Edition #16: April 2021

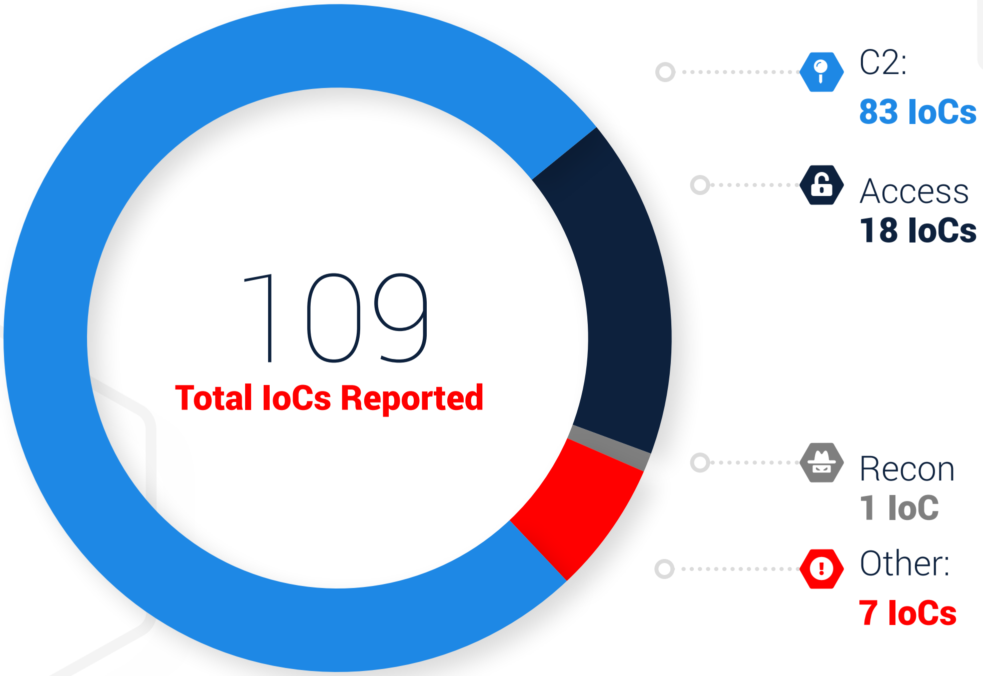
IronNet: Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community

March 1 – March 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

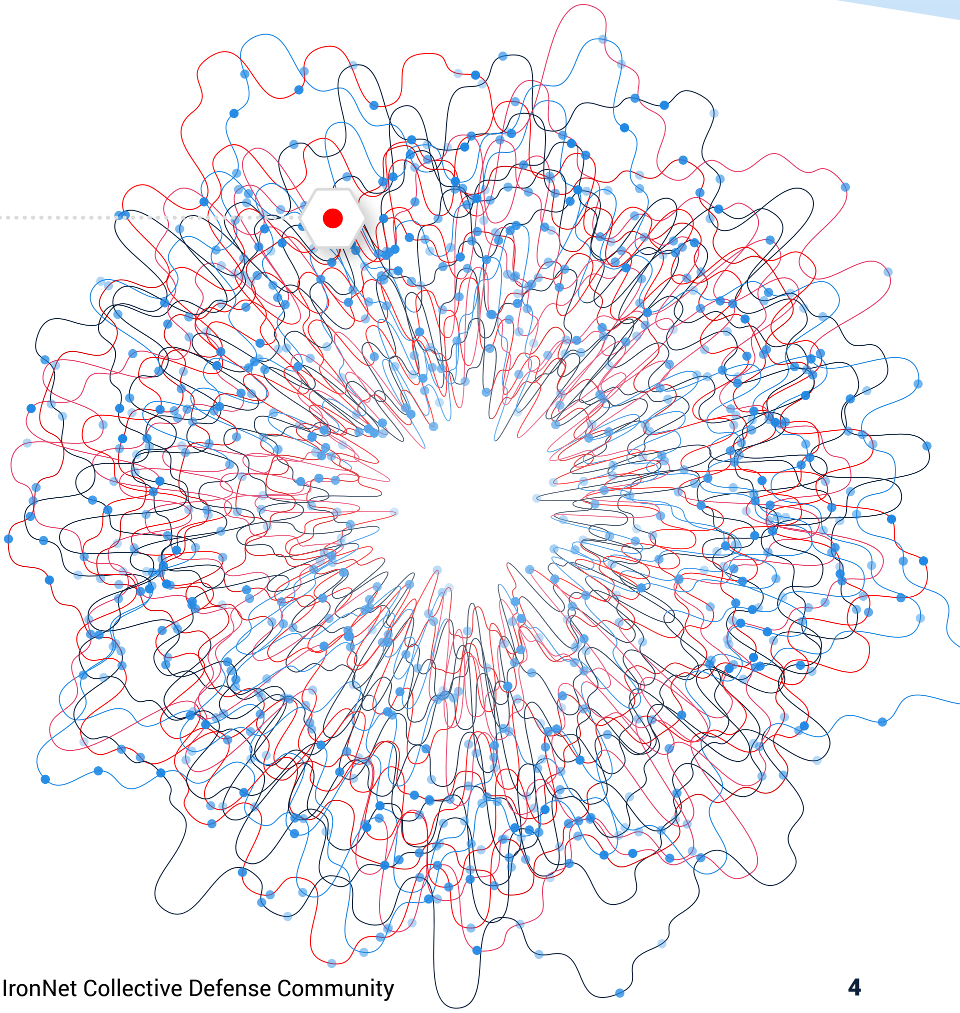
Domain/IP	Rating	Analyst Insight
ark[.]xyz	SUSPICIOUS	The presence of this domain may be indicative of the AMZ tool, an unwanted Chrome extension.
window98originalmain[.]live	SUSPICIOUS	This domain is associated with ad redirect software. In the traffic in question, the user was redirected to multiple sites associated with ad redirect software, including basque[.]buzz, window98originalmain[.]live, and comppiwareresfai[.]tk. There were no downloads observed, but the techniques used were indicative of malspam. We recommend blocking traffic to this domain.
ofertaexpressa[.]com	SUSPICIOUS	This domain provides email content in a phishing attempt involving password changes. We recommend blocking the domain.
amads[.]xyz	SUSPICIOUS	This IoC is related to an adware injector which injects a malicious PHP script into vulnerable WordPress installations.
feignoccasionedmound[.]com	SUSPICIOUS	This domain supplies an unknown script within certain ecommerce sites and may indicate the ability to conduct credit card skimming attacks. We recommend blocking the domain.
ifadulakvefin[.]tk	SUSPICIOUS	This domain serves as a clickbait ad-redirector. The domain presents a JavaScript to the client browser that then redirects the user to a site that encourages the user to click on a prize which could download riskware. We recommend blocking the domain.
root464providecatch[.]live	SUSPICIOUS	This is a flagged phishing site. If seen in your network, inspect the traffic and ensure the domain is blocked.
ark-btc[.]net	SUSPICIOUS	This is a Bitcoin phishing domain. If seen in your network, investigate the traffic and clients for potential loss of personally identifiable information (PII) and currency and block the domain.
avanquest[.]com	SUSPICIOUS	This domain may install software claiming to improve the user's system. This could impose risks to the organization's IT assets. If seen in your network, block the domain and investigate for unwanted traffic or software installed on clients' computers.
poolunbelievably[.]com	SUSPICIOUS	This is a TerraClicks-related redirect. If seen in your network, investigate the surrounding traffic for delivery of unwanted applications.

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.

13,299

Threat Intel Rules Developed This Month



202,774

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:

- Command and control (C2) domains associated with ZBot spyware
- Indicators associated with Nobelium malware
- Additional LokiBot indicators
- IoCs surrounding Hafnium's exploitation of Microsoft Exchange
- IoCs surrounding other hacking groups involved in the Microsoft Exchange exploitation
- C2 domains for the AZORult malware
- C2 domains for the Nanocore malware
- IoCs surrounding a new variant of Gafgyt that may be connected to the Necro botnet group
- C2 domains for the FormBook malware
- C2 domains for the Zeus Panda Trojan, which steals banking credentials and other sensitive information
- Malware delivery domains for the AgentTesla, Dridex, and Wacatac malwares
- C2 domains related to the NjRat malware, a backdoor RAT (Remote Access Trojan) that may attempt to steal user credentials and other information
- Malware delivery domains for Gafgyt and Dridex

Rating alerts diminishes “alert fatigue” for your SOC.

This Month in the IronDome

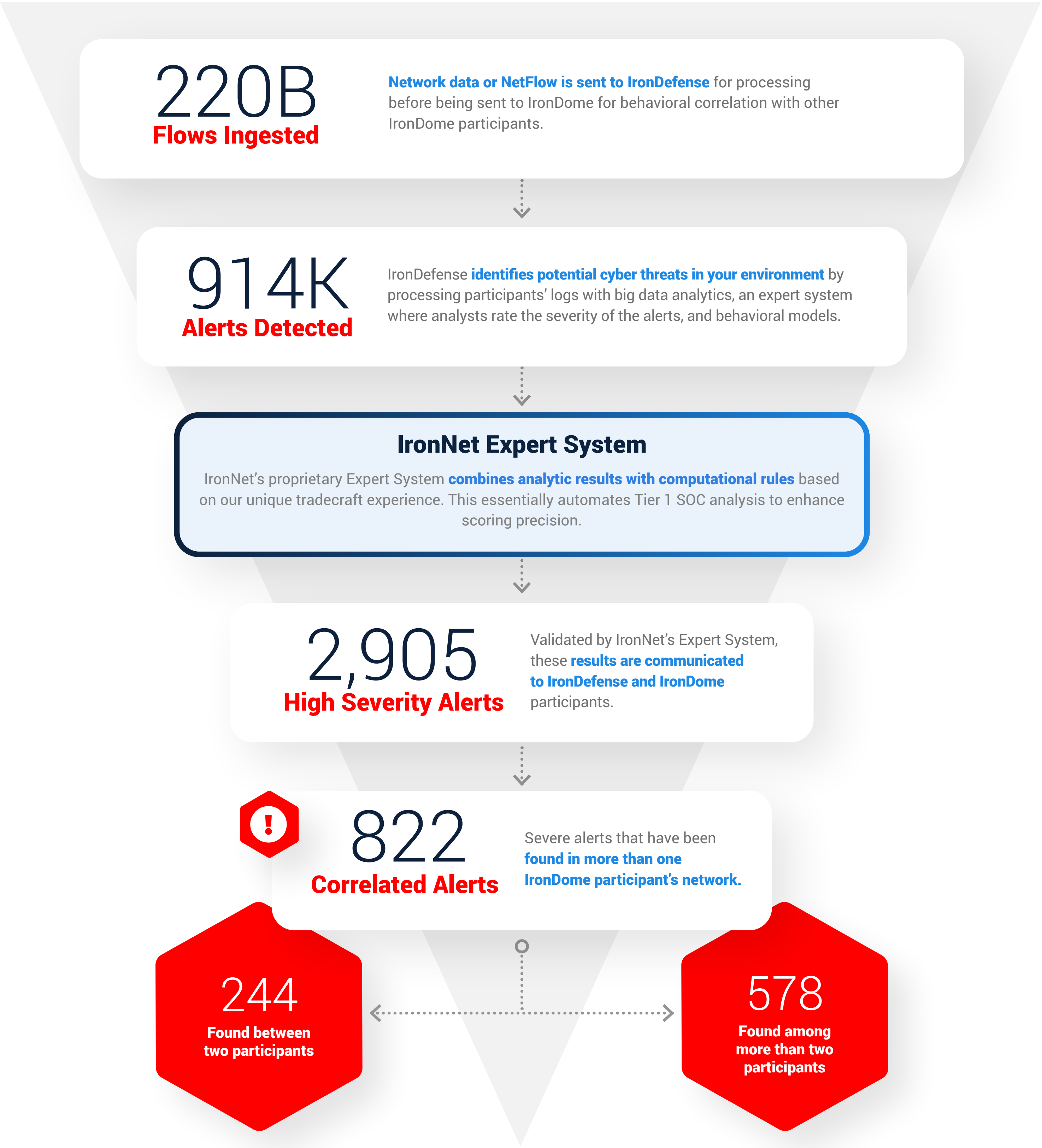
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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



220B
Flows Ingested

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

914K
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.

2,905
High Severity Alerts

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

822
Correlated Alerts

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

244
Found between two participants

578
Found among more than two participants

Tracking **Industry Threats**

Hafnium Targets Exchange Zero-day Vulnerabilities

On-premise instances of Microsoft Exchange have been identified as active exploits in a series of attacks utilizing a collection of zero-day vulnerabilities. The four vulnerabilities affect unpatched, on-premise Exchange servers from version 2013 to 2019, excluding Exchange Online (Office 365). These exploits and corresponding attacks have been attributed to Chinese advanced persistent threat (APT) Hafnium. Historically, this group has targeted U.S. entities with the goal of exfiltrating information from several industry sectors, including law firms, infectious disease researchers, higher education institutions, defense contractors, non-governmental organizations (NGO), and policy think tanks. Although Hafnium originated in China, it primarily operates from leased virtual private servers (VPS) in the U.S. to conceal its true location, exploiting the legal restriction that prohibits intelligence agencies from inspecting systems based in the U.S.

Though Hafnium is believed to have been exploiting these flaws since January 6th, Microsoft did not publicly acknowledge the vulnerabilities until March 2nd. Microsoft released several security updates to address the vulnerabilities, recommending administrators install the patches immediately. Since these vulnerabilities became well-known, numerous threat actors beyond Hafnium have also been conducting attacks: a total of five distinct hacking groups have been identified as exploiting these critical flaws in Microsoft's email software.

The threat actors exploit these vulnerabilities as part of an attack chain, in which they bypass authentication to secure access to an Exchange server and then create a web shell to take control of the system and execute remote commands. In this process, threat actors secure access to an Exchange Server either by utilizing stolen credentials or by exploiting CVE-2021-26855, a Server Side Request Forgery (SSRF) vulnerability that allows a remote attacker to send arbitrary HTTP requests to the Exchange Server and authenticate to it. After this initial attack, the attacker has bypassed authentication and is able to steal the full contents of multiple user mailboxes. As part of the attack chain, the threat actor then exploits other vulnerabilities. This includes CVE-2021-26857, which enables the attacker to run code as SYSTEM on the Exchange Server and post-authentication arbitrary file write vulnerabilities (CVE-2021-26858 and CVE-2021-27065) to deploy web shells to the compromised host in order to control the server remotely. The web shells (ASPX files) allow threat actors to steal data and conduct further operations on the compromised system. Following this, the attackers perform a wide range of post-exploitation activities, such as dumping LSASS process memory using Procdump, using 7-Zip to compress stolen data into ZIP files for exfiltration, exporting mailbox data through the use of Exchange PowerShell snap-ins, and using PowerCat (downloaded from GitHub) to open a connection to a remote server.

Further Details Emerge About Microsoft Exchange Zero-day Exploit

More information has surfaced about the Microsoft Exchange attacks and the timeline of exploits. Although Microsoft first stated that the attacks were “limited and targeted,” reports of much broader mass exploitation by multiple threat groups continue to emerge. It has been confirmed that various threat actors exploited the vulnerabilities prior to Microsoft’s release of the patch. This means that some Exchange users who deployed the patches on the same day Microsoft released them may have already been compromised by threat actors other than the China-based groups. All of the new reports raise the question of how so many hacking groups had access to the same information before it was made public.

GENERAL TIMELINE

The first in-the-wild exploitation of the vulnerabilities was reported by Volexity to have begun on January 3rd, 2021. Microsoft was alerted to these vulnerabilities by the security testing firm DEVCORE two days later. Other security firms began reporting active exploitation of the Microsoft Exchange vulnerabilities in late January/ early February, attributing the activity to the Chinese state-sponsored APT Hafnium. Around February 28th, researchers noticed that the vulnerabilities were being used by other threat groups, starting with Tick and followed closely by LuckyMouse, Calypso, and Winnti Group. After Microsoft publicly acknowledged the exploits and released patches to plug the zero-day flaws on March 2nd, mass exploitation expanded as multiple additional threat actors sought to capitalize on the vulnerabilities before organizations patched their servers.

EXPLOITERS AND TARGET ENTITIES

Researchers reported that at least ten different APT groups have used the Exchange vulnerabilities (or hijacked the webshells dropped by other groups) to compromise email servers. There are four known APTs that are believed to have begun exploits prior to the patch release:

- Tick, whose main goal seems to be intellectual property and classified information theft, compromised the web server of an IT company based in East Asia.

- LuckyMouse (aka. APT 27 or Emissary Panda) compromised the server of a governmental entity in the Middle East.
- Calypso compromised the servers of governmental entities in the Middle East and South America, targeting additional servers of government organizations and private companies in Africa, Asia, and Europe in the following days.
- Winnti Group (aka. APT 41 or Barium) compromised servers of an oil company and construction equipment organization based in East Asia.

There are several known APTs who targeted vulnerable servers *after* the patch release, including:

- CactusPete (aka. Tonto Team), who compromised the servers of a procurement company and a software development/cybersecurity consulting company based in Eastern Europe.
- Mikroceen (aka. Vicious Panda), who compromised the server of a utility company in Central Asia.
- DLTMiner, a group linked to a known cryptomining campaign who deployed PowerShell downloaders on multiple email servers that were previously targeted using the Exchange vulnerabilities.

There are also clusters of malicious activity that are so far unattributed to a specific APT, including:

A new cluster of activity dubbed Websiic, in which seven servers of private companies (IT, telecommunications, and engineering) in Asia and a governmental entity in Eastern Europe were targeted prior to the patch release.

ShadowPad activity, in which modular backdoor Shadowpad was dropped by an attacker to compromise the servers of a software development company in East Asia and a real estate company in the Middle East.

“Opera” Cobalt Strike activity targeting around 650 servers in the U.S. and Europe.

IIS backdoors, in which webshells were used to install IIS backdoors on at least four servers located in Asia and South America.

MAIN CONCERNS

Right now, the hacking appears to be focused on cyber espionage, but evidence of cybercriminal exploitation is emerging. On March 11th, Microsoft reported that there is a new family of ransomware that encrypts computer files, known as DearCry, that is being deployed after the initial compromise of Exchange servers. Kryptos Logic reported on March 12th that it discovered almost 7,000 exposed webshells initially installed by Hafnium that are now extremely vulnerable to the deployment of DearCry. If these webshells are not removed, the compromised servers remain open to intrusion by both the hackers who initially installed the backdoors and other threat actors who piggyback off of Hafnium.

It is very uncommon for so many different cyber espionage groups to have access to the same zero-day exploits before they are made public, raising questions of how so many hacking groups were able to exploit these vulnerabilities prior to Microsoft’s acknowledgment of them. There is a possibility that it happened to be simultaneous discovery or that China sold access to the exploit to distract from its overall objectives. There is evidence that, in some cases, the webshells were dropped into Offline Address Book (OAB) configuration files and appeared to be accessed by more than one group, possibly indicating some kind of collusion. However, there is wide speculation that the information was leaked from Microsoft itself or one of its partners. Microsoft is currently investigating possible ties between one of its partner security firms and the attack code leak, as the exploit tools deployed in the attacks are allegedly similar to PoC (proof of concept) code that was privately distributed by Microsoft to vendors.

SilverFish

Swiss cyber threat intelligence company PRODAFT recently released a report outlining its discovery of the sophisticated cyber espionage group SilverFish. The group is responsible for cyber attacks on over 4,720 targets, including government entities, defense contractors, aviation manufacturers, global IT providers, and Fortune 500 companies. Known to have strong ties to the SolarWinds attack and the Russian cybercriminal group EvilCorp, SilverFish targets institutions in the U.S. and E.U., focusing specifically on critical infrastructure and organizations with a market value of over $100 million.

HOW DID PRODAFT DISCOVER SILVERFISH?

After detecting a domain (databasegalore[.]com) related to the SolarWinds IoCs released by FireEye, PRODAFT's threat intelligence (PTI) team was able to create a unique fingerprint profile for the subject server. The PTI team then ran global scans of the IPv4 range to find a matching fingerprint, and within 12 hours, it identified over 200 hosts with similar characteristics. After filtering out false positives, the team detected and gained access to SilverFish's C2 server, through which it was able to acquire significant information about the group's modus operandi, victims, and command execution.

WHAT ARE THE GROUP'S GOALS AND MODUS OPERANDI?

SilverFish's executed tasks indicate that the group's main objectives are covert network reconnaissance and data exfiltration. SilverFish attackers use a variety of software and scripts for both initial and post-exploitation activities, making extensive use of publicly available red teaming tools, like Empire, Cobalt Strike, and Mimikatz, as well as specially-crafted PowerShell, JavaScript, and HTA (HTML application) files. With most of its activity occurring on weekdays between 8:00 and 20:00 UTC, the group follows a strong behavioral pattern that includes enumerating domain controllers and trusted domains, displaying memory resident credentials and admin user accounts, and launching scripts for post-exploit reconnaissance and data exfiltration activities.

WHAT MAKES SILVERFISH UNIQUE?

When looking inside the C2 server, the PTI team discovered that the main dashboard of the SilverFish C2 panel featured a section labeled "Active Teams" involving comments (in both English and Russian) on victim records entered by different user groups (e.g., Team 301, 302, 303, and 304). This indicates that SilverFish adopted a team-based workflow model and triage system akin to project management applications like JIRA. SilverFish is also unique because its C2 server had a hierarchical structure, meaning each team is assigned new victims by an administrator (or has victims auto-assigned to them by the system based on the current workload) and can only access the victims allocated to them. It is quite uncommon to see accounts with differing permission levels managing a C2 server.

SilverFish also designed an unprecedented malware detection sandbox formed by real enterprise victims. This enabled the group to test out its malicious payloads on live victim servers with various enterprise antivirus and endpoint detection and response (EDR) solutions, including Sophos Antivirus, Norton Security, and CrowdStrike Falcon Sensor, further supporting the high success rate of its attacks. Tracking the detection rate of its payloads in real time, SilverFish has used this system to periodically test its malicious payloads on over 6,000 victim devices, scripts, and implants.

Updates to SilverFish and Microsoft Exchange Vulnerabilities

SILVERFISH

Since the release of PRODAFT's March 18th report on the sophisticated cyber-espionage group SilverFish, IronNet's Threat Analysis and Emerging Threats and Detection Research (ETDR) teams have joined together to further analyze the malware used in these cyberattacks. Our teams were able to retrieve malicious post-exploitation scripts and observed some of the GET requests to adversary infrastructure, which included host information such as username, domain, and IP addresses, encoded in base64. The Threat Analysis and ETDR teams are working to unpack the malicious executable in order to understand adversary targets and post-exploitation objectives, and identify new IoCs.

MICROSOFT EXCHANGE

The Shadowserver Foundation, a nonprofit security organization, has recently released a report stating it has discovered 21,248 different Exchange servers that appear to be compromised by a backdoor and are communicating with the domain brian[.]krebsonsecurity[.]top. Using a combination of internet scans and honeypots, Shadowserver searched for attacks on Microsoft Exchange servers, keeping a close eye on hundreds of unique backdoor variants that cybercrime groups have employed to gain control of unpatched Exchange servers. On March 26th, Shadowserver identified attempts to install a new backdoor, known as Babydraco, on compromised systems. In each case, the hacked hosts deployed the backdoor in the same location: /owa/auth/babydraco.aspx. Shadowserver's honeypots witnessed numerous compromised hosts with the Babydraco backdoor conducting identical activity: a Microsoft PowerShell script runs and grabs the file krebsonsecurity.exe from the IP address 159.65.136[.]128. The file installs a root certificate, modifies the system registry, and instructs Windows Defender not to scan the file. The Krebsonsecurity file will then attempt to open an encrypted connection between the compromised Exchange server and the IP address mentioned above, sending a small amount of traffic to it that gradually grows by the minute.

The motivations of the cybercriminals behind the brian[.]krebsonsecurity[.]top domain are unclear so far, but the domain itself is known to have recent connections to other cybercrime activity. Security expert Brian Krebs from KrebsOnSecurity has stated that he is not the one behind these attacks. This is far from the first time that malware has abused his name or website trademarks.

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**

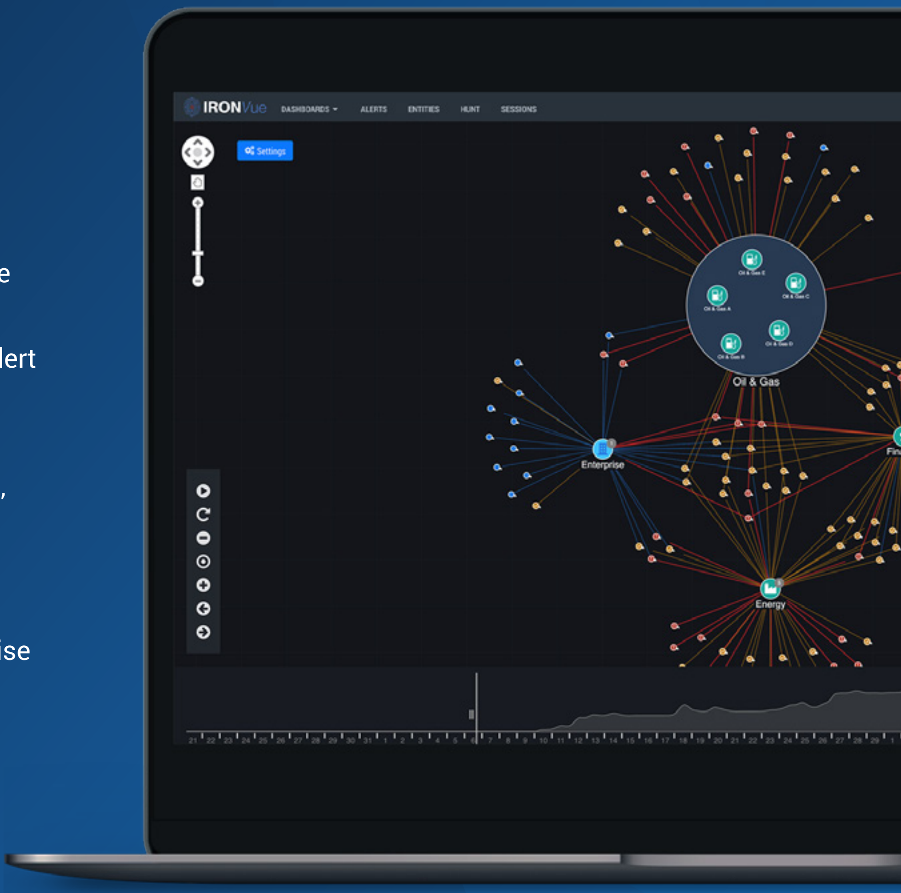
This report features threat findings, analysis, and research shared across IronDome, the industry’s first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations so IronDome participants can work together in near-real-time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

IronNet

STRONGER AS ONE:
The Case for Collective Defense

ACCESS THE BOOK →

IronNet.com