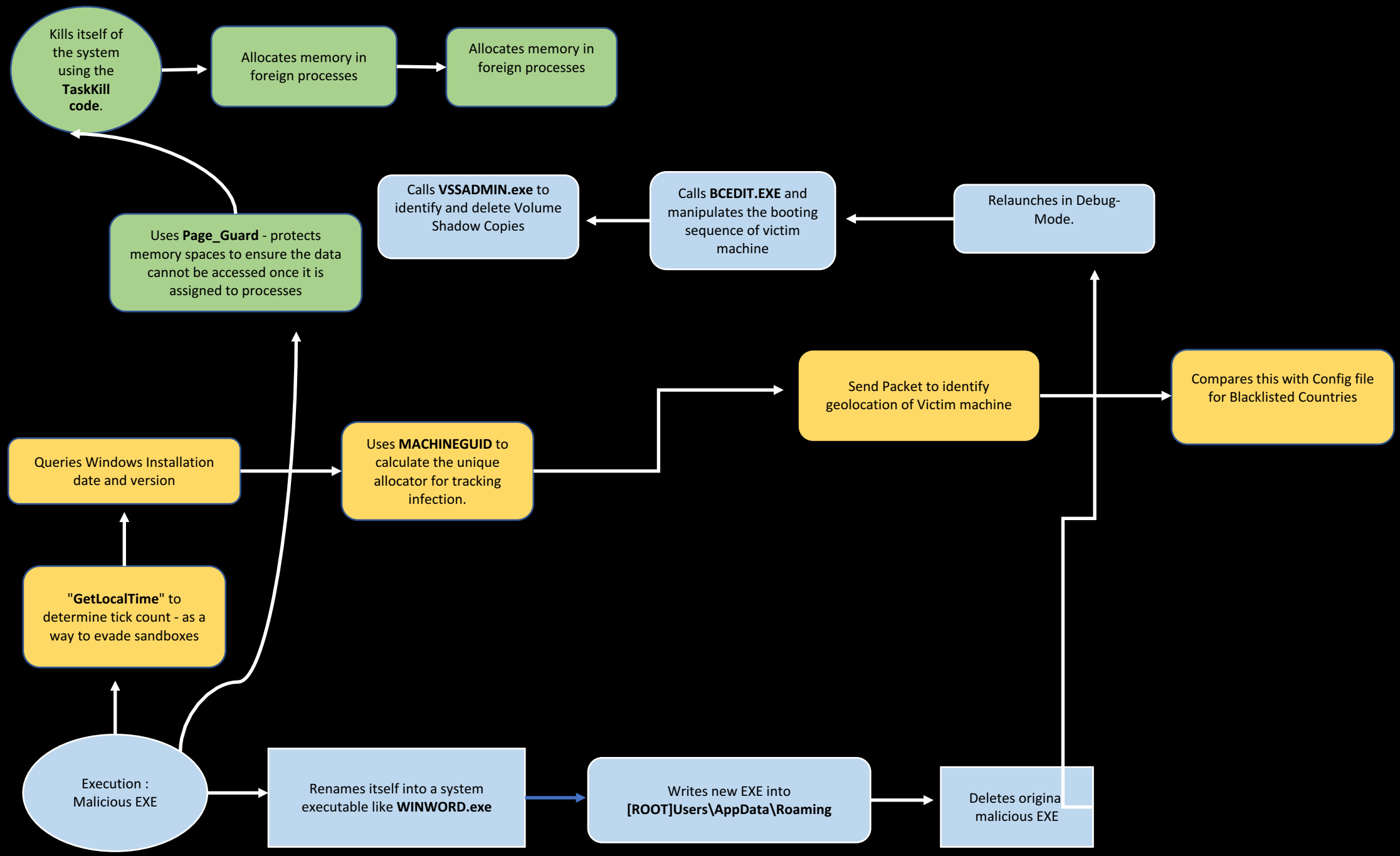

Static Code Analysis
Version Information
PE Header
API's Imported
Hash Fingerprinting
Strings
Entropy
Dynamic Analysis
Virus Total Sandbox
YARA
Code Obfuscation
Procmon
Network Analysis
Wireshark Captures
Malicious Packets
Post Exploitation
Digital Forensics
Memory Forensics
Registry Forensics
Network Forensics
System Artefacts

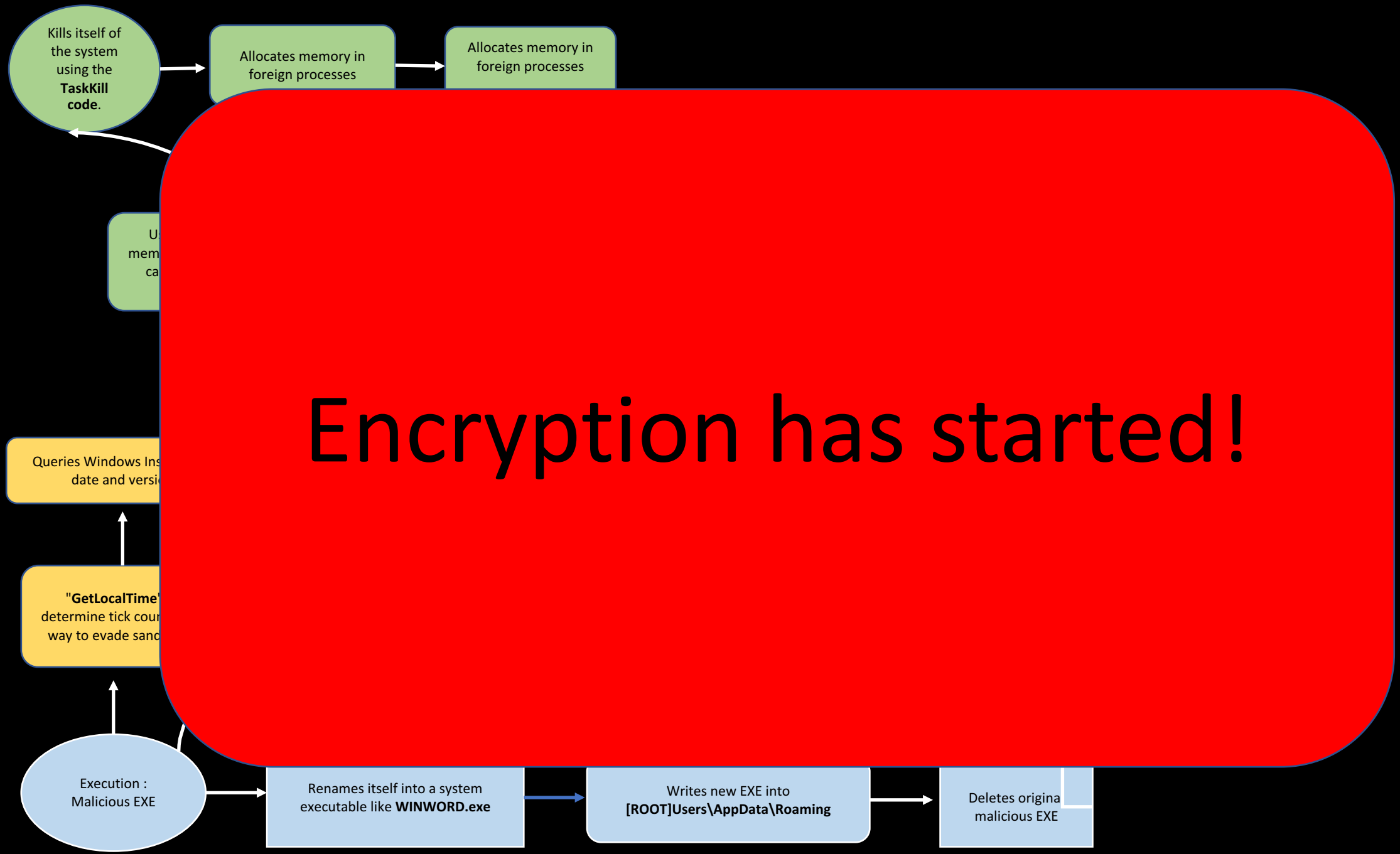

Static Code Analysis
Version Information
PE Header
API's Imported
Hash Fingerprinting
Strings
Entropy
Dynamic Analysis
Virus Total Sandbox
YARA
Code Obfuscation
Procmon
Network Analysis
Wireshark Captures
Malicious Packets
Post Exploitation
Digital Forensics
Memory Forensics
Registry Forensics
Network Forensics
System Artefacts
DNA CODING

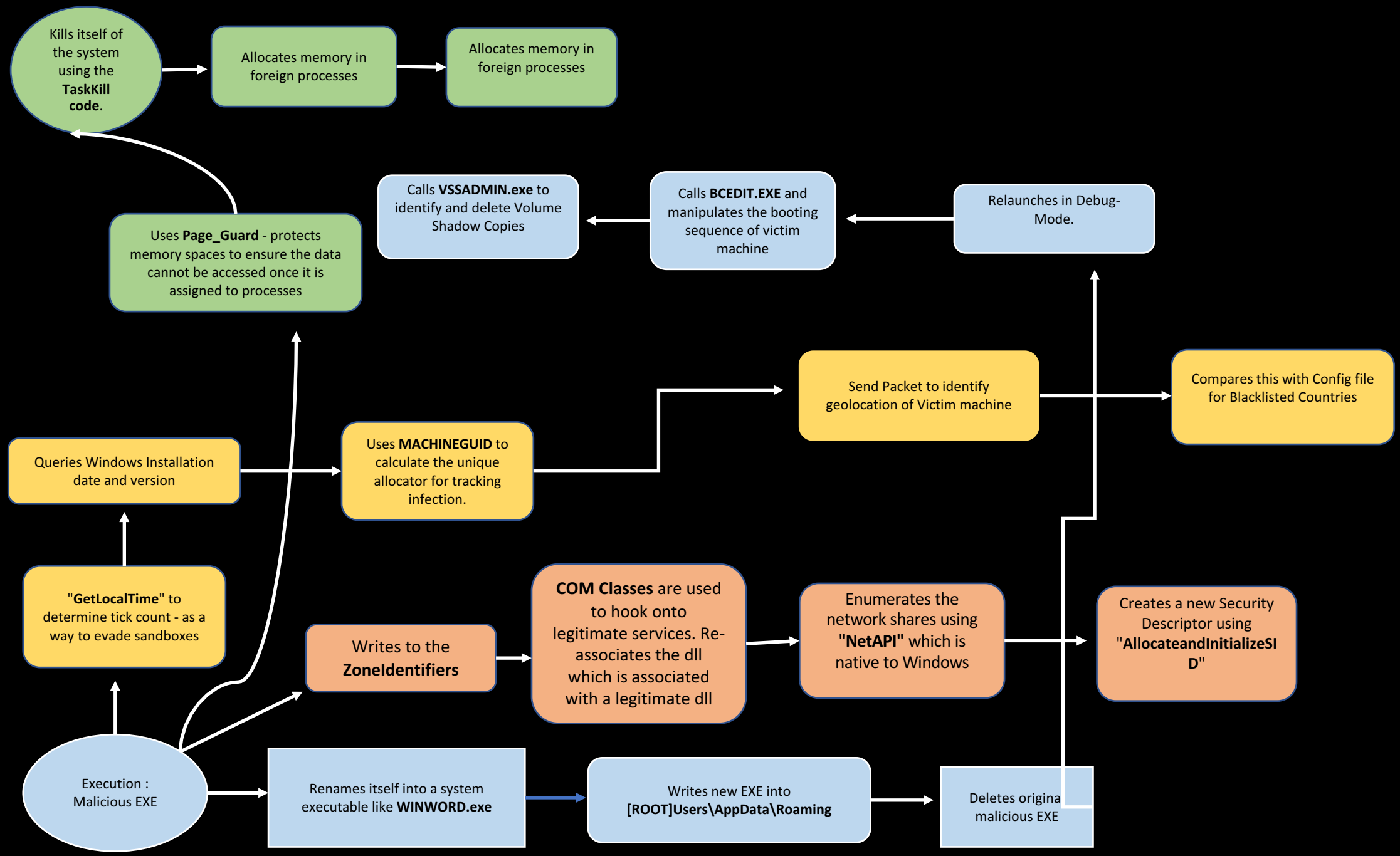
CERBER EXECUTION FLOW

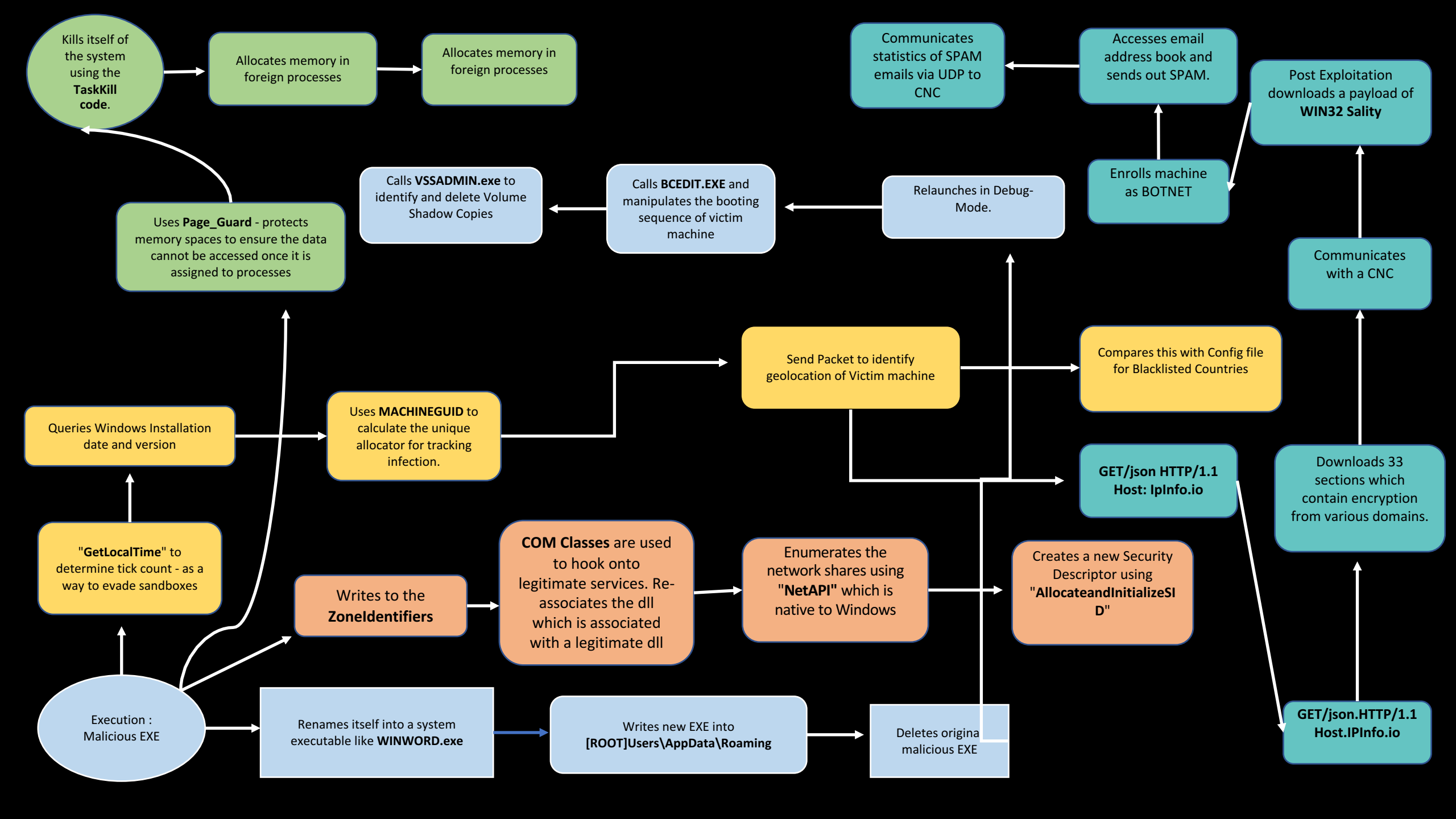

Execution :
Malicious EXE
"GetLocalTime" to determine tick count - as a way to evade sandboxes
Queries Windows Installation date and version
Uses MACHINEGUID to calculate the unique allocator for tracking infection.
Send Packet to identify geolocation of Victim machine
Compares this with Config file for Blacklisted Countries


Calls **VSSADMIN.exe** to identify and delete Volume Shadow Copies
Calls **BCEDIT.EXE** and manipulates the booting sequence of victim machine
Relaunches in Debug-Mode.
Send Packet to identify geolocation of Victim machine
Compares this with Config file for Blacklisted Countries
Queries Windows Installation date and version
Uses **MACHINEGUID** to calculate the unique allocator for tracking infection.
"**GetLocalTime**" to determine tick count - as a way to evade sandboxes
Execution : Malicious EXE
Renames itself into a system executable like **WINWORD.exe**
Writes new EXE into **[ROOT]Users\AppData\Roaming**
Deletes origina malicious EXE


Kills itself of the system using the **TaskKill code**.
Allocates memory in foreign processes
Allocates memory in foreign processes
Uses **Page_Guard** - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes
Calls **VSSADMIN.exe** to identify and delete Volume Shadow Copies
Calls **BCEDIT.EXE** and manipulates the booting sequence of victim machine
Relaunches in Debug-Mode.
Queries Windows Installation date and version
Uses **MACHINEGUID** to calculate the unique allocator for tracking infection.
Send Packet to identify geolocation of Victim machine
Compares this with Config file for Blacklisted Countries
"**GetLocalTime**" to determine tick count - as a way to evade sandboxes
Execution : Malicious EXE
Renames itself into a system executable like **WINWORD.exe**
Writes new EXE into **[ROOT]Users\AppData\Roaming**
Deletes origina malicious EXE


Kills itself of the system using the **TaskKill code**.
Allocates memory in foreign processes
Allocates memory in foreign processes
Queries Windows Ins
date and versi
"**GetLocalTime**'
determine tick cou
way to evade sand
Execution :
Malicious EXE
Renames itself into a system executable like **WINWORD.exe**
Writes new EXE into **[ROOT]Users\AppData\Roaming**
Deletes origina
malicious EXE
Encryption has started!


Kills itself of the system using the **TaskKill code**.
Allocates memory in foreign processes
Allocates memory in foreign processes
Uses **Page_Guard** - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes
Calls **VSSADMIN.exe** to identify and delete Volume Shadow Copies
Calls **BCEDIT.EXE** and manipulates the booting sequence of victim machine
Relaunches in Debug-Mode.
Queries Windows Installation date and version
Uses **MACHINEGUID** to calculate the unique allocator for tracking infection.
Send Packet to identify geolocation of Victim machine
Compares this with Config file for Blacklisted Countries
"**GetLocalTime**" to determine tick count - as a way to evade sandboxes
Writes to the **ZoneIdentifiers**
COM Classes are used to hook onto legitimate services. Re-associates the dll which is associated with a legitimate dll
Enumerates the network shares using "**NetAPI**" which is native to Windows
Creates a new Security Descriptor using "**AllocateandInitializeSID**"
Execution : Malicious EXE
Renames itself into a system executable like **WINWORD.exe**
Writes new EXE into **[ROOT]Users\AppData\Roaming**
Deletes origina malicious EXE


Kills itself of the system using the **TaskKill code**.
Allocates memory in foreign processes
Allocates memory in foreign processes
Communicates statistics of SPAM emails via UDP to CNC
Accesses email address book and sends out SPAM.
Post Exploitation downloads a payload of **WIN32 Sality**
Enrolls machine as BOTNET
Relaunches in Debug-Mode.
Calls **BCEDIT.EXE** and manipulates the booting sequence of victim machine
Calls **VSSADMIN.exe** to identify and delete Volume Shadow Copies
Uses **Page_Guard** - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes
Communicates with a CNC
Send Packet to identify geolocation of Victim machine
Compares this with Config file for Blacklisted Countries
Queries Windows Installation date and version
Uses **MACHINEGUID** to calculate the unique allocator for tracking infection.
GET/json HTTP/1.1 Host: IpInfo.io
Downloads 33 sections which contain encryption from various domains.
"**GetLocalTime**" to determine tick count - as a way to evade sandboxes
Writes to the **ZoneIdentifiers**
COM Classes are used to hook onto legitimate services. Re-associates the dll which is associated with a legitimate dll
Enumerates the network shares using "**NetAPI**" which is native to Windows
Creates a new Security Descriptor using "**AllocateandInitializeSID**"
Execution : Malicious EXE
Renames itself into a system executable like **WINWORD.exe**
Writes new EXE into **[ROOT]Users\AppData\Roaming**
Deletes origina malicious EXE
GET/json.HTTP/1.1 Host.IPInfo.io

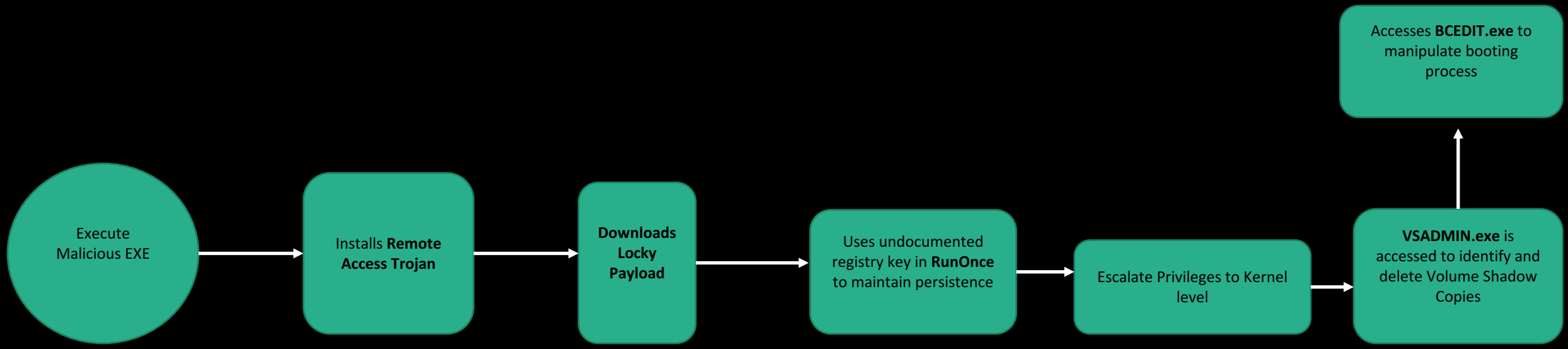
LOCKY EXECUTION FLOW

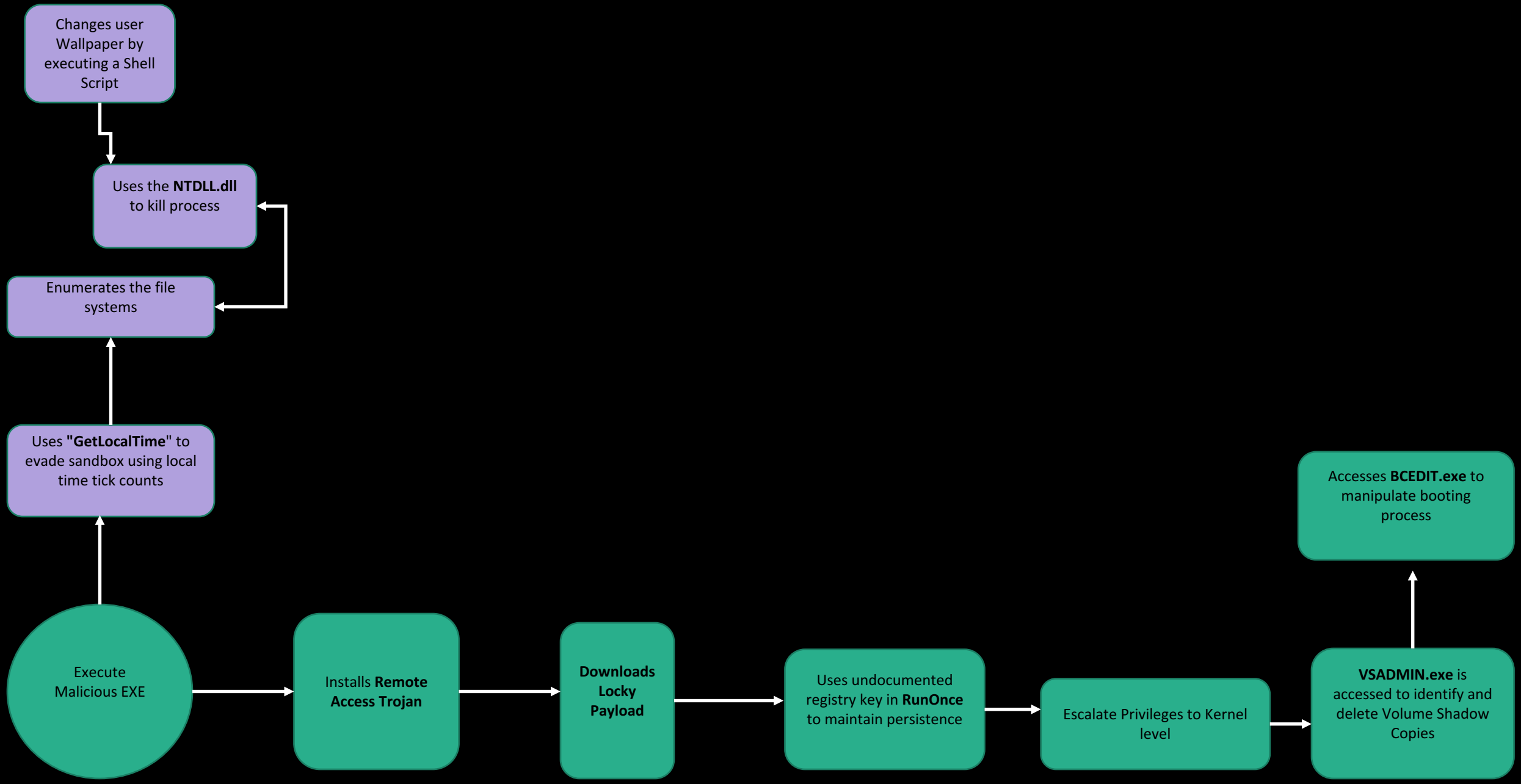
TECHNOLOGICALLY IMPAIRED HACKER

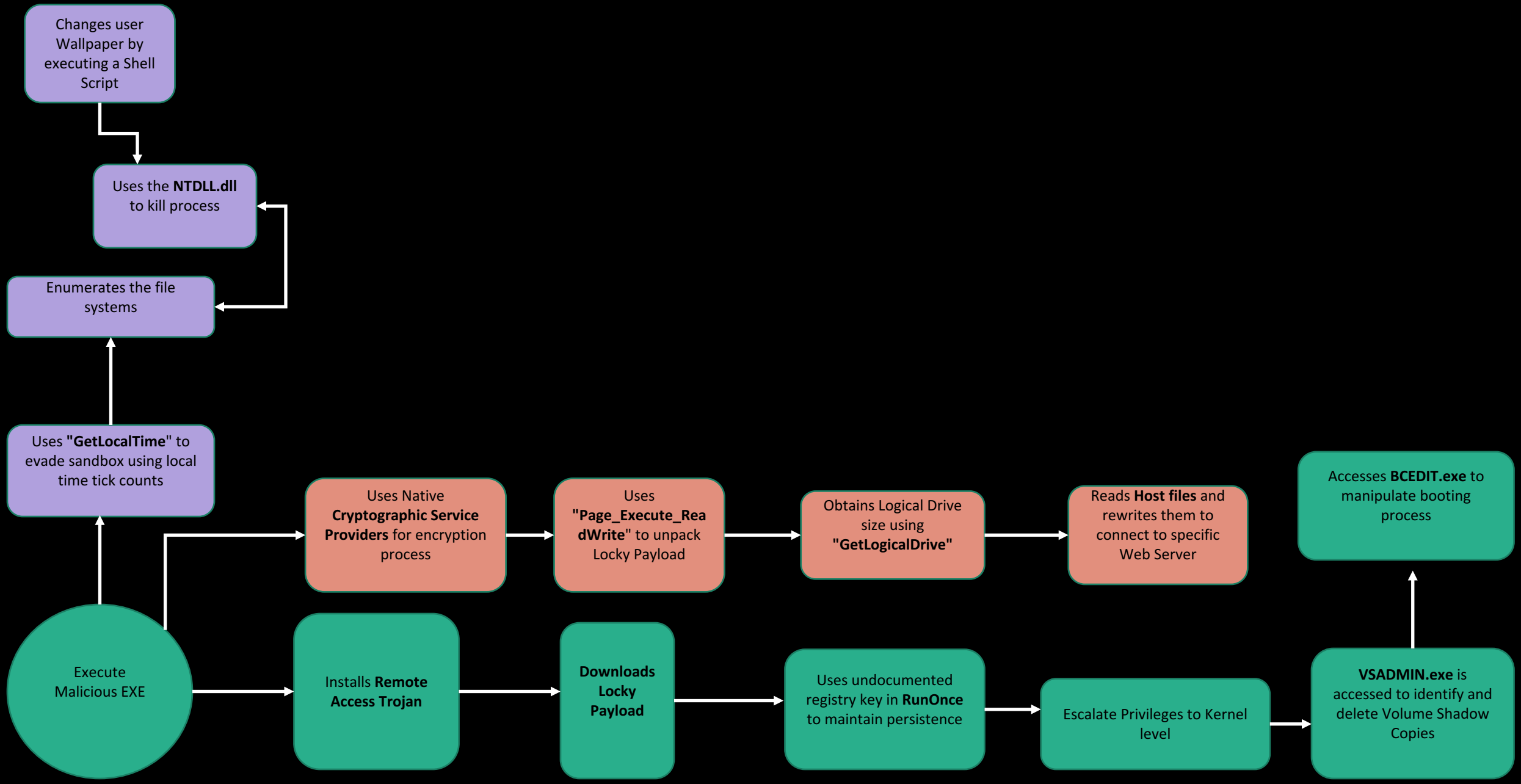
uploads his malware to VirusTotal to see if it can be detected by any of the antivirus vendors VirusTotal shares new samples with

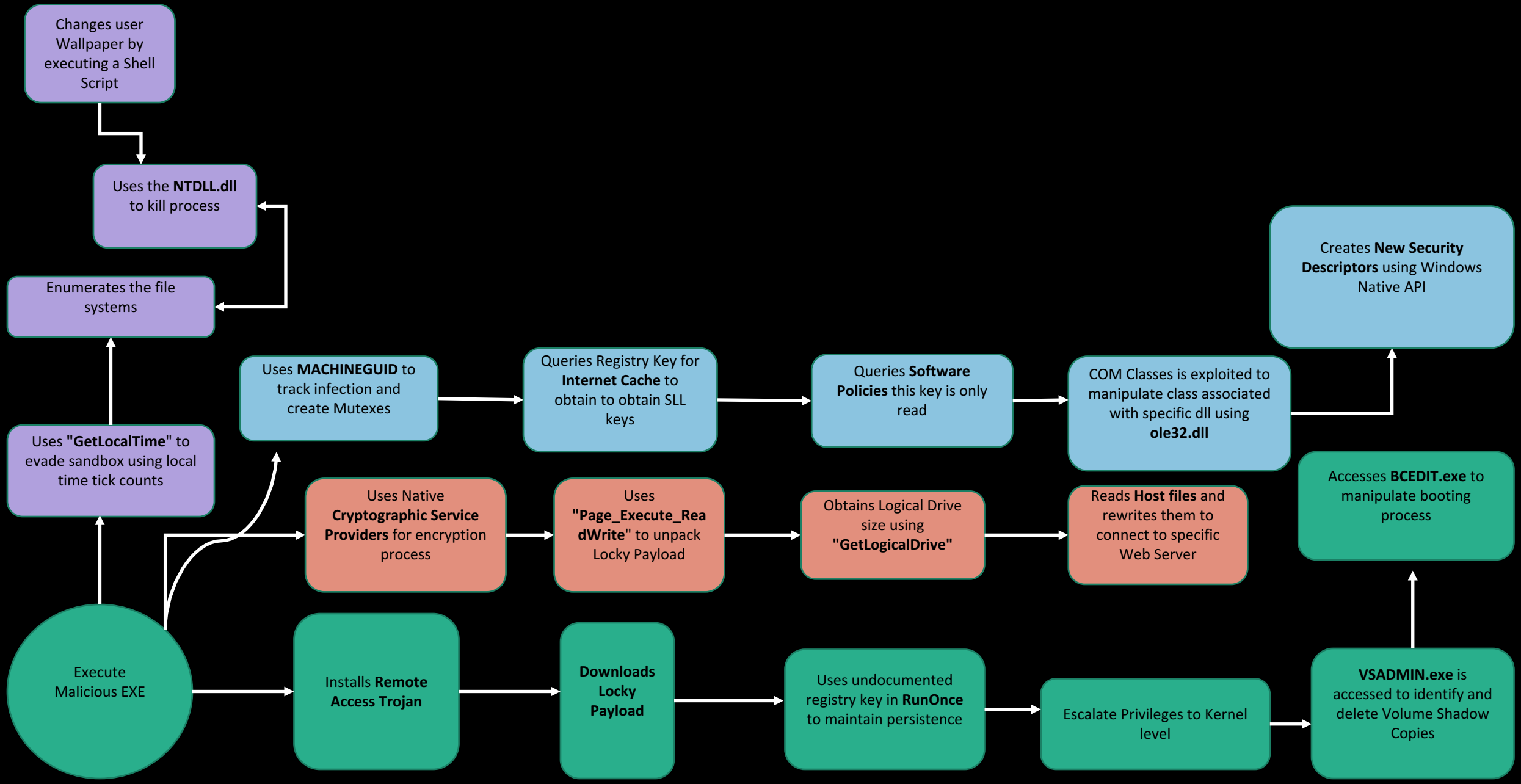
This is Your Evidence?

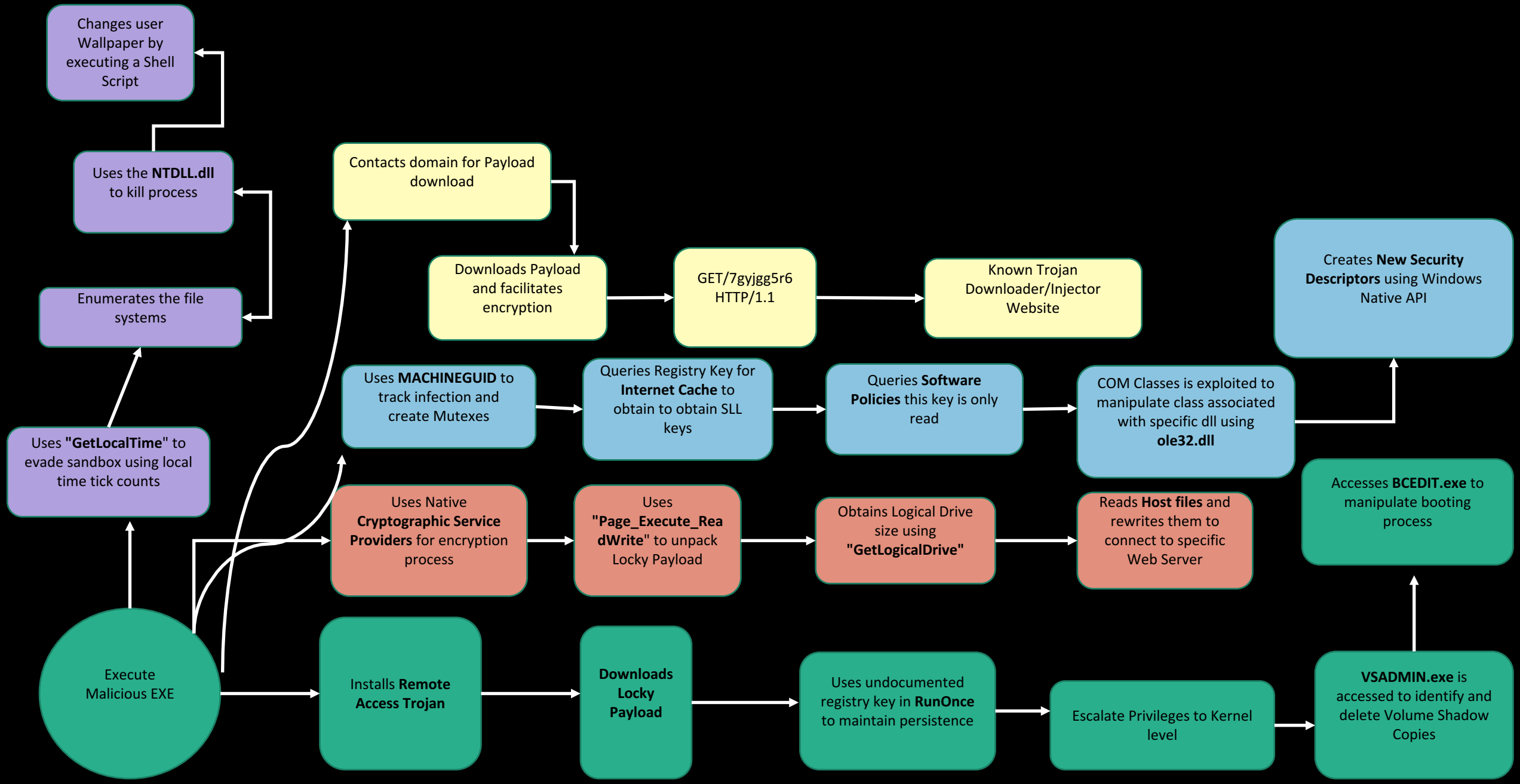
It doesn't Even have a Timestamp on it

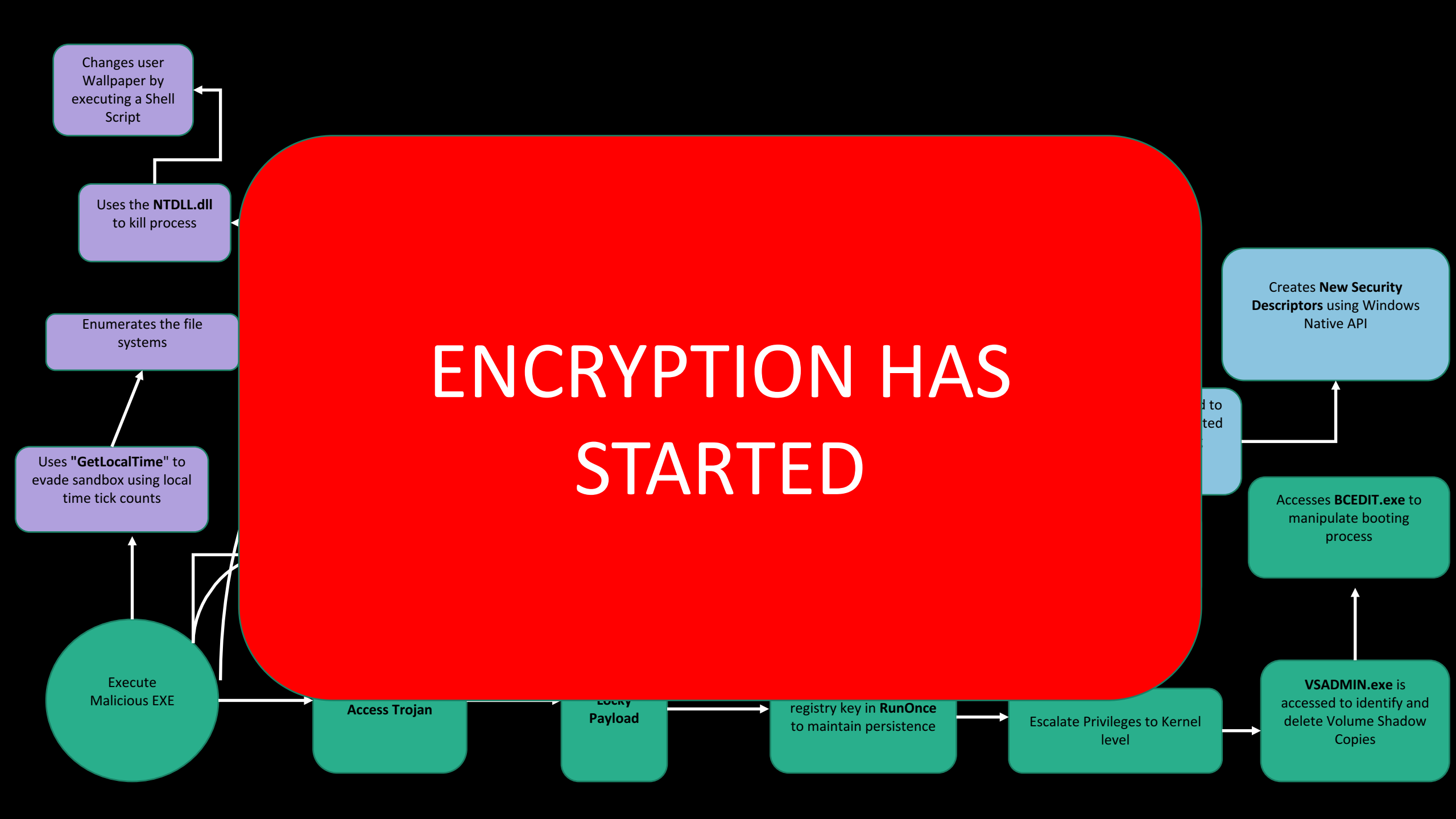

Execute Malicious EXE
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies
Accesses **BCEDIT.exe** to manipulate booting process


Changes user Wallpaper by executing a Shell Script
Uses the **NTDLL.dll** to kill process
Enumerates the file systems
Uses "**GetLocalTime**" to evade sandbox using local time tick counts
Execute Malicious EXE
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies
Accesses **BCEDIT.exe** to manipulate booting process


Changes user Wallpaper by executing a Shell Script
Uses the **NTDLL.dll** to kill process
Enumerates the file systems
Uses **"GetLocalTime"** to evade sandbox using local time tick counts
Execute Malicious EXE
Uses Native **Cryptographic Service Providers** for encryption process
Uses **"Page_Execute_ReadWrite"** to unpack Locky Payload
Obtains Logical Drive size using **"GetLogicalDrive"**
Reads **Host files** and rewrites them to connect to specific Web Server
Accesses **BCEDIT.exe** to manipulate booting process
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies


Changes user Wallpaper by executing a Shell Script
Uses the **NTDLL.dll** to kill process
Enumerates the file systems
Uses **"GetLocalTime"** to evade sandbox using local time tick counts
Execute Malicious EXE
Uses **MACHINEGUID** to track infection and create Mutexes
Queries Registry Key for **Internet Cache** to obtain to obtain SLL keys
Queries **Software Policies** this key is only read
COM Classes is exploited to manipulate class associated with specific dll using **ole32.dll**
Creates **New Security Descriptors** using Windows Native API
Uses Native **Cryptographic Service Providers** for encryption process
Uses **"Page_Execute_ReadWrite"** to unpack Locky Payload
Obtains Logical Drive size using **"GetLogicalDrive"**
Reads **Host files** and rewrites them to connect to specific Web Server
Accesses **BCEDIT.exe** to manipulate booting process
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies


Changes user Wallpaper by executing a Shell Script
Uses the **NTDLL.dll** to kill process
Enumerates the file systems
Uses **"GetLocalTime"** to evade sandbox using local time tick counts
Execute Malicious EXE
Contacts domain for Payload download
Downloads Payload and facilitates encryption
GET/7gyjgg5r6 HTTP/1.1
Known Trojan Downloader/Injector Website
Creates **New Security Descriptors** using Windows Native API
Uses **MACHINEGUID** to track infection and create Mutexes
Queries Registry Key for **Internet Cache** to obtain to obtain SLL keys
Queries **Software Policies** this key is only read
COM Classes is exploited to manipulate class associated with specific dll using **ole32.dll**
Uses Native **Cryptographic Service Providers** for encryption process
Uses **"Page_Execute_ReadWrite"** to unpack Locky Payload
Obtains Logical Drive size using **"GetLogicalDrive"**
Reads **Host files** and rewrites them to connect to specific Web Server
Accesses **BCEDIT.exe** to manipulate booting process
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies


Changes user Wallpaper by executing a Shell Script
Uses the **NTDLL.dll** to kill process
Enumerates the file systems
Uses **"GetLocalTime"** to evade sandbox using local time tick counts
Execute Malicious EXE
ENCRYPTION HAS STARTED
Creates **New Security Descriptors** using Windows Native API
Accesses **BCEDIT.exe** to manipulate booting process
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies
Escalate Privileges to Kernel level
registry key in **RunOnce** to maintain persistence
Payload
Access Trojan


Changes user Wallpaper by executing a Shell Script
Uses Victim Machine to send out SPAM
Downloads the Zeus Bot Downloader
Uses Remote Access Trojan to create Backdoor onto system
Forms part of the EK Malware Campaign
Sent to DGA created domains
Uses the **NTDLL.dll** to kill process
Contacts domain for Payload download
Uses HTTP POST to exfilltrate pre-encryption data.
Enumerates the file systems
Downloads Payload and facilitates encryption
GET/7gyjgg5r6 HTTP/1.1
Known Trojan Downloader/Injector Website
Creates **New Security Descriptors** using Windows Native API
Uses **MACHINEGUID** to track infection and create Mutexes
Queries Registry Key for **Internet Cache** to obtain to obtain SLL keys
Queries **Software Policies** this key is only read
COM Classes is exploited to manipulate class associated with specific dll using **ole32.dll**
Uses **"GetLocalTime"** to evade sandbox using local time tick counts
Uses Native **Cryptographic Service Providers** for encryption process
Uses **"Page_Execute_ReadWrite"** to unpack Locky Payload
Obtains Logical Drive size using **"GetLogicalDrive"**
Reads **Host files** and rewrites them to connect to specific Web Server
Accesses **BCEDIT.exe** to manipulate booting process
Execute Malicious EXE
Installs **Remote Access Trojan**
Downloads Locky Payload
Uses undocumented registry key in **RunOnce** to maintain persistence
Escalate Privileges to Kernel level
VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

MAKTUB EXECUTION FLOW

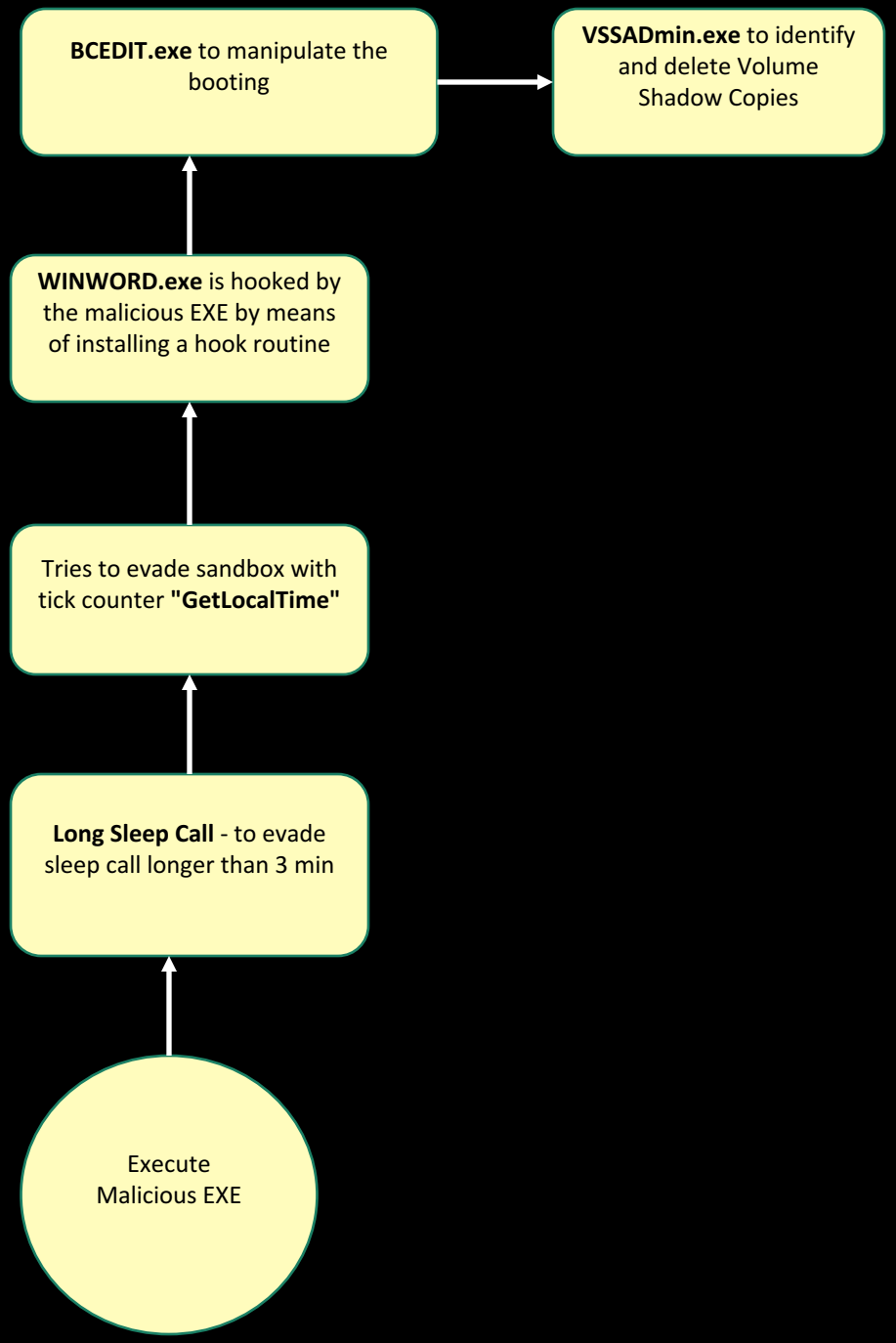
I GOT ATTACKED BY RANSOMWARE
AND WAS ASKED FOR MONEY...

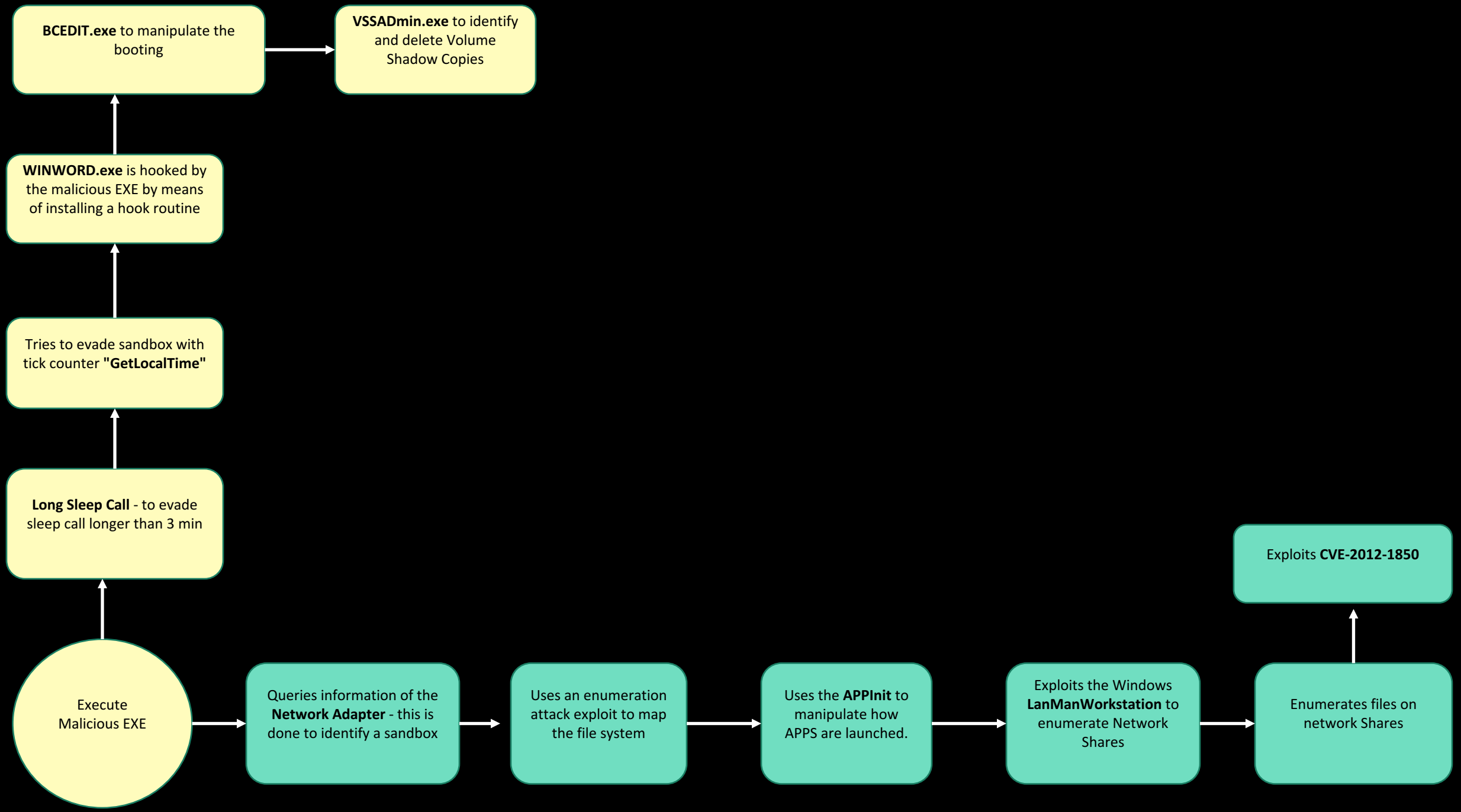
.

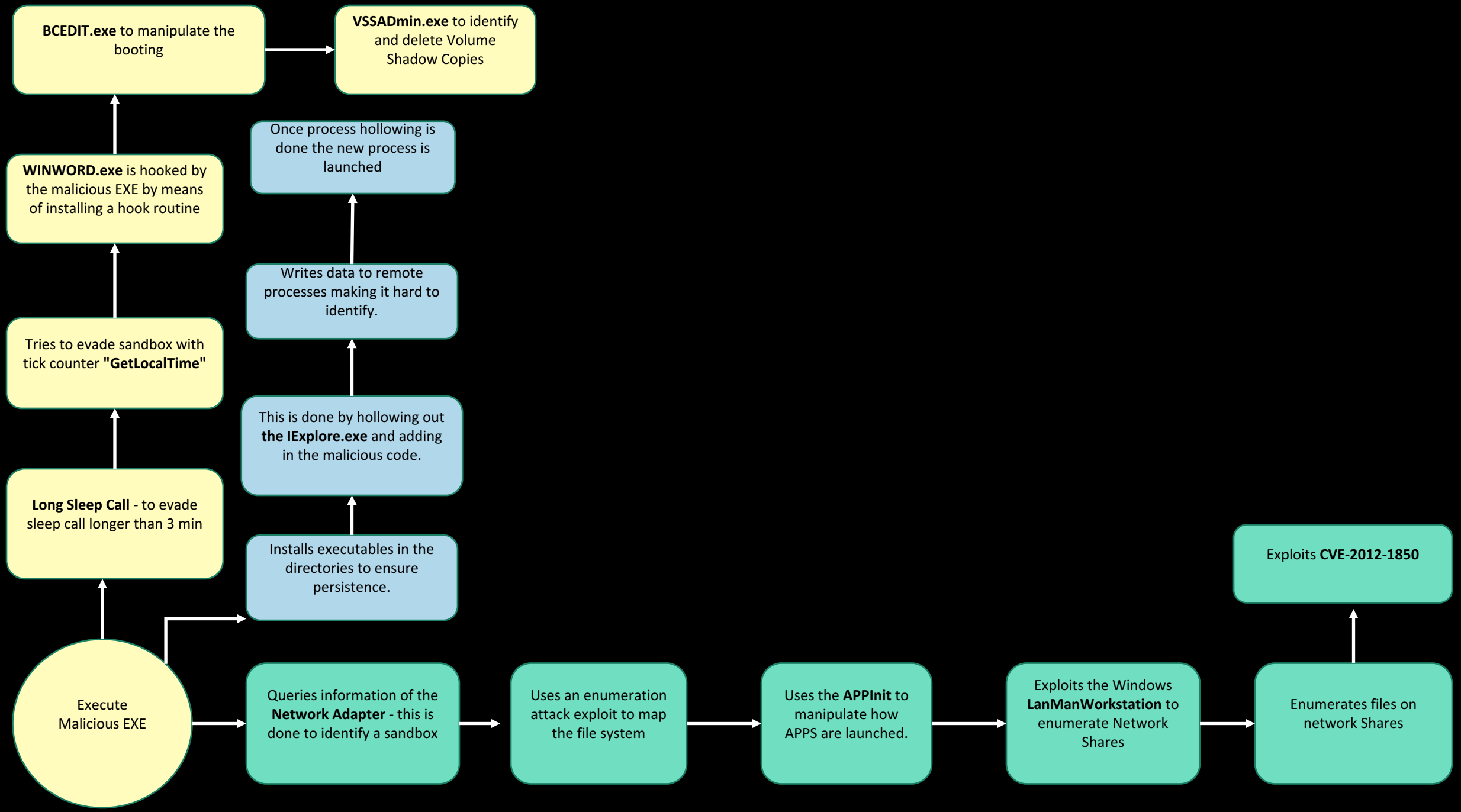
.

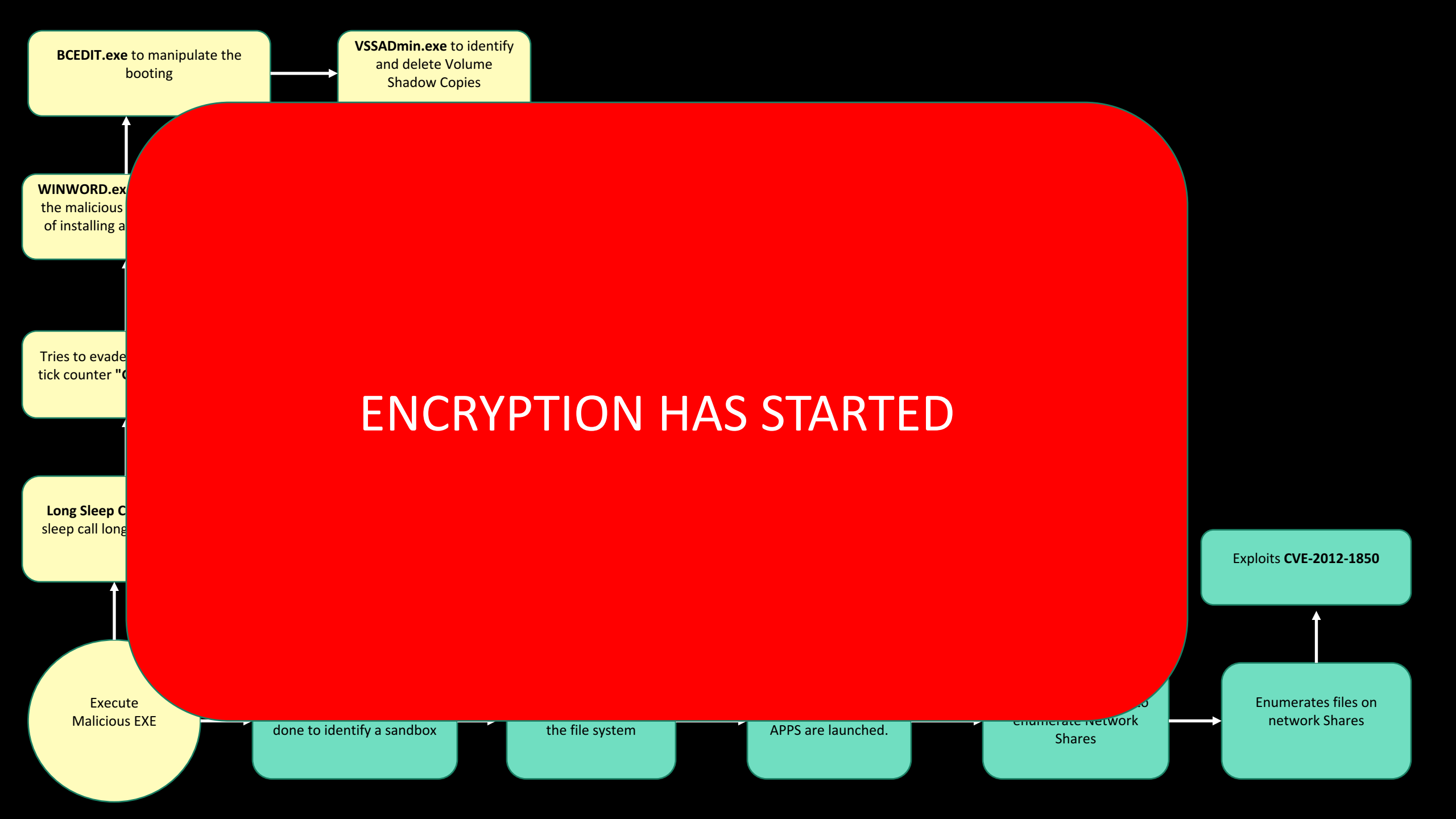
.

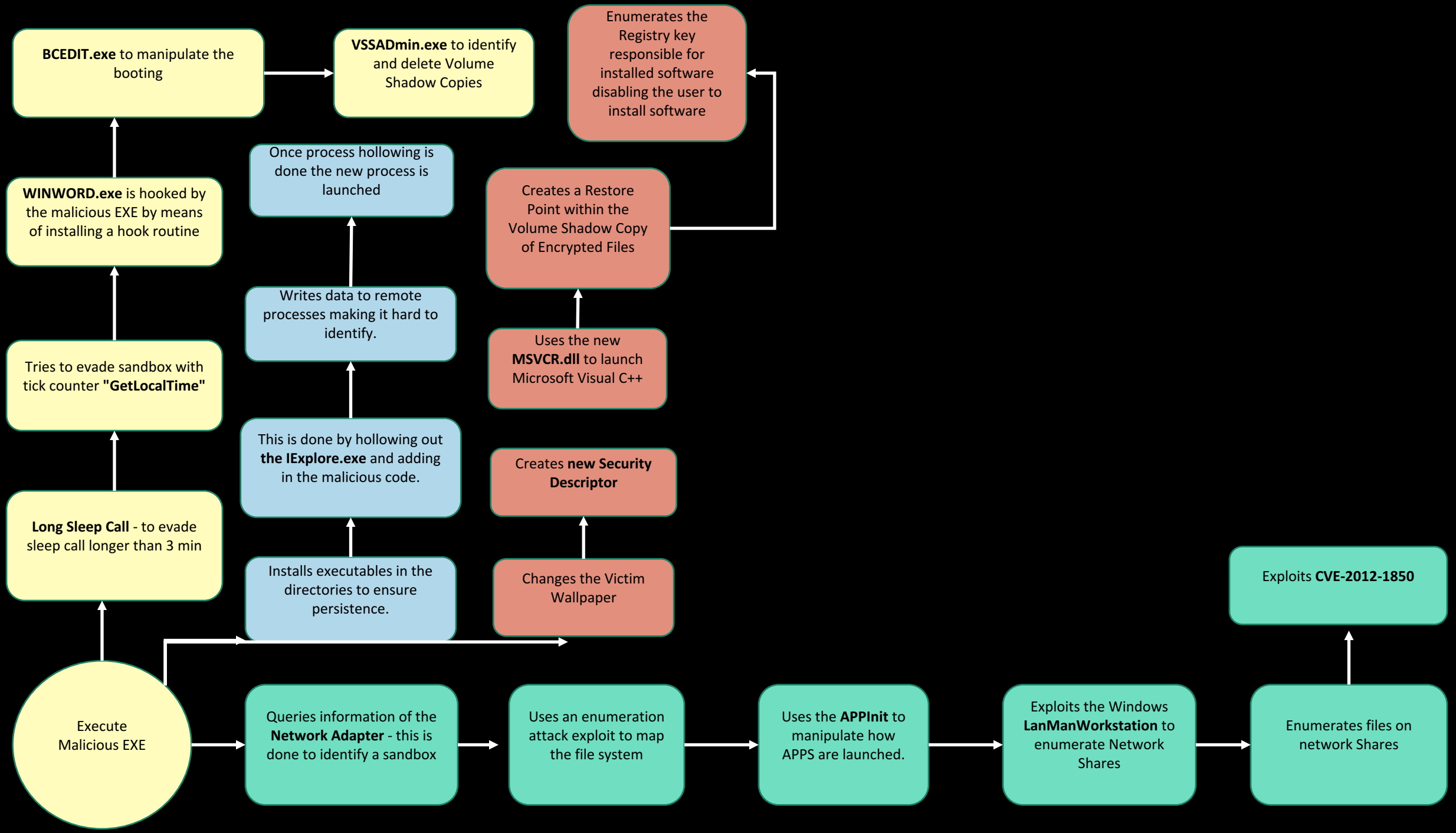
I SENT THEM MY SALARY SLIP...
IMMEDIATELY THEY THEMSELVES
REMOVED IT FROM MY SYSTEM. 😂😂


BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
Tries to evade sandbox with tick counter **"GetLocalTime"**
Long Sleep Call - to evade sleep call longer than 3 min
Execute Malicious EXE


BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
Tries to evade sandbox with tick counter **"GetLocalTime"**
Long Sleep Call - to evade sleep call longer than 3 min
Execute Malicious EXE
Queries information of the **Network Adapter** - this is done to identify a sandbox
Uses an enumeration attack exploit to map the file system
Uses the **APPInit** to manipulate how APPS are launched.
Exploits the Windows **LanManWorkstation** to enumerate Network Shares
Enumerates files on network Shares
Exploits **CVE-2012-1850**


BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
Once process hollowing is done the new process is launched
Tries to evade sandbox with tick counter **"GetLocalTime"**
Writes data to remote processes making it hard to identify.
Long Sleep Call - to evade sleep call longer than 3 min
This is done by hollowing out **the IExplore.exe** and adding in the malicious code.
Installs executables in the directories to ensure persistence.
Exploits **CVE-2012-1850**
Execute Malicious EXE
Queries information of the **Network Adapter** - this is done to identify a sandbox
Uses an enumeration attack exploit to map the file system
Uses the **APPInit** to manipulate how APPS are launched.
Exploits the Windows **LanManWorkstation** to enumerate Network Shares
Enumerates files on network Shares

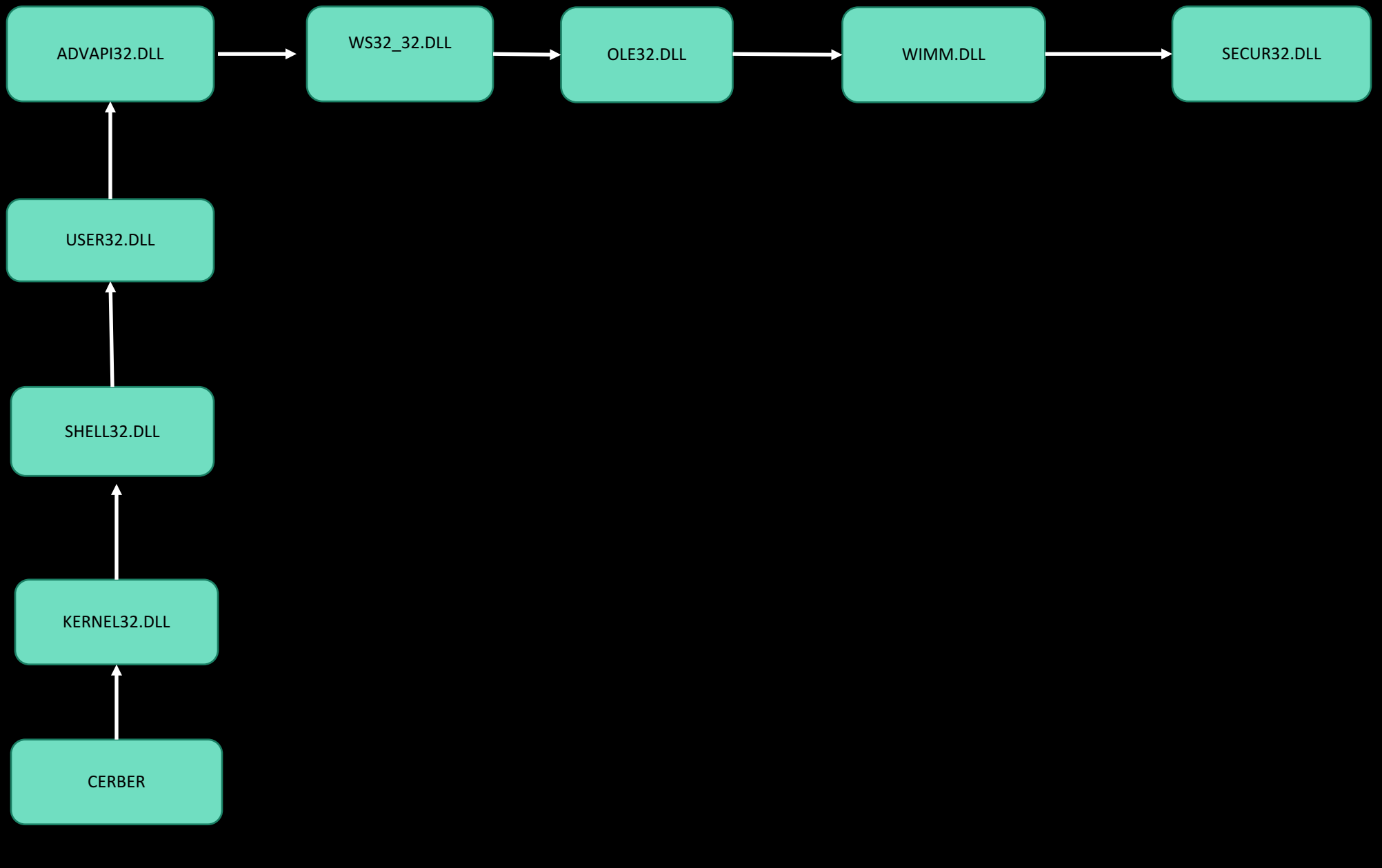

BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies
WINWORD.ex
the malicious
of installing a
Tries to evade
tick counter "
Long Sleep C
sleep call long
ENCRYPTION HAS STARTED
Execute Malicious EXE
done to identify a sandbox
the file system
APPS are launched.
Shares
Exploits **CVE-2012-1850**
Enumerates files on network Shares

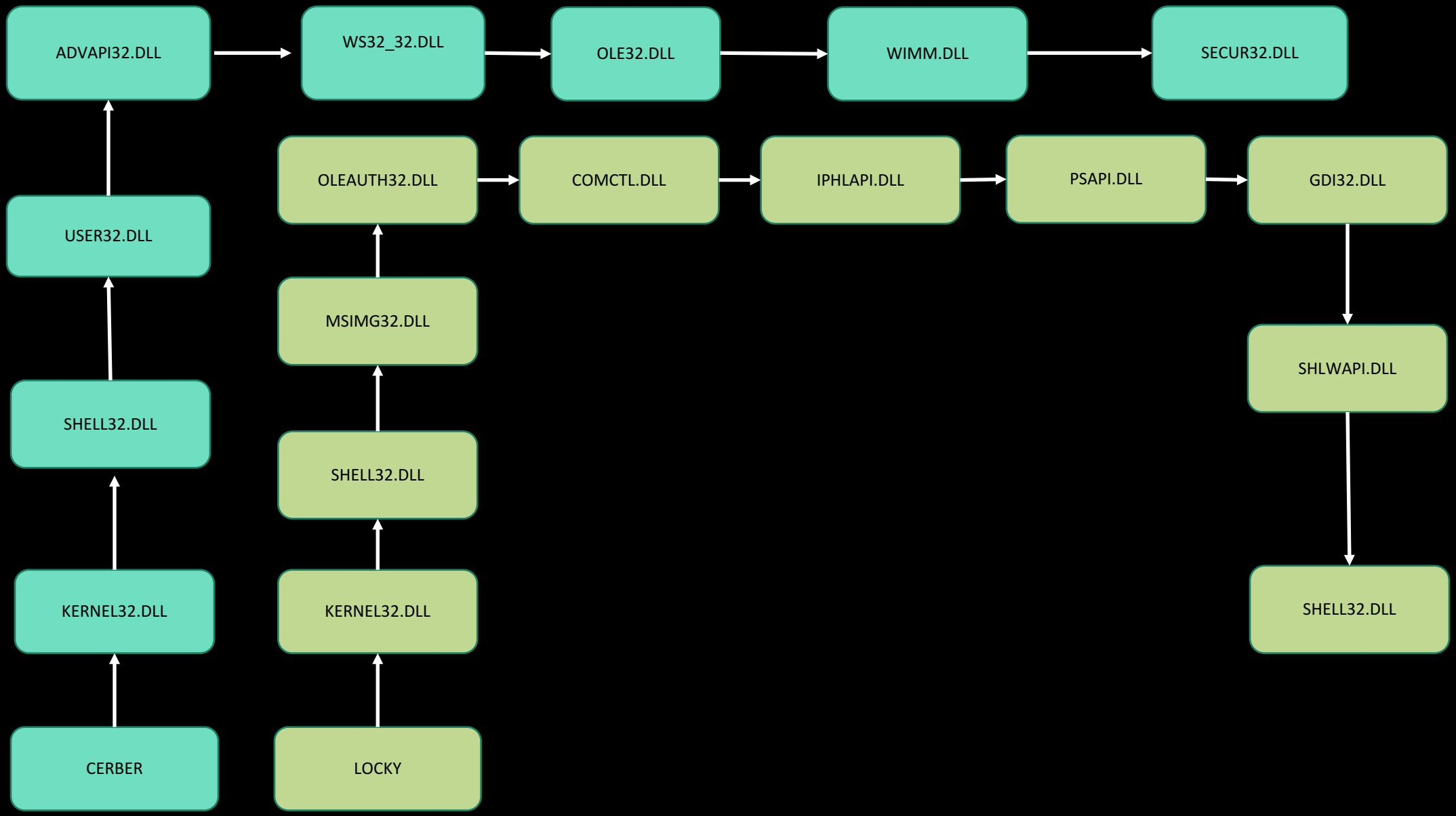

Execute Malicious EXE
Queries information of the **Network Adapter** - this is done to identify a sandbox
Uses an enumeration attack exploit to map the file system
Uses the **APPInit** to manipulate how APPS are launched.
Exploits the Windows **LanManWorkstation** to enumerate Network Shares
Enumerates files on network Shares
Exploits **CVE-2012-1850**
Installs executables in the directories to ensure persistence.
Changes the Victim Wallpaper
Creates **new Security Descriptor**
This is done by hollowing out **the IExplore.exe** and adding in the malicious code.
Writes data to remote processes making it hard to identify.
Once process hollowing is done the new process is launched
Long Sleep Call - to evade sleep call longer than 3 min
Tries to evade sandbox with tick counter **"GetLocalTime"**
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies
Enumerates the Registry key responsible for installed software disabling the user to install software
Creates a Restore Point within the Volume Shadow Copy of Encrypted Files
Uses the new **MSVCR.dll** to launch Microsoft Visual C++


Execute Malicious EXE
Queries information of the **Network Adapter** - this is done to identify a sandbox
Uses an enumeration attack exploit to map the file system
Uses the **APPInit** to manipulate how APPS are launched.
Exploits the Windows **LanManWorkstation** to enumerate Network Shares
Enumerates files on network Shares
Exploits **CVE-2012-1850**
Monitors the HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkProvider\HWOrder
Enumerates the value for **the SASLProfle** responsible for the Simple Authentications and Security Layer
Also used by Boskouk.exe which is classified as a **Troj.Fakeav.sm49**
Queries **Software Policies** to identify which policies are in place
Uses an **OLE-Automation Service** to manipulate the way the executable functions
Enumerates the Registry key responsible for installed software disabling the user to install software
Creates a Restore Point within the Volume Shadow Copy of Encrypted Files
Uses the new **MSVCR.dll** to launch Microsoft Visual C++
Creates **new Security Descriptor**
Changes the Victim Wallpaper
Installs executables in the directories to ensure persistence.
This is done by hollowing out **the IExplore.exe** and adding in the malicious code.
Writes data to remote processes making it hard to identify.
Once process hollowing is done the new process is launched
Long Sleep Call - to evade sleep call longer than 3 min
Tries to evade sandbox with tick counter **"GetLocalTime"**
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies


Execute Malicious EXE
Queries information of the **Network Adapter** - this is done to identify a sandbox
Uses an enumeration attack exploit to map the file system
Uses the **APPInit** to manipulate how APPS are launched.
Exploits the Windows **LanManWorkstation** to enumerate Network Shares
Enumerates files on network Shares
Exploits **CVE-2012-1850**
Exploits the UPnP protocol over port 1900
Accesses UPnP devices to enumerate files
Uses SSDP protocol to send out **SSDP Reflective/Amplified attacks**
Also used by a **Remote Access Trojan**
Monitors the HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkProvider\HWOrder
Enumerates the value for **the SASLProfle** responsible for the Simple Authentications and Security Layer
Also used by Boskouk.exe which is classified as a **Troj.Fakeav.sm49**
Uses an **OLE-Automation Service** to manipulate the way the executable functions
Queries **Software Policies** to identify which policies are in place
Enumerates the Registry key responsible for installed software disabling the user to install software
Creates a Restore Point within the Volume Shadow Copy of Encrypted Files
Uses the new **MSVCR.dll** to launch Microsoft Visual C++
Creates **new Security Descriptor**
Changes the Victim Wallpaper
Installs executables in the directories to ensure persistence.
This is done by hollowing out **the IExplore.exe** and adding in the malicious code.
Writes data to remote processes making it hard to identify.
Once process hollowing is done the new process is launched
Long Sleep Call - to evade sleep call longer than 3 min
Tries to evade sandbox with tick counter **"GetLocalTime"**
WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine
BCEDIT.exe to manipulate the booting
VSSADmin.exe to identify and delete Volume Shadow Copies

WINDOWS API’S EXPLOITED


ADVAPI32.DLL
WS32_32.DLL
OLE32.DLL
WIMM.DLL
SECUR32.DLL
USER32.DLL
SHELL32.DLL
KERNEL32.DLL
CERBER

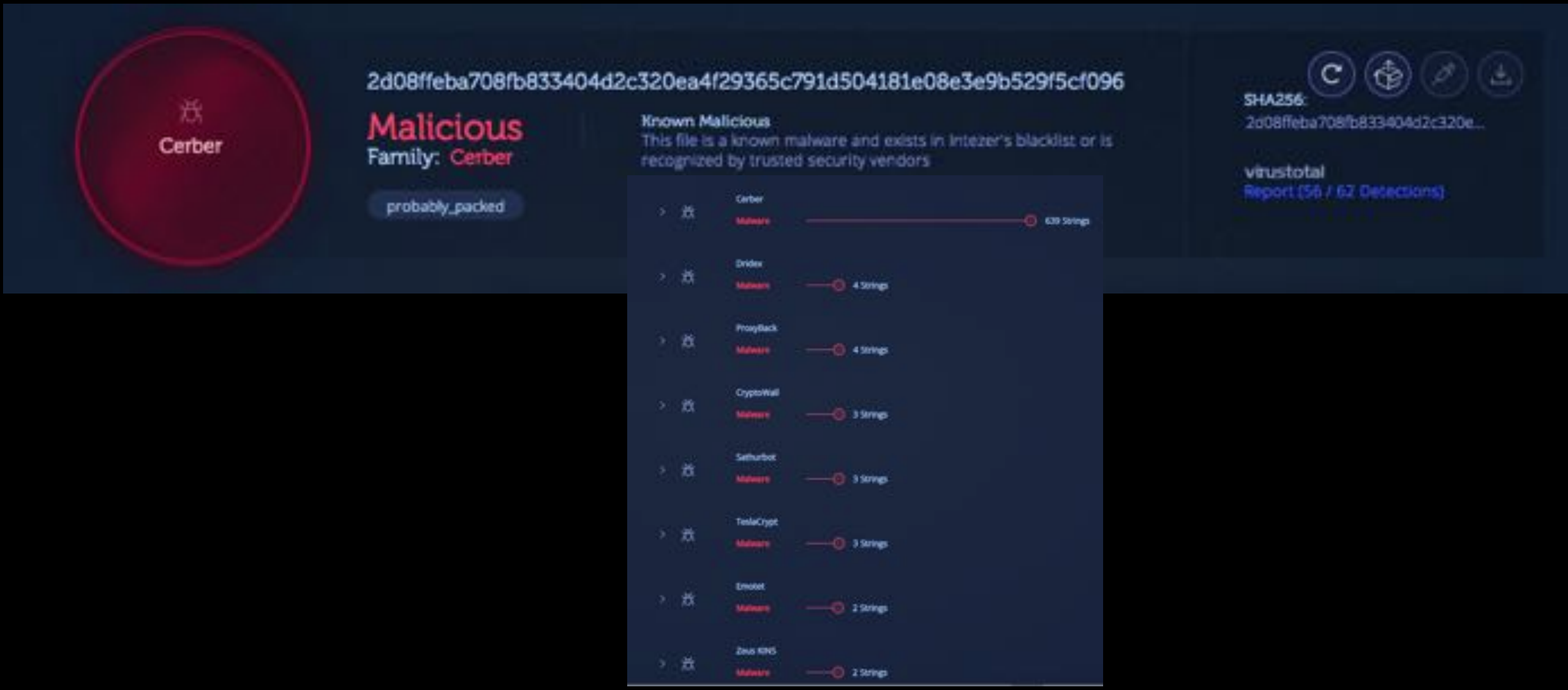

ADVAPI32.DLL
WS32_32.DLL
OLE32.DLL
WIMM.DLL
SECUR32.DLL
USER32.DLL
OLEAUTH32.DLL
COMCTL.DLL
IPHLAPI.DLL
PSAPI.DLL
GDI32.DLL
SHELL32.DLL
MSIMG32.DLL
SHLWAPI.DLL
KERNEL32.DLL
SHELL32.DLL
SHELL32.DLL
CERBER
KERNEL32.DLL
LOCKY


ADVAPI32.DLL
WS32_32.DLL
OLE32.DLL
WIMM.DLL
SECUR32.DLL
USER32.DLL
SHELL32.DLL
KERNEL32.DLL
CERBER
OLEAUTH32.DLL
COMCTL.DLL
IPHLAPI.DLL
PSAPI.DLL
GDI32.DLL
MSIMG32.DLL
SHELL32.DLL
KERNEL32.DLL
LOCKY
GDI32.DLL
SECUR32.DLL
ADVAPI32.DLL
USER32.DLL
KERNEL32.DLL
WS32_32.DLL
MAKTUB
WIMM.DLL
OLE32.DLL
SHLWAPI.DLL
SHELL32.DLL

CERBER DNA


Cerber
2d08ffeba708fb833404d2c320ea4f29365c791d504181e08e3e9b529f5cf096
Malicious
Family: Cerber
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
2d08ffeba708fb833404d2c320e...
virustotal
Report (56 / 62 Detections)

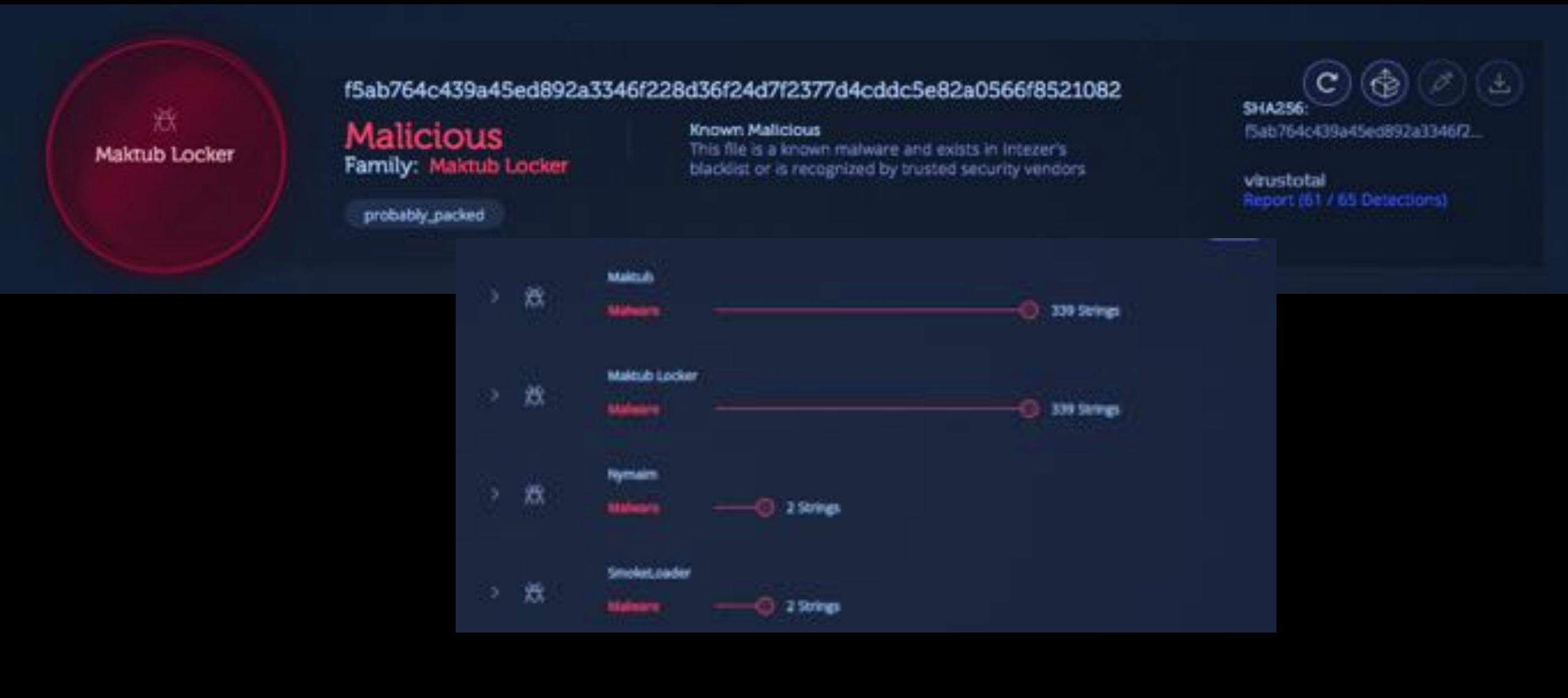
CERBER DNA


Cerber
2d08ffeba708fb833404d2c320ea4f29365c791d504181e08e3e9b529f5cf096
Malicious
Family: Cerber
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
2d08ffeba708fb833404d2c320e...
virustotal
Report (56 / 62 Detections)
Cerber
Malware
639 Strings
Dridex
Malware
4 Strings
ProxyBack
Malware
4 Strings
CryptoWall
Malware
3 Strings
Sathurbot
Malware
3 Strings
TeslaCrypt
Malware
3 Strings
Emotet
Malware
2 Strings
Zeus KINS
Malware
2 Strings

MAKTUB DNA


Maktub Locker
f5ab764c439a45ed892a3346f228d36f24d7f2377d4cddc5e82a0566f8521082
Malicious
Family: Maktub Locker
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
f5ab764c439a45ed892a3346f2...
virustotal
Report (61 / 65 Detections)

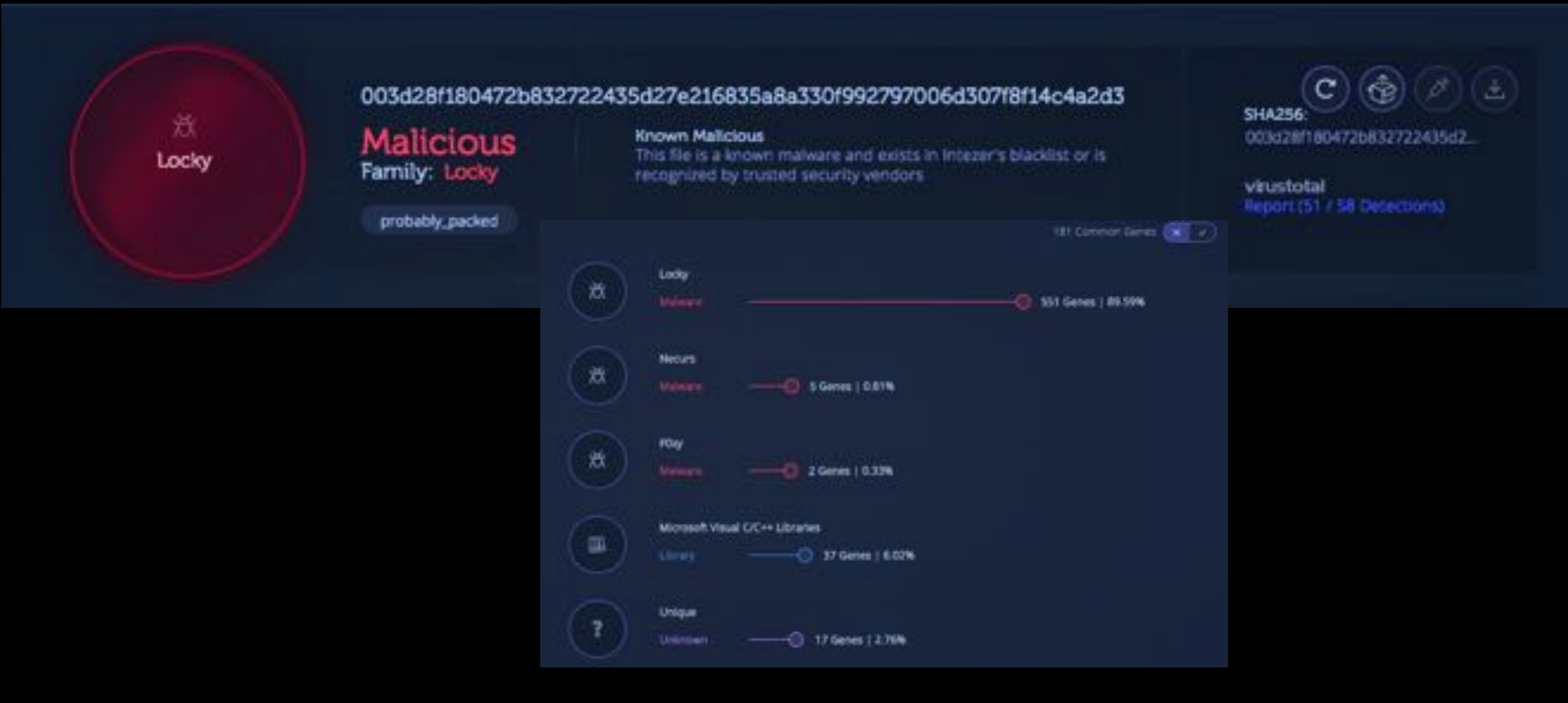
MAKTUB DNA


Maktub Locker
f5ab764c439a45ed892a3346f228d36f24d7f2377d4cddc5e82a0566f8521082
Malicious
Family: Maktub Locker
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
f5ab764c439a45ed892a3346f2...
virustotal
Report (61 / 65 Detections)
Maktub
Malware
339 Strings
Maktub Locker
Malware
339 Strings
Nymaim
Malware
2 Strings
SmokeLoader
Malware
2 Strings

LOCKY DNA


Locky
003d28f180472b832722435d27e216835a8a330f992797006d307f8f14c4a2d3
Malicious
Family: Locky
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
003d28f180472b832722435d2...
virustotal
Report (51 / 58 Detections)

LOCKY DNA


Locky
003d28f180472b832722435d27e216835a8a330f992797006d307f8f14c4a2d3
Malicious
Family: Locky
probably_packed
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors
SHA256:
003d28f180472b832722435d2...
virustotal
Report (51 / 58 Detections)
Locky
Malware
551 Genes | 89.59%
Necurs
Malware
5 Genes | 0.81%
FOxy
Malware
2 Genes | 0.33%
Microsoft Visual C/C++ Libraries
Library
37 Genes | 6.02%
Unique
Unknown
17 Genes | 2.76%

CONTACT DETAILS:

VERONICA SCHMITT (VEE)
+27 82 040 1520
@Po1Zon_P1x13
veronica@dfirlabs.com
https://medium.com/@veronica_66606