IronNet™

Edition #7: July 2020

IRONLENS

Collective Defense Updates from the **IronDome**

Top Observed Threats from IronNet Collective Defense Community

June 1 – June 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.

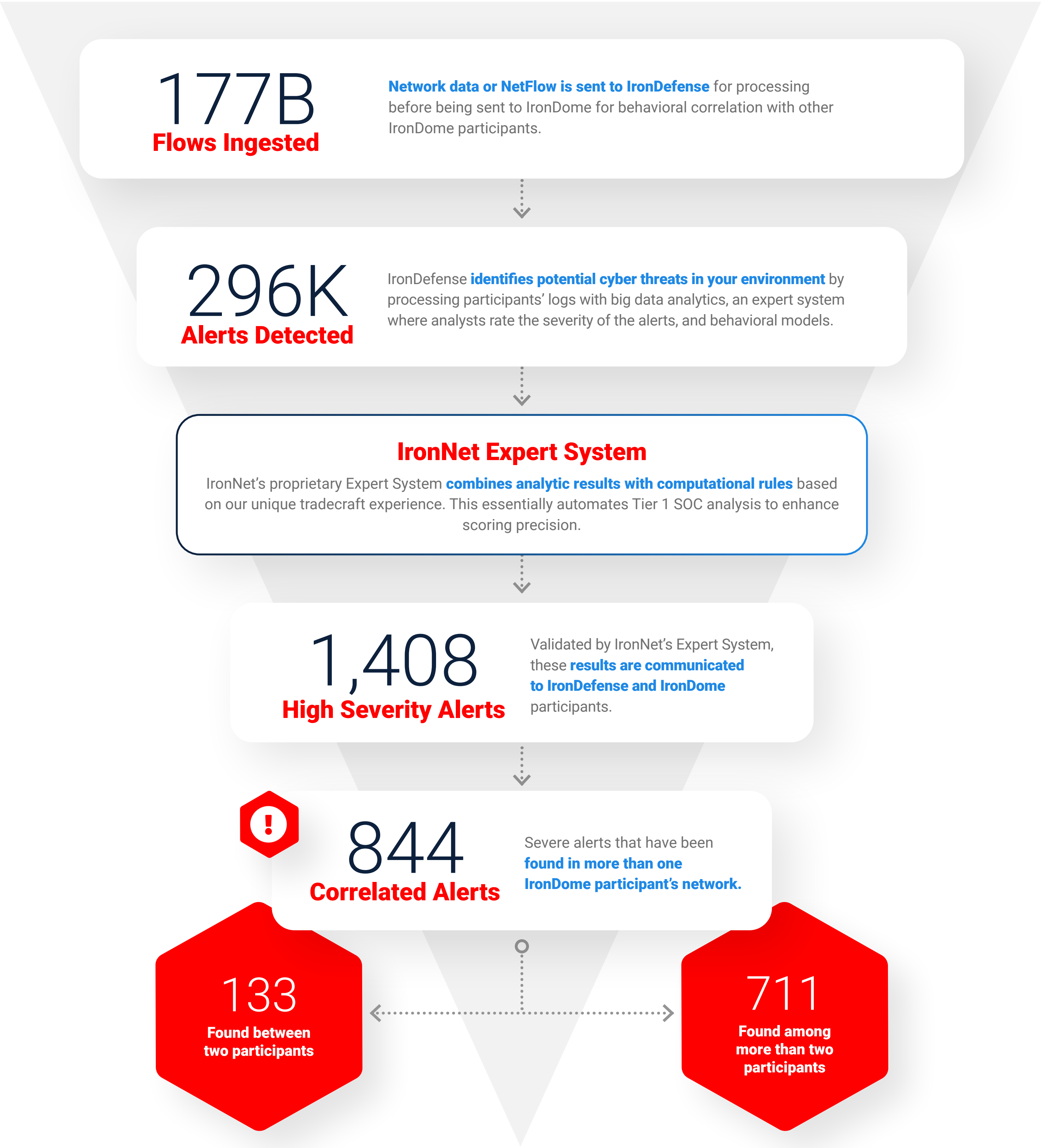
This Month in the IronDome

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.

Monthly Alert Snapshot



177B
Flows Ingested

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

296K
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.

1,408
High Severity Alerts

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

844
Correlated Alerts

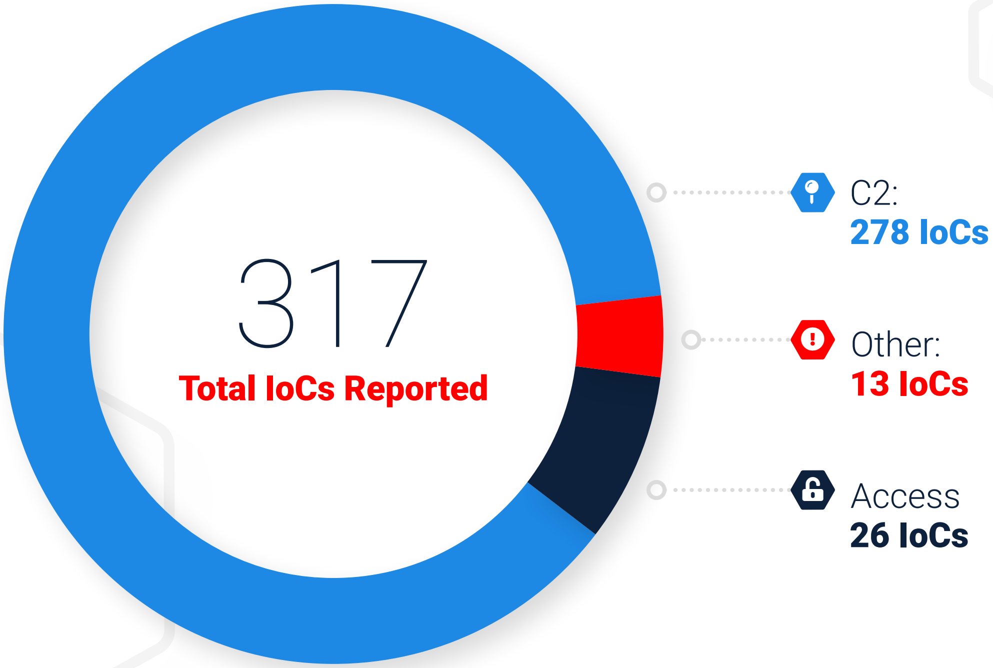
Severe alerts that have been **found in more than one IronDome participant's network.**

133
Found between two participants

711
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
tftpd64[.]com	MALICIOUS	Visiting this website will trigger the download of a ZIP file that has been marked by many OSINT sources as malicious based on the file's MD5 hash. The downloaded ZIP file appears to be a TFTP server. TFTP is a protocol used to transfer files.
www.gocgle-analytics[.]com	MALICIOUS	gocgle-analytics[.]com is a known MageCart credit card skimming domain. Verify that no POST requests to this domain were successful.
latestmobilesprice[.]icu	MALICIOUS	This is a phishing site targeting users' Microsoft Office credentials.
htmlcomponentservice[.]com	MALICIOUS	This domain appears to be hosting active PayPal phishing sites. htmlcomponentservice[.]com could harvest user PII (personally identifiable information) such as account credentials or payment information. If seen in your network traffic, the site should be investigated. IronNet recommends blocking the domain.
dalcar[.]ru	MALICIOUS	The domain dalcar[.]ru/libraries/en/ redirects the user to a page impersonating a Cash App login.
fishingbigstore[.]com	MALICIOUS	This site has been noted by multiple OSINT sources as malware and a Malicious site hosting Emotet payloads.
wofinodo-howe[.]com	MALICIOUS	After researching multiple OSINT resources, IronNet's hunt team determined this domain is Malicious. The site hosts numerous malicious/suspicious executables. This particular activity occurred after the user was redirected from download.app[.]kiwi/getappkiwi.php, which provides a fake Android application package (APK) downloader. Hash: a1ea5446a255f5cc21d0030cd30c94cc65108696070d-b4e00ce51dfc78c9a2a4
minesweeper-online-game[.]info	SUSPICIOUS	Activity from this domain is likely related to the Chrome extension pegppianpcilihojlakkopcgpknflkag, a Minesweeper game playable via a web browser. The extension has access to all data on the browser as well as the capability to modify data. The extension periodically reaches out to the domain to pass browser metrics and analytics. This extension should be categorized as a potentially unwanted Chrome extension.
ischeck[.]xyz	SUSPICIOUS	The effective URL for this domain is checkandgo[.]info, which is notorious for encouraging users to subscribe to browser notifications so the domain can consistently serve ads to the user.
allmygoodlife[.]com	SUSPICIOUS	This domain is Suspicious and network traffic should be investigated for malvertising. This domain has a reputation for redirecting to unwanted sites.

Threat Rules Developed

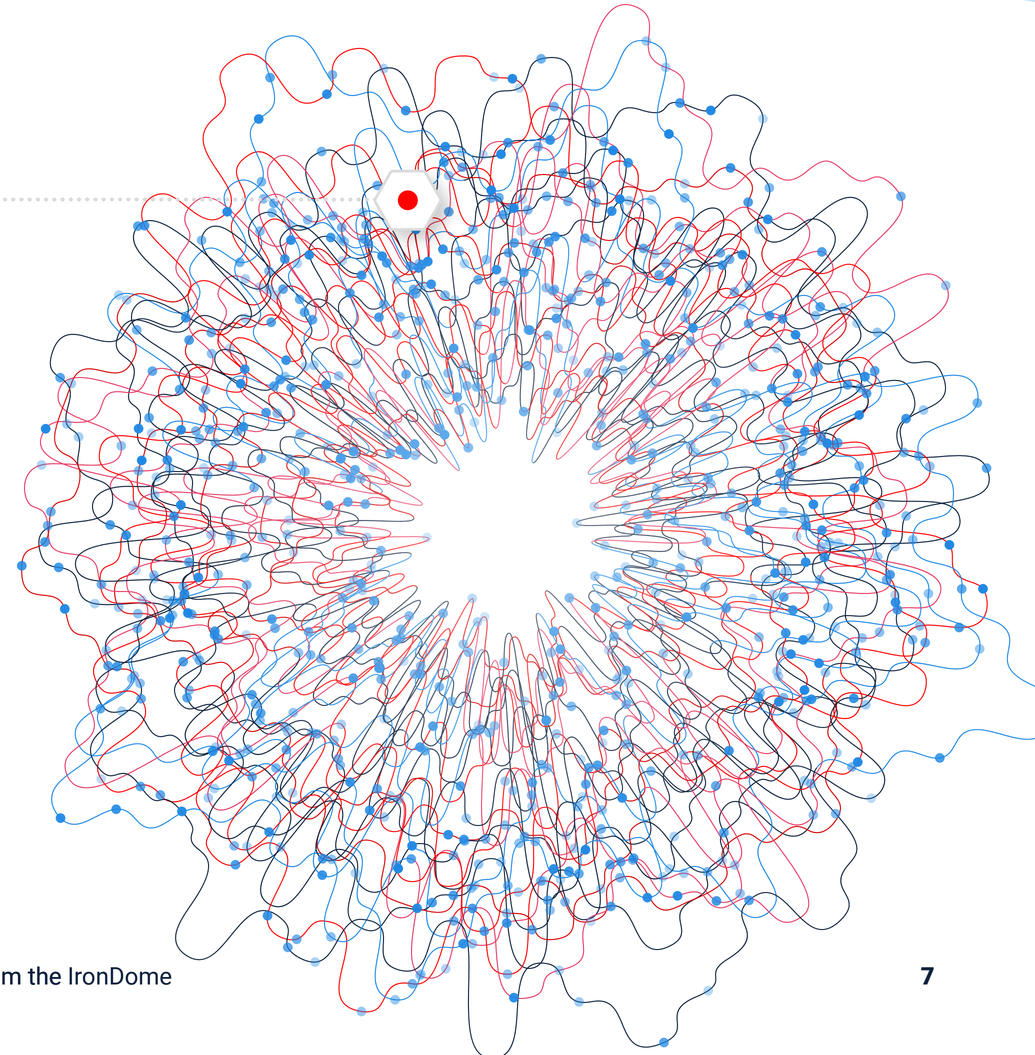
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

8,739

Threat Intel Rules Developed This Month

116,693

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 a variety of IronNet analytics, including Suspicious File Download, Credential Phishing, Periodic Beaconing HTTP, Encrypted Communications, Phishing HTTPS, Domain Analysis TLS, Domain Analysis HTTP, and TLS Invalid Certificate Chain. Additionally, rules were created for indicators identified during malware triage conducted by the IronNet Threat Research team. Finally, IronNet threat intelligence analysts routinely monitor research put out by the wider cybersecurity community and ensure rules are created for documented indicators. Some topics covered by this month's threat research include:

- Valak malware related to command and control domains
- Stealthworker malware performing brute force attacks
- Turla Group's new Kazuar malware, which abuses the SysInternals brand
- APT15-related Ketrum malware attacking government and military entities in India and Europe
- Updated information on Chinese-speaking threat group Cycldek (also known as Goblin Panda and Conimes) and its operations against governments in Southeast Asia
- Analysis of a Polish-language malspam campaign delivering ZLoader malware
- A look at fraudulent Italian company CloudEyE, which provides malware obfuscation services to its cybercriminal customers
- An investigation into a coordinated spyware operation against human rights defenders
- Analysis of a toolset utilized by the InvisiMole Group in late 2019, which targeted Eastern European high-profile organizations in the military sector and diplomatic missions
- Connecting the dots on probable Sandworm infrastructure
- CryCryptor ransomware posing as a Canadian COVID-19 tracing app for Android
- Investigation of newly-uncovered Indicators of Compromise associated with a North Korea-linked Hidden Cobra malware family known as Copperhedge
- A look at a Sodinokibi ransomware campaign designed to identify credit card or point-of-sale software on victim networks

Tracking **Industry Threats**

Maze Ransomware Infects U.S. Military Contractors

The group behind Maze ransomware has continued its steady pace of successfully infiltrating and encrypting files within various enterprise networks. Since April 2020, Maze ransomware has managed to infect several high-profile companies such as Cognizant, the insurance provider Chubb, and Conduent (an IT services company). Recently, it was revealed that the ransomware group infiltrated two companies that handle U.S. military contracts: Westech International and VT San Antonio Aerospace (VT SAA). Westech International is currently contracted to maintain, refit, and overhaul the Minuteman III program. Westech represents a significant portion of the U.S. long-range nuclear arsenal and is a contractor for several other U.S. military branches. VT SAA is contracted to perform maintenance, refits, and overhauls of military aircraft and is also one of the largest firms on the Singaporean exchange. VT SAA has contracts with many governments around the world.In each incident, the threat actor engaged in largescale theft of files from the respective networks prior to conducting the file encryption. This may have provided an opportunity for detection by a behavior-based analytic that looks for unusually large volumes of data transfer coming in or out of a network prior to the files being encrypted. IronDefense's Extreme Rates, Extreme Rates TLS, and Unusual Day analytics all target this type of behavior. Read more about Maze ransomware and how IronNet detects this growing threat.

Details Emerge on Chinese APT Targeting of U.S. Utilities Sector

Newly-published research from Proofpoint has identified a malware family known as FlowCloud. Proofpoint analysts have linked FlowCloud to the LookBack phishing campaigns, which targeted the U.S. utilities sector in summer and fall of 2019. These two campaigns share a number of tactics, including the timeframes they were active, the use of attachment macros in phishing emails, the installation techniques used, and overlapping infrastructure. Like LookBack, the FlowCloud campaign appears to have targeted the utilities sector using well-crafted phishing emails impersonating professional organizations within the industry, such as the American Society of Civil Engineers. The LookBack and FlowCloud campaigns have been attributed to the TA410 group, but Proofpoint researchers also noted similarities to the tactics used by TA429 (also known as APT10). APT10 built a high public profile during this time due to the publication of multiple reports on the group and a related U.S. indictment of Chinese actors. Given this, it is unclear whether the two groups' activities are truly related or whether this was a deliberate attempt by those responsible to plant "false flags" to hide attackers' identities.

Dark Basin (aka Mercenary.Amanda) Hack-for-hire Operation Uncovered

Recent analysis by multiple cybersecurity research groups has detailed the tactics, techniques, and procedures (TTP) utilized by a "hack-for-hire" group operating out of India referred to as Dark Basin or Mercenary.Amanda. Technical evidence has linked this group to the now defunct technology company BellTroX InfoTech Services. The group is accused of conducting cyber espionage against journalists, government officials, non-profit groups, and commercial companies in various industries including the finance, energy, and legal sectors. This discovery illustrates how lucrative it is to mine open source intelligence. The initial seed that started off the investigative chain was the discovery of shortened URLs within phishing emails. The code utilized to create the URL shortening service contained a flaw which made it very easy to identify additional shortened URLs, map them to their corresponding landing pages, and therefore identify other individuals or groups targeted by the actor as well as identify phishing landing pages utilized for credential harvesting. The identification of these operations also highlights the existence of mercenary hackers, providing the type of cyber espionage capabilities previously available only to nation-states to rogue regimes, unscrupulous corporations, or private entities with the budget to finance these types of actions. In IronDefense, the application of Expert System Rules to alerts which span the various stages of the cyber kill chain assist in identifying some of the key elements that OSINT research would bring to the table when conducting investigations into particular indicators of compromise.

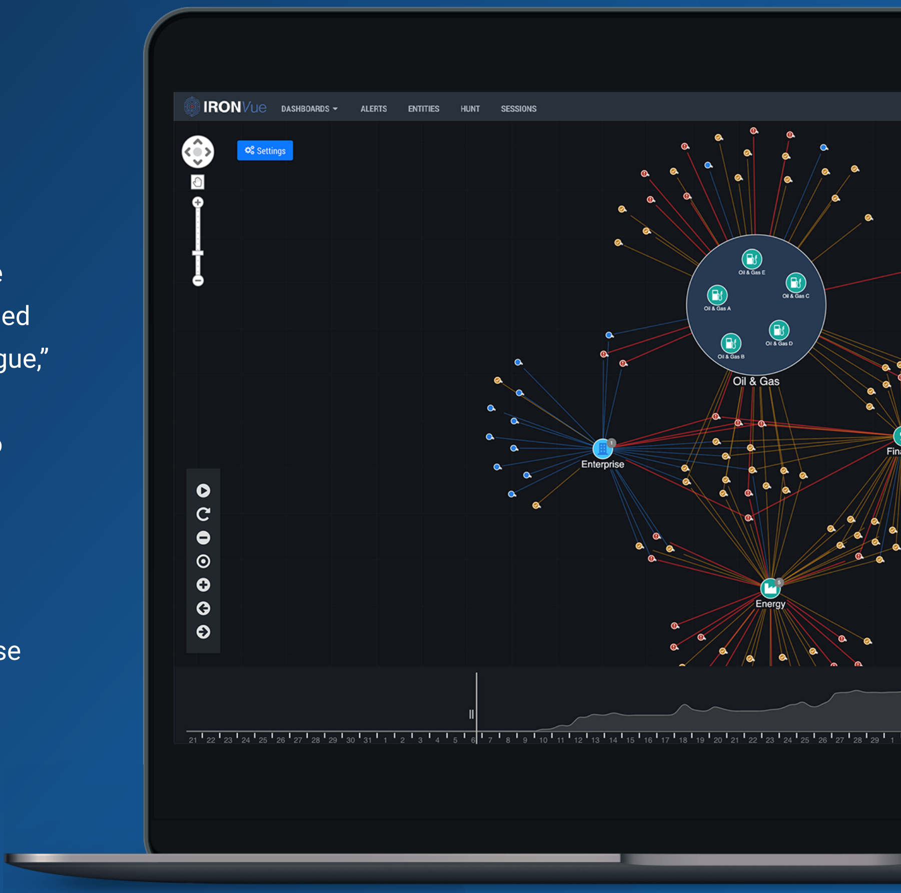
“Copy-Paste Compromises” TTPs Utilized to Target Australian Networks

On June 18, 2020, the Australian Cyber Security Centre (ACSC) issued an advisory acknowledging sustained targeting of Australian entities by an unnamed nation-state. Targets included the Australian government, key infrastructure, and the private sector. ACSC noted that successful initial access attempts were observed via exploitation of known vulnerabilities in public-facing infrastructure. When these attempts were unsuccessful, the actor turned to spearphishing activities. Legitimate Australian websites were compromised with the placement of web shells in order to serve as command and control servers, making identification of malicious network activity more difficult. There is speculation that the unnamed nation-state is China. Experts hypothesize that China may be retaliating against Australia’s recent call for an international inquiry into the source of the COVID-19 pandemic, Australia’s recommendation that tourists and students abstain from visiting China, and escalating trade tensions between the two nations. The United States has also recently condemned attempts by China linked cyber actors to steal U.S. intellectual property and data related to coronavirus research, though the extent to which this campaign has touched the U.S.—if at all—is unknown. The exploits utilized by the actor over the course of this campaign are publicly known and have patches or mitigations available. Additionally, network indicators shared by ACSC as relevant to this campaign have been deployed as threat intelligence rules in IronDefense.

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.

IronNet

STRONGER AS ONE:

The Case for Collective Defense

ACCESS THE BOOK →

IronNet.com

IronNet™