IronNet

IronLens:

Collective Defense Updates from the IronDome

Top Observed Threats from IronNet Collective Defense Community
April 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

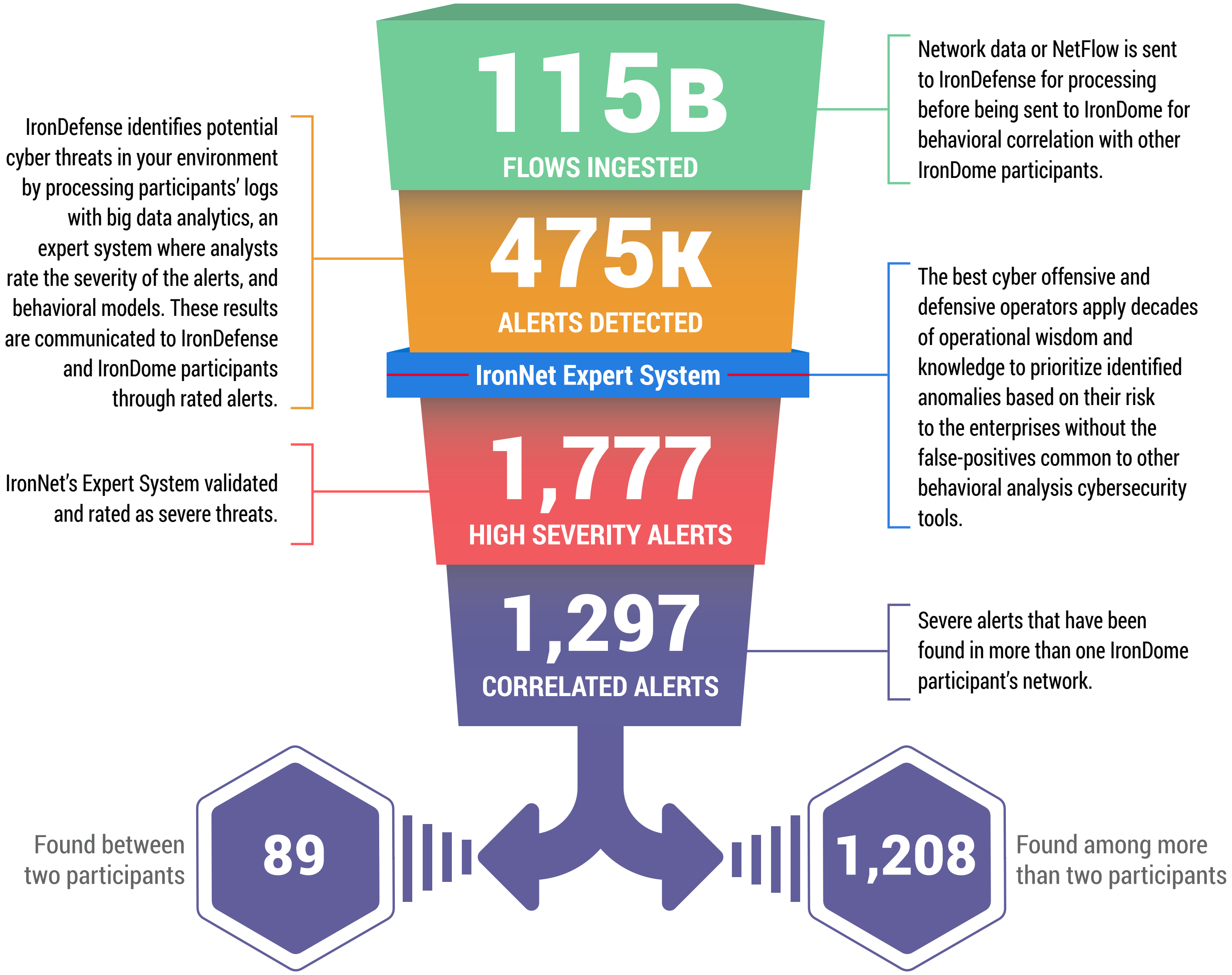
This report features threat findings, analysis, and research shared across IronDome, the industry's first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations so IronDome participants can work together in near-real-time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

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.



115B

FLOWS INGESTED

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

475K

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. These results are communicated to IronDefense and IronDome participants through rated alerts.

IronNet Expert System

The best cyber offensive and defensive operators apply decades of operational wisdom and knowledge to prioritize identified anomalies based on their risk to the enterprises without the false-positives common to other behavioral analysis cybersecurity tools.

1,777

HIGH SEVERITY ALERTS

IronNet’s Expert System validated and rated as severe threats.

1,297

CORRELATED ALERTS

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

89

Found between two participants

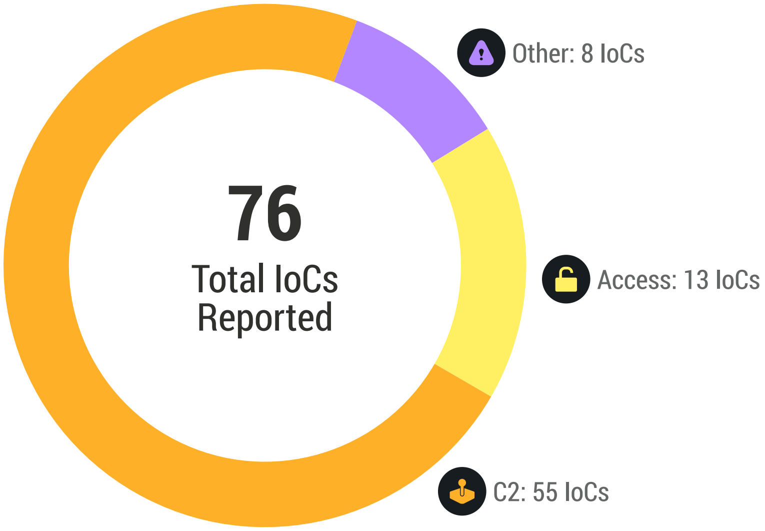
1,208

Found among more than two participants

IronNet

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
googe-js-config[.]com	Malicious	This appears to be a new credit card skimming domain (IP address 194.36.188.75). The scripts associated with the skimming are: googe-js-config[.]com/js/mo.js and googe-js-config[.]com/js/m.js. Investigate traffic if seen on your network for personally identifiable information (PII) loss or block the domain.
user-temporary-account[.]com	Malicious	The domain paypal.user-temporary-account[.]com is a phishing site that impersonates a valid PayPal account login. A user may lose their PayPal account credentials if they input them into this login. The site appeared to be taken down on or around April 9, 2020. If seen in your network, investigate the traffic and contact users to ensure no loss of personally identifiable information (PII) has occurred.
www.southerncarparts[.]com	Malicious	The domain www.southerncarparts[.]com (176.119.1.69) appears to have the following credit card skimming domains embedded on its site: googleanaiytlcs[.]com/st/hotjar.js and google-anaiytlcs[.]com/min.3.14.7.js. Investigate if seen in your network to ensure personally identifiable information (PII) has not been lost. We recommend blocking the domains and IP in question.
gocgle-analytics[.]com	Malicious	This domain is associated with MageCart credit card skimming attacks.
com-zx[.]ru	Suspicious	This is a potential phishing domain related to the online multiplayer game RuneScape. If traffic is seen in your network, investigate to ensure no unintended downloads or installations occurred on client systems.
nusojog[.]com	Suspicious	This domain is associated with a potentially unwanted Chrome extension that performs periodic check-ins and updates the extension by downloading a newer version outside of the Chrome store. This Chrome extension has been identified by multiple security vendors as malware.
spotify[.]ga	Suspicious	This domain appears to be typo-squatting, posing as a legitimate Spotify subscription provider. Open source research has revealed the domain as a possible scam as prices are far less than the legitimate subscription fee.
hbreakingnewsplus[.]com	Suspicious	This domain is related to potentially unwanted Chrome extensions. If there are numerous requests to this domain, verify whether unwanted extensions are present on the endpoint.
hdcaerialbundledcable[.]com	Suspicious	This domain is a website for a cable manufacturing company and has been observed in the past as a potential phishing site targeting Microsoft Office users.
basketballninja[.]com	Suspicious	This domain could result in the download of Locky ransomware.

THREAT RULES DEVELOPED

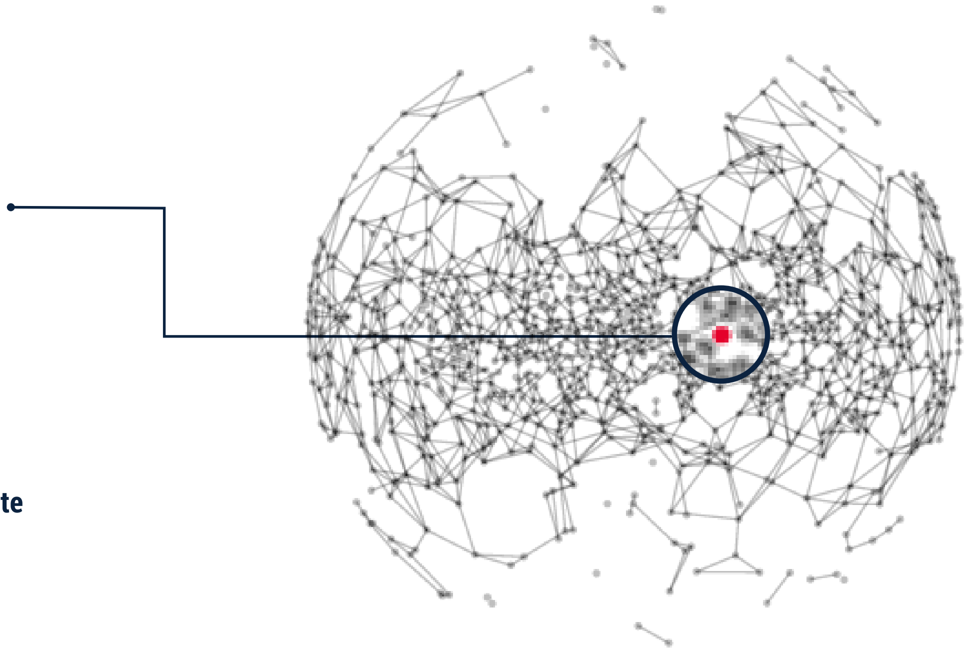
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

8,977

Threat Intel Rules Developed This Month

98,682

Threat Intel Rules Developed to Date



This week's threat intelligence rules include signatures looking for URLs known to be hosting malicious payloads based upon findings from the IronNet Threat Research Team as well as rules derived from information sharing communities. Rules were also 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 recent phishing campaign that uses VPN access for remote work as a lure
- Large-scale attacks on Android smartphones by actors using the xHelper Trojan
- Multiple campaigns that continue to leverage various coronavirus and COVID-19-themed lures
- A deep dive into cross-platform, Chinese government-backed APT espionage attacks targeting Linux, Windows, and Android
- New Internet of Things (IoT) botnet called dark_nexus which is used for DDoS services
- The Speculoos Backdoor targeting organizations globally
- Another look at how attackers are abusing the COVID-19 pandemic by utilizing this high-interest news item as a theme in phishing campaigns and domain registrations for malicious purposes
- A phishing campaign targeting customers of GitHub by fraudulently claiming that users' accounts have been modified or have had unauthorized activity identified

- A detailed survey of surveillance campaigns enabled by mobile malware and conducted by various nation-state groups
- An examination of the PhantomLance campaign executed by the Vietnam-linked OceanLotus threat group and distributed via the Google Play Android app store
- Analysis of the Asnarok trojan used to collect and exfiltrate data from compromise Sophos firewalls
- Additional reporting on coronavirus-themed malicious websites used by cyber criminals

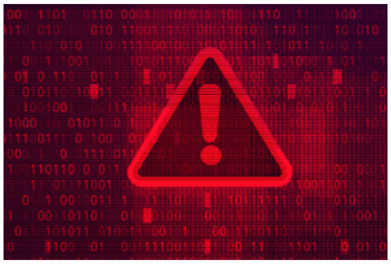
TRACKING INDUSTRY THREATS

U.S. Executive Branch Recommends FCC Oust China Telecom

On April 9th, the U.S. Department of Justice published a recommendation to revoke China Telecom Corporation's authorization to operate in the United States. This decision was based on unanimous agreement among the Executive Branch agencies. The press release cited several reasons for the recommendation, including the People's Republic of China's "role in malicious cyber activity targeting the United States," concerns that China Telecom might be vulnerable to undue influence from the Chinese government, and inaccurate information provided to the U.S. government with respect to China Telecom's data storage and cybersecurity practices.

China Telecom had previously been involved in several incidents of Border Gateway Protocol (BGP) misdirection, resulting in large amounts of internet traffic being unnecessarily routed through mainland China. While it is not clear whether these incidents were deliberate or accidental, the concerns arising from these episodes likely contributed to the Executive Branch's decision to push forward with the recommendation.

Winnti Group Linked to DNS Tunneling Technique



QuoIntelligence recently released research describing a previously unknown malware sample that they have tied to the China-linked Winnti group (which likely correlates to groups tracked as APT41 and Barium by various companies). The malware was used to target German chemical company Lanxess, potentially as far back as 2015 based on artifacts contained within the malware.

Of note, this malware uses DNS tunneling for command and control, a technique that has not been previously associated with Winnti actors. The malicious command and control technique relies on leveraging a free dynamic DNS service to direct DNS requests to a server controlled by the threat actors. The malware also uses a custom implementation of open source DNS tunneling software Iodine, using NULL and TXT DNS request types as the preferred communications mechanisms.

These findings raise the question of what other victims may have been targeted with these tools since their apparent development in 2015 and how widespread their use was.

IT Services Provider Cognizant Hit with Maze Ransomware

RANSOMWARE ATTACK
You only have 3 days to submit the payment, or your files will be lo
Time Left
02:23:59:06

On April 17th, Cognizant, one of the largest IT services providers in the world, was hit with Maze ransomware. Managed service providers like Cognizant are ripe targets for cyber threat actors, largely because of their ability to serve as an easy pivot point into the networks of other companies of interest.

Maze ransomware operators are known for threatening to publish stolen files on the internet if their ransom demands are not met. Victims will often perceive that paying a ransom to recover encrypted files is risky since there is no guarantee that the attacker can even provide a recovery key. Maze operators attempt to mitigate ransom rejections and increase their chances of receiving a payout by providing victims with three decrypted files "for free."

Multiple opportunities for detection exist for this type of campaign since the threat actor was likely on the victim's network for a while before making their presence known. The initial access probably occurred in one of the following ways:

1. Via an exploit kit delivered when an end-user visited or was redirected to a malicious or compromised website.
2. Via a remote desktop connection into the network where weak credentials were used.
3. Via a phishing email with a malicious macro embedded in an attached Word document.

Lateral movement and exfiltration of stolen files back to command and control servers would additionally present potential network detection points prior to the start of individual file encryption.

CISA Warns of Pulse Secure VPN Exploits

On January 10, the Department of Homeland Security Cybersecurity Infrastructure Security Agency (DHS CISA) issued an alert for unpatched Pulse Secure VPN servers that were vulnerable to arbitrary file reading. This issue appears to have been a persistent vulnerability within the Pulse Secure VPN applications since April 2019. Pulse Secure issued alerts to their customers urging the application of patches to mitigate the risks from this vulnerability.

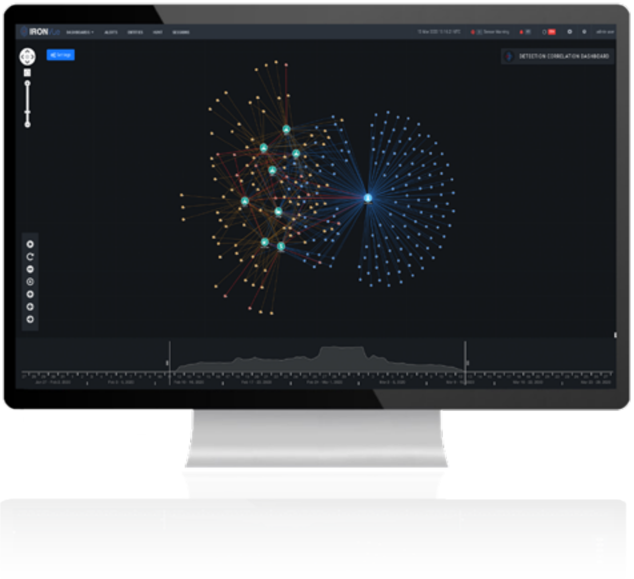
An updated alert was issued on April 16, 2020 that encourages organizations to change credential information for previously affected devices. Stolen credentials that are still valid would still allow malicious actors to access networks and move laterally within the system. CISA provided detection tools and mitigation methods for affected organizations in this latest alert.

Some actor TTPs (tactics, techniques, and procedures) included the utilization of Tor infrastructure and virtual private servers to obfuscate and hide their presence within the network. Access to networks was gained using the stolen credentials within the Pulse Secure appliance. After enacting obfuscation strategies, an actor typically sets up scheduled tasks that would allow for persistence in the network for gathering useful files for mass exfiltration and/or deploying ransomware.

Remnants of scheduled tasks not set by systems administrators should be investigated by individual organizations. Additionally, IoCs were distributed as a part of this alert which would provide opportunities for detection.

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 >