IronNet™

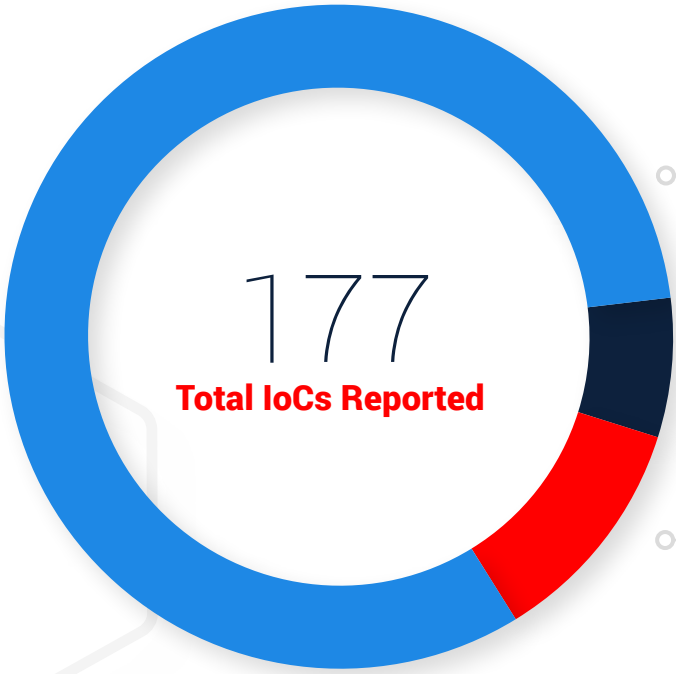
Edition #15: March 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
February 1 – February 28, 2021

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:
145 IoCs

Access
12 IoCs

Other:
20 IoCs

Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
542782[.]com	MALICIOUS	This domain appears to be part of an eBay live chat scam. If seen in your network, investigate for loss of personally identifiable information (PII) and block the domain.
sec-doc-w[.]com	MALICIOUS	This is a redirection domain involving the Buer Loader Malware-as-a-Service (MaaS) campaign. If seen in your network, inspect the traffic for payloads that include indicators of JPG or Java files and verify communications were blocked.
cdn.googapi[.]com	MALICIOUS	This domain is associated with MageCart credit card skimming injections. If seen in your network, we recommend investigating whether the supplied JavaScript was able to run and blocking the domain.
sadiras[.]net	MALICIOUS	This domain is hosting malicious web skimmer code that is injected into hacked websites. If seen in your network, ensure no credentials were entered into the hacked website.
43bwabxrduicndiocpo[.]net	MALICIOUS	This domain is indicative of the WannaCry ransomware application. Many WannaCry domains have now been sinkholed. Sinkholing is a network security technique that redirects malicious traffic to a safe server for research and analysis. If this domain is seen in your network, verify if the alert is due to security testing or an actual infection.
macbethbroy[.]ga	MALICIOUS	This is a generic phishing domain attempting to harvest login credentials. At the time of triage, the site had been taken down.
thansendmaterial-10[.]live	SUSPICIOUS	This domain was recently created to temporarily act as a clickbait ad-redirector to insecure sites. The domain will offer a JavaScript to the client browser that redirects through a series of sites, landing the client on a site that encourages the user to click on a prize or download riskware. The redirector could be the result of adware within a recently downloaded program, browser extension, or ads on the hosted site. We recommend blocking the domain.
showplaytime-13[.]life	SUSPICIOUS	After investigating network traffic and researching multiple OSINT resources, this domain has been identified as a common redirect used by advertisements/suspicious sites which could lead to further ads or unwanted applications. Previous redirects involving the site were associated with the Emotet malware.
neagersir[.]club	SUSPICIOUS	This domain is used on hacked WordPress websites to aggregate user information via the user agent.
app883576[.]work	SUSPICIOUS	This site and associated subdomains have been used for generic phishing. If seen in your network, ensure the domain is blocked.

Threat Rules Developed

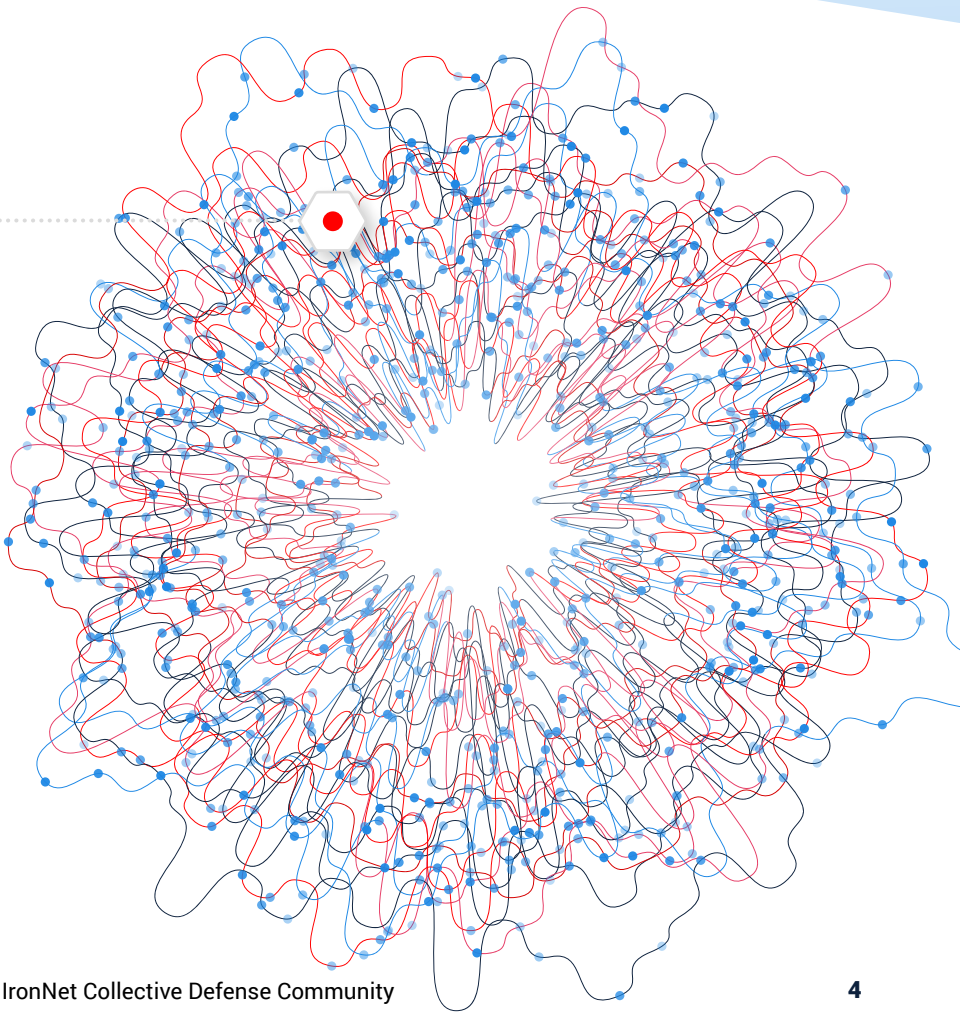
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

8,325

Threat Intel Rules Developed This Month

188,825

Threat Intel Rules Developed to Date



THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise identified by the IronNet Threat Research team as associated with phishing or malware delivery. IronNet threat intelligence analysts also routinely monitor research distributed by the wider cybersecurity community and ensure rules are created for documented indicators. Some examples of this month's research include indicators associated with the following threats and campaigns:

- TeamTNT malware targeting Kubernetes
- SystemBC malware, a Remote Access Trojan (RAT) associated with recent Ryuk and Egregor ransomware attacks
- CinaRAT
- Defray ransomware, which has historically targeted healthcare companies
- The state-sponsored, pro-India Confucius APT Android spyware
- The Bazar Trojan, which was spotted sending phishing emails claiming the user had received a bonus
- The Russian state-sponsored APT28 and its use of the Downdelph downloader
- A DocuSign-themed malspam pushing TrickBot to users
- New Ryuk infrastructure discovered in February
- The banking Trojan Dridex
- The REvil Ransomware-as-a-Service (RaaS) campaign
- BazarLoader, a dropper used to distribute TrickBot and Ryuk ransomware

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

Tracking **Industry Threats**

The SolarWinds Saga Continues

The fallout of the SUNBURST attack has revealed new threats and concerns regarding cybersecurity. Threat actors believed to be associated with China may have exploited SolarWinds software in the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture (USDA). In contrast to the original supply chain attack, it is speculated that China may have exploited a separate bug in the Orion software to aid in lateral movement through a compromised network. The details of this additional compromise are sparse at present, but IronNet will continue to track them as they develop. It is currently unknown what was stolen in the breach or how many other agencies or companies were affected.

The National Finance Center processes payroll for several government agencies, including the FBI, State Department, Homeland Security, and Department of Treasury. As such, the agency houses what China would regard as a treasure trove of PII, such as social security numbers and bank account numbers, linked to specific U.S. government employees. Access to this information could improve China's ability to collect intelligence on U.S. national security operations. If this incident is validated, it could provide some clarity around the SUPERNOVA malware web shell, which you can read more about here.

Egregor Ransomware Affiliates Arrested

According to reporting from ZDNet and the British security company Sophos, Egregor ransomware operators have been arrested in Ukraine as part of a joint operation by French and Ukrainian authorities. The operators' command infrastructure has also been reported to be down. Egregor operates on a Ransomware-as-a-Service model, where individuals or threat groups buy or lease the ransomware tools from the developers instead of writing the code themselves. In December, Sophos issued a report detailing the ransomware operators' use of the SystemBC RAT, which has been linked to this Egregor ransomware attack, as well as to the recent Ryuk ransomware attack.

This is just the latest instance of authorities taking down cyber criminal gangs in recent months. In early February, the Emotet malware was taken down thanks to a widespread, coordinated defense effort by Europol; the FBI; the U.K. National Crime Agency; and the Dutch, German, Lithuanian, Canadian, and Ukrainian Police.

You can read about our current threat research on ransomware, including common characteristics, on IronNet's blog. Wondering if your current security controls can detect the System BC RAT? Use our guide to the MITRE ATT&CK Framework to assess your capabilities.

Sandworm Exploiting Centreon IT Monitoring Tool

Although there were some recent concerns about another wave of SolarWinds-related threats, this is not entirely accurate. While Russia may be at it again on a broad scale, their latest threat appears to use a different delivery mechanism than what was used in the SolarWinds attack. Moreover, this attack was likely the work of the Russian intrusion set known as Sandworm. (Researchers suspect the Turla group was behind the SolarWinds compromise.)

In this case, Sandworm targeted a software suite tool commonly used in Europe from the French company Centreon. The victims are mostly IT firms and web hosting companies running CentOS, according to ANSSI. It is important to note that this is an outdated, open-source, legacy tool. It is the free version of CentOS instead of the paid software suite. With known vulnerabilities, it was an attractive backdoor for Sandworm, which breached P.A.S. web shell and Exaramel. These information-gathering techniques are very different from those used in the SolarWinds attack; however, the scope of both attacks seems to be fairly broad.

Clarifying Palo Alto Malware Name Choice

On February 19, Palo Alto Networks published a report about a Turla malware they have dubbed "IronNetInjector." We would like to emphasize that this malware is completely unrelated to IronNet Cybersecurity. The name "IronNetInjector" is a portmanteau of the two key aspects of this malware: IronPython and a tool called NetInjector. We believe Palo Alto coined this name innocuously.

VMware Remote Code Execution Vulnerability

VMware vCenter Server is server management software that supplies a centralized platform for administrators to manage large networks of virtual servers. The vSphere Client, an HTML5-based web client part of the vCenter Server, was discovered to contain a Remote Code Execution (RCE) vulnerability in the vRealize Operations (vROPs) plugin. Deriving from a lack of authentication in the vROPs plugin, which is present in all default installations, this vulnerability allows an unauthorized user with network access to port 443 to upload specially crafted files to vCenter servers. If successful, this access allows the user to execute arbitrary commands with escalated privileges in the underlying operating system. In Windows, an attacker could gain system privileges through a custom-made .jsp file. In Linux, an attacker could upload a public key to the server's authorized key path and subsequently connect to the server through SSH.

The vulnerability, which has a severity score of 9.8 out of 10 on the Common Vulnerability Scoring System Version 3.0. (CVSSv3), was first discovered by a researcher at Positive Technologies who reported it to VMware privately on October 2, 2020. Though VMware began working on plans to fix the vulnerabilities in early October 2020, it first addressed CVE-2021-21972, along with two less severe vulnerabilities, in an advisory issued on February 23, 2021. With this advisory, VMware also released updates to remediate the vulnerabilities and provided workarounds for clients who could not immediately update their systems. This vulnerability should serve as a reminder to defenders to continue to lock down public access to sensitive private services and applications that should only be accessible internally. Furthermore, vulnerabilities of this nature highlight the need for robust network visibility and detections to identify attackers taking advantage of highly privileged servers with broad visibility for lateral movement.

Why **Collective Defense?**

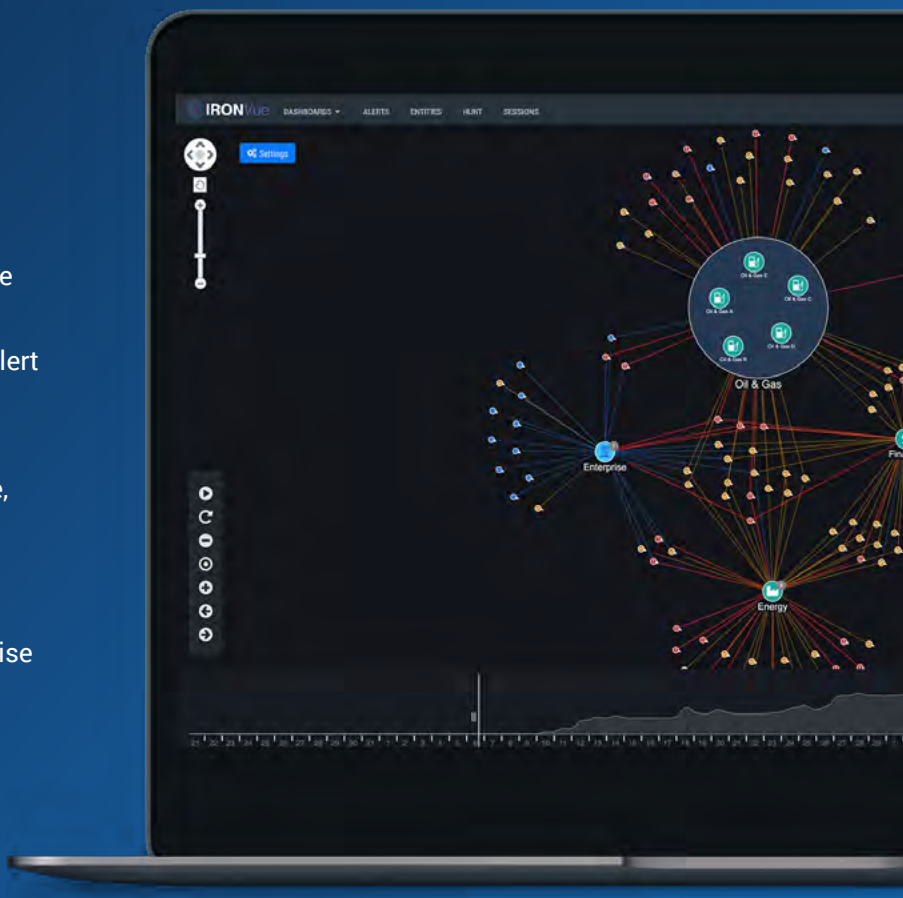
> **IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."**
>
> **— CISO, Industry-Leading North American Energy Company**

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.

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 ecosystem 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