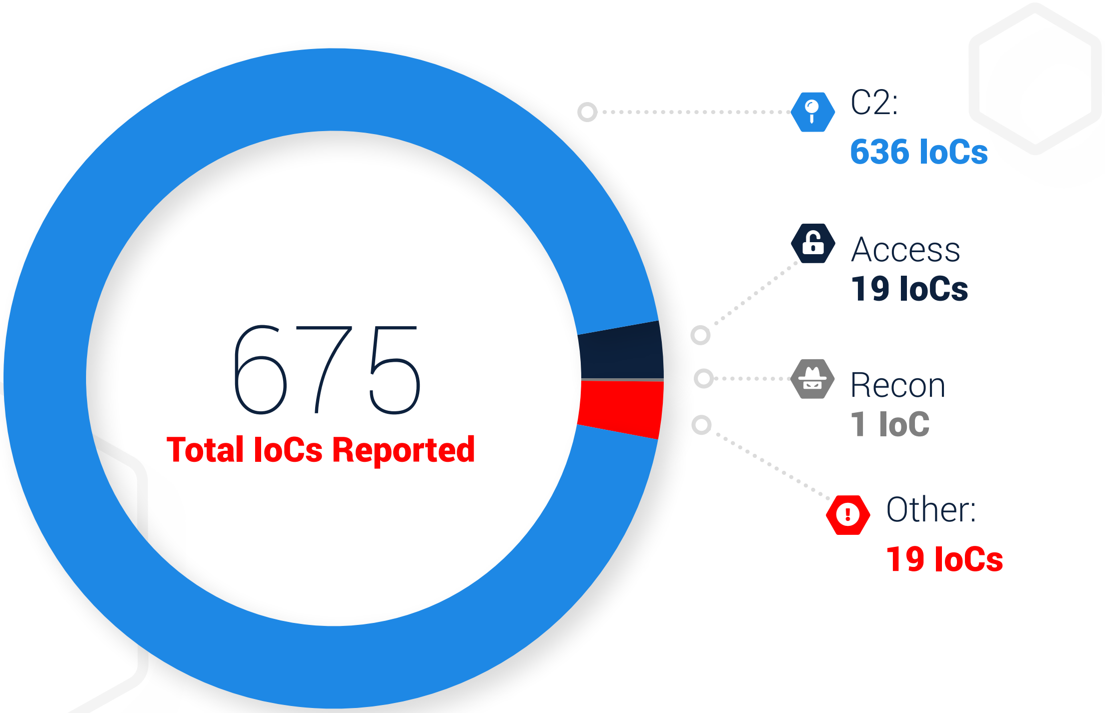
Edition #17: May 2021

# IronNet:
# Threat Intelligence Brief

## Top Observed Threats from IronNet Collective Defense Community
## April 1 – April 30, 2021

# Significant **Community Findings**

This month, IronDefense deployed across IronDome participants' environments identified a number of network behavioral anomalies that were rated as Suspicious or Malicious by IronNet and/or participant analysts.



# Recent Indicators of Compromise

| Domain/IP | Rating | Analyst Insight |
|---|---|---|
| ifollc-onedrive[.]com | MALICIOUS | This domain hosts a phishing site. The URL ifollc-onedrive[.]com/next.php was one of multiple referred URLs that resulted from a user clicking a link in a spearphishing email. If this domain is seen in your network, ensure no data was extracted from the endpoint and block appropriately. |
| smittylatimer[.]com | MALICIOUS | This is an uncategorized website that has been associated with phishing and malware. OSINT indicates with high confidence that the site is Malicious. |
| stats-dss2145-serving[.]com | SUSPICIOUS | The user may be redirected to this domain via another clickbait site posing as a dating service. Ensure connections to this site are blocked and investigate as needed. |
| bigbinnd[.]info | SUSPICIOUS | This domain will encourage the user to install unwanted programs and extensions. We recommend blocking the domain. |
| securecloud-smlnd[.]com | SUSPICIOUS | This site serves as a clickbait ad-redirector. The domain presents a JavaScript to the client browser that then redirects the user to a site enticing the user to click on a prize, potentially downloading riskware. If seen in your network, ensure the domain is blocked. |
| straitreedanimated[.]com | SUSPICIOUS | This domain is related to TerraClicks; the user likely arrived here via redirect. If seen in your network, scan for adware and remove any unwanted software on the endpoint. |
| globadocuments[.]com | SUSPICIOUS | This is an online store that sells fake IDs, passports, and other identification materials. This site violates most corporate acceptable use policies and laws in numerous jurisdictions. |
| realdocument[.]online | SUSPICIOUS | This is an online store that sells fake IDs, passports, and other identification materials. This site violates most corporate acceptable use policies and laws in numerous jurisdictions. |
| ngrok[.]io | SUSPICIOUS | This endpoint may have been hosting or serving phishing content. If seen in your network, investigate the network traffic and block the fully-qualified domain name (FQDN). |
| modificationdispatch[.]com | SUSPICIOUS | This domain hosts TerraClicks-based redirects. If seen in your network, block the domain and investigate any redirects. |

# **Threat Rules** Developed

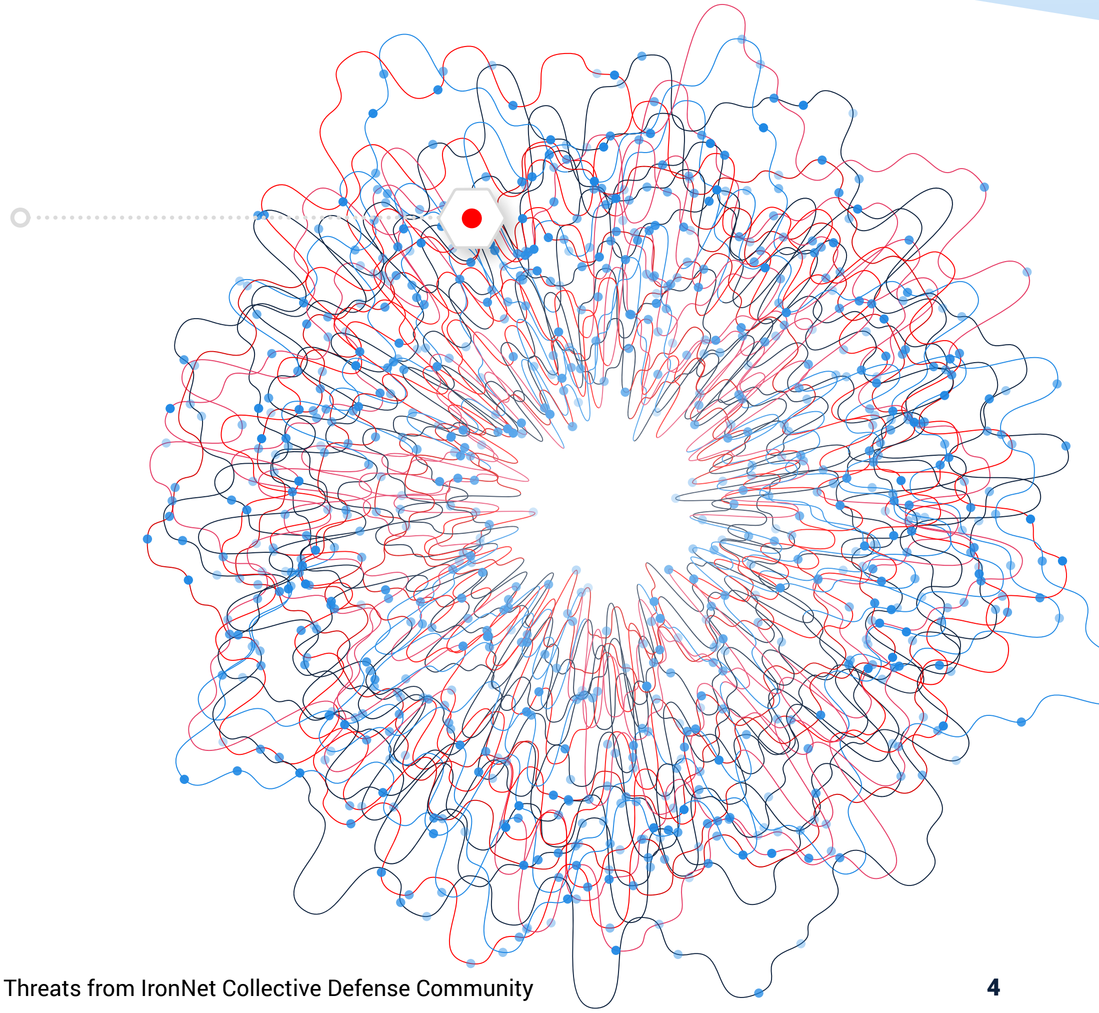
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants. These TIRs are continually distributed to each IronDefense deployment as they are created, ensuring that customers receive the most up-to-date detection capabilities.

5,284

**Threat Intel Rules Developed This Month**

**208,058**

Threat Intel Rules Developed to Date



# THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise identified by the IronNet Threat Research team as associated with phishing or malware delivery. IronNet threat intelligence analysts also routinely monitor research distributed by the wider cybersecurity community and ensure rules are created for documented indicators. Some examples of this month's research include indicators associated with the following threats and campaigns:

- Malware delivery domains for Gafgyt, AgentTesla, and Dridex malware
- Command and control (C2) domains for FluBot malware, which targets Android smartphones
- IoCs for the new Iranian SideTwist malware
- C2 domains for Locky ransomware
- Malware delivery domains for Gafgyt, AgentTesla, and Morila malware
- C2 domains for DarkComet malware, a Remote Access Trojan (RAT) and backdoor
- C2 domains for Neutrino malware
- Malware delivery domains for Gafgyt, AgentTesla, and Convagent malware
- C2 domains for FormBook malware, an infostealer with a new variant deployed in phishing attacks
- IoCs indicating FluBot infection
- C2 domains for Nemucod ransomware
- Malware delivery domains for Gafgyt and DarkComet malware
- C2 domains for Nivdort, a data-stealing Trojan
- IoCs surrounding the NAIKON campaign

**Rating alerts diminishes “alert fatigue” for your SOC.**

# This Month in the IronDome

## The IronDefense network detection and response solution detects behavior-based anomalies as follows:

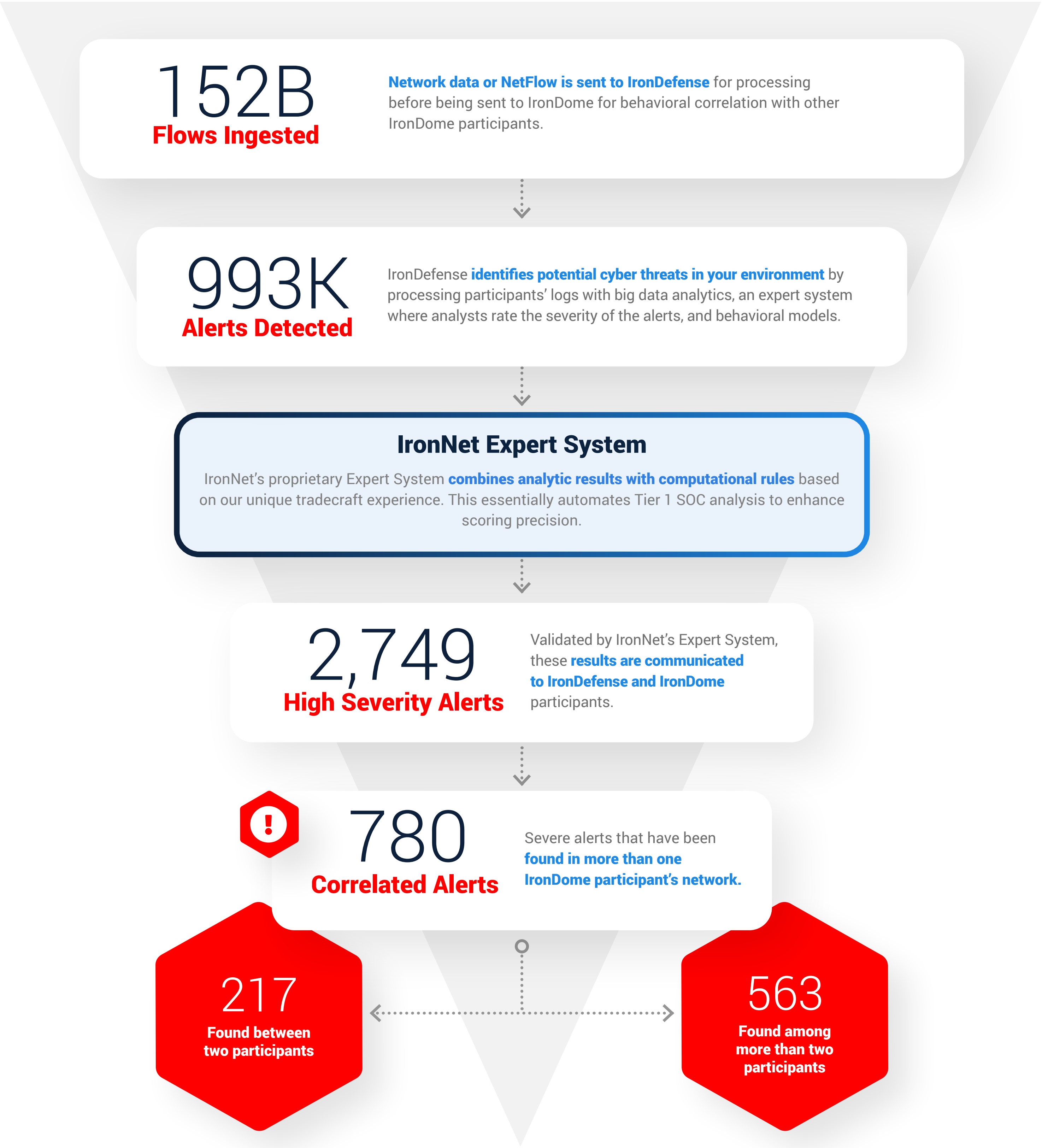
- The NetFlow or enriched network metadata (“IronFlows”) collected by IronNet sensors is analyzed by a participating enterprise’s IronDefense instance before being sent to IronDome for higher order analysis and correlation with other IronDome members.

- IronNet’s IronDome Collective Defense platform delivers a unique ability to correlate patterns of behavior across IronDome participants within an enterprise’s business ecosystem, industry sector, or region.

This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses.

On the following page is a snapshot of this month’s alerts.

# Monthly Alert Snapshot



**152B**
**Flows Ingested**

**Network data or NetFlow is sent to IronDefense** for processing before being sent to IronDome for behavioral correlation with other IronDome participants.

**993K**
**Alerts Detected**

IronDefense **identifies potential cyber threats in your environment** by processing participants' logs with big data analytics, an expert system where analysts rate the severity of the alerts, and behavioral models.

## IronNet Expert System

IronNet's proprietary Expert System **combines analytic results with computational rules** based on our unique tradecraft experience. This essentially automates Tier 1 SOC analysis to enhance scoring precision.

**2,749**
**High Severity Alerts**

Validated by IronNet's Expert System, these **results are communicated to IronDefense and IronDome** participants.

**780**
**Correlated Alerts**

Severe alerts that have been **found in more than one IronDome participant's network.**

**217**
**Found between two participants**

**563**
**Found among more than two participants**

# Tracking **Industry Threats**

## IcedID Malware

First detected in 2017, the IcedID info-stealing malware is a modular banking Trojan that can be used to steal credentials and financial information as well as move laterally through target networks to compromise additional systems and deploy second-stage malware payloads, such as Trickbot, Qakbot, and Ryuk ransomware. In April 2021, the Microsoft 365 Defender Threat Intelligence Team detected new behavior in a campaign that delivers the IcedID malware, noting the campaign as highly evasive due to the threat actors' abuse of legitimate infrastructure to bypass protections.

This phishing campaign has found a way to circumvent CAPTCHA protections using emails generated by the contact forms on company websites to flood enterprises with seemingly legitimate phishing emails. Victims receive a company contact form response email containing fake legal threats and a link to a Google page (sites.google[.]com) that requires recipients to sign in with their Google credentials. After the recipient signs in to the page, a ZIP file containing a heavily obfuscated JavaScript is downloaded and executed to drop the IcedID payload and a Cobalt Strike beacon, allowing the attackers to gain remote control of the compromised device. There also appears to be a secondary attack chain, or a backup attack flow, for when the sites.google[.]com page employed in the primary attack chain has been taken down. In this secondary chain, users are redirected to a domain ending in .top while at the same time inadvertently accessing a Google User Content page, which downloads the malicious ZIP file.

These emails appear legitimate as they originate from the victim's own contact form on their website, match what would typically be expected from a real customer interaction or inquiry, and are sent from legitimate, trusted email web servers. Typically, phishing attempts that use a personal or "bad" email address would be blocked. However, due to the added authentication layer of the link requiring victims to sign in with their Google credentials, security detection technologies may fail in recognizing these emails as malicious.

## Codecov Breach

A software supply chain attack targeting customers of the software auditing company Codecov was discovered on April 1st. Codecov's software is used by over 29,000 customers, including Atlassian, The Washington Post, GoDaddy, and Proctor and Gamble. So far, it is unknown how many of these customers were actually affected by the hack.

Codecov provides tools that help developers measure how much of the source code executes during testing in a process known as code coverage, which highlights the potential for undetected bugs that exist in the code. Bash Uploader, Codecov's tool that allows customers to send code coverage reports back to their servers, was accessed by an unauthenticated user and modified without the company's permission. Although this intrusion was first detected by a customer in April, researchers believe that the software supply chain attack first occurred in late January.

The threat actors, who have yet to be identified, were able to alter the Bash Uploader due to an error in Codecov's Docker image creation process that allowed the attackers to extract the credentials required to modify the company's Bash script. In a report released April 15th, Codecov notes that the modified version of the Bash Uploader script could allow for attackers to potentially export information stored in customers' continuous integration (CI) environments. This could include any credentials or keys passed through users' CI runners that would be accessible when the Bash Uploader script was executed; datastores and application code that could be accessed with these credentials or keys; or git remote information of repositories using the Bash Uploaders. Not all IoCs have been released due to the ongoing federal investigation. Additionally, Codecov has hired a third-party forensics company to help determine the scope of the attack and identify customers that may have been compromised.

## Pulse Secure VPN

Mandiant has been tracking 12 malware families related to the exploitation of Pulse Secure VPN devices. The exploits have all been observed in separate investigations, likely indicating they were created by multiple threat actors. APTs have been exploiting Pulse Secure vulnerabilities ranging from previously disclosed CVEs from 2019 to a new CVE from April 2021. In one investigation, the Chinese-backed hacking group UNC2630 was observed using legitimate account credentials harvested from various Pulse Secure VPN login flows to move laterally in compromised environments, maintaining persistence by utilizing modified Pulse Secure binaries and scripts on the VPN device. The malware families enable the attackers to bypass single and multi-factor authentication and establish backdoor access on Pulse Secure VPN devices. Once past the "front door," APTs will immediately employ obfuscation techniques to "live off the land" and remain undetected, highlighting the need for user behavior analytics.

## Prometei Botnet

Unpatched Microsoft Exchange servers are being targeted in a series of cryptomining attacks. Attackers exploit Exchange server flaws to install the China Chopper web shell and gain backdoor access to deploy a cryptomining payload known as Prometei. The main objectives of the Prometei attacks are to deploy the cryptomining payload and spread it to other machines on the network. Prometei ("Prometheus" in Russian) is a multi-modular botnet believed to have been around since 2016 that has recently been upgraded with backdoor capabilities with support for a wide range of commands, including the ability to exfiltrate sensitive data in addition to mining Monero coins. Research suggests that these Prometei attacks are likely not sponsored by a nation-state and are probably financially motivated. Given that many state-sponsored hackers moonlight as cybercriminals to draw in extra income, there is a high possibility that state-sponsored hackers are exploiting the recently discovered Exchange vulnerabilities on the side to make extra money with this skillset.

## Emotet Malware Nuked on April 25

In January, coordinated international law enforcement from the U.S., the U.K., Germany, Canada, and other countries conducted a global operation in which investigators were able to take control of the Emotet botnet's servers and disrupt the malware's operation, taking down the botnet's entire infrastructure from the inside. Emotet, which is known as one of the most dangerous email spam botnets, is often used by threat groups to deploy second-stage malware payloads, such as QBot and Trickbot, on infected machines.

Following the takedown operation, law enforcement pushed an Emotet uninstaller module to infected systems that would automatically uninstall the malware on April 25, 2021. In addition, the FBI removed ProxyLogon web shells from U.S.-based Exchange servers without warning the servers' owners in mid-April. While these kinds of malware removal operations by law enforcement are unprecedented, it is possible we will see more operations such as this in the future.

## Codecov

In early April, a software supply chain attack was discovered targeting the software auditing company Codecov, whose tools are used by over 29,000 customers worldwide. HashiCorp, a notable open-source software tool and infrastructure provider, has recently announced it was the latest company impacted by the attack. The Codecov supply chain attack has reportedly impacted a subset of HashiCorp's Continuous Integration (CI) pipelines, exposing its GPG (GNU Privacy Guard) signing key that it uses to verify software releases. There has been no knowledge to date of any companies or open-source projects observing post-compromise activity by a malicious actor through this supply chain attack vector; however, Codecov customers are taking the initiative and changing all of their credentials and keys as a precaution.

## NAIKON Campaign

In a recent investigation into the abuse of vulnerable legitimate software, Bitdefender Labs uncovered an attack campaign conducted by the threat group NAIKON that ran from at least June 2019 to March 2021. Likely tied to the People's Republic of China (PRC), NAIKON has been active for more than a decade and is known to pursue high-profile targets, such as government agencies and military organizations, specifically in the Asia Pacific (APAC) region.

In its most recent campaign, NAIKON abused legitimate software to side-load malicious payloads, namely the first-stage backdoor RainyDay and the second-stage malware Nebulae. NAIKON deployed the RainyDay backdoor (also known as FoundCore) to perform reconnaissance, upload reverse proxy tools, perform lateral movement, execute password dump tools, and establish persistence. The first-stage malware RainyDay is also used to deploy second-stage payloads, including the Nebulae backdoor, which is believed to be used as a precautionary measure to maintain persistence in case the infection is detected. Nebulae provides the added capabilities of collecting system information, manipulating data, downloading files from the C2 server, executing processes, and more.

Aiming this campaign at military organizations in APAC for purposes of espionage and data exfiltration, NAIKON was able to drop these malicious payloads by exploiting side-loading and DLL (dynamic link library) hijacking vulnerabilities. These payloads impacted legitimate software such as ARO 2012 Tutorial, VirusScan On-Demand Scan Task Properties (McAfee), Sandboxie COM Services, Outlook Item Finder (Microsoft), and Mobile Popup Application. Employing a heavy use of side-loading DLLs, NAIKON plants malicious DLLs in legitimate locations and then executes the legitimate program to load the DLLs, which helps mask their malicious actions under a legitimate, trusted process.

# Why **Collective Defense?**

> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

**This report features threat findings, analysis, and research shared across IronDome**, the industry's first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations so IronDome participants can work together in near-real-time to collaboratively defend against sophisticated cyber adversaries.

# Your Partner in Collective Defense

IronNet's goal is to strengthen Collective Defense by detecting unknown threats using behavior-based analysis, rating these threats to reduce "alert fatigue," and sharing them within the IronDome ecosystem to empower SOC teams across the community to prioritize and accelerate response, and defend better, together.

By working together in this way, we can raise the bar on cybersecurity defense at your enterprise or organization, across sectors at large, and on behalf of nations.

## Learn more about Collective Defense in our eBook.

IronNet

STRONGER AS ONE:

The Case for Collective Defense

**ACCESS THE BOOK →**

IronNet™

IronNet.com