IronNet™

Edition #10: October 2020

IRONLENS

Collective Defense Updates from the **IronDome**

Top Observed Threats from IronNet Collective Defense Community
September 1 – September 30, 2020

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.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of IronNet Cybersecurity, Inc.

Rating alerts diminishes "alert fatigue" for your SOC.

This Month in the IronDome

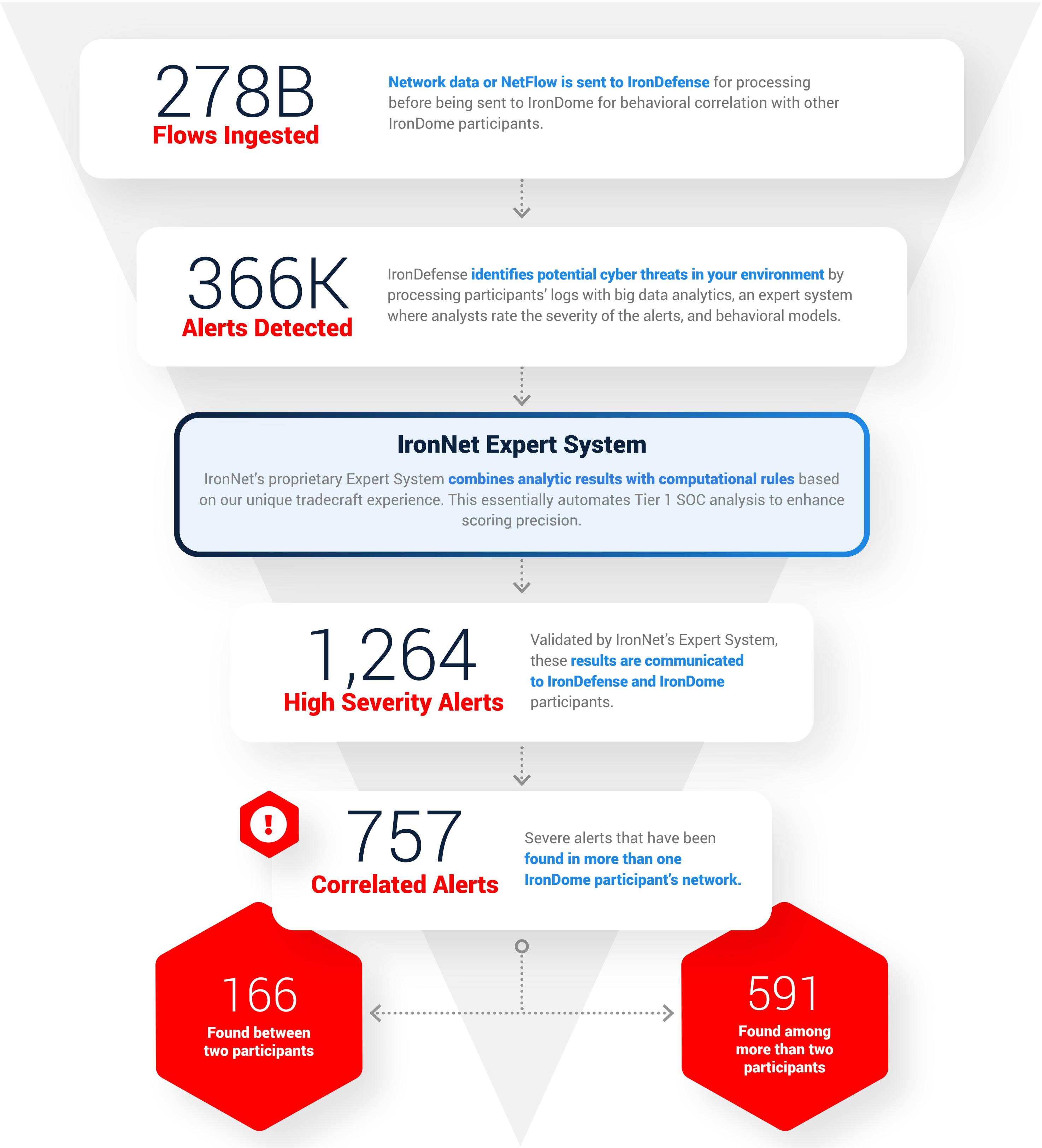
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



278B
Flows Ingested

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

366K
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.

1,264
High Severity Alerts

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

757
Correlated Alerts

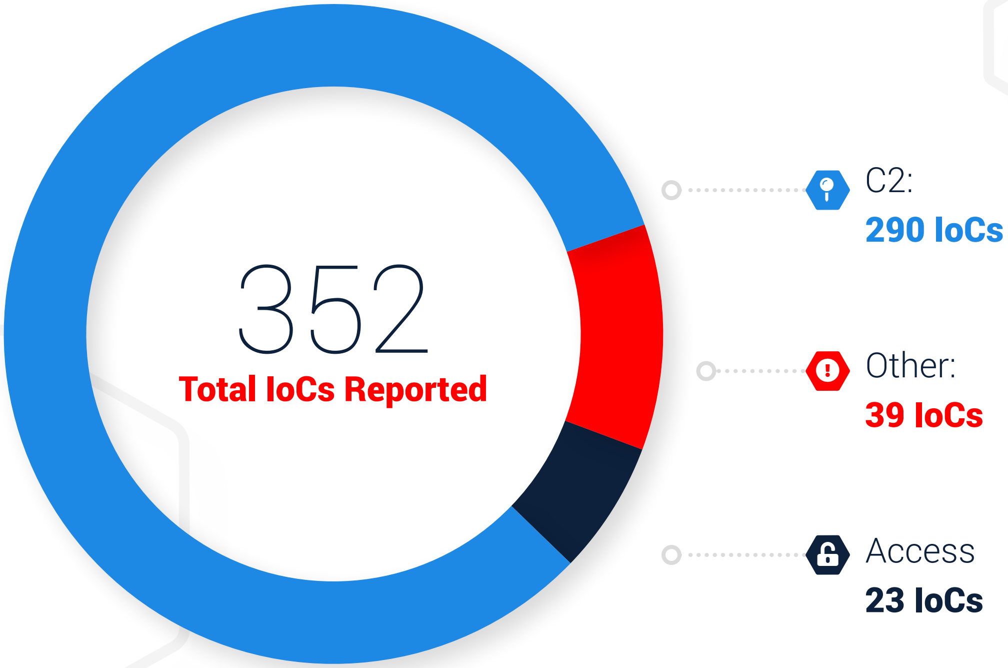
Severe alerts that have been **found in more than one IronDome participant's network.**

166
Found between two participants

591
Found among more than two participants

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
canadalife[.]xyz	MALICIOUS	After researching OSINT resources, the IronNet Hunt team determined this is a phishing website mimicking a suspected Microsoft Outlook web access (OWA) login. Many login credentials were compromised, including credentials from the financial, legal, and real estate sectors. Although the landing page is currently offline, visits to the domain should be investigated for leaked credentials.
hajjumrahinfo[.]com	MALICIOUS	This domain appears to be hosting an active Chase Bank phishing login page. Many of the links and content of the site send the user to the legitimate Chase Bank website. The site appears to be harvesting credentials and security verification information, such as social security number, email address, and login information. If seen in your network, investigate the traffic for loss of personally identifiable information (PII) and block the domain.
yikuvjmme[.]com	MALICIOUS	This domain is a Microsoft phishing login page. At the time of triage, the site appeared to still be active. If seen in your network, investigate the traffic for loss of PII and block the domain.
amastybootstrap[.]host	MALICIOUS	Upon investigation by the IronNet hunt team, amastybootstrap[.]host was hosting a credit card skimming code used by the Indian clothing shop jiofab[.]com. Users should exercise caution when visiting this website as there is a strong possibility their credit card could be compromised.
ihf8rrn[.]com	MALICIOUS	This domain (IP address 185.228.233.214) was involved in a potential Valak-related phishing attempt. A malicious email was sent to a user with a malicious Word document attached.
x-t[.]xyz	MALICIOUS	After researching multiple OSINT resources, the IronNet Hunt team determined that this URL was involved in a phishing campaign targeting Microsoft Office 365 credentials. Phishing emails were sent from co[.]jp domains and the referral URL was t.enews.mercedes-benz.co[.]uk. If seen in your environment, investigate for possible credential loss.
kmart-com[.]com	SUSPICIOUS	This appears to be a spam domain used for click revenue generation. Although the site shows “Copyright Kmart,” there is no affiliation with Kmart in the domain’s Whois. We recommend blocking the domain as well as any domain ending in “-com.com”.
id.rakuten.co.jp.rakutenlkfefcbfsdbdcebe[.]icu	SUSPICIOUS	This domain is associated with phishing activity for Rakuten, an online commerce site. The domain targets login credentials and account information. If traffic is seen in your network, investigate for personally identifiable information (PII) data loss.
creopmzx[.]cf	SUSPICIOUS	This appears to be a phishing domain posing as an Amazon login page. The site appears to be currently offline. If traffic is seen in your network, investigate for PII data loss.
mcdnn[.]me	SUSPICIOUS	This domain hosts a MageCart credit card skimmer. The user visited vedicvaani[.]com, which loaded the MageCart script.

Threat Rules Developed

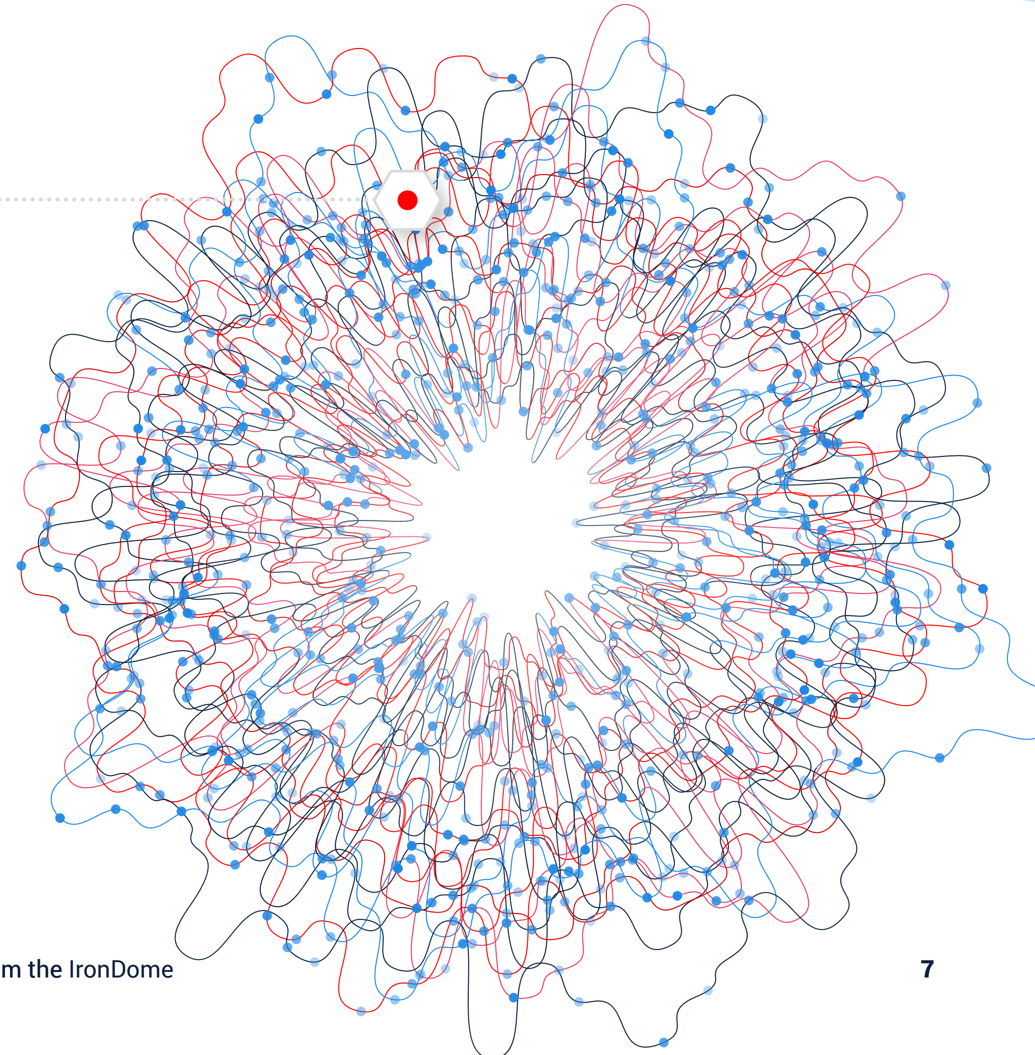
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

15,078

Threat Intel Rules Developed This Month

152,129

Threat Intel Rules Developed to Date



THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise as identified by IronNet analytics including Domain Analysis TLS, Domain Analysis HTTP, Domain Generation Algorithm, DNS Tunneling, Periodic Beaconing HTTP, Phishing HTTPS, TLS Invalid Certificate Chain, and Suspicious File Download. Additionally, rules were created for indicators identified by the IronNet Threat Research team as associated with phishing or malware delivery. Finally, IronNet threat intelligence analysts 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:

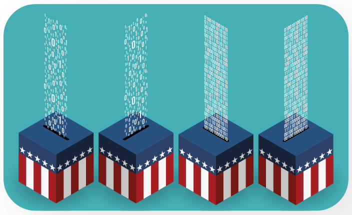
- Various domain-squatting sites targeting major brands such as Facebook, Apple, and Amazon
- Continued targeting of the Tibetan community by the China-linked TA413 group using Sepulcher malware
- A phishing campaign using EPPlus software to create malicious Microsoft Office documents to avoid detection
- The Baka e-commerce skimmer that has been observed on several merchant websites across multiple global regions
- Multiple malvertising campaigns using exploit kits to deliver Smoke Loader and Raccoon Stealer malware
- Indicators associated with the Salfram email phishing campaign leveraging legitimate web hosting platforms that assist in evading detection and mitigation
- Analysis linking the Lucifer, Blacksquid, and Spreadminer cross-platform cryptomining malware families
- An Iran-linked cyber espionage campaign using Windows and Android-based malware to target dissidents and anti-regime organizations
- Exposed Docker servers infected with malicious payloads for cryptomining and Distributed Denial-of-Service (DDoS) attacks
- Identification of a new campaign by APT28 (also known as Fancy Bear or STRONTIUM) targeting NATO member countries using a Delphi version of their Zebrocy malware
- Analysis of recent spam campaigns delivering the URSA/Mispadu banking Trojan to Spanish- and Portuguese-speaking regions
- Details on techniques used by the Jointworm/EvilNum group to penetrate financial services and IT services companies

Tracking **Industry Threats**

Recent Mac OS Malware "Notarized" by Apple

An instance of malicious software targeting Mac users was recently identified by cybersecurity researcher Patrick Wardle. In a blog post, Wardle described a piece of malware that appears to have been legitimately "notarized" by Apple. Apple introduced the notarization process with the release of Mac OS Catalina in late 2019, which requires software developers to submit applications to Apple for review and approval prior to distribution. Such notarization allows for applications to be trusted by the operating system. This incident calls into question the security of the notarization process itself. This particular payload was observed delivering the Shlayer malware, which in turn installs various Mac OS adware.

This example illustrates the importance of defense-in-depth and the pitfalls of over-reliance on individual security controls. Behavioral detection techniques also become particularly valuable for detecting malicious activity when trusted processes are co-opted or compromised, as appears to have occurred in this case.



Multiple Foreign Cyber Actors Targeting U.S. Elections

Last week, Microsoft announced they had detected malicious activity from multiple state-sponsored cyber threat actors targeting the 2020 U.S. presidential campaigns and other related entities. The announcement specifically described activity by Russian, Chinese, and Iranian linked groups. This follows previous announcements by the U.S. Director of National Intelligence and Google describing attempts by these nations to infiltrate U.S. political campaigns or conduct operations designed to influence U.S. voters and undermine confidence in the election process.

Microsoft also released accompanying technical analysis of the Russia-linked Strontium group. This analysis illustrates a shift in the group's preferred tactics, with a move from spearphishing to brute-force and password-spraying attacks. The group has also employed a large-scale anonymization service, undoubtedly designed to make attribution and detection of this activity more difficult. Leveraging advanced behavioral detection capabilities at machine-speed will be key in identifying such campaigns as they continue to grow in scale and sophistication.

U.S. Government Exposes Multiple Chinese Threat Groups

Last week, the United States government released alerts detailing intrusion activity associated with Chinese state-sponsors hackers. The Department of Justice also announced the indictment of five Chinese nationals for criminal network intrusions into over 100 victim companies in the U.S. and abroad. The indictment describes the theft of source code, software code signing certificates, customer data, and business data by a group of individuals with likely ties to the Chinese Ministry of State Security (MSS) operating out of Chengdu. A FLASH notice released by the FBI contained technical details on the tactics, techniques, and procedures (TTP) and command and control infrastructure used by the group.

The Cybersecurity and Infrastructure Security Agency (CISA) also released analysis of TTPs used by the MSS to target U.S. government agencies. CISA maps these TTPs to the MITRE ATT&CK matrix, describing the threat actors' use of commercially available information sources, open-source exploitation tools, and high-profile, publicly identified vulnerabilities. IronDefense implements several analytics designed to detect techniques, such as Network Service Scanning (T1046) and Phishing (T1566), utilized by these actors.

China-linked APT Abuses Azure Cloud for C2

Recent analysis released by Microsoft indicates that threat actors known as GADOLINIUM (also tracked as APT40) have, on multiple occasions, attempted to use cloud-native services within Azure to conduct malicious command and control. While the activity was proactively identified and disrupted, the threat actors appear to have specifically designed malware to abuse proprietary cloud services including the Outlook Task API, OneDrive API, and Microsoft Graph API.

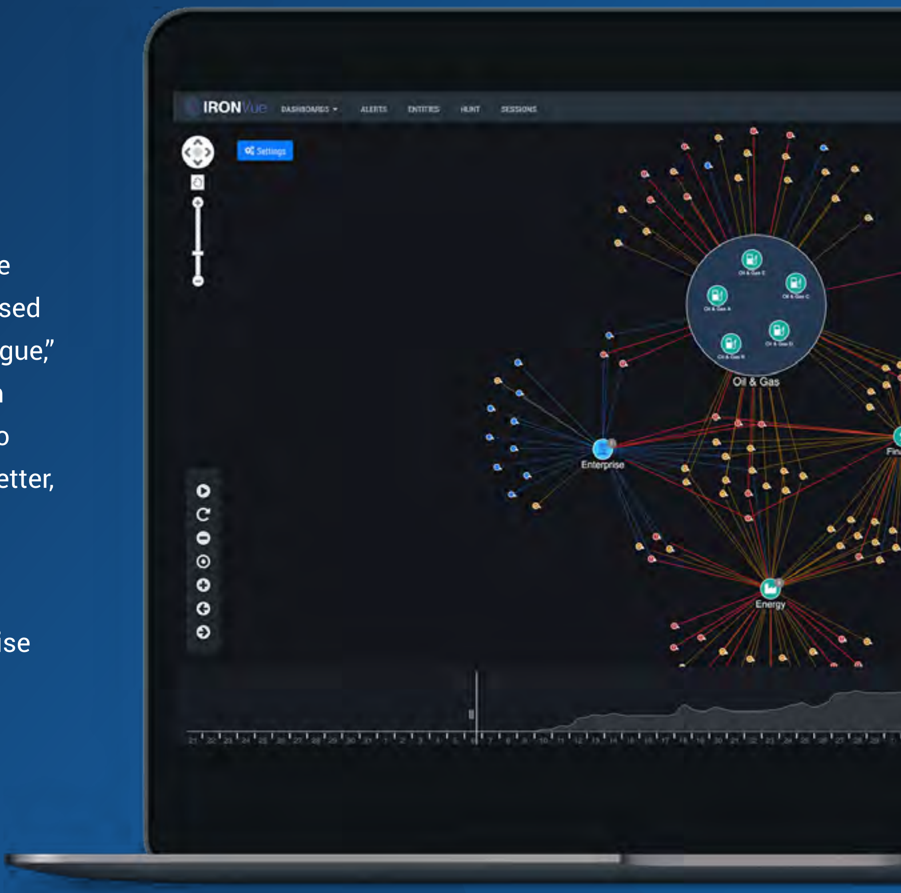
GADOLINIUM has previously been linked to the Chinese Ministry of State Security. The group's historic targets have included the maritime, transportation, and health sectors. Recent activities targeted academic and governmental organizations in the Asia-Pacific region.

Abuses of cloud services such as these are becoming increasingly common threat vectors as more and more organizations take advantage of cloud computing. Cloud-native threats underscore the importance of employing dynamic cross-domain security solutions to identify such malicious behaviors, whether occurring across traditional on-premises network infrastructure, cloud resources, or hybrid solutions.

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 ecosytem 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.

ACCESS THE BOOK →

IronNet

STRONGER AS ONE:

The Case for Collective Defense

IronNet™

IronNet.com