Rooma Sec

[APT32]

ATTACK ANALYSIS REPORT

Rooma X-WING NG-EDR **AI Generation**

Number of tokens consume **10200**

Generation Duration **3'02"**

Generated Time: Feb.9, 2024; 17:36

Classification: For Internal Use Only Contact us： support@xrooma.com

INTRUSION SUMMARY

ATTACK OVERVIEW

APT32

Origin

Vietnam

Target Country

4 (China, Cambodia, Laos, Philippines)

Target Industry

5 (Government, Research Institutions, Maritime Agencies, Marine Construction, Shipping Companies)

Severity

High

Affected Hosts

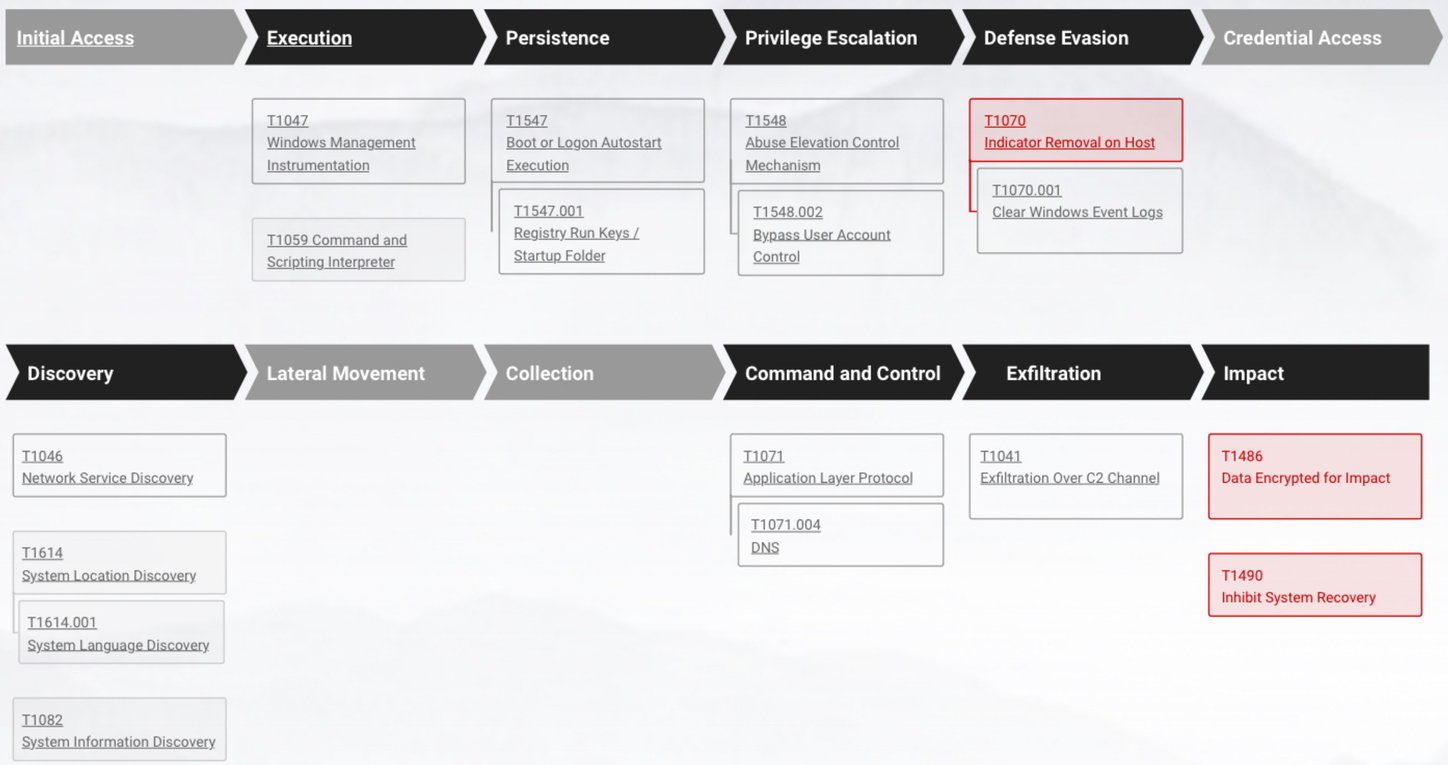
1 important host

Detection Time

Feb. 8, 2024, 18:18:50

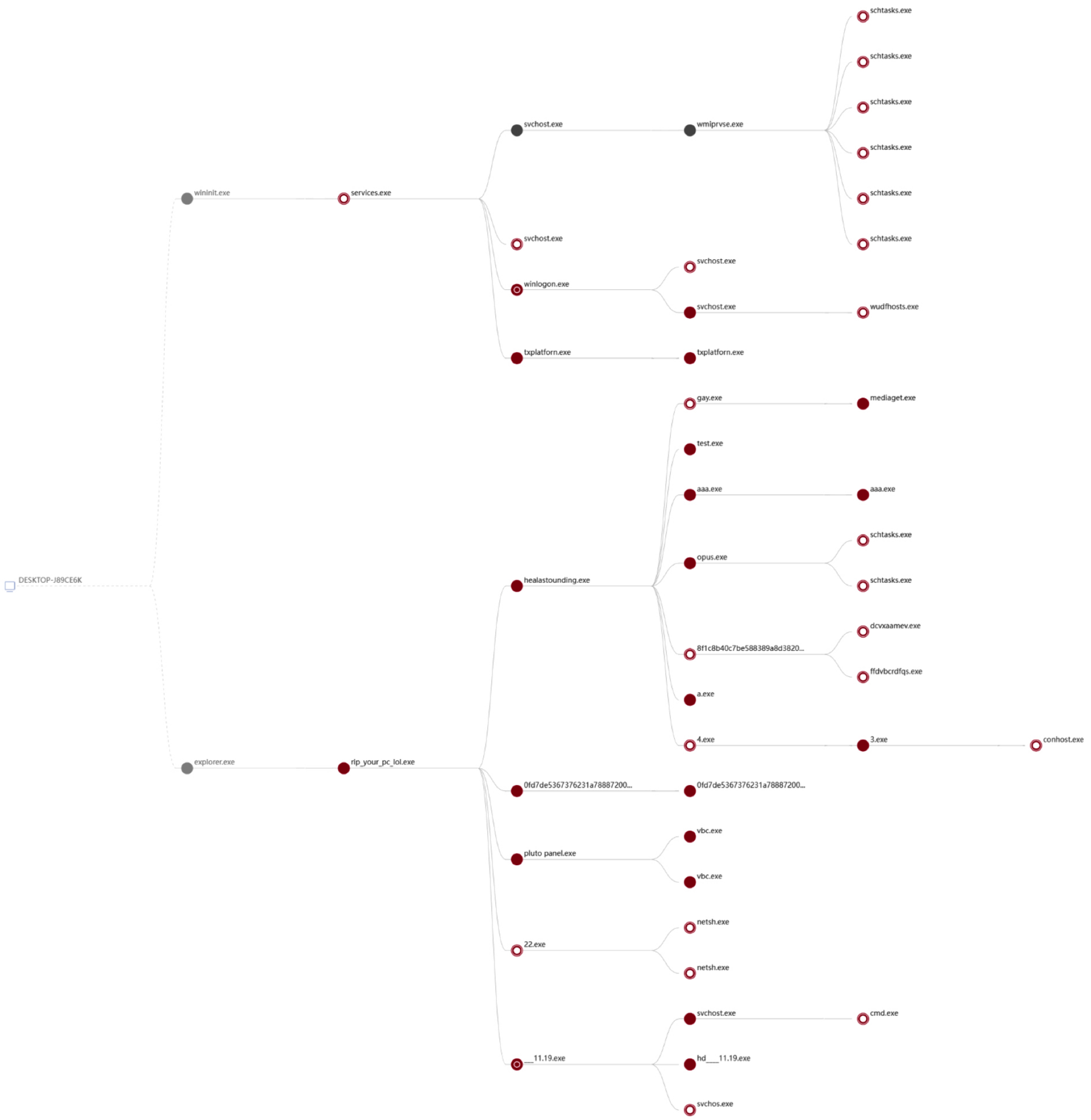
Attack Review Overview

The attackers employed various techniques and tactics mentioned in the ATT&CK security framework to attempt to bypass security measures, escalate privileges, implant backdoor programs, and execute malicious software opportunistically, aiming to ransom users through file encryption.



ATTACK GRAPH

Rooma X-WING reconstructs the attack process and generates the following attack graph.



INTRUSION ANALYSIS

WAS I ATTACKED?

Attack Type

Malware propagation

Severity

High

Detected Time

Feb.8, 2024; 18:18:50

Security GPT Conclusion

The malware sample employed various tactics and techniques to attempt to bypass security measures, elevate its privileges, and implant backdoors. Specific analysis is as follows:

1. utilized Windows Management Instrumentation (WMI) to execute programs, potentially for remote control or information gathering.
2. attempted to bypass User Account Control (UAC) to execute malicious code without the user's knowledge.
3. injected malicious code into normal processes via process injection technique to evade detection by security software.
4. hijacked execution flow and modified process entry points to control the program's execution flow.
5. utilized memory code loading technique to directly load malicious code into memory, avoiding leaving file traces.
6. disguised itself as legitimate program to deceive users and defense systems.
7. may set itself to start up through registry settings for persistence.
8. attempted to disable or modify the system firewall to degrade system security.
9. hid itself and related files and directories to evade detection.
10. may steal various user credentials, including browser credentials, passwords, etc.
11. may capture sensitive information using screen capture technique.
12. may utilize Office application add-ins for autostart.
13. may realize scheduled execution via task scheduler.
14. may possess anti-virtual machine function to counter against virtualization security solutions
15. may have anti-debugger function to counter against debugger analysis.

In summary, the sample exhibited a variety of malicious behaviors and may be a sophisticated backdoor program with the intent on information theft, remote control, and persistence, etc. It is recommended to take appropriate security measures for prevention and removal.

SCOPE OF IMPACT

WHICH HOSTS WERE AFFECTED?

1 important host(s)

DESKTOP-A4PH56B

Host ID
bd1af8f153e8483aa952d2f2ab15bea3

Status	Importance
Online	Important host

Last Detected Time	First Detected Time
Feb.8, 2024; 18:18.50	Feb.8, 2024; 18:18:50

OS Version	Type	External IP
Windows 10	Workstation	202.103.1.4

Connection IP	Sensor version	Uesr
192.168.100.1	5.0.0.1181	UMFD-3

Last login Time	Comments
Feb. 8, 2024, 18:18:50	123

ATTACKER PROFILE

WHO ATTACKED ME?

APT32

OCEANLOTUS, COBALT KITTY, APT-C-00,
SEALOTUS, CANVAS CYCLONE, BISMUTH

Status
Active

Origin
Vietnam

Target Country
4 (China, Cambodia, Laos, Philippines)

Target Industry
5 (Government, Scientific Research Institutes, Maritime Agencies, Marine Construction, Shipping Companies)

Last activity date
Sep. 2023

First activity date
Sep. 2023

Published date
2021

Last modified date
Jun. 2023

Attack type
Crime

Motivation
Criminal

APT Group Description

Since April 2012, this group has launched organized, planned, and targeted long-term attacks on the Chinese government, scientific research institutes, maritime agencies, marine construction, shipping companies and other relevant important areas. In addition to attacking targets in China, OceanLotus also carried out attacks on targets in Southeast Asian countries such as Cambodia, the Philippines, and Vietnam. The group has a functionally complete set of malicious code and combines it with commercial tools to carry out attacks. After February 2014, OceanLotus entered an active period of attack, and launched its largest round of spear-phishing attacks in May 2014, and a large number of victims were infected with specially crafted trojans by opening poisonous email attachments. To this day, the group’s attacks in China continue.

IOC

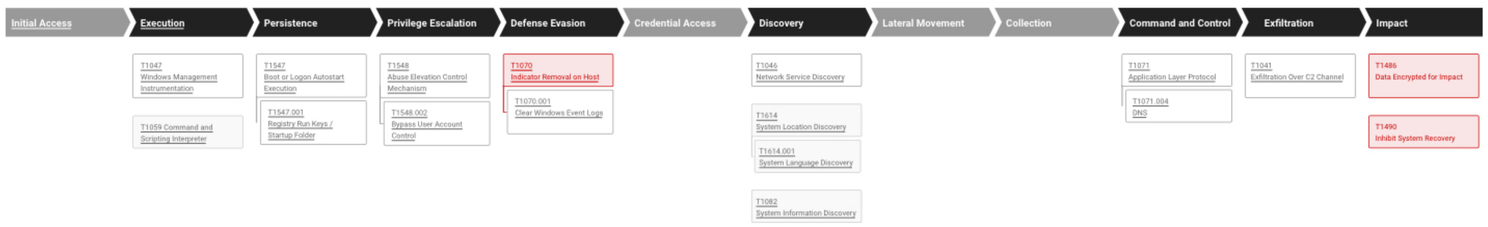
Hash:
6C5C2692597B5BBDF2ECEE9C9F667134 Domain:
VIDEO.CNHARDWARE.INFO
IP:
81.95.7.12
URL:
DLOAD01 S3.AMAZONAWS COM/B89FDBF4-9F80-11E7-ABC4-2209CEC27886B50A/
FIREFOXINSTALLER.EXE

ATTACK TRACING

HOW DID THE ATTACKER GET IN?

- **ATT&CK - Panorama**

ATT&CK Mapping



TA0002
T1204 - User Execution
T1204.002 - Malicious File
TA0005
T1620 - Memory Code Loading
TA0011
T1071 - Application Layer Protocol
T1071.001-Web Protocol
TA0004
T1548 - Abuse Elevation Control Mechanism T1548.002 - Bypass User Account Control
TA0005
T1548 - Abuse Elevation Control Mechanism T1548.002 - Bypass User Account Control
TA0002
T1106 - Execution Through Native API
TA0010
T1041 - Data Exfiltration Over C2 Channel
TA0005
T1112 - Modify Registry
TA0007
T1057 - Process Discovery

DNS Activity in the Incident (Top5)

osuyet.net

Network Activity in the Incident (Top5)

164.155255.240

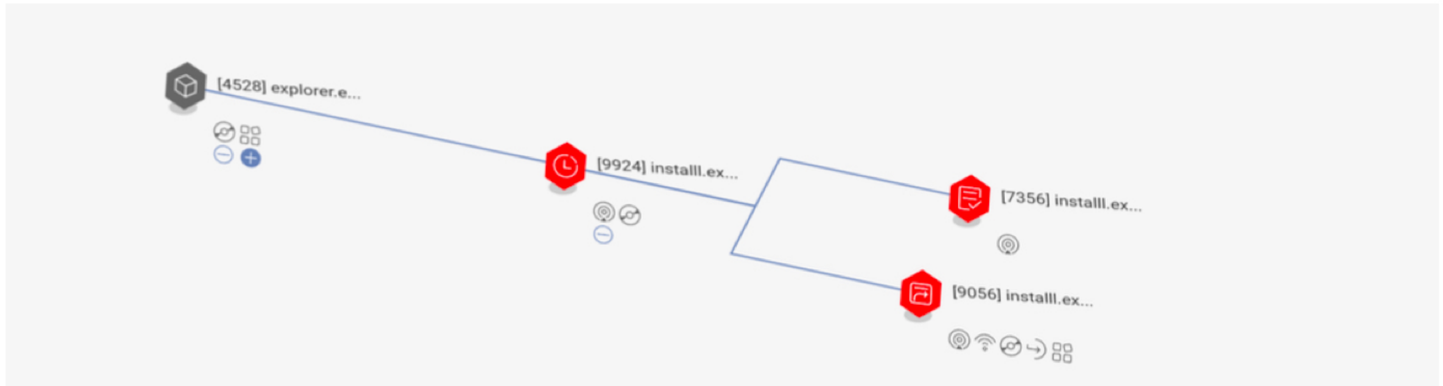
SHA1 of Processes in the Incident (Top5)

9E7F0305F63958789060EE094BC0901869BAF9D1

ATTACK TRACING

HOW DID THE ATTACKER GET IN?

Attack Procedures-Process Chain



Analysis Overview of Attack Procedures

Process chain analysis of this sample shows that the attack started with the explorer.exe process. It is Windows Resource Manager which is usually started manually by the user. On top of that, the explorer.exe process started a sub-process named test.exe which further executed 4plo5w.exe. According to threat analysis, 4plo5w.exe had the behavior of in-memory code loading, suggesting that the sample utilized memory-resident techniques to evade detection. Additionally, test.exe created command and control communication over Web protocol, indicating that it may receive instructions from the attacker through the web channel. Based on the overall analysis, the threat source may be that the user manually launched the malware without knowing it, resulting in the entire attack incident.

DNS Activity in Detections (Top5)

osuyet.net

Network Activity in Detections (Top5)

164,155255.240

SHA1 of Processes in Detections (Top5)

9E7F0305F63958789060EE094BC0901869BAF9D1
7ED61C5188FBCFF1904A6A0F0DEB5605837A4298

ATTACK TRACING

General Information of Process

[7836] explorer.exe

General Information of Process

Name: explorer.exe
Path: C:\windows\explorer.exe
Command Line: C:\windows\Explorer.EXE
MD5: 4BF8CF1A2379B005486DEC220CA32989
SHA1: E94FC38810C097A64F7419960F2D21052D1CB2E7
Process Security: Safe
Product Name: Microsoft® windows® operating system
Company Name: Microsoft Corporation
Signature: Microsoft windows, Microsoft corporation, Redmond, Washington, US

Process IOA (Indicators of Attack) Hits (Top 5)

IOA Name: Process downloads files suspiciously
IOA Description: Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications
ATTACK TID: T1041

IOA Name: Create process snapshot
IOA Description: Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software / applications running on systems within the network. Adversaries my use the information from Process Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
ATT&CK TID: T1057

IOA Name: PE file ManualMap
IOA Description: Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk. Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).
ATT&CK TID: T1620

IOA Name: Access to malicious IP
IOA Description: Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of these commands, will be embedded within the protocol traffic between the client and server.
ATT&CK TID: T1071.001

IOA Name: Create suspended process
IOA Description: Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIS provide a controlled means of calling low-level os services within the kernel, such as those involving hardware/devices, memory, and processes. These native APIS are leveraged by the os during system boot (when other system components are not yet initialized) as well an carrying out tasks and requests during routine operations
ATT&CK TID: T1106

ATTACK TRACING

HOW DID THE ATTACKER GET IN?

Process Network Operation (Top 5)

Local IP: 192.168.220.167
Remote IP: 20.24 121 134
Port: 443
Network Protocol: TCP

Process disk operation

File Read (Top3)

C:\Program Files\rooma\rmroot\data\LICENSE.txt

C:\Users\%username%\AppData\Local\IconCache.db

New executable Write (Top3)

C:\Windows\System32\drivers\rmkernel.sys

PROCESS DNS REQUESTS

Suspicious DNS Requests (Top3)

No suspicious DNS request detected

DNS Requests (Top3)

Domain： assets.msn.com

Process Registry Operation (Top 5)

Registry Value Changes (Top3)

Operation： Value Added
Value name： {e28f0235-8b2a-4b34-9e3c-7f38fd9cabf4}
Key： \REGISTRY\MACHINE\BCD00000000\Description
Value： 0x1

Operation： Value Added
Value name： {a3a94dc3-bf3c-47d1-8239-617e31a9d10b}
Key:
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BFE\Parameters\Policy\Persistent\Callout
Value： 0x1

Operation： Value Added
Value name： {5bb254fc-9050-421a-9085-0c6a31e3bfa8}
Key:
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BFE\Parameters\Policy\Persistent\Filter
Value： 0x1

RECOMMENDATIONS

WHAT SHOULD I DO NEXT?

Activate the emergency plan promptly

The emergency plan formulated in advance should be activated in a timely manner, and the detailed disposal should be carried out according to the established steps.

Isolate and clean up the affected hosts in time

Firstly, disconnect the Internet connection and dedicated connection of the affected hosts to avoid lateral movement between networks.
Secondly, strictly inspect the affected hosts for backdoors, trojans, and other malicious programs, completely remove all malicious files from the host, and clear any malicious code residing in memory to ensure thorough removal of malicious programs from the host. If necessary, reinstall the operating system and install the latest security patches.
Thirdly, reset password of the compromised account involved in this attack, improve password strength and enable multi-factor authentication.

Reconnect the cleaned hosts to the network

Redeploy relevant services, configure related networks, and resume online on the cleaned-up hosts.

PREVENTIVE MEASURES

HOW CAN I PREVENT THIS FROM REOCCURRING?

Focus on Installing Security Patches: Ensure that security patches are installed and vulnerabilities are fixed in a timely manner.

It is recommended that all critical assets such as operating systems, applications, and network devices install security patches in time to fix known vulnerabilities and issues.

Pay attention to Network Security Protection: Deploy effective network security detection and defense products.

Taking into account perimeter security, endpoint security, data security, and supply chain security, and other aspects, deploy effective detection and defense products. When choosing network security products, it is essential to assess their offensive and defensive capabilities, and configure them correctly to avoid being unable to effectively defend against attacks.

Emphasize on Network Management Security: Such as network segmentation, multi-factor authentication, and the use of blacklist and whitelist.

In daily network management, the network can be divided into multiple isolated areas and access control policies can be set as needed. This can reduce the attacker's ability to move laterally through the network. Additionally, implementing multi-factor authentication and strengthening password and credential management can effectively reduce the risk of credential theft. Using application blacklisting and whitelisting mechanisms can also effectively reduce the probability of successful attacks.

Strengthen Employee Security Awareness: Train employees to prevent social engineering attacks.

Conduct regular security awareness training for employees to prevent them from clicking on unknown emails, files, or links and phishing by attackers.

Develop Data Backup and Recovery Strategies: Back up critical data on a regular basis.

It is important to back up critical data regularly and store it in a secure, offline location. Test and validate the recovery process in advance to ensure quick data recovery when needed.