IronNet

IronLens:

Collective Defense Updates from the IronDome

Top Observed Threats from IronNet Collective Defense Community
May 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.

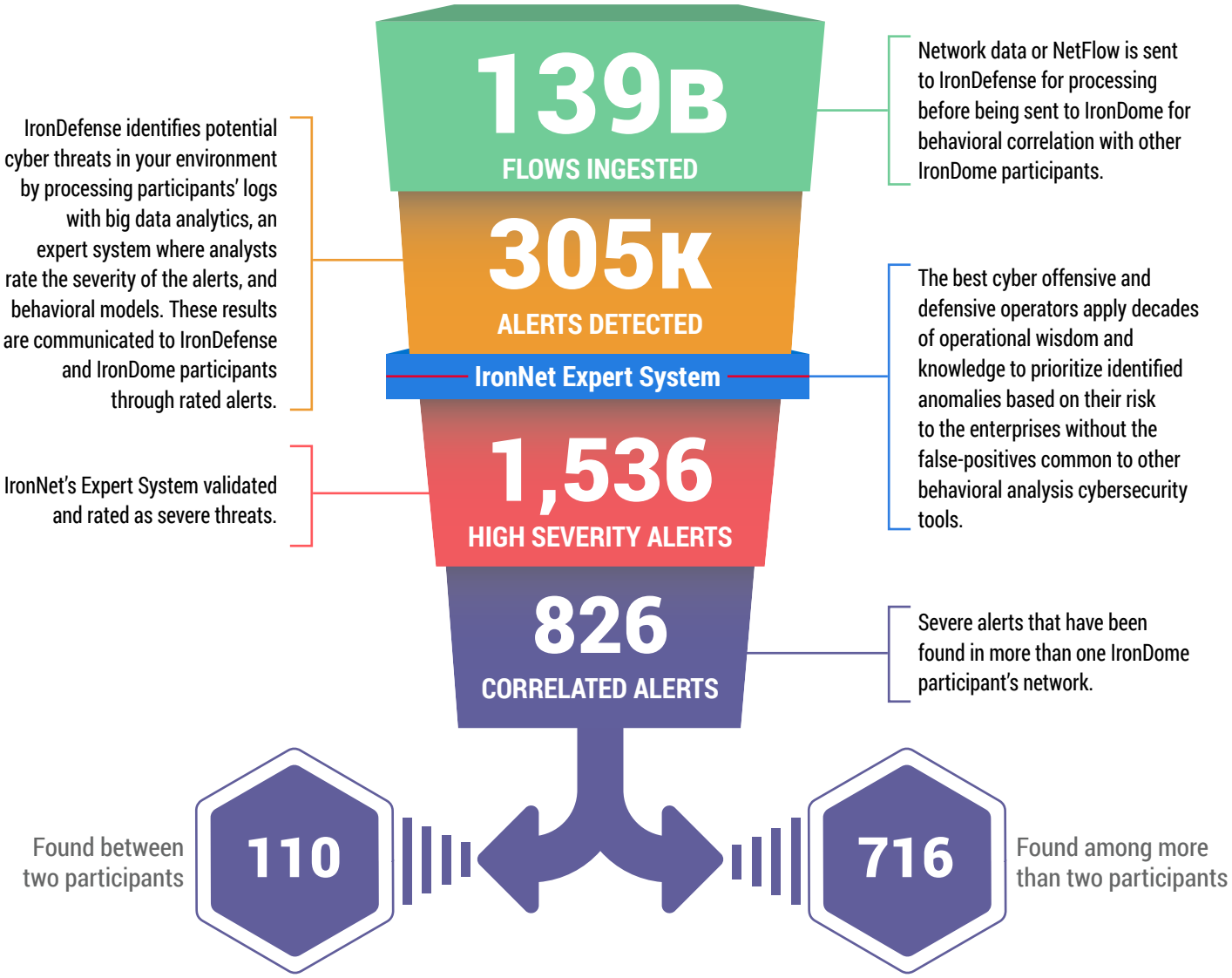
IronNet

THIS MONTH IN THE IRONDOME

The IronDefense network traffic analysis solution detects behavior-based anamolies. 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.

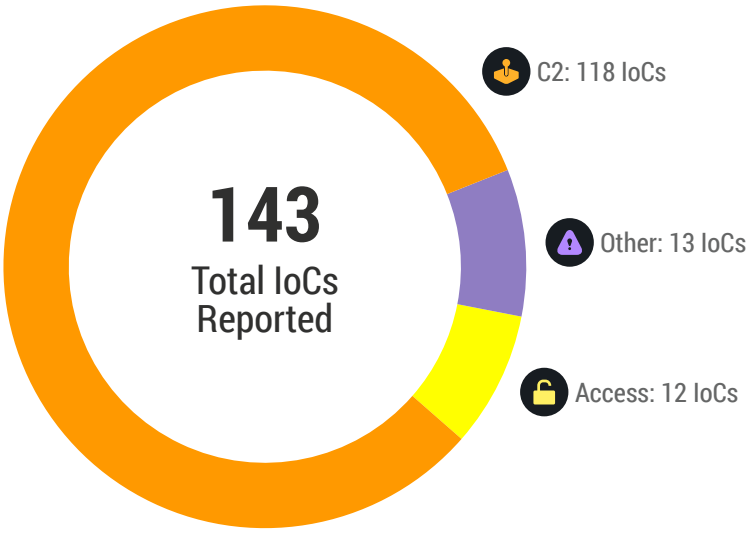
IronNet's IronDome Collective Defense platform delivers a unique ability to correlate patterns of behavior across IronDome participants within an enterprise's business ecosystem, industry sector, or region. This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses. Weighing the alerts also diminishes "alert fatigue" for your SOC.

Below is a snapshot of this month's alerts.



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
natashacape[.]buzz	Malicious	This domain hosts a Trojan posing as a fake Microsoft login page targeting corporate login credentials. Future traffic to this domain should be monitored to ensure that no successful login attempts are seen in a POST path to the domain.
emotors[.]bz	Malicious	This domain is a scam site posing as eBay Motors (eBay's auto parts and vehicles site) but hosting fake listings while using a copied version of the actual eBay site. Purchasing an item through this domain has the ability to compromise credentials as well as personal information. The user is requested to pay for the purchased item via the scam domain's invoice system. If seen in your network, investigate to confirm that no POSTs occurred that could compromise user information or loss of funds.
m2mfbpsqgq0e2e20[.]com	Malicious	This domain is used to host Valak malware and has been rated Malicious and Unexpected. Confirm any follow-on activity to this domain before taking further actions.
web-mail-manager[.]com	Suspicious	After researching multiple OSINT resources and investigating network traffic, IronNet's hunt team has deemed mail.web-mail-manager[.]com Suspicious. Its URL and involvement in a potential phishing campaign led to this determination.
unity-shipping-carriers[.]com	Suspicious	This site is posing as a shipping company and could be attempting to gain business information.
apl-cma-cgm[.]com	Suspicious	At the time of triage, this domain was hosting a fake login page for Plesk, a German commercial web hosting platform. Future traffic to this domain should be monitored to ensure corporate users do not post their credentials to login forms related to this URL.
flashit[.]xyz	Suspicious	Activity from this domain may be related to the FlashIT Chrome extension, which is a known browser hijacker. If multiple redirections are observed, investigate to determine whether unwanted software or extensions are present on the endpoint.
google-anaiytlcs[.]com	Suspicious	Activity to 176.119.1[.]69 or google-anaiytlcs[.]com is related to the MageCart credit card skimming campaign. Investigate the endpoint to ensure there were no successful POST requests to the domain or IP address.
theinsiderstories[.]com	Suspicious	Multiple OSINT resources indicate this website, which uses WordPress, has been compromised. Currently, it hosts various adware-related redirect scripts to websites telling users they have won a prize.
infinity-electronic[.]hk	Suspicious	This domain indicates it is potentially associated with a wire fraud scam.

THREAT RULES DEVELOPED

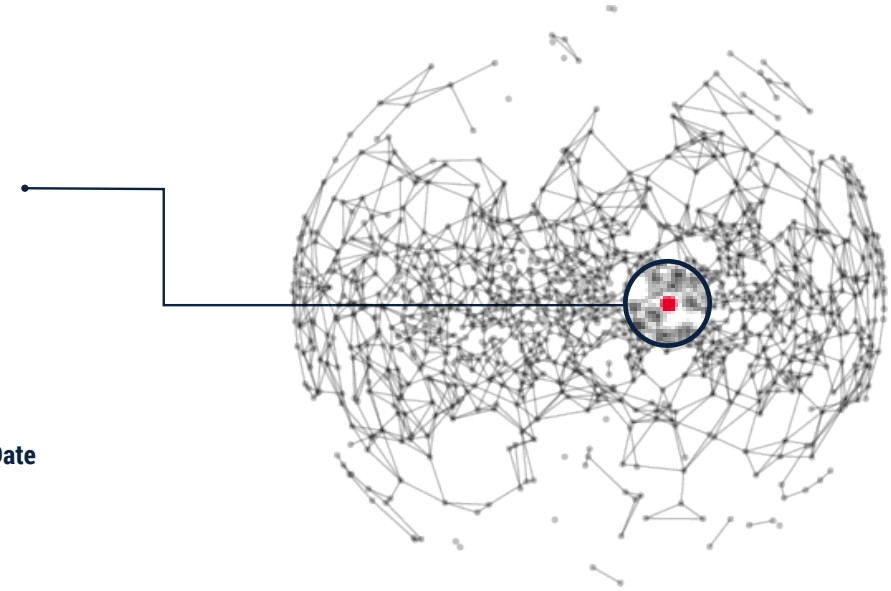
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

9,272

Threat Intel Rules Developed This Month

107,954

Threat Intel Rules Developed to Date



This month's threat intelligence rules include signatures looking for Indicators of Compromise identified by a variety of IronNet analytics, including Suspicious File Download, Domain Generation Algorithm, and Phishing HTTPS. Additionally, rules were created for indicators identified during malware triage conducted by the IronNet Threat Research team (e.g., specifically looking at an emerging Remcos RAT campaign and a Parallax RAT campaign), as well as indicators identified by the IronNet Threat Research Team and information-sharing communities. Rules also were created to search for recent activities documented by researchers in the wider cybersecurity community. Some topics covered by this month's threat research include:

- A look at the Chinese malware Kaiji targeting servers and IoT devices via SSH brute force
- Analysis of the Loki infostealer propagating through LZH files
- An examination of a threat leveraging illegitimate Zoom installers to drop malware
- Examining the Astaroth malware's obfuscation techniques and creative C2 communications
- Looking at recent SilverTerrier cybercrime group activities
- Responding to an alert from the FBI and CISA about the Lazarus Group's usage of COPPERHEDGE, TAINTESCRIBE, and PEBBLEDASH malwares
- Researching a new information stealer malware, Poulight, that is most likely related to Russia
- Research into a variant of the Ursnif malware, which uses binaries that are "living off the land" (i.e., utilizing tools that are already on a target system)
- Identification of a new Android malware dubbed WolfRAT that targets Thai users and is likely linked to notorious spyware vendor Wolf Research

- Analysis of a Tropic Trooper campaign targeting physically isolated (air-gapped) military computer systems in Southeast Asia using USB-enabled malware
- Analysis of malicious backdoors included within illegitimate Zoom installers
- A look at the latest activities undertaken by the infamous Turla espionage group, including using the Gmail web interface for command and control
- Technical evaluation of malware backdoors associated with APT15, which is thought to be a cluster of teams backed by the Chinese government

TRACKING INDUSTRY THREATS

Phantom in the Command Shell Campaign Targeting Financial Industry

A new campaign dubbed "Phantom in the Command Shell" has been identified targeting the global financial sector with an updated variant of EVILNUM malware. Although this campaign began on May 3, 2020, EVILNUM malware was originally discovered in 2018. This newest variant appears to have incorporated new methods for evading both host- and network-based detection mechanisms.

The infection chain begins with an end-user accessing a link to a file hosted in Google Drive. Utilizing cloud service providers to host malicious files is a tactic employed by threat groups who know that these types of links typically will not be blocked by security appliances. In this case, the URL ultimately directs the user to download a compressed file that contains several other files masquerading as various types of images that surreptitiously invoke JavaScript once opened.

The malware then conducts some system enumeration and alters actions (such as determining what to use for command and control) by evaluating which antivirus products are detected on the host machine. Ultimately, this malware is capable of stealing files and cookies and may be able to load additional payloads onto infected systems.

Valak Malware Demonstrates Evolving Sophistication

Cybersecurity researchers published a detailed analysis of Valak malware, which was first observed as a malware loader in late 2019 but rapidly evolved to a potentially major threat. This malware has the ability to conduct reconnaissance, collecting user, machine, and network information to send back to control servers. Additionally, it is geolocation aware, can grab screenshots from infected machines, and can download additional malware. Notably, this malware was recently observed collecting sensitive information from Microsoft Exchange mail systems. Due to early associations with Ursnif and IcedID banking trojans, Valak is thought to be attributed to Russian threat actors.

The network behaviors exhibited by this malware are able to be detected by IronNet analytics such as Periodic Beaconing HTTP and Domain Generation Algorithm.

Recently Identified Iranian Campaigns Target Middle East and South Asia

Two recently published analyses have shed light on previously unidentified cyber espionage campaigns believed to be tied to Iranian threat actors.

Based on reporting from Symantec, the Greenbug group appears to have targeted multiple telecommunications companies in South Asia between fall of 2019 and spring of 2020. Although the evidence is not conclusive, Greenbug actors may have been behind the infamous Shamoon attacks. The group was also involved in previous targeting of telecom companies in the Middle East in 2017. Obtaining sustained access to the networks of such phone and internet service providers has long been highly desirable for state-sponsored intelligence gathering.

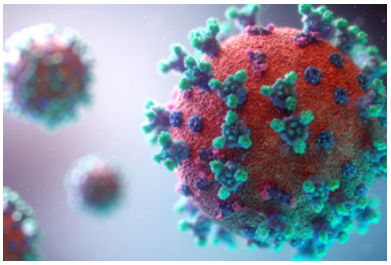
Separate reporting from Bitdefender identified campaigns perpetrated by the Iran-linked Chafer group. Chafer's campaigns targeted air transportation and government entities in Saudi Arabia and Kuwait in 2018 and 2019.

Both Greenbug and Chafer used living off the land techniques to facilitate their activities. As mentioned in the Threat Rules Created section of this report, living off the land refers to an actor using existing software tools on the victim's systems to facilitate further exploitation of and lateral movement throughout the victim's network. The use of such legitimate tools makes distinguishing potentially malicious activity from benign systems administration especially difficult for defenders.

Astaroth Malware Increased Sophistication

Malware is constantly evolving, and the threats present in the current cybersecurity landscape are constantly adapting. The information stealer malware strain known as Astaroth has shown to be both creative and evasive due to its many evolutions. This malware variant so far has targeted only hosts in Brazil, but the techniques demonstrated in this variant could prove to be problematic if malicious actors should consider widening their target base. An interesting note is that this malware has the ability to use YouTube, a website that is generally reachable on most networks, as a means for enabling communications with command and control servers.

COVID-19 Themed Phishing Campaign

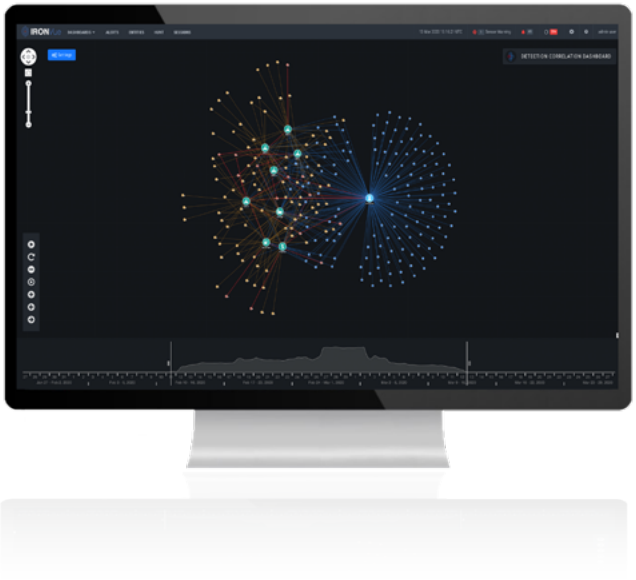


The trend of COVID-19-themed phishing campaigns continues with a set of ten different campaigns sent out by three Nigerian-based criminal groups tracked collectively as SilverTerrier. This phishing campaign has recently sent out around 170 emails to local and regional governments, insurance companies, medical centers, and universities with medical research programs. The organizations were located in the United States, United Kingdom, Italy, Australia, and Canada.

IronNet

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 speed up response — in turn defending the nation collaboratively. 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. This tetonic shift in cybersecurity strategy is IronNet's way to advance collective defense in today's environment — where network threats far outweigh the availability and impact of siloed, individual resources to defend against them.



Learn more about Collective Defense in our eBook.

Access the eBook >