IronNet™

Edition #8: August 2020

IRONLENS

Collective Defense Updates from the **IronDome**

Top Observed Threats from IronNet Collective Defense Community

July 1 – July 31, 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 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.

307K
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.

1,217
High Severity Alerts

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

804
Correlated Alerts

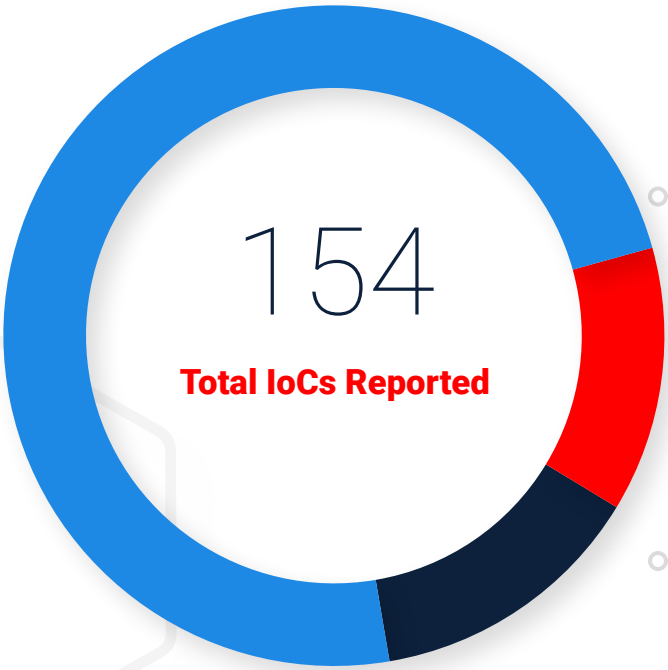
Severe alerts that have been **found in more than one IronDome participant's network.**

76
Found between two participants

728
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.



C2:
113 IoCs

Other:
20 IoCs

Access
21 IoCs

Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
1163be24e7453e9ac96027b434b92488[.]icu	MALICIOUS	This domain appears to be a Japanese language phishing page posing as an Amazon login. There is potential for personally identifiable information (PII) loss, including payment information. Investigate or block the domain if seen in your network.
joyshoul[.]com	MALICIOUS	This domain is related to the LNKR ad injector campaign, which uses browser extensions to perform unwanted redirections and malvertising. Verify what endpoint initiated the activity to the domain to determine if any unwanted programs/extensions are present. The JavaScript resource observed from this traffic was: joyshoul[.]com/22bd1a92d57466cd6c.js"}"
jquerylab[.]pw	MALICIOUS	Activity observed from this domain is related to a MageCart credit card skimming campaign. The JavaScript associated with this domain was: https[:]//jquerylab[.]pw/cdn/analytics-cdn[.]js.
instagramtechsupport[.]com	MALICIOUS	This domain appears to be an Instagram phishing website. If seen in your network, we recommend investigating the traffic and blocking the domain.
starcoolac[.]com	MALICIOUS	This site has been observed targeting user email addresses for phishing purposes by requesting users to log in with their credentials. If seen in your network, verify no successful communications took place and no credentials were transmitted.
google-anaiytlcs[.]com	SUSPICIOUS	While browsing to a compromised site (southerncarparts[.]com), a user was led to credit card skimming JavaScript files from google-anaiytlcs[.]com/hotjar[.]js.
mobilegiftcenter[.]xyz	SUSPICIOUS	This domain is related to a scam involving credential harvesting. It is unclear if the domain successfully harvested user credentials at the time of alert closure.
routerloginnet[.]tips	SUSPICIOUS	This website provides online support and guidance for logging into routers. We are rating the domain as Suspicious because it may be phishing for PII or router access. We recommend blocking the domain.
cov19rapidtests[.]com	SUSPICIOUS	This may be a phishing or scam site related to COVID-19 testing kits. The site is not included on the FDA's list of self-testing providers. Interactions with the site could lead to a loss of PII.
vn.fro-vmseg[.]xyz	SUSPICIOUS	This appears to be a phishing domain targeting users' Microsoft Office login credentials. If seen in your network, we recommend verifying if traffic was blocked by the firewall.

Threat Rules Developed

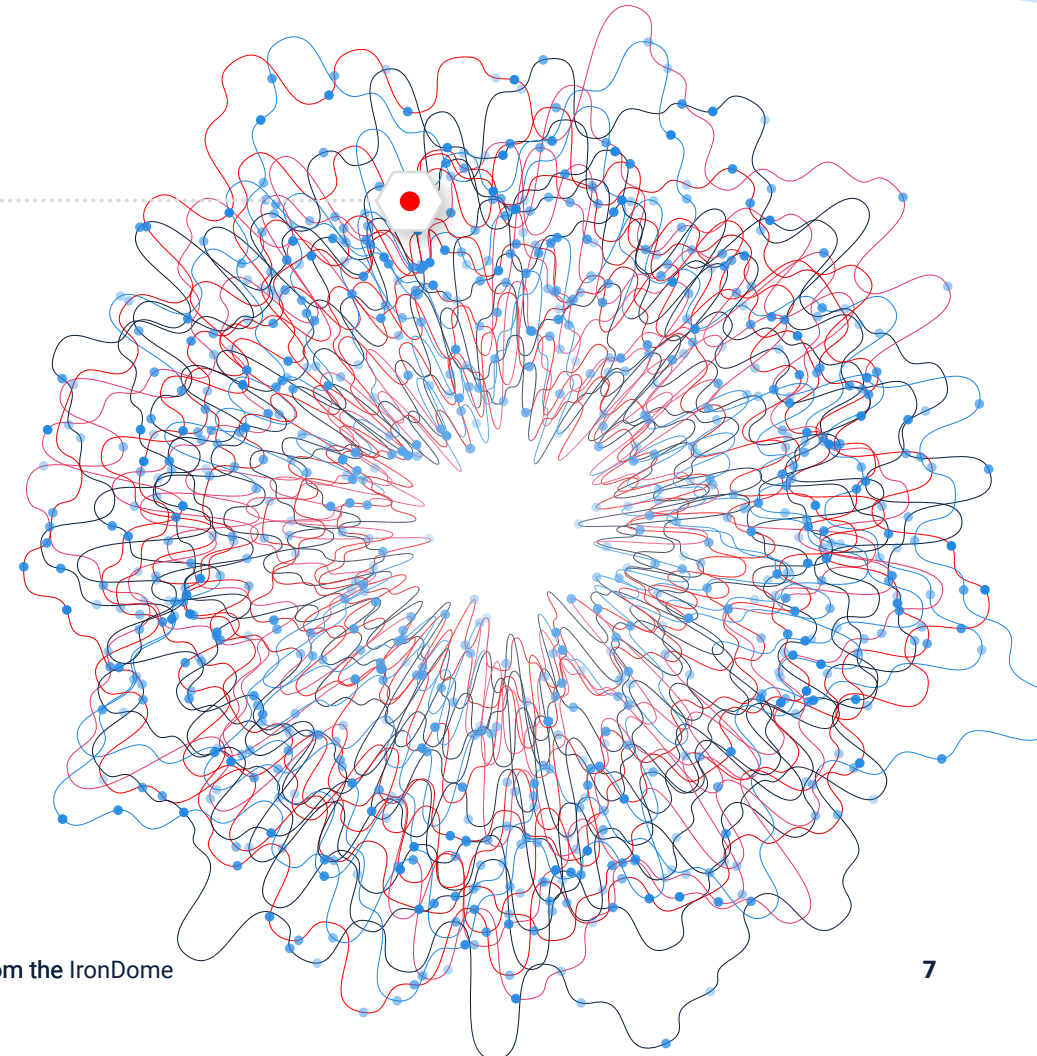
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

11,260

Threat Intel Rules Developed This Month

127,473

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 several IronNet analytics including Domain Analysis TLS, Domain Analysis HTTP, Phishing HTTPS, Periodic Beaconing HTTP, Encrypted Communications, and Domain Generation Algorithm. 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 published by the wider cybersecurity community and ensure rules are created for documented indicators. Some topics covered by this month's research include:

- The new Conti family of ransomware
- Cosmic Lynx business email compromise (BEC) campaigns targeting executives at Fortune 500 and Global 2000 corporations
- A credit card skimming operation targeting e-commerce websites
- A backdoor named ServHelper associated with the hacking group TA505 deploying information stealers
- An implant named NewPass linked to the Russian threat group Turla
- A cyber-espionage campaign in the Middle East targeting Android users via the malicious Welcome Chat application
- A Brazilian criminal group targeting foreign countries and banks
- Variant of an OilRig-associated tool referred to as RDAT
- A cluster of activity impersonating cybersecurity vendors
- Four attacks in early 2020 that utilized tools from the Golden Chickens (GC) Malware-as-a-Service (MaaS) portfolio
- Several Catholic Church-related organizations were targeted by RedDelta, a Chinese state-sponsored threat actor
- The Doki malware was observed abusing the Dogecoin cryptocurrency blockchain in a unique way

Tracking Industry Threats

Evilnum Group Targets Financial Technology Companies

Researchers at the cybersecurity company ESET have analyzed the cybercrime group Evilnum and highlighted some of the group's notable tactics, techniques, and procedures (TTP). Evilnum, which has been active since at least 2018, has consistently targeted financial technology companies as a means to steal financial information from both the targeted companies and their customers.

Ever popular amongst cyber criminals, spearphishing represents the initial infection vector favored by the Evilnum actors. Customer support and account management employees are often the targets of phishing, as emails are often crafted to appear as customers seeking assistance. To deliver their malware, Evilnum attaches a Google Drive-hosted ZIP file to the email. The ZIP file contains several shortcut files that extract and execute a malicious JavaScript component and open a decoy document to help minimize user suspicion.

While the JavaScript malware acts as a backdoor and establishes contact with a command and control server, the Evilnum operators often deploy additional malware on victim systems, with each type of malware using its own independent command and control server. Of note, the group also appears use tools purchased from a Malware as a Service provider known as Golden Chickens, whose malicious tools have previously been used by other cybercrime groups such as FIN6 and Cobalt Group.

OPSEC Error Exposed Espionage Group's Training Videos to the Internet

Researchers identified an unsecured Virtual Private Server (VPS) hosting what appear to be videos created by APT35, also known as Charming Kitten, to train new analysts on techniques for monitoring compromised accounts and building profiles for targets of interest. The availability of these videos has provided insight into current and previous targeting conducted by the group, confirming that APT35 still operates in support of multiple long-term objectives aligning to Iranian government strategic interests. Historically, the group has targeted U.S. and Middle Eastern government-related organizations. From these videos, researchers were able to identify specific U.S. and Greek Navy personnel whose accounts had been compromised. APT35 is known for employing complex social engineering campaigns, and the videos demonstrated the efforts taken to monitor and manage compromised accounts to build meticulous profiles on targets.

The need for multi-factor authentication (MFA), password rotation, and password managers are underscored by the details that came to light with this OPSEC error.

APT29 Targeting COVID-19 Research

According to a recent advisory from GCHQ, APT29 (also known as Cozy Bear) is currently targeting organizations in Canada, the U.S., and the U.K. who are engaging in COVID-19 vaccine research. The report includes descriptions of malware families referred to as WellMess and WellMail, which were not previously associated with APT29. Other TTP include basic vulnerability scanning against external IP addresses of organizations of interest and looking for opportunities to employ publicly available exploits that have been well-documented in recent months for use against vulnerabilities in Citrix, Pulse Secure, FortiGate, and Zimbra products.

Historically, APT29 has targeted thinktanks and the Government, Healthcare, and Energy sectors. The importance of operating a robust vulnerability and patch management process are underscored by the description of this threat. TTPs such as these are not limited to this campaign.

U.S. Applying Pressure to China as Tensions Grow

This past week the U.S. government has been applying pressure on China with a series of diplomatic and law enforcement actions designed to inflict consequences for the theft of intellectual property by Chinese intelligence operatives.

On July 21st, the U.S. Justice Department indicted two Chinese hackers allegedly working on behalf of the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS), China's national intelligence agency. The hackers have been accused of breaching dozens of networks over the last decade, primarily targeting high technology industries to steal intellectual property.

The same day, the U.S. ordered the shutdown of the Chinese consulate in Houston, Texas. While the exact reasons for this action have not been made public, a U.S. State Department spokesperson stated the order was issued "to protect American intellectual property and Americans' private information." In turn, the Chinese Foreign Ministry announced on Friday that the U.S. consulate in Chengdu was being ordered to close, specifically in response to the closure of the Houston consulate.

Additionally, the Justice Department also charged four Chinese nationals with visa fraud after allegedly lying about their statuses as members of the Chinese military. All four appear to have been participating in research within the U.S. in fields including brain disease and machine learning.

A deescalation in Chinese cyber activity is unlikely to occur in this era of heightened tensions between the nations, requiring a coordinated collective defense in order to ensure maximum protection against future threat campaigns.

WastedLocker Ransomware Targets Large U.S. Corporations

Over the course of the last two months, cybersecurity researchers have observed an uptick in WastedLocker ransomware activity. The operators of this ransomware appear to favor highly targeted intrusions as opposed to a "spray and pray" approach. This is likely an effort to maximize impact and increase the chances of receiving a larger ransom payout. The majority of recently observed targeted organizations are based in the United States and span sectors from utilities and energy to transportation and logistics.

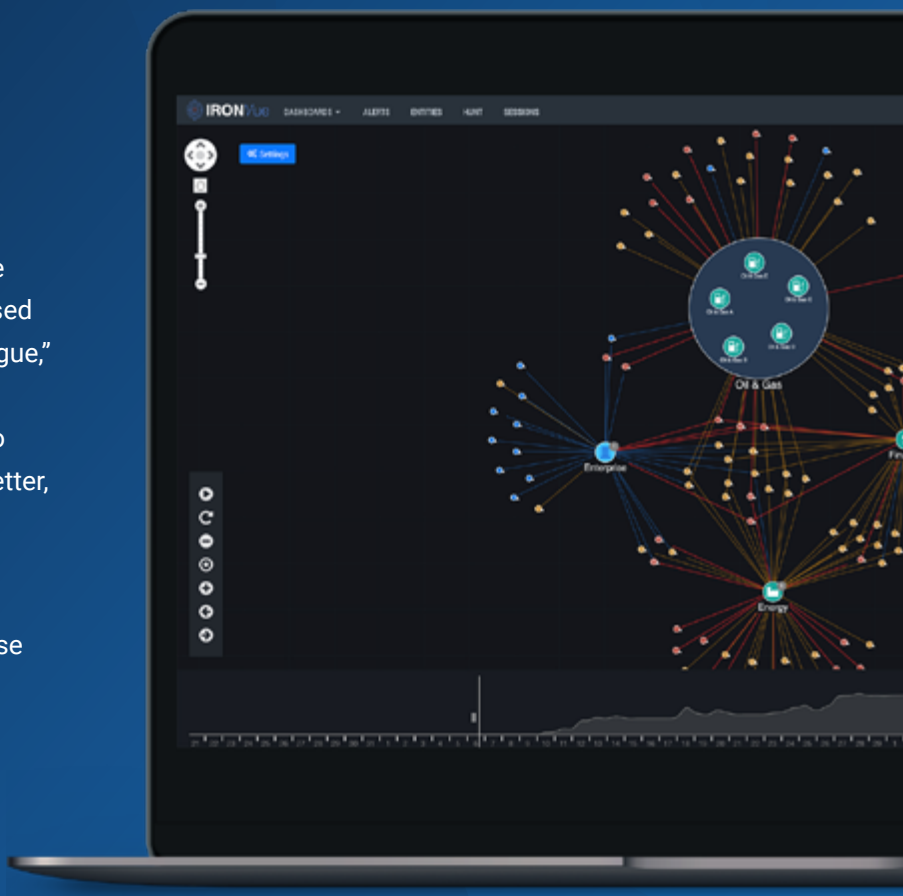
The most commonly observed initial infection vector for WastedLocker was via ZIP files masquerading as legitimate software updates. These ZIP files contain malicious SocGholish JavaScript framework loader components, which then profile the victim's systems. PowerShell is utilized to deploy CobaltStrike payloads, followed by lateral movement to identify additional systems for payload deployment. Researchers report the most likely targets are systems that are used for backups, internal systems that are high load, and external-facing systems that facilitate revenue generation.

IronNet's behavioral analytics have proven especially effective in identifying malicious behaviors relevant to this type of activity, especially via analytics like Suspicious File Download and multiple phishing analytics.

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™

IronNet.com