IronNet™

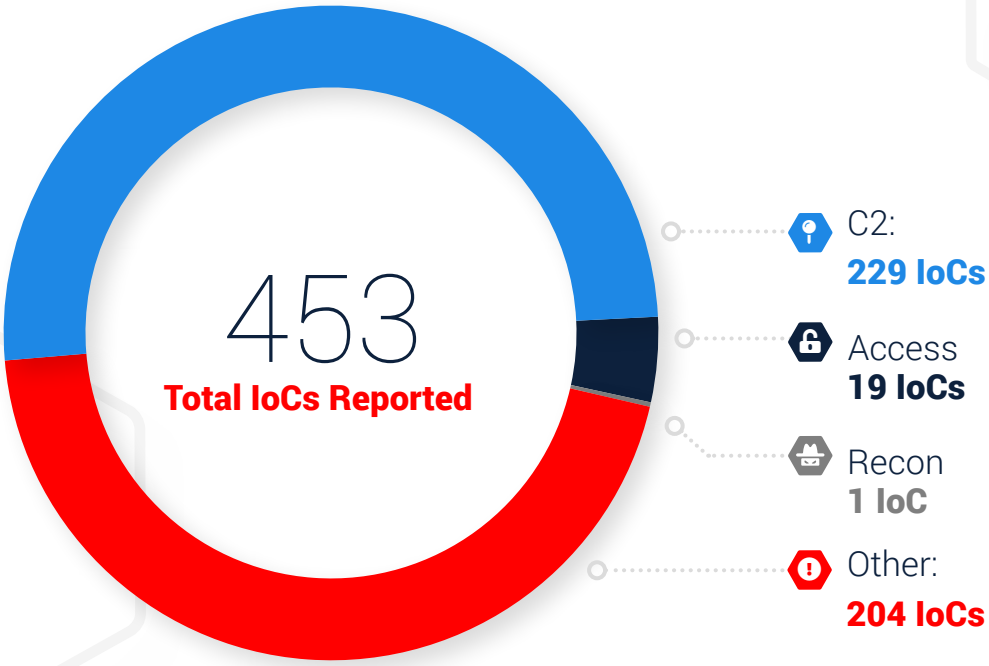
Edition #20: August 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
July 1 – July 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
chilicuoghi[.]com	MALICIOUS	This is a phishing domain that could lead to potential personally identifiable information (PII) data loss. We recommend blocking the domain if it is seen in your network.
danakabob[.]com	MALICIOUS	danakabob[.]com is a domain involved with email spearphishing attempts. If the spearphishing attempt is successful, the client will navigate to https://danakabob[.]com/OV5, landing on a spoofed site that attempts to lure the user into providing credentials and/or downloading a possible Trojan. Ensure the connection is blocked.
www.peaksandpines[.]in	MALICIOUS	This is a phishing scam that has been taken down. Ensure no data from your network has been posted.
peaksandpines[.]in	MALICIOUS	This is a phishing scam that has been taken down. Ensure no data from your network has been posted.
modernnorth-fast[.]top	MALICIOUS	This domain was reported to be part of a phishing campaign and was registered recently on July 27, 2021. Ensure the domain is blocked and that no bidirectional traffic ensued.
search.modernnorth-fast[.]top	MALICIOUS	This domain was reported to be part of a phishing campaign and was registered recently on July 27, 2021. Ensure the domain is blocked and that no bidirectional traffic ensued.
172.58.188[.]150	SUSPICIOUS	This may be an internet scanner looking for web vulnerabilities. The related IP address 192.241.221[.]9 is another internet scanner looking for Chromecast devices.
vnoprescmed[.]com	SUSPICIOUS	This domain is a fraudulent online pharmacy site and has been categorized as spam by OSINT and at least one security vendor. The site has numerous negative reviews and is described as unregulated and untrustworthy.
gmai[.]com	SUSPICIOUS	This is a redirect to a suspicious domain that appears to be phishing for Gmail credentials. The initial domain observed was abuelos[.]com, which redirected a user to gmai[.]com. IronNet recommends investigating any traffic to this domain and blocking the domain.
parshaops[.]ga	SUSPICIOUS	This is a potential scam site claiming to sell merchandise. We recommend using caution when browsing this site.

Threat Rules Developed

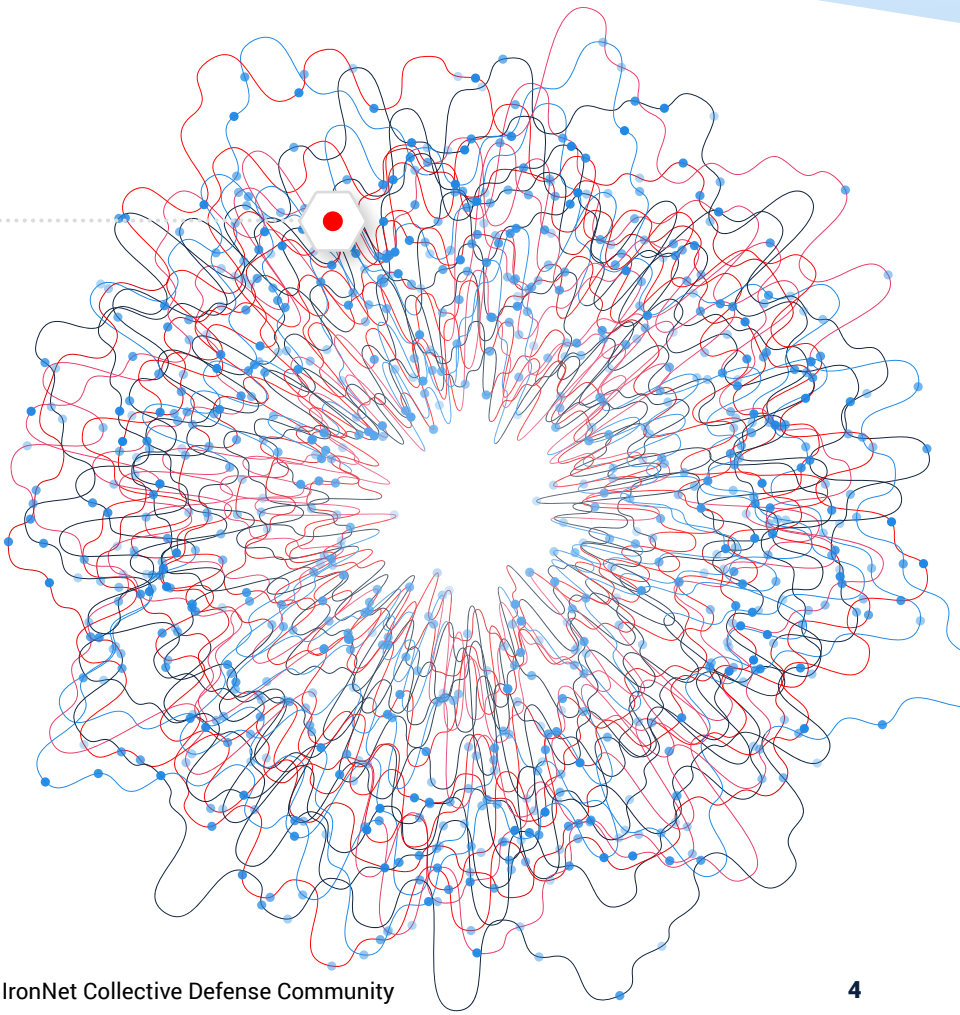
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants. 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.

7,909

Threat Intel Rules Developed This Month

258,895

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, Dridex, Seraph, and Morila malware
- IoCs related to Cobalt Strike beacon payload distribution and command and control (C2)
- IoCs surrounding the Chinese state-sponsored group tracked as Threat Activity Group 22 (TAG-22)
- IoCs surrounding the Iranian Tortoiseshell Facebook campaign
- IOCs surrounding NSO Group's Pegasus spyware
- IoCs surrounding the Shlayer malvertising campaigns

This Month in the IronDome

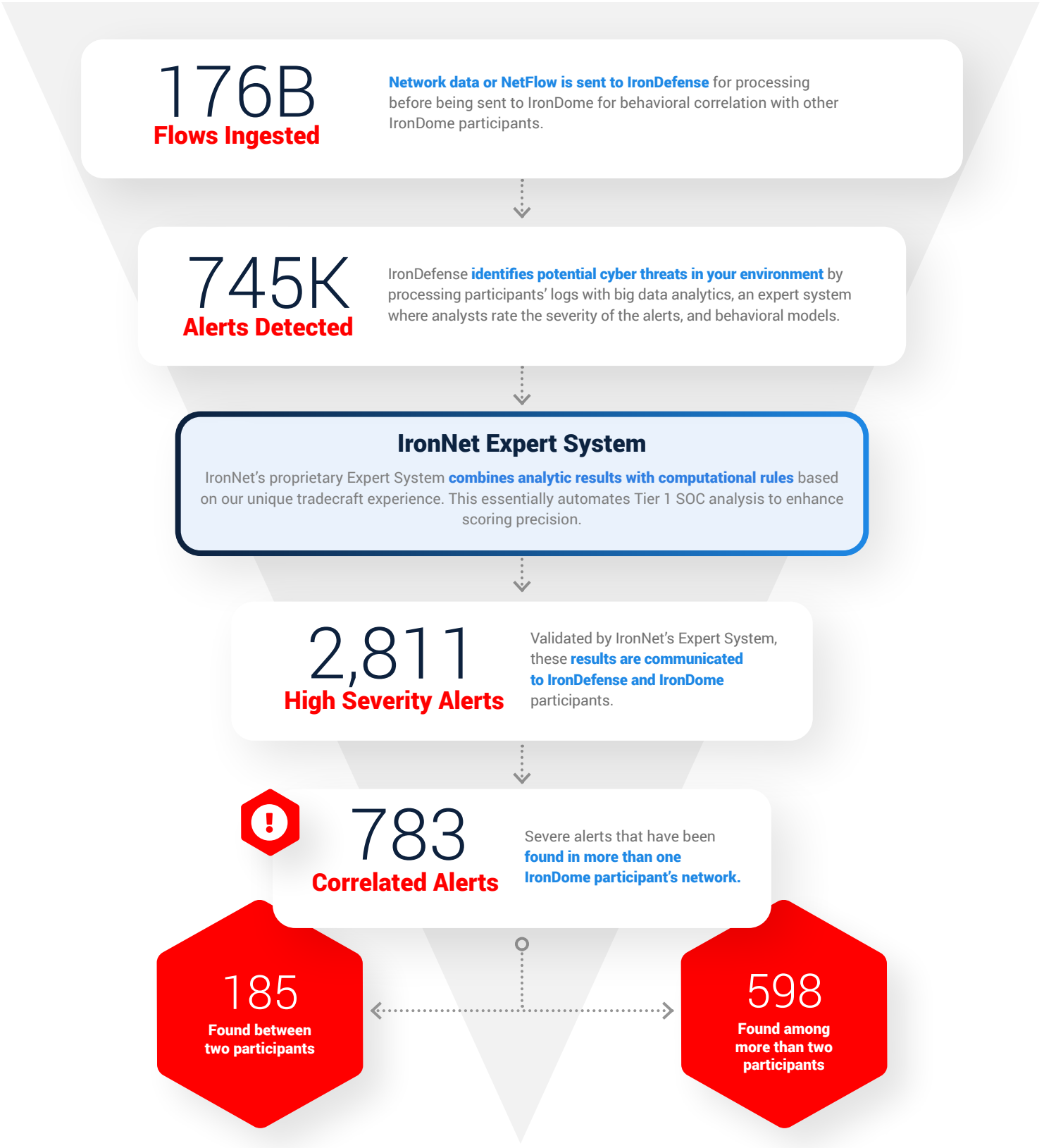
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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

Formbook XLoader (MaaS)

According to AnyRun Malware Trends Tracker, Formbook is the fourth most popular malware used in 2020. Formbook is an information-stealing malware that harvests credentials, collects screenshots, logs keystrokes, and downloads and executes files based on orders received from its C2 servers. Although Formbook was initially designed to be a simple keylogger, cybercriminals immediately saw its potential as a universal tool. This led the original malware author to halt all product sales before rebranding and relaunching.

It was in February 2020 that Formbook was reborn as XLoader and began popping up in the dark web underground forum. Reverse engineering revealed the code base of Formbook and XLoader are very similar. The author of XLoader admitted on the forum the original author of Formbook contributed a lot of the code for XLoader. Sporting several new capabilities, such as the ability to operate in the macOS, the XLoader malware helps to fool sandboxes and keep real C2 servers hidden. The malware uses 90,000 domains in network communications, but only 1,300 are the real C2 domains (1.5% of the total traffic). The other 88,000 domains are legitimate sites, but the malware sends malicious C2 traffic to those domains as well, creating a dilemma for researchers in determining which are the real C2 servers.

As XLoader popped up in early 2020, it moved to a malware-as-a-service (MaaS) model. Under this model, customers can only buy the malware for a limited time and must use the C2 servers provided by the author. No custom or private control panels are sold, which grants control back to the author to manage how the customers use the malware. Different versions of the malware (Windows vs. macOS) and the length of time in which the customer can use the malware carry different price tags, with the most expensive being the three-month lease of the Windows executable for $129. MaaS has become the optimal approach for both the engineer and the salesperson, as the engineer is able to focus on ensuring a quality product, while sales can focus on managing the day-to-day operations. Though this is more efficient for the malware threat actors, it can also be more efficient for counter cyber operations because cyber teams only need to target known servers for successful operations and can worry less about decentralized architecture.

REvil Linux Variant and IndigoZebra Targets Central Asia

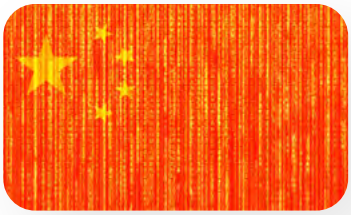
REVIL LINUX VARIANT

The REvil ransomware group has expanded its arsenal to include a Linux variant, which allows the group to target ESXi and NAS (network-attached storage) devices. Similar to the Windows version of the ransomware that has targeted big names such as JBS, Acer, and Travelex, the Linux variant was first observed affecting ESXi and Linux systems in the wild in late May 2021. It is believed that REvil rapidly developed a Linux variant of its ransomware to compete against the Linux version of DarkSide that was released in March 2021. The development of a Linux variant of REvil ransomware poses a great threat and could be devastating to systems that rely on operational technology (OT)—such as critical infrastructure in the energy sector—since many devices on OT networks are Linux-based.

INDIGOZEBRA TARGETS CENTRAL ASIA

An advanced persistent threat (APT) group dubbed IndigoZebra has been identified conducting an ongoing spearphishing campaign against the Afghan government. Previously attributed to China, IndigoZebra has been observed targeting other Central Asian countries, including Kyrgyzstan and Uzbekistan, since at least 2014. In the infection chain used against the Afghan government, the threat actors begin with an email containing a malicious password-protected RAR archive (NSC Press conference.rar), which thwarts some sandbox solutions because it requires user interaction.

The RAR archive drops the extracted file (NSC Press conference.exe), which then drops and executes the BoxCaon backdoor (spools.exe). The BoxCaon backdoor, which is a variant of the xCaon malware family, uses Dropbox as a C2 server, sending and receiving commands contained in a specific folder in an attacker-created Dropbox account. The threat actors' use of Dropbox for C2 communications aids in masking the malicious traffic in the victim's network and appears as benign activity in user environments where Dropbox is used (Dropbox is a default program on some Windows computers). The backdoor uses a hardcoded access token and can download, upload, and execute files. Other malware that the group has used in 2020-2021 (primarily against political entities in Kyrgyzstan and Uzbekistan) are hosted on ASN 20473 (CHOOPA) and Vultr, a subsidiary of CHOOPA that is commonly used for malicious purposes by criminals and Chinese APTs.



U.S. and Allies Condemn China and IcedID

U.S. AND ALLIES CONDEMN CHINA

On July 19th, the U.S. government and its allies—including the European Union, the Five Eyes countries, and NATO—publicly condemned and blamed the People's Republic of China (PRC) for a series of malicious cyber attacks, including the Microsoft Exchange Hacks, global ransomware attacks, and cyber attacks against medical research institutes and universities. In addition, the U.S. Department of Justice released an indictment in May (unsealed July 16th) that charged four Chinese nationals with a campaign to hack into the computer systems of dozens of companies, universities, and governmental entities around the world from 2011 to 2018. The nationals are believed to be members of the group tracked as APT40, which is connected to the PRC Ministry of State Security (MSS) Hainan State Security Department (HSSD). The indictment alleges China has been leading a worldwide hacking and economic espionage campaign, using cyber attacks to steal intellectual property in disregard of bilateral and multilateral agreements. On July 19th, the NSA, FBI, and CISA (Cybersecurity and Infrastructure Security Agency) also released a list of TTPs (tactics, techniques, and procedures) and IoCs related to APT40 observed between 2009 and 2018, along with a series of suggested mitigations.

ICEDID

IcedID started as a banking Trojan used to steal financial information in 2017. As of late 2020, IcedID is a popular modular malware being used as a dropper for other malware. In 2021, it was observed that the REvil and Conti ransomware groups both used IcedID in several attacks to gain an initial foothold in victim environments. For initial access, a malicious Word document is executed, which drops and executes an HTA (HTML Application) file. The malicious HTA file is used to download IcedID in the form of a JPG file (which is actually a Windows DLL file). IcedID then downloads second-stage payloads to get Cobalt Strike onto the network, which is used to pivot to other systems in the victim environment. Anti-virus did slow down the attackers, frustrating them to the point where they left the environment for 11 days before returning with more Cobalt Strike beacons. They used these beacons to pivot throughout the domain utilizing WMI (Windows Management Instrumentation), but the adversaries remained unable or unwilling to accomplish their final objectives and ended up ultimately leaving the environment.

This attack chain is ranked as low-medium sophistication because of the following:

1. The attackers' use of HTTP beacons is not encrypted, making it likely they will be caught by more mature environments.

2. Their use of HTTP beacons without domain fronting indicates only a medium-level of sophistication.

These affiliated threat actors are frequently receiving too much credit for running commodity malware, which is not an advanced TTP because AV blocks most of the activity. However, it is important to note that when AV fails, logging records the activity.

TA456 and BlackMatter

TA456

Proofpoint researchers have identified a years-long social engineering and targeted malware campaign by TA456. TA456 is an Iranian state-aligned threat actor focused on espionage efforts against defense industrial base (DIB) targets, specifically those supporting efforts in the Middle East. Under the persona of "Marcella Flores," TA456 members built an online relationship across corporate and personal communications platforms with an employee of a subsidiary of an aerospace defense contractor. In June 2021, TA456 attempted to capitalize on the ongoing email communications to deliver target malware, sending the victim a malicious email with a personalized document containing macros. The malware—an updated version of Liderc dubbed "LEMPO"—first establishes persistence and then performs reconnaissance. Following reconnaissance, TA456 uses hardcoded credentials via Microsoft CDO (what allows software to send emails) to exfiltrate data over SMTPS on port 465 to an email account controlled by a threat actor.

On July 15th, Facebook announced they had disrupted a network of Facebook and Instagram personas, including Marcella's, demonstrating how TA456 had established an expansive network of online personas to enable cyberespionage operations. With evidence that Marcella began interacting with the target on social media in late 2019, this campaign exemplifies how TA456 was willing to spend years building personal relationships with a target's employee to gain access to a high-security environment within the DIB.

BLACKMATTER

Researchers believe a "new" ransomware group that has recently surfaced, named BlackMatter, is a rebrand of the DarkSide ransomware gang. Responsible for the ransomware attack on Colonial Pipeline, DarkSide was forced to shut down in May after losing access to its infrastructure and having some of its ransom payments seized by law enforcement. The new BlackMatter group, which emerged in late July, is observed to be actively targeting multiple victims, and has already received a $4 million ransom from one victim to delete stolen information and obtain a Windows and Linux ESXi decrypt.

BlackMatter was found by Fabian Wosar (Emsisoft CTO) to be using the same unique encryption routine and custom Salsa20 matrix as DarkSide. Though this is not 100% proof that BlackMatter is a rebrand of DarkSide, several similar characteristics—such as encryption algorithms, code overlaps, and even similar color schemes and language used on their TOR sites—point to this being the case. Nonetheless, BlackMatter has already exhibited itself to be a highly skilled threat actor that can compromise various device architectures, including Linux, Windows, and ESXi servers, and it is a group to keep an eye on as it targets larger and more well-known victims.

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