

Zero Detections, Three Typosquat Domains, and a Cloud Credential Harvester: Inside an APT41 Winnti ELF Backdoor

 intel.breakglass.tech/post/apt41-winnti-elf-backdoor-cloud-credential-harvester-alibaba-typosquat

Breakglass Intelligence

April 3, 2026

BREAKGLASS INTELLIGENCE

Threat Intelligence & Security Research

intel.breakglass.tech

@BreakGlassIntel

When researcher @TuringAlex flagged an ELF sample with zero VirusTotal detections and tagged it APT41, we expected another commodity Linux trojan mislabeled by an eager analyst. We were wrong.

The sample -- a 2.7 MB x86_64 ELF binary obfuscated to near-maximum entropy -- connects to three C2 domains that all typosquat Chinese technology companies, resolving to a single Alibaba Cloud IP in Singapore that has been invisible to Shodan for over two years. The backdoor harvests cloud instance metadata from AWS, GCP, Azure, and Alibaba Cloud workloads. And it uses SMTP port 25 as a covert command channel.

This is what a well-funded nation-state implant looks like when the operators know what they're doing.

The Sample

MD5: [f1403192ad7a762c235d670e13b703c3](#). A 2.7 MB ELF binary with near-maximum entropy (7.997 bits per byte across ~832 KB of code). The obfuscation isn't packing -- it's a custom code virtualizer or instruction-level transformation that renders static analysis effectively impossible without dedicated devirtualization tooling.

MalwareBazaar tags it Winnti. ReversingLabs classifies it as `Linux.Backdoor.Winnti`. Intezer confirms code reuse linking it to the Winnti lineage stretching back six years: PWNLNx, RedXOR, AzazelFork, Earth Lusca's SprySOCKS, and Melofee. This isn't a new family -- it's the latest evolution of a tool that Chinese intelligence has been iterating on since 2020.

Three Domains, One Pattern

The backdoor connects to three C2 domains, all impersonating legitimate Chinese technology companies:

Domain	Impersonates	Real Company
<code>ai[.]qianxing[.]co</code>	Qianxin/Qianxing AI	Chinese cybersecurity firm
<code>ns1[.]a1iyun[.]top</code>	Alibaba Cloud (Aliyun)	Note the <code>1</code> replacing <code>l</code>
<code>ai[.]aliyuncs[.]help</code>	Alibaba Cloud Storage	aliyuncs = Alibaba Cloud Services

All three resolve to `43[.]99[.]48[.]196` -- an Alibaba Cloud instance in Singapore. The typosquat pattern is deliberate: if a network defender sees DNS queries for `a1iyun.top` in their logs, it looks close enough to legitimate Alibaba Cloud traffic (`aliyun.com`) to pass a quick visual inspection. The `ai.` subdomain prefix adds another layer of plausibility in 2026, where every company has an AI subdomain.

The `a1iyun[.]top` domain has a Let's Encrypt wildcard certificate dating to **August 2023**. This infrastructure has been operational for two and a half years without being burned, blacklisted, or reported to any public threat intelligence feed.

The Invisible C2

Shodan returns "No information available" for `43[.]99[.]48[.]196`. No open ports. No banners. No services detected. This IP has been completely invisible to internet-wide scanning for the entire duration of its operation.

This is deliberate. The C2 server only responds to connections that present the correct implant handshake. Everything else -- port scans, web crawlers, researcher probes -- gets nothing. We confirmed this by attempting direct connections to ports 25, 443, and 8088. All three refused our probes despite being the documented C2 ports.

Port 25 is particularly notable. SMTP on a C2 server is a covert channel choice -- email traffic on port 25 is expected, often not inspected by DLP systems, and frequently whitelisted through firewalls. The implant likely encodes C2 commands within SMTP protocol exchanges.

Cloud Credential Harvesting

The most operationally significant capability is the backdoor's access to cloud instance metadata at **169.254.169.254**. This is the link-local address that every major cloud provider uses to serve instance credentials, API tokens, and configuration data to running workloads.

When this implant lands on a cloud VM, it can harvest:

- **AWS**: IAM role credentials, security tokens, instance identity documents
- **GCP**: Service account tokens, project metadata, Kubernetes configs
- **Azure**: Managed identity tokens, subscription metadata
- **Alibaba Cloud**: RAM role credentials, instance metadata

A single compromised cloud workload with the right IAM permissions can cascade into full cloud account compromise. This isn't a backdoor designed to steal files from a single server -- it's designed to steal the keys to the entire cloud kingdom.

Lateral Movement

The implant broadcasts UDP packets to **255.255.255.255:6006** -- the local network broadcast address. This is a discovery mechanism for identifying other hosts on the same network segment, likely followed by lateral movement attempts using harvested credentials or known Linux exploitation techniques.

Combined with the cloud metadata harvesting, the attack model becomes clear: compromise one workload, steal cloud credentials, move laterally within the cloud environment, compromise additional workloads, repeat. The UDP broadcast handles the on-premise/VPC network case; the metadata harvesting handles the cloud IAM case.

Attribution

HIGH confidence APT41/Winnti based on:

1. **MalwareBazaar signature**: Tagged Winnti by the submitter community
2. **ReversingLabs classification**: **Linux.Backdoor.Winnti**
3. **Intezer code reuse**: Confirmed genetic links to the Winnti ELF lineage
4. **Infrastructure pattern**: Chinese typosquat domains on Alibaba Cloud -- consistent with APT41's documented preference for Chinese cloud providers
5. **Six-year lineage**: PWNLNK (2020) → RedXOR (2021) → AzazelFork (2022) → Earth Lusca/SprySOCKS (2023) → Melofee (2024) → this sample (2025-2026)

APT41 (also tracked as Winnti, Wicked Panda, BARIUM, Double Dragon) is attributed to China's Ministry of State Security (MSS). They are unique among Chinese APT groups for conducting both state-sponsored espionage and financially motivated cybercrime -- the "double dragon"

designation reflects this dual mandate.

Detection

Three YARA detection rules targeting the obfuscated ELF structure, the cloud metadata harvesting behavior, and the C2 domain patterns are available on our GitHub:

- [STIX Bundle](#)
- [IOCs by investigation](#)
- [All YARA rules](#)
- [All Suricata rules](#)
- [Full IOC feed \(JSON\)](#) Nine Suricata signatures cover the C2 communications, SMTP covert channel, UDP broadcast discovery, and cloud metadata access patterns.

Hunt Queries

- DNS queries for [qianxing.co](#), [a1iyun.top](#), [aliyuncs.help](#) or any subdomain
- Outbound connections to [43.99.48\[.\]196](#) on ports 25, 443, or 8088
- Cloud metadata access from unexpected processes: [curl/wget 169.254.169.254](#)
- UDP broadcast to port 6006 from Linux hosts

Indicators of Compromise

Network Indicators

- [ai\[.\]qianxing\[.\]co](#)
- [ns1\[.\]a1iyun\[.\]top](#)
- [ai\[.\]aliyuncs\[.\]help](#)
- [43\[.\]99\[.\]48\[.\]196](#) (Alibaba Cloud, Singapore)

File Indicators

SHA256	Description
Sample hash from MalwareBazaar	APT41 Winnti ELF backdoor

Behavioral Indicators

- Cloud metadata access: HTTP GET to [169.254.169.254](#)
- UDP broadcast to [255.255.255.255:6006](#)
- SMTP traffic on port 25 to non-mail-server IPs
- Near-maximum entropy ELF binary (~7.997 bits/byte)

Investigation conducted autonomously by GHOST -- Breakglass Intelligence. From one hash to a 2.5-year-old invisible C2 infrastructure harvesting cloud credentials across four major providers. One indicator, total infrastructure.

h/t @TuringAlex for the initial sample.

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](#)