Resecurity | F5 BIG-IP Source Code Leak Tied to State-Linked Campaigns Using BRICKSTORM Backdoor

Published: 2025-10-22 · Archived: 2026-04-29 02:06:35 UTC

Overview

The China-nexus threat cluster **UNC5221** is actively targeting organizations that deploy **F5 BIG-IP** after a confirmed breach of F5 in which a nation-state actor stole internal development data, including portions of BIG-IP source code and vulnerability information. On **October 15, 2025**, CISA issued **Emergency Directive ED-26-01**, warning of an **imminent threat** to federal networks and ordering urgent inventory, hardening, and patching of affected F5 devices. The stolen code raises the risk of rapid 0-day discovery and weaponization against internet-exposed management services.

F5 revealed that attackers, discovered on its systems on August 9 and informed customers that the hackers remained in the company's network for **at least 12 months** as reported by Bloomberg. The announcement follows authorization from the U.S. Department of Justice, which allowed F5 **to delay public disclosure of the breach** under Item 1.05(c) of Form 8-K due to ongoing law enforcement considerations.

The vendor stated that it is not aware of any undisclosed critical or remote code execution vulnerabilities that could have been exploited by the attackers, and there is no evidence that any non-public flaws were used in actual attacks.

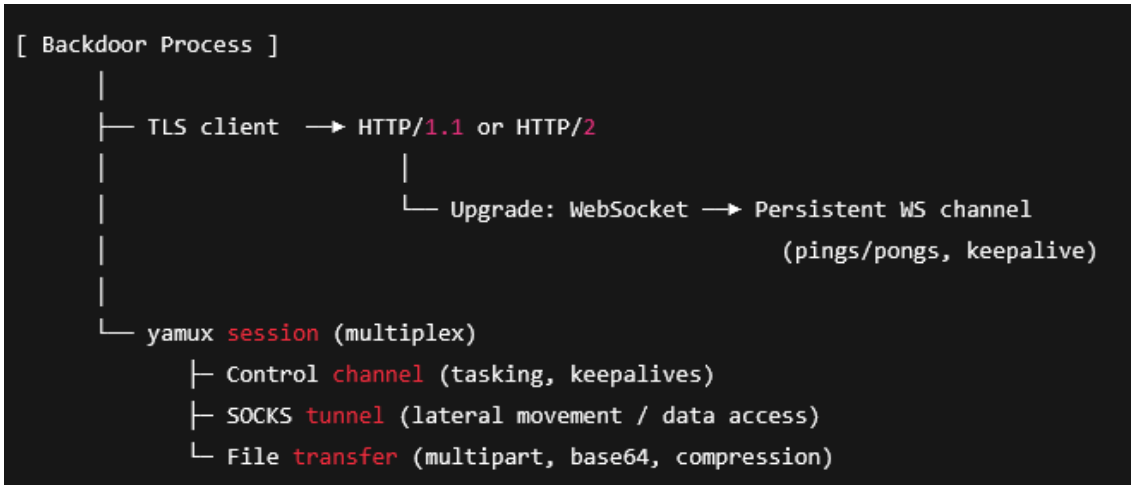
According to an 8-K form filed with the Securities and Exchange Commission, the company first became aware of unauthorized access Aug. 9 and initiated standard incident response measures, including enlisting external cybersecurity consultants. In September, the Department of Justice **permitted F5 to withhold public disclosure** of the breach, which the government allows if a breach is determined to be a "**a substantial risk to national security or public safety**."

Technical Details

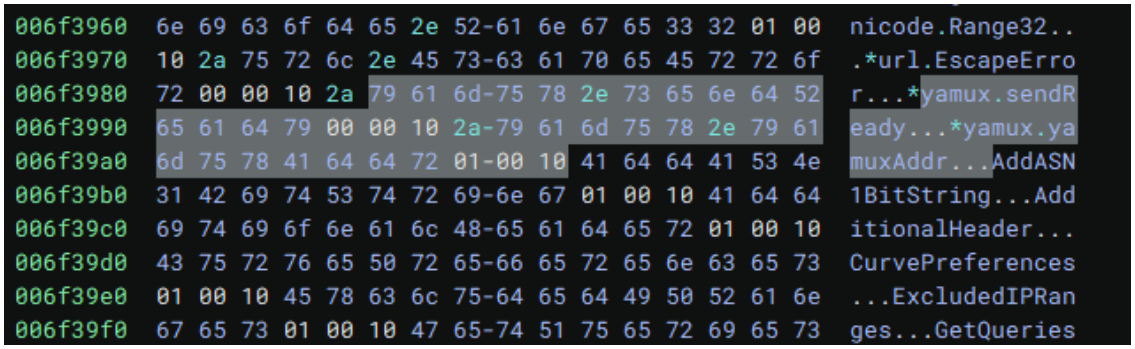
Resecurity is the first to release the BRICKSTORM backdoor analysis, providing additional details on the involvement of threat actors from China. During our investigation, our team collected multiple artifacts associated with UNC5221's appliance-focused tradecraft. The most relevant items preserved in evidence include:

- **A statically linked Go ELF backdoor** consistent with the **BRICKSTORM** family
- **Small deployment scripts** used to stage and persist the backdoor on edge devices.
- **A servlet filter web component** used by the same actor set to harvest credentials post-foothold.

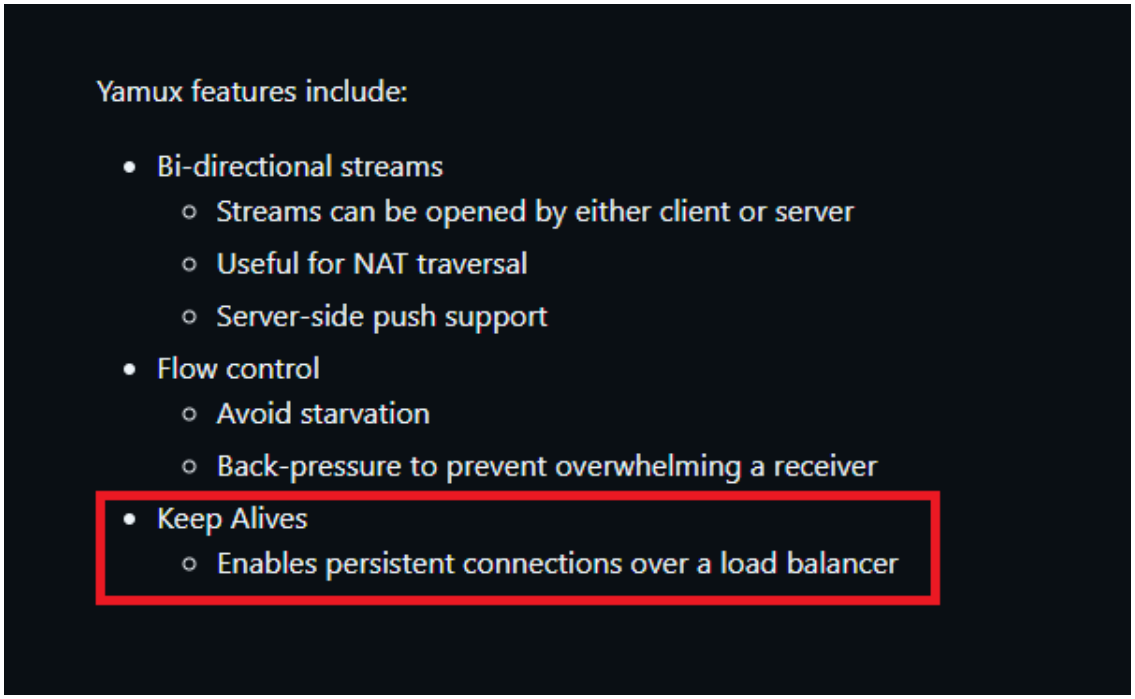
Our analysis below is anchored in static/dynamic review of those artifacts:



The backdoor is a **self-contained, dependency-free executable** (Go, linux/amd64) packaged for appliances with limited userland; it embeds full web transport (TLS client, HTTP/1.1/HTTP/2 paths, WebSocket upgrade/session handling), **Yamux** for multiplexing many logical streams over one socket, a **SOCKS** mechanism for TCP pivoting, and a complete **multipart/form-data** stack for web-looking file staging/exfil.

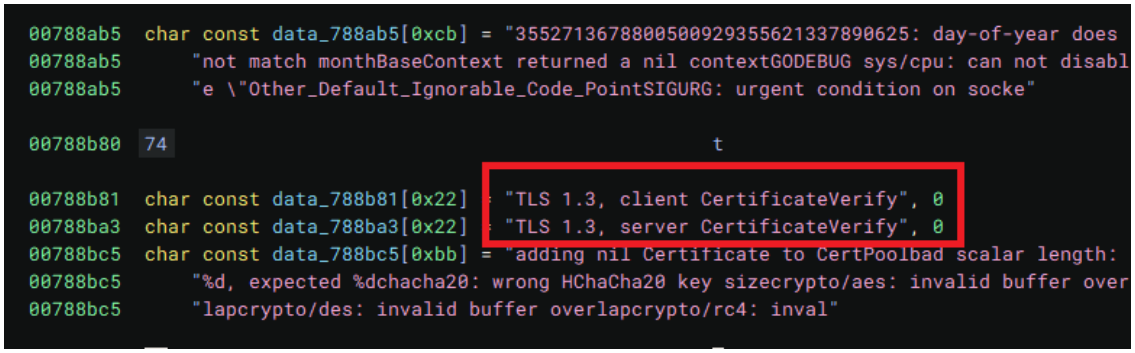


Yamux is a multiplexing library for Golang. It relies on an underlying connection to provide reliability and ordering, such as TCP or Unix domain sockets, and provides stream-oriented multiplexing.



Yamux is inspired by SPDY. SPDY was introduced by Google in **late 2009** as an experimental protocol to improve web performance. However, SPDY was officially **deprecated in early 2016**.

For this attack, the attacker used an exploit and deploys an **ELF file** on the BIG-IP device after gaining code execution, configures it to establish outbound **TLS** that negotiates HTTP/2 and upgrades the connection to WebSocket for a persistent C2 tunnel, then launches it with operator-supplied C2 parameters to multiplex concurrent streams over a single socket via **Yamux**.



Within that session the actor enables a **SOCKS-style proxy** to reach internal applications from the appliance's management IP, moves data over the same channel using **multipart/form-data** with **base64/quoted-printable** and compression so exfiltration resembles ordinary web traffic.

```
0053968d  if (&__return_addr u<= *(*(fsbase - 8) + 0x10))
00539708      sub_4695a0(rdi, rsi)
00539708      noreturn
00539708
005396a2  int64_t var_40 = arg1
005396a6  int64_t var_38 = 0xa
005396be  int64_t var_40_1 = 0
005396cd  char const* const var_38_1 = "illegal base64 data at input
005396d2  int64_t var_30_1 = 0x22
005396db  int64_t var_30
005396db  int64_t var_28_1 = var_30
005396e0  int64_t var_28
005396e0  int64_t var_20 = var_28
005396e5  sub_451740(sub_479740(rdi, rsi))
005396f4  int64_t result
```

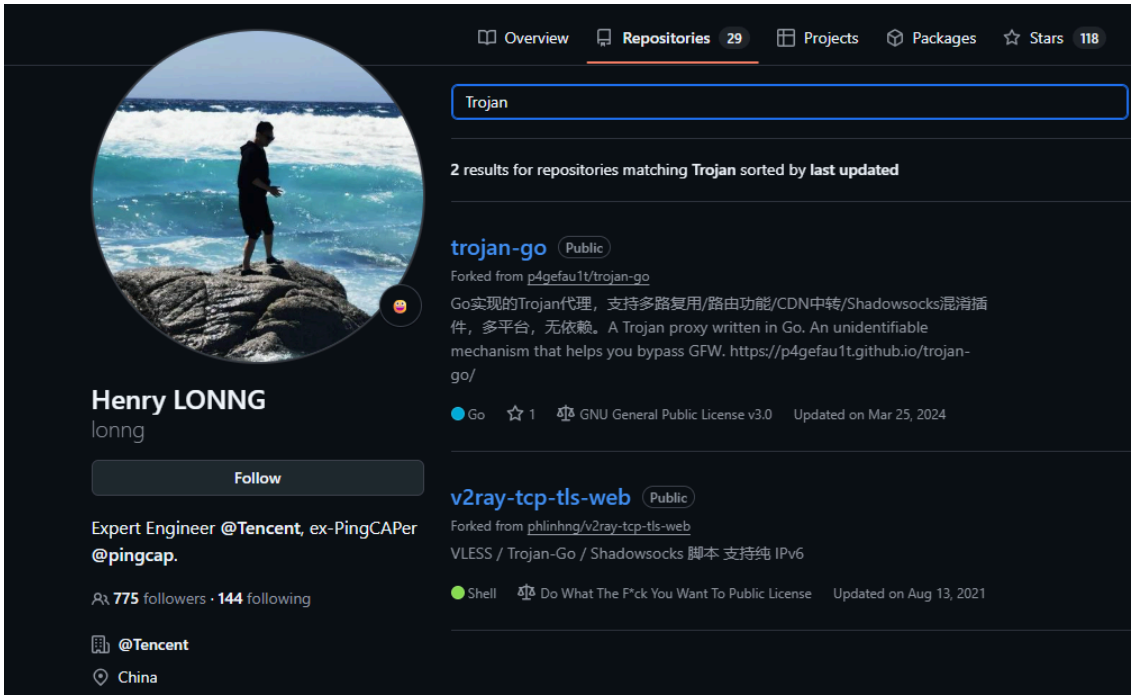
We have noticed there are no hardcoded domains or credentials in the ELF file, which suggests the attackers likely used a zero-day to gain access and can connect back to the target without issue.

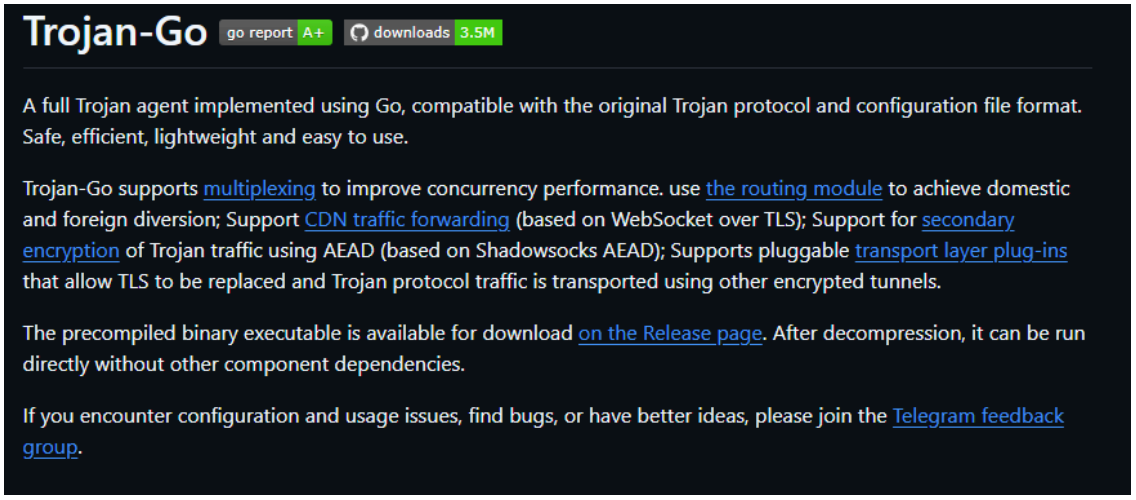
If an attacker gets code execution (via 0-day or weakly secured services), **BRICKSTORM** can turn a **BIG-IP** into a stealth egress point and internal proxy, with minimal logs and long dwell.

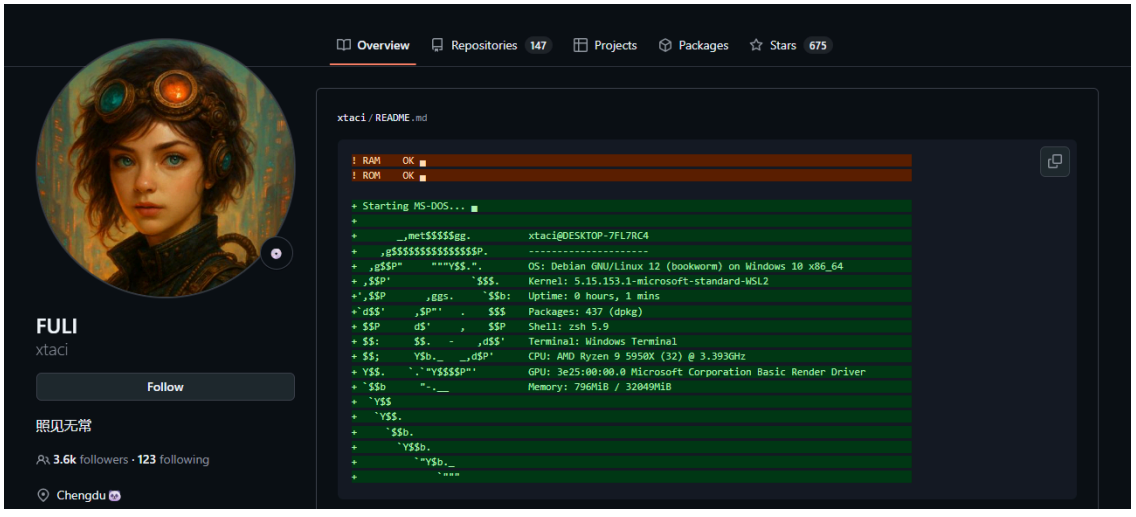
The Origin

Our analysis found attackers leveraging publicly available repositories; portions of the codebase appear to have originated from repositories maintained in China. Some of these projects in the repositories are maliciously designed to attack user systems.

```
007dda4b  char const data_7dda4b[0x0] =
007dda4b  {
007dda4b  }
007dda4b                                        00 00 14 7a 65              ...ze
007dda50  72 6f 52 54 54 51 75 65-75 65 44 75 72 61 74 69  roRTTQueueDurati
007dda60  6f 6e 00 00 00 00 00 00-00 00 15 67 69 74 68 75  on...........githu
007dda70  62 2e 63 6f 6d 2f 6c 6f-6e 6e 6e 67 2f 6e 65 78  b.com/lonnng/nex
007dda80  char const data_7dda80[0x0] =
007dda80  {
007dda80  }
007dda80  00 00 15 69 6e 74 65 72-6e 61 6c 2f 73 69 6e 67  ...internal/sing
007dda90  6c 65 66 6c 69 67 68 74-00 00 15 69 6e 74 65 72  leflight...inter
007ddaa0  6e 61 6c 2f 75 6e 73 61-66 65 68 65 61 64 65 72  nal/unsafeheader
007ddab0  char const data_7ddab0[0x0] =
```







UPDATE (December 19, 2025):

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency, and Canadian Centre for Cyber Security released an update to the Malware Analysis Report BRICKSTORM Backdoor with indicators of compromise (IOCs) and detection signatures for additional BRICKSTORM samples.

This update provides information on additional samples, including Rust-based samples. These samples demonstrate advanced persistence and defense evasion mechanisms, such as running as background services, and enhanced command and control capabilities through encrypted WebSocket connections.

MITRE ATT&CK Techniques

Tactic	Technique ID	Technique name	Description	Evidence / Notes
Initial Access	**T1190**	Exploit Public-Facing Application	Compromise of internet-exposed BIG-IP management/services to gain code execution (risk amplified by stolen source and vuln intel).	0-day discovery and weaponization; attacker used an exploit and deploys an ELF on BIG-IP.
Execution	**T1204.002**	Malicious File	Operator launches the ELF backdoor on the appliance with runtime C2 parameters.	Deploys an ELF file; launches it with operator-supplied C2 parameters.
Execution	**T1106**	Native API	Implant performs system/file/network ops via OS/runtime APIs.	Self-contained executable with full web transport and file staging/exfil.
Persistence	**T1543.002**	Create/Modify System Process: systemd	Create/modify a systemd unit so the implant auto-starts on boot.	Modifies systemd entries for persistence.
Defense Evasion	**T1027**	Obfuscated/Compressed Files & Info	Wraps data in base64/quoted-printable and compression inside multipart to evade content inspection.	multipart/form-data with base64/quoted-printable and compression.
Defense Evasion	**T1036**	Masquerading	C2/file moves over HTTP/2 and WebSocket to blend with normal web traffic.	HTTP/2; WebSocket; web-looking file staging/exfil.

Tactic	Technique ID	Technique name	Description	Evidence / Notes
Credential Access	**T1556**	Modify Authentication Process	Servlet filter/web component on adjacent infra (e.g., vCenter) captures credentials during login.	Servlet filter web component used to harvest credentials post-foothold.
Lateral Movement	**T1090**	Proxy	SOCKS-style proxying from the appliance's management IP to reach internal services.	Enables a SOCKS-style proxy to reach internal applications.
Lateral Movement	**T1572**	Protocol Tunneling	Multiplex multiple logical streams over a single TLS/WS socket using **yamux**.	Multiplex concurrent streams over one socket via **Yamux**.
Command & Control	**T1071.001**	Web Protocols (HTTPS)	Primary C2 over TLS/HTTP(S), often negotiating HTTP/2 (ALPN h2).	Establish outbound TLS that negotiates HTTP/2.
Command & Control	**T1071.004**	Application Layer Protocol: WebSocket	Long-lived bidirectional **WebSocket** tunnel for C2.	Upgrades the connection to **WebSocket** for a persistent C2 tunnel.
Command & Control	**T1573**	Encrypted Channel	**TLS** protects all C2 and data movement.	Outbound **TLS**; persistent tunnel.
Command & Control	**T1090.003**	Multi-hop Proxy	Appliance acts as a stealth **egress point** into the environment.	Turn a BIG-IP into a stealth **egress point** and internal proxy.
Collection	**T1005**	Data from Local System	Stage files locally and prepare for transfer over the C2 channel.	File staging/exfil over **multipart/form-data**.
Exfiltration	**T1041**	Exfiltration Over C2 Channel	Send data through the established **TLS/WebSocket** channel using multipart frames.	Moves data over the same channel… resembles ordinary web traffic.

Tactic	Technique ID	Technique name	Description	Evidence / Notes
Collection / Prep	**T1560**	Archive Collected Data	Compress/encode data prior to transfer to reduce detectability.	Compression + **base64/quoted-printable** within multipart.

Patch Now

F5 has disclosed **over twenty vulnerabilities** spanning **BIG-IP (all modules)**, **F5OS (A/C)**, and **BIG-IP Next (SPK/CNF)**, with several issues that could enable **remote exploitation of internet-exposed management services**. If you operate any **affected versions** listed above, **treat this as an emergency**: remove public exposure of management planes, restrict egress, and **upgrade to the vendor's latest fixed releases immediately**. After patching, **verify** that devices no longer match the affected version ranges, re-enable only necessary services, and monitor for anomalous **HTTP/2/WebSocket** egress from appliance subnets.

Vulnerability	Affected Product
CVE-2025-53868	BIG-IP (all modules)
CVE-2025-61955	F5OS-A; F5OS-C
CVE-2025-57780	F5OS-A; F5OS-C
CVE-2025-60016	BIG-IP (all modules); BIG-IP Next SPK; BIG-IP Next CNF
CVE-2025-48008	BIG-IP (all modules)
CVE-2025-59781	BIG-IP (all modules)
CVE-2025-41430	BIG-IP SSL Orchestrator
CVE-2025-55669	BIG-IP ASM
CVE-2025-61951	BIG-IP (all modules)
CVE-2025-55036	BIG-IP SSL Orchestrator
CVE-2025-54479	BIG-IP PEM; BIG-IP Next CNF
CVE-2025-46706	BIG-IP (all modules)
CVE-2025-59478	BIG-IP AFM
CVE-2025-61938	BIG-IP Advanced WAF/ASM
CVE-2025-54858	BIG-IP Advanced WAF/ASM

Vulnerability	Affected Product
CVE-2025-58120	BIG-IP Next SPK; BIG-IP Next CNF
CVE-2025-53856	BIG-IP (all modules)
CVE-2025-61974	BIG-IP (all modules); BIG-IP Next SPK; BIG-IP Next CNF
CVE-2025-58071	BIG-IP (all modules); BIG-IP Next CNF
CVE-2025-53521	BIG-IP APM
CVE-2025-61960	BIG-IP APM
CVE-2025-54854	BIG-IP APM
CVE-2025-53474	BIG-IP APM
CVE-2025-61990	BIG-IP (all modules); BIG-IP Next SPK; BIG-IP Next CNF
CVE-2025-58096	BIG-IP (all modules)
CVE-2025-61935	BIG-IP Advanced WAF/ASM

Indicators of Compromise (IOCs)

SHA-256: 90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035

Filename: Pg_update
Classification: BRICKSTORM (Go ELF backdoor)
Notes: System/update helper to blend in.

SHA-256: 2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df
Filename: Listener
Classification: BRICKSTORM (Go ELF backdoor)
Notes: Listener component; used for C2/socket handling.

SHA-256: aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878
Filename: Vmprotect
Classification: BRICKSTORM (Go ELF backdoor)
Notes: VMProtect Version
