# Dark Web Profile: CyberXero

By SD SOCRadar Dark Web Team

Published: 2026-11-10 · Archived: 2026-11-12 02:00:31 UTC

CyberXero is a Russian-speaking, financially motivated Initial Access Broker (IAB) active on Dark Web forums, including Dread and HackForums. The actor runs two parallel operations: an opportunistic global campaign that mass-exploits WordPress, Magento and other e-commerce platforms for access and payment data, and a directed campaign that conducts curated reconnaissance against Ukrainian energy and utilities organizations.

What sets CyberXero apart is its AI layer, with up to 51 specialized Claude Code agents on its primary workstation and a PentAGI deployment wired into a Cobalt Strike Team Server through the Anthropic API. The SOCRadar Threat Research Unit has tracked the actor's infrastructure since July 2026, and CyberXero remained active at the time of publication.

This profile is based on the findings of our prior research into CyberXero.

## Who Is CyberXero?

CyberXero came to light after SOCRadar identified an exposed open directory on an attacker-controlled HTTP server. The server held more than 90,000 files and 3,000 subdirectories from an active Linux workstation, including engagement folders named after target domains, exploitation toolkits, AI agent configurations, session logs and victim database exports.




*CyberXero threat actor card*

The actor's own Dread post describes a progression from having no prior knowledge to dumping emails and password hashes from vulnerable databases, running into tokenization while trying to obtain credit card data, and

moving toward digital skimming. That account matches the order of the compromises documented in its infrastructure, although the actor's five to nine years of web hosting administration contradicts the claim of having "started from scratch".

CyberXero's activity centers on three revenue streams:

- **Access brokering:** Compromised WordPress administration panels, webshells and network footholds, consistent with an IAB model built around selling access
- **Payment and personal data theft:** Database dumps, payment tables and a card skimmer endpoint tested against a production payment flow
- **Cryptocurrency payments:** A self-hosted payment gateway that accepts Bitcoin, Litecoin, Ethereum, USDT (ERC-20 and TRC-20) and Monero

### From an Open Directory to the CyberXero Alias

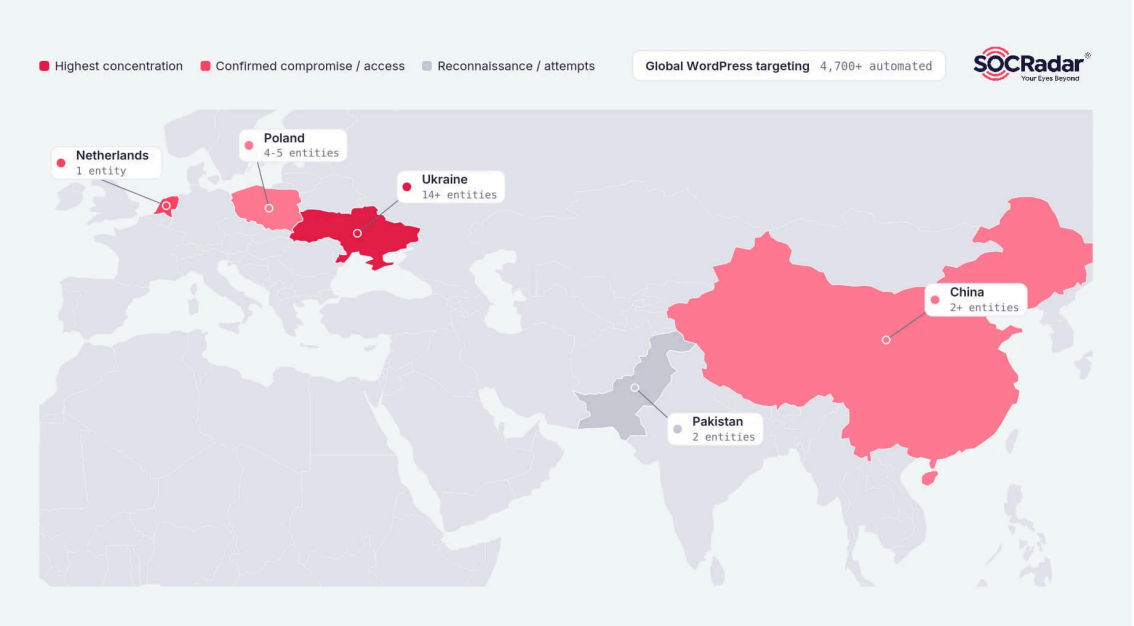
Attribution to the CyberXero alias rests on three independent lines of evidence. The open directory contained the operator's Claude Code account data, the session logs showed the actor citing a Dread post written by the CyberXero account as proof of "owning" the forum, and external verification confirmed that the post was published by CyberXero and describes the same TTP progression observed in the infrastructure.

Five independent identity anchors were collected across Anthropic, Apple, Google, Twitter/X and OpenAI accounts, and a record on a Russian freelance marketplace that requires identity verification adds further weight. Two additional Telegram accounts receive notifications from the actor's operational bot and are assessed as either a second alias or a trusted collaborator; their exact relationship to the primary operator could not be resolved with the available data.

The actor works in the Moscow time zone (UTC+3), supported by a provisioning timezone directive and 1,269 timestamped activity events peaking at 22:00 MSK, with virtually no activity between 02:00 and 08:00. Russian is the primary operational language, confirmed through script comments, a custom Claude Code instruction file and a mid-session language switch after a model refusal.

## What Are the Targets of CyberXero?

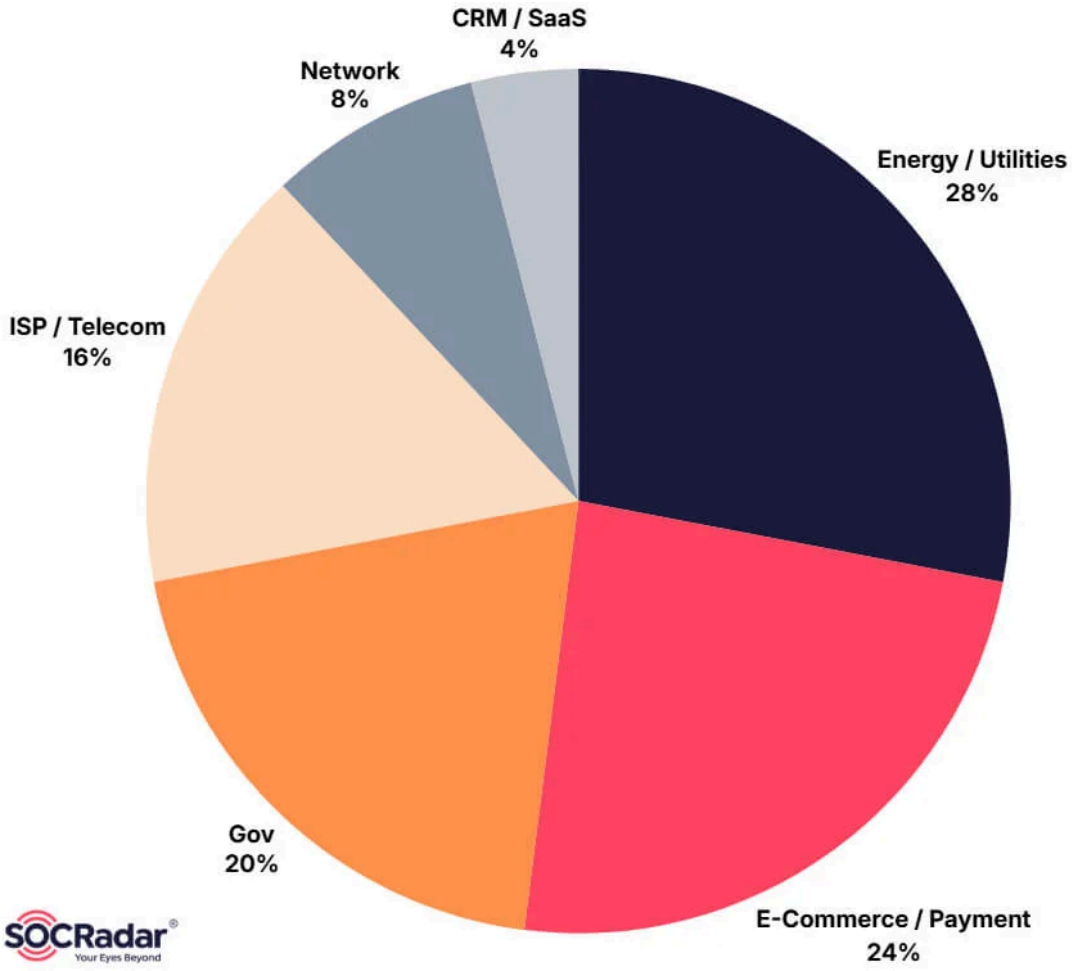
SOCRadar identified more than 40 affected organizations across Ukraine, Poland, China, Pakistan and the Netherlands, excluding the 4,500+ WordPress sites hit through mass exploitation.




*Geographic distribution of confirmed CyberXero victims*

Ukraine carries the highest concentration, with 14 or more entities identified at different stages of the compromise chain, mostly in the energy and utilities sector, plus four organizations in telecommunications, e-commerce and CRM compromised through the opportunistic pipeline. Seven Ukrainian energy and utilities entities, including the national transmission system operator and the country's largest private energy holding, were subjected to curated reconnaissance; one file alone lists 95 enumerated subdomains of the two largest, covering mail, VPN, network dispatch and data platforms.

Poland follows with four to five affected entities, two of them confirmed e-commerce compromises, and 284 scanned Polish domains with a heavy concentration of government institutions. The actor also compromised a Chinese corporate network cluster spanning at least three internal segments, attempted WAF bypass and credential spraying against two Pakistani national security government entities without confirmed success, and accessed a Dutch company through an exposed Magento configuration.




*Sector distribution of confirmed CyberXero victims*

Energy and utilities account for 28% of confirmed victims, followed by e-commerce and payment (24%), government (20%), ISP and telecom (16%), corporate networks (8%) and CRM and SaaS (4%).

The scale of the confirmed impact stands out in two figures:

- **More than 628,000 records:** Personal data of Ukrainian individuals in the actor's possession, including home addresses and login IP addresses of residents of Kharkiv, a city on an active war front
- **429 administration panels:** WordPress panels confirmed accessible in a single automated run that scanned 4,708 targets and deployed shells on 32 hosts in 61 seconds

The opportunistic pipeline fits a conventional IAB model, while the focus on Ukrainian critical infrastructure has no obvious direct monetization path. The most plausible explanation is access brokering to a buyer with a specific interest in that infrastructure, although no evidence of a sale, buyer communication or tasking was found.

## What Are the Techniques of CyberXero?

CyberXero runs an opportunistic pipeline and a targeted pipeline from the same workstations, sharing part of the same arsenal during the same period. Its infrastructure spans eight correlated nodes across three ASNs, linked through unique provisioning tokens, a shared internal hostname, command histories and staging logs.

## Initial Access Through Mass WordPress Exploitation

The actor's in-house tool, wp2shell, is a five-module Python package that abuses a desynchronization in the WordPress REST API batch endpoint (/wp-json/batch/v1), where the validation and execution handlers apply different authorization contexts. It adaptively selects union-based, error-based or time-based blind SQL injection, writes a new administrator directly to the database, logs in and deploys a WSO-family webshell registered as an active plugin.

Rogue administrators follow the pattern wp2_ plus eight random hexadecimal characters. A companion script, sc.py, works through the target queue and pushes each compromise to a rotating Telegram bot with the panel URL, credentials and shell status. Across the actor's files, more than 56,000 URLs were scanned, 500 hosts were exploitable and 72 rogue administrator accounts were created during the primary observation period.

## Targeted Intrusions Against Ukrainian Organizations

The targeted pipeline relies on deeper, manual chains. Against a Ukrainian classifieds and e-commerce portal, the actor combined blind SQL injection to recover an administrator email, a time-constrained password reset token extraction and a PHP deserialization chain built with phpggc, reaching remote code execution and dumping MySQL, MongoDB and Redis databases with 24,132 active sessions and 864 API tokens.

Against Kharkiv's district heating service, no exploitation was needed: a hardcoded administrator credential let a multithreaded scraper pull 564,073 subscriber records and 213,340 login log entries. Other confirmed exfiltration hit a regional ISP (63,621 customer records and 75,811 cleartext access credentials) and a gas provider (27 employee accounts with active session tokens).

## AI Augmentation and Safety Evasion

CyberXero uses AI in two independent layers. On its primary workstation, a swarm of 51 Claude Code agents covers offensive, reconnaissance and post-exploitation roles, from c2-operator and exploit-chainer to scada-attacker and data-exfiltrator. On the Team Server, PentAGI connects to Cobalt Strike through the Anthropic API, with the payload-generation role assigned the highest token limit and reasoning level.

A dedicated scope-guard agent wraps every task in a fictional "authorized pentest on own infrastructure" framing to lower the chance of model refusals, and the same ownership claim appears verbatim across four unrelated victims. When a model still refused, the actor reopened the task in a fresh session with the framing preloaded. The logs record repeated refusals nonetheless, including four declined requests to scan Dread, where the model asked for token-based ownership verification and rejected the actor's attempt to paste the token back into the chat.

## Rapid Weaponization of Vulnerabilities

CyberXero turns disclosed vulnerabilities into working exploits quickly. CVE-2026-4815 in Support Board 3.8.7 was published in June 2026, and a functional exploit with proxy rotation and automatic timing calibration appears in files dated July 2026, a cycle of less than 30 days. The arsenal also includes CVE-2026-63030 and CVE-2026-60137 in WordPress and CVE-2015-1397 in Magento.

## Command and Control With Cracked Cobalt Strike

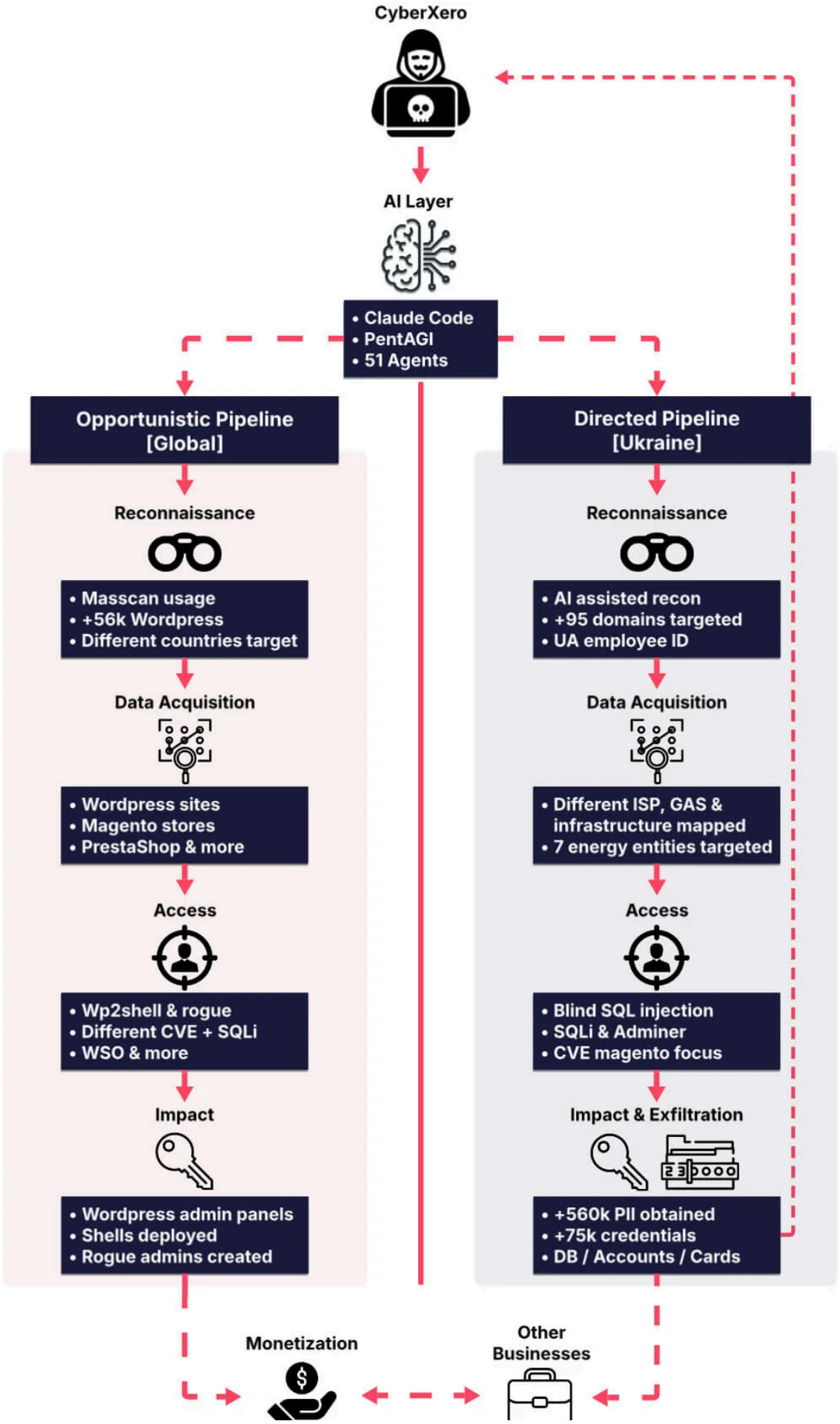
The actor runs Cobalt Strike 4.9.1 from a pirated build distributed through a Telegram channel, with a “Major Cobalt Strike” TLS certificate shared by about 184 other hosts that should not be treated as CyberXero infrastructure. The C2 receives HTTPS beacons on port 1002, serves HTTP staging on port 8044 and delivers PowerShell stagers on port 8033.

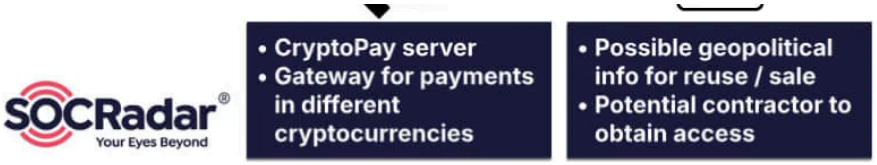
## Lateral Movement in a Chinese Network Cluster

A separate campaign gained access to a Chinese corporate network by abusing a misconfigured Redis server through a rogue master-replication technique that planted the actor’s SSH key. From there, beacons enumerated the network, brute-forced a ZTE gateway with default credentials, moved laterally over WMI through a passwordless account, checked hosts for EternalBlue patch status and created the UpdSvc Windows service for persistence. Successful EternalBlue exploitation was not confirmed in the available logs.

## Monetization and Competitor Suppression

A cryptocurrency payment gateway built on FastAPI and Celery, with local Litecoin and Monero full nodes, receives payments for sold access and data. The actor also built a card skimmer endpoint against a production payment flow, which had reached functional testing with about 50 masked card records. A script named abuse_monitor.py files abuse reports against competitors to URLhaus, VirusTotal and hosting providers under a fake fraud-analyst persona, a TTP undocumented in comparable IAB profiles.


CyberXero
AI Layer
• Claude Code
• PentAGI
• 51 Agents
Opportunistic Pipeline [Global]
Reconnaissance
• Masscan usage
• +56k Wordpress
• Different countries target
Data Acquisition
• Wordpress sites
• Magento stores
• PrestaShop & more
Access
• Wp2shell & rogue
• Different CVE + SQLi
• WSO & more
Impact
• Wordpress admin panels
• Shells deployed
• Rogue admins created
Directed Pipeline [Ukraine]
Reconnaissance
• AI assisted recon
• +95 domains targeted
• UA employee ID
Data Acquisition
• Different ISP, GAS & infrastructure mapped
• 7 energy entities targeted
Access
• Blind SQL injection
• SQLi & Adminer
• CVE magento focus
Impact & Exfiltration
• +560k PII obtained
• +75k credentials
• DB / Accounts / Cards
Monetization
Other Businesses




*CyberXero's opportunistic and directed pipelines, orchestrated through the AI layer*

## How Can Organizations Defend Against CyberXero?

The controls below map to CyberXero's documented TTPs, ordered along its intrusion chain from initial access to post-compromise activity.

### Hunt for Rogue WordPress Administrators

Review WordPress user tables for any account whose username matches wp2_ followed by eight hexadecimal characters, and check the plugins directory for paths matching wp2shell_ with the same suffix. Either artifact indicates that wp2shell touched the host, even if the webshell is no longer active, so treat the site as compromised and rotate all administrator credentials.

### Patch Exposed Web Applications Within Days

With a weaponization cycle under 30 days, patch windows measured in months leave WordPress, Magento, PrestaShop and Support Board deployments exposed. Prioritize CVE-2026-63030, CVE-2026-60137 and CVE-2026-4815, and confirm that configuration files such as Magento's app/etc/env.php are not publicly reachable.

### Remove Hardcoded and Default Credentials

Several CyberXero intrusions needed no exploit at all. Audit administration panels for shared or hardcoded credentials, replace default passwords on network devices such as gateways and routers, and eliminate local accounts with blank passwords that enable WMI-based lateral movement.

### Lock Down Internet-Facing Redis

Do not expose Redis to the internet, require authentication, and disable or rename the SLAVEOF/REPLICAOF command where replication is not needed. Monitor authorized_keys files on Redis hosts for unexpected changes.

### Block and Hunt Known C2 Infrastructure

Block the IP addresses listed in the IOC section and search historical logs for outbound connections to 42.193.227.214 on ports 1002, 8044 or 8033. Hunt for the UpdSvc service and PowerShell download cradles on Windows endpoints.

### Treat AI Agent Session Logs as Sensitive Data

The CyberXero investigation shows that AI agent session logs record every planned task, target and workaround, making them the equivalent of a keylogger of the operator's activity. Organizations running AI agents with terminal, network or data access should apply the same retention, encryption and access controls to these logs as to credential stores, and audit them for repeated attempts at the same refused task.

### Integrate Dark Web and Threat Intelligence Monitoring

CyberXero advertises on Dread and HackForums, and IAB listings often surface before access is used. Monitoring Dark Web forums and Telegram channels for references to your domains, brands and infrastructure gives an early signal that access may be for sale. SOCRadar Threat Intelligence's Advanced Dark Web Monitoring (ADWM) module provides this coverage.

## What Are the MITRE ATT&CK TTPs of CyberXero?

| Tactic | Technique | ID |
|---|---|---|
| Reconnaissance | Active Scanning: Vulnerability Scanning | T1595.002 |
| Reconnaissance | Gather Victim Network Information: DNS | T1590.002 |
| Reconnaissance | Gather Victim Org Information | T1591 |
| Resource Development | Acquire Infrastructure: Virtual Private Server | T1583.003 |
| Resource Development | Obtain Capabilities: Tool | T1588.002 |
| Resource Development | Obtain Capabilities: Exploits | T1588.005 |
| Initial Access | Exploit Public-Facing Application | T1190 |
| Initial Access | Valid Accounts: Local Accounts | T1078.003 |
| Initial Access | Brute Force: Password Spraying | T1110.003 |
| Execution | Command and Scripting Interpreter: PowerShell | T1059.001 |
| Execution | Command and Scripting Interpreter: Unix Shell | T1059.004 |
| Execution | Windows Management Instrumentation | T1047 |
| Execution | Software Deployment Tools | T1072 |
| Persistence | Server Software Component: Web Shell | T1505.003 |
| Persistence | Create or Modify System Process: Windows Service | T1543.003 |
| Persistence | Account Manipulation: SSH Authorized Keys | T1098.004 |
| Persistence | Create Account: Local Account | T1136.001 |
| Stealth | Obfuscated Files or Information | T1027 |

| Tactic | Technique | ID |
|---|---|---|
| Stealth | Masquerading: Match Legitimate Resource Name or Location | T1036.005 |
| Credential Access | OS Credential Dumping: LSASS Memory | T1003.001 |
| Credential Access | OS Credential Dumping: Security Account Manager | T1003.002 |
| Credential Access | Input Capture: Web Portal Capture | T1056.003 |
| Credential Access | Steal Web Session Cookie | T1539 |
| Discovery | Network Service Discovery | T1046 |
| Discovery | System Information Discovery | T1082 |
| Discovery | System Network Configuration Discovery | T1016 |
| Lateral Movement | Use Alternate Authentication Material: Pass the Hash | T1550.002 |
| Lateral Movement | Remote Services: SMB/Windows Admin Shares | T1021.002 |
| Collection | Data from Local System | T1005 |
| Collection | Data from Information Repositories | T1213 |
| Collection | Data from Cloud Storage | T1530 |
| Command and Control | Application Layer Protocol: Web Protocols | T1071.001 |
| Command and Control | Web Service: Bidirectional Communication | T1102.002 |
| Command and Control | Proxy: Multi-hop Proxy | T1090.003 |
| Exfiltration | Exfiltration Over C2 Channel | T1041 |
| Exfiltration | Exfiltration Over Web Service: Exfiltration to Cloud Storage | T1567.002 |
| Impact | Data Manipulation: Stored Data Manipulation | T1565.001 |

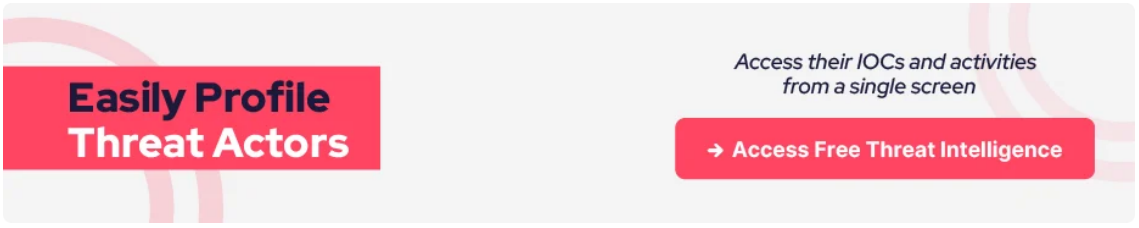
## What Are the IOCs of CyberXero?

| Type | Indicator | Description |
|---|---|---|
| IP | 46.21.250.135 | Primary workstation, |

| Type | Indicator | Description |
|---|---|---|
| | | open directory seed node |
| IP | 45.88.106.2 | Provisioning server (port 1500) |
| IP | 212.193.31.189 | Cryptocurrency payment gateway |
| IP | 42.193.227.214 | Cobalt Strike Team Server and PentAGI |
| IP | 91.208.184.148 | Secondary workstation |
| IP | 45.88.106.78 | Mass scanning server |
| IP | 49.234.12.182 | Staging and payload delivery server (Chinese cluster) |
| IP | 42.193.100.94 | Redis exploitation node and PentAGI agents |
| IP:Port | 42.193.227.214:1002 | Cobalt Strike HTTPS beacon |
| IP:Port | 42.193.227.214:8044 | Cobalt Strike HTTP staging |
| IP:Port | 42.193.227.214:8033 | Cobalt Strike PowerShell stager delivery |
| SHA256 | 92a789444708fa1cb4cc5a89e0aa6cc7a279b62a7b8a4d2857255a18197d0090 | stager32.bin, Cobalt Strike x86 stager |

| Type | Indicator | Description |
|---|---|---|
| | | (4.9.1 pirated build) |
| MD5 | 3870a559b5b6ea6076f5f90029c180b7 | stager32.bin, Cobalt Strike x86 stager |
| SHA256 | a5ae0aab352871bc0b038b3aa43b03eb223425628c884af7b9fc592cd34eb86c | Obfuscated WSO webshell |
| SHA256 | 71e21094c1ac1cf0275c91ed377965e248bca1c12711f6dd20e2682681fc1192 | 1.bin, Chinese cluster staging payload |
| SHA256 | 59c535f47ab4d35f6d9fc8b8aec4a72438ea0b89e5a4dcea74b05d2d32cfa483 | config.bin, Chinese cluster staging payload |

Behavioral indicators, weaponized CVEs and YARA rules are covered in the full threat research report. For additional IOCs and detection rules, you can visit the CyberXero threat actor profile on the SOCRadar platform.




---

Source: https://socradar.io/blog/dark-web-profile-cyberxero/