IronNet™

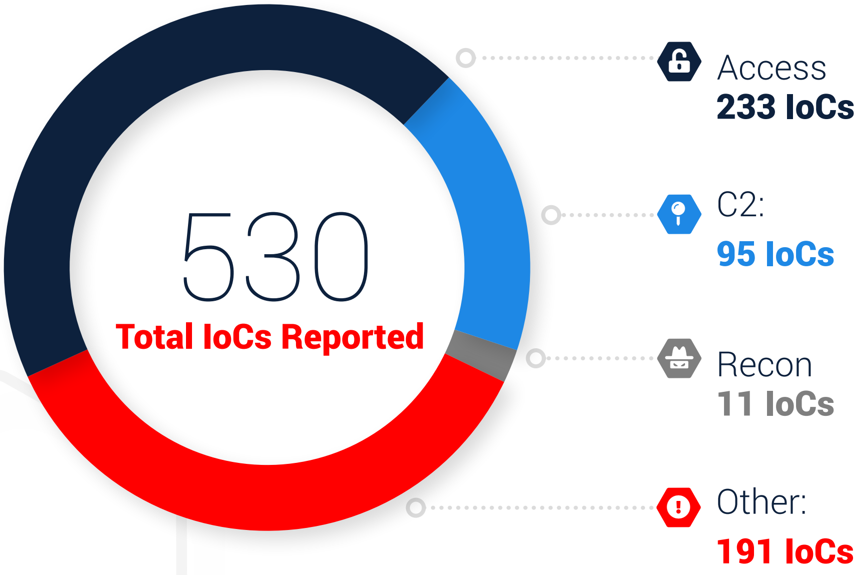
Edition #23: November 2021

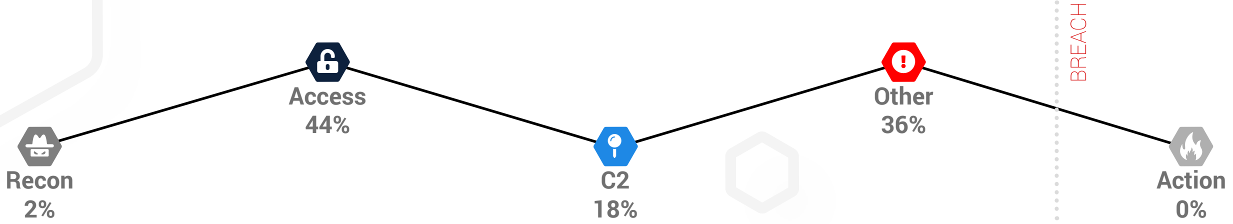
IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
October 1 – October 31, 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.





Recent Indicators of Compromise

Domain/IP	Rating	Analyst Insight
freefiles-8[.]de	MALICIOUS	A suspicious file downloaded from this domain triggered an alert. The downloaded file is identified as a malicious DownloadGuide by numerous security vendors. These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We recommend blocking this domain.
bringexpose[.]top	MALICIOUS	This domain was found within a URL that was imbedded in an email. When clicked, the link redirected the user to http://preferabletask[.]xyz/euNXv7bp/Amul-wa/?_t=1633881723rpv. What is hosted on this site is unknown, but similar redirects by this domain include phishing scams urging the user to claim a prize, which can result in potentially unwanted programs (PUP). We recommend blocking the domain.
payapl[.]com	MALICIOUS	The typo-squatting domain payapl[.]com/us/webapps/mpp/requesting-payments was found as a link submitted via a user agent in Microsoft Office Excel 2014. We recommend blocking the domain.
gravelyelectricthicket[.]com	SUSPICIOUS	This domain is associated with Terraclicks, a known browser redirector. Redirected clients can result in drive-by downloads that open up unwanted exposure to future injection sources. Connection attempts to these domains should be investigated and the domains and IPs blocked.
alcoholicsort[.]com	SUSPICIOUS	This domain is related to spam/phishing activity and was reported as Suspicious by VirusTotal, McAfee, and Symantec OSINT.
auntietraumatizemobile[.]com	SUSPICIOUS	This is a Terraclicks-related domain. Ads served by Adsterra are known to redirect traffic to sites hosting malicious content. We recommend blocking this IP and any related domains.
1337x[.]to	SUSPICIOUS	This domain was flagged for JAWS Webserver Unauthenticated Shell Command Execution. This attempt appears to have been unsuccessful, and we recommend blocking the domain.
glimpsemankind[.]com	SUSPICIOUS	Traffic to glimpsemankind[.]com currently resolves to 192.243.59.20, which is a known Terraclicks IP. We recommend blocking the domain.
online-reschedule-check[.]com	SUSPICIOUS	hermes.online-reschedule-check[.]com is a phishing scam impersonating the German postal carrier, Hermes.
guanggoo[.]net	SUSPICIOUS	This domain potentially sells scam products. We recommend using caution when browsing this site.

Threat Rules Developed

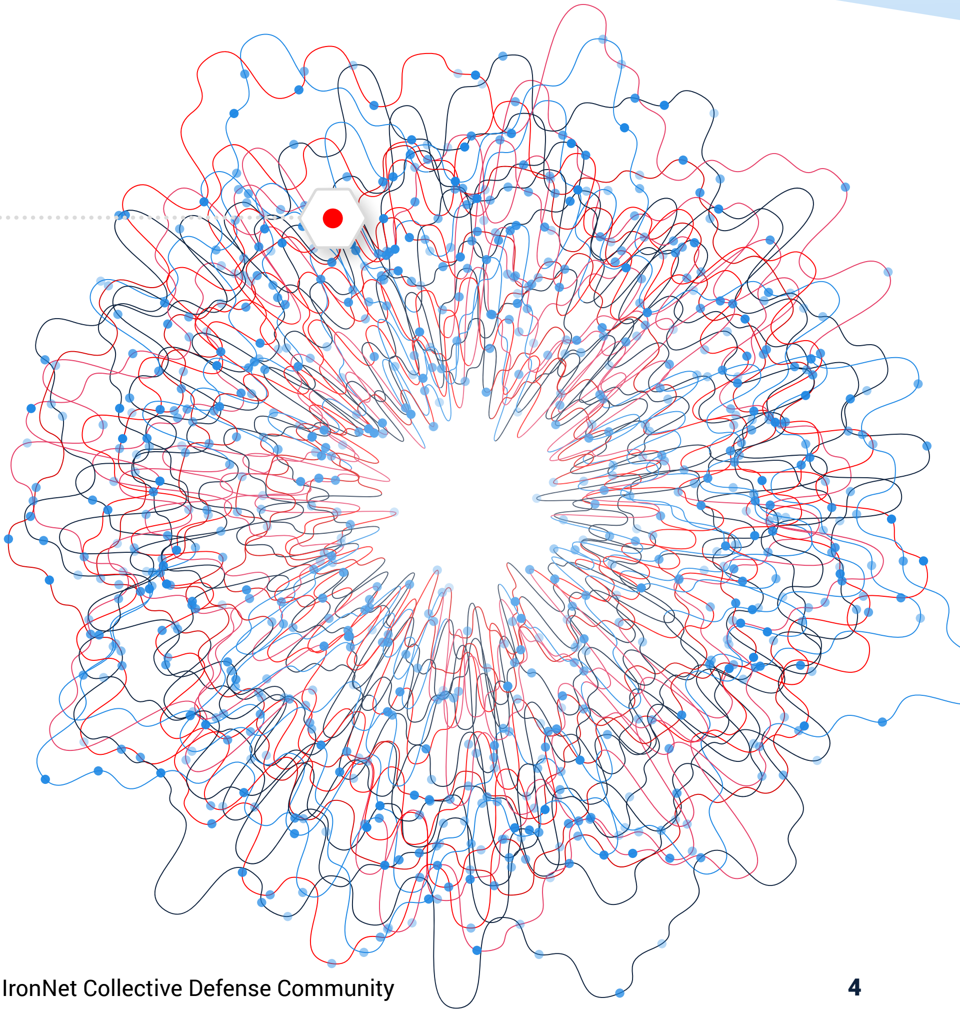
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

6,048

Threat Intel Rules Developed This Month

275,115

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:

- Malware delivery domains for Gafgyt, AgentTesla, Sabsik, Dridex, Nekark, and LnxGafgyt malware
- IoCs related to Cobalt Strike beacon payload distribution and Command and Control
- IoCs surrounding the Chinese state-sponsored APT41 threat group
- IoCs surrounding Dopplepaymer and Hancitor malware activity
- IoCs related to FIN12's use of the DaveShell loader
- IoCs related to SolarMarker malware activity

Rating alerts diminishes alert fatigue for your SOC.

This Month in the IronDome

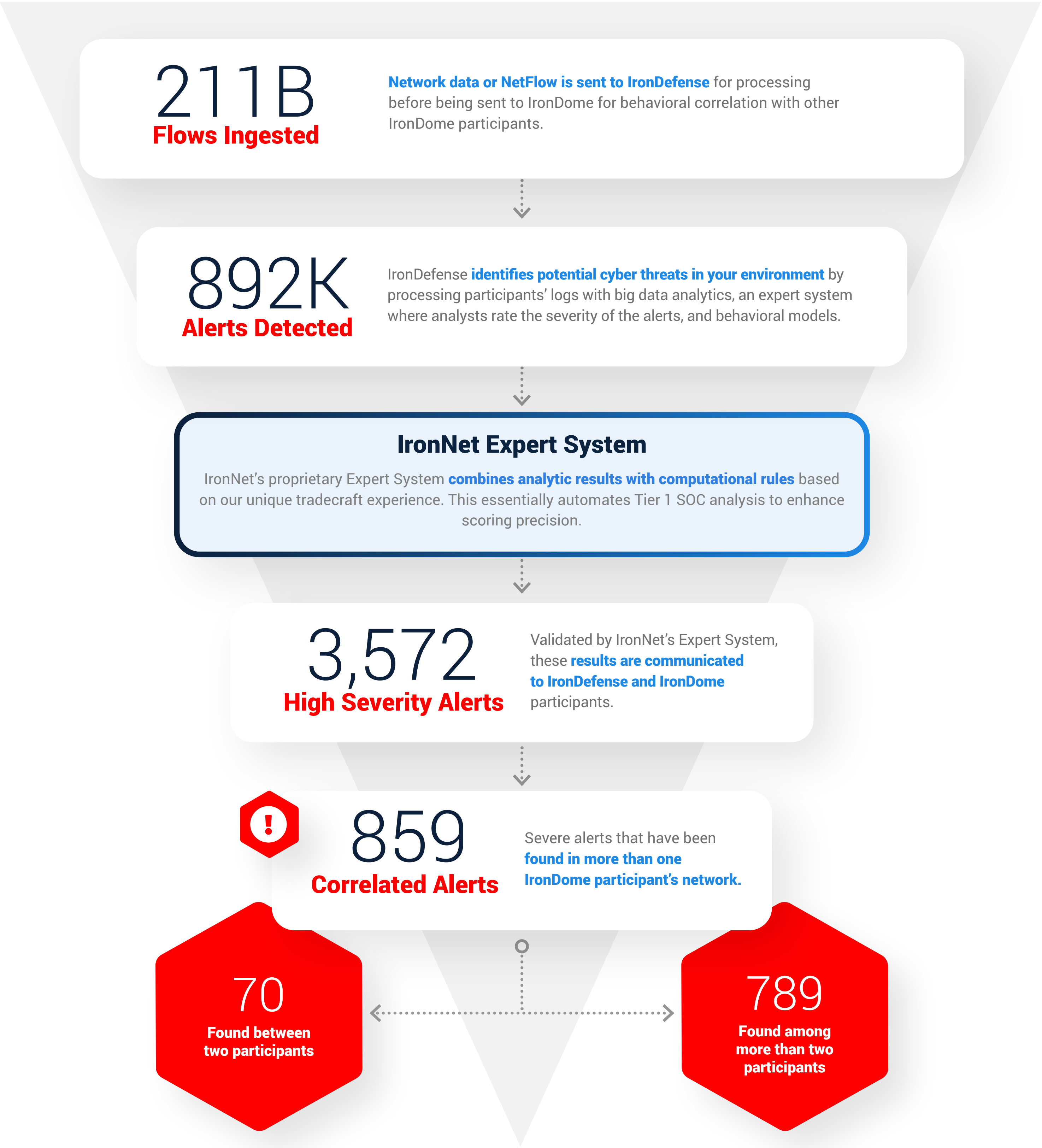
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



211B

Flows Ingested

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

892K

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.

3,572

High Severity Alerts

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

859

Correlated Alerts

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

70

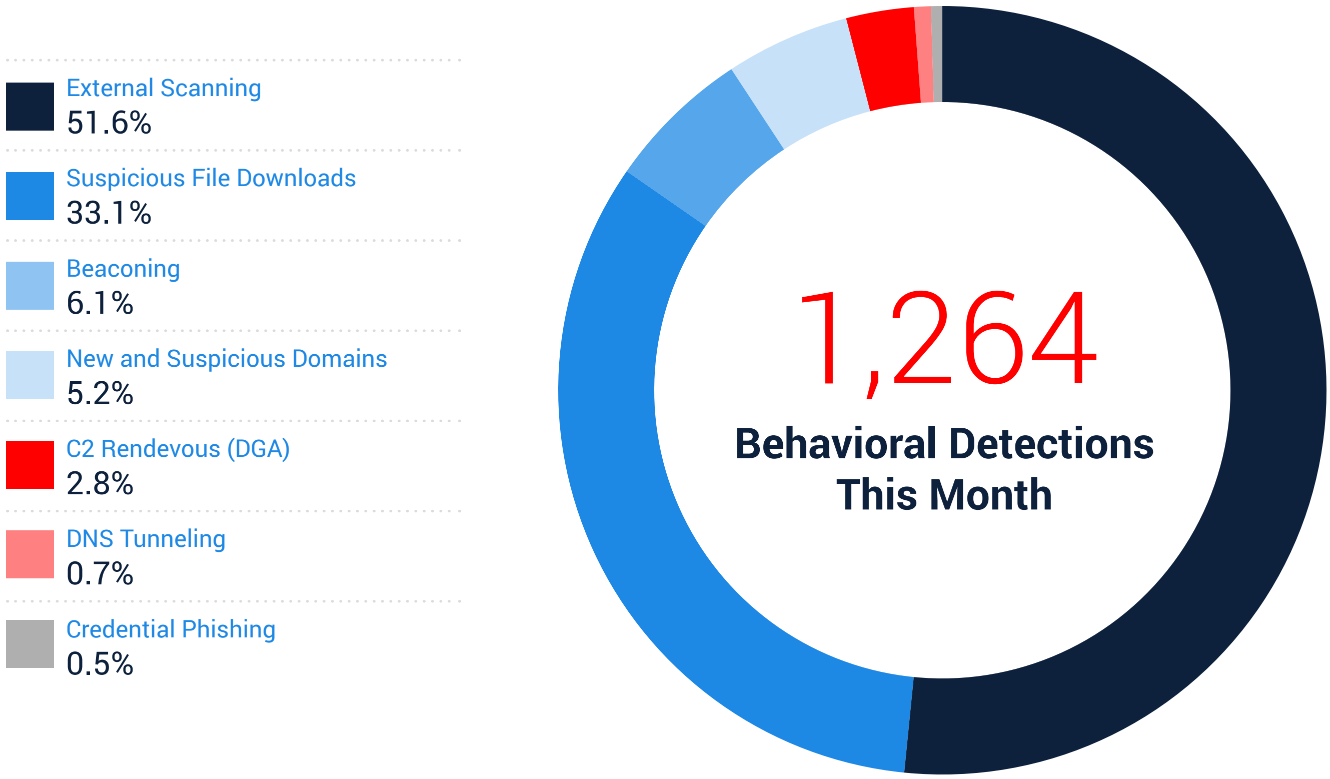
Found between two participants

789

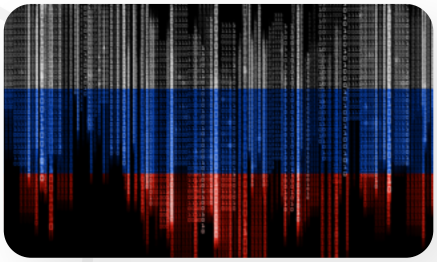
Found among more than two participants

Top Most Frequent Behavioral Analytics

IronDome's unique cross-sector visibility and Collective Defense capabilities highlight each month's most frequent behaviors, enabling us to track trends over time.



Tracking Industry Threats



Russia Turns Up the Heat

Recent research from Microsoft reveals that between July 2020 and June 2021, Russia was responsible for approximately 58% of all nation-state attacks. As opposed to disruption, this increased targeting of government agencies is mainly for intelligence gathering purposes. Targeting government entities—mainly agencies involved in foreign policy, defense, and national security—to gather intelligence has become one of Russia's primary objectives, catapulting from 3% of their targets last year to 53% this year. And not only are the number of attacks rising, so is the success rate of their operations. Attacks from Russian state-sponsored threat actors rose from a 21% successful compromise rate in 2020 to a 32% rate in 2021, with the majority of their targets being in the U.S., the U.K., and Ukraine. During this time, the most active Russian state-sponsored APT was APT29 (aka, Nobelium), constituting 92% of notifications about Russia-based threat activity that Microsoft sent to its customers over the past year.

Reinforcing the threat from malicious Russian cyber activity, Google has recently detected a widespread phishing campaign attributed to APT28 (aka, Fancy Bear). APT28 has been connected to Russia's General Staff Main Intelligence Directorate (GRU) and was responsible for big-name attacks, such as the compromise of the Democratic National Committee (DNC) and Hillary Clinton's campaign in 2016. Google identified a larger than usual number of alerts in September that were traced to a small number of wide-target campaigns that were blocked. As a result, Google has warned roughly 14,000 of its users that they might be victims of a state-sponsored phishing campaign from APT28. Gmail blocked all the phishing emails from the APT28 campaign, automatically classifying them as spam and redirecting them from going to the users' inboxes. APT28 typically runs operations for the purpose of exfiltration and espionage activity. It is likely they were using this campaign as an effort to gain initial infiltration into various networks that may be of intelligence value to the Russian government.

APT35 Phishing Campaign

Google's Threat Analysis Group (TAG) reported that in early 2021, Iranian state-sponsored APT35 compromised a website affiliated with a U.K. university to use it for credential phishing purposes. The threat actors sent emails that contained links to this compromised website, instructing users to activate an invitation to a fake webinar by entering their login credentials. The phishing kit also asked for multi factor authentication (MFA) codes. APT35 has leveraged this technique since 2017, continuously using compromised websites to appear legitimate.

In addition, APT35 is known to impersonate conference officials to carry out phishing campaigns. For example, in the campaign just discussed, the attackers used the Munich Security and the Think-20 (T20) Italy conferences as lures in initial non-malicious contact emails. Once users respond, then the attackers send the phishing links in follow-up correspondence. Targets would typically have to navigate through at least one redirect before landing on a phishing domain. APT35 also uses Telegram API to notify operators, embedding JavaScript into phishing pages to notify when the page is being loaded. Google made Telegram aware of this bot, and Telegram is actively working to remove it.

SquirrelWaffle Malspam Campaigns

SquirrelWaffle is a malware loader that provides threat actors with an initial foothold into networks, allowing them to drop additional malware. Beginning in mid-September 2021, researchers observed malicious spam (malspam) campaigns being used to deliver Microsoft Office documents that serve as the initial stage of the infection process. The campaigns appear to be leveraging email thread hijacking, and they are designed to trick the potential victim into accessing the included hyperlink to download a ZIP archive, which contains malicious Microsoft Office files.

Throughout the campaigns, multiple efforts were made to evade detection. The Microsoft Office documents contain a malicious code that uses string reversal for obfuscation, writes a VBS script, and then executes it. This action fetches SquirrelWaffle from one of the five hardcoded URLs and delivers it as a DLL file onto the infected system. The DLL functions as a malware loader, enabling the infections to be used to deploy additional malware. In these campaigns, SquirrelWaffle has been frequently observed coinciding with Qakbot and Cobalt Strike installations. The loader also uses an IP block list consisting of several known sandboxes and analysis platforms, and one of the distribution servers appears to have had antibot deployed shortly before the SquirrelWaffle campaigns using this server launched.

Over the past few years, Emotet has been one of the primary threats delivered via malspam campaigns. Since the coordinated law enforcement takedown of the Emotet botnet in January, many have been waiting for another threat to fill the void left by Emotet's exit. While SquirrelWaffle is not yet reaching the same level seen previously with threats like Emotet, it appears to be used consistently and its appearances may increase over time as the threat actors infect more users and increase the size of their botnet.

APT 29 Targets MSPs and NPM Library Hijacked

APT29 TARGETS MSPS

Microsoft recently published a report detailing APT29's latest actions abusing trusted relationships and targeting the IT supply chain. APT29, also known as Nobelium, has been connected to Russia's Foreign Intelligence Service (SVR) and is most well-known for its compromise of SolarWinds. Since May 2021, the group has targeted 140 managed service providers (MSP) across the U.S. and Europe, successfully breaching 14. Microsoft has informed 609 customers a total of 22,868 times that they had been targeted by APT29 since the beginning of July. This is a big shift from the total of 20,500 notifications sent out to customers over the past three years about attacks from all nation-state actors.

The main targets in this campaign are resellers and technology service providers that deploy and manage cloud services. The goal is to target the privileged accounts of upstream providers to move laterally in cloud environments and gain access to downstream customers. Essentially, they want to piggyback on any access that resellers may have to their customers' systems. In one example intrusion chain observed by Microsoft, APT 29 chained together artifacts from four other distinct providers to reach their end target, exemplifying the breadth of tactics, techniques, and procedures (TTP) APT29 leverages to exploit trusted relationships. These attacks are a continuation of APT29's dynamic and diverse toolkit that includes token theft, sophisticated malware, password sprays, and spear phishing to gain access to privileged accounts.

NPM LIBRARY HIJACKED

Hackers hijacked the NPM library UA-Parser-JS, an incredibly popular library with millions of downloads per week that parses a browser's user agent. On October 22nd, the attackers published three malicious versions of the library to install cryptominers and password-stealing Trojans on Windows and Linux devices. The threat actors were able to gain access by targeting the NPM account of one of the developers of the project, who only noticed something was unusual after receiving hundreds of spam emails.

On Linux systems, a preinstall.sh script checks if the user is located in Russia, Ukraine, Belarus, or Kazakhstan. If it determines they are not, the script will download a program called jsextension, which is an XMRig Monero miner. This program uses only 50% of the device's CPU (central processing unit) to avoid detection. On Windows systems, the batch file will download jsextension and a dynamic link library (DLL) for a password-stealing Trojan, possibly DanaBot, that begins stealing the user's passwords for a variety of programs, including Chrome, WinVNC, Windows Credentials (local creds), mail programs, and more.

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**

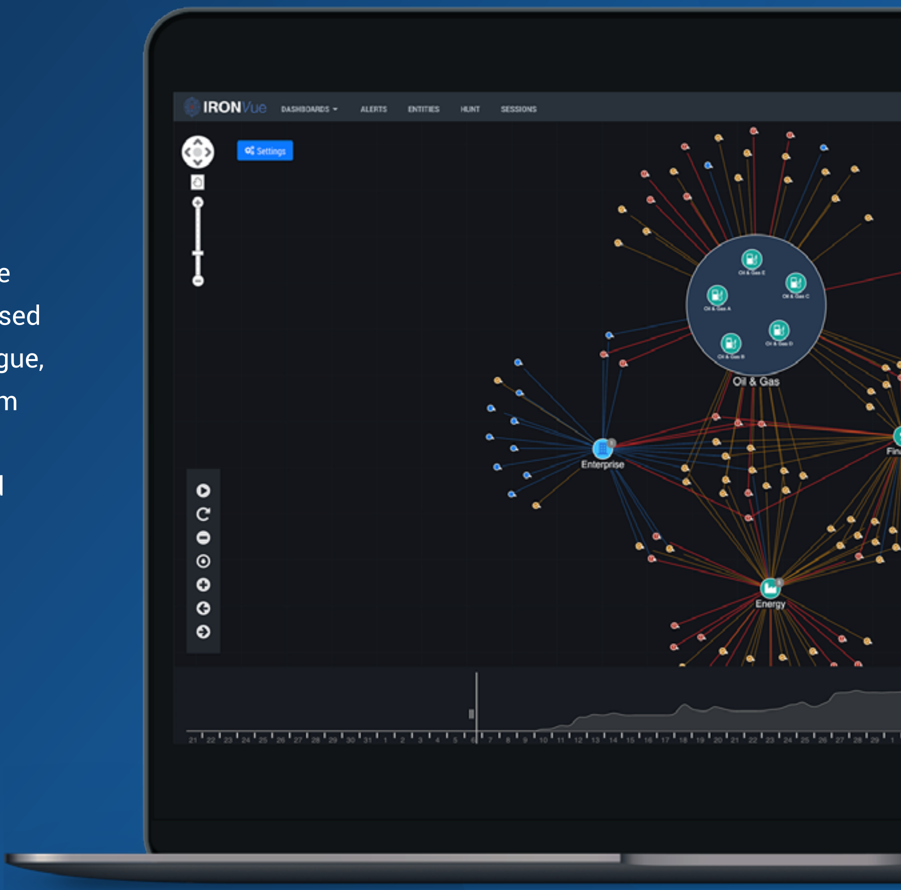
This report features threat findings, analysis, and research shared across IronDome, the industry’s first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations. IronDome participants work together in near-real-time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

Information in this document is for public use and 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, 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, 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.

IronNet

Collective Defense: A radar-like view of cyber threats

ACCESS THE BOOK →

IronNet™

IronNet.com