IronNet™

Edition #9: September 2020

IRONLENS

Collective Defense Updates from the **IronDome**

Top Observed Threats from IronNet Collective Defense Community

August 1 – August 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

222B
Flows Ingested

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

353K
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.

1,084
High Severity Alerts

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

881
Correlated Alerts

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

134
Found between two participants

747
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:
216 IoCs

Other:
14 IoCs

Access
26 IoCs

Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
cssjs[.]co	MALICIOUS	After consulting multiple OSINT resources, this domain appears to be associated with credit card skimming, specifically the MageCart campaign. We recommend blocking the domain and investigating traffic for loss of personally identifiable information (PII) and payment information.
16b86fe6-c648-40c5-b714-17567427d821[.]server-100[.]deeponlines[.]com	MALICIOUS	This domain is associated with the Glupteba malware strain. If seen in your network, ensure there are no follow-on communications related to Glupteba Command and Control (C2) servers, which are well documented in OSINT.
newstrackerdaily[.]com	SUSPICIOUS	This alert was a Threat Intelligence Rule Match for activity related to newstrackerdaily[.]com and smartpackagetracker[.]com. These websites are related to potentially unwanted and suspicious Google Chrome extensions.
ecandles[.]xyz	SUSPICIOUS	Ecandles[.]xyz appears to be an online shopping website, but it is unclear if the site is legitimate. The site collects personally identifiable information (PII). We are marking this activity as Suspicious and recommend blocking the domain because there is little information indicating it is a legitimate merchant site.
pexeso[.]xyz	SUSPICIOUS	After researching multiple OSINT resources, the IronNet Hunt team determined this domain was part of a redirect campaign originating from a bootleg movie site. The user passes through a few pop-up redirections before reaching pexeso[.]xyz. Although this is a common ad redirect chain, it also included known malvertising domains.
ga-fishinginformation[.]com	SUSPICIOUS	This domain is scam related. Although it claims to be a registration portal for fishing in the state of Georgia, the website redirects to govassistanceservices[.]com, which has a reputation of scamming users.
clickstat360[.]com	SUSPICIOUS	This domain has been categorized as a site containing malicious software. If seen in your network, verify no downloads or suspicious redirections occurred around the time of activity.
discoxt[.]com	SUSPICIOUS	Activity from this domain is associated with software downloads that have been characterized by multiple security vendors as malware. If seen in your network, verify no downloads occurred around the time of activity.
developerstatss[.]ga and stock[.]developerstatss[.]ga	SUSPICIOUS	These domains are associated with the Donatello malware, which primarily targets vulnerable WordPress-based websites. The malware is known to cause redirections to malicious domains.
klisige[.]top	SUSPICIOUS	Traffic to this domain may indicate users visiting sites with crack software or getting or attempting to crack licenses. If downloaded, the cracked software could contain or be considered malware. This instance is related to various PC game downloads and the domain fasrsound705.weebly[.]com. We recommend blocking the domain.

Threat Rules Developed

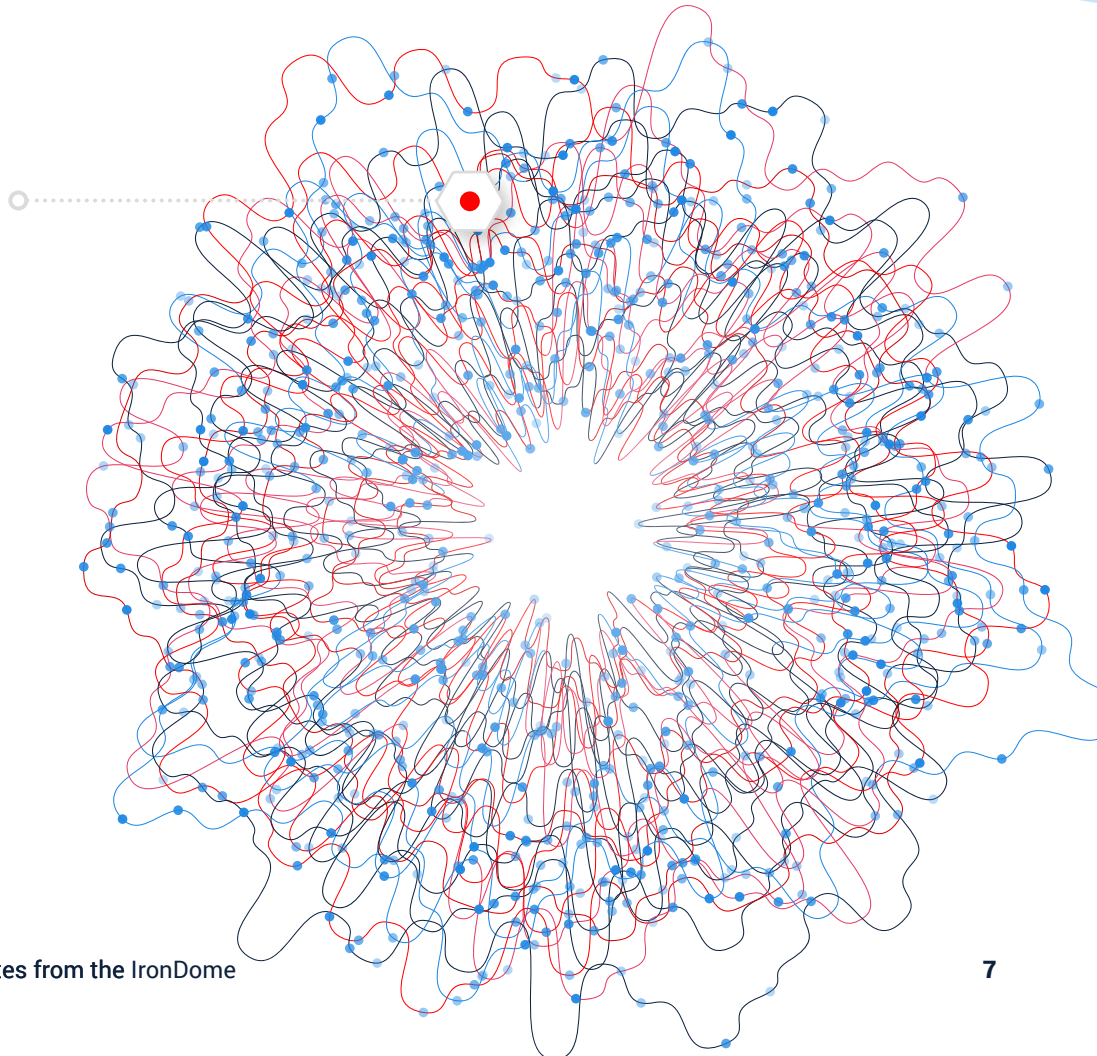
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

9,578

Threat Intel Rules Developed This Month

137,051

Threat Intel Rules Developed to Date

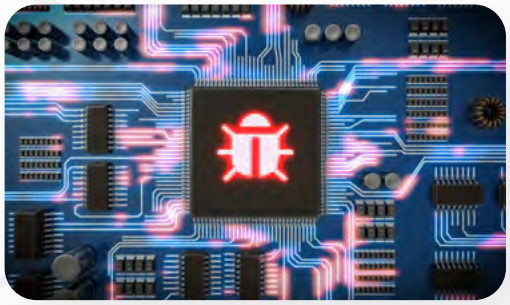


THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise as identified by a variety of IronNet analytics, including Domain Analysis HTTP, Domain Analysis TLS, Phishing HTTPS, Suspicious File Download, Domain Generation Algorithm, and others. Additionally, rules were created for indicators identified during malware triage conducted by the IronNet Threat Research team as associated with phishing or malware delivery. 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:

- IDOOR malware variant used by Chinese government cyber actors
- New MageCart-style credit card skimming campaign leveraging internationalized domain name (IDN) homographs for obfuscation
- Analysis of spearphishing campaigns targeting Office 365 accounts of U.S. and Canada business executives
- Additional infrastructure likely associated with TA551 distribution of Valak and IcedID malware
- Analysis of script-based malware exploiting Microsoft Internet Explorer (IE) to infect Windows systems
- New variants of the venerable Agent Tesla Remote Access Trojan (RAT) distributed via COVID-19-themed phishing campaigns
- Analysis of new TeamTNT group cryptomining worm that can steal Amazon Web Services (AWS) credentials and scan for insecure Docker APIs (application programming interfaces)
- Transparent Tribe APT and its Crimson Remote Access Trojan (RAT)
- PurpleWave new infostealer malware which has emerged on Russian-language cybercrime forums
- Analysis of an aggressive cryptojacker Lemon_Duck which targets enterprises to take advantage of hefty computing resources
- Phishing emails purporting to come from a government agency but actually delivering Ursnif
- A detailed look at Qbot, a notorious banking Trojan that is not recent but still a dangerous and persistent threat to organizations

Tracking **Industry Threats**



China-linked Chimera Targets Taiwanese Semiconductor Industry

During the Black Hat virtual conference, researchers from cybersecurity company CyCraft presented information linking an intrusion campaign targeting the Taiwanese semiconductor industry to a prolific Chinese threat group known as Winnti. The group, tracked by CyCraft as Chimera, is believed to have compromised at least seven Taiwanese chip makers over the past two years and stolen intellectual property, including source code and design schematics.

Notably, the Chimera threat actors leveraged a variety of tactics to evade detection, including hosting their command and control infrastructure on popular cloud services (Google and Microsoft) and using stolen credentials and legitimate software features to move laterally within the victims' networks.

Targeted, strategic attacks like these illustrate opportunities for key sectors of industry to defend collectively. IronDome provides a platform specifically designed to identify these types of coordinated intrusion campaigns by correlating alert data from across the community at machine-speed and sharing threat intelligence in near-real-time.

NSA and FBI Release Detailed Analysis of Russian GRU Malware

In August, the NSA and FBI released a joint report detailing the functionality of a malware toolset dubbed Drovorub. The agencies assert this malware has been used by Russian security services to facilitate cyber espionage operations. The report specifically attributes the malware to a military unit within the Russian General Staff Main Intelligence Directorate (GRU). This report is the third in recent months where the U.S. Intelligence Community has publicly attributed malicious cyber operations to Russian state actors.

Drovorub consists of multiple components, including a Linux implant and kernel module rootkit, which communicate with actor-controlled infrastructure using the WebSocket protocol. The endpoint malware contains functionality to support file transfer, port forwarding, and remote shells, while the Drovorub kernel module effectively hides artifacts of its presence on the infected system.

Sophisticated obfuscation techniques such as these once again highlight the importance of leveraging behavior-based detection solutions such as IronDefense and the urgent need to collectively defend against state-sponsored threats.

Duri Campaign Leveraging HTML Smuggling Technique

Cybersecurity researchers have recently detailed a malicious campaign dubbed Duri which leverages a technique known as HTML smuggling. The malicious actors behind Duri begin by delivering a hyperlink, which in turn redirects the victim multiple times before landing on an HTML page. The page launches JavaScript code to generate a blob object from a base64-encoded variable. A ZIP file containing an executable is then downloaded to the victim's system, which relies on user action to execute. The malicious file is dynamically constructed within the client browser, as opposed to being transferred directly from the server. This technique successfully evades network security devices, such as sandboxes and traditional proxies.

Techniques like HTML smuggling illustrate the limitations of traditional network-based security solutions and the importance of comprehensive defense-in-depth and collaborative solutions to combat evolving cyber threats.

BeagleBoyz Resume Targeting Financial Institutions to Fund North Korean Regime

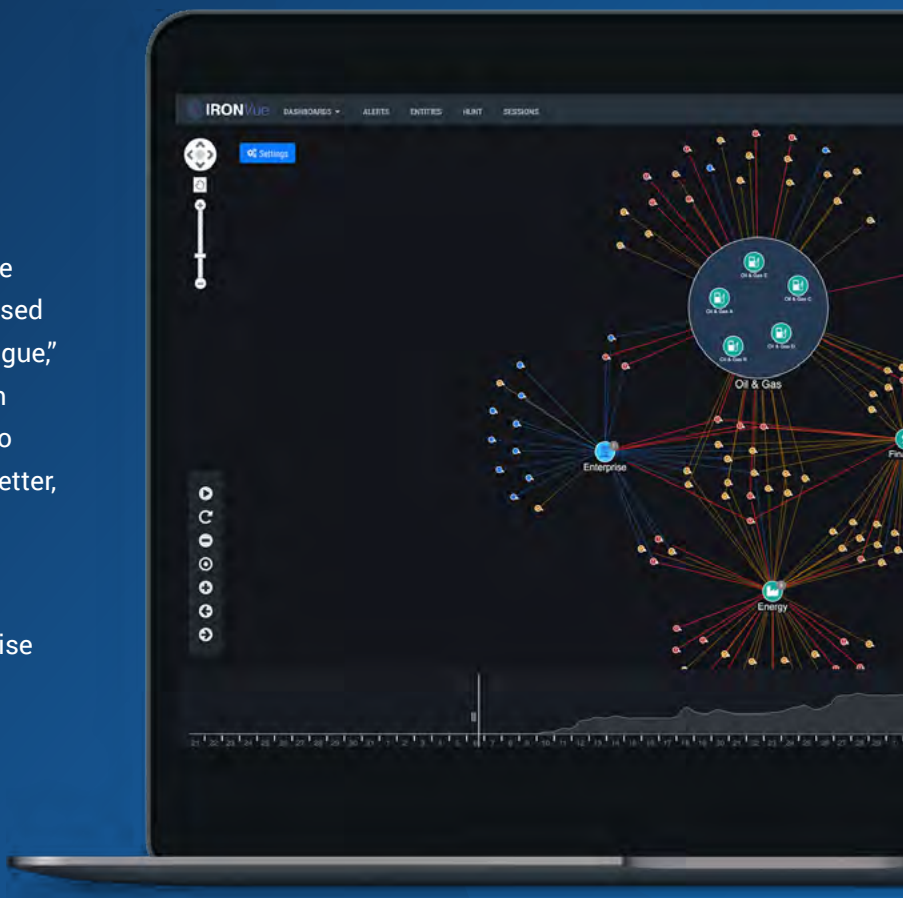
In a joint advisory published by the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Treasury, the Federal Bureau of Investigation (FBI), and U.S. Cyber Command, the U.S. government advised that a threat group known as BeagleBoyz has returned to targeting financial institutions after a brief lull at the end of 2019. BeagleBoyz is most known for stealing 81 million dollars from the Bank of Bangladesh in 2016. The group is also responsible for ATM cash-out campaigns referred to as FASTCash, which target banks' retail payment system infrastructures in order to enable ATM cash-outs.

BeagleBoyz have consistently demonstrated the ability to adapt tools and techniques to different target infrastructures over time. They may also be working in conjunction with other criminal hacking groups who develop initial accesses using commodity malware before turning the accesses over for follow-on exploitation. Attackers who demonstrate this level of adaptability must be countered with a solution that identifies behavioral abnormalities across all stages of the Cyber Kill Chain in order to increase the odds of detection before serious losses are incurred.

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