

Cloud insights

 darktrace.com/blog/react2shell-reflections-cloud-insights-finance-sector-impacts-and-how-threat-actors-moved-so-quickly

Nathaniel Jones

January 14, 2026



January 14, 2026

React2Shell Reflections: Cloud Insights, Finance Sector Impacts, and How Threat Actors Moved So Quickly

This blog breaks down how attackers rapidly weaponized the React2Shell vulnerability, with a particular focus on cloud-native financial environments. Drawing on Darktrace's honeypot research, it explores emerging threat actor tooling, exploitation timelines, and why behavioral-anomaly-led security is critical in today's cloud landscape.



Introduction

Last month's disclosure of CVE 2025-55812, known as React2Shell, provided a reminder of how quickly modern threat actors can operationalize newly disclosed vulnerabilities, particularly in cloud-hosted environments.

The vulnerability was discovered on December 3, 2025, with a patch made available on the same day. Within 30 hours of the patch, a publicly available proof-of-concept emerged that could be used to exploit any vulnerable server. This short timeline meant many systems remained unpatched when attackers began actively exploiting the vulnerability.

Darktrace researchers rapidly deployed a new honeypot to monitor exploitation of CVE 2025-55812 in the wild.

Within two minutes of deployment, Darktrace observed opportunistic attackers exploiting this unauthenticated remote code execution flaw in React Server Components, leveraging a single crafted request to gain control of exposed Next.js servers. Exploitation quickly progressed from reconnaissance to scripted payload delivery, HTTP beaconing, and cryptomining, underscoring how automation and pre-positioned infrastructure by threat actors now compress the window between disclosure and active exploitation to mere hours.

For cloud-native organizations, particularly those in the financial sector, where Darktrace observed the greatest impact, React2Shell highlights the growing disconnect between patch availability and attacker timelines, increasing the likelihood that even short delays in remediation can result in

real-world compromise.

In contrast to traditional enterprise networks built around layered controls, cloud architectures are often intentionally internet-accessible by default. When vulnerabilities emerge in common application frameworks such as React and Next.js, attackers face minimal friction. No phishing campaign, no credential theft, and no lateral movement are required; only an exposed service and exploitable condition.

The activity Darktrace observed during the React2shell intrusions reflects techniques that are familiar yet highly effective in cloud-based attacks. Attackers quickly pivot from an exposed internet-facing application to abusing the underlying cloud infrastructure, using automated exploitation to deploy secondary payloads at scale and ultimately act on their objectives, whether monetizing access through cryptomining or to burying themselves deeper in the environment for sustained persistence.

Cloud Case Study

In one incident, opportunistic attackers rapidly exploited an internet-facing Azure virtual machine (VM) running a Next.js application, abusing the React/next.js vulnerability to gain remote command execution within hours of the service becoming exposed. The compromise resulted in the staged deployment of a Go-based remote access trojan (RAT), followed by a series of cryptomining payloads such as XMrig.

Initial Access

Initial access appears to have originated from abused virtual private network (VPN) infrastructure, with the source IP (146.70.192[.]180) later identified as being associated with Surfshark

Figure 1: The IP address above is associated with VPN abuse leveraged for initial exploitation via Surfshark infrastructure.

The use of commercial VPN exit nodes reflects a wider trend of opportunistic attackers leveraging low-cost infrastructure to gain rapid, anonymous access.

Parent process telemetry later confirmed execution originated from the Next.js server, strongly indicating application-layer compromise rather than SSH brute force, misused credentials, or management-plane abuse.

Payload execution

Shortly after successful exploitation, Darktrace identified a suspicious file and subsequent execution. One of the first payloads retrieved was a binary masquerading as “vim”, a naming convention commonly used to evade casual inspection in Linux environments. This directly ties the payload execution to the compromised Next.js application process, reinforcing the hypothesis of exploit-driven access.

Command-and-Control (C2)

Network flow logs revealed outbound connections back to the same external IP involved in the inbound activity. From a defensive perspective, this pattern is significant as web servers typically receive inbound requests, and any persistent outbound callbacks — especially to the same IP — indicate likely post-exploitation control. In this case, a C2 detection model alert was raised approximately 90 minutes after the first indicators, reflecting the time required for sufficient behavioral evidence to confirm beaconing rather than benign application traffic.

Cryptominers deployment and re-exploitation

Following successful command execution within the compromised Next.js workload, the attackers rapidly transitioned to monetization by deploying cryptomining payloads. Microsoft Defender observed a shell command designed to fetch and execute a binary named “**x**” via either curl or wget, ensuring successful delivery regardless of which tooling was available on the Azure VM.

The binary was written to `/home/wasiluser/dashboard/x` and subsequently executed, with open-source intelligence (OSINT) enrichment strongly suggesting it was a cryptominer consistent with XMRig-style tooling. Later the same day, additional activity revealed the host downloading a static XMRig binary directly from GitHub and placing it in a hidden cache directory (`/home/wasiluser/.cache/.sys/`).

The use of trusted infrastructure and legitimate open-source tooling indicates an opportunistic approach focused on reliability and speed. The repeated deployment of cryptominers strongly suggests re-exploitation of the same vulnerable web application rather than reliance on traditional persistence mechanisms. This behavior is characteristic of cloud-focused attacks, where publicly exposed workloads can be repeatedly compromised at scale more easily.

Financial sector spotlight

During the mass exploitation of React2Shell, Darktrace observed targeting by likely North Korean affiliated actors focused on financial organizations in the United Kingdom, Sweden, Spain, Portugal, Nigeria, Kenya, Qatar, and Chile.

The targeting of the financial sector is not unexpected, but the emergence of new Democratic People's Republic of Korea (DPRK) tooling, including a Beavertail variant and EtherRat, a previously undocumented Linux implant, highlights the need for updated rules and signatures for organizations that rely on them.

EtherRAT uses Ethereum smart contracts for C2 resolution, polling every 500 milliseconds and employing five persistence mechanisms. It downloads its own Node.js runtime from `nodejs[.]org` and queries nine Ethereum RPC endpoints in parallel, selecting the majority response to determine its C2 URL. EtherRAT also overlaps with the Contagious Interview campaign, which has targeted blockchain developers since early 2025.

Read more finance-sector insights in Darktrace's white paper, [The State of Cyber Security in the Finance Sector](https://www.darktrace.com/resources/the-state-of-cybersecurity-in-the-finance-sector).

Threat actor behavior and speed

Darktrace's honeypot was exploited just two minutes after coming online, demonstrating how automated scanning, pre-positioned infrastructure and staging, and C2 infrastructure traced back to "bulletproof" hosting reflects a mature, well-resourced operational chain.

For financial organizations, particularly those operating cloud-native platforms, digital asset services, or internet-facing APIs, this activity demonstrates how rapidly geopolitical threat actors can weaponize newly disclosed vulnerabilities, turning short patching delays into strategic opportunities for long-term access and financial gain. This underscores the need for a behavioral-anomaly-led security posture.

Credit to Nathaniel Jones (VP, Security & AI Strategy, Field CISO) and Mark Turner (Specialist Security Researcher)

Edited by Ryan Traill (Analyst Content Lead)

Appendices

Indicators of Compromise (IoCs)

146.70.192[.]180 – IP Address – Endpoint Associated with Surfshark

References

<https://www.darktrace.com/resources/the-state-of-cybersecurity-in-the-finance-sector>

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.



Written by

Nathaniel Jones

VP, Security & AI Strategy, Field CISO

[Share this post](#)

Latest blogs



[Maduro Arrest Used as a Lure to Deliver Backdoor](#)

[Network](#)

•

[January 9, 2026](#)

[Tara Gould](#)

[Malware Research Lead](#)



Runtime Is Where Cloud Security Really Counts: The Importance of Detection, Forensics and Real-Time Architecture Awareness

Cloud

•

January 13, 2026

Adam Stevens

Senior Director of Product, Cloud | Darktrace