Remcos RAT Analysis

Incident Response Exercise

Q3 2022

Analyst: C. K.
Light on Security
lightonsec@gmail.com

Table of Contents

Light on Security
lightonsec@gmail.com

Introduction : Incident Response Exercise

Purpose
The primary objective of this report was to practice skills in the following domains:

- Incident Response
- Digital Forensics
- Malware Analysis
- Reverse Engineering

Light on Security
lightonsec@gmail.com

Skills from these domains are used for the purpose of responding to real-time incidents, or proactively developing IOCs for the purpose of threat hunting.

Lab
This incident response exercise was conducted in a modest lab environment with the following specifications:

- Hypervisor: Oracle Virtual Box 6.1
- Guest: Windows 10 Pro x64
- Host: Kali, Linux 5.17.0-kali3-amd64
- Network: Host-only 192.168.56.0/24

Scenario
A user received a phishing email with a malicious attachment, and executed the unauthorized software on a company asset.

Light on Security
lightonsec@gmail.com

Threat
The threat analyzed in this exercise was Remcos Remote Control & Surveillance Software v3.5.1, released 20 May 2022. The trojan variant examined in this report was obtained through Malware Bazaar; the URL to the sample is available in *Appendix B – Resources, Malware Bazaar Sample*.

Incident Response Lifecycle
This exercise operates within the framework of CISA's Incident Response Process as seen below:

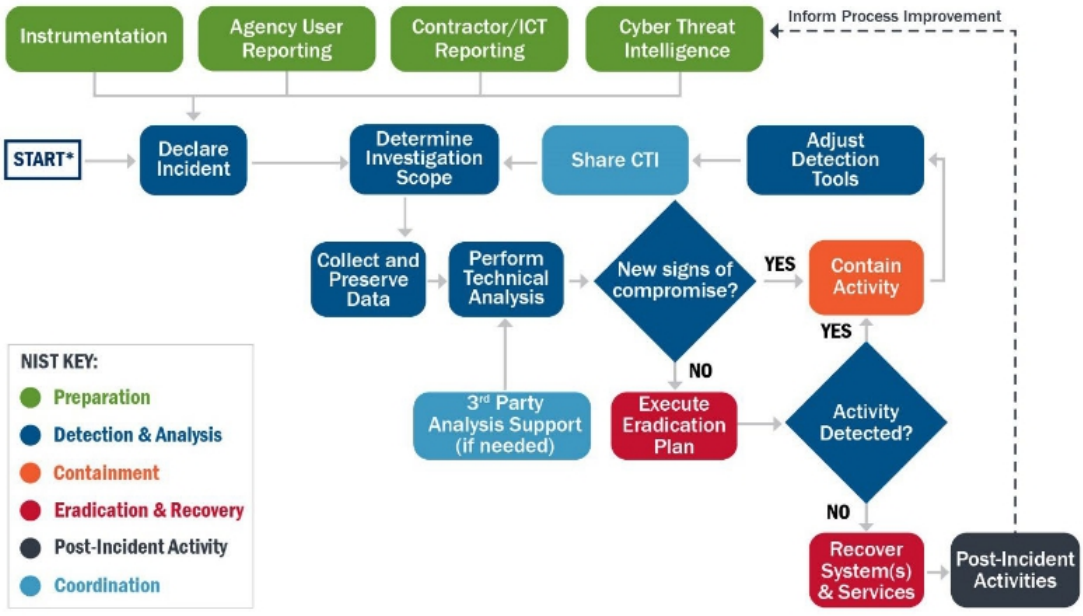


Figure 1 : Cybersecurity & Infrastructure Security Agency Incident Response Process

This exercise covers the following Incident Response phases:

- Phase I Cyber Threat Intelligence
- Phase II Detection and Analysis
- Phase III Containment
- Phase IV Eradication and Recovery Options
- Phase V Post-Incident Activities

Light on Security
lightonsec@gmail.com

Phase I : Cyber Threat Intelligence

Authority:

"Actively monitor intelligence feeds for threat or vulnerability advisories from government, trusted partners, open sources, and commercial entities."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 7.

Phase I : Cyber Threat Intelligence introduces Remcos; the origin, TTPs, recent news coverage, and threat actors known to use Remcos in their campaigns are briefly discussed.

Introduction to Remcos

Light on Security

Remcos is distributed by a company called Breaking Security; in their own words:

BreakingSecurity is a CyberSecurity and Software Engineering company registered in Rome, Italy.
It was born from a lifetime passion for computers, technology, and security.
We create and provide several software and services, especially focused on Defensive/Offensive CyberSecurity, Surveillance, Penetration Testing, to individuals and companies all over the world.

We have over 12 years of experience in the CyberSecurity field and in Software Development in many programming languages, including C, C++, Delphi, PHP, VB6, and more.
We also provide CyberSecurity courses to companies and organizations.

Figure 2 : About Breaking Security

Remcos Description from Breaking Security:

"Control remotely your computers, anywhere in the world. Remcos is a lightweight, fast and highly customizable Remote Administration Tool with a wide array of functionalities."

Light on Security

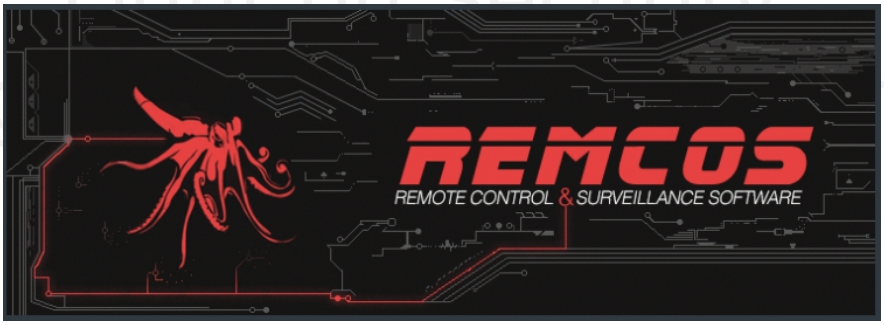


Figure 3 : Remcos Sigil

Functionalities:

Screen capture, file manager, file search, process manager, service manager, registry editor, installed programs, window manager, clipboard manager, execute command, command line, remote scripting, set wallpaper, power manager, webcam, microphone, keylogger, screen logger, browser history, password recovery, activity notification, SOCKS proxy, chat, message box, downloader, open webpage, logins cleaner, dll loader, audio player, fun functions, rename, ping, reconnect, restart, show, elevate, update, close, uninstall.

Relevant Version Information:

- v3.8.0, Released 21 August 2022 : Latest version as of this writing.
- v3.5.1, Released 20 May 2022 : Version analyzed in this report.
- V 1.0, Released 21 Jul 2016 : First public release of Remcos.

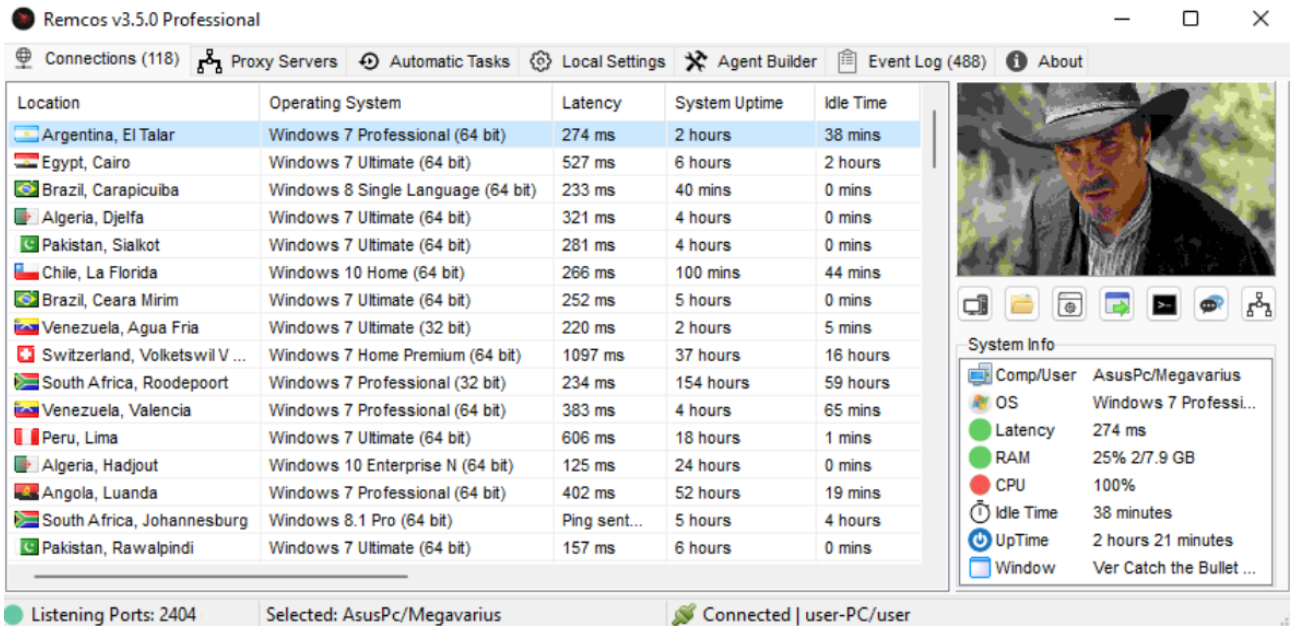


Figure 4 : Remcos v3.5.0 Professional Dashboard

Threat Intelligence

Tracking Remcos:

Remcos is an active threat as proven by the Spamhaus Botnet Threat Update report; the graphs below illustrate how Remcos increased activity from position #11 in Q1 to position #7 in Q2 of 2022:

Light on Security
lightonsec@gmail.com

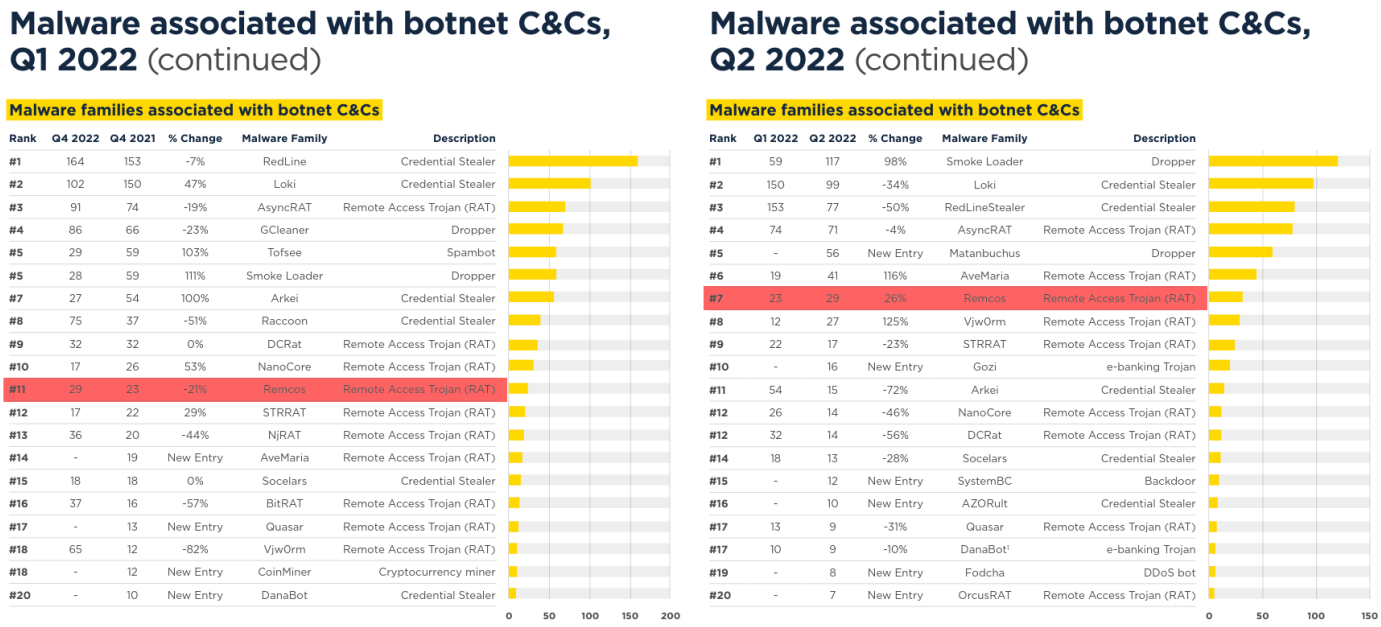


Figure 5 : Q1 vs Q2 Spamhaus Botnet Threat Update

Associated Threat Actors:

- **APT33** : Active since 2013; associated with Iran. Multi-industry attacks with emphasis in aviation and energy sectors. Targets include United States, Saudi Arabia, South Korea.
- **The Gorgon Group** : Associated with Pakistan; targeted attacks against governments of UK, Spain, Russia, United States.
- **LazyScripter** : Active since 2018; primary target is the airline industry; heavy reliance on open-source tools.

Q2 2022 News:

2022-04-06 · Fortinet · Xiaopeng Zhang
The Latest Remcos RAT Driven By Phishing Campaign
https://www.fortinet.com/blog/threat-research/latest-remcos-rat-phishing

2022-04-12 · HP · Patrick Schläpfer
Malware Campaigns Targeting African Banking Sector
https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/

2022-05-05 · Muhammad Hasan Ali
Analysis of MS Word to drop Remcos RAT | VBA extraction and analysis | IoCs
https://muha2xmad.github.io/mal-document/remcosdoc/

MITRE ATT&CK TTP:

Domain	ID	Name
Enterprise	T1548 .002	Abuse Elevation Control Mechanism: Bypass User Account Control
Enterprise	T1123	Audio Capture
Enterprise	T1547 .001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Enterprise	T1115	Clipboard Data

Enterprise	T1059 .003	Command and Scripting Interpreter: Windows Command Shell
Enterprise	T1059 .006	Command and Scripting Interpreter: Python
Enterprise	T1083	File and Directory Discovery
Enterprise	T1105	Ingress Tool Transfer
Enterprise	T1056 .001	Input Capture: Keylogging
Enterprise	T1112	Modify Registry
Enterprise	T1027	Obfuscated Files or Information
Enterprise	T1055	Process Injection
Enterprise	T1090	Proxy
Enterprise	T1113	Screen Capture
Enterprise	T1125	Video Capture
Enterprise	T1497 .001	Virtualization/Sandbox Evasion: System Checks

This concludes *Phase I : Cyber Threat Intelligence*; this section briefly profiled Remcos to include details on its origin, TTPs, recent news coverage, and threat actors known to use Remcos in their campaigns. The reader should now understand Remcos is a Remote Surveillance & Control Software first released in 2016 by Italian company Breaking Security, and continues to remain in development. The Spamhaus Botnet Threat Report for Q2 2022 observed an increase in Remcos botnet activity, suggesting it continues to be weaponized in threat actor campaigns; it is used by at least three well known threat actors with interests against United States, as well as industries focused on aviation and the energy sector. Remcos poses a serious threat against system confidentiality, integrity, and availability as it has a variety of stealth features including screen capture, keylogging, remote command execution, and more.

Phase II : Detection and Analysis

Phase II : Detection and Analysis is the most dense section of this report; it achieves the following objectives:

1. Develop a timeline to explain the incident
2. Extract malware indicators of compromise
3. Integrate IOCs into existing security monitoring tools to detect, contain, and remediate compromised endpoints

Section A : Declare Incident

Authority:

“An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”

NIST Glossary, “Computer Security Incident”

Scenario

A user received an email with an attached excel spreadsheet entitled *SHIPPING ADVICE#NEW*. When the spreadsheet didn't open as expected, the user reported this malfunction to the service desk. Using Ivanti Remote Control, the call center technician identified a strange process running on the endpoint called *zaymjsmod.exe* and escalated the ticket to the Computer Security Incident Response team.

This hypothetical scenario is well suited for the Remcos trojan, given it has a history of distribution via phishing campaigns (see *Phase I : Cyber Threat Intelligence, Threat Intelligence, Q2 2022 News*). Furthermore in 2022, IBM Security X-Force reported threat actors continue to use Phishing (T1566) as a Top Initial Access vector:

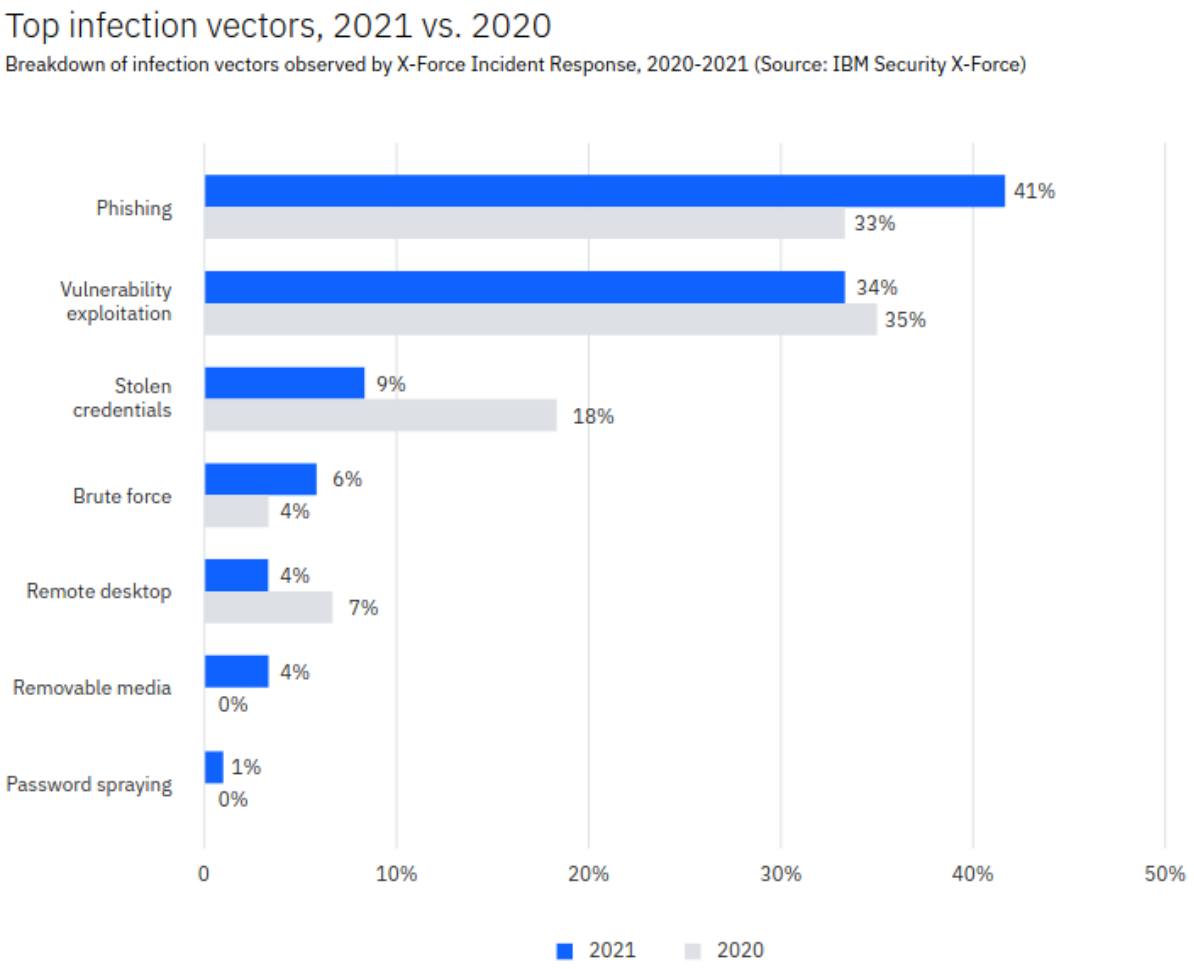


Figure 6 : IBM Security X-Force Threat Intelligence Index 2022

In accordance with the NIST definition above, this event qualifies as a computer security incident due to user execution of unauthorized software on a company asset which violates the CIA of the endpoint; therefore the next step in the investigation is to collect and verify evidence of the compromised system.

Section B : Collect and Preserve Data

Authority:

"Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution. When necessary and possible, such information should be preserved and safeguarded as best evidence for use in any potential law enforcement investigation."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 10.

lightonsec@gmail.com

Section B : Collect and Preserve Data will discuss the acquisition and verification of disk, memory, and network traffic obtained from the live Windows 10 Pro guest after the Remcos infection occurred.

Task 1 : Evidence Acquisition

Evidence from the compromised Windows 10 guest was acquired through the following methods:

- Live disk imaged from the guest with Cygwin/dd.
- Live memory dumped from the guest with Comae/DumpIt.
- Live traffic captured from the guest with Wireshark.

Evidence acquisition is not documented in this report. All evidence files were transferred from Windows 10 guest to Kali host via Virtual Box shared folder.

Light on Security
lightonsec@gmail.com

Task 2 : Evidence Verification

Evidence files must be verified before the investigation can begin; this involves two steps:

1. Calculating evidence file hashes
2. Proving evidence files are functional

Hash algorithms are one way functions used to verify the integrity of data. Modified evidence will corrupt the credibility of a forensic investigation; therefore the hashing of evidence files is used to verify evidence integrity hasn't been compromised during forensic analysis. Figure 7 below illustrates a sha256 hash for each read-only evidence file (disk, memory, network traffic):

```
.../analysis-i-remcosrat/forensics/disk/remcos-disk.dd
-r--r--r-- 1 ... ... 50G Jul 20 14:25
ae2187c7bfe96e230d2797228c30cdf34e6fbe653f2d87066491b7948e4b83ff

.../analysis-i-remcosrat/forensics/memory/remcos-mem.dmp
-r--r--r-- 1 ... ... 8.0G Jul 20 13:41
3c82c93bec653c9421f0b29e9b8c4973ec46ed82f5232b608a9e991f5b3cf464

.../analysis-i-remcosrat/forensics/network/remcos-traffic.pcapng
-r--r--r-- 1 ... ... 282K Jul 20 15:37
4d268ec249e34028ad22d0b312a3aa24dabf0c90f9dbedceec6301250965f3e4
```

Figure 7 : sha256sum output for all evidence files

After calculating evidence hashes, the next step is to ensure all evidence is functional; then the examination can begin. In the image below, fdisk is used to identify the partitions of the image file taken using Cygwin/dd:

```
$ fdisk -l disk/remcos-disk.dd
Disk disk/remcos-disk.dd: 50 GiB, 53687091200 bytes, 104857600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x6d78763b

Device                Boot     Start       End   Sectors  Size Id Type
disk/remcos-disk.dd1  *         2048    104447    102400   50M  7 HPFS/NTFS/exFAT
disk/remcos-disk.dd2          104448 103809676 103705229 49.5G  7 HPFS/NTFS/exFAT
disk/remcos-disk.dd3       103811072 104853503   1042432  509M 27 Hidden NTFS WinRE
```

Figure 8 : Available partitions listed using fdisk

All partitions appear intact; partition two is highlighted as it is the most critical, given that is where the evidence is located. Next, log2timeline/plaso must be able to read the partitions:

```
Checking availability and versions of dependencies.
[OK]

The following partitions were found:

Identifier      Offset (in bytes)              Size (in bytes)
p1              1048576 (0x00100000)           50.0MiB / 52.4MB (52428800 B)
p2              53477376 (0x03300000)          49.5GiB / 53.1GB (53097077248 B)
p3              53151268864 (0xc60100000)      509.0MiB / 533.7MB (533725184 B)

Please specify the identifier of the partition that should be
processed. All partitions can be defined as: "all". Note that you can
abort with Ctrl^C.

Partition identifier(s):
```

Figure 9 : Log2timeline can read the partitions

The final test is to verify the disk image can be mounted as read only and the evidence files can be accessed / extracted:

```
root@siftworkstation:/media/sf_disk_1#
root@siftworkstation:/media/sf_disk_1#
root@siftworkstation:/media/sf_disk_1# mount -ro,loop,offset=53477376 remcos-disk.dd /mnt/windows_mount
root@siftworkstation:/media/sf_disk_1#
root@siftworkstation:/media/sf_disk_1# sha256sum /mnt/windows_mount/.../SHIPPING\ ADVICE#NEW.exe
900274d5916f078ac30bedfc6b3bf5812c09de4cc1bdddd4e25d5efa1e3bb1c3
root@siftworkstation:/media/sf_disk_1#
root@siftworkstation:/media/sf_disk_1#
root@siftworkstation:/media/sf_disk_1# xxd /mnt/windows_mount/.../SHIPPING\ ADVICE#NEW.exe | head
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 d800 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: e571 4aa8 a110 24fb a110 24fb a110 24fb  .qJ...$...$...$.
00000090: 2f18 7bfb a310 24fb a110 25fb 3b10 24fb  /.{...$...%.;.$.
root@siftworkstation:/media/sf_disk_1#
```

Figure 10 : Verifying disk image on SIFT Workstation.

The commands are as follows:

#	Command	Description
1	mount -ro,loop,offset=53477376 [image.dd] /mnt/windows_mnt	Mount the image as read-only beginning at offset 53477376 for partition 2
2	sha256sum [file.exe]	Identify the hash of the malware
3	xxd [file.exe] | head	Examine the file header of malware using hex / ascii

Eight on Security
lightonsec@gmail.com

This completes the disk evidence verification process; the next objective is to verify the memory is intact.

The image below is output from Volatility 3; it confirms Volatility version information, processor type, Windows version, root directory, and the system timestamp. In-depth analysis of this memory dump will not be included in this report, however it will be used for the purpose of timeline creation; see *Section C : Perform Technical Analysis, Task 1 : Correlate Events and Document Timeline, Memory Events.*

```
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f8044ee00000
DTB     0×1aa000
Symbols file:///home/analyst/Documents/tools/volatilit
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 WindowsCrashDump64Layer
base_layer      2 FileLayer
KdVersionBlock  0×f8044fa0f378
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      3
SystemTime      2022-07-20 18:40:48
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Aug 30 12:18:27 1973
```

Figure 11 : ./vol.py -f [image.dd] windows.info.Info

The final objective is to verify the functionality of the packet capture file:

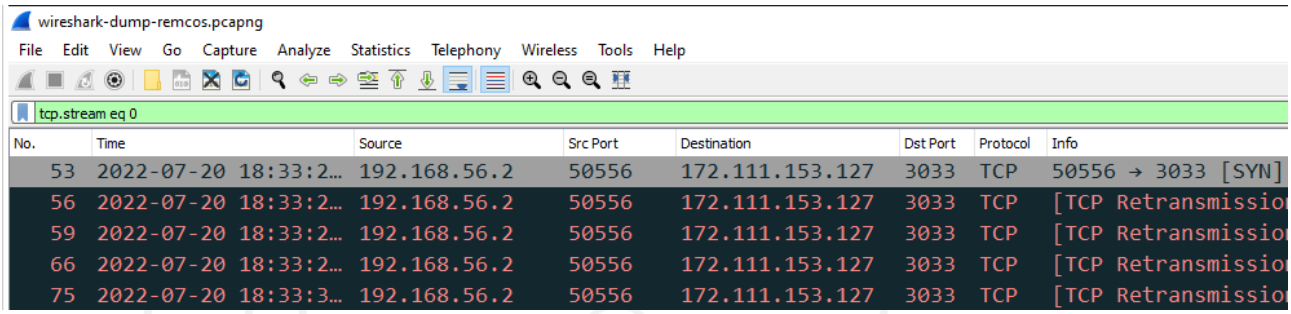


Figure 12 : Wireshark displaying Follow TCP Stream

All evidence files are proven functional; now to proceed to the technical analysis.

Section C : Perform Technical Analysis

Authority:

"Develop a technical and contextual understanding of the incident... The goal of this analysis is to examine the breadth of data sources throughout the environment to discover at least some part of an attack chain, if not all of it."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 10.

Section C : Perform Technical Analysis is composed of three tasks:

- Task 1 : Correlate Events and Document Timeline
- Task 2 : Gather Incident Indicators
- Task 3 : Adjust Tools

Task 1 : Correlate Events and Document Timeline

Authority:

"Acquire, store, and analyze logs to correlate adversarial activity. Create a timeline of all relevant findings. The timeline will allow the team to account for all adversary activity on the network and will assist in creating the findings report at the conclusion of the response."

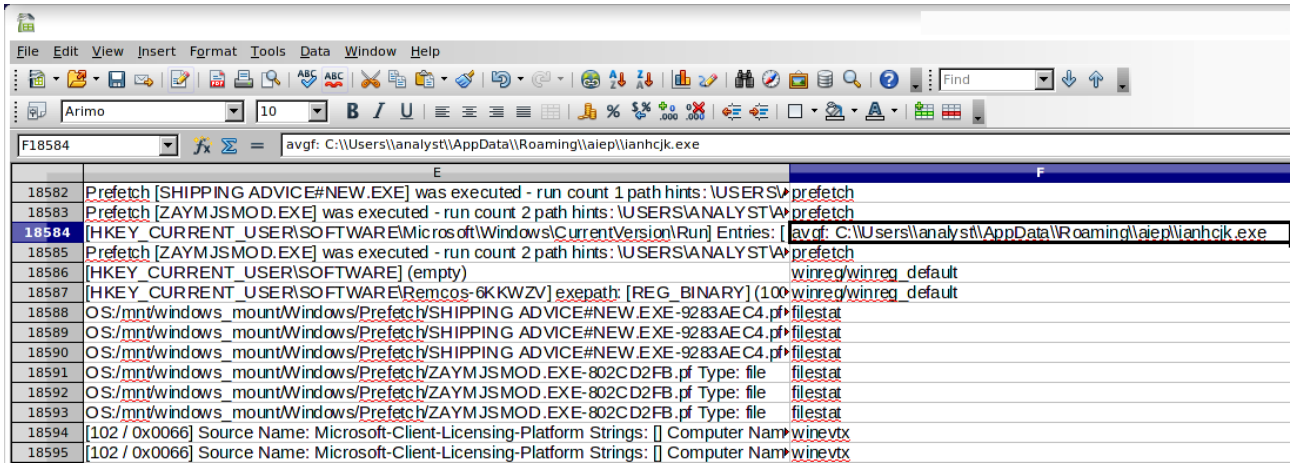
Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 11.

Task 1 : Correlate Events and Document Timeline develops a basic timeline to obtain a high-level understanding of the Remcos infection on the host. This involves the merger of network, file system, and memory logs into a single timeline. Such a timeline is useful for identifying basic IOCs and designing a rapid containment and remediation strategy in the early stages of an incident.

Filesystem Events

Remcos requires read/write/execute permissions to the disk; therefore indicators of compromise will be present on the system via $MFT and other system log files; such logs can be parsed using Log2timeline/Plaso.

Figure 13 below shows a raw log2timeline csv file; prefetch files provide evidence of execution for the installer *SHIPPING ADVICE#NEW.EXE* and the trojan *zaymjsmod.exe*. In addition, two entries show modification to registry keys in the HKEY Current User hive. Notice in Figure 13 line 18,584, this Remcos trojan has used the standard CurrentVersion\Run key persistence tactic:

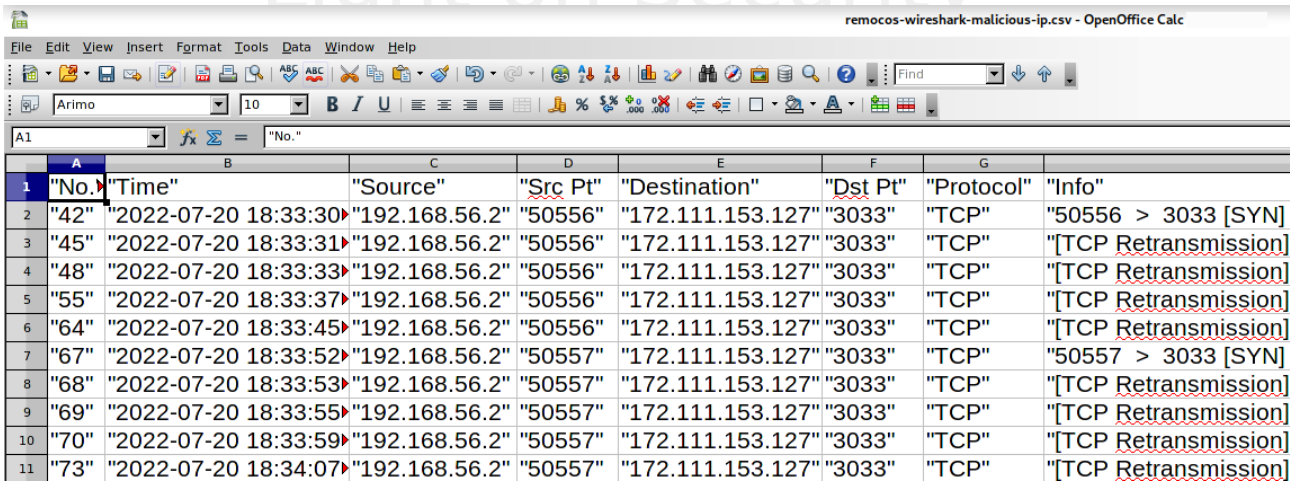


	E	F
18582	Prefetch [SHIPPING ADVICE#NEW.EXE] was executed - run count 1 path hints: \USERS\	prefetch
18583	Prefetch [ZAYMJSMOD.EXE] was executed - run count 2 path hints: \USERS\ANALYST\A	prefetch
18584	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] Entries: [	avgf: C:\\Users\\analyst\\AppData\\Roaming\\aiep\\ianhcjk.exe
18585	Prefetch [ZAYMJSMOD.EXE] was executed - run count 2 path hints: \USERS\ANALYST\A	prefetch
18586	[HKEY_CURRENT_USER\SOFTWARE] (empty)	winreg/winreg_default
18587	[HKEY_CURRENT_USER\SOFTWARE\Remcos-6KKWZV] exepath: [REG_BINARY] (100	winreg/winreg_default
18588	OS:/mnt/windows_mount/Windows/Prefetch/SHIPPING ADVICE#NEW.EXE-9283AEC4.pf	filestat
18589	OS:/mnt/windows_mount/Windows/Prefetch/SHIPPING ADVICE#NEW.EXE-9283AEC4.pf	filestat
18590	OS:/mnt/windows_mount/Windows/Prefetch/SHIPPING ADVICE#NEW.EXE-9283AEC4.pf	filestat
18591	OS:/mnt/windows_mount/Windows/Prefetch/ZAYMJSMOD.EXE-802CD2FB.pf Type: file	filestat
18592	OS:/mnt/windows_mount/Windows/Prefetch/ZAYMJSMOD.EXE-802CD2FB.pf Type: file	filestat
18593	OS:/mnt/windows_mount/Windows/Prefetch/ZAYMJSMOD.EXE-802CD2FB.pf Type: file	filestat
18594	[102 / 0x0066] Source Name: Microsoft-Client-Licensing-Platform Strings: [] Computer Nam	winevtx
18595	[102 / 0x0066] Source Name: Microsoft-Client-Licensing-Platform Strings: [] Computer Nam	winevtx

Figure 13 : Raw log2timeline csv

Network Events

The Remcos agent needs to establish a network connection back to the controller for the purpose of agent management; this behavior is observed below in Figure 14:



remocos-wireshark-malicious-ip.csv - OpenOffice Calc

	A	B	C	D	E	F	G	
1	"No."	"Time"	"Source"	"Src Pt"	"Destination"	"Dst Pt"	"Protocol"	"Info"
2	"42"	"2022-07-20 18:33:30	"192.168.56.2"	"50556"	"172.111.153.127"	"3033"	"TCP"	"50556 > 3033 [SYN]
3	"45"	"2022-07-20 18:33:31	"192.168.56.2"	"50556"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
4	"48"	"2022-07-20 18:33:33	"192.168.56.2"	"50556"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
5	"55"	"2022-07-20 18:33:37	"192.168.56.2"	"50556"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
6	"64"	"2022-07-20 18:33:45	"192.168.56.2"	"50556"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
7	"67"	"2022-07-20 18:33:52	"192.168.56.2"	"50557"	"172.111.153.127"	"3033"	"TCP"	"50557 > 3033 [SYN]
8	"68"	"2022-07-20 18:33:53	"192.168.56.2"	"50557"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
9	"69"	"2022-07-20 18:33:55	"192.168.56.2"	"50557"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
10	"70"	"2022-07-20 18:33:59	"192.168.56.2"	"50557"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]
11	"73"	"2022-07-20 18:34:07	"192.168.56.2"	"50557"	"172.111.153.127"	"3033"	"TCP"	"[TCP Retransmission]

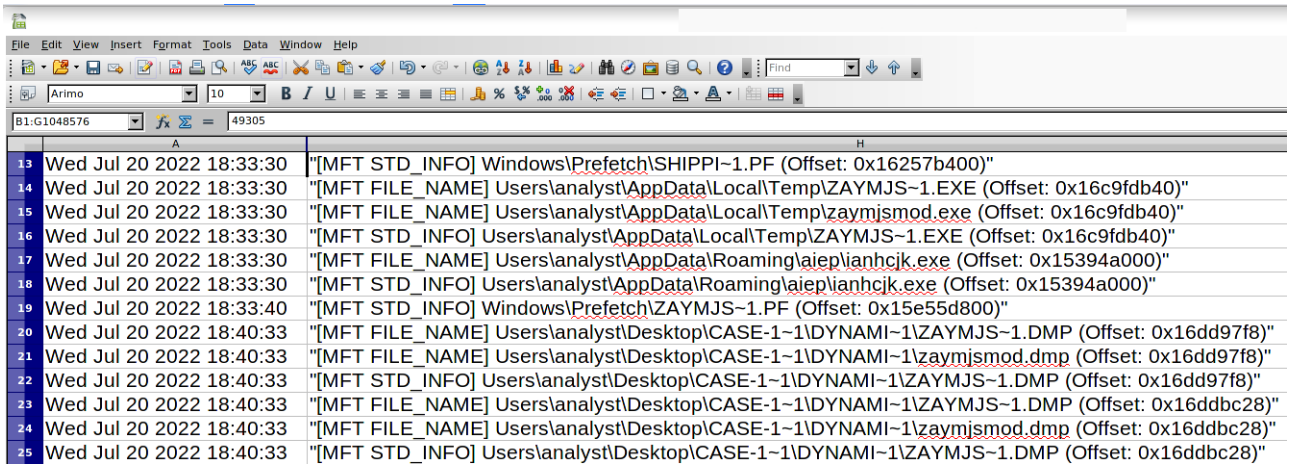
Figure 14 : Wireshark timeline events in csv export

In the figure above, it becomes evident the Remcos agent was configured to establish a session to destination port 3033; with each failed outbound TCP SYN request, the high port on the client increments until eventually the agent will give up trying to access the controller. This data was obtained using the Wireshark display filter `tcp.dstport==3033`, followed by exporting the relevant packets to csv format.

Memory Events

The raw data for the memory timeline in Figure 15 was obtained from the tool Autotimeliner; it uses the mftparser plugin from Volatility to extract $MFT events from memory, and Sleuthkit mactime to chronologically order events. The log entries are preceded by two MFT attributes: STD_INFO and FILE_NAME; STD_INFO is used for basic metadata for the file (Timestamps, Security ID, Owner ID, etc). FILE_NAME is used for file name, directory indexing,

timestamps, logical/disk size, etc. Next, the file path and name is listed; afterward the physical memory offset is provided. An interesting artifact is listed in row 14; it displays the path to the Remcos trojan and the corresponding physical memory address of 0x16c9fdb40.



	A	H
13	Wed Jul 20 2022 18:33:30	"[MFT STD_INFO] Windows\Prefetch\SHIPPI~1.PF (Offset: 0x16257b400)"
14	Wed Jul 20 2022 18:33:30	"[MFT FILE_NAME] Users\analyst\AppData\Local\Temp\ZAYMJS~1.EXE (Offset: 0x16c9fdb40)"
15	Wed Jul 20 2022 18:33:30	"[MFT FILE_NAME] Users\analyst\AppData\Local\Temp\zaymjsmod.exe (Offset: 0x16c9fdb40)"
16	Wed Jul 20 2022 18:33:30	"[MFT STD_INFO] Users\analyst\AppData\Local\Temp\ZAYMJS~1.EXE (Offset: 0x16c9fdb40)"
17	Wed Jul 20 2022 18:33:30	"[MFT FILE_NAME] Users\analyst\AppData\Roaming\aiep\ianhcjk.exe (Offset: 0x15394a000)"
18	Wed Jul 20 2022 18:33:30	"[MFT STD_INFO] Users\analyst\AppData\Roaming\aiep\ianhcjk.exe (Offset: 0x15394a000)"
19	Wed Jul 20 2022 18:33:40	"[MFT STD_INFO] Windows\Prefetch\ZAYMJS~1.PF (Offset: 0x15e55d800)"
20	Wed Jul 20 2022 18:40:33	"[MFT FILE_NAME] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\ZAYMJS~1.DMP (Offset: 0x16dd97f8)"
21	Wed Jul 20 2022 18:40:33	"[MFT FILE_NAME] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\zaymjsmod.dmp (Offset: 0x16dd97f8)"
22	Wed Jul 20 2022 18:40:33	"[MFT STD_INFO] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\ZAYMJS~1.DMP (Offset: 0x16dd97f8)"
23	Wed Jul 20 2022 18:40:33	"[MFT FILE_NAME] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\ZAYMJS~1.DMP (Offset: 0x16ddbc28)"
24	Wed Jul 20 2022 18:40:33	"[MFT FILE_NAME] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\zaymjsmod.dmp (Offset: 0x16ddbc28)"
25	Wed Jul 20 2022 18:40:33	"[MFT STD_INFO] Users\analyst\Desktop\CASE-1~1\DYNAMI~1\ZAYMJS~1.DMP (Offset: 0x16ddbc28)"

Figure 15 : Raw Autotimeliner events
Command: ./autotimeline.py -f remcos-mem.dmp -t 2022-07-20..2022-07-21

Event Timeline Correlation

This section correlates the raw file system, network, and memory csv logs into a single refined timeline; the end result is seen in Figure 16:

	UTC Time	Source	MITRE ATT&CK	File	Comment	Event Detail
2	2022-05-25 16:24:32	Disk	Defense evasion: Timestomp	5tq9d2mjcoubez	Possible shellcode	NTFS:\$MFT File reference: 49306-3 Attribute name: $STANDARD_INFORMATION Path hints: \Users\analyst\AppData\Local\Temp\5tq9d2mjcoubez
3	2022-05-25 16:24:32	Disk	Defense evasion: Timestomp	qmkhkh	Possible shellcode	NTFS:\$MFT File reference: 49349-3 Attribute name: $STANDARD_INFORMATION Path hints: \Users\analyst\AppData\Local\Temp\qmkhkh
4	2022-05-25 16:24:40	Disk	Defense evasion: Timestomp	zaymjsmod.exe	Remcos	NTFS:\$MFT File reference: 49350-3 Attribute name: $STANDARD_INFORMATION Path hints: \Users\analyst\AppData\Local\Temp\zaymjsmod.exe
5	2022-07-20 18:32:03	Memory	Execution: User Execution, Malicious File	SHIPPING ADVICE#NEW.exe	Installs Remcos	"[MFT FILE_NAME] Users\analyst\Desktop\CASE-1~1\NEWFOL~1\SHIPPING ADVICE#NEW.exe (Offset: 0x3248dc00)"
6	2022-07-20 18:33:00	Disk	Defense Evasion: Modify Registry	zaymjsmod.exe	Exe path and license	[HKEY_CURRENT_USER\SOFTWARE\Remcos-6KKWZV] exepath: [REG_BINARY] (100 bytes) licence: [REG_SZ]
7	2022-07-20 18:33:30	Memory	Defense Evasion: Deobfuscate/Decode Files or Information	zaymjsmod.exe	Remcos	"[MFT FILE_NAME] Users\analyst\AppData\Local\Temp\ZAYMJS~1.EXE (Offset: 0x16c9fdb40)"
8	2022-07-20 18:33:30	Memory	Defense Evasion: Hide Artifacts	ianhcjk.exe	Copy of Remcos	"[MFT FILE_NAME] Users\analyst\AppData\Roaming\aiep\ianhcjk.exe (Offset: 0x15394a000)"
9	2022-07-20 18:33:30	Disk	Persistence: Boot or Logon Autostart Execution, Registry Run Keys / Startup Folder	ianhcjk.exe	Run key persistence	[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run] Entries: [avgf: C: \\Users\\analyst\\AppData\\Roaming\\aiep\\ianhcjk.exe
10	2022-07-20 18:33:30	Network	Command and Control: Non-Standard Port	zaymjsmod.exe	TCP Outbound Traffic	192.168.56.2:50556 → 172.111.153.127:3033
11	2022-07-20 18:33:31	Network			Beacon	192.168.56.2:50556 → 172.111.153.127:3033
12	2022-07-20 18:33:33	Network			Beacon	192.168.56.2:50556 → 172.111.153.127:3033
13	2022-07-20 18:33:37	Network			Beacon	192.168.56.2:50556 → 172.111.153.127:3033
14	2022-07-20 18:33:45	Network			Beacon	192.168.56.2:50556 → 172.111.153.127:3033
15	2022-07-20 18:33:52	Network			Beacon	192.168.56.2:50557 → 172.111.153.127:3033
16	2022-07-20 18:33:53	Network			Beacon	192.168.56.2:50557 → 172.111.153.127:3033
17	2022-07-20 18:33:55	Network			Beacon	192.168.56.2:50557 → 172.111.153.127:3033
18	2022-07-20 18:33:59	Network			Beacon	192.168.56.2:50557 → 172.111.153.127:3033
19	2022-07-20 18:34:07	Network			Beacon	192.168.56.2:50557 → 172.111.153.127:3033

Figure 16 : Final timeline produced from raw network, disk, and memory events

Here is a summary of the most important findings from this timeline:

- User execution initiates the incident (row 5)
  - Trojan installer is called *SHIPPING ADVICE#NEW.exe*
- Installer drops Remcos and shellcode / configuration files (rows 2-4)
  - Timestomp tactic used to evade detection (rows 2-4)
  - Installer used to evade trojan detection (row 7)
- Registry is used for persistence and configuration (rows 6, 9)

- Remcos tries to hide a copy of itself for persistence (rows 8-9)
- Outbound beaconing to 172.111.153.127:3033 (Rows 10+)

This concludes *Task 1 : Correlate Events and Document Timeline.* Raw logs obtained from memory, disk, and network evidence files were extracted and refined to expose how this Remcos trojan infects an endpoint. The timeline in Figure 16 is sufficient for identifying basic IOCs to design a rapid containment and remediation strategy in the early stages of an incident. Task 2 will build upon the basic IOCs with further analysis using static, dynamic, and reverse engineering methods.

Light on Security
lightonsec@gmail.com

Task 2 : Gather Incident Indicators

Authority:

"Identify and document indicators that can be used for correlative analysis on the network. Indicators can provide insight into the adversary's capabilities and infrastructure. Indicators as standalone artifacts are valuable in the early stages of incident response."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 11.

Task 2 : Gather Incident Indicators will closely examine Remcos capabilities using static and dynamic methods; the light use of debugging and disassembly software will reveal additional IOCs to use for detection and containment purposes.

Light on Security
lightonsec@gmail.com

Static Analysis

Static Analysis involves examination of the malware without executing it; it begins with *SHIPPING ADVICE#NEW.exe*, the initial trojan distributed from the threat actor to unsuspecting users. The first objective is to positively identify the file type as a portable executable:

```
└─$ xxd 'SHIPPING ADVICE#NEW.exe'| head
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 d800 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: e571 4aa8 a110 24fb a110 24fb a110 24fb  .qJ...$...$...$.
00000090: 2f18 7bfb a310 24fb a110 25fb 3b10 24fb  /.{...$...%.;.$.
```

Figure 17 : Standard MZ header for PE files

lightonsec@gmail.com

Next, the file fingerprint is calculated using three hash algorithms (md5, sha1, sha256):

```
└─$ rahash2 -a md5,sha1,sha256 'SHIPPING ADVICE#NEW.exe'
0x00000000-0x00088315 md5: ee78ff11f8acf5c63c5df8ee1a314462
0x00000000-0x00088315 sha1: bda3f8d1087deacdc2827035a9075b17decf358a
0x00000000-0x00088315 sha256:
900274d5916f078ac30bedfc6b3bf5812c09de4cc1bdddd4e25d5efa1e3bb1c3
```

The md5 hash is then submitted to Virus Total to determine the file's reputation among anti-virus vendors:

Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.39691575	Alibaba	Trojan:Win32/Injector.696138b8
ALYac	Trojan.GenericKD.39691575	Avast	Win32:InjectorX-gen [Trj]
AVG	Win32:InjectorX-gen [Trj]	Avira (no cloud)	TR/Injector.xjwyn
BitDefender	Trojan.GenericKD.39691575	BitDefenderTheta	Gen:NN.ZexaCO.34682.luW@aOZRc5hi
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Injector.AYB.gen!Eldorado
DrWeb	Trojan.Siggen17.57060	Elastic	Malicious (moderate Confidence)
Emsisoft	Trojan.GenericKD.39691575 (B)	eScan	Trojan.GenericKD.39691575
ESET-NOD32	A Variant Of Win32/Injector.ERRU	Fortinet	W32/Injector.ERRU!tr
GData	Win32.Trojan.PSE.1MA53XA	Gridinsoft (no cloud)	Ransom.Win32.Wacatac.sa
Ikarus	Trojan-Spy.Agent	K7AntiVirus	Trojan (005936c01)
K7GW	Trojan (005936c01)	Kaspersky	HEUR:Backdoor.Win32.Remcos.gen
Kingsoft	Win32.Hack.Undef.(kcloud)	Lionic	Trojan.Win32.Remcos.m!c
Malwarebytes	Malware.AI.4078506333	MAX	Malware (ai Score=99)
McAfee	Artemis!EE78FF11F8AC	McAfee-GW-Edition	BehavesLike.Win32.Dropper.hc
Microsoft	Trojan:Win32/Remcos.KA!MTB	Palo Alto Networks	Generic.ml
Rising	Trojan.Injector!8.C4 (CLOUD)	Sangfor Engine Zero	Backdoor.Win32.Remcos.gen
Sophos	Mal/Generic-S	SUPERAntiSpyware	Backdoor.Andromeda/Variant
Symantec	ML.Attribute.HighConfidence	Tencent	Win32.Backdoor.Remcos.Anfs
Trellix (FireEye)	Trojan.GenericKD.39691575	TrendMicro-HouseCall	TROJ_GEN.F0D1C00EP22
ViRobot	Trojan.Win32.Z.Agent.557846	Acronis (Static ML)	Undetected

lightonsec@gmail.com

Figure 18 : Virus Total Results for md5 ee78ff11f8acf5c63c5df8ee1a314462

Of sixty-nine vendors, forty-one positively identify this binary as malicious; this is a 59% true positive detection rate. Noteworthy vendor descriptors include *trojan*, *generic*, *injector*, *Remcos*, *backdoor*, and *win32*. Below is Fortinet's definition regarding the label *W32/Injector.ERRU!tr:*

Threat Encyclopedia

W32/Injector.ERRU!tr

Analysis

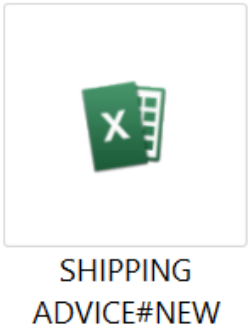
W32/Injector.ERRU!tr is classified as a trojan.

A trojan is a type of malware that performs activites without the user's knowledge. These activities commonly include establishing remote access connections, capturing keyboard input, collecting system information, downloading/uploading files, dropping other malware into the infected system, performing denial-of-service (DoS) attacks, and running/terminating processes.

Figure 19 : Fortinet Threat Profile of *W32/Injector.ERRU!tr*

Fortinet has correctly classified this malware as a trojan; below is an image of the thumbnail the

targeted user would encounter:



Light on Security
lightonsec@gmail.com

Figure 20 : Remcos RAT installer disguised as friendly shipping advice in Excel spreadsheet

A trojan is malicious software masquerading as legitimate software; it is designed to deceive the user into executing the covert malware. The threat actor understands Excel is an application trusted by millions of unsuspecting end users, and the title *Shipping Advice#New* assists in the social engineering effort.

Moving on to strings analysis: the threat actor used the Nullsoft Scriptable Install System to unpack and install the trojan into the user's temporary directory:

```
The installer you are trying to use is corrupted or incomplete.
This could be the result of a damaged disk, a failed download or a virus.
You may want to contact the author of this installer to obtain a new copy.
It may be possible to skip this check using the /NCRC command line switch
(NOT RECOMMENDED).
Error writing temporary file. Make sure your temp folder is valid.
verifying installer: %d%%
Error launching installer
unpacking data: %d%%
SeShutdownPrivilege
GetUserDefaultUILanguage
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
RegDeleteKeyExA
GetDiskFreeSpaceExA
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><assembly xmlns="urn:schemas-microsoft
86" name="Nullsoft.NSIS.exehead" type="win32"/><description>Nullsoft Install System v2.28</de
equestedExecutionLevel level="asInvoker" uiAccess="false"/></requestedPrivileges></security><
```

Figure 21 : View of NSIS installer configuration data using strings analysis

PEStudio reveals this 545 KB portable executable has a high entropy value of eight and verifies a Nullsoft Plugin Mini Packager signature; this further confirms the 32-bit executable is packed for the purpose of defense evasion.

Light on Security
lightonsec@gmail.com

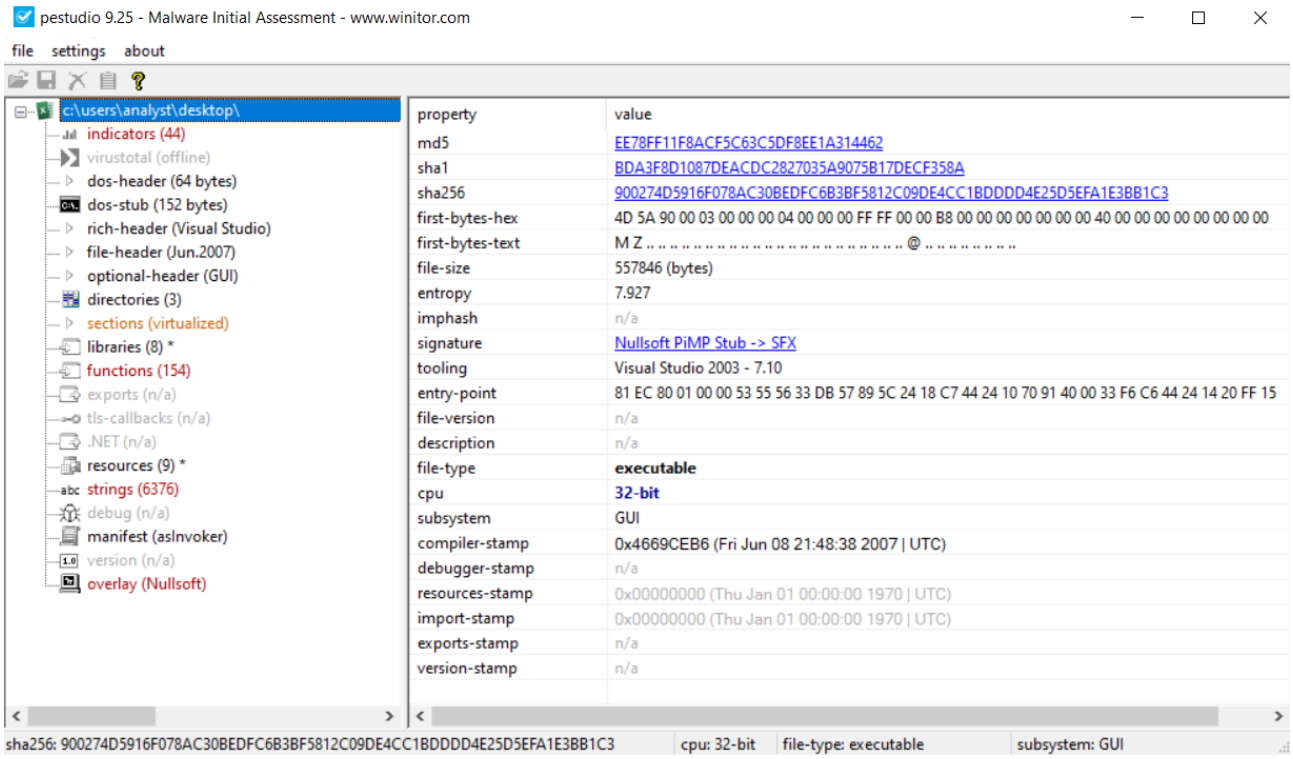


Figure 22 : Pestudio file metadata

PeStudio has listed several suspicious indicators, including an Overlay section with an entropy of eight and a file ratio of 88.62%. Remcos is likely embedded here and will become available for analysis once unpacked.

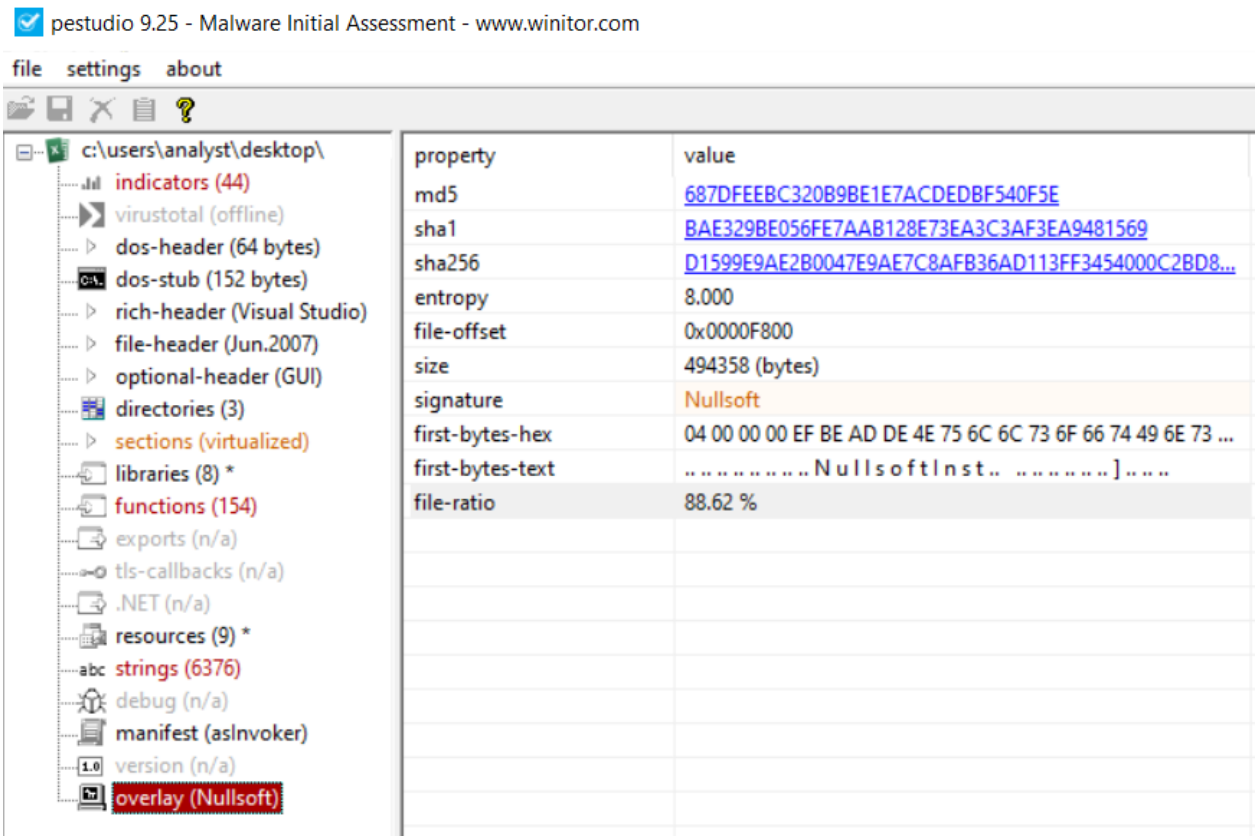


Figure 23 : Overlay section with embedded, high entropy data

Here are the file header sections for the installer; the .ndata section will be initialized during execution as it is writable, virtualized, and has a raw size of 0 bytes and a virtual size of 32 KB.

property	value	value	value	value	value
name	.text	.rdata	.data	.ndata	.rsrc
md5	7CB79F1EDBB8203E6F08196...	69C5211E1A88679CC11FD27...	80B7704433C7161CD9D68...	n/a	BC98D6CB6EC13FA05C1FD6...
entropy	6.458	5.175	4.981	n/a	5.199
file-ratio (11.20%)	4.13 %	0.83 %	0.18 %	n/a	6.06 %
raw-address	0x00000400	0x00005E00	0x00007000	0x00000000	0x00007400
raw-size (62464 bytes)	0x00005A00 (23040 bytes)	0x00001200 (4608 bytes)	0x00000400 (1024 bytes)	0x00000000 (0 bytes)	0x00008400 (33792 bytes)
virtual-address	0x00401000	0x00407000	0x00409000	0x00424000	0x0042C000
virtual-size (204462 bytes)	0x000059AC (22956 bytes)	0x0000117A (4474 bytes)	0x0001AFD8 (110552 bytes)	0x00008000 (32768 bytes)	0x000083B0 (33712 bytes)
entry-point	**0x000032FA**	-	-	-	-
characteristics	0x60000020	0x40000040	0xC0000040	0xC0000080	0x40000040
writable	-	-	x	x	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	-
initialized-data	-	x	x	-	x
uninitialized-data	-	-	-	x	-
unreadable	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	x	-
file	n/a	n/a	n/a	n/a	n/a

Figure 24 : PE section headers in pestudio

It is confirmed through multiple artifacts *SHIPPING ADVICE#NEW.exe* is packed, therefore the static analysis section of this file is complete; statically analyzing the installer any further is of little value when Remcos is available to unpack for IOC extraction.

Light on Security
lightonsec@gmail.com

Dynamic Analysis

Observing Process And File System Activity

When executing *SHIPPING ADVICE#NEW.exe*, the NSIS installer unpacks Remcos; this behavior was observed in Sysinternals Process Monitor via the following process tree:

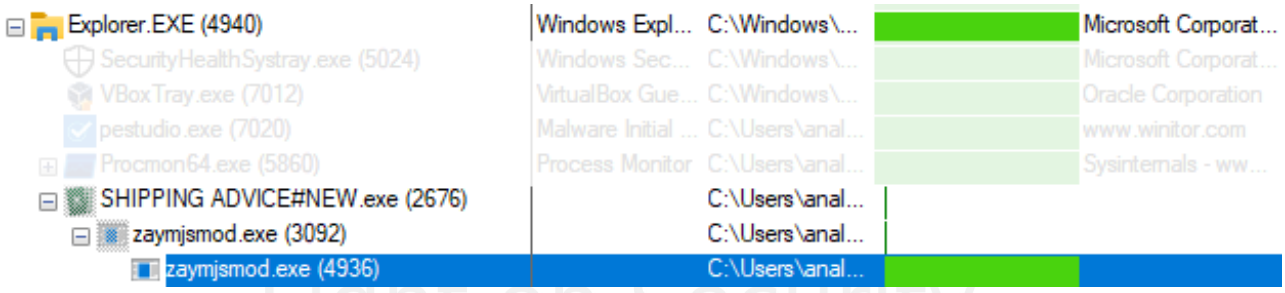
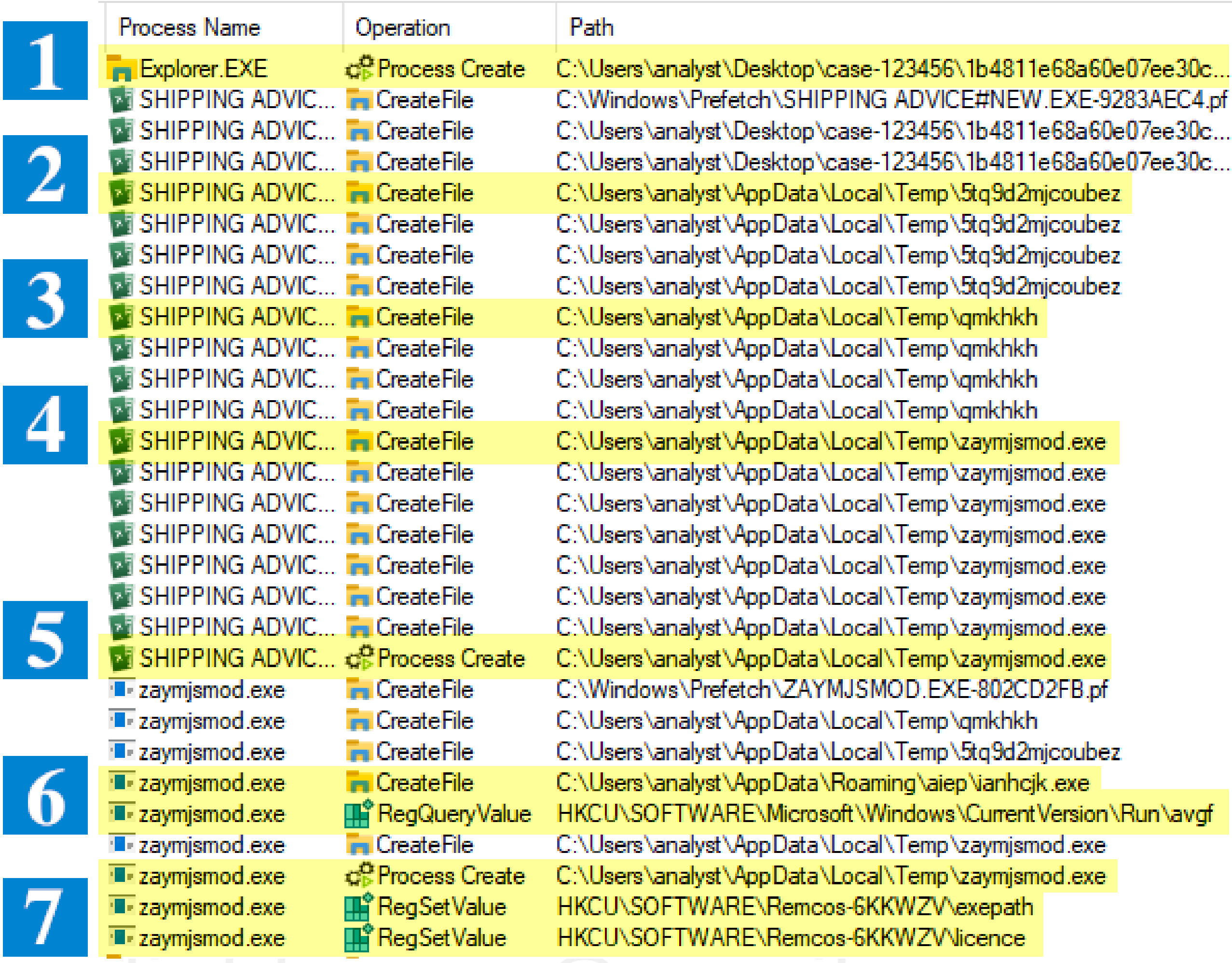


Figure 25 : Remcos Process Tree In ProcMon

Light on Security
lightonsec@gmail.com

In addition to displaying process trees, Process Monitor can also enumerate file system changes. In Figure 26 below, both the installer and Remcos perform several changes to the operating system; seven phases are displayed with explanations below:



lightonsec@gmail.com

Figure 26 : Filtered Malware Events in ProcessMonitor

The general execution summary is as follows:

1. The trojan installer is executed
2. The installer writes possible shellcode/config 1 to disk
3. The installer writes possible shellcode/config 2 to disk
4. The installer writes Remcos to disk
5. The installer runs Remcos with shellcode/config 2 as a cmdline argument
6. Remcos copies itself into the Roaming directory; a Run key value points to the Remcos copy in Roaming directory
7. Remcos spawns a child process of itself; the child process writes license and execution keys to the Software registry in the HKEY Current User hive.

Autoruns confirms the persistence mechanism as the typical Run key:
Light on Security

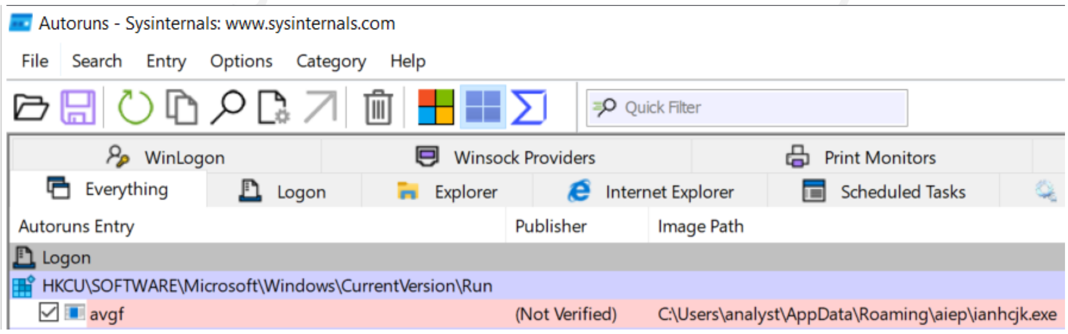
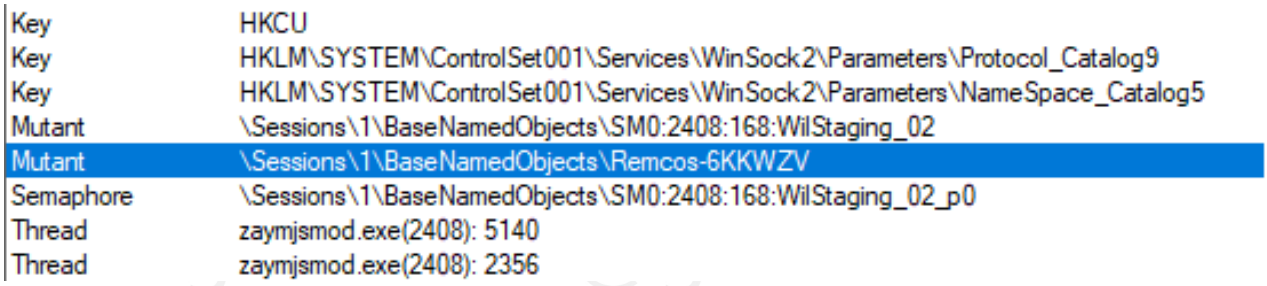


Figure 27 : Unverified publisher in CurrentVersion\Run is suspicious

Dynamic analysis also reveals two mutex through Process Explorer:



Key	HKCU
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
Mutant	\Sessions\1\BaseNamedObjects\SM0:2408:168:WilStaging_02
Mutant	\Sessions\1\BaseNamedObjects\Remcos-6KKWZV
Semaphore	\Sessions\1\BaseNamedObjects\SM0:2408:168:WilStaging_02_p0
Thread	zaymjsmod.exe(2408): 5140
Thread	zaymjsmod.exe(2408): 2356

Figure 28 : Viewing process handles for zaymjsmod.exe in Process Explorer

A mutex authorizes single thread access to a shared object; proper locking prevents multiple threads from accessing a shared object at the same time, which could lead to race conditions, data corruption, and other problems. Malware authors often use mutexes as a unique identifier to verify whether a system has been infected or not; incident responders and threat hunters use mutexes for the same purpose.

To see available mutexes in Process Explorer, select the running process of interest and press Ctrl + H; this will display all process handles for the application.

Interesting to note mutex *SM0:pid:handle:WilStaging_02* is associated with other malware such as Redline Stealer and RedNet.

Light on Security
lightonsec@gmail.com

Analyzing NTFS Timestomping with x32dbg

This section will briefly discuss the defense evasion tactic of timestomping. The intention of this commonly used tactic is to blend malicious files into the native operating system and delay incident responders and forensic analysts during investigation. Figure 29 below displays the timestamps of three malicious files put on the system by the installer *SHIPPING ADVICE#NEW.exe*; they all show a timestomp date of 5/25/2022 06:24 AM:

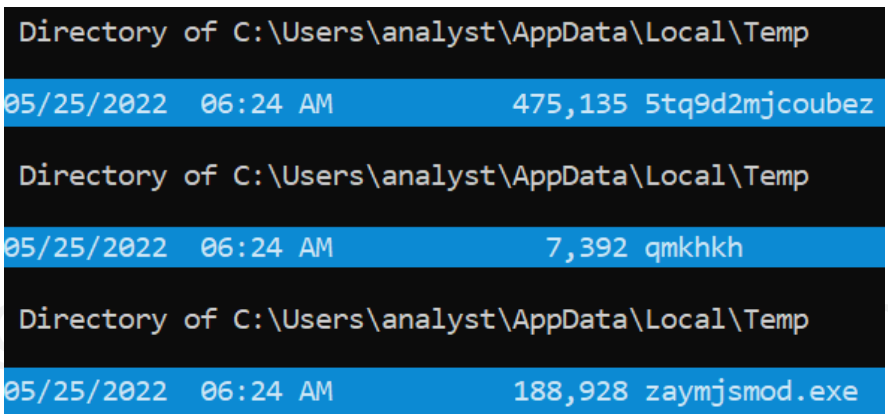


Figure 29 : cmd.exe displaying timestomped files

Two API functions were used by *SHIPPING ADVICE#NEW.exe* to apply this anti-forensic technique; the first is SetFileTime:

SetFileTime function (fileapi.h)

Article • 10/13/2021 • 2 minutes to read

Sets the date and time that the specified file or directory was created, last accessed, or last modified.

Syntax

C++ Copy

```
BOOL SetFileTime(
  [in]           HANDLE         hFile,
  [in, optional] const FILETIME *lpCreationTime,
  [in, optional] const FILETIME *lpLastAccessTime,
  [in, optional] const FILETIME *lpLastWriteTime
);
```

Figure 30 : SetFileTime function can modify three FILETIME attributes

Figure 31 below displays the SetFileTime function in x32dbg debugger:

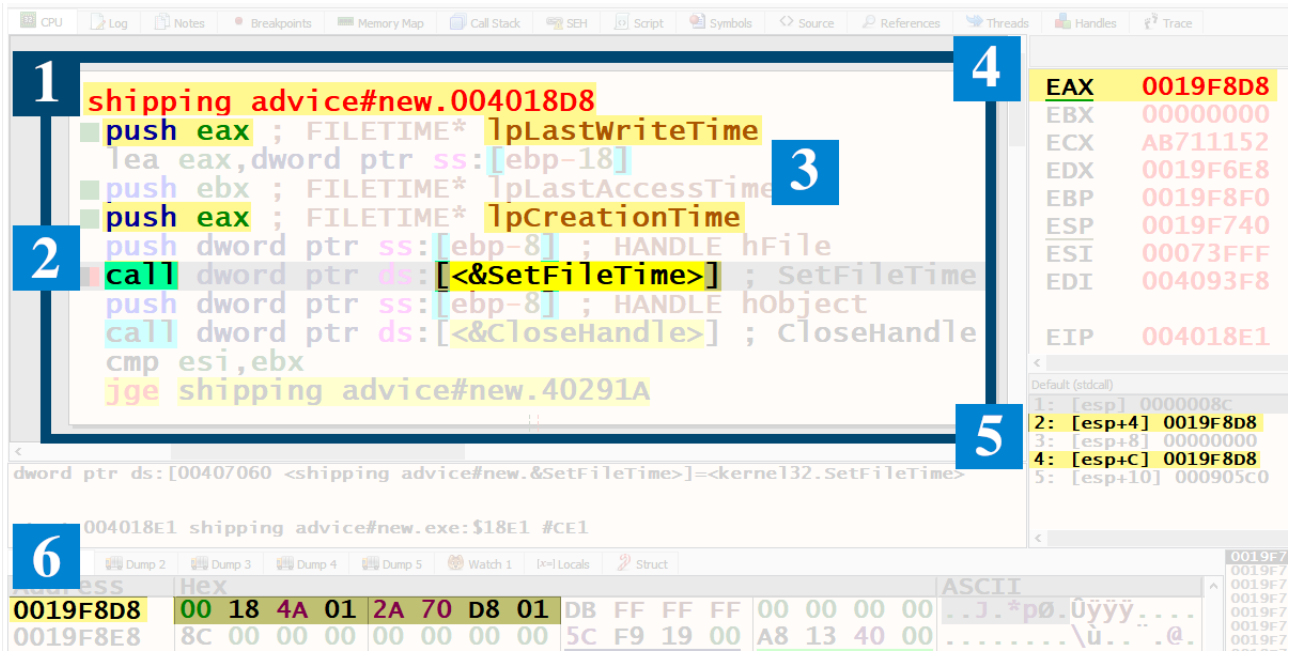


Figure 31 : x32dbg debugger reveals how SetFileTime is applied

Light on Security
lightonsec@gmail.com

Here is an explanation of the numerical values in the screenshot:

1. The first timestomp function *SetFileTime* is displayed in the graphical CPU window of x32dbg.
2. The debugger has paused on a software breakpoint; it is a call to the SetFileTime API.
3. Register EAX is pushed onto the stack for two parameters: lpCreationTime and lpLastWriteTime .
4. Register EAX contains memory address 0019F8D8.
5. Register EAX, containing address 0019F8D8, is seen on the stack.
6. Memory address 0019F8D8 contains the little Endian hexadecimal value 00 18 4A 01 2A 70 D8 01.

7. The hex value 00 18 4A 01 2A 70 D8 01 is entered into Dcode (Figure 32 below)
8. The timestomp value is correctly displayed as 2022-05-25 06:24:32:

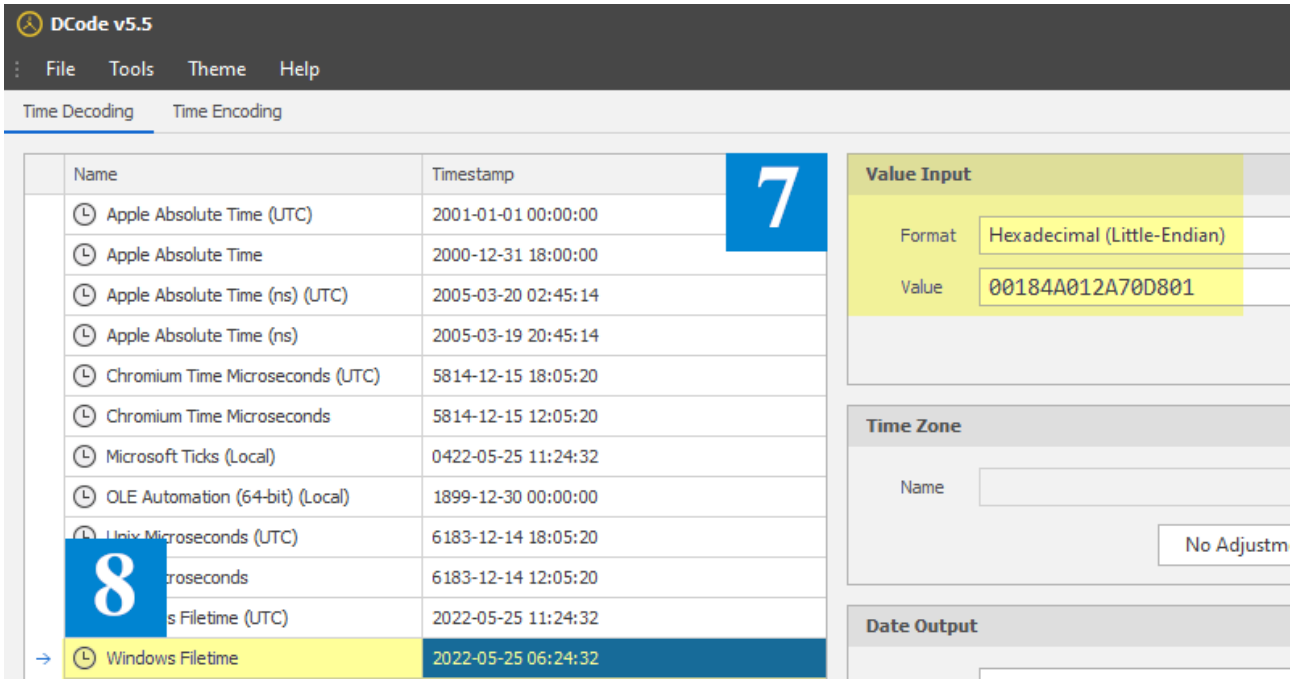


Figure 32 : Little Endian hexadecimal decoded to timestomp value

After initializing the timestomp value with SetFileTime, the Remcos installer proceeds to do this with NtSetInformationFile also.

NtSetInformationFile function (ntifs.h)

Article • 03/11/2022 • 5 minutes to read

The **NtSetInformationFile** routine changes various kinds of information about a file object.

Syntax

C++ Copy

```
__kernel_entry NTSYSCALLAPI NTSTATUS NtSetInformationFile(
  [in]  HANDLE                 FileHandle,
  [out] PIO_STATUS_BLOCK       IoStatusBlock,
  [in]  PVOID                  FileInformation,
  [in]  ULONG                  Length,
  [in]  FILE_INFORMATION_CLASS FileInformationClass
);
```

Figure 33 : NtSetInformationFile modifies FileInformation attribute for timestomping

Figure 34 : NtSetInformationFile function displays in graphical CPU window of x32dbg

1. The second timestomp function is displayed; it is a call to NtSetInformationFile.
2. The debugger has paused on a software breakpoint; it is an instruction to push eax ; PVOID FileInformation. This parameter is a “Pointer to a buffer that contains the information to set for the file.”
3. Register EAX contains a new address, 0019F70C.
4. Address 0019F70C contains the hexadecimal value of 00 18 4A 01 2A 70 D8 01, previously decoded to 2022-05-25 06:24:32

Light on Security
lightonsec@gmail.com

Various differences exist between SetFileTime and NtSetInformationFile with regard to timestamp modification, however they will not be discussed here.

Observing Network Traffic With Wireshark

As previously observed in *Task 1 : Correlate Events and Document Timeline, Network Events*, the Remcos agent *zaymjsmod.exe* produces network beacon activity over outbound tcp 172.111.153.127:3033:

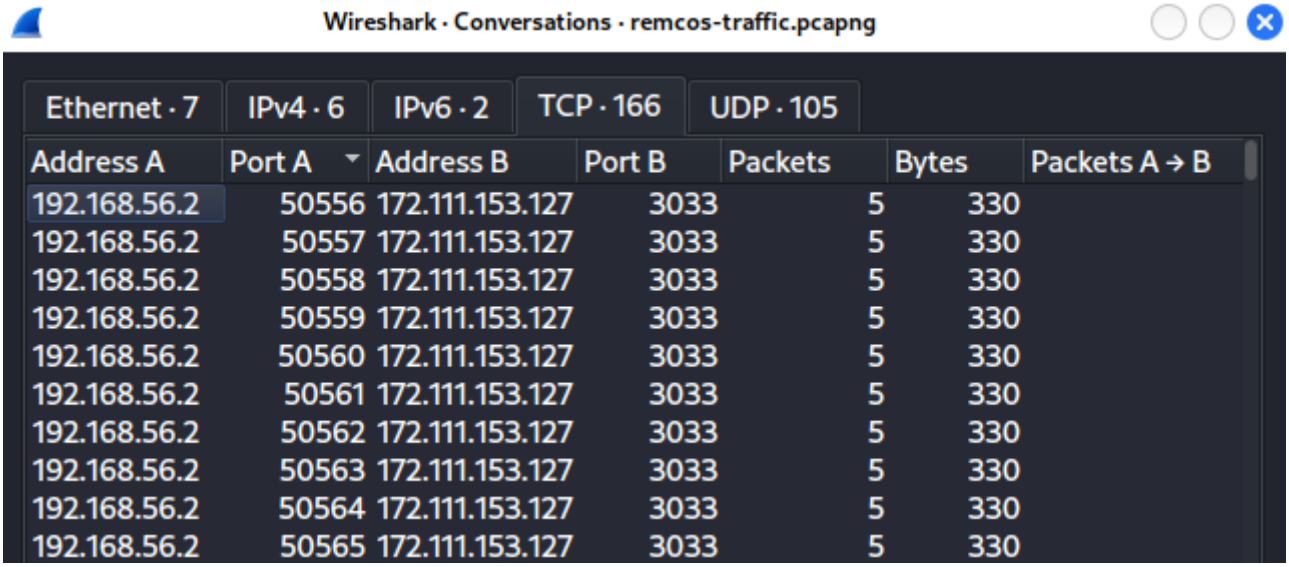


Figure 35 : Wireshark shows 166 tcp outbound connection attempts to 172.111.153.127:3033

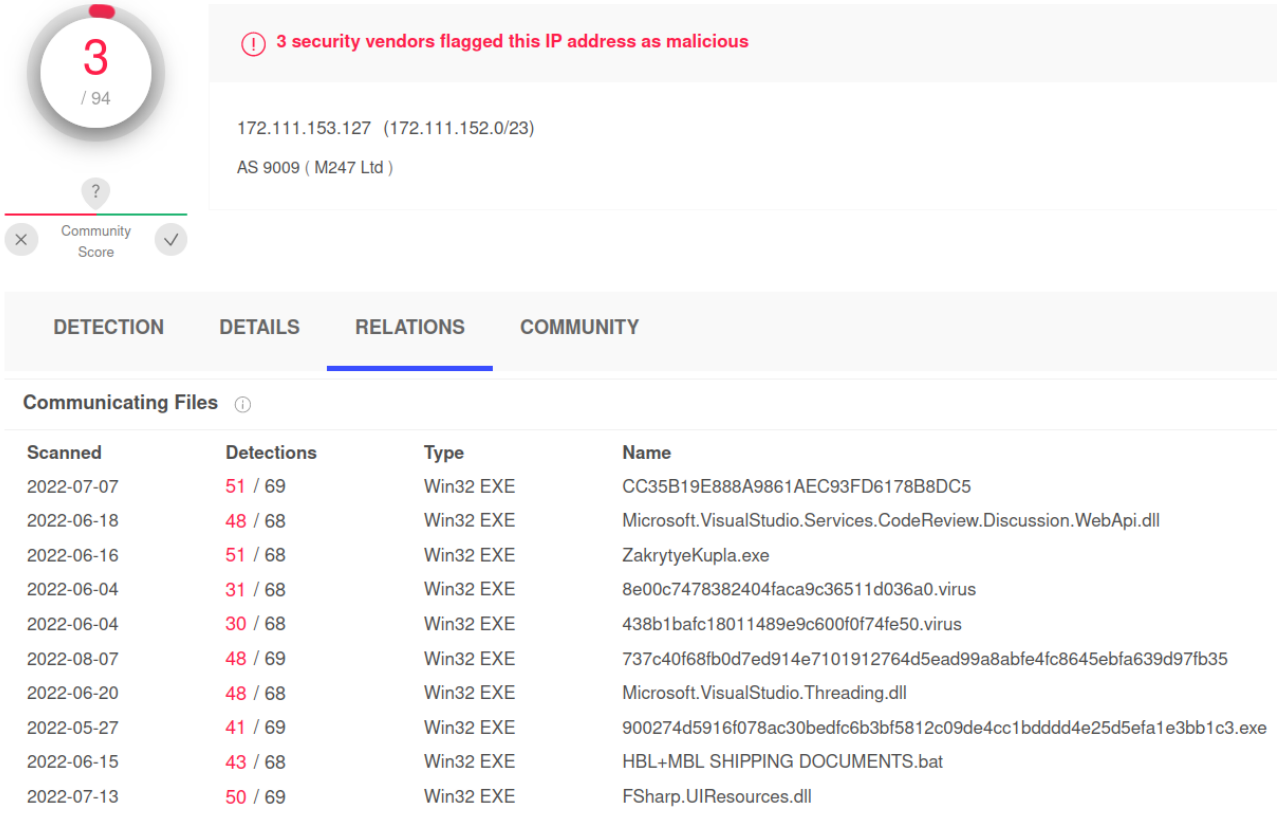
Here is the record from the Internet Assigned Numbers Authority for port 3033:

Service Name	Port Number	Transport	Description	Assignee	Contact
pdb	3033	tcp	PDB	[Don_Bowman]	[Don_Bowman]
pdb	3033	udp	PDB	[Don_Bowman]	[Don_Bowman]

Light on Security
lightonsec@gmail.com

PDB is presumably the Pluggable Database for Oracle Real Application Clusters (RAC). Be advised network settings for Remcos are configurable; port 3033 is not universally used. Rather usage of port 3033 is indicative of a particular campaign being carried out by threat actors.

Virus Total and Alien Vault OTX report destination IP address 172.111.153.127 as having a malicious reputation:



Scanned	Detections	Type	Name
2022-07-07	51 / 69	Win32 EXE	CC35B19E888A9861AEC93FD6178B8DC5
2022-06-18	48 / 68	Win32 EXE	Microsoft.VisualStudio.Services.CodeReview.Discussion.WebApi.dll
2022-06-16	51 / 68	Win32 EXE	ZakrytyeKupla.exe
2022-06-04	31 / 68	Win32 EXE	8e00c7478382404faca9c36511d036a0.virus
2022-06-04	30 / 68	Win32 EXE	438b1bafc18011489e9c600f0f74fe50.virus
2022-08-07	48 / 69	Win32 EXE	737c40f68fb0d7ed914e7101912764d5ead99a8abfe4fc8645ebfa639d97fb35
2022-06-20	48 / 68	Win32 EXE	Microsoft.VisualStudio.Threading.dll
2022-05-27	41 / 69	Win32 EXE	900274d5916f078ac30bedfc6b3bf5812c09de4cc1bdddd4e25d5efa1e3bb1c3.exe
2022-06-15	43 / 68	Win32 EXE	HBL+MBL SHIPPING DOCUMENTS.bat
2022-07-13	50 / 69	Win32 EXE	FSharp.UIResources.dll

Figure 36 : Virus Total Relations tab correlating malicious files with 172.111.153.127

Most of the files listed in Figure 36 are true positive detections for Remcos; the earliest Relation entry is listed for 5/27/2022 which is close to the timeframe this campaign began (Malware Bazaar, First Seen : 2022-05-26 10:41:43 UTC).

Light on Security
lightonsec@gmail.com

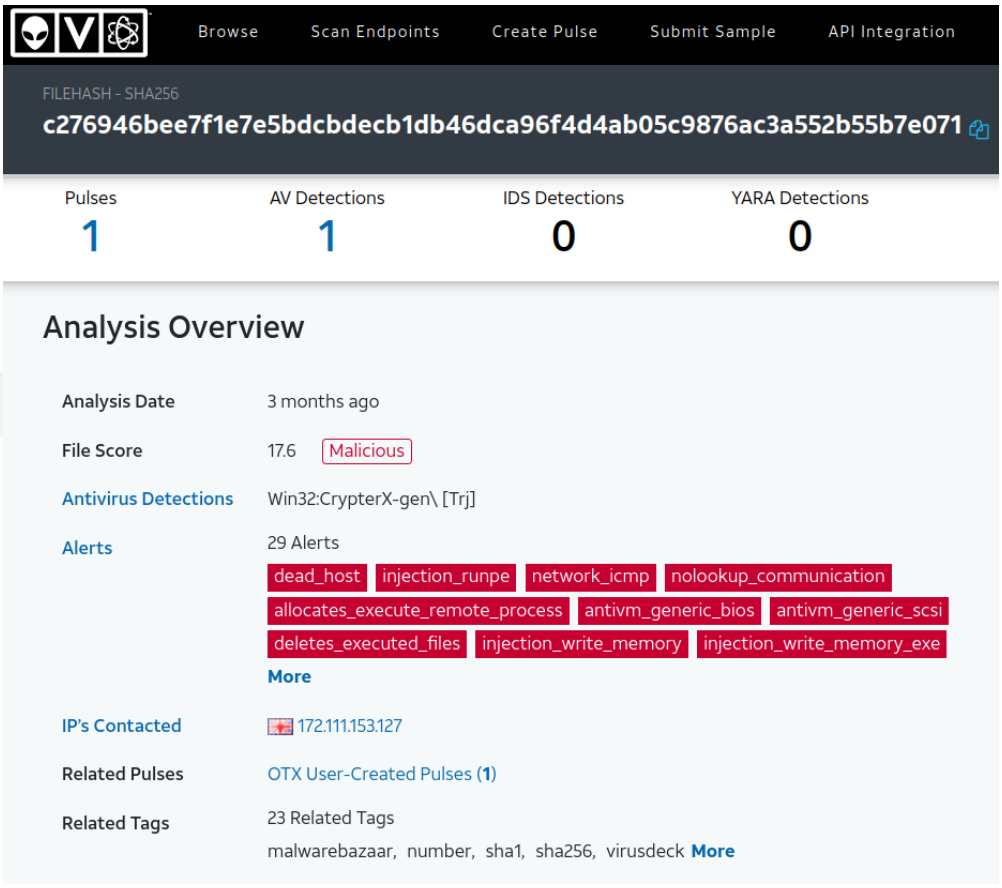


Figure 37 : AlienVault OTX, 172.111.153.127 seen used with other malware

AlienVault OTX lists two file hashes of the type Win32:CrypterX-gen\ [Trj] associated with 172.111.153.127; both files have a Remcos-[A-Z0-9]{6} mutex; the file hash displayed in Figure 37 shares the same Remcos mutex, *Remcos-6KKWZV,* as the file analyzed in this report. This information suggests a campaign relied on using 172.111.153.127 to communicate with a few Remcos variants.

Figure 38 below displays the Remcos agent's failure to complete the TCP three way handshake:

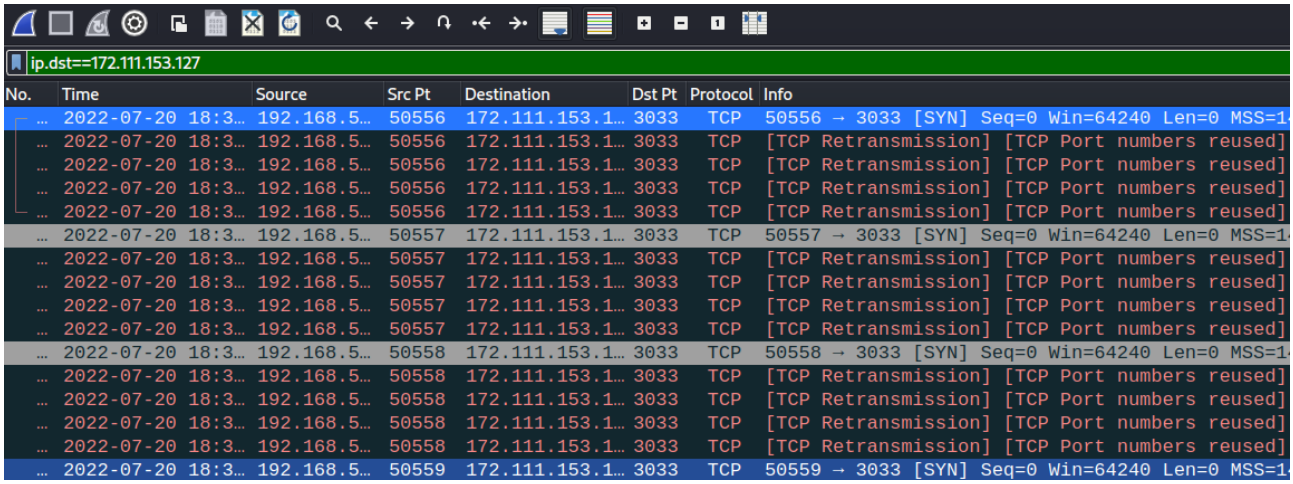


Figure 38 : Wireshark display filer ip.dst==172.11.153.127 displaying TCP retransmission

TCP retransmission is due to packet loss; this packet loss is due to traffic being contained in an isolated lab environment. As a result, the Remcos agent never produced any traffic beyond the transport layer. Had application layer payloads been available, they would have been encrypted at the presentation layer using TLS v1.3.

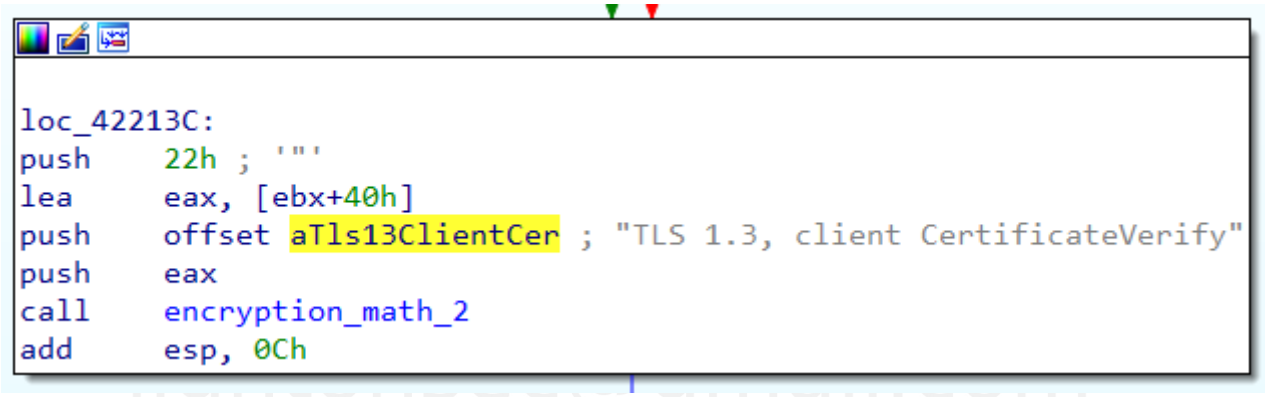


Figure 39 : TLS v1.3 offset in IDA Free

Now it is time to examine Remcos using basic reverse engineering.

Basic Reverse Engineering

During dynamic analysis, Remcos *zaymjsmod.exe* was dumped from live memory using PE-Sieve. This section will briefly examine a few features of the dumped binary in IDA Free disassembler. This section does not discuss the complete logic and functionality of this Remcos agent; instead it highlights three notable features for the purpose of contextualizing indicators of compromise. This analysis covers the following trojan features:

- Analysis 1 – Privilege Elevation: Access Token Manipulation
- Analysis 2 – Defense Evasion: Abuse Elevation Control Mechanism
- Analysis 3 – Collection: Input Capture

Analysis 1 – TA0004 : Privilege Elevation

T1134, Access Token Manipulation

AdjustTokenPrivileges

Remcos has authorization to shutdown the operating system via SeShutdownPrivilege. Examination of Remcos Security Properties in Process Explorer displays SeShutdownPrivilege as available, yet disabled:

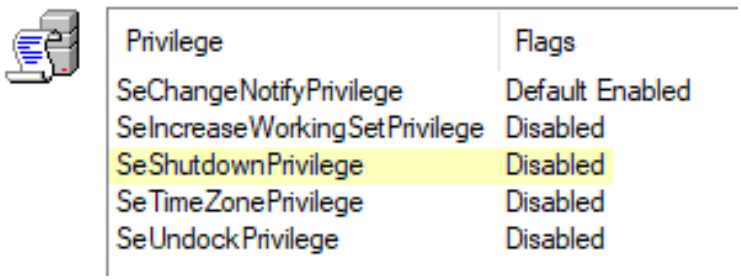


Figure 40 : Remcos privileges in Process Explorer

Examination of the binary in IDA Free reveals the method to enable SeShutdownPrivilege; a group of API functions are called as seen below in Figure 41:

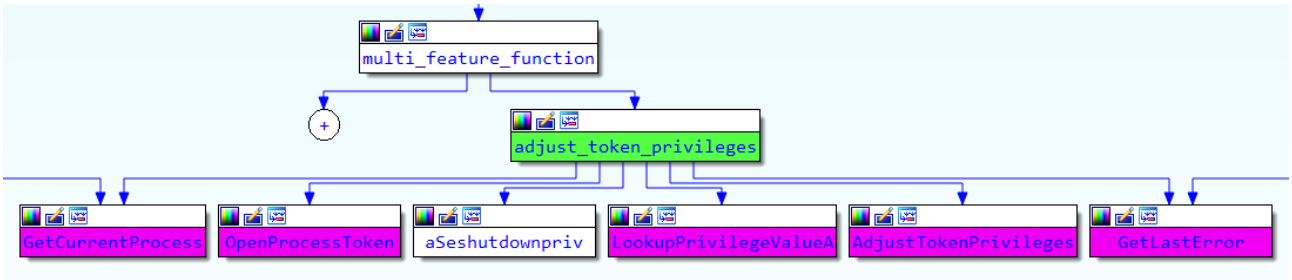


Figure 41 : Proximity browser subview In IDA Free

Below is Figure 42; it displays the subroutine adjust_token_privileges which achieves the following task:

1. GetCurrentProcess - Retrieves a pseudo handle to the current process.
2. OpenProcessToken - Opens the access token of the current process.
3. LookupPrivilegeValueA - Examines SeShutdownPrivilege value of the current process.
4. AdjustTokenPrivileges - Modifies permissions to enable SeShutdownPrivilege; this is done by setting NewState.Privileges.Attributes to SE_PRIVILEGE_ENABLED or 0x00000002.

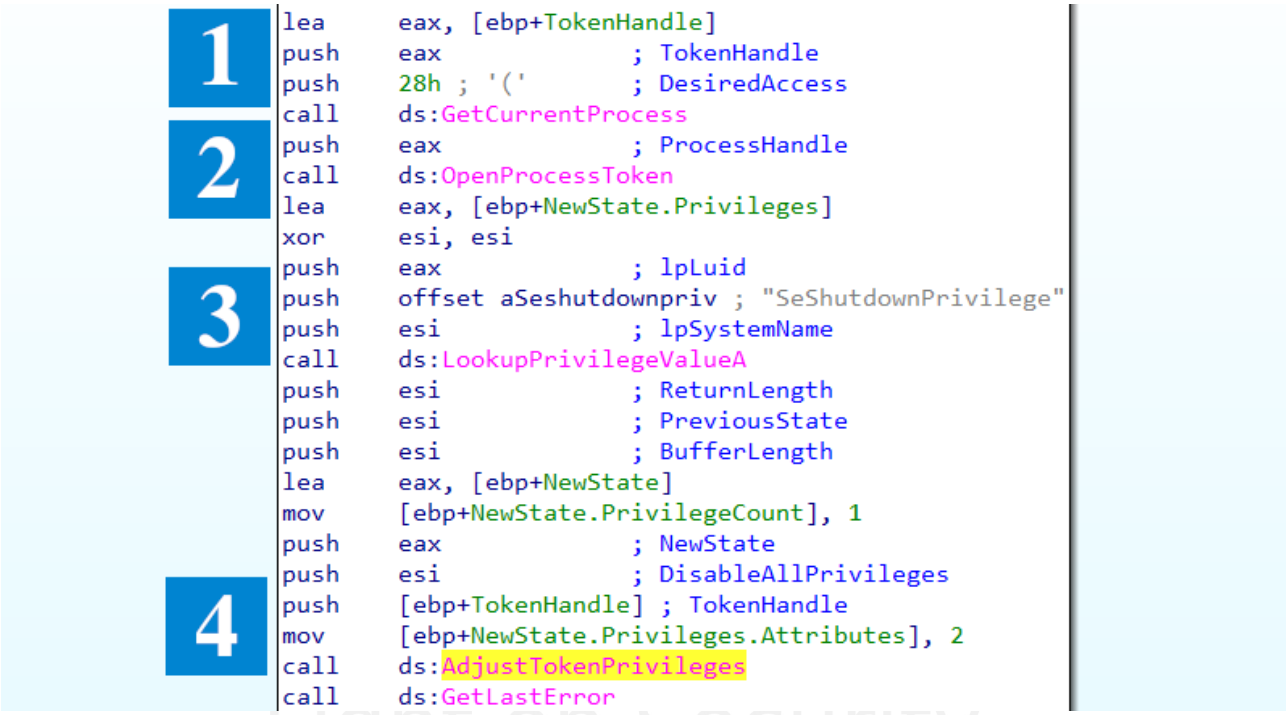


Figure 42 : Graph view of adjust_token_privilege subroutine in IDA Free.

When this subroutine completes, Remcos will have enabled SeShutdownPrivilege; applying this tactic can result in a denial of service via unauthorized shutdown of the operating system (Impact, T1529 System Shutdown).

Analysis 2 – TA0005 : Defense Evasion

T1548 Abuse Elevation Control Mechanism
.002 Bypass User Account Control

During strings analysis of the dumped Remcos binary, the following command was found:

```
override
3.5.1 Pro
/k %windir%\System32\reg.exe ADD
    HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Pol-
    icies\System /v EnableLUA /t REG_DWORD /d 0 /f
C:\Windows\System32\cmd.exe
StartForward
StartReverse
```

Figure 43 : Lines 2713-2714 reveal intent to modify registry using cmd.exe / reg.exe

As seen in Figure 44 below, IDA Free displays the strings in context:

- CreateProcessA is called to run ApplicationName cmd.exe
- dwCreationFlags stipulates there will be no visible console window
- The CommandLine parameter for cmd.exe to execute is reg.exe ADD HKLM...

```
push    eax             ; lpProcessInformation
lea     eax, [ebp+StartupInfo]
push    eax             ; lpStartupInfo
push    edi             ; lpCurrentDirectory
push    edi             ; lpEnvironment
push    8000000h        ; dwCreationFlags
push    edi             ; bInheritHandles
push    edi             ; lpThreadAttributes
push    edi             ; lpProcessAttributes
push    offset CommandLine ; "/k %windir%\\System32\\reg.exe ADD HKLM"...
push    offset ApplicationName ; "C:\\Windows\\System32\\cmd.exe"
call    ds:CreateProcessA
```

Figure 44 : CreateProcessA with cmd.exe to modify registry

Here is an explanation of the command parameters:

```
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
```

Parameter	Description
/k	Passed to cmd.exe; carries out the command specified by string.
ADD	Specifies the full path of the subkey or entry to be added.
/v <Valuename>	Specifies the name of the add registry entry.
/t <Type>	Specifies the type for the registry entry.
/d <Data>	Specifies the data for the new registry entry.
/f	Adds the registry entry without prompting for confirmation.

The registry value *EnableLUA* refers to the Limited User Account feature of User Account Control. The parameter value 0 indicates an attempt to disable LUA as cited by Microsoft:

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "EnableLUA"

Type: REG_DWORD

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Disabling this policy disables the "administrator in Admin Approval Mode" user type.
0x00000001	This policy enables the "administrator in Admin Approval Mode" user type while also enabling all other User Account Control (UAC) policies.

Figure 45 : EnableLUA registry values

The purpose of this registry modification command is to disable the User Account Control, Admin Approval Mode security policy. When enabled, the Admin Approval Mode security policy displays a UAC prompt to the built-in Administrator account before software is authorized to run. With this policy disabled, the built-in Administrator account will run all applications with full administrative privileges and no UAC prompt to hinder program execution. This security policy setting of *0 - Disable Admin Approval Mode* poses a risk to systems that have the built-in Administrator account enabled; by default this account should be disabled.

Analysis 3 – TA0009 : Collection

T1056 Input Capture

.001 Keylogging

Strings analysis revealed Remcos has online and offline keylogging capabilities; this is shown in Figure 46 below. IDA Free displays the keylogger strings from the .rdata section of the binary, which holds globally accessible read only data for the program:

Address	Length	Type	String
.rdata:0046130C	0000001A	C	Offline Keylogger Started
.rdata:00461328	00000029	C	Keylogger initialization failure: error
.rdata:004613A8	00000019	C	Online Keylogger Started
.rdata:004613C4	00000019	C	Online Keylogger Stopped
.rdata:004613E0	0000001A	C	Offline Keylogger Stopped

Figure 46 : “Keylogger” strings located using Quick Filter in IDA Free

This section will briefly examine the online keylogger subroutine.

Observe Figure 47 below. Analysis begins with the online_keylogger_started subroutine. This subroutine invokes the call_to_keylogger_initialization subroutine:

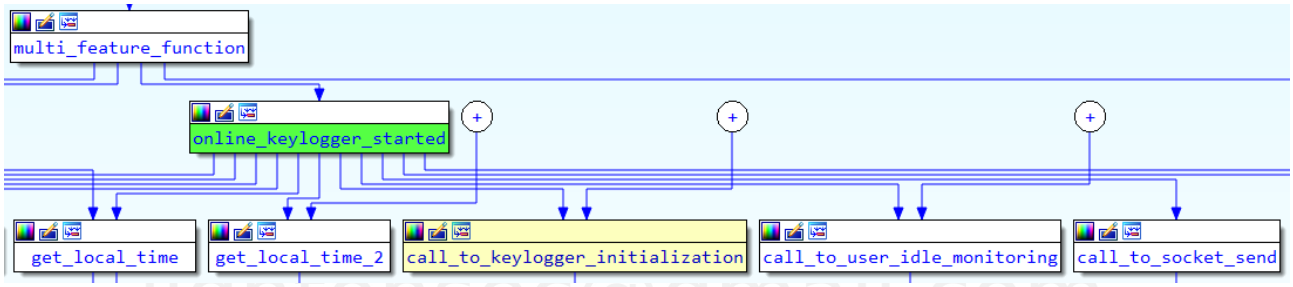


Figure 47 : online_keylogger_started invokes call_to_keylogger_initialized

Inside online_keylogger_started is a call to CreateThread. The lpStartAddress is pushed onto the stack with the offset value of subroutine call_to_intitialize_keylogger:

```
push    ebx             ; lpThreadId
push    ebx             ; dwCreationFlags
push    esi             ; lpParameter
push    offset call_to_keylogger_initialization ; lpStartAddress
push    ebx             ; dwStackSize
push    ebx             ; lpThreadAttributes
call    edi ; CreateThread
```

Figure 48 : online_keylogger_started creates a thread for call_to_keylogger_initialized

Inside call_to_keylogger_initialization, the SetWindowsHookExA function is present; this is seen below in Figure 49. The SetWindowsHookExA function is a hook; a hook intercepts events including keystrokes and mouse clicks. Hooks initialize hook procedures; the purpose of a hook procedure is to take action on the events it receives from the hook.

```
push    edi             ; dwThreadId
push    edi             ; lpModuleName
call    ds:GetModuleHandleA
push    eax             ; hmod
push    offset fn       ; lpfn
push    0Dh             ; idHook
call    ds:SetWindowsHookExA
mov     [esi], eax
test    eax, eax
jnz     short get_message_a
```

Figure 49 : SetWindowsHookExA used to monitor keystrokes

Look at Figure 49. Notice idHook above SetWindowsHookExA; it has an ascii value of 13. Microsoft cites the value of idHook 13 as follows:

Value	Meaning
WH_KEYBOARD_LL 13	Installs a hook procedure that monitors low-level keyboard input events. For more information, see the LowLevelKeyboardProc hook procedure.

This analysis revealed how Remcos creates a new thread for hooking and hook procedures to intercept low-level keyboard input, thereby monitoring user keystrokes. This technique violates data confidentiality and can result in exfiltration of passwords, intellectual property, bank account numbers, and more.

Light on Security
lightonsec@gmail.com

Task 3 : Adjust Tools

Authority:

"The IR team should use its developing understanding of the adversary's TTPs to modify tools to slow the pace of the adversarial advance and increase the likelihood of detection. The focus should be on preventing and detecting tactics— such as execution, persistence, credential access, lateral movement, and command and control—to minimize the likelihood of exfiltration and/or operational or informational impact. IOC signatures can be incorporated into prevention and detection tools to impose temporary operational cost upon the adversary and assist with scoping the incident. However, the adversary can introduce new tools to the network and/or modify existing tools to subvert IOC-centric response mechanisms"

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 13.

This task will explain how to use tools and IOCs to detect the following Remcos Tactics:

- TA0002 – Execution, Carbon Black EDR and Yara
- TA0002 – Execution, Qualys EDR
- TA0009 – Collection, Symantec EDR
- TA0011 – Command and Control, Snort and Arcsight Logger

TA0002 – Execution, Carbon Black and Yara

As observed in *Task 2 : Gather Incident Indicators, Dynamic Analysis*, two files are used in this malware infection:

- Installer - SHIPPING ADVICE#NEW.exe
- Remcos - zaymjsmod.exe

Light on Security
lightonsec@gmail.com

Brief analysis of the *SHIPPING ADVICE#NEW.exe* installer didn't reveal unique strings to qualify for a Yara signature; however examination of strings in the Remcos binary *zaymjsmod.exe* produced the following distinct identifier:

hint (75)	value (1636)
function	FlushFileBuffers
function	GetConsoleCP
function	HeapAlloc
function	HeapReAlloc
function	SetEndOfFile
function	HeapSize
function	IsValidLocale
function	GetUserDefaultLCID
file	C:\vixzo\gbshmc\icik\c1d0476e27774464ae3c107701906afe\pbcaah\gquyncxg\Release\gquyncxg.pdb
file	KERNEL32.dll
file	urlmon.dll
file	rtm.dll
file	ODBC32.dll
file	MAPI32.dll
file	mscms.dll
file	SHELL32.dll

Figure 50 : *zaymjsmod.exe* strings in PE Studio

The file path seen in Figure 50 shows a program database (.pdb) file, also known as a symbol file. These files are created as a result of compiling a program; they store information such as names of functions, addresses, resources, and symbols to assist with debugging. A fully qualified pdb path can assist with classifying malware families and creating IOCs for detection purposes.

The following Yara signature was developed using the unique pdb path seen in Figure 50 and detects the following files:

Remcos	C:\Users\analyst\AppData\Local\Temp**zaymjsmod.exe**
Copy of Remcos	C:\Users\analyst\AppData\Roaming\aiep**ianhcjk.exe**

```
rule remcos_trojan_v3_5_1pro
        {
        meta:
                first_seen      = "2022-05-26 10:41:43 UTC"
                description     = "detects unpacked remcos trojan v3.5.1 pro"
                sample          = "https://bazaar.abuse.ch/sample/1b4811e68a60e07ee30cd003d2bcb961d12038ab9ed4aef71577933a59ad5fed/"
                about_remcos    = "https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos"
                installer_vt    = "https://www.virustotal.com/gui/file/900274d5916f078ac30bedfc6b3bf5812c09de4cc1bdddd4e25d5efa1e3bb1c3"
                trojan_vt       = "https://www.virustotal.com/gui/file/c9c7b9634a4d5b49017f804207361a09ed20df84b5d31367278e51a8e5e5e75d"
                trojan_jsandbox = "https://www.joesandbox.com/analysis/634090/0/html"
                tlp             = "white"

        strings:
                $pdb_path       = "C:\\vixzo\\gbshmc\\icik\\c1d0476e27774464ae3c107701906afe\\pbcaah\\gquyncxg\\Release\\gquyncxg.pdb"

        condition:
                uint16(0) == 0×5a4d and filesize < 186KB and $pdb_path
}
```

Figure 51 : This yara rule text is available in *Appendix B - Resources*

The rule was tested in the Kali lab environment to verify a true positive detection:

```
└─$ yara -s -r remcos-trojan.yar ../../malware
remcos_trojan_v3_5_1pro ../../malware/zaymjsmod.exe
0×2a584:$pdb_path: C:\vixzo\gbshmc\icik\c1d0476e27774464ae3c107701906afe\pbcaah\gquyncxg\Release\gquyncxg.pdb
```

Figure 52 : True positive Yara detection

The above command tells Yara to do the following:

Option	Meaning
-s	List the strings in the malicious file that matched the strings in the yara rule
-r	Search recursively
remcos-trojan.yar	Search using this rule file
../../malware	Search in this directory

Light on Security
lightonsec@gmail.com

This .yar file can be uploaded via the Yara Rules Manager in Carbon Black; the server interface of the Yara Rules Manager is seen below:

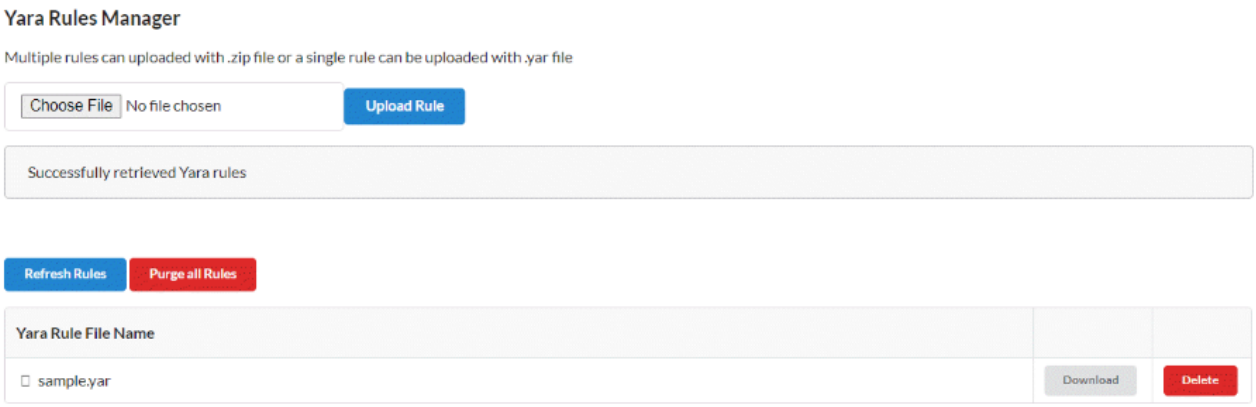


Figure 53 : Yara Rules Manager

Light on Security
lightonsec@gmail.com

Once the .yar rule is uploaded to the Rules Manager, the Yara Connector will use it to scan binary files seen by the EDR server. For more information, see the references in *Appendix B – Resources*.

TA0002 – Execution, Qualys Endpoint Detection and Response

Previously *Task 2 : Gather Incident Indicators*, *Dynamic Analysis* revealed the mutex *Remcos-6KKWZV* for this trojan variant; this mutex can be used to detect TA0002 Execution with Qualys EDR.

Figure 54 below displays the Qualys EDR Hunting interface; this image was obtained from the section *Remediation Action* from the manual *Endpoint Detection and Response : Getting Started Guide* (See Appendix B). At the bottom of Figure 54 a *Malicious Mutex Event* is highlighted with the options to remediate via *Kill Process*.

Light on Security
lightonsec@gmail.com

The following query will discover hosts that have the *Remcos-6KKWZV* mutex open as a file handle for the Remcos trojan (query results not displayed below):

```
handle.name: "\Sessions\1\BaseNamedObjects\Remcos-6KKWZV"
```

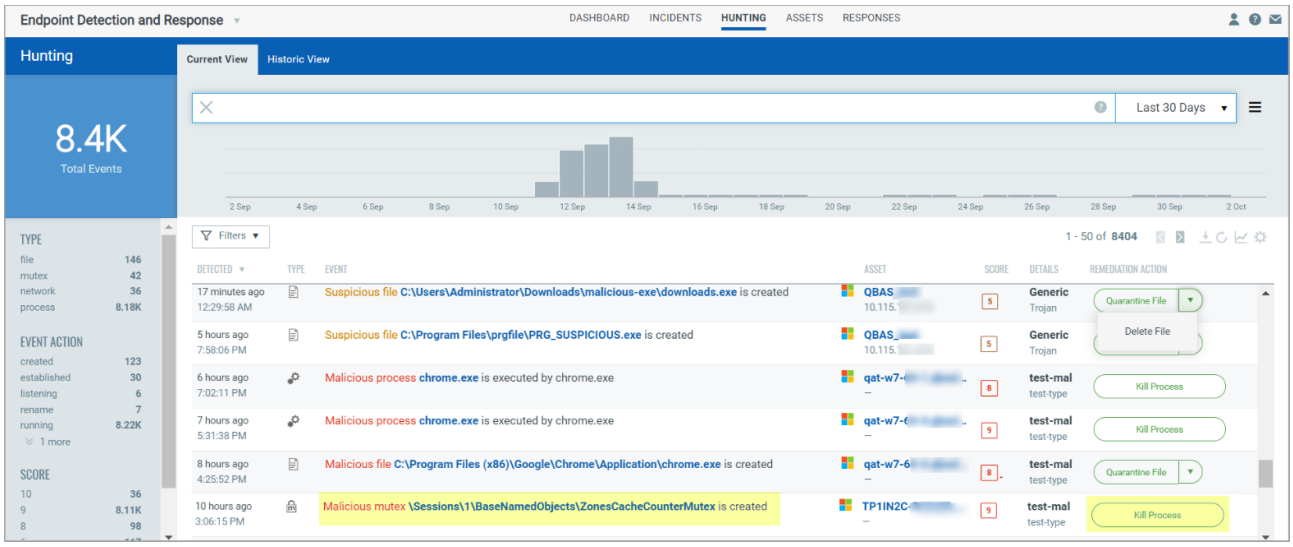


Figure 54 : Qualys EDR Displaying Malicious Mutex

TA0009 – Collection, Symantec EDR

Symantec EDR is designed to identify API calls using the following search parameter:

Field name	Type	Description
api_name	string	The API call that is detected.

Task 2 : Gather Incident Indicators, Basic Reverse Engineering revealed Remcos uses a group of API calls to perform keylogging; Remcos also uses a group of API calls for clipboard surveillance, however they have not been discussed until now. Below is an example of a nested query that could be used to identify Remcos activity based on malicious API calls for keylogger and clipboard surveillance activity:

```
type_id:8001 AND operation:1 AND process.file.name:zaymjsmod.exe
AND
      (api_name:SetWindowsHookExA OR
      api_name:GetForegroundWindow OR
      api_name:GetKeyState OR
      api_name:OpenClipboard OR
      api_name:SetClipboardData OR
      api_name:CloseClipboard OR
      api_name:EmptyClipboard OR
      api_name:GetClipboardData)
```

Type ID 8001 with the operation value of 1 indicates a process has been created; zaymjsmod.exe is provided as the process name with the applicable API calls listed for both keyboard and clipboard surveillance. References to Threat Hunting with Symantec EDR is available in Appendix B.

TA0011 - Command and Control, Snort and Arcsight Logger

During *Dynamic Analysis* in *Task 2 : Gather Incident Indicators*, Remcos revealed C2 beaconing activity to destination 172.111.153.127:3033. This section will discuss a custom Snort signature designed to detect this outbound activity, and how to create a custom dashboard in

Arcsight Logger for ongoing incident monitoring using this signature. Below is the custom signature to identify beaconing activity from Remcos:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 3033 (msg:"Remcos RAT C2
Callback"; flags:S; window:64240;
reference:url,https://www.joesandbox.com/analysis/634090/0/html;
classtype:trojan-activity; sid:7000001; rev:1;
metadata:affected_product win32, malware_family Remcos,
signature_severity Major, created 202208;)
```

lightonsec@gmail.com

This signature creates an alert “Remcos RAT C2 Callback” when the following conditions are true:

- Traffic is detected over transport layer tcp
- Traffic is coming from the home network
- Traffic is going outbound to the external network
- Traffic is traveling to destination port 3033
- The tcp SYN flag is set
- The packet window size is 64240
- Go to joesandbox.com/... for more information on the threat

The signature above was written with non-payload options, as Remcos never progressed beyond the tcp three way handshake. This rule was tested in the lab environment to verify a true positive detection:

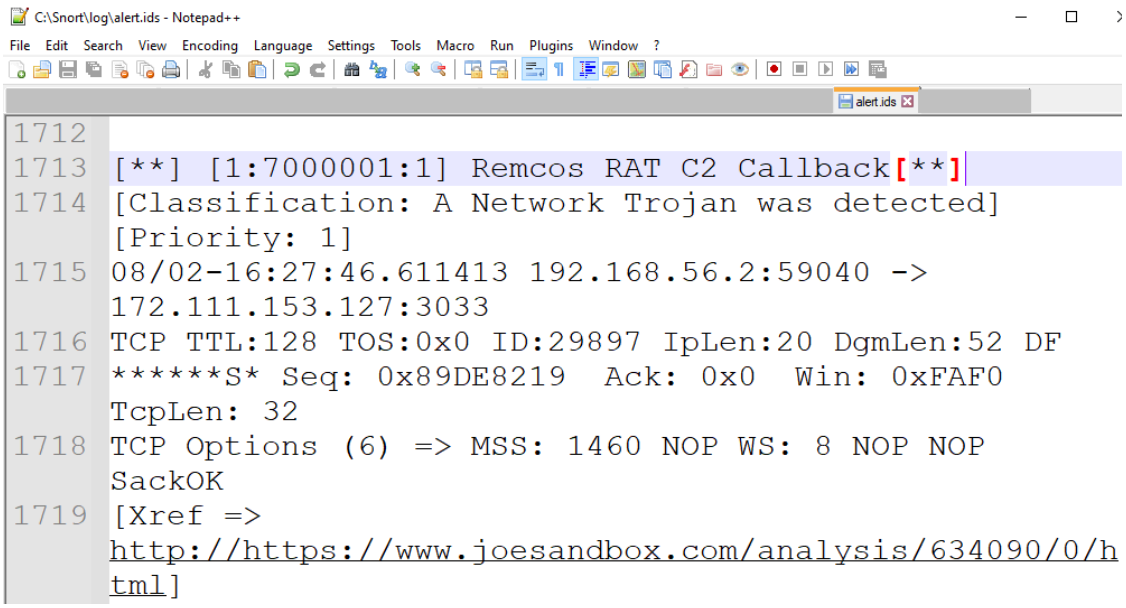


Figure 55 : Remcos network activity detected using Snort

lightonsec@gmail.com

Note: The Remcos process was permitted to run in the lab environment for over an hour and produced a total of 829 packets; this signature has the potential to produce noise unless a correlation threshold/alert is setup.

With a true positive IDS signature available, a custom shared dashboard in Arcsight Logger can help the incident response team maintain vigilance for newly infected hosts. To create a custom dashboard, begin by navigating to *Analyze* in Arcsight Logger. A search field is available as seen below in Figure 56:

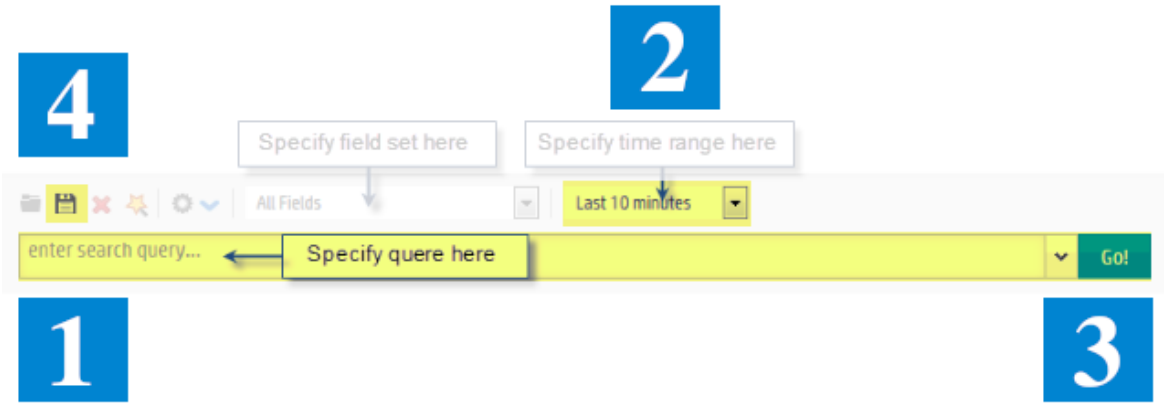


Figure 56 : Arcsight Logger search query field

The instructions to locate Snort events in Arcsight Logger are as follows:

1. Enter search query
   ```
   agentType = "snort_ids" | where name = "Remcos RAT C2 Callback"
   ```
2. Specify timeframe
3. Go !
4. Save Query
   Name: “Remcos Case 123456 Ongoing High Severity”
   Save as: Saved Search

Now move to *Dashboards* and complete the following tasks:

1. Select a customized dashboard (example dashboard name, “Ongoing Incidents”)
2. Select Tools

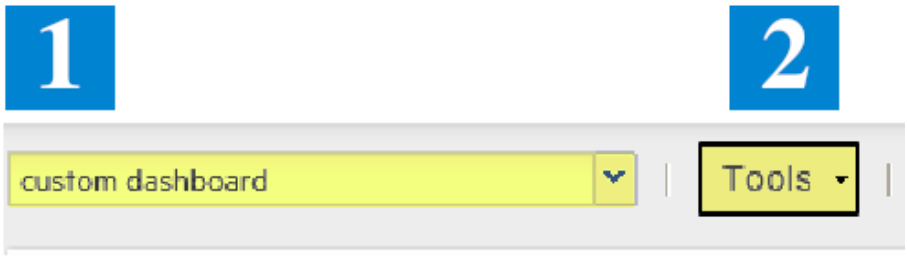


Figure 57 : Custom Dashboard setup in Arcsight Logger

3. Select Add Panel
4. Choose the Saved Search entitled “Remcos Case 123456 Ongoing High Severity”

Now the panel is added to the custom dashboard and incident responders can monitor hosts identified with the Snort signature “Remcos RAT C2 Callback.”

Phase III – Containment

Authority:

The objective is to prevent further damage and reduce the immediate impact of the incident by removing the adversary's access. The particular scenario will drive the type of containment strategy used."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 14.

lightonsec@gmail.com

This section presents three layers of containment strategies: perimeter, internal, and endpoint. The containment options presented here are not exhaustive and their applicability will differ according to infrastructure maturity, security policy stipulations, resource availability, and other considerations.

Perimeter Network Options

Technology	Action
Firewall	• Deny inbound / outbound 172.111.153.127/32 • Deny inbound / outbound 192.168.56.2/32 ○ After the endpoint has been removed from the network, eliminate this rule so the new owner of this dhcp lease can access the Internet • Deny outbound tcp dst port 3033
IPS	• Apply "Remcos RAT C2 Callback" signature with Block action
Inbound Mailers	• Search all mailboxes with attachment "SHIPPING ADVICE#NEW.exe" • Delete unread email from mailboxes. • Export list of users with email marked as read; remediate hosts as needed. • Delete read email from mailboxes.

Internal Network Options

Technology	Action
Switch/Router	• Quarantine infected host with ACL deny rule

Light on Security

Endpoint Options

lightonsec@gmail.com

Technology	Action
Anti-Virus	• Verify current definitions detect and eliminate Remcos variant • If vendor doesn't identify sample as malicious, submit to vendor for analysis. Tag virus submission as high priority. • Push client update to host • Push virus definition update to host

Endpoint Detection and Response	• Identify infected host with malicious process • Select remediation task (Isolate/Quarantine/Kill Process/etc)
Engage Local Desktop Support	• Create high priority child ticket and send to Desktop Support queue • Request endpoint removal from network • Request endpoint re-image with standard enterprise image • Follow up with courtesy phone call to Desktop Support regarding ticket
Engage User	• Call the user and tell them to unplug the computer from the network.

Phase IV – Eradication and Recovery

Authority:

The objective of this phase is to allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 15.

The incident is now over. It is time to resume operations as they were before the incident occurred.

Perimeter Network Options

Technology	Action
Firewall	• Remove deny inbound / outbound 192.168.56.2/32

Internal Network Options

Technology	Action
SIEM	• Remove Remcos Snort panel from Ongoing Incidents dashboard after 24-72 hours of 0 detections
Switch/Router	• Remove host from quarantine on switch/route ACL

Endpoint Options

Technology	Action
Anti-Virus	• Verify all files, registry entries, running processes are terminated from system • Ensure all endpoints are running the latest virus definitions and client version; if not, deploy updates to endpoints
Endpoint Detection and Response	• Remove endpoint from quarantine

Engage Local Desktop Support	• Verify Desktop Support child ticket is resolved and user has resumed work with re-imaged endpoint
Engage User	• Call user and help them understand how to identify phishing attacks

Phase V – Post Incident Activities

Authority:

"The goal of this phase is to document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents."

Source: Cybersecurity Incident & Vulnerability Response Playbooks, page 15.

Schedule meetings with Incident Response team, Desktop Support, Secure Email Gateway, Network Security, and other teams as applicable to discuss lessons learned, process improvement, infrastructure hardening options, etc.

Perimeter Options

Technology	Action
Firewall	• Deny outbound port 2404 (Default Remcos port)
Inbound Mailers	• Deny executable attachments on inbound mailers • Deny, quarantine, or sandbox zip attachments on inbound mailers

Endpoint Options

Technology	Action
Anti-Virus	• Ensure all endpoints are up to date on client and definition versions
EDR	• Consider automating quarantine or remediation of infected endpoints
User Awareness	• Counsel user via phone conversation and in writing regarding phishing emails • Assign security awareness training to user

Incident Response Team

Task	Description
Meet with Management, Incident Response Leads, Team Members	• Discuss failures encountered in the incident • Discuss successes encountered in the incident • Identify tools, resources, skills, training, network and

	endpoint visibility, and other variables needed to improve incident response capabilities
Meet with Other IT Teams	• Discuss measures to harden the environment to prevent future incidents of similar nature
Update RAT playbook	• Add Remcos details as applicable
Team Cross Training	• Examine skill gaps and assign internal training / mentoring to fill gaps ◦ Within IR team ◦ With other teams as needed (Desktop Support, System Administrators, etc)
Eliminate Process Hurdles	• Identify communication, escalation, process, documentation, ticketing, and other hurdles that delayed resolution of the incident; for instance: ◦ Update contact lists ◦ Eliminate busywork in processes ◦ Clarify vague documentation ◦ Delegate simple tasks to junior IR members ◦ Write automation scripts ◦ Etc

Light on Security
lightonsec@gmail.com

Conclusion

This concludes analysis of Remcos RAT using v3.5.1 Pro, originally detected on 2022-05-26 10:41:43 UTC. This exercise was not intended to be a complete analysis of Remcos as it is feature rich; rather through this exercise, Remcos was examined through CISA's Incident Response Lifecycle phases where the following key findings were learned:

Phase	Objective	Key Findings
Phase I	Cyber Threat Intelligence	• Remcos was first seen in 2016; still active in 2022 • Infection results in confidentiality breach due to keylogging, screen capture, file system access, and other features • Threat Actors use Remcos to target aviation, energy sector, and other industries in West, Middle East, Asia, and African territories
Phase II	Detection and Analysis	• Two binary files present in infection: Installer and Remcos RAT • Defense Evasion techniques include Timestomping and File Obfuscation • Run key for persistence • Outbound C2 172.111.153.127:3033 • Several creative ways to detect Remcos using Snort, Yara, Carbon Black / Qualys / Symantec EDR, Arcsight Logger
Phase III	Containment	• Prioritize removing phishing emails from user mailboxes to prevent further infection

		• Track and monitor existing infections via firewall or IPS logs • Ensure AV signatures detect Remcos variant and push to endpoints
Phase IV	Eradication and Recovery	• Ensure endpoint is clean via EDR, AV, or system re-image • Remove host / IP address from quarantine / deny / block policies
Phase V	Post-Incident Activities	• Discuss how to improve incident response lifecycle with incident response and other teams • Advocate to harden the environment to prevent future incidents of similar nature

Light on Security

Appendix A – Indicators of Compromise

Simple IOCs

Light on Security
lightonsec@gmail.com

File:

File	Path	sha1
SHIPPING ADVICE#NEW.exe	C:\Users\analyst\Desktop	bda3f8d1087deacdc2827035a9075b17decf358a
zaymjsmod.exe	%LOCALAPPDATA%\Temp	21020cd355cbbdbda37eaa4e335bd32970d25270
ianhcjk.exe	%APPDATA%\aiep	21020cd355cbbdbda37eaa4e335bd32970d25270
qmkhkh	%LOCALAPPDATA%\Temp	73f6b3c9d1d115d521df6f26bb7fd3d09eb054ff
5tq9d2mjcoubez	%LOCALAPPDATA%\Temp	b94ee185568392960724e4102cc289289c5827dc

Registry:

Light on Security
lightonsec@gmail.com

Registry Hive\Subkeys\Key	Registry Value
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avgf	C:\Users\User\AppData\Roaming\aiep\ianhcjk.exe
HKCU\SOFTWARE\Remcos-6KKWZV\exepath	Binary value
HKCU\SOFTWARE\Remcos-6KKWZV\licence	[0-9A-F]{33}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	0

Network:

Destination IPv4	Destination Port	Transport Protocol
172.111.153.127	3033	TCP

DNS:

Domain	URL	Ipv4 Address
geoplugin.net	http://geoplugin.net/json.gp	178.237.33.50

Light on Security
lightonsec@gmail.com

Mutex:

Name
SM0:3840:168:WilStaging_02
Remcos-6KKWZV

Advanced IOCs

MITRE ATT&CK Tactic, Technique, Mitigation, and Detection

Light on Security
lightonsec@gmail.com

The table below combines IOCs from the installer and Remcos trojan given they are co-dependent for this variant.

Tactic	Technique	ID	IOC	Mitigation	ID	Detection	ID
Initial Access	Phishing	T1566	SHIPPING ADVICE#NEW.exe	Antivirus/ Antimalware, Network Intrusion Prevention, Software Configuration, User Training	M1049, M1031, M1054, M1017	Application Log Content, File Creation, Network Traffic Content, Network Traffic Flow	DS0015, DS0022, DS0029
Execution	User Execution, Malicious File	T1204.002	C:\Users\analyst\Desktop\SHIPPING ADVICE#NEW.exe	User Training, Execution Prevention, Behavior Prevention on Endpoint	M1017, M1038, M1040	Process Creation, File Creation	DS0009 DS0022
Execution	Command and Scripting Interpreter, Windows Command Shell	T1059.003	CreateProcessA, ShellExecuteW: C:\Windows\System32\cmd.exe	Execution Prevention	M1038	Command Execution, Process Creation	DS0017 DS0009
Execution	Command and Scripting Interpreter, Visual Basic	T1059.005	ShellExecuteW 'CreateObject ("WScript.Shell").Run "cmd /c """	Execution Prevention, Disable or Remove Feature or Program	M1038, M1042	Command Execution, Process Creation	DS0017 DS0009
Persistence, Privilege	Boot or Logon Autostart	T1547.001	HKCU\SOFTWARE\Microsoft\Windows\	Not easily mitigated	N/A	Windows Registry,	DS0024

Escalation	Execution, Registry Run Keys		CurrentVersion\Run\ avgf			Windows Registry Key Creation	
Privilege Escalation	Access Token Manipulation	T1134	AdjustTokenPrivileges set to SE_PRIVILEGE_ ENABLED on SeShutdownPrivilege	Not easily mitigated	N/A	OS API Execution	DS0009
Defense Evasion	Masquerading	T1036	SHIPPING ADVICE#NEW.exe has Excel spreadsheet thumbnail	Execution Prevention, Code Signing, User Security Awareness Training	M1038, M1045	Not easily detected	N/A
Defense Evasion	Obfuscated Files or Information	T1027. 002	Nullsoft PiMP Stub	Antivirus/ Antimalware, Behavior Prevention on Endpoint	M1049, M1040	File, File Metadata	DS0022
Defense Evasion	Indicator Removal on Host, Timestomp	T1070. 006	%TEMP%\ qmkhkh	Not easily mitigated	N/A	File Metadata , File Modification	DS0022
Defense Evasion	Indicator Removal on Host - Timestomp	T1070. 006	%TEMP%\ 5tq9d2mjcoubez	Not easily mitigated	N/A	File Metadata , File Modification	DS0022
Defense Evasion	Indicator Removal on Host - Timestomp	T1070. 006	%TEMP%\ zaymjsmod.exe	Not easily mitigated	N/A	File Metadata , File Modification	DS0022
Defense Evasion	Virtualization/ Sandbox Evasion, System Checks	T1497. 001	OutputDebugStringW IsDebuggerPresent GetTickCount	Not easily mitigated	N/A	Process, OS API Execution	DS0009
Defense Evasion	Modify Registry	T1112	HKCU\SOFTWARE\ Remcos-6KKWZV	Restrict Registry Permissions	M1024	Windows Registry, Windows Registry Key Creation	DS0024
Defense Evasion	Abuse Elevation Control Mechanism, Bypass User Account Control	T1548. 002	/k %windir %\System32\reg.exe ADD HKLM\SOFTWARE\ Microsoft\Windows\ CurrentVersion\ Policies\System /v En ableLUA /t REG_DWORD /d 0 /f	Audit, Privileged Account Management, Update Software, User Account Control	M1047 M1026 M1051 M1052	Command Execution, Process Creation, Process Metadata, Windows Registry Key Modification	DS0017, DS0009, DS0024
Defense Evasion	Abuse Elevation Control Mechanism, Bypass User Account Control	T1548. 002	ShellExecuteW Software\\Classes\\ mscfile\\shell\\open\\ command Eventvwr.exe	Audit, Privileged Account Management, Update Software, User Account Control	M1047 M1026 M1051 M1052	Command Execution Process Creation Process Metadata Windows Registry Key Modification	DS0017 DS0009 DS0024
Discovery	Query Registry	T1012	RegEnumValueA , RegEnumKeyA ,	Not easily mitigated	N/A	OS API Execution,	DS0009, DS0024

Light on Security
lightonsec@gmail.com

			RegQueryValueExA			Windows Registry Key Access	
Discovery	System Location Discovery	T1614	http://geoplugin.net/json.gp	DNS Blackhole with daily reporting	N/A	Domain Name	DS0038
Discovery	System Location Discovery, System Language Discovery	T1614.001	HKLM\SYSTEM\CurrentControlSet\Control\NLS\Language	Not easily mitigated	N/A	OS API Execution, Windows Registry Key Access	DS0009, DS0024
Discovery	System Time Discovery	T1124	GetSystemTimeAsFileTime	Not easily mitigated	N/A	OS API Execution	DS0009
Collection	Screen Capture	T1113	CreateDCA CreateCompatibleDC CreateCompatibleBitmap SelectObject StretchBlt GetDIBits GetObjectA	Not easily mitigated	N/A	OS API Execution	DS0009
Collection	Audio Capture	T1123	waveInOpen waveInClose waveInStart waveInStop	Not easily mitigated	N/A	OS API Execution	DS0009
Collection	Clipboard Data	T1115	CloseClipboard EmptyClipboard GetClipboardData OpenClipboard SetClipboardData	Not easily mitigated	N/A	OS API Execution	DS0009
Collection	Input Capture, Keylogging	T1056.001	SetWindowsHookEx	Not easily mitigated	N/A	OS API Execution	DS0009
Collection	Video Capture	T1125	OpenCamera CloseCamera GetFrame FreeFrame	Not easily mitigated	N/A	OS API Execution	DS0009
Command and Control	Non-Standard Port	T1571	Outbound TCP dst port 3033	Network Segmentation, Network Intrusion Prevention	M1030, M1031	Network Traffic Flow	DS0029
Command and Control	Encrypted Channel, Asymmetric Cryptography	T1573.002	CryptAcquireContextA CryptGenRandom CryptReleaseContext TLS 1.3 TLS_AES_128_GCM_SHA256	Network Intrusion Prevention, SSL/TLS Inspection	M1031, M1020	Network Traffic Content	DS0029
Impact	System Shutdown	T1529	Enable SeShutdownPrivilege via AdjustTokenPrivileges	Not easily mitigated	N/A	Command Execution Process Creation Host Status	DS0017, DS0009, DS0013
Impact	Data Destruction	T1485	DeleteFileA DeleteFileW	Data Backup	M1053	File, File Deletion	DS0022
Impact	Service Stop	T1489	ControlService	Restrict File and	M1022	OS API	DS0009,

Lightcyber Security

			ChangeServiceConfigW	Directory Permissions		Execution, Windows Registry, Windows Registry Key Modification	DS0024

Light on Security
lightonsec@gmail.com

Appendix B – Resources

Malware Bazaar Sample

https://bazaar.abuse.ch/sample/1b4811e68a60e07ee30cd003d2bcb961d12038ab9ed4aef71577933a59ad5fed/

Summary of tools used

Tool	Resource
AutoRuns	https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
Autotimeliner	https://github.com/andreafortuna/autotimeliner
Cygwin/dd	https://www.cygwin.com
DCode	https://www.digital-detective.net/dcode/
DumpIt	https://www.comae.com/ https://github.com/Crypt2Shell/Comae-Toolkit
IDA Free	https://hex-rays.com/ida-free/
Kali	https://www.kali.org/get-kali/
Log2timeline/Plaso	https://github.com/log2timeline/plaso Also available on the SANS SIFT workstation
PE-Sieve	https://github.com/hasherezade/pe-sieve
PEStudio	https://www.winitor.com/
Process Explorer	https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer
Process Monitor	https://learn.microsoft.com/en-us/sysinternals/downloads/procmon
SIFT Workstation	https://www.sans.org/tools/sift-workstation/
Snort	https://www.snort.org/downloads
Virtual Box	https://www.virtualbox.org/wiki/Downloads
Volatility 2/3	https://www.volatilityfoundation.org/releases
Windows 10	https://www.microsoft.com/en-us/software-download/windows10ISO
Wireshark	https://www.wireshark.org/
x64dbg	https://x64dbg.com/
Yara	https://yara.readthedocs.io/en/stable/gettingstarted.html

Yara Rule

```
rule remcos_trojan_v3_5_1pro
	{
	meta:
		first_seen	= "2022-05-26 10:41:43 UTC"
		description	= "detects unpacked remcos trojan v3.5.1 pro"
		sample		=
"https://bazaar.abuse.ch/sample/1b4811e68a60e07ee30cd003d2bcb961d12038ab9ed4aef71577933a59ad5fed/
"
		about_remcos	= "https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos"
		installer_vt	=
"https://www.virustotal.com/gui/file/900274d5916f078ac30bedfc6b3bf5812c09de4cc1bdddd4e25d5efa1e3b
b1c3"
		trojan_vt	=
"https://www.virustotal.com/gui/file/c9c7b9634a4d5b49017f804207361a09ed20df84b5d31367278e51a8e5e5
e75d"
		trojan_jsandbox	= "https://www.joesandbox.com/analysis/634090/0/html"
		tlp		= "white"

	strings:
		$pdb_path	=
"C:\\vixzo\\gbshmc\\icik\\c1d0476e27774464ae3c107701906afe\\pbcaah\\gquyncxg\\Release\\gquyncxg.p
db"

	condition:
		uint16(0) == 0x5a4d and filesize < 186KB and $pdb_path
}
```

Detection Tools - Documentation

ArcSight Logger v6.7

- https://www.youtube.com/watch?v=cet5uluHxRo
- https://community.microfocus.com/cyberres/productdocs/w/logger/38737/logger-documentation-list

Carbon Black EDR User Guide

- https://docs.vmware.com/en/VMware-Carbon-Black-EDR/7.5/VMware%20Carbon%20Black%20EDR%207.5%20User%20Guide.pdf

Carbon Black Yara Connector

- https://github.com/carbonblack/cb-yara-connector

Symantec Threat Hunting Guide

- https://techdocs.broadcom.com/content/dam/broadcom/techdocs/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/generated-pdfs/sedr_threat_hunting_guide_4.6.pdf

Symantec EDR Search Query

- https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-5/search-fields-and-descriptions-v126755396-d38e59231.html

Symantec EDR Event Summary Type IDs

- https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-detection-and-response/4-5/search-fields-and-descriptions-v126755396-d38e59231/event-summary-type-ids-v121987556-d38e58861.html

Qualys EDR Getting Started Guide

- https://www.qualys.com/docs/qualys-edr-getting-started-guide.pdf

Qualys EDR Search Query Syntax

- https://qualysguard.qg2.apps.qualys.com/ioc/help/edr/search_tips/search_ui_events.htm

Research

CISA Incident Response Playbook

- https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Breaking Security, Remcos

- https://breakingsecurity.net/about/
- https://breakingsecurity.net/remcos/
- https://breakingsecurity.net/remcos/changelog/

AlienVault OTX

- https://otx.alienvault.com/indicator/file/c276946bee7f1e7e5bdcbdecb1db46dca96f4d4ab05c9876ac3a552b55b7e071
- https://otx.alienvault.com/indicator/ip/172.111.153.127

Fortinet Threat Encyclopedia / W32/Injector.ERRU!tr

- https://www.fortiguard.com/encyclopedia/virus/10091678

IANA Service Names and Port Numbers

- https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

IBM Security X-Force Threat Intelligence Index 2022

- https://www.ibm.com/downloads/cas/ADLMYLAZ

MITRE ATT&CK Remcos

- https://attack.mitre.org/versions/v11/software/S0332/

Mandiant

- *Definitive Dossier of Devilish Debug Details – Part One: PDB Paths and Malware:*
- https://www.mandiant.com/resources/blog/definitive-dossier-of-devilish-debug-details-part-one-pdb-paths-malware

Remcos Q2 2022 News

- https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

Spamhaus Botnet Reports

- https://www.spamhaus.com/custom-content/uploads/2022/04/Botnet-Report-Q1-2022.pdf
- https://www.spamhaus.com/custom-content/uploads/2022/07/2022-Q2-Botnet-Threat-Update.pdf

Threat Actors Using Remcos

- https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
- https://attack.mitre.org/versions/v11/software/S0332/

Microsoft UAC - Admin Approval Mode

- https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-admin-approval-mode-for-the-built-in-administrator-account

Light on Security lightonsec@gmail.com