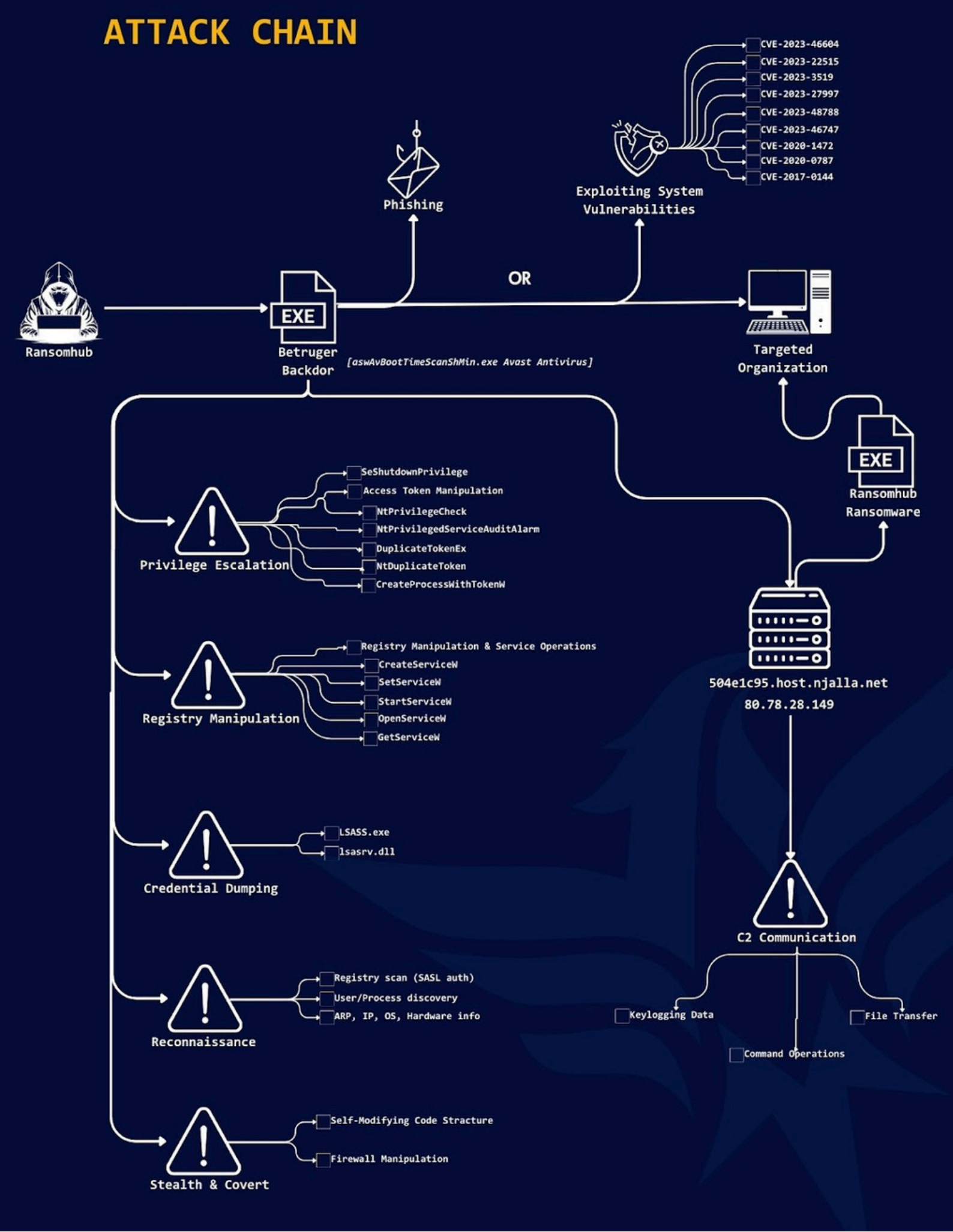
ThreatMon
Under Cyber Wings

RANSOMHUB GROUP & NEW BETRUGER BACKDOOR


ATTACK CHAIN
CVE-2023-46604
CVE-2023-22515
CVE-2023-3519
CVE-2023-27997
CVE-2023-48788
CVE-2023-46747
CVE-2020-1472
CVE-2020-0787
CVE-2017-0144
Exploiting System Vulnerabilities
Phishing
OR
Ransomhub
EXE
Betruger Backdor
[aswAvBootTimeScanShMin.exe Avast Antivirus]
Targeted Organization
EXE
Ransomhub Ransomware
SeShutdownPrivilege
Access Token Manipulation
NtPrivilegeCheck
NtPrivilegedServiceAuditAlarm
DuplicateTokenEx
NtDuplicateToken
CreateProcessWithTokenW
Privilege Escalation
Registry Manipulation & Service Operations
CreateServiceW
SetServiceW
StartServiceW
OpenServiceW
GetServiceW
Registry Manipulation
504e1c95.host.njalla.net
80.78.28.149
LSASS.exe
lsasrv.dll
Credential Dumping
C2 Communication
Registry scan (SASL auth)
User/Process discovery
ARP, IP, OS, Hardware info
Reconnaissance
Keylogging Data
File Transfer
Command Operations
Self-Modifying Code Stracture
Firewall Manipulation
Stealth & Covert

DIAMOND MODEL

Ransomhub Ransomware As a Service (RaaS)

Financially Motivated

Dark Web Presence

Betruger Backdoor (Rust-based)

Credential Dumping

Keylogging

Self-modifying code

Privilege escalation

File exfiltration

Command and Control (C2) Communication

Possible Ransomware Infection

Masquerading

Multi-Functionality

Firewall Manipulation

Registry & Service Manipulation

Discovery

504e1c95.host.njalla.net

80.78.28.149

WSS over TLS/SSL communication

ransomxifxwc5eteopdobynonjctkxx
vap77yqifu2emfbecgbqdw6qd.onion

4D598799696AD5399FABF7D40C4D1BE9F05D74
CFB311047D7391AC0BF64BED47B56EEE66A528

Primary: USA (53.06%)

Secondary: Canada (14.29%)

More Countries - Global Attacks

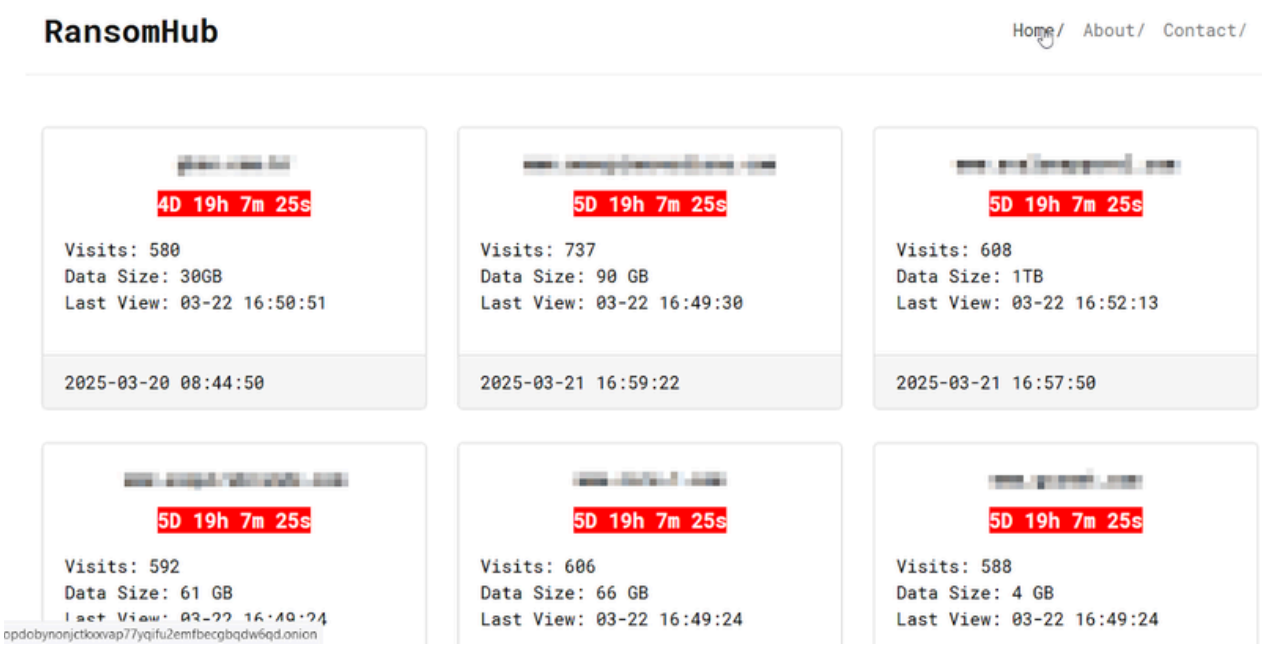
Technology (20.83%)

Manufacturing (20.83%)

Healthcare (20.83%)

More Sectors - Global Attacks

About Ransomhub Group



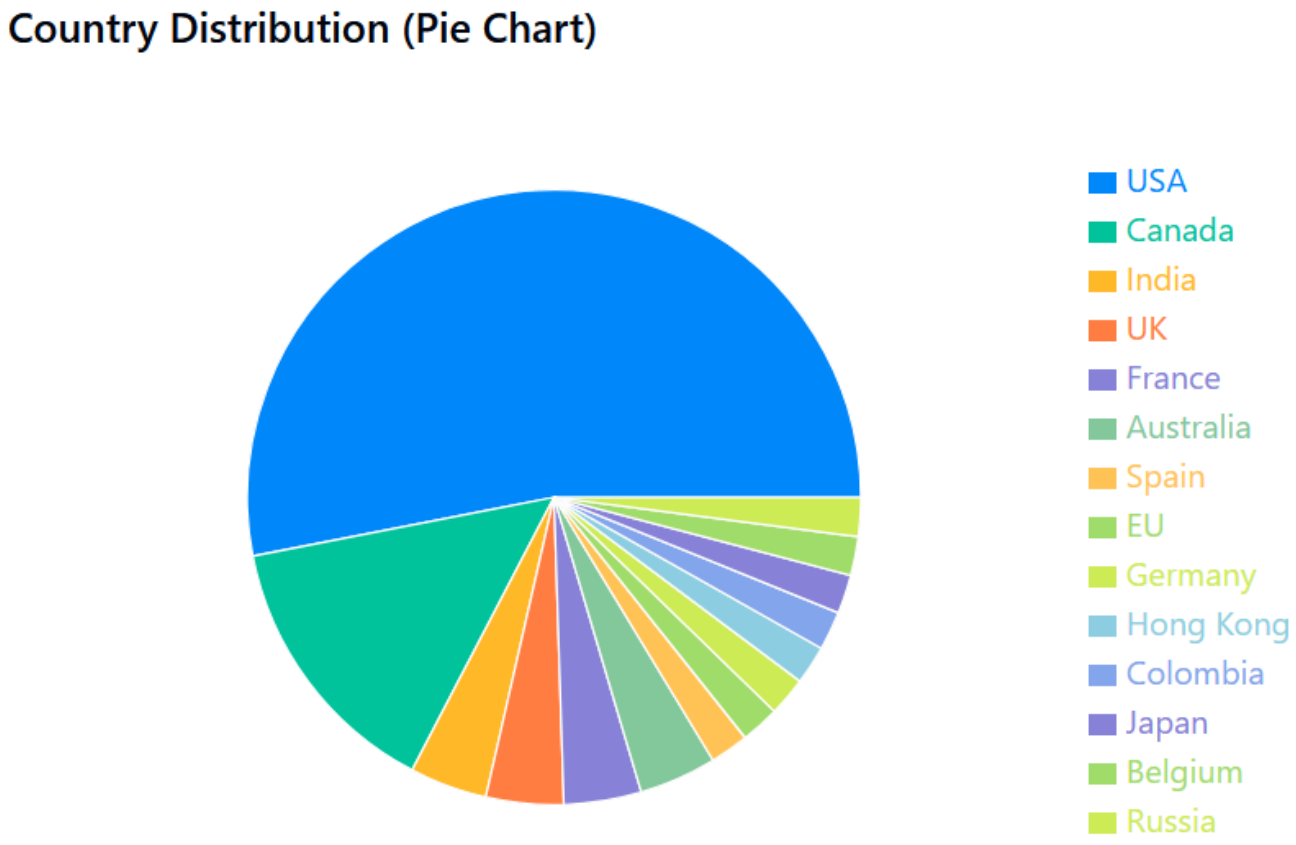
Ransomhub Official Dark Web Website

RansomHub is a **ransomware group** that targets organizations **worldwide**, encrypting their data and demanding payment for decryption. Operating as a **Ransomware-as-a-Service (RaaS)** platform, the group collaborates with affiliates who carry out attacks using RansomHub's tools and infrastructure. In addition to encrypting data, RansomHub threatens to leak stolen information if victims refuse to pay, increasing pressure on targeted organizations.

Like most ransomware groups, RansomHub is **financially motivated**, seeking to maximize its profits by extorting victims. The group often demands payments in **cryptocurrency** to make transactions harder to trace, and it carefully selects targets that are likely to pay large sums to **recover their data**. By compromising **networks** and **exfiltrating** sensitive information, RansomHub increases its leverage, making it more difficult for organizations to refuse their demands.

The group employs various techniques to infiltrate systems, including **exploiting security vulnerabilities**, **phishing attacks**, and abusing **remote access tools.** Their targets often include **large corporations, government agencies,** and **critical infrastructure providers**, as these entities are more likely to suffer significant operational and **financial damage** if their data is compromised.

Ransomhub Threat Analysis / 2025
Targeted Country Distribution / March 2025



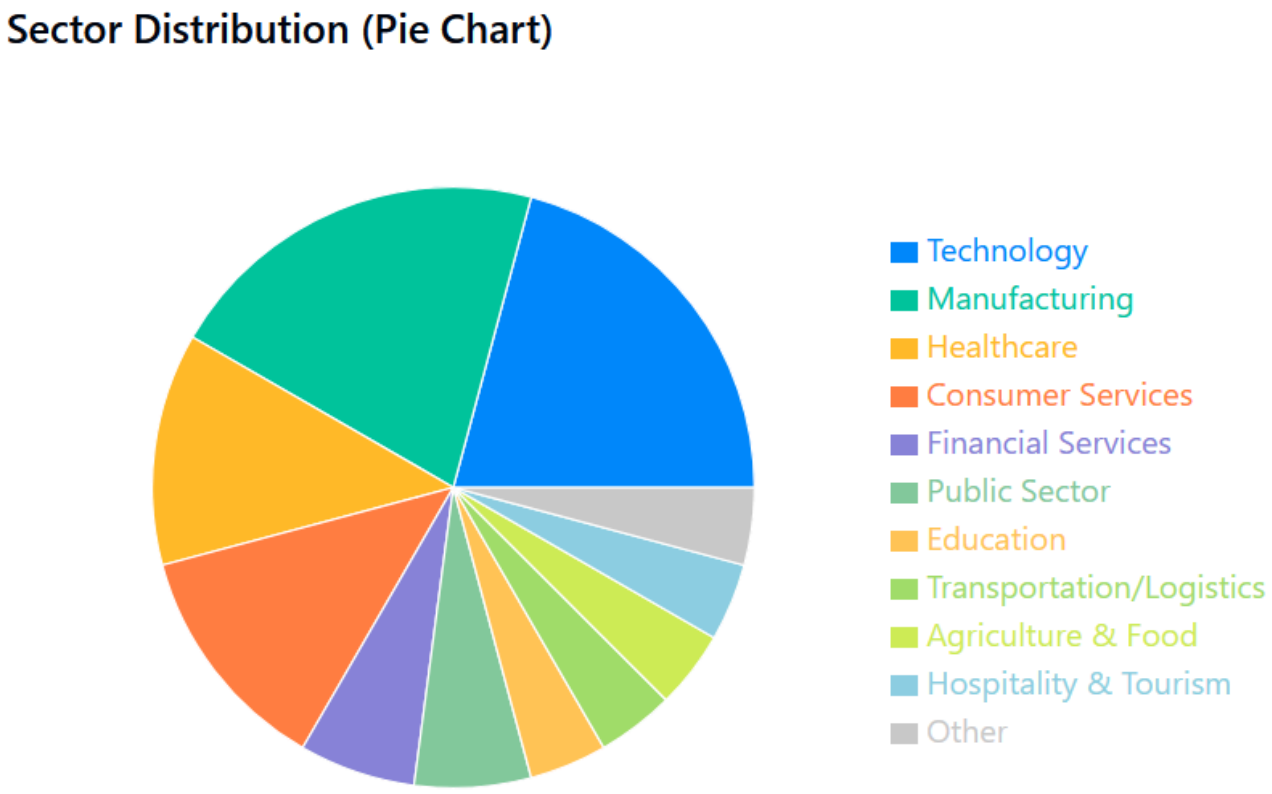
Country Distribution Graph

Based on the country information, the United States is by far the most targeted country (53.06%), followed by Canada (14.29%). Together, these North American countries account for over 67% of all attacks..

Key Findings - Country Analysis

Findings & Analysis
• ***North American Focus:*** *USA and Canada are the primary targets (67.35% combined)*
• ***Global Reach:*** *Attacks span at least 14 different countries across multiple continents*
• ***Secondary Markets:*** *India, UK, France, and Australia each appear twice in the data*
• ***English-Speaking Countries:*** *A notable preference for targeting English-speaking nations*

Targeted Sectoral Distribution / March 2025



Sectoral Distribution Graph

Based on the detailed sector information, Technology and Manufacturing are tied as the most targeted sectors (20.83% each), followed by Healthcare and Consumer Services (12.50% each).

Key Findings - Sector Analysis

Findings & Analysis
• ***Technology & Manufacturing:*** *These sectors are the most targeted (10 victims each)*
• ***Healthcare & Consumer Services:*** *Second most targeted sectors (6 victims each)*
• ***Financial Services & Public Sector:*** *These critical infrastructure sectors represent the third tier of targets*
• ***Diverse Targeting:*** *Ransomhub attacks span at least 12 different sectors, showing broad targeting*
• ***Critical Services:*** *Many targeted organizations provide essential services or possess sensitive data*

Tools Used - Ransomhub

Source: ransomware.live

Tool Name	Category	Description
AnyDesk	RMM Tools	Remote desktop software that allows access and control of computers from a distance.
Atera	RMM Tools	All-in-one RMM and PSA platform for IT professionals to monitor, manage, and support networks remotely.
N-Able	RMM Tools	Comprehensive RMM solution that provides network monitoring, patch management, and remote support capabilities.
ScreenConnect	RMM Tools	Remote support software (now called ConnectWise Control) that enables technicians to connect to and control remote devices.
Splashtop	RMM Tools	Remote desktop solution that allows users to access and control computers from various devices.
Angry IP Scanner	Discovery	Fast and lightweight network scanner that pings IP addresses and ports to find active hosts.
Nmap	Discovery	Powerful network discovery and security auditing tool for scanning networks and identifying running services.
Softperfect Netscan	Discovery	Network scanner that can discover devices, scan ports, and map network resources.

Metasploit	Offsec	Advanced open-source framework for developing, testing, and executing exploits against remote targets.
Cobalt Strike	Offsec	Commercial penetration testing tool that enables adversary simulations and red team operations.
CrackMapExec	Offsec	Post-exploitation tool designed to assess and exploit Windows networks.
Sliver	Offsec	Cross-platform adversary emulation/red team framework.
Kerbrute	Offsec	Tool designed to perform Kerbero's pre-auth bruteforcing to enumerate valid Active Directory accounts.
Impacket	Offsec	Collection of Python classes for working with network protocols, used for network penetration testing.
PSCP	Exfiltration	Command-line tool that securely transfers files between computers using SSH.
RClone	Exfiltration	Command-line program for managing files on cloud storage, which can synchronize, copy, and transfer data.
WinScp	Exfiltration	Free SFTP, SCP, Amazon S3, WebDAV, and FTP client for Windows, used for secure file transfer.
BITSAdmin	LOLBAS	Command-line tool that creates and monitors download or upload jobs using the Background Intelligent Transfer Service.
PsExec	LOLBAS	Lightweight tool that lets you execute processes on remote systems without manually installing client software.
Mimikatz	Credential Theft	Post-exploitation tool that can extract plaintext passwords, hash, PIN codes and kerberos tickets from memory.

Vulnerabilities Used - Ransomhub

VENDOR	PRODUCT	CVE	SEVERITY	SOURCE
Apache	ActiveMQ	CVE-2023-46604	Critical	cisa.gov, ransomware.live
Atlassian	Confluence Data Center & Server	CVE-2023-22515	Critical	cisa.gov, ransomware.live
Citrix	NetScaler ADC & Gateway	CVE-2023-3519	Critical	cisa.gov, ransomware.live
Fortinet	FortiOS SSL-VPN & FortiProxy	CVE-2023-27997	Critical	cisa.gov, ransomware.live
Fortinet	FortiClientEMS	CVE-2023-48788	Critical	cisa.gov, ransomware.live
F5	BIG-IP	CVE-2023-46747	Critical	cisa.gov, ransomware.live
Windows	NetLogon	CVE-2020-1472	Medium	cisa.gov, ransomware.live
Windows	BITS	CVE-2020-0787	High	cisa.gov, ransomware.live
Windows	SMBv1	CVE-2017-0144	High	cisa.gov, ransomware.live

TTP List - Ransomhub

Source: ransomware.live

Execution (TA0002)	Defense Evasion (TA0005)	Lateral Movement (TA0008)	Impact (TA0040)
Windows Management Instrumentation (T1047) The ransomware deletes shadow copies using the WMIC.exe utility.	**Indicator Removal: Clear Windows Event Logs (T1070.001)** The ransomware clears the victim machine's application, system, and security event logs using the wevtutil.exe utility.	**Lateral Tool Transfer (T1570)** Affiliates were identified using: psexec.exe, PsExec.exe, and smbexec.exe for lateral movement.	**Service Stop (T1489)** The Windows IIS service stop command is executed using iisreset.exe. Allows for encryption of web applications hosted on IIS servers as files linked to these applications are typically locked while IIS is running.
Command and Scripting Interpreter: Windows Command Shell (T1059.003) The ransomware utilizes cmd.exe to execute various Windows utilities to implement various other techniques.	**Impair Defenses: Disable or Modify Tools (T1562)** Threat actors use files such as: STONESTOP and POORTRY to load drivers for the purpose of disabling and deleting AV files.		**Inhibit System Recovery (T1490)** The ransomware deletes system shadow copies to inhibit system recovery.
			Service Stop (T1489) The Windows IIS service stop command is executed using iisreset.exe. Allows for encryption of web applications hosted on IIS servers as files linked to these applications are typically locked while IIS is running.

Active Website - Ransomhub

Onion Link
ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion

Contact Information - Ransomhub

Tox ID
4D598799696AD5399FABF7D40C4D1BE9F05D74CFB311047D7391AC0BF64BED47B56EEE66A528

Active Malicious URLs & Domains - Ransomhub / 2025

Download the Full List:
https://github.com/ThreatMon/ThreatMon-Reports-IOC

Malicous URLs - Ransomhub in 2025	Malicous Domains - Ransomhub in 2025
URL hxxp[:]//40031[.]co **URL** hxxp[:]//12301230[.]co **URL** hxxp[:]//samuelelena[.]co **URL** hxxp[:]//504e1c95.host[.]njalla{.]net	**Domain** 40031[.]co **Domain** 12301230[.]co **Domain** samuelelena[.]co **Domain** 504e1c95.host[.]njalla{.]net

Active Malicious IPs - Ransomhub / 2025

Download the Full List:
https://github.com/ThreatMon/ThreatMon-Reports-IOC

Malicous URLs - Ransomhub in 2025	
IPv4	34{.[132{.[102[.]6
IPv4	34[.]136[.]111[.]81
IPv4	80[.]78[.]28[.]149
IPv4	5[.]8[.]63[.]178

Active Malicious Hash List - Ransomhub / 2025

Download the Full List:
https://github.com/ThreatMon/ThreatMon-Reports-IOC

Malicous Sha256 - Ransomhub in 2025	
Sha256	ae35a3ee27cb81230a3f546253641bece5f4f6b72490e26fd3d019fbcb4b8ec1
Sha256	83654c500c68418142e43b31ebbec040d9d36cfbbe08c7b9b3dc90fabc14801a
Sha256	ae35a3ee27cb81230a3f546253641bece5f4f6b72490e26fd3d019fbcb4b8ec1
Sha256	f95e46257efbdc06b1e3297420257aca75bc8e9e82f4ffa97430370729be01f3
Sha256	ec77a2d8ba5409d9dbf4d36a4ce511687f66e3d5cc3db022614ba5fd1f3489ba
Sha256	0d886ec0eeb7e0197591bf69a6090ba7d9a26ae1b1bb6e571a445c520952a84e
Sha256	ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00
Sha256	36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e
Sha256	490a7515445c2ebf8dfbe3791383ac050cd7fca5dcf0c4539f276ad21aa1afe7
Sha256	595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb
Sha256	104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2
Sha256	6bf404c84f05a15c62b1108336ef1b56dd9b47283deeea6412074747bf6b12cb
Sha256	94f76f44c9e0e20c0041234164eff18658ef1b961e5d1d40e9f2a2e967a059f5
Sha256	80a1ce8db3c3c02080b844418f344e386f77622d02a10b5a5f23681580ce1437
Sha256	3e54451622d485b9e0f5d953109f537b4e1dd119446f32f8fb9c3aca4cc3ea47
Sha256	e654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23

Sha256	50d4a24a25be1e16b7805c6aff4436bae13623c5e26658871863875b2960771d
Sha256	2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad
Sha256	7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2
Sha256	7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a
Sha256	34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087
Sha256	342b7b89082431c1ba088315c5ee81e89a94e36663f2ab8cfc27e17f7853ca2b
Sha256	f6663774f9e46cb408c6865f725b27dcb314efbf5c9f3191484caeed32ead66f
Sha256	8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7

About Betruger Backdoor

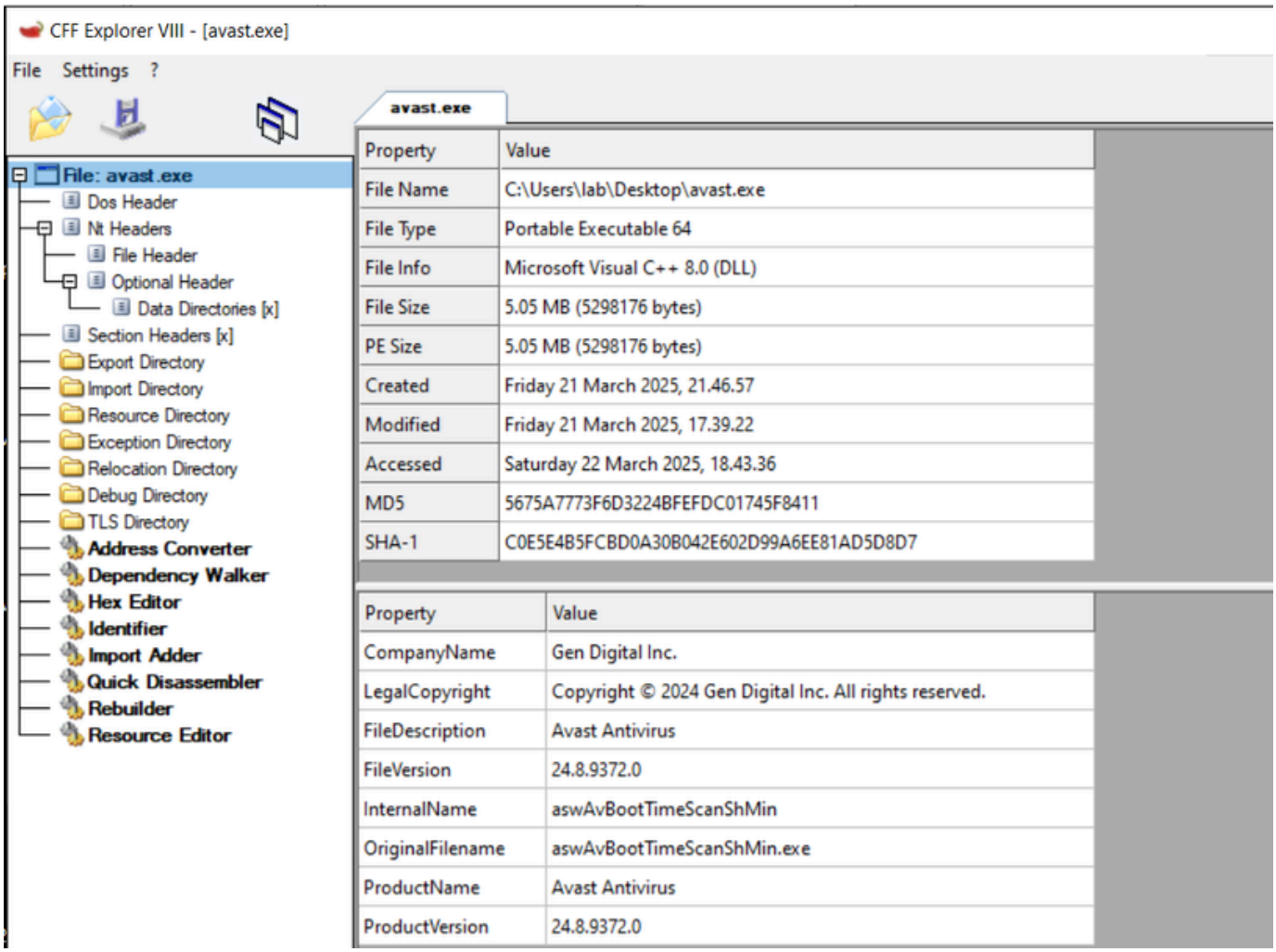
Threat Intelligence

"**Betruger**" is a multi-functional **backdoor** named by security researchers and identified as being used by a **RansomHub** member. It is primarily deployed before **ransomware infections**, facilitating ransomware attacks by establishing **initial access** and **gathering critical system information.** Written in **Rust**, it features **self-modifying code**, making detection and analysis more challenging. It targets **LSASS** for **credential theft**, includes **keylogging capabilities,** and performs network reconnaissance to map potential attack vectors. Betruger also communicates with its **command-and-control (C2)** server using encrypted channels, ensuring stealthy data exfiltration.

Additionally, the malware masquerades as **Avast Antivirus**, able to **manipulate the firewall rules** to maintain access, and leverages **privilege escalation** techniques to gain higher system control. By executing these actions, it enables ransomware deployment by preparing the environment, including generating RSA keys for encryption.

Technical Analysis of the malware is covered in the below title.

Technical Malware Analysis



SignerCertificate	Status	Path
	NotSigned	avast.exe

Background processes (38)						
Avast Antivirus	0%	9.8 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate	0%	2.3 MB	0 MB/s	0 Mbps	Very low	Very low
COM Surrogate	0%	2.9 MB	0 MB/s	0 Mbps	Very low	Very low

Basic Characteristics & Digital Sign & Background Process

The malicious software takes up around 5.05MB of space on the disk. Its original file name is **aswAvBootTimeScanShMin.exe**, and it imitates Avast Antivirus security program. Although it does not have a digital signature, an average computer user may perceive it as the original Avast Antivirus software. In particular, the file's assembly information closely replicates that of Avast Antivirus.

Research shows that the malware can change depending on the targeted company, business, or institution. Besides imitating Avast, its assembly properties may vary according to the developed attack scenario. It is also known to attempt attacks under the names **mailer.exe** and **turbomailer.exe**, in addition to Avast.

Network Activities

Zaman	Olay	Yerel Adres	Uzak Adres	Protokol	Durum
12:35:36	NEW_CONNECTION	192.168.38.159:1847	80.78.28.149:443	TCP	SYN_SENT
11:01:07	CLOSED_CONNECTION	192.168.38.156:65271	80.78.28.149:443	TCP	CLOSED
11:01:07	NEW_CONNECTION	192.168.38.156:65327	80.78.28.149:443	TCP	SYN_SENT
11:00:47	NEW_CONNECTION	192.168.38.156:65271	80.78.28.149:443	TCP	SYN_SENT
10:57:49	CLOSED_CONNECTION	192.168.38.156:64813	80.78.28.149:443	TCP	CLOSED
10:57:49	NEW_CONNECTION	192.168.38.156:64864	80.78.28.149:443	TCP	SYN_SENT
10:57:28	CLOSED_CONNECTION	192.168.38.156:64757	80.78.28.149:443	TCP	CLOSED
10:57:28	NEW_CONNECTION	192.168.38.156:64813	80.78.28.149:443	TCP	SYN_SENT
10:57:08	NEW_CONNECTION	192.168.38.156:64757	80.78.28.149:443	TCP	SYN_SENT
10:53:15	CLOSED_CONNECTION	192.168.38.156:64522	80.78.28.149:443	TCP	CLOSED
10:53:15	NEW_CONNECTION	192.168.38.156:64575	80.78.28.149:443	TCP	SYN_SENT

Image of Anka Malware Analysis Tool

After the malware is executed on the system, it establishes a connection with a remote server at IP address **80.78.28.149**, which has the hostname **504e1c95.host.njalla.net**.

Hostname:	***504e1c95.host.njalla.net***
IP Address:	***80.78.28.149***

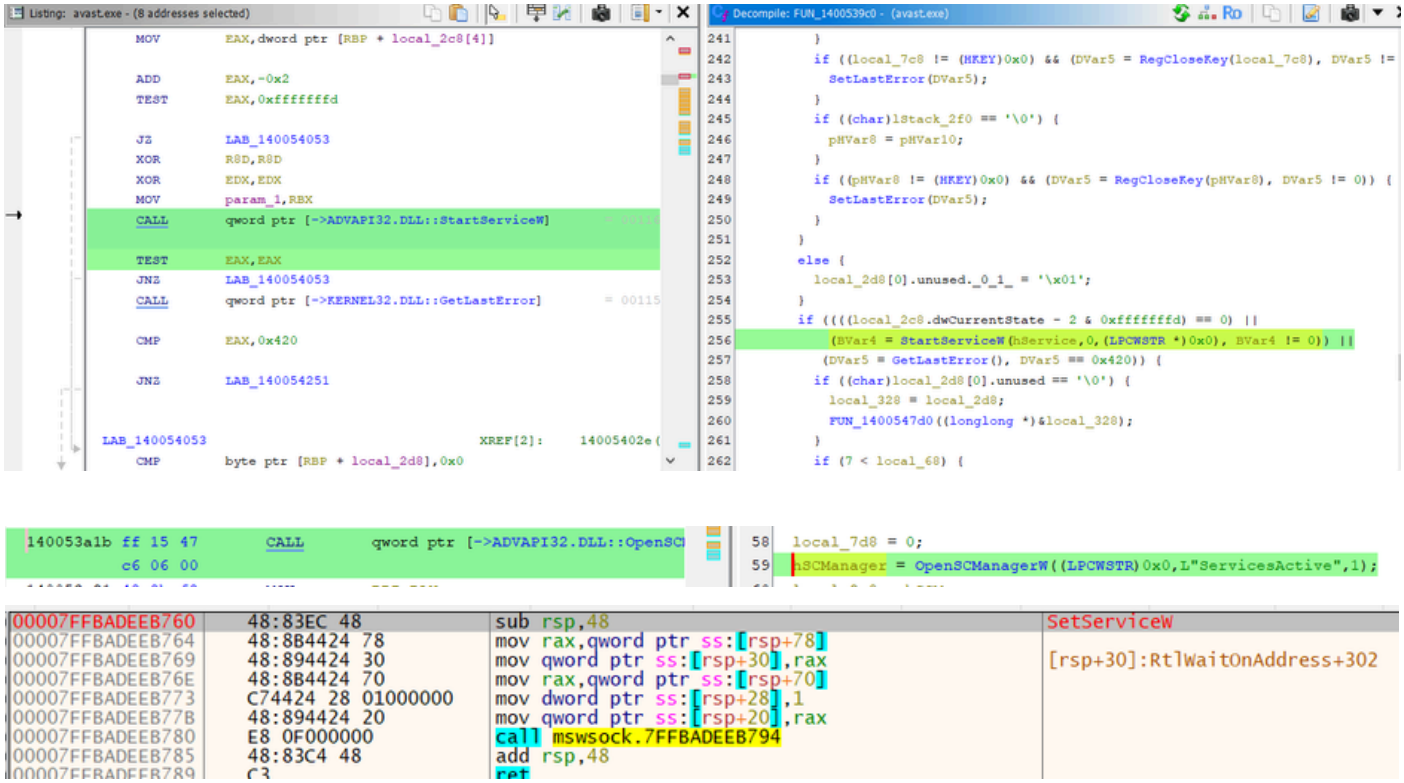


Image of Ghidra & X64dbg

Analysis confirms that the Betruger Backdoor can modify the structure of an existing service with service manipulation. While no changes were observed during execution in a virtual machine, **X64dbg and Ghidra** reveal its ability to alter service configurations via SetServiceW. This capability can be exploited for **privilege escalation, AV evasion, and ransomware deployment.**

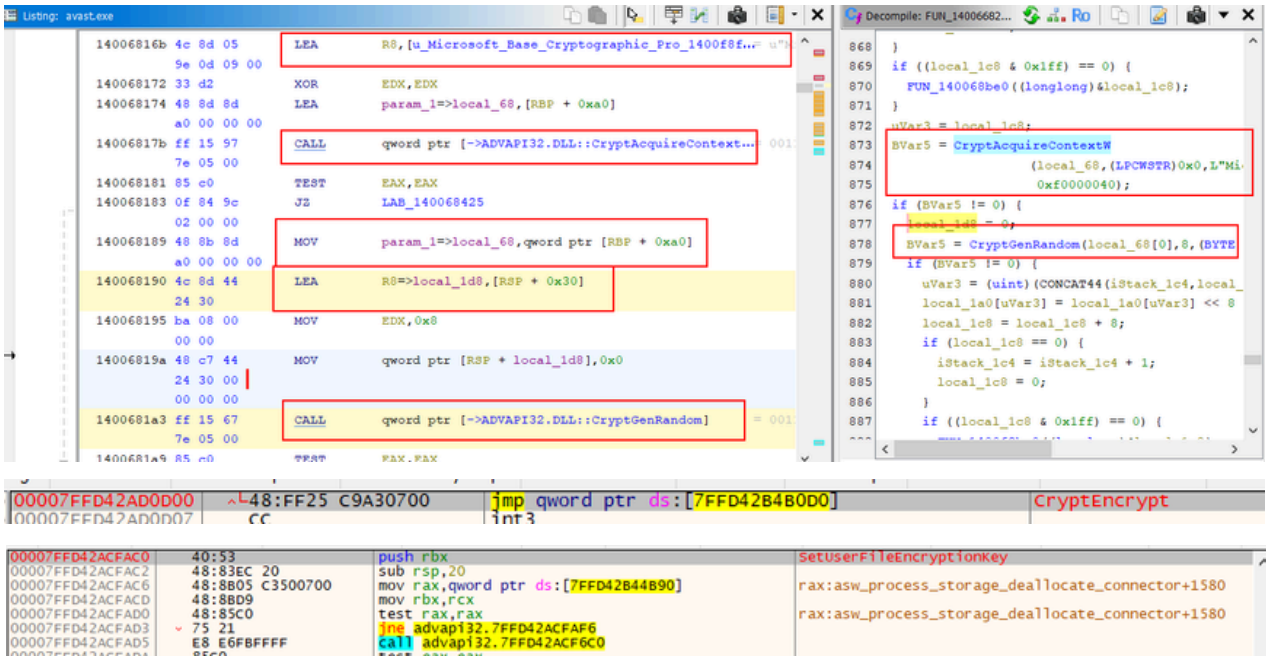
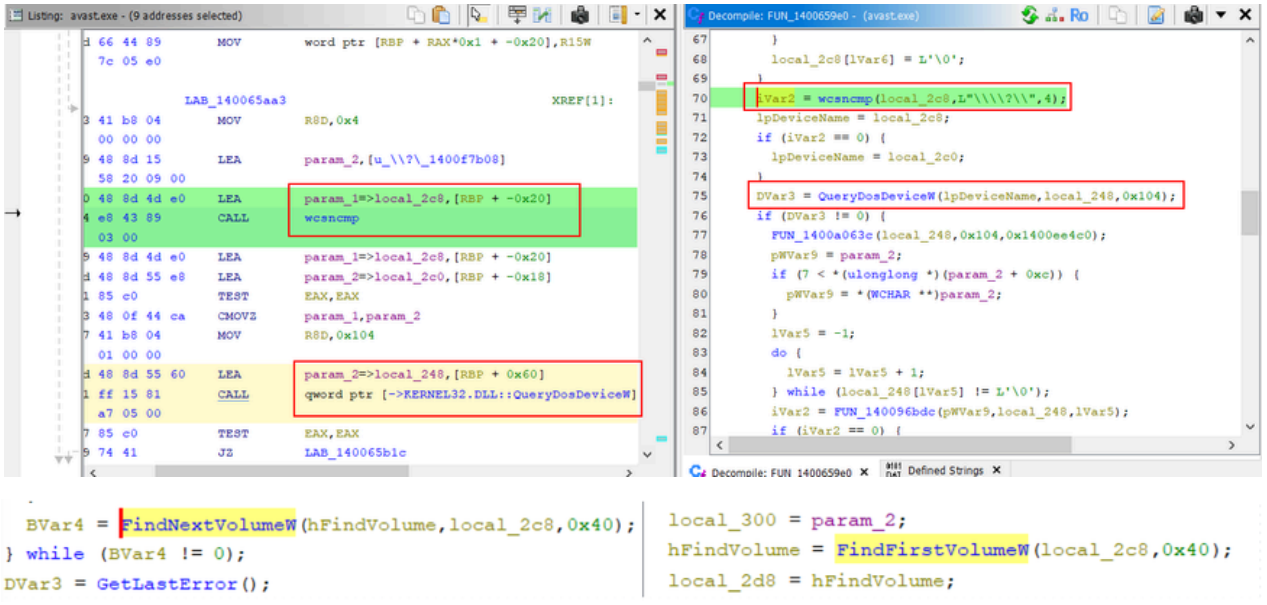


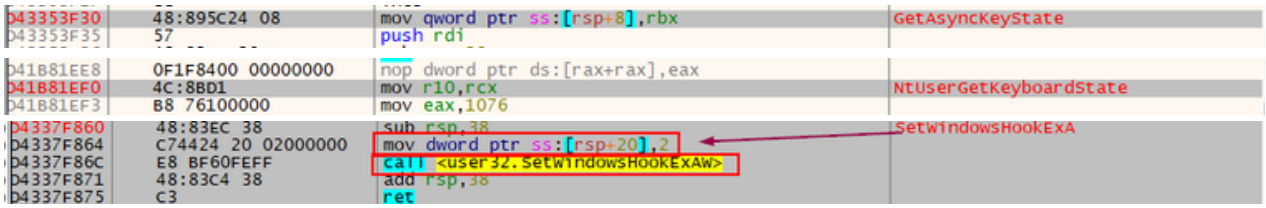
Image of Ghidra & x64dbg

During the static/dynamic analysis process, the backdoor malware exhibits behaviors that prepare for ransomware deployment. Specifically, tracking APIs such as **CryptAcquireContextW**, **CryptGenRandom**, **SetUserEncryptionKey**, and **CryptEncrypt** within the stub suggests that the backdoor may have the capability to generate an **RSA key for the ransomware**.



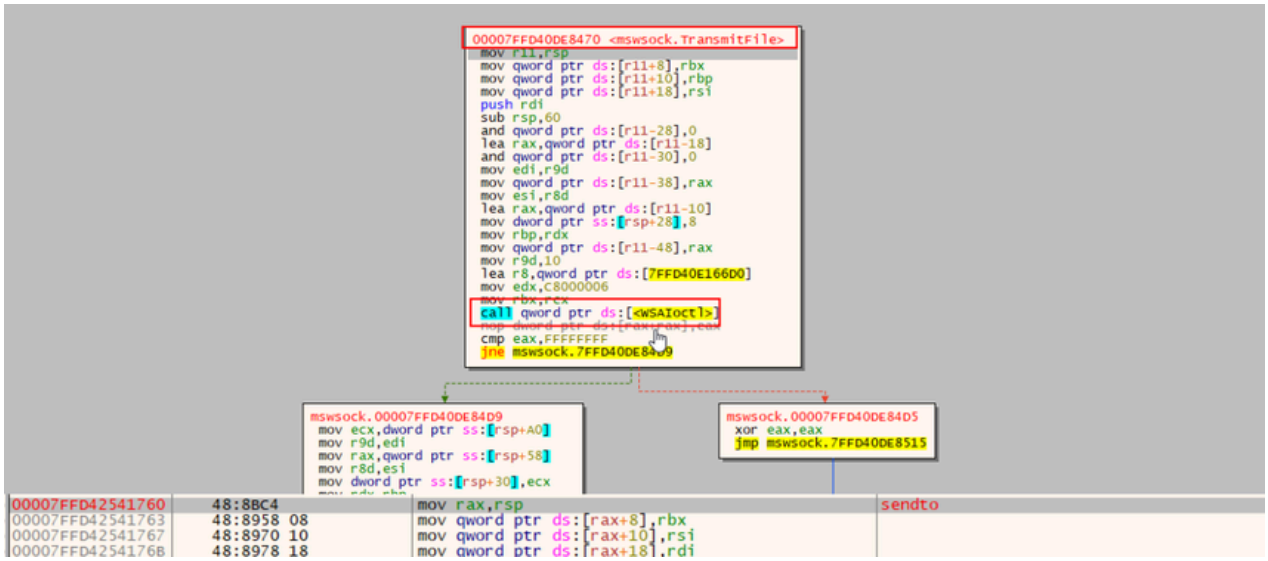
Images of Ghidra

Prior to the ransomware infection, another possible activity was detected. The Betruger backdoor malware was engaged in **disk discovery** and **disk access** activities on the compromised device



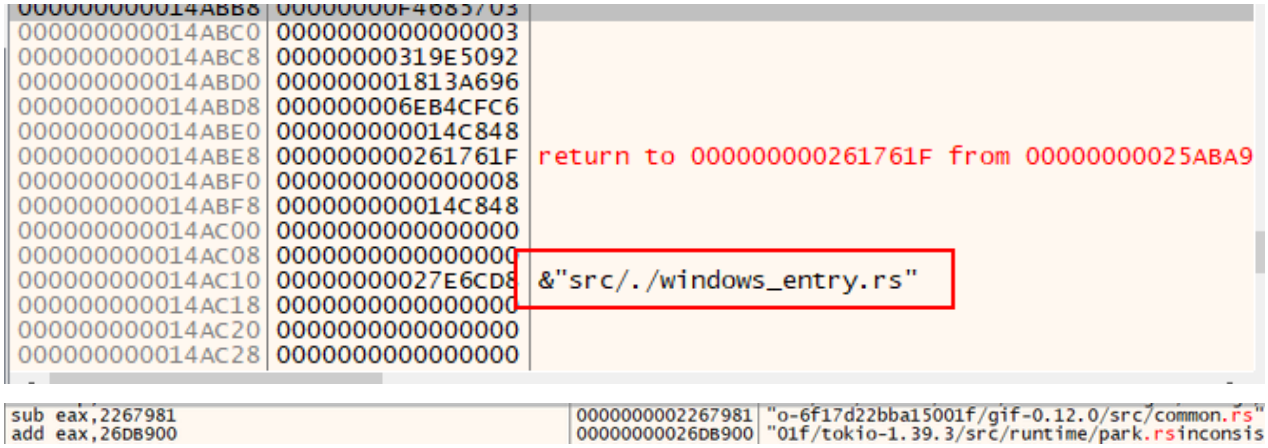
Images of X64dbg

A **keylogging** structure has been detected within the **backdoor**. After the malware is executed on the system, it calls APIs such as **GetAsyncKeyState, GetKeyState, GetKeyboardState, and SetWindowsHookEx**. Specifically, before calling SetWindowsHookEx, the idHook value being set to 2 indicates the **WH_KEYBOARD** hook type, which is a clear **keylogging behavior.**



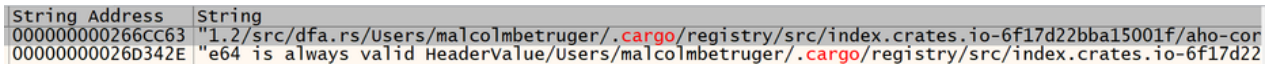
Images of X64dbg

It has been clearly analyzed that **file transfer operations** can take place within the **backdoor**. This situation, especially in ransomware attacks, not only involves the encryption of data but also creates the risk of **data leaks**. It is known that Ransomhub can **publicly share** the data if the ransom payment is refused.



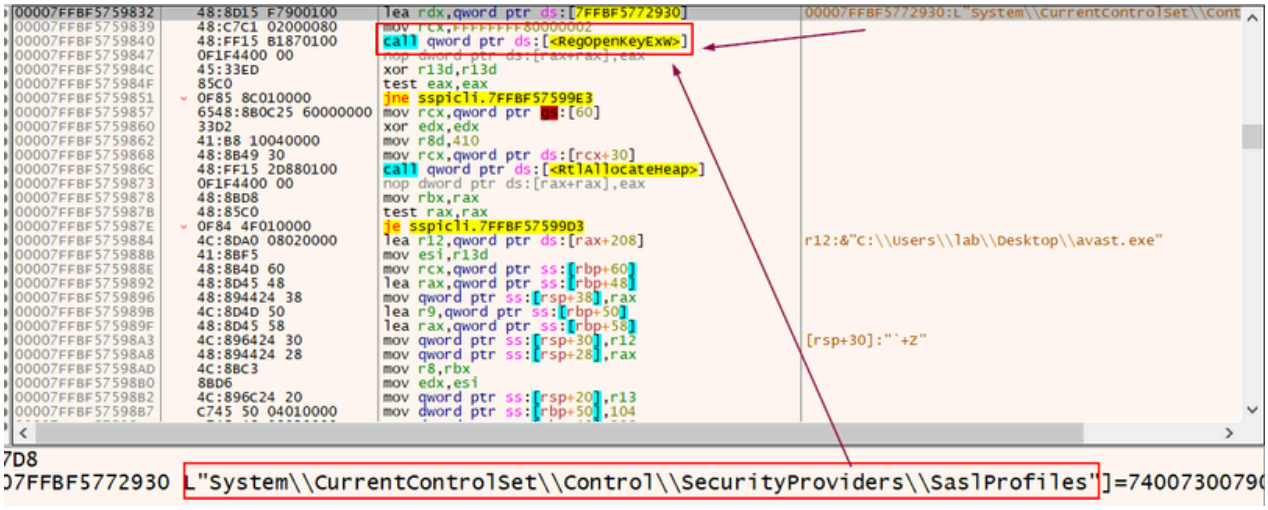
Images of X64dbg

During the dynamic analysis of the malware, a reference to **src/windows_entry.rs** was observed in memory. This file manages the malware's Windows-specific entry point and system integration, indicating that **Betruger Malware** was developed in the **Rust programming language.**



Images of X64dbg

Memory dump strings confirm the project was developed in Rust, indicated by .**rs** files and crates.io references. Debug symbols left during compilation suggest it was built on a computer with the username "**malcolmbetruger**." While this name belongs to a game character, it may also be (not definitively) a **Ransomhub** member's alias.

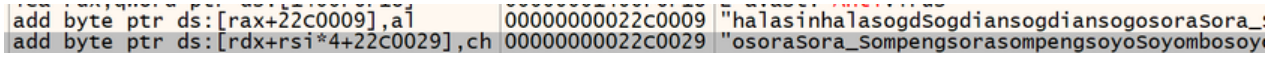


Images of X64dbg

SASL is a framework that forms the authentication infrastructure for many critical protocols **(LDAP, SMTP, IMAP)**, and the Betruger Backdoor directly targets this framework through the registry path;

System\CurrentControlSet\Control\SecurityProviders\saslProfiles.

It accesses the authentication configuration using the **RegOpenKeyExW** API. This indicates that the Betruger Backdoor exhibits **lateral movement** capabilities.

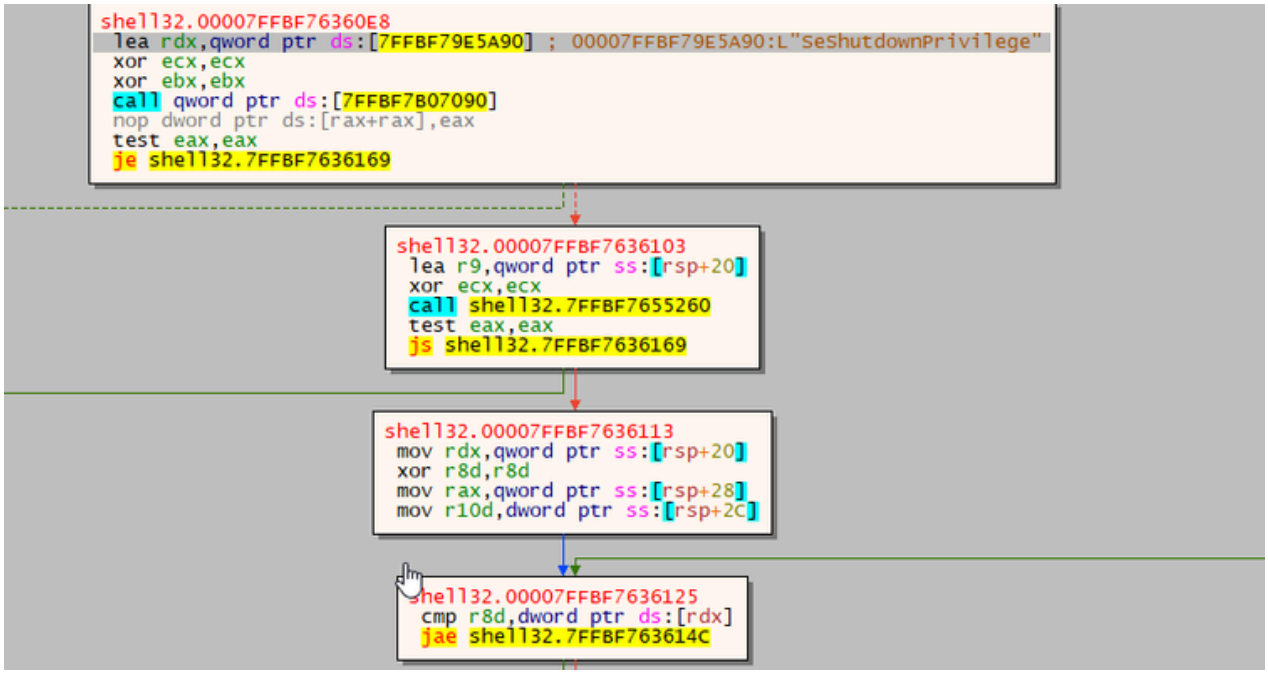


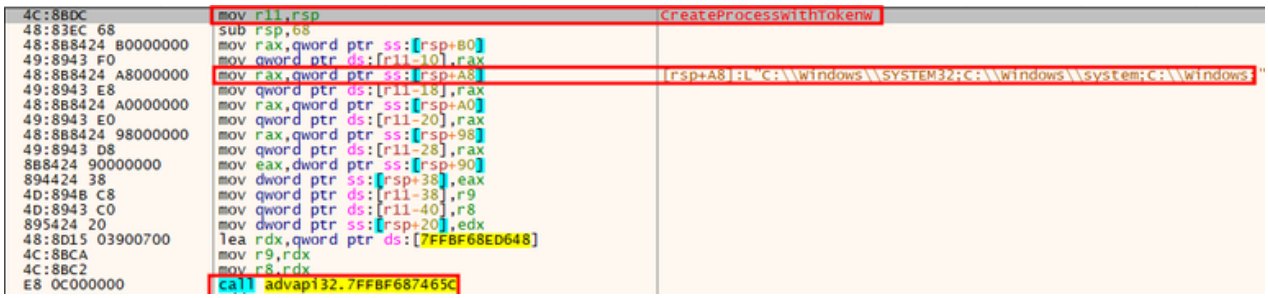
Images of X64dbg

It has been determined that the **self-modifying code** technique is used for **anti-analysis** functionality. This technique is utilized by the backdoor using **memory manipulation** on addresses **0x22C0009** and **0x22C0029**, modifying string data during runtime to generate dynamic payloads and implement encrypted command and control communication while evading detection.

Images of X64dbg

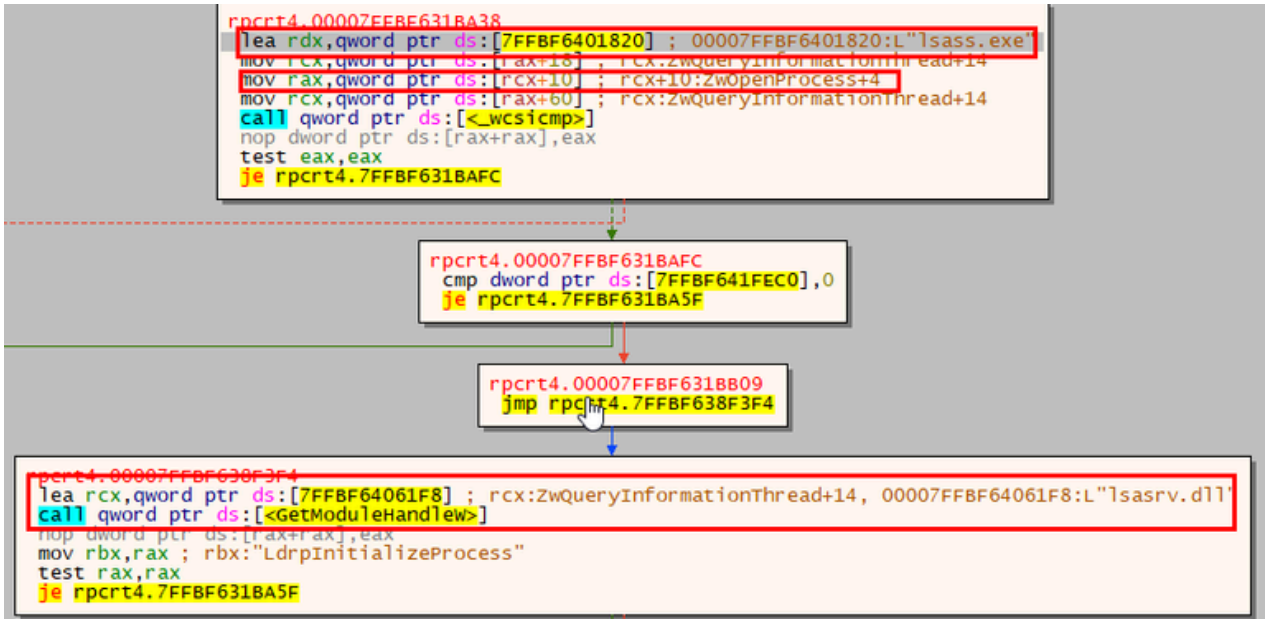
It has been determined that the **WSS** protocol is used for **Server-Client** communication. WSS is a real-time, bidirectional communication protocol and is utilized by Betruger in an encrypted manner using **TLS/SSL** for purposes such as file transfers, keylogger data transmission, and command execution.





Images of X64dbg

With the **SeShutdownPrivilege** structure, **shutdown** and **restart** privileges are obtained. Additionally, the usage of the **CreateProcessWithTokenW** API from **advapi32.dll** and attempts to access the **System32** directory are observed, which are used for **privilege escalation.**

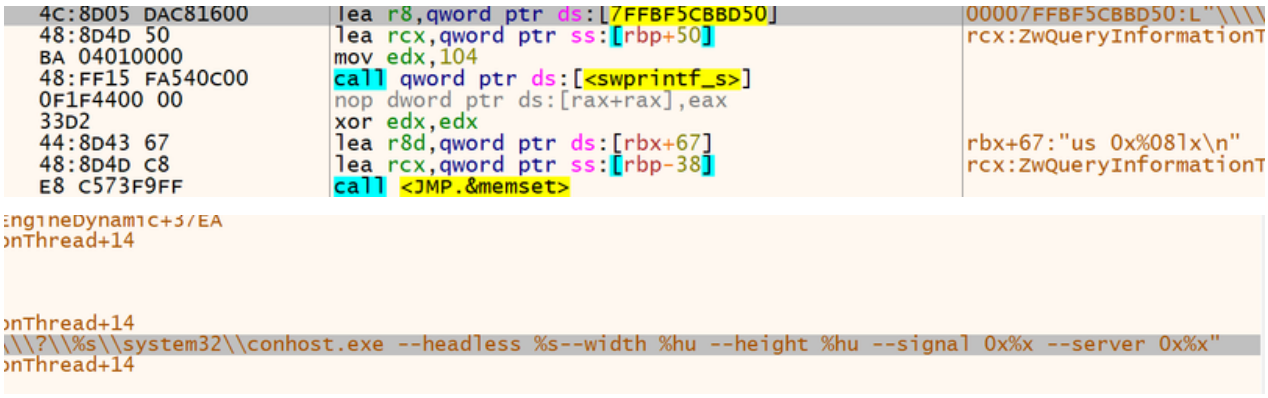


Images of X64dbg

The **Betruger Backdoor** targets the **LSASS** process. It uses **ZwOpenProcess** to access **LSASS.exe**, and loads **lsasrv.dll** via **GetModuleHandleW**.

lsasrv.dll is a key LSASS component that manages authentication and security policies, and provides access to credential data.

This shows that the malware attempts **credential dumping.**

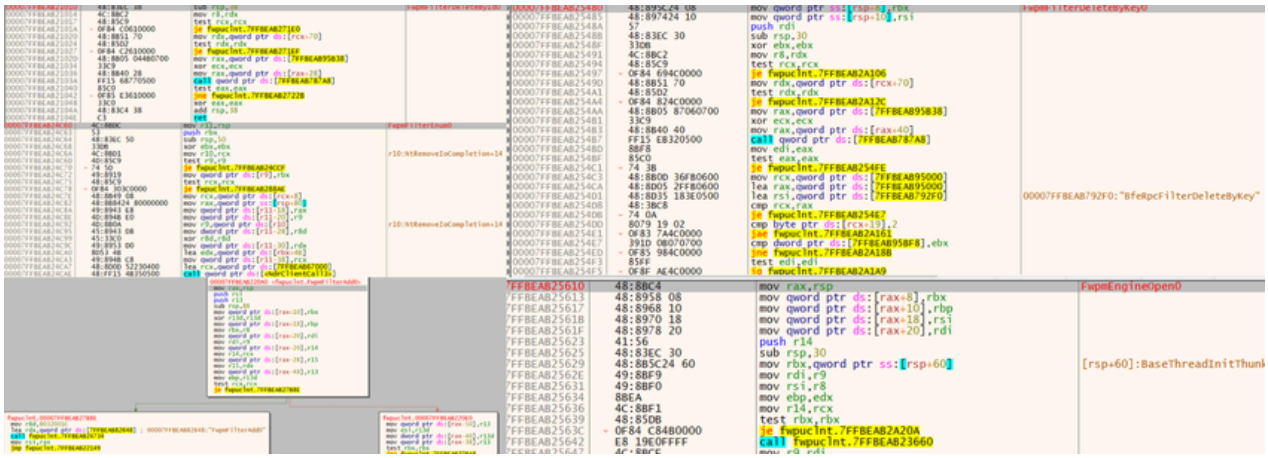


Images of X64dbg

Arguments are being passed to conhost.exe as follows:

--headless %s --width %hu --height %hu --signal 0x%x --server 0x%x

Here, a console window appears to be used for executing a command, but with the --**headless** option, it runs **without being visible** to the user.
One of the most **critical** aspects of this command structure is the **--signal and --server** arguments. This structure allows for command exchange with a **remote server**, and in the case of malicious software, a **reverse shell** mechanism has been observed.



Images Firewall Operations

During the analysis process, some firewall operations associated with Windows Filtering Platform (WFP) were found. It was observed that the malware can access Windows Firewall structures and perform operations such as **adding rules, listing existing rules and deleting rules.**

Images Multiple Discovery & Reconnaissance Operations

Also, the following findings related to discovery and reconnaissance activities have been identified:

● Obtaining hardware information from the infected device
● Retrieving extended user information
● Gathering information about system architecture and processor type
● Obtaining operating system details
● Retrieving the machine name
● Obtaining the IP address assigned to the machine
● Resolving network addresses
● Obtaining ARP table information

● Accessing the service control manager
● Listing active TCP/UDP connections
● Enumerating account privileges of active users
● Gathering information about active user accounts
● Retrieving the system time of the infected device
● Obtaining detailed information about running processes
● Determining the locations of system folders

Categorization & IOC List

Threat Group	Identified Threat Categories
Ransomhub	Backdoor Trojan
	Keylogger

You can download the IOC List from ThreatMon Github

IOC List	
DOMAIN	504e1c95[.]host[.]njalla[.]net
IPv4	80[.]78[.]28[.]149
SHA256	ae7c31d4547dd293ba3fd3982b715c65d731ee07a9c1cc402234d8705c01dfca
SHA256	b058c128c801e2ee03874e183239ff369c599f3a2324905ff73f99d16d3b1a16

Mitre & Attack Table

Tactics	ID	Name	Description
Initial Access	T5566	Phishing	Betruger backdoor can be delivered via a phishing attack
Privilege Escalation	T1134	Access Token Manipulation	Uses CreateProcessWithTokenW API from advapi32.dll for privilege escalation
	T1134.002	Access Token Manipulation: Create Process with Token	Evidence of the SeShutdownPrivilege structure used for token manipulation
	T1543.003	Create or Modify System Process: Windows Service	Able to modify and manipulate a windows service.
Defense Evasion	T1027	Obfuscated Files or Information	Malicious code is encrypted to evade detection.
Credential Access	T1003.001	OS Credential Dumping: LSASS Memory	Betruger Backdoor targets the LSASS process" and "loads lsasrv.dll via GetModuleHandleW
Lateral Movement	T1021	Remote Services	Possible to spread within the network via remote connections.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	Communicates with C2 server using WSS protocol with TLS/SSL encryption
	T1573.002	Encrypted Channel: Asymmetric Cryptography	Uses encrypted communication channels for stealthy data exfiltration
	T1105	Ingress Tool Transfer	Capabilities for downloading additional payloads

Impact	T1041	Data Exfiltration	Sensitive data is stolen from the target system.
Collection	T1056.001	Input Capture: Keylogging	Contains keylogging structure using SetWindowsHookEx with WH_KEYBOARD hook type
Discovery	T1082	System Information Discovery	Obtaining hardware information, system architecture, processor type, and OS details
	T1083	File and Directory Discovery	Determining locations of system folders and disk discovery
	T1124	System Time Discovery	Retrieving system time of the infected device
	T1016	System Network Configuration Discovery	Retrieving IP addresses, MAC addresses, ARP tables, and routing tables
	T1033	System Owner/User Discovery	Gathering information about user accounts and privileges
	T1057	Process Discovery	Obtaining detailed information about running processes
	T1012	Query Registry	Accesses authentication configuration using RegOpenKeyExW API
	T1018	Remote System Discovery	Network discovery capabilities to map potential attack vectors
Exfiltration	T1041	Exfiltration Over C2 Channel	Able to send stolen data to its c2
Impact	T1486	Data Encrypted for Impact	Prepares environment for ransomware by generating RSA keys for encryption

Yara Rule

You can download the yara rule from [ThreatMon Github]

```
rule Betruger_Backdoor_YaraRule {
        meta:
    description = "Enhanced YARA rule for detecting Betruger Backdoor
used by Ransomhub"
    author = "Aziz Kaplan"
    email = "aziz.kaplan@threatmonit.io"
    reference = "https://threatmonit.io/"
    threat_level = 10
    severity = "critical"
    family = "Ransomhub.Betruger"
    tlp = "GREEN"
    mitre_att = "T1486, T1490, T1083, T1057, T1082"

        strings:
    $str1 = "Avast Antivirus" wide ascii
    $str2 = "avast-av" wide ascii
    $str3 = "IDI_ASWAVBOOTTIMESCANSHMIN" wide ascii
    $str4 = "AV Boot-time Scanner" wide ascii

    $str5 = "Windows Registry Editor" wide ascii
    $str6 = "lifetime_creation_monitor_holder" wide ascii
    $str7 = "/runassvc /winre" wide ascii nocase

    $op1 = {4? 8d 4c ?4 40 e8 26 18 00 00}
    $op2 = {80 7d c8 00 75 09 4? 8b cf 4? 89 4d c0}
    $op3 = {ff 15 7f b1 0b 00 85 c0 74 08 8b c8 ff 15 db b5 0b 00}
    $op4 = {ff 15 af 54 0b 00 85 c0 74 2d 4? 8d 4c ?4 60}

    $op5 = {4? 8d 84 ?4 c8 00 00 00 4? 89 44 ?4 28}
    $op6 = {ff 15 6d 2f 06 00 85 c0 0f 84 dd 00 00 00}
```

```
$op7 = {4? 8d 4d 70 4? c7 45 70 00 00 00 00 ff 15 3c 99 05 00}
   $op8 = {4? 8d 55 78 ?? ?? ?? ?? ?? ff 15 26 90 05 00}

   $op9 = {4? 8d 44 ?4 30 ba 08 00 00 00}
   $op10 = {4? c7 44 ?4 30 00 00 00 00 ff 15 67 7e 05 00}

   $op11 = {ba ff ff ff ff 4? 8b ca 4? 8b c2 4? 8b cf ff 15 cf b9 06 00}
   $op12 = {ff 15 67 bb 06 00 4? 8b d8 4? 89 45 0f}

   $op13 = {ff 15 74 5a 05 00 4? 8d 0d 0d ee 08 00 4? 89 4c ?4 20}

   $op14 = {4? 8d 57 40 4? 8d 4d e0 ff 15 6b a8 05 00}
   $op15 = {4? 8d 15 58 20 09 00 4? 8d 4d e0 e8 43 89 03 00}

   $op16 = {4? 8b d0 4? 8b ce ff 15 4d 17 08 00}

       condition:
   uint16(0) == 0x5A4D and
   filesize > 5MB and filesize < 10MB and
   (
        (all of ($op*) and all of ($str*))
        or
        (all of ($op*) and 4 of ($str*))
        or
        all of ($op*)
   )
}
```

Sigma Rules

You can download the Sigma Rules from [ThreatMon Github]

```
title: Trojanized Avast Binary C2 Communication
 id: f8a12b2e-d45f-4a84-9b4b-1e0e3e8f5a7d
 status: test
 description: Detects suspicious C2 communication from trojanized avast.exe binary to
malicious servers.
 author: Aziz Kaplan <aziz.kaplan@threatmonit.io>
 date: 2025-03-23
 references:
 - ThreatMon Malware R&D
 logsource:
 product: windows
 category: network_connection
 detection:
 selection:
      Image|endswith: '\avast.exe'
      DestinationHostname|contains: 'njalla.net'
      Initiated: 'true'
 condition: selection
 falsepositives:
 - Legitimate Avast security software updates
 - Downloading virus definitions
 level: high

title: Fake Avast Application Detected
 id: 762f3a9c-5d2b-42e3-bc4f-16c7f8d94856
 status: test
 description: Detects execution of a malicious avast.exe application that mimics the
legitimate Avast security software.
 author: Aziz Kaplan <aziz.kaplan@threatmonit.io>
 date: 2025-03-23
 references:
 - ThreatMon Malware R&D
 logsource:
 product: windows
 category: process_creation
 detection:
```

```
selection:
      Image|endswith: '\avast.exe'
      CurrentDirectory|contains:
    - '\Desktop\'
    - '\Downloads\'
     - '\Documents\'
 filter:
      IntegrityLevel: 'System'
      ParentImage|endswith:
     - '\Program Files\Avast Software\Avast\AvastSvc.exe'
     - '\Program Files (x86)\Avast Software\Avast\AvastSvc.exe'
 condition: selection and not filter
 falsepositives:
 - User executing normal Avast installer from desktop

level: high
title: Suspicious Avast Repetitive C2 Connection Attempts
 id: e02a4c10-7193-4a79-af9b-75d580b1d68c
 status: test
 description: Detects fake avast.exe making repetitive connection attempts to the same
domain within short time intervals
 author: Aziz Kaplan <aziz.kaplan@threatmonit.io>
 date: 2025-03-23
 references:
 - ThreatMon Malware R&D
 logsource:
 product: windows
 category: network_connection
 detection:
 selection:
      Image|endswith: '\avast.exe'
      DestinationHostname|contains:
     - 'njalla.net'
      Initiated: 'true'
 timeframe: 5m
 condition: selection | count() > 5
falsepositives:
 - Heavy update activity
 level: high
```

```
title: Suspicious Avast Application Hosts File Access
 id: d16b0f5e-6c2f-4d3f-ab43-76cfc7510e2c
 status: test
 description: Detects malicious avast.exe application reading Windows hosts file
 author: Aziz Kaplan <aziz.kaplan@threatmonit.io>
 date: 2025-03-23
 references:
 - ThreatMon Malware R&D
 logsource:
 product: windows
 category: file_event
 detection:
 selection:
      Image|endswith: '\avast.exe'
      TargetFilename: 'C:\Windows\System32\drivers\etc\hosts'
      Access: 'ReadData'
 filter:
      CurrentDirectory|contains:
     - '\Program Files\Avast Software\Avast\'
     - '\Program Files (x86)\Avast Software\Avast\'
 condition: selection and not filter
 falsepositives:
 - Legitimate Avast software reading network configuration
 level: medium
```

Windows Defender Custom Detection Rule

You can download the detection rule from [ThreatMon Github]

```
<Detections>
 <Detection>
      <Name>Betruger Backdoor Detection</Name>
      <Description>Detects Betruger backdoor malware associated with RansomHub
group</Description>
      <Severity>High</Severity>
      <FileSha256
Detect="Equals">ae7c31d4547dd293ba3fd3982b715c65d731ee07a9c1cc402234d8705c01dfca</File
Sha256>
      <FileSha256
Detect="Equals">b058c128c801e2ee03874e183239ff369c599f3a2324905ff73f99d16d3b1a16</File
Sha256>
      <FileName Detect="Contains">aswAvBootTimeScanShMin.exe</FileName>
      <FileName Detect="Contains">mailer.exe</FileName>
      <FileName Detect="Contains">turbomailer.exe</FileName>
      <NetworkConnection>
     <RemoteIP Detect="Equals">80.78.28.149</RemoteIP>
     <RemoteDomain Detect="Contains">504e1c95.host.njalla.net</RemoteDomain>
      </NetworkConnection>
 </Detection>
</Detections>
```

Mitigations - General

●Implement a rigorous vulnerability management program focusing on internet-facing systems

- Prioritize patching of critical vulnerabilities mentioned in the report (CVE-2023-46604, CVE-2023-22515, CVE-2023-3519, etc.)
- Block known malicious IPs and domains provided within the report
- Implement network segmentation to limit lateral movement
- Maintain offline backups that are disconnected from the network
- Implement the 3-2-1 backup strategy (3 copies, 2 different media, 1 offsite)
- Implement email scanning for malicious attachments and links
- Train users to identify suspicious emails, especially those with attachments
- Apply the principle of least privilege for all accounts
- Implement multi-factor authentication across all systems
- Deploy EDR solutions that can detect the IOCs mentioned in the report
- Implement the provided Yara rules and Sigma rules for detection
- Add the Windows Defender Custom Detection Rule to security solutions
- Block execution of binaries from unusual locations (Desktop, Downloads, etc.)
- Develop and test an incident response plan specific to ransomware attacks
- Establish an offline communication channel for emergencies
- Disable unnecessary remote management tools (especially those mentioned in the report: AnyDesk, Atera, etc.)
- Implement strict monitoring of remote access tools
- Implement application whitelisting to prevent unauthorized executables
- Verify digital signatures on software installations
- Be particularly vigilant with software that masquerades as legitimate security tools like Avast
- Set up alerts for suspicious command-line parameters (especially those containing "--headless" flags)

Monitor for suspicious registry modifications, especially to authentication providers

Mitigations - CVE

Apache ActiveMQ (CVE-2023-46604)

- Upgrade to Apache ActiveMQ versions 5.15.16, 5.16.7, 5.17.6, or 5.18.3 (or newer)
- If immediate patching isn't possible, implement network filtering to block remote access to the ActiveMQ admin console
- Monitor for unusual connection attempts to ActiveMQ instances
- Restrict access using firewall rules to allow connections only from trusted IP addresses

Atlassian Confluence (CVE-2023-22515)

- Immediately update to fixed versions (7.19.16, 8.3.3, 8.4.3, 8.5.2, or later)
- Implement web application firewalls to filter malicious requests
- Monitor authentication logs for unexpected admin account creation
- Consider temporarily disabling public access until patching is complete

Citrix NetScaler ADC & Gateway (CVE-2023-3519)

- Update to recommended firmware versions that fix this vulnerability
- Implement IP restrictions for management interfaces
- Deploy proper TLS inspection for encrypted traffic
- Consider implementing additional authentication mechanisms

Fortinet FortiOS SSL-VPN & FortiProxy (CVE-2023-27997)

- Update to the latest FortiOS versions with the security patches
- Enforce multi-factor authentication for VPN access
- Implement geolocation-based access restrictions
- Monitor for unusual VPN connection patterns

Fortinet FortiClientEMS (CVE-2023-48788)

- Apply the latest security patches from Fortinet
- Segment networks where FortiClient management servers are located
- Restrict administrative access to these systems

F5 BIG-IP (CVE-2023-46747)

- Apply the hotfixes provided by F5
- Implement control plane access restrictions
- Consider implementing proper management network isolation
- Use the latest BIG-IP iApp templates with security settings enabled

Windows NetLogon (CVE-2020-1472, aka Zerologon)

- Apply Microsoft security updates
- Enable enforcement mode for secure RPC
- Monitor for unauthorized attempts to reset machine account passwords
- Implement Windows Event log monitoring to detect exploitation attempts

Windows BITS (CVE-2020-0787)

- Apply appropriate Microsoft security patches
- Consider disabling the BITS service if not essential
- Implement application control to prevent unauthorized use of BITSAdmin
- Monitor for suspicious BITS transfer jobs using event logs

Windows SMBv1 (CVE-2017-0144, aka EternalBlue)

- Disable SMBv1 completely across the enterprise
- Block SMB ports (TCP 445) at network boundaries
- Implement strict network segmentation for legacy systems that require SMBv1
- Use Microsoft's SMB security features like SMB signing and encryption

Additional technical mitigations:

- Implement specific detection and alerting for lateral movement attempts using these vulnerabilities
- Deploy network traffic analysis to detect exploitation attempts
- Consider micro-segmentation to isolate critical assets that might be targeted via these vulnerabilities
- Conduct regular vulnerability scanning focused on these specific CVEs
- Develop incident response playbooks specific to exploitation of these vulnerabilities

ThreatMon
Under Cyber Wings

More Information About ThreatMon

One Platform for all intelligence needs.

ThreatMon End-to-end intelligence is a cutting-edge, cloud-based SaaS platform that continuously monitors the dark and surface web, providing early warnings and actionable insights into emerging threats.

We are a SaaS platform designed to help businesses proactively detect and address threats before a cyber attack occurs. Unlike traditional cyber threat intelligence, we provide comprehensive and holistic cyber intelligence.

- *Attack Surface Intelligence*
- *Fraud Intelligence*
- *Dark and Surface Web Intelligence*
- *Threat Intelligence*

Contact Us:

Email Address
team@threatmonit.io

https://x.com/MonThreat

https://www.linkedin.com/company/threatmon