Forensic Post Mortem
CERBER, MAKTUB, LOCKY

VERONICA SCHMITT
https://medium.com/@veronica_66606
VERONICA@DFIRLABS.COM
NEW APPROACH TO MALWARE
NEW APPROACH TO MALWARE

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

SEEMS THAT MALWARE ENCRYPTED OUR FILES

INCLUDING OUR BITCOIN WALLET
Execution:
Malicious EXE

Queries Windows Installation date and version

"GetLocalTime" to determine tick count - as a way to evade sandboxes

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
Execution:

- Malicious EXE

Queries Windows Installation date and version

"GetLocalTime" to determine tick count - as a way to evade sandboxes

Uses MACHINEGUID to calculate the unique allocator for tracking infection.

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

Renames itself into a system executable like WINWORD.exe

Writes new EXE into [ROOT]Users\AppData\Roaming

Deletes original malicious EXE

Calls BEDIT.EXE and manipulates the booting sequence of victim machine
Execution : Malicious EXE

Queries Windows Installation date and version

"GetLocalTime" to determine tick count - as a way to evade sandboxes

Uses Page_Guard - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes

Allocates memory in foreign processes

Allocates memory in foreign processes

Calls VSSADMIN.exe to identify and delete Volume Shadow Copies

Uses MACHINEGUID to calculate the unique allocator for tracking infection.

Calls BCEDIT.EXE and manipulates the booting sequence of victim machine

Send Packet to identify geolocation of Victim machine

Compares this with Config file for Blacklisted Countries

Relaunches in Debug Mode.

Kills itself of the system using the TaskKill code.

Renames itself into a system executable like WINWORD.exe

Writes new EXE into [ROOT]Users\AppData\Roaming

Deletes original malicious EXE

Allocates memory in foreign processes

Allocates memory in foreign processes
Encryption has started!

- Execution: Malicious EXE
  - Renames itself into a system executable like WINWORD.exe
  - Writes new EXE into [ROOT]\Users\AppData\Roaming
  - Deletes original malicious EXE
- Allocates memory in foreign processes
- Queries Windows Installation date and version
  - Uses MACHINEGUID to calculate the unique allocator for tracking infection.
  - Compares this with Config file for Blacklisted Countries
  - Send Packet to identify geolocation of Victim machine
  - 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
  - Allocates memory in foreign processes
  - Kills itself of the system using the TaskKill code.
  - Encryption has started!
Execution: Malicious EXE

Queries Windows Installation date and version

"GetLocalTime" to determine tick count - as a way to evade sandboxes

"AllocateandInitializeSID"

CALLS VSSADMIN.EXE to identify and delete Volume Shadow Copies

Uses MACHINEGUID to calculate the unique allocator for tracking infection.

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

Uses Page_Guard - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes

Allocates memory in foreign processes

Allocates memory in foreign processes

Kills itself of the system using the TaskKill code.

Renames itself into a system executable like WINWORD.exe

Write new EXE into [ROOT]\Users\AppData\Roaming

Relaunches in Debug Mode.

Relaunches in Debug Mode.

Send Packet to identify geolocation of Victim machine

Compares this with Config file for Blacklisted Countries

Deletes original malicious EXE

Creates a new Security Descriptor using "AllocateandInitializeSID"
Execution: Malicious EXE

Queries Windows Installation date and version

“GetLocalTime” to determine tick count - as a way to evade sandboxes

Uses Page_Guard - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes

Uses MACHINEGUID to calculate the unique allocator for tracking infection.

Allocates memory in foreign processes

Calls VSSADMIN.exe to identify and delete Volume Shadow Copies

Calls BCEDIT.EXE and manipulates the booting sequence of victim machine

Communicates statistics of SPAM emails via UDP to CNC

Enables email address book and sends out SPAM.

Accesses email address book and sends out SPAM.

Compares this with Config file for Blacklisted Countries

Downloads 33 sections which contain encryption from various domains.

Creates a new Security Descriptor using "AllocateAndInitializeSID"

Enumerates the network shares using "NetAPI" which is native to Windows

Relaunches in Debug-Mode.

VSSADMIN.exe to identify and delete Volume Shadow Copies

Calls BCEDIT.EXE and manipulates the booting sequence of victim machine

Send Packet to identify geolocation of Victim machine

Uses MACHINGUID to calculate the unique allocator for tracking infection.

COM Classes are used to hook onto legitimate services. Re-associates the dll which is associated with a legitimate dll

Write to the ZoneIdentifiers

Kills itself of the system using the TaskKill code.

Allocates memory in foreign processes

Allocates memory in foreign processes

Enumerates the network shares using "NetAPI" which is native to Windows

Resets itself into a system executable like WINWORD.exe

Write new EXE into [ROOT]Users\AppData\Roaming

Deleting original malicious EXE

Enrolls machine as BOTNET

Communicates with a CNC

Post Exploitation downloads a payload of WIN32 Salty

GET/json HTTP/1.1 Host: IpInfo.io

DELETE GET/json HTTP/1.1 Host: IpInfo.io

Downloads 33 sections which contain encryption from various domains.

Communicates statistics of SPAM emails via UDP to CNC

Enumerates the network shares using "NetAPI" which is native to Windows

Uses Page_Guard - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes

Queries Windows Installation date and version

“GetLocalTime” to determine tick count - as a way to evade sandboxes

Uses MACHINEGUID to calculate the unique allocator for tracking infection.

Allocates memory in foreign processes

Allocates memory in foreign processes

Enumerates the network shares using "NetAPI" which is native to Windows

Resets itself into a system executable like WINWORD.exe

Write new EXE into [ROOT]Users\AppData\Roaming

Deleting original malicious EXE

Enrolls machine as BOTNET

Communicates with a CNC

Post Exploitation downloads a payload of WIN32 Salty

GET/json HTTP/1.1 Host: IpInfo.io

DELETE GET/json HTTP/1.1 Host: IpInfo.io

Downloads 33 sections which contain encryption from various domains.

Communicates statistics of SPAM emails via UDP to CNC

Enumerates the network shares using "NetAPI" which is native to Windows

Uses Page_Guard - protects memory spaces to ensure the data cannot be accessed once it is assigned to processes

Queries Windows Installation date and version

“GetLocalTime” to determine tick count - as a way to evade sandboxes

Uses MACHINEGUID to calculate the unique allocator for tracking infection.
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
Executes a malicious EXE
Installs Remote Access Trojan
Downloads Locky Payload
Uses undocumented registry key in RunOnce to maintain persistence
Escalate Privileges to Kernel level
Accesses BCEDIT.exe to manipulate booting process
Accesses VSADMIN.exe to identify and delete Volume Shadow Copies
Execute Malicious EXE

Installs Remote Access Trojan

Downloads Locky Payload

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Changes user Wallpaper by executing a Shell Script
Execute Malicious EXE

- Installs Remote Access Trojan
- Downloads Locky Payload
- Uses Native Cryptographic Service Providers for encryption process
- Uses "Page_Execute_ReadOnlyWrite" to unpack Locky Payload
- Uses undocumented registry key in RunOnce to maintain persistence
- Uses "GetLocalTime" to evade sandbox using local time tick counts
- Enumerates the file systems
- Uses the NTDLL.dll to kill process
- Changes user Wallpaper by executing a Shell Script
- Obtains Logical Drive size using "GetLogicalDrive"
- Escalate Privileges to Kernel level
- Reads Host files and rewrites them to connect to specific Web Server

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies
Execute Malicious EXE

Installs Remote Access Trojan

Downloads Locky Payload

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Obtains Logical Drive size using "GetLogicalDrive"

Reads Host files and rewrites them to connect to specific Web Server

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses "Page_Execute_ReadOnlyWrite" to unpack Locky Payload

Uses Native Cryptographic Service Providers for encryption process

Uses MACHIN

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses the NTDLL.dll to kill process

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Uses the NTDLL.dll to kill process

Changes user Wallpaper by executing a Shell Script

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses MACHIN

Queries Registry Key for Internet Cache to obtain SSL keys

Queries Software Policies this key is only read

COM Classes is exploited to manipulate class associated with specific dll using ole32.dll

Accesses BCEDIT.exe to manipulate booting process

VSADMIN.exe is accessed to identify and delete Volume Shadow Copies

Executes Malicious EXE

Installs Remote Access Trojan

Downloads Locky Payload

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Obtains Logical Drive size using "GetLogicalDrive"

Reads Host files and rewrites them to connect to specific Web Server

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses "Page_Execute_ReadOnlyWrite" to unpack Locky Payload

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINE
Execute Malicious EXE

Installs Remote Access Trojan

Downloads the Zeus Bot Downloader

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Uses the NTDLL.dll to kill process

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "GetLogicalDrive" to obtain to obtain SLL keys

Queries Registry Key for Internet Cache to obtain to obtain SLL keys

Obtains Logical Drive size using "GetLogicalDrive"

Reads Host files and rewrites them to connect to specific Web Server

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 HTTP POST to exfiltrate pre-encryption data.

Sent to DGA created domains

Forms part of the EK Malware Campaign

Contacts domain for Payload download

Uses HTTP POST to exfiltrate pre-encryption data.

Downloads the Zeus Bot Downloader

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses the NTDLL.dll to kill process

Enumerates the file systems

Uses "GetLocalTime" to evade sandbox using local time tick counts

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"

Uses Native Cryptographic Service Providers for encryption process

Uses MACHINEGUID to track infection and create Mutexes

Contacts domain for Payload download

Downloads Payload and facilitates encryption

Uses "Page_Execute_Rea dWrite" to unpack Locky Payload

Uses Documented registry key in RunOnce to maintain persistence

Uses Remote Access Trojan to create Backdoor onto system

Uses undocumented registry key in RunOnce to maintain persistence

Escalate Privileges to Kernel level

Accesses BCEDIT.exe to manipulate booting process

Uses MSEXPORT to manipulate "Page_Execute_Rea dWrite"
I got attacked by ransomware and was asked for money...
.
.
I sent them my salary slip... immediately they themselves removed it from my system. 😂 😂
Execute Malicious EXE

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

WinWORD.exe is hooked by the malicious EXE by means of installing a hook routine

Long Sleep Call - to evade sleep call longer than 3 min

Tries to evade sandbox with tick counter "GetLocalTime"

BEDIT.exe to manipulate the booting

VSSADmin.exe to identify and delete Volume Shadow Copies
Execute Malicious EXE

BCEDIT.exe to manipulate the booting

WINWORD.exe is hooked by the malicious EXE by means of installing a hook routine

Tries to evade sandbox with tick counter "GetLocalTime"

VSSADmin.exe to identify and delete Volume Shadow Copies

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.

Query 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.

Installs executables in the directories to ensure persistence.

Exploits the Windows LanManWorkstation to enumerate Network Shares

Exploits CVE-2012-1850

Enumerates files on network Shares

Written data to remote processes making it hard to identify.

Once process hollowing is done the new process is launched
Execute Malicious EXE

- 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

This is done by hollowing out the IExplore.exe and adding in the malicious code.

ENCRYPTION HAS STARTED

WINWORD.exe to manipulate 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

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

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
**Execute Malicious EXE**

**WINWORD.exe** is hooked by the malicious EXE by means of installing a hook routine

**Long Sleep Call** - to evade sleep call longer than 3 min

**Tries to evade sandbox with tick counter “GetLocalTime”**

**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

Once process hollowing is done the new process is launched

Creates a Restore Point within the Volume Shadow Copy of Encrypted Files

Uses the new MSVCRT.dll to launch Microsoft Visual C++

Creates new Security Descriptor

Uses the new MSVCR.dll to launch Microsoft Visual C++

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.

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

Exploits CVE-2012-1850

Enumerates files on network Shares

Exploits the Windows LanManWorkstation to enumerate Network Shares

Enumerates files on network Shares
Execute Malicious EXE

- 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
- Uses an OLE-Automation Service to manipulate the way the executable functions
- Queries Software Policies to identify which policies are in place
- Uses SSDP protocol to send out SSDP Reflective/Amplified attacks
- Accesses UPnP devices to enumerate files
- Exploits the UPnP protocol over port 1900
- Exploits CVE-2012-1850
- Enumerates files on network Shares

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

- This is done by hollowing out the IExplore.exe and adding in the malicious code.
- Creates new Security Descriptor
- Uses the new MSVCR.dll to launch Microsoft Visual C++
- Enumerates the value for the SASProfile responsible for the Simple Authentications and Security Layer
- Also used by Boskouk.exe which is classified as a Troj.Fakeav.sm49
- Also used by a Remote Access Trojan

- Uses SSDP protocol to send out SSDP Reflective/Amplified attacks

- Winword.exe is hooked by the malicious EXE by means of installing a hook routine

- 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.
- Uses the APPInit to manipulate how APPS are launched.
- Exploits the Windows LanManWorkstation to enumerate Network Shares
- Exploits the Windows LanManWorkstation to enumerate Network Shares
- Enumerates files on network Shares

- Monitors the HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\NetworkProvider\HWOrder
- Uses SSDP protocol to send out SSDP Reflective/Amplified attacks

- Accesses UPnP devices to enumerate files
- Exploits the UPnP protocol over port 1900
- Exploits CVE-2012-1850
- Enumerates files on network Shares

- Uses the new MSVCR.dll to launch Microsoft Visual C++
- Creates a Restore Point within the Volume Shadow Copy of Encrypted Files
- Changes the Victim Wallpaper
- Instantiates the executables in the directories to ensure persistence.
- Writes data to remote processes making it hard to identify.
- Writes data to remote processes making it hard to identify.
- Also used by Boskouk.exe which is classified as a Troj.Fakeav.sm49
- Also used by a Remote Access Trojan
- Uses the new MSVCR.dll to launch Microsoft Visual C++
WINDOWS API’S EXPLOITED
CERBER
KERNEL32.DLL
SHELL32.DLL
USER32.DLL
ADVAPI32.DLL
WS23_32.DLL
OLE32.DLL
WIMM.DLL
SECUR32.DLL
USER32.DLL
SHELL32.DLL
KERNEL32.DLL
CERBER
CERBER DNA

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

- Cerber
- Malware
- Packed

- Driller
- Malware
- 4 Strings

- Proyback
- Malware
- 4 Strings

- CryptoWall
- Malware
- 3 Strings

- Setubot
- Malware
- 3 Strings

- TeslaCrypt
- Malware
- 3 Strings

- Emotet
- Malware
- 2 Strings

- Zeus KINS
- Malware
- 2 Strings

SHA256:
2d08ffe708/fb83340d2c320ea4f29365c791d50418e08e3e9b529f5cf096

virus.total
Report (56 / 62 Detections)
MAKTUB DNA
MAKTUB DNA
LOCKY DNA

003d28f180472b832722435d27e216835a8a330f992797006d307f8f14c4a2d3

Malicious
Family: Locky
Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors.

SHA256: 003d28f180472b832722435d2

virusotal:
Report (51 / 58 Detections)
LOCKY DNA
CONTACT DETAILS:

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