Edition #14: February 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
January 1 – January 31, 2021

IronNet Threat Intelligence
2020 Year in Review

IronNet™

The power of behavioral analytics

IronNet's IronDome Collective Defense Platform correlates patterns of network behavior across participant environments using anonymized threat data. Analyzing and correlating seemingly unrelated instances is critical to identify novel threats before they infiltrate networks.

1.98 trillion

Data flows ingested in IronDefense

We look at the network, where the truth is in the traffic.

8,601

Alerts correlated across IronDome in real time

Correlation cuts down on alert fatigue by providing higher-order analysis of anomalies seen in two or more environments.

4.6 million

Alerts created

Behavioral analytics detect threats that signature-based tools can't see.

15,093

High Severity Alerts created

An Expert System scores, ranks, and filters alerts.

Proactive defense capabilities

2,089

IoCs reported in 2020.
Stay a step ahead of known compromises seen in other environments.

112,806

Threat intelligence rules developed
Our curated and community-sourced threat feed supports defense in depth.

KEY DETECTIONS OF 2020

- SUNBURST: A wakeup call for all
- PoloBear: Tell-tale signs of C2
- VALAK: An updated variant

Get our monthly threat intelligence briefs.

✉ SUBSCRIBE TO SEE THEM ALL →

Shining the light on SUNBURST:

IRONNET BEHAVIORAL ANALYTICS + COLLECTIVE DEFENSE

Perhaps the **biggest cybersecurity news of 2020** was the **SolarWinds/SUNBURST breach**.

WHO?

Presumably nation-state adversaries of Russian origin

WHAT?

A malware attack that used an IT management software update as a "backdoor" to a vast supply chain

WHERE?

Globally exposed 18,000 customers of SolarWinds IT management software

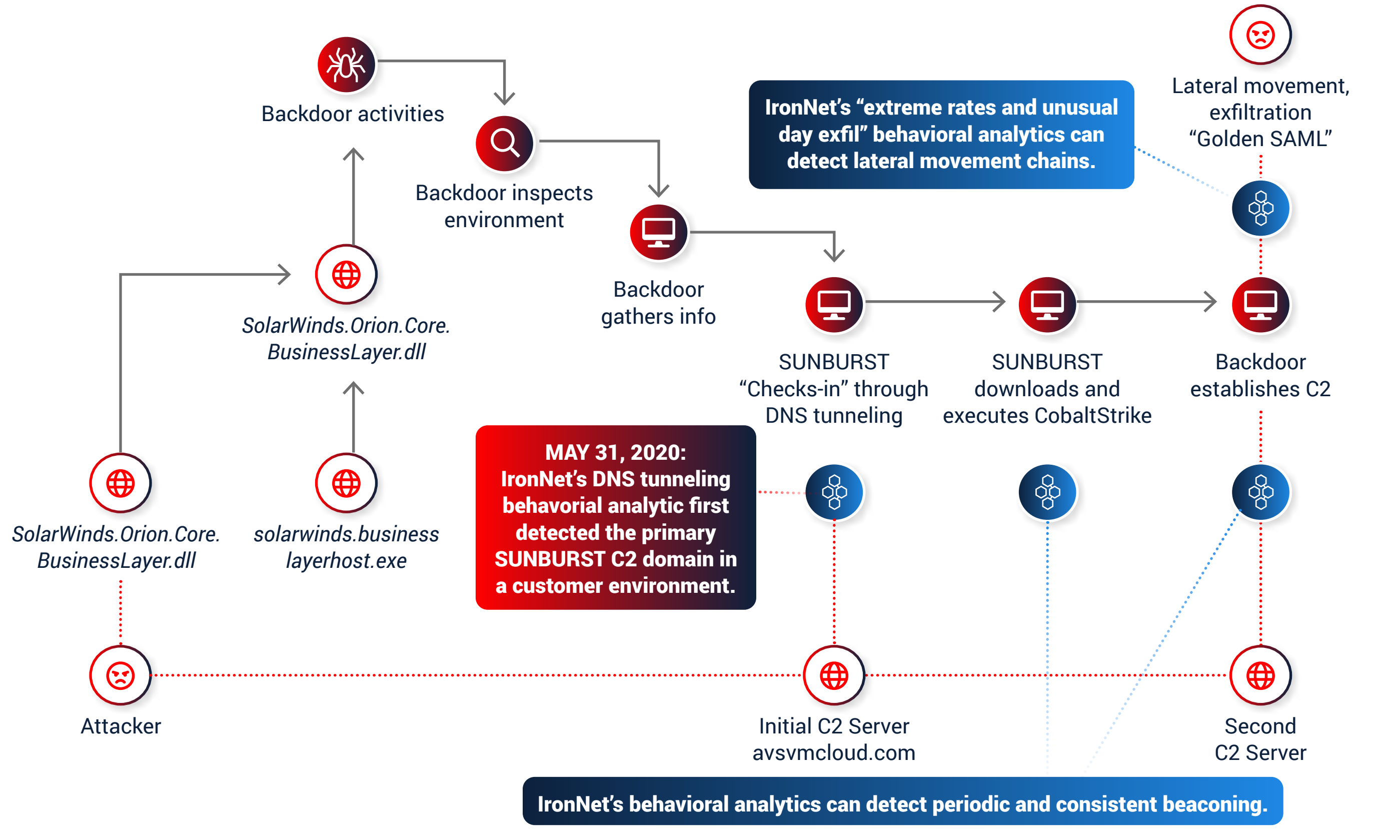
WHY?

Presumably to piggyback on a supply chain backdoor to access federal government networks in the U.S.

HOW?

By using sophisticated techniques to hide command and control traffic, such as mimicking SolarWinds Orion traffic and leveraging cloud providers to masquerade as trusted geolocated environments

WHICH IRONNET BEHAVIORIAL ANALYTICS CAN DETECT SUNBURST TECHNIQUES?



Backdoor activities

Backdoor inspects environment

Backdoor gathers info

IronNet's "extreme rates and unusual day exfil" behavioral analytics can detect lateral movement chains.

Lateral movement, exfiltration "Golden SAML"

SolarWinds.Orion.Core. BusinessLayer.dll

SUNBURST "Checks-in" through DNS tunneling

SUNBURST downloads and executes CobaltStrike

Backdoor establishes C2

MAY 31, 2020: IronNet's DNS tunneling behavorial analytic first detected the primary SUNBURST C2 domain in a customer environment.

SolarWinds.Orion.Core. BusinessLayer.dll

solarwinds.business layerhost.exe

Attacker

Initial C2 Server avsvmcloud.com

Second C2 Server

IronNet's behavioral analytics can detect periodic and consistent beaconing.

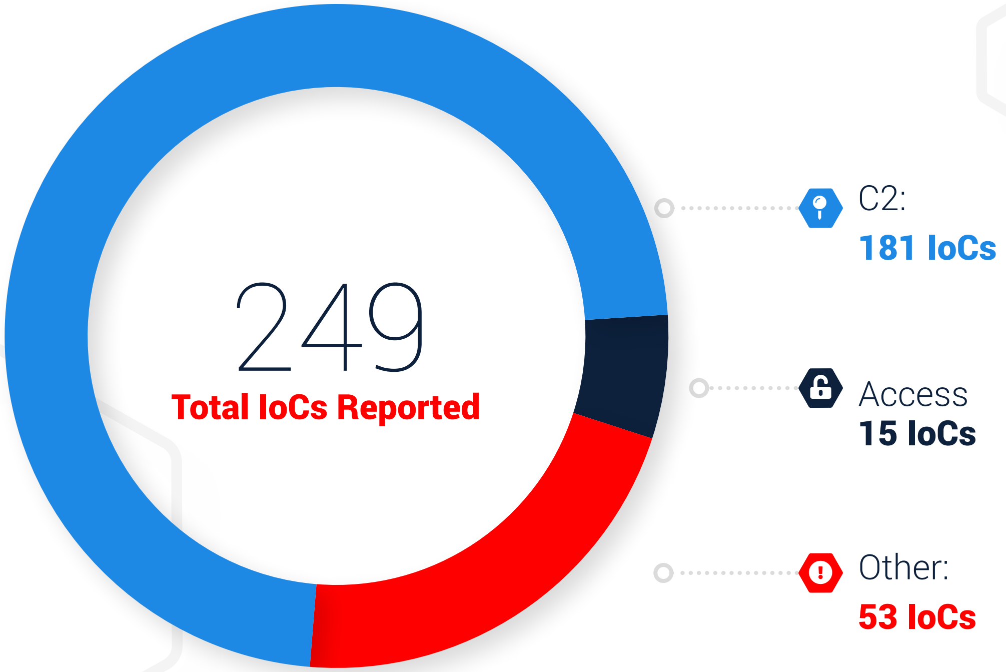
IronNet aided customer response to SUNBURST by supporting investigations, collaborating with customers, and using alerting to help provide context.

Visit IronNet.com to schedule a live demo

> *"IronNet is a partner, not a vendor. You are the first call I make when I need support and a second set of eyes to help determine "what's next."*
>
> — LARGE ENERGY UTILITY COMPANY, IN RESPONSE TO IRONNET'S SUNBURST SUPPORT

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

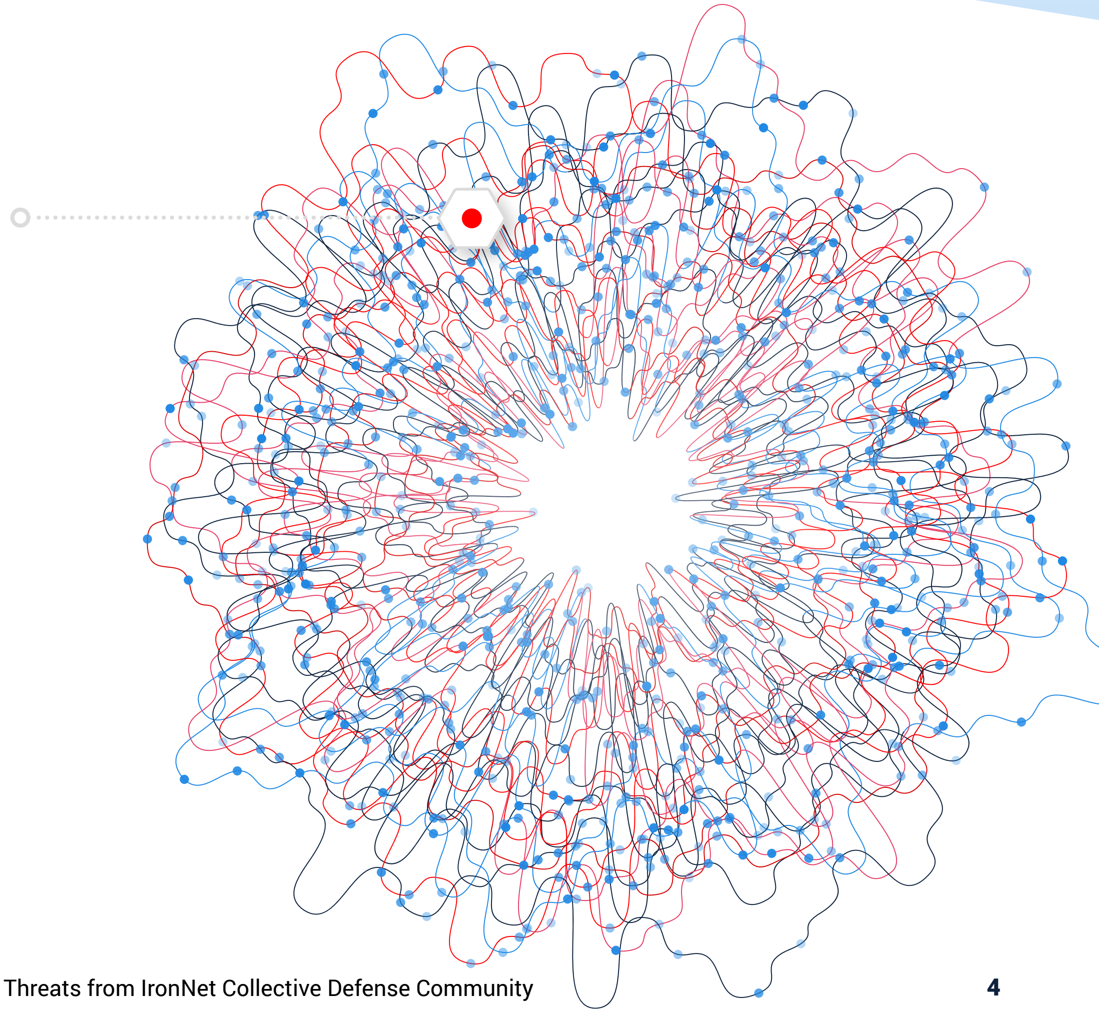
Domain/IP	Rating	Analyst Insight
avsvmcloud[.]com	MALICIOUS	This is a known-bad domain that was used for command and control (C2) communications in the SolarWinds SUNBURST attack. For more information about SolarWinds, please see this blog post on IronNet's website.
yjckxfdwcvxubkw[.]yt	MALICIOUS	This domain was generated as a result of the Locky domain generation algorithm (DGA). If this traffic is seen in your network, isolate the originating box and check for any external connections that have received a DNS Response.
1q4k2mx1a8lcco1au0n0v0lt4ge[.]net	MALICIOUS	This domain was generated by the ZBot DGA. The English-related word "v0lt4ge" was modified and used as the domain name. By modifying "v0lt4ge" instead of "voltage," the actors were attempting to elude detection mechanisms.
1789westernmortgagesaint[.]com	MALICIOUS	Upon examining network traffic and OSINT, this domain is hosting a phishing scam mimicking a login page for Fidelity Investments. The IoC brotherjames.co[.]uk is related and appears in redirects.
com-activty-updates[.]org	MALICIOUS	This was once an Amazon-themed phishing domain, but it was inactive at the time of triage. If seen in your network, investigate for loss of personally identifiable information (PII) or payment information and block the domain. The full site associated with this activity is secure.amazon.com-activty-updates[.]org.
glitch[.]me	MALICIOUS	This domain hosts a fake Microsoft login page meant to harvest user credentials. Traffic to this domain and its subdomain microsoft-outlook-office365-onedrive.glitch[.]me is considered unsafe.
arwks[.]com	MALICIOUS	On 24 January 2021, IronDefense created a Domain Analysis HTTP alert to arwks[.]com. This domain appears to be hosting a phishing attack against Amazon TV activation and may lead to further Amazon account credential harvesting.
o-su[.]xyz	MALICIOUS	This is a generic phishing site that utilized a hacked site (christies[.]com) to send emails as part of its phishing campaign. The email subject line was "Your Meeting attendees are waiting!" Alerts to either domain should be investigated until vulnerabilities at christies[.]com are remediated.
dolwcadcd[.]ru	MALICIOUS	This domain is hosting a phishing login page targeting Microsoft Office 365 users. In this case, the user arrived at the site via a phishing email. If traffic to this domain is seen in your network, investigate the POST data and block the domain.
ahmedashmawy[.]com	SUSPICIOUS	This domain hosts a WordPress-based website for a doctor's office. The site has been hacked numerous times. At one point in Q4 2020, it hosted files infected with Emotet malware. Currently the site still displays some ads, but no malicious content at the time of triage.

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.

7,613

Threat Intel Rules Developed This Month



180,500

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 DarkComent C2 infrastructure
- The identification of a large number of C2 domains for the NanoCore Remote Access Trojan (RAT)
- Indicators associated with the Gamaredon advanced persistent threat (APT) group and their phishing campaigns targeting Ukraine throughout 2020
- Indicators associated with a new variant of Ursnif that uses invoice malspam
- Indicators associated with the Hancitor DocuSign malspam
- Indicators associated with Charming Kitten phishing campaigns
- Indicators associated with the AveMaria RAT
- Indicators associated with C2 conducted by the Conti group using CobaltStrike
- Additional indicators associated with the CozyBear APT
- Indicators associated with the TA551 campaign and its push to distribute the banking Trojan Qakbot
- Indicators associated with the Groundhog botnet
- Additional indicators associated with UNC1878 infrastructure, a group known to target hospitals using ransomware

Rating alerts diminishes “alert fatigue” for your SOC.

This Month in the IronDome

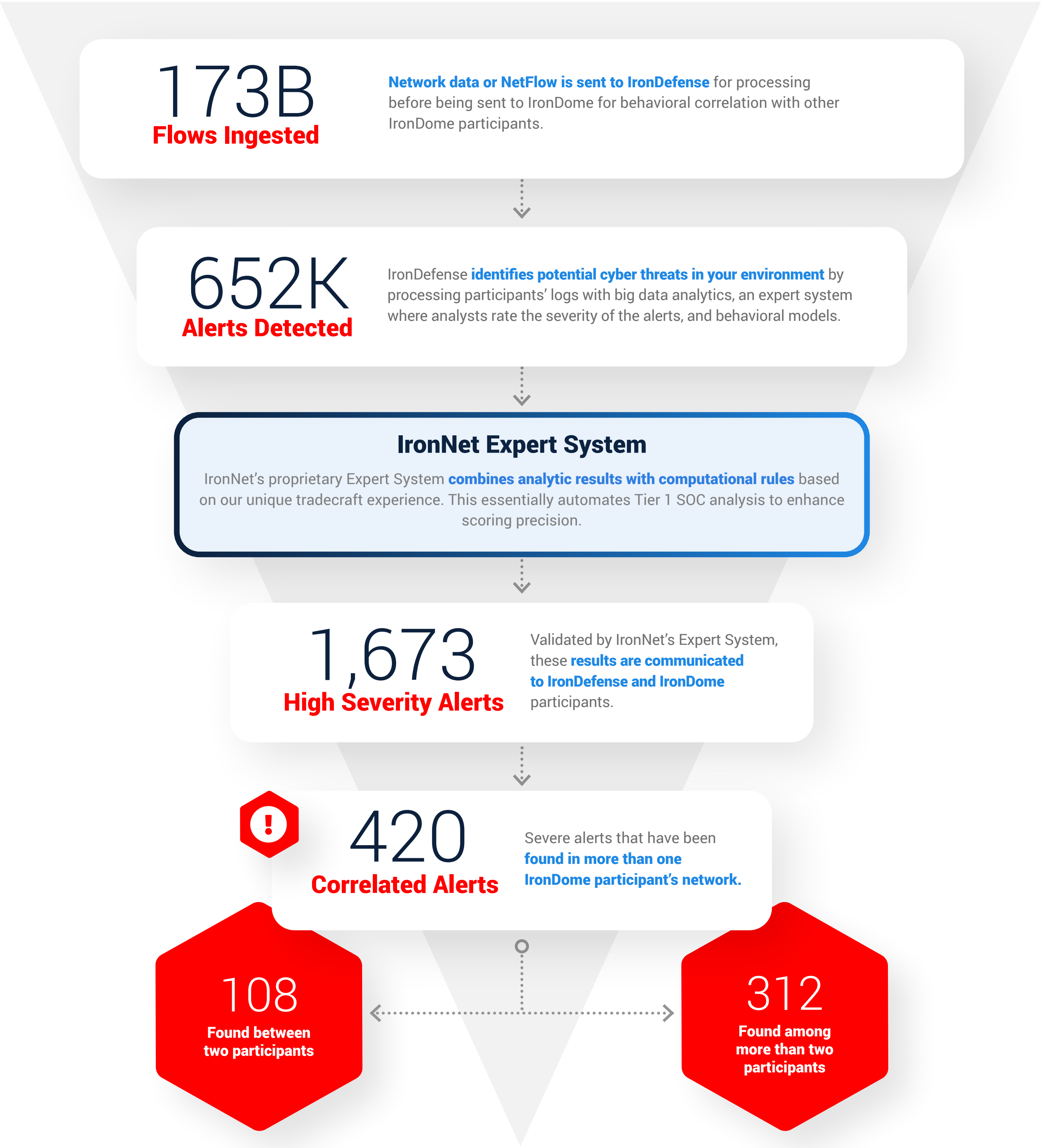
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



173B
Flows Ingested

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

652K
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.

1,673
High Severity Alerts

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

420
Correlated Alerts

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

108
Found between two participants

312
Found among more than two participants

Tracking Industry Threats

Adversary Infrastructure Report 2020

A recent report from Recorded Future detailed C2 infrastructure seen in the past year. The report states that over half of the C2 servers detected were not in any open source feeds and that a third of the C2 servers were hosted in the United States, with Amazon and Digital Ocean being the most prevalent. Metasploit and Cobalt Strike dominated as the tools of choice for C2 servers. The report also discussed the significant number of lesser-known open source tools in use, which reaffirms the criticality of dedicated threat intelligence resources allocated to tracking new tools used by adversaries.

The rise in the use of reputable hosting providers and the lack of more than half of these C2 domains appearing in open source feeds highlights the need for behavioral detections to cover these blind spots. Recorded Future predicts Cobalt Strike to remain the top tool of choice for 2021, but also expects to see an uptick in other open source tools, such as OctopusC2, Mythic, and Covenant.

SUNSPOT Build Process Implant

On January 11, CrowdStrike released a report detailing the SUNSPOT implant used to inject the SUNBURST backdoor into the SolarWinds Orion platform. The implant was found in the SolarWinds build environment and monitored for processes involved in the compiling of the Orion IT management product. During compilation, SUNSPOT replaces key source files with ones that contain SUNBURST. SUNSPOT takes many precautions to ensure the build does not fail, as this would draw scrutiny from SolarWinds developers.

SonicWall Breach

On Friday, January 22, the cybersecurity firm SonicWall disclosed a security breach where “highly sophisticated threat actors” leveraged probable zero-day vulnerabilities in the firm’s secure remote access products. At this time, the Secure Mobile Access (SMA) version 10.x appears to be the only affected product. NetExtender VPN client version 10.x was also originally thought to be affected, but SonicWall has since ruled it out.

For organizations using the affected products, SonicWall currently recommends enabling multi-factor authentication (MFA), allowing only safe listed IP address ranges to interact with the SMA devices, and disabling access to firewalls via the NetExtender client. Safe listing will present a challenge for security administrators due to the rise of remote workforces. Enabling multi-factor authentication is critical to ensure remote employees are securely accessing internal resources.

As of February 3, SonicWall has announced a patch for affected SMA firmware. IronNet continues to track this threat and, although we do not use any SonicWall solutions, will remain vigilant with our remote access products. We encourage all IronNet customers to do the same to safeguard internal enterprise applications.

Sudo Vulnerability Patched

On January 27, a critical vulnerability in the Sudo utility discovered by Qualys researchers was patched. This vulnerability has affected most Linux systems for the past 10 years and allows any local user who does not have root access to have full access to the entire machine using a heap-based buffer overflow. The bug cannot be exploited remotely and can only be used for privilege escalation. Administrators are encouraged to update their systems with the patch as soon as possible. If updating is not a possibility, it is critical that defenders are able to detect phishing, malware delivery, and C2 activity before threat actors are able to act.

Emotet Takedown

The Emotet malware has been brought down thanks to a widespread, coordinated defense effort. Dedicated collaboration among Europol; the FBI; the U.K. National Crime Agency; and the Dutch, German, Lithuanian, Canadian, and Ukrainian Police dismantled what is presumed to be the largest botnet in existence. Fernando Ruiz, Head of Ops for Europol's EC3, stated, "This is probably one of the biggest operations in terms of impact that we have had recently and we expect it will have an important impact." This takedown is a major win and illustrates what Collective Defense can accomplish.

The Emotet malware family is a common precursor to ransomware attacks. Although IronNet can detect Emotet on customer networks at a variety of stages using the Phishing HTTPS, TLS Invalid Certificate Chain, Encrypted Communications, and Consistent Beaconing analytics, the malware can still have dire consequences if it remains undiscovered. You can learn more about the evolution of Emotet in our recent on-demand webinar.

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.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of IronNet Cybersecurity, Inc.

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

STRONGER AS ONE:

The Case for Collective Defense

IronNet™

IronNet.com