

XWorm V6.0 Multi-Stage Campaign — "backupallfresh2030" — Breakglass Intelligence Report

 intel.breakglass.tech/post/xworm-backupallfresh

Breakglass Intelligence

April 4, 2026



TLP: WHITE **Date:** 2026-04-03 **AnalystClassification:** Cybercrime — Remote Access Trojan (RAT) **Source:** Twitter tip from @smica83 / @JAMESWT_WT, tagged #XWorm

Executive Summary

A Turkish-origin threat actor operating under the GitHub alias [flexhere687-art](#) (email: [flexhere687@gmail\[.\]com](mailto:flexhere687@gmail[.]com)) is conducting an active XWorm V6.0 campaign using a multi-layered delivery chain. The campaign abuses Google Blogger (via custom domain [backupallfresh2030\[.\]com](#)), Filemail for payload hosting, and GitHub for secondary payload staging. The actor deploys at least THREE distinct delivery vectors: obfuscated JavaScript droppers, BAT files with UAC bypass, and trojanized Python 3.12 distributions carrying encrypted shellcode. The campaign has been active since at least 2026-03-22 and targets English-speaking victims through tax document, invoice, and shipping lures.

Key Findings

- **XWorm V6.0** ([@XCoderTools](#)) RAT deployed via multi-stage infection chain

- **Actor email exposed:** [flexhere687@gmail\[.\]com](mailto:flexhere687@gmail.com) via GitHub commit history (OPSEC failure)
- **Turkish-origin indicators:** BAT dropper contains Turkish comments ("Yonetici izni kontrolu"), payload named "sigortasevdalisi" (Turkish for "insurance enthusiast")
- **GitHub staging repos:** [flexhere687-art/xvxc-](#) and [flexhere687-art/vxcxc-xcv](#) (created 2026-03-22, STILL LIVE)
- **5 malicious executables** hosted on GitHub, including 2 variants of XWorm (.NET)
- **Trojanized Python 3.12 distribution** with PythonForWindows + PyCryptodome for in-memory shellcode loading
- **Filemail abuse** for hosting 14MB trojanized Python ZIP payload
- **Two Blogspot staging domains** confirmed: [backupallfresh2030\[.\]com](#) and [marchcap28.blogspot\[.\]com](#)
- **Persistence via:** Registry Run key (mimics Realtek "RtkAudUService"), schtasks, Startup folder, LOLBin abuse ([SyncAppvPublishingServer.vbs](#))
- **Defender evasion:** Excludes entire C:\ drive, .exe/.bat/.ps1 extensions, and the install process from Defender scanning

Attack Chain

```
[EMAIL LURE] (tax docs, invoices, FedEx, CVs)
|
v
[JS DROPPER] (.js with fake double extension: "document.pdf" .js")
|
+---> [PowerShell -EncodedCommand]
|
|       |
|       v
|       [Filemail Download] -> python312x64.zip (14MB trojanized Python)
|       |
|       v
|       [Protected.py] -> AES+XOR decrypt shellcode -> Reflective DLL load
|       |
|       v
|       [XWorm V6.0 RAT] (in-memory, no disk artifact)
|
+---> [BAT DROPPER] (UAC bypass via VBS elevation)
|
|       v
|       [GitHub raw download] -> dddd.exe / sigortasevdalisi.exe
|       |
|       v
|       [Startup folder + Run key persistence]
|       |
|       v
|       [XWorm V6.0 RAT] (disk-based .NET assembly)
```

Infrastructure Analysis

Domain Infrastructure

Domain	Type	Registrar	Created	NS
backupallfresh2030[.]com	Custom domain	Namecheap	2025-11-04	lola/rodrigo.ns.cloudflare.com
marchcap28.blogspot[.]com	Blogspot	Google	Unknown	Google

Delivery Infrastructure

Service	URL/Identifier	Purpose	Status
Google Blogger	Blog ID 6582486935030313121	Delivery page (CNAME via www)	LIVE
Google Blogger	Blog ID 4350113143311731351	Second staging (#APRL 1 CAP#)	LIVE
Filemail	filekey=53VkMz8l67SvighkrcVFIAwFCS9tbjRQ...	Trojanized Python ZIP hosting	LIVE
GitHub	flexhere687-art/xvxc-	Malware payload hosting (5 EXEs)	LIVE
GitHub	flexhere687-art/vxcxc-xcv	Second payload repo	LIVE

GitHub Repository Contents (flexhere687-art/xvxc-)

File	Size	SHA256 (prefix)	Type	Purpose
dddd.exe	71KB	8d82e375...	.NET XWorm V6.0	Primary RAT payload
31.exe	3.2MB	a32a687c...	.NET assembly	Secondary payload
sigortasevdalisi.exe	8.4MB	d0081085...	PE32+ x86-64	Loader/crypter (Turkish name)
Update_XCEmCHCVGH.exe	9.8MB	Unknown	PE executable	Update/loader

WHOIS & Registration

- **Registrar:** Namecheap, Inc.
- **Registration Date:** 2025-11-04T23:38:16Z (5 months before campaign activity)
- **Expiry:** 2027-11-04
- **Privacy:** Withheld for Privacy ehf (Iceland)
- **Cloudflare NS Pair:** lola / rodrigo (shared account indicator)

Malware Analysis

Sample 1: dddd.exe (XWorm V6.0)

Field	Value
SHA256	8d82e3757e9db0fc247350ab3140a21badcf8d6c60dfe79200d7d1e2a93dba14
MD5	781f4d43b2bbe30677f88b32fbf8b3ec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Type	PE32 .NET assembly (Mono)
Size	71,680 bytes
Compile Time	2026-03-22 15:51:01 UTC
Framework	.NET 4.0.30319 (VB.NET)
XWorm Version	V6.0 (@XCoderTools)

Capabilities (from User Strings analysis):

- Remote shell execution (RunShell)
- DDoS attacks (StartDDos/StopDDos)
- File management (FM, DW, LN)
- URL opening (Urlopen, Urlhide)
- System control (PCShutdown, PCRestart, PCLogoff)
- Plugin system (plugin, sendPlugin, savePlugin, RemovePlugins)
- Keylogger (keyboard hook via GetKeyState/GetKeyboardLayout)
- Screen capture (\$Cap, #CAP)
- Recovery data theft (RunRecovery)
- Credential harvesting (OfflineGet)
- Hosts file manipulation (Hosts, Shosts)
- UAC bypass (UACFunc)
- File encryption/decryption (ENC/DEC)

- Process injection (injRun)
- Telegram C2 notification (bot API + chat_id)
- Sandbox/VM detection (VMware, VirtualBox, SbieDll.dll, VIRTUAL, microsoft corporation)
- Anti-analysis (hosting check via ip-api.com)

Encrypted Config (AES-ECB, custom key derivation — config extraction pending):

- Config stored in .NET #US heap as 15 encrypted strings
- Key derivation uses non-standard method (not MD5/SHA256 of plaintext key)

Sample 2: Protected.py (Multi-Stage Python Loader)

Obfuscation Layers:

1. Arithmetic expression obfuscation (chr values computed via complex math)
2. Base64 + zlib + reverse + ROT13 + XOR(16) for code strings
3. Custom builtins class reimplementation to hide exec/eval
4. Junk string insertion throughout

Encryption Keys Extracted:

- AES Key: `a34c243e8fae4a20ad13a0e6be19749c9b0ba47ac8e79af0e4da57f59373c003`
- AES IV: `ad4b127c683d974dbeab87331b864884`
- XOR Key 1: `aab57c82934f7296a1cf7e8095eca567`
- XOR Key 2: `811ea130857d3fd0c8d32f8b401518e9`

Persistence Mechanism:

- Registry: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run -> RtkAudUserService`
- LOLBin: `SyncAppvPublishingServer.vbs -> PowerShell -> pythonw.exe Protected.py`
- Install path: `%APPDATA%\Templates\python312x64\`

Sample 3: BAT Dropper (864eed)

Field	Value
SHA256	864eedb88690d3a8479f9deb175e8cd8762b73459c5944684cc05055d14fde27
Type	BAT script (Unicode UTF-8)
Language	Turkish comments

Actions:

1. UAC elevation via VBScript (getadmin.vbs)
2. Disable Windows Defender Enhanced Notifications

3. Add exclusions: C:, .exe, .bat, .ps1, Microsys.exe process, Startup folder
4. Download **dddd.exe** from GitHub raw
5. Install as **Microsys.exe** in Startup folder
6. Registry persistence: **HKLM\...\CurrentVersion\Run** -> "SysWOW64"

JS Dropper Analysis (0794ad)

Obfuscation: String interleaving with junk pattern **IaYvjggOMp** **Execution:** WScript.Shell -> powershell -EncodedCommand **Payload:** Downloads trojanized Python from Filemail, extracts to %APPDATA%\Templates, executes Protected.py **Fake signature:** Microsoft Authenticode signature block appended to appear legitimate

Threat Actor Profile

Attribution Assessment

- **Confidence:** HIGH
- **Country:** Turkey
- **Evidence:**
 - Turkish language in BAT dropper ("Yonetici izni kontrolu" = "Admin permission check")
 - Filename "sigortasevdalisi.exe" (Turkish: "insurance enthusiast")
 - Email: flexhere687@gmail[.]com (exposed in GitHub commits)
 - GitHub account created 2026-03-22 (purpose-built for this campaign)
 - Consistent UTC+3 activity window in commit timestamps

OPSEC Failures

1. **GitHub email exposed:** flexhere687@gmail[.]com in every commit
2. **Turkish language artifacts** not scrubbed from BAT dropper
3. **Turkish filename** in payload repository
4. **Blog title left as operational note:** "#2030 domain# namecheap# ALL INJECT"
5. **All infrastructure still live** 12+ days into the campaign

Actor Timeline

Date	Event
2025-11-04	Domain backupallfresh2030[.]com registered via Namecheap
2026-03-22 00:15	GitHub account flexhere687-art created
2026-03-22 00:25	First repo (vxcxc-xcv) created with initial dddd.exe
2026-03-22 15:51	dddd.exe compiled (XWorm V6.0)

Date	Event
2026-03-24	Payload updates pushed
2026-03-25	First MalwareBazaar submissions (FedEx lure)
2026-03-28	More payload uploads
2026-03-30	BAT dropper variant submitted to MalwareBazaar
2026-04-01	Tax document JS dropper variants (smica83/JAMESWT_WT reports)
2026-04-01	marchcap28 blogspot updated ("#APRL 1 CAP#")

Social Engineering Lures

Lure Filename	Theme	Vector	Date
James_Smith_Tax_Documents_2025.pdf.js	US Tax	JS dropper	2026-04-01
Fedex_statement_of_accounts_inv_03_24_2026_pdf.js	FedEx Invoice	JS dropper	2026-03-25
DSB confirmation of funds transfers.js	Bank Transfer	JS dropper	2026-03-25
Maria Popescu cv 24-03-26.js	CV/Resume	JS dropper	2026-03-26
IMG-01252610-W0W63-CAM087IMG.jpeg.bat	Image File	BAT dropper	2026-03-30
Swift_Copy-40125.exe{124~KB}.exe	SWIFT Transfer	EXE	2026-04-03
Order Request..exe	Purchase Order	EXE	2026-04-03
1014578922 INV_PL SWB Specimen.xlam	Invoice	CVE-2017-11882	2026-03-24

MITRE ATT&CK Mapping

Tactic	Technique	ID	Application
Initial Access	Phishing: Spearphishing Attachment	T1566.001	Email with JS/BAT/XLAM attachments

Tactic	Technique	ID	Application
Execution	User Execution: Malicious File	T1204.002	JS/BAT dropper execution
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	Encoded PowerShell commands
Execution	Command and Scripting Interpreter: Python	T1059.006	Trojanized Python distribution
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	BAT dropper
Persistence	Boot or Logon Autostart: Registry Run Keys	T1547.001	RtkAudUService, SysWOW64
Persistence	Boot or Logon Autostart: Startup Folder	T1547.001	Microsys.exe in Startup
Persistence	Scheduled Task	T1053.005	schtasks for minute-interval execution
Defense Evasion	Impair Defenses: Disable Windows Defender	T1562.001	Add-MpPreference exclusions
Defense Evasion	Masquerading	T1036	Fake Realtek audio service name
Defense Evasion	Obfuscated Files or Information	T1027	Multi-layer JS/Python obfuscation
Defense Evasion	Signed Binary Proxy Execution	T1216	SyncAppvPublishingServer.vbs LOLBin
Defense Evasion	Virtualization/Sandbox Evasion	T1497	VMware/VirtualBox/Sandboxie detection
Discovery	System Information Discovery	T1082	CPU, GPU, RAM, OS enumeration
Collection	Screen Capture	T1113	\$Cap/#CAP commands
Collection	Input Capture: Keylogging	T1056.001	LowLevelKeyboardProc hook
Command & Control	Application Layer Protocol: Web	T1071.001	HTTP POST C2 communication
Command & Control	Web Service	T1102	Telegram bot API for notifications

Tactic	Technique	ID	Application
Exfiltration	Exfiltration Over C2 Channel	T1041	Data sent via XWorm C2 protocol

IOC Summary

Network Indicators

- [backupallfresh2030\[.\]com](#) (Blogger delivery domain)
- [www\[.\]backupallfresh2030\[.\]com](#) (CNAME -> ghs.google.com)
- [marchcap28\[.\]blogspot\[.\]com](#) (Second staging domain)
- [hxxps://2007\[.\]filemail\[.\]com/api/file/get?filekey=53VkMz8l67SvighkrcVFIAwFCS9tbjRQNSIziw1sS8FshApkve0_aRg5y3k](#) (Payload ZIP)
- [hxxps://raw\[.\]githubusercontent\[.\]com/flexhere687-art/xvxc-/main/dddd.exe](#) (GitHub payload)
- [hxxp://ip-api\[.\]com/line/?fields=hosting](#) (Sandbox detection)

File Indicators

SHA256	Filename
8d82e3757e9db0fc247350ab3140a21badcf8d6c60dfe79200d7d1e2a93dba14	dddd.exe
a864e410c00b15f65d31ebfeb96b061dbba7ca0615063d9ab59ef8b6b593d8b2	dddd.exe (v2)
a32a687c22c7c8a2466bf4f84cd7faab3f27a3f03c8ac507d87d542966675aa9	31.exe
d00810850aade1b7624660fedcd4753fea29a9dfe4bebbf4afe933d3aa981b93	sigortasevdalisi.
687f0be5399d54a1b841fdae68c75d2e46dd12f1c76f14687da58222191bbb08	python312x64.zi
333aae0b09f9a443c3fd9b381f04f684e87aa6ad8fc55f8ac3293e8df80b45d5	James_Smith_T
0794add65a271388acc6ab87a0dc2fe47373b40921f22dec12c02f74fbe6b154	2license.js

SHA256	Filename
c6c0e723cfc8bc80ec71b0f02627cf3030c27f6aa209b23cbd94d041eab64384	James_Smith_T
864eedb88690d3a8479f9deb175e8cd8762b73459c5944684cc05055d14fde27	IMG-01252610-1 CAM087IMG.jpg

Behavioral Indicators

- **Registry:** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\RtkAudUService
- **Registry:** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SysWOW64
- **Registry:** HKLM\SOFTWARE\Microsoft\Windows Defender Security Center\Notifications\DisableEnhancedNotifications
- **Scheduled Task:** Minute-interval task for persistence
- **Install Path:** %APPDATA%\Templates\python312x64\
- **Startup File:** %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\Microsys.exe
- **Log File:** \Log.tmp
- **Mutex:** Encrypted (extraction pending)
- **User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
- **Imphash:** f34d5f2d4577ed6d9ceec516c1f5a744

Actor Indicators

- **GitHub:** flexhere687-art (User ID 270032735)
- **Email:** flexhere687@gmail[.]com
- **Blogger IDs:** 6582486935030313121, 4350113143311731351

Recommended Actions

Immediate (24-48 hours)

- Block all IOC domains/URLs at proxy/firewall
- Search for RtkAudUService and SysWOW64 registry Run key entries
- Search for %APPDATA%\Templates\python312x64\ directory
- Search for Microsys.exe in Startup folders
- Search for SyncAppvPublishingServer.vbs LOLBin execution in EDR logs
- Report GitHub repos flexhere687-art/xvxc- and flexhere687-art/vxcxc-xcv for takedown

Short-term (1-2 weeks)

- Submit [flexhere687@gmail\[.\]com](mailto:flexhere687@gmail.com) to abuse databases
- Report [backupallfresh2030\[.\]com](mailto:backupallfresh2030[.]com) to Namecheap abuse
- Report Blogger abuse for Blog IDs 6582486935030313121 and 4350113143311731351
- Report Filemail link as malicious
- Deploy YARA and Suricata rules (see below)

Medium-term (1-3 months)

- Monitor for new domains using same Cloudflare NS pair (lola/rodrigo)
- Monitor GitHub for new repos from same actor
- Track XWorm V6.0 @XCoderTools variants

Abuse Reports

GitHub

- Repository: <https://github.com/flexhere687-art/xvxc-> (malware hosting)
- Repository: <https://github.com/flexhere687-art/vxcxc-xcv> (malware hosting)
- Report via: <https://github.com/contact/report-content>

Namecheap

- Domain: backupallfresh2030[.]com
- Email: abuse@namecheap.com
- Evidence: Used as custom domain for malware delivery via Blogger

Google (Blogger)

- Blog IDs: 6582486935030313121, 4350113143311731351
- Report via: <https://www.blogger.com/go/report-abuse>

Filemail

- Link: [hxxps://2007\[.\]filemail\[.\]com/api/file/get?filekey=53VkMz8l67SvighkrcVFIAwFCS9tbjRQNSlziw1sS8FshApkve0_aRg5y3k](https://2007[.]filemail[.]com/api/file/get?filekey=53VkMz8l67SvighkrcVFIAwFCS9tbjRQNSlziw1sS8FshApkve0_aRg5y3k)
- Content: Trojanized Python distribution with XWorm RAT loader

References

- Twitter tip: @smica83 / @JAMESWT_WT #XWorm
- MalwareBazaar XWorm tag: <https://bazaar.abuse.ch/browse/tag/XWorm/>
- XWorm V6.0 analysis: XCoderTools Telegram channel

- SyncAppvPublishingServer.vbs LOLBin: <https://lolbas-project.github.io/lolbas/Binaries/SyncAppvPublishingServer/>

Share 

Indicators of Compromise(16)

ip128.0.0.0

domainrodrigo.ns.cloudflare.com

domainvb.net

domainip-api.com

domainnamecheap.com

domainwww.blogger.com

sha2568d82e3757e9db0fc247350ab3140a21badcf8d6c60dfe79200d7d1e2a93dba14

sha256a34c243e8fae4a20ad13a0e6be19749c9b0ba47ac8e79af0e4da57f59373c003

sha256864eedb88690d3a8479f9deb175e8cd8762b73459c5944684cc05055d14fde27

sha256a864e410c00b15f65d31ebfeb96b061dbba7ca0615063d9ab59ef8b6b593d8b2

sha256a32a687c22c7c8a2466bf4f84cd7faab3f27a3f03c8ac507d87d542966675aa9

sha256d00810850aade1b7624660fedcd4753fea29a9dfe4bebbf4afe933d3aa981b93

sha256687f0be5399d54a1b841fdae68c75d2e46dd12f1c76f14687da58222191bbb08

sha256333aae0b09f9a443c3fd9b381f04f684e87aa6ad8fc55f8ac3293e8df80b45d5

sha2560794add65a271388acc6ab87a0dc2fe47373b40921f22dec12c02f74fbe6b154

sha256c6c0e723cfc8bc80ec71b0f02627cf3030c27f6aa209b23cbd94d041eab64384

Related Reports

[high](#)

[REFUNDEE: Inside a Shadow Panel Phishing-as-a-Service Operation](#)

[4/12/2026](#)

[high](#)

[AllSyDevs C2 Infrastructure](#)

[4/10/2026](#)