DARKTRACE

2024 Cloud Forensics Threat Report

Contents

Introduction

As cloud technology adoption accelerates, the sophistication and frequency of cloud-focused malware campaigns have surged. Darktrace is excited to present its 2024 Cloud Forensics Threat Report, offering an in-depth look at key discoveries over the past year. This report aims to help security professionals with the insights needed to stay ahead in protecting organizations, based on tactics used by threat actors to compromise environments.

Key Insights

New services exploited for resource hijacking

While resource hijacking has long been an issue for cloud environments, this year we identified new services being targeted. Cryptominers are still highly prevalent in web environments across multiple cloud platforms, with XMRig miner still being the most popular. In one campaign, vulnerable Cloudflare WARP instances were targeted as initial access to deploy XMRig. In addition to Cloudflare WARP, 2024 saw the first reported exploitation of Selenium Grid to deliver a cryptominer. Previously undocumented, the miner "Perfcc" or "Perfctl" was identified, targeting Selenium Grid. Parallel to the Perfcc campaign, we reported a secondary campaign targeting Selenium Grid for proxyjacking.

Misconfigured services continue to be a target rich environment

Following trends from previous years, misconfigured cloud instances continue to be targeted. These services include Docker, Redis, Apache Hadoop YARN, and Confluence, with attacks ranging from cryptojacking to credential stealing. One such campaign identified was Spinning YARN, a wide spanning cloud campaign delivering malware to deploy cryptominers and spread to other servers. On a similar theme, another campaign, Commando Cat was detailed this year by Darktrace's research team, in which exposed Docker API endpoints were exploited to deliver a backdoor, cryptominer and credential stealer.

Rust and Golang are still favored by malware developers

Following trends from the past few years, Rust and Golang are continuing to increase in popularity for malware developers. Using these languages is a good choice for threat actors due to higher evasion, cross compatibility, better performance, and making analysis more challenging - specifically Rust. In addition to the increase of Rust and Golang malware, the targeting of macOS with Rust and Golang has increased significantly over the past year. Two examples discovered were Cthulhu Stealer, written in Golang and the Meeten campaign, implemented in Rust.

About the Darktrace Research Team

Threat Intelligence

Darktrace's research team acquires threat intelligence data from a variety of custom sources, such as honeypots, OSINT (Open Source Intelligence), and client engagements. Frequently, work performed to establish such data sources contributes to the wider engineering effort, as these are typically complex engineering projects in themselves.

In addition to these custom sources, our threat intelligence researchers conduct routine monitoring of public malware and threat intelligence repositories. When new threats are discovered, they are analyzed to understand their behaviors and indicators. These insights are then translated into detections that are built into the Darktrace platform, as well as reporting for the community at large.

By constantly updating and incorporating new threat intelligence, we not only strengthens the security posture of our customers, but also empowers the wider security community. Through this collaborative effort, the team strives to disseminate knowledge of the cloud threat landscape, enabling organizations and security professionals to better defend against evolving threats.

Malware Analysis

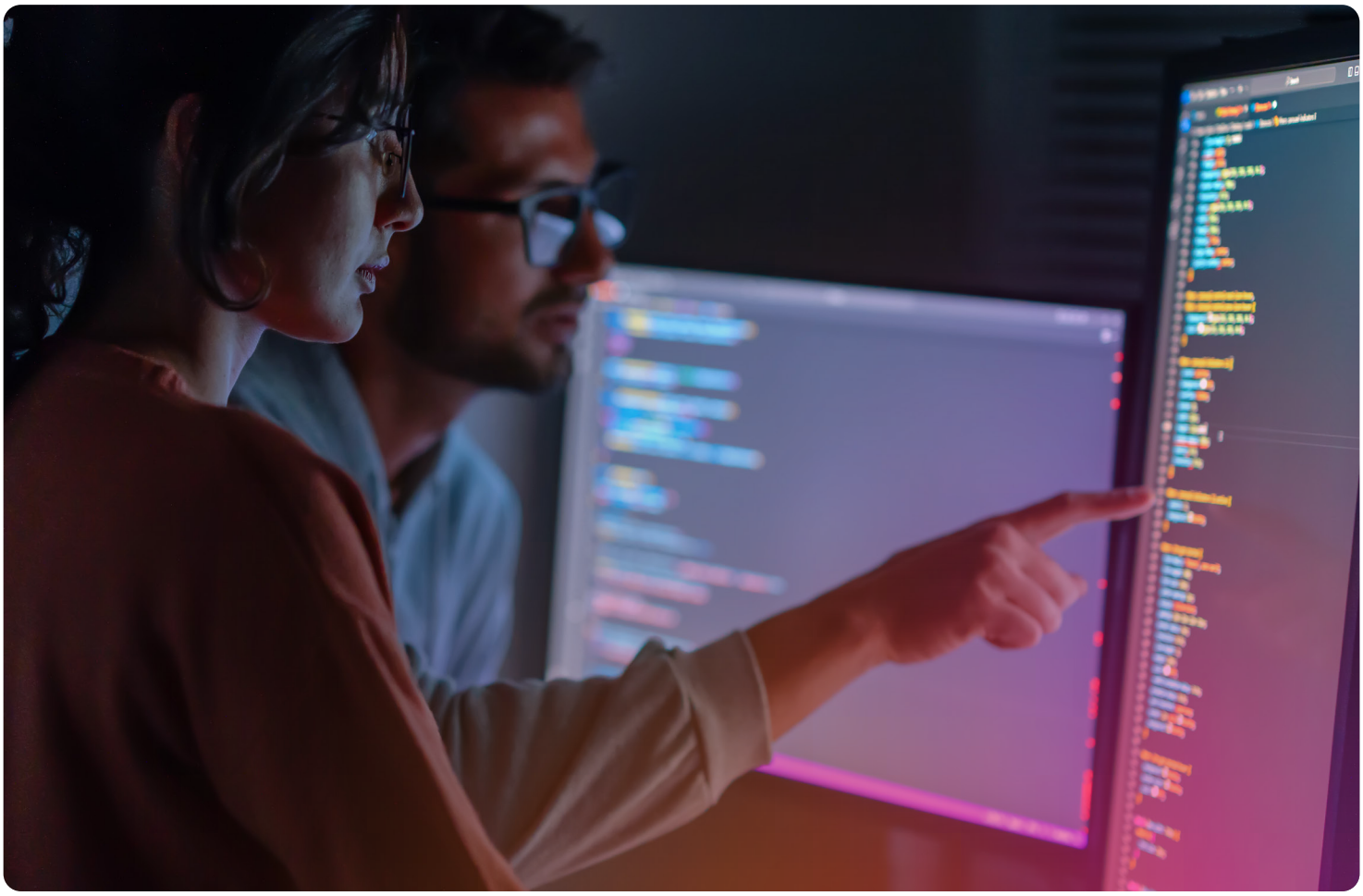
Once threat intelligence has been conducted, malware samples are quickly triaged and any novel malware is analyzed using a combination of off-the-shelf and custom tooling. This typically begins with an initial triage from an analyst. If any interesting Tactics, Techniques, and Procedures (TTPs) or attributes are observed in the sample in question, malware analysts will move on to static and dynamic analysis using various tools to disassemble and debug the code.

Malware samples or campaigns targeting cloud environments with a clear cloud focus are of particular importance to our customers. However, we also investigate any novel malware campaigns, including those targeting Windows, *nix environments. Any such samples are analyzed in-depth and their behaviors and indicators are documented and published for use by the broader security community, with detections added to the Darktrace Platform.

Darktrace / Forensic Acquisition & Investigation supports malware detection through the use of pattern matching technologies such as YARA. The platform also has its own proprietary behavioral detection mechanism, allowing analysts to define malicious behaviors of both malware and human adversaries. Threat intelligence research directly informs the creation of detections for these technologies, allowing Darktrace to alert users when such threats are discovered during evidence processing.

The task of detection engineering extends beyond the mere creation of detection rules; the team is also responsible for ensuring the ongoing effectiveness and relevance of detections as complex malware campaigns and attack patterns evolve. Darktrace detection rules undergo continuous revisions to adapt to the evolving threat landscape. In addition, rigorous testing mechanisms are implemented to minimize false positives and identify any potential regressions.

This aspect of the platform holds immense significance, as solid detection engineering is paramount to providing users with the ability to quickly pivot an investigation based on key malicious activity and gain an in-depth understanding of cyber security incidents.



Research and Development

The Darktrace research team works closely with the Forensic Acquisition & Investigation engineering team to seamlessly integrate threat intelligence into the product. By leveraging their expertise in cloud security and advanced programming, the team rapidly prototypes new features and enhancements based on emerging threat intelligence and evolving Tactics, Techniques, and Procedures (TTPs) used by cloud threat actors.

One key example of an engineering project shaped by our research is VARC (Volatile Artifact Collector), a free tool designed to streamline volatile data collection for the security community. Beyond tool development, the team also maintains proprietary detection rulesets, which define malware behaviors and attack patterns. These rules are integrated into the platform to detect malicious activity, serving as critical pivot points for analysts during investigations.

Detection engineering within Darktrace / Forensic Acquisition & Investigation isn't just creating detection rules. The team ensures ongoing effectiveness by continuously refining detections in response to sophisticated malware campaigns and evolving attack techniques. Detection rules undergo regular updates, rigorous testing, and validation to minimize false positives and prevent regressions. This continuous refinement is crucial, as strong detection engineering empowers users to swiftly identify malicious activity, pivot investigations effectively, and gain deeper insights into cybersecurity incidents.

Notable Campaigns from 2024

Over the past year, our research has provided critical insights into the evolving threat landscape, uncovering emerging attack techniques, vulnerabilities, and adversary behaviors. Through a series of in-depth research and technical analyses, we have identified multiple campaigns ranging from sophisticated cloud-based intrusions to novel malware.

▪ Campaign #1

Perfcc Miner Targeting Selenium Grid

In August 2024, the research team set up a Selenium Grid honeypot based on research published by Wiz. Selenium Grid, widely used for web browser testing, becomes vulnerable when improperly configured. From the Selenium Grid honeypot, we identified two malicious campaigns exploiting misconfigured Selenium Grid instances, which lack authentication by default, to deploy cryptomining and proxyjacking malware. In these attacks, threat actors inject base64-encoded Python scripts via the "goog:chromeOptions" configuration, leading to the installation of a sophisticated cryptominer named "perfcc." This malware utilizes the XMRig mining tool and employs techniques like UPX packing and Shell Script Compiler (SHC) compilation to evade detection.

▪ Campaign #2

Cthulhu Stealer

In August 2024, we identified "Cthulhu Stealer", a macOS-targeting malware campaign. The malware was distributed as a disk image (DMG) masquerading as legitimate software. Upon installation, it prompts users via osascript to enter their system and MetaMask passwords, which are then stored in /Users/Shared/NW. The malware employs Chainbreak to extract Keychain passwords and compiles the stolen data into a zip archive for exfiltration. It also gathers system information, including IP addresses. Notably, Cthulhu Stealer targets various credentials and cryptocurrency wallets, such as MetaMask, Coinbase, and browser cookies. Its functionality closely mirrors that of "Atomic Stealer", a popular macOS info stealer, suggesting possible code modification. The operators, known as "Cthulhu Team," have marketed the stealer on malware marketplaces and Telegram for $500 per month. However, reports indicate that affiliates have accused the developers of withholding payments, leading to a permanent ban from certain marketplaces. This case underscores the importance of macOS users exercising caution when installing software from unofficial sources, as the platform remains susceptible to sophisticated malware threats.

▪ Campaign #3

Spinning YARN

This was a new malware campaign, dubbed "Spinning YARN" targeting misconfigured Linux servers running Apache Hadoop YARN, Docker, Confluence, and Redis. Attackers employed four novel Golang-based tools to automate the discovery and exploitation of these services, leveraging common misconfigurations and known vulnerabilities, such as CVE-2022-26134 in Confluence, to achieve remote code execution. Upon gaining access, they deployed shell scripts to install cryptocurrency miners, establish reverse shells using the Platypus utility, and maintain persistence through user-mode rootkits that conceal malicious processes. The tactics observed share similarities with previous attacks attributed to groups like TeamTNT and WatchDog, emphasizing the need for organizations to secure their web-facing services against such threats.

▪ Campaign #4

New Evolutions in P2PInfect

We observed significant developments in the P2Pinfect malware, a Rust-based botnet previously noted for its dormancy during 2024. Initially, P2Pinfect propagated primarily through Redis and limited SSH spreading without executing any specific payload. Recent updates have introduced ransomware and cryptomining functionalities, marking a shift towards more aggressive and financially motivated operations. The malware now actively encrypts files on compromised systems and deploys cryptocurrency miners, enhancing its impact and threat level. This evolution underscores the importance of securing services like Redis and SSH to prevent exploitation by such sophisticated threats.

▪ Campaign #5

Meeten Stealer

In December of 2024, we uncovered a sophisticated scam targeting Web3 professionals, involving the distribution of the "Realst" information stealer malware on both macOS and Windows platforms. The threat actors established fake companies operating under the name "Meetio" with AI-generated websites and social media profiles to enhance credibility. The threat actors initiate contact through platforms like Telegram, sometimes impersonating known associates of the target, to propose business opportunities and schedule video calls. Victims are then directed to download a purported meeting application from the fraudulent website, which is actually Realst info stealer. Notably, these malicious websites also contain JavaScript designed to steal cryptocurrency stored in web browsers, even before any malware is installed. This campaign underscores the importance of verifying the authenticity of unsolicited communications and exercising caution when downloading software from unfamiliar sources.

▪ Campaign #6

New Linux Variant of Cerber Ransomware

We identified a Linux variant of the Cerber ransomware, which has been deployed onto servers running the Confluence application by exploiting the CVE-2023-22518 vulnerability. This vulnerability allows attackers to reset the Confluence application and create a new administrator account via an unprotected configuration restore endpoint. Once access is gained, attackers install a web shell to execute arbitrary commands, leading to the download and execution of the Cerber ransomware payload. The primary payload, written in C++ and packed with UPX, connects to a command-and-control server to retrieve additional components, including a log checker and the main ransomware module. The ransomware encrypts files on the system, particularly targeting data associated with the Confluence application. This campaign underscores the importance of promptly applying security patches and ensuring proper configuration to prevent unauthorized access.

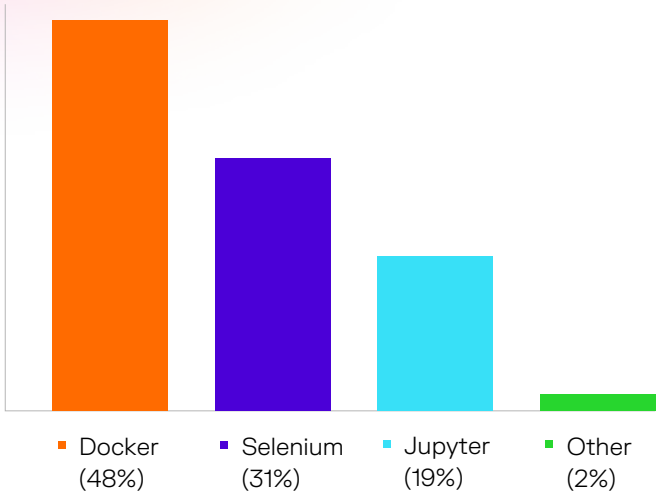
Key Technical Findings

Background

Darktrace maintains honeypot infrastructure across four geographically diverse regions to gather cloud attacker telemetry. Initially, our honeypots relied on simulated services, similar to those in T-Mobile's open-source Tpot project. While these solutions enable the rapid deployment of realistic honeypots for various services, their low-interaction nature eventually became a constraint.

Darktrace also maintains Cloudypots, an advanced honeypot system designed to uncover novel attack techniques targeting cloud services. Unlike traditional low-interaction honeypots, Cloudypots leverages OpenStack to deploy high-interaction virtual machines (VMs), providing deeper insights into attack lifecycles. This approach enables the safe and efficient emulation of vulnerable services, such as GitLab and Confluence, which were previously challenging to honeypot. By utilizing Open Container Initiative (OCI) images within these VMs, Cloudypots can securely run untrusted code, enhancing the detection and analysis of emerging threats in cloud environments. First deployed in 2023, Darktrace still uses and maintains Cloudypots, adding services to honeypot such as Jenkins and Selenium Grid this year.

▪ **Docker Decreases As The Most Targeted Honeypot**



Over the course of 2024, the top three honeypot attacks were Docker, Selenium Grid, and Jupyter. The IP targeting the most was a Korean IP targeting Selenium Grid, with China being the most prevalent IP. However these may not provide much context due to the common use of VPNs.

▪ **Top 20 IPs and Countries Witnessed in Our Honeypot Network**

IP Address	Number of Views in Honeypot	Country of Origin
211.234.111.116	578	KR
152.53.32.152	396	DE
156.238.252.213	318	US
191.243.199.74	73	BR
125.88.207.126	68	CN
142.93.188.216	54	US
60.191.137.103	54	CN
113.200.98.17	53	CN
171.15.113.20	43	CN
36.99.163.23	37	CN
122.227.52.58	36	CN
221.130.29.85	30	CN
165.232.152.69	29	US
223.247.154.13	29	CN
101.91.148.86	28	CN
63.141.252.2	28	US
80.114.121.175x	28	NL
124.74.110.230	25	CN
220.181.1.163	24	CN
88.173.200.156	24	FR

Observations

Threat actors are continuing to target new services

Threat actors are increasingly exploiting web-facing services to gain initial access to cloud environments. Attackers have targeted services such as Docker, Redis, Kubernetes, and Jupyter, and continue to do so. However recent activity indicates an expansion into additional services, including Jenkins and Selenium Grid. This shift highlights the evolving tactics of threat actors as they seek new entry points to compromise cloud environments.

During these campaigns, threat actors typically are looking for misconfigured services that can be exploited for credential stealing, cryptomining and to gain backdoor access. Misconfigured services can be as a result of default configurations in a platform, or by the organisation themselves.

Following publications of Selenium Grid being exploited, the research team set up a honeypot to observe for any malicious activity. Shortly after the honeypot was deployed, we observed two campaigns targeting Selenium Grid. In the first campaign, a previously undocumented cryptominer was deployed named “Perfcc” or “Perfctl”. At the same time, a second campaign exploited the misconfigured service to install a reverse shell used to set up a proxyjacker. As Selenium Grid is misconfigured by default, the service is an easy target for threat actors.

Spinning YARN a wide spanning Linux malware campaign

Spinning YARN was a new campaign that was discovered by the research team in early 2024. This campaign targets a multitude of services, including:

- Apache Hadoop
- Confluence
- Docker
- Redis

For Docker and Hadoop, the attack relies on the services being exposed without authentication in order to compromise them, by spawning malicious Docker containers or Hadoop tasks. Similarly for Redis, it relies on them being open to the internet and abuses the configuration to add a malicious cron job. Confluence however makes use of CVE-2022-26134, an unauthenticated arbitrary code execution vulnerability.

This is an unprecedented number of initial access vectors in one payload, with almost all other campaigns observed using typically two at most. This versatility greatly increases the number of hosts the Spinning YARN can compromise.

Spinning Yarn also makes use of four Go binaries, including an open-source shell called Platypus, as well as several scripts. The campaign features advanced techniques such as a user mode rootkit, used to hide the shell and the miner deployed. You can read more about Spinning YARN here.

Rust and Golang malware continues to increase

Programming languages Rust and Golang have been increasing in the past few years as they provide significant advantages for malware developers. One of their key benefits is the ability to compile code for multiple operating systems and architectures without requiring direct access to those systems, along with low detection rates. This flexibility enables threat actors to create cross-platform malware more efficiently thus increasing the amount of targets.

The majority of malware analyzed in 2024 was written in Rust or Golang. In addition to threats targeting cloud environments, we identified multiple campaigns targeting macOS and Windows that were implemented in Golang and Rust. One example of this was Cthulhu Stealer, a Golang information stealer that targeted macOS users to steal crypto wallets. In a second campaign, we identified a campaign named Meeten targeting both macOS and Windows with the Rust info stealer Realst.

In the Cloud, we documented updates to the P2PInfect botnet. Also written in Rust, the malware targeted Redis servers spreading as a worm with an SSH password sprayer. Additionally, the botnet also dropped a cryptominer, rootkit and ransomware.

Conclusions & recommendations

As organizations increasingly adopt cloud technologies, it is critical that security teams reassess their internal tools and approaches in order to ensure their ability to properly identify, investigate, and respond to emerging cloud threats. With this report, we aim to help security professionals gain a better understanding of how attackers are exploiting cloud-based technologies, and in turn, enable them to build a more robust internal security program.

Here are a few key recommendations we believe should be considered by security teams to ensure effective and efficient incident handling in the cloud:

▪ Recommendation #1

Establish a policy of regularly reviewing the security of deployed services in your cloud estate, particularly if they include the services described here.

▪ Recommendation #2

Consider reducing your attack surface by only deploying public-facing services when necessary and making use of networking security features (security groups, etc.) that your CSP provides.

▪ Recommendation #3

Ensure you are collecting and aggregating logs from both your CSP's control plane and for the individual services you intend to run in your account. Establish periodic review and automated alerting for anomalies found in these log sources.

About Darktrace

Darktrace has been building a new model for cybersecurity since 2013. Founded by global experts in AI and cyber defense, we knew that with the advent of AI, companies would need AI cybersecurity to move faster, to stay ahead of threats, and to ignite innovation. Today, Darktrace is a global leader in cybersecurity AI, delivering the essential cybersecurity platform to protect organizations today and for an ever-changing future.

In 2025, Darktrace brought to the market the first truly automated cloud forensics and incident response solution. The platform leverages the scale and speed of the cloud to automate the end-to-end incident response process – from data capture and processing to investigation and response. This enables security teams to gain immediate access to forensic-level data in multi-cloud, container, and serverless environments.

Evidence items extracted from cloud-provider logs, disk, memory and more, are processed in parallel to drastically reduce time to investigation. The platform was built to empower security analysts of all levels by automatically highlighting the most important events related to an incident, including its root cause, scope, and impact.

This product forms part of Darktrace's ActiveAI Security Platform, which provides preemptive visibility into security posture, real-time detection, and autonomous response to known and unknown threats, across the cloud, network, email, OT, endpoints and more.

If you're interested in learning more, contact us to get a demo.

Request a demo →

About Darktrace

Darktrace is a global leader in AI for 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 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://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