FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

15 February 2024

FLASH Number

MU-000174-MW

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP: CLEAR**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

www.fbi.gov/contact-us/field-offices

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Identification and Disruption of the Warzone Remote Access Trojan (RAT)

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the Warzone Remote Access Trojan (RAT), also identified as “Ave Maria” through open-source reporting and FBI investigation. On 7 February 2024, the FBI and international partners executed a coordinated operation to disrupt Warzone RAT infrastructure worldwide. The FBI is releasing this product to maximize awareness on the service and to seek additional reporting from victims.

Beginning in October 2018, the Warzone service offered a malware-as-a-service (MaaS) remote access trojan, along with other malware products and attracted a customer database of over 7,000 users. The products were used by cyber criminals and nation state actors to engage in remote control, keylogging, data theft, or other methods of discovering and collecting victim system information.

The FBI's Internet Crime Complaint Center (IC3) has established a dedicated page for organizations or victims of the Warzone RAT to report key findings at https://wzvictims.ic3.gov.

Technical Details

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques.

Overview

The Warzone RAT, also identified as Ave Maria due to variations of the text "Ave_Maria" appearing in the code, was used in nation-state attack campaigns, spam or phishing campaigns by cyber criminals, and as a precursor to follow-on exfiltration and extortion attacks. The tool, which was written in C++ and compatible with all Windows releases, was available for purchase on a publicly available website beginning in October 2018. The tool listed additional features which included, but was not limited to, remote webcam, hidden remote desktop (HRDP), password recovery, live keylogger, offline keylogger, remote desktop, Windows defender bypass, privilege escalation, reverse proxy, persistence, and mass execute.

The Warzone service offered multiple associated malware products, including a premium RAT called "Poison" with advanced features such as a rootkit to hide processes, files, and startup; premium customer support; and premium Dynamic Domain Name System (DDnS) services. Warzone also offered a dedicated crypter designed to obfuscate binary files generated with a Warzone RAT builder, allowing them to go undetected by antivirus solutions. Builders for document-based exploit delivery, including a "reg dropper", aka registry dropper, and three Microsoft-based exploit builders, were available for sale by the administrators. The Microsoft exploits, which allowed malware to be embedded into a .doc or Excel file, exploited the reported Common Vulnerabilities and Exposures (CVEs), in particular CVE-2017-8570, CVE-2017-11882, and CVE-2018-0802. Malicious files generated by the exploit builders were typically delivered via phishing email.

The Warzone website previously offered multiple DDnS services, which were used by attackers to obfuscate the location of their Command and Control (C2) servers.

Threat Actor Group Utilization

According to open-sources and prior US Cybersecurity Advisories (CSAs), the Warzone RAT was used by the following threat actors:

Table 1: Threat Actor Group Utilization

Group / Campaign	Notes
Scattered Spider	Used for enabling remote access to a victim's systems. Please see JCSA product ID AA23-320A for further details.
Confucius APT Group	Campaign targeting governments in mainland China and other South Asian countries.
Spearphishing Campaign	Campaign attempting to compromise government employees and military personnel of India's National Informatics Centre (NIC).
Phishing Campaign	Phishing campaign spoofing official Hungarian government employee communications
Sandworm (Russian APT)	Cyber espionage attack(s) against Ukrainian telecommunication providers.
APT-C-36 Campaign	Phishing email campaign targeting various entities in South America.
Yorotrooper Espionage Campaign	Espionage campaign targeting CIS countries, embassies, and EU health care agency.

FBI investigative efforts identified significant usage of Warzone by unidentified or unaffiliated threat actors operating independently of the above examples. Warzone has more than 7,000 customers who together paid approximately $2 million to use the service since 2018, with payments ranging from $50 to $2,100 per month.

Distribution

Warzone RAT was primarily distributed as a malicious attachment in an email (T1566), either through broad malware spam (malspam) campaigns or targeted phishing attempts. The malware was often also distributed with or through malicious Microsoft Office files (T1221), which exploit Microsoft CVE-2017-11882, a CVE that has been in multiple Top Routinely Exploited Vulnerabilities reports coauthored by the Cybersecurity and Infrastructure Security Agency's (CISA), the FBI, the NSA and FVEY partners. This distribution approach required the recipient to click on the attachment for deployment (T1204). The RAT can however be distributed by or with other malicious software or tools.

Persistence

During installation, the malware gains persistence by copying itself to *C:\Users\User\AppData\Roaming* and creating a registry key with a value set to the location of Warzone's executable binary to enable automatic execution of the code after each machine reboot.

Communication

The malware communicates with C2 servers via TCP over a configurable port which defaults to port 5200. The C2 IP address and port associated with a given Warzone RAT file is stored in a dedicated '.bss' section of the file in encrypted form alongside the key needed to decrypt it. The C2 communication packets payload is also encrypted using RC4 encryption, typically with the passwords "warzone160\x00" or "nevergonnagiveyouup". Variations in the C2 communications could be attributable to the progressive versions of the malware sold by the developers. After decrypting the communication and connecting with the C2 server, the malware collects basic system information about the compromised host, such as PC name and operating system, and sends it back to the C2 server.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 2 for all referenced threat actor tactics and techniques in this advisory, as well as corresponding detection and/or mitigation recommendations. For additional mitigations, see the Mitigations section.

Table 2: Warzone RAT ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
Phishing: Spearphishing Attachment	T1566.001	Warzone RAT has been distributed as a malicious attachment within an email.

Table 3: Warzone RAT ATT&CK Techniques for Enterprise – Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Warzone RAT can use PowerShell to download files and execute commands and use and cmd.exe to execute malicious code.
Native API	T1106	Warzone RAT can use a variety of API calls on a compromised host.
User Execution: Malicious File	T1204.002	Warzone RAT has relied on a victim to open a malicious attachment within an email for execution.

Table 4: Warzone RAT ATT&CK Techniques for Enterprise – Persistence

Technique Title	ID	Use
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	Warzone RAT can add itself to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UIF2IS20VK Registry keys.
Event Triggered Execution: Component Object Model Hijacking	T1546.015	Warzone RAT can perform COM hijacking by setting the path to itself to the HKCU\Software\Classes\Folder\shell\open\command key with a DelegateExecute parameter.

Table 5: Warzone RAT ATT&CK Techniques for Enterprise – Defense Evasion

Technique Title	ID	Use
Impair Defense: Disable or Modify Tools	T1562.001	Warzone RAT can disarm Windows Defender during the UAC process to evade detection.
Process Injection	T1055	Warzone RAT has the ability to inject malicious DLLs into a specific process for privilege escalation.
Modify Registry	T1112	Warzone RAT can create HKCU\Software\Classes\Folder\shell\open\command as a new registry key during privilege escalation.
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002	Warzone RAT can use sdclt.exe to bypass UAC in Windows 10 to escalate privileges; for older Windows versions WarzoneRAT can use the IFileOperation exploit to bypass the UAC module.
Deobfuscate/Decode Files or Information	T1140	Warzone RAT can use XOR 0x45 to decrypt obfuscated code.
Hide Artifacts	T1564	Warzone RAT can masquerade the Process Environment Block on a compromised host to hide its attempts to elevate privileges through IFileOperation.
Rootkit	T1014	Warzone RAT can include a rootkit to hide processes, files, and startup.

Template Injection	T1221	Warzone RAT has been installed via template injection through a malicious DLL embedded within a template RTF in a Word document.

Table 6: Warzone RAT ATT&CK Techniques for Enterprise – Credential Access

Technique Title	ID	Use
Credentials from Password Stores	T1555	Warzone RAT has the capability to grab passwords from numerous web browsers as well as from Outlook and Thunderbird email clients.

Table 7: Warzone RAT ATT&CK Techniques for Enterprise – Discovery

Technique Title	ID	Use
File and Directory Discovery	T1083	Warzone RAT can enumerate directories on a compromised host.
Process Discovery	T1057	Warzone RAT can obtain a list of processes on a compromised host.
System Information Discovery	T1082	Warzone RAT can collect compromised host information, including OS version, PC name, RAM size, and CPU details.

Table 8: Warzone RAT ATT&CK Techniques for Enterprise – Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Warzone RAT has the ability to control an infected PC using RDP
Remote Services: VNC	T1021.005	Warzone RAT has the ability to perform remote desktop access via a VNC console.

Table 9: Warzone RAT ATT&CK Techniques for Enterprise – Collection

Technique Title	ID	Use
Data from Local System	T1005	Warzone RAT can collect data from a compromised host.
Input Capture: Keylogging	T1056.001	Warzone RAT has the capability to install a live and offline keylogger, including through the use of the `GetAsyncKeyState` Windows API.

Video Capture	T1125	Warzone RAT can access the webcam on a victim's machine.

Table 10: Warzone RAT ATT&CK Techniques for Enterprise – Command and Control

Technique Title	ID	Use
Encrypted Channel: Symmetric Cryptography	T1573.001	Warzone RAT can encrypt its C2 with RC4 with the password warzone160\x00.
Ingress Tool Transfer	T1105	Warzone RAT can download and execute additional files.
Non-Application Layer Protocol	T1095	Warzone RAT can communicate with its C2 server via TCP over port 5200.
Proxy	T1090	Warzone RAT has the capability to act as a reverse proxy.

Table 11: Warzone RAT ATT&CK Techniques for Enterprise – Exfiltration

Technique Title	ID	Use
Exfiltration Over C2 Channel	T1041	Warzone RAT can send collected victim data to its C2 server.

Indicators of Compromise

The following are strings that can be used to identify and detect unpacked Warzone payload inside memory:

- "warzone160\x00"
  - Encryption password/key for communication with C2 server
- "Ave_Maria Stealer"
  - String in the binary code of the RAT
- "nevergonnagiveyouup"
  - Encryption password/key for communication with C2 server

The following are other embedded communication passwords identified through the FBI's analysis of data associated with the malware:

- "warzoneTURBO"
- "MushroomFunguy"
- "doghoroscopes"

Recommended Mitigations:

The FBI recommends network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise:

Preparing for Cyber Incidents:

- **Maintain offline backups of data**, and regularly maintain backup and restoration.
- **Ensure all backup data is encrypted, immutable**, and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.
- **Review the security posture of third-party vendors and those interconnected with your organization**. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- **Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs** under an established security policy.
- **Document and monitor external remote connections**. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).

Protective Controls and Architecture:

- **Segment networks to prevent the spread of malware** or actor traversal. Network segmentation can help prevent the spread of malware by controlling traffic flows between, and access to, various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal with a networking monitoring tool**. To aid in detecting malware and actor activity, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software on all hosts**.
- **Secure and closely monitor remote desktop protocol (RDP) use**.

- Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.

The FBI recommends the following mitigation measures be taken within the first 72 hours of detection:

Prepare Your Environment for Incident Response.

- Establish out-of-band Communication methods for dissemination of intrusion response plans and activities, inform network operations centers (NOCs) and computer emergency response teams (CERTs) according to institutional policy and standard operating procedures (SOPs).
- Maintain and actively monitor centralized host and network logging solutions after ensuring all devices have logging enabled and their logs are being aggregated to those centralized solutions.
- Disable all remote (including remote desktop protocol and virtual private network) access until a password change with two-factor authentication has been completed.
- Implement full secure socket layer (SSL) / transport layer security (TLS) inspection capability (on perimeter and proxy devices).
- Monitor accounts and devices that are determined to be part of the compromise to prevent reacquisition attempts.
- Collect forensic images including memory capture of devices determined to be part of the compromise.

Implement core mitigations to prevent re-exploitation (within 72 hours).

Implement a network-wide password reset with two-factor authentication (preferably with local host access only, no remote changes allowed) to include:

- All domain accounts (especially high-privileged administrators)
- Local Accounts
- Machine and System Accounts

Patch all systems for critical vulnerabilities:

- A patch management process which regularly patches vulnerable software remains a critical component in raising the difficulty of intrusions for cyber operators.
- While a few adversaries use zero-day exploits to target victims, many adversaries still target known vulnerabilities for which patches have been released, capitalizing on slow patch processes and risk decisions by network owners not to patch certain vulnerabilities or systems.
- Ensure you are patched against older vulnerabilities commonly exploited by cyber operators, such as CVE-2017-11882.

After initial response activities, deploy and properly configure a mitigation tool kit. All hosts and servers on the network should implement mitigation toolkits.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. The FBI's Internet Crime Complaint Center (IC3) has established a dedicated page for organizations or victims of the Warzone RAT to report key findings at https://wzvictims.ic3.gov.

With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and designated point of contact.

Administrative Note

This product is **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.