IronNet™

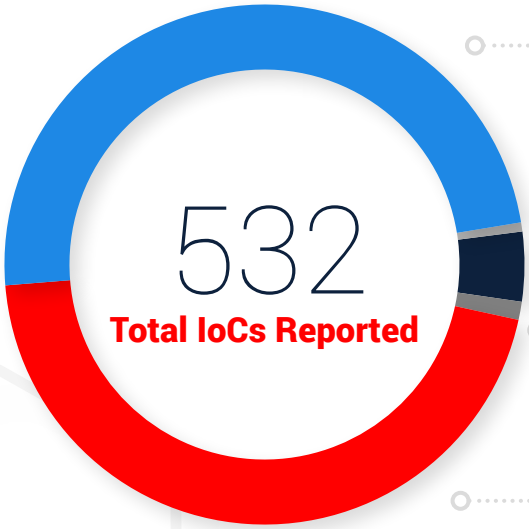
Edition #21: September 2021

# IronNet:
# Threat Intelligence Brief

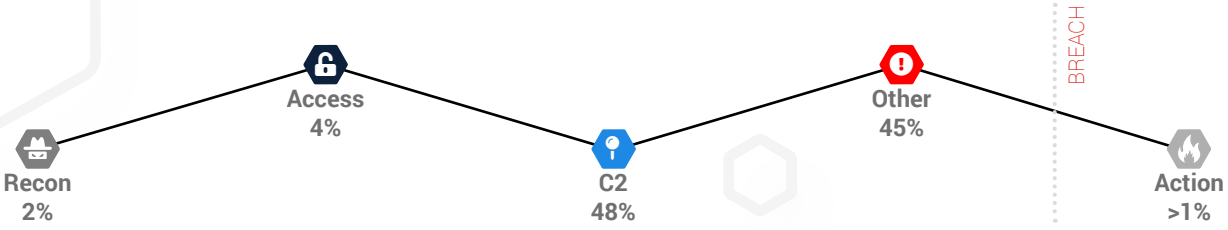
## Top Observed Threats from IronNet Collective Defense Community
## August 1 – August 25, 2021

# 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: **259 IoCs**
- Action **3 IoCs**
- Access **23 IoCs**
- Recon **6 IoCs**
- Other: **241 IoCs**



# Recent Indicators of Compromise

| Domain/IP | Rating | Analyst Insight |
|---|---|---|
| sql1q12u73[.]com | MALICIOUS | This domain is part of a redirect chain involving pucopum[.]info and box20files[.]com. When visited, it serves an encrypted ZIP file after providing the unzip password to the user. The binary file contained adware along with a malicious version of msimg32[.]dll. |
| pipelinecrm[.]email | MALICIOUS | This domain hosts a phishing scam targeting pipeline customer relationship management. |
| fnacgbik9v14[.]com | MALICIOUS | This is a known spyware/malware infection source. Clients are redirected to this domain from infected sites. |
| 2ozglttd7ftas1xm[.]com | SUSPICIOUS | This domain navigates to a mobile-optimized site that appears to be adult-themed Tik Tok videos. Mobile users are redirected to the related domains vqtxxbkqhss7tncw[.]jewelry and rbl4all.caroline26[.]com. |
| ringexpressbeach[.]com | SUSPICIOUS | This is a Terraclicks-related domain hosting ad redirects. We recommend blocking the domain. |
| securesearchnow[.]com | SUSPICIOUS | This IP address is a possible internet scanner rated as Suspicious by OSINT. |
| easforcom[.]biz | SUSPICIOUS | This site redirects users to userscloud[.]com, which presents the user with a potentially unwanted program (PUP) download option and browser notifications. |
| amads[.]uno | SUSPICIOUS | This domain invokes a pop-under redirect to grandprize[.]xyz. The suspicious traffic was a result of landing on a compromised site. If seen in your network, ensure any redirects and amads[.]uno are blocked. |
| lowerbeforwarden[.]ml | SUSPICIOUS | This domain is indicative of a hacked WordPress site injected with adware/malvertising. The domain may lead to unwanted redirects. If seen in your network, investigate any redirects. |
| alcoholicsort[.]com | SUSPICIOUS | This domain is associated with adware/Terraclicks. Ensure connections are blocked. |

# Threat Rules Developed

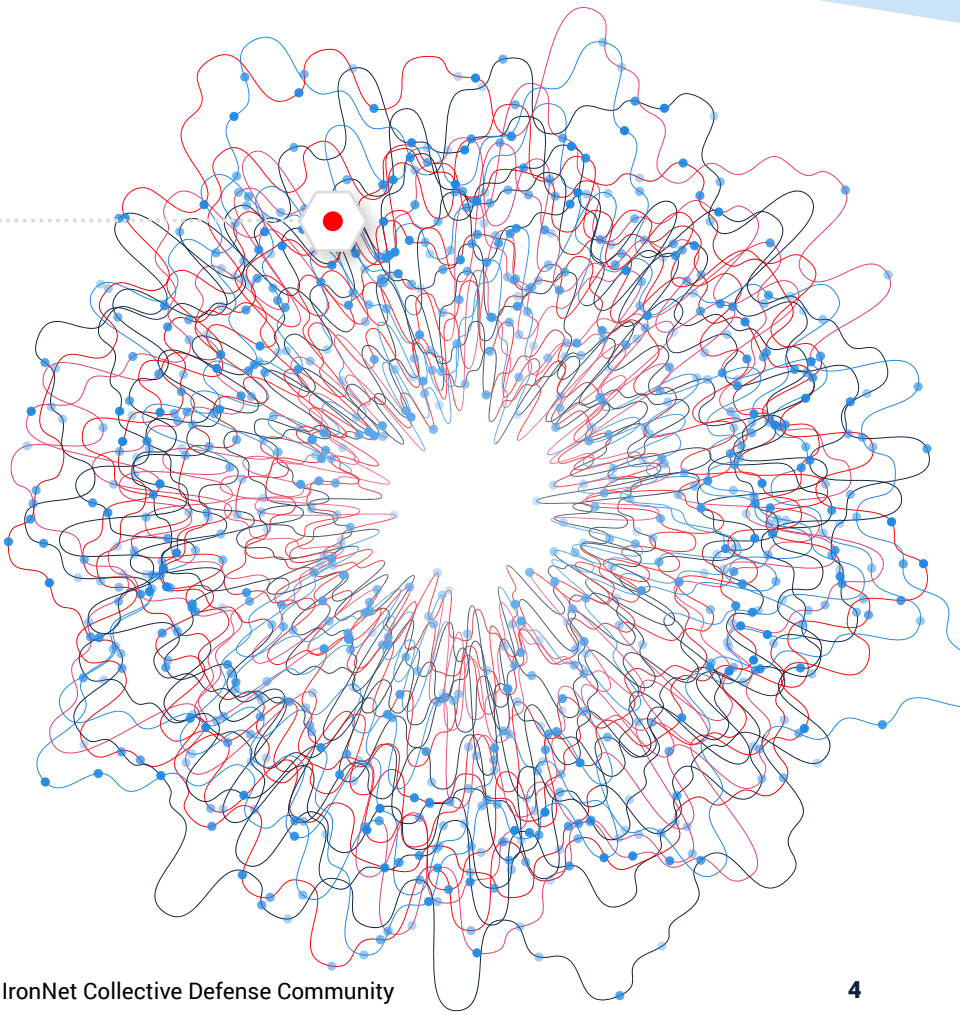
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

4,301

**Threat Intel Rules Developed This Month**

**263,196**

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 AgentTesla, Gafgyt, Sabsik, and Dridex malware
- IoCs surrounding Chinese state-sponsored threat group APT40
- IoCs surrounding ShadowPad malware
- IoCs related to Cobalt Strike beacon payload distribution and Command and Control (C2)
- Malware delivery domains used by TA551/Shathak threat group to deliver Trickbot malware


# 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

**240B**
**Flows Ingested**

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

**581K**
**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.

**2,435**
**High Severity Alerts**

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

**429**
**Correlated Alerts**

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

**69**
**Found between two participants**

**360**
**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.

- New and Suspicious Domains 55.46%
- C2 Rendezvous (DGA) 23.84%
- Credential Phishing 10.54%
- Internal Enumeration 3.28%
- Beaconing 3.60%
- Invalid Certificates 1.48%
- DNS Tunneling 0.71%
- External Scanning 0.64%
- Lateral Movement 0.26%
- Data Exfiltration 0.19%

# Tracking Industry Threats

## ProxyShell and New Typosquatting

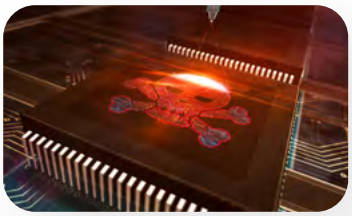
### PROXYSHELL

ProxyShell is the name for three vulnerabilities that are chained together to accomplish unauthenticated remote code execution on Microsoft Exchange servers. Exploited remotely through Microsoft Exchange's Client Access Service (CAS), these vulnerabilities were reportedly patched in April and May of 2021. However, there are still approximately 400,000 unpatched servers vulnerable to exploitation.

As discussed by Orange Tsai at this year's Black Hat Cybersecurity conference, one of the components of the ProxyShell attack chain targets the Autodiscover service of Microsoft Exchange, which was developed to auto-configure the mail client with minimal input from the user. After more details about the vulnerability were released, attackers modified their scans to exploit the Autodiscover/autodiscover.json path to access MAPI, causing the victim's IIS to then write out files and execute commands. Since the patches for the ProxyShell vulnerability have already been released, any subsequent ProxyLogon attacks should not be as successful like the ones that occurred in March. However, as discovered in some system administration blogs, administrators have been hesitant to upgrade due to the update's incompatibility with antivirus (AV) software. For example, the Cumulative Update 21 is noted to add in support for Antimalware Scan Interface (AMSI), which does not work well with AV products like Sophos as it causes CPU usage to max out. Sophos suggests disabling AMSI integration with Exchange Server 2016 and 2019 to work around this issue.

### TYPOSQUATTING CAMPAIGN

IronNet's Cyber Operations Center (CyOC) has been researching a recent typosquatting campaign in which customers were targeted through common services. Also called URL hijacking, typosquatting involves hackers tricking users into visiting malicious websites with domains that are common misspellings of legitimate websites. In the campaign uncovered by IronNet, no malicious traffic has been detected to any of these subdomains. There has been some web traffic to these domains, but this is only due to user misspellings confirmed by the associated customer. The IPs that these domains resolve to are owned by Trellian ASN, which hosts hundreds of other phishing domains, many of which host parking pages as well. IronNet's CyOC is tracking many other potential phishing domains owned by Trellian ASN that have been seen in IronDome during July.



## UNC215 (China)

A cyber-espionage group based out of China called UNC215 has been identified conducting concurrent operations against Israeli government entities, IT providers, and telecommunications companies since January 2019.

For initial access, UNC215 was observed exploiting the Microsoft SharePoint vulnerability to deploy webshells and FOCUSFJORD payloads at select government and academic entities in the Middle East and Central Asia. After establishing an initial foothold, UNC215 used both publicly available and non-public tools to carry out extensive internal network reconnaissance, which included credential harvesting and executing ADFind on the Active Directory. After conducting internal recon, the threat actors moved laterally to deploy their signature FOCUSFJORD payload for the initial stages of an intrusion and later deployed HYPERBRO for additional information collection capabilities, such as screen capture and keylogging.

In 2019, UNC215 operators were able to access their primary target via RDP (Remote Desktop Protocol) through a trusted third-party using stolen credentials. These credentials allowed them access to remotely execute its FOCUSFJORD malware on their target. Upon initial execution, FOCUSFJORD writes its encrypted C2 configuration to registry to set up persistence, which enables the operators to obfuscate the configured C2 servers from automated sandbox runs. UNC215 makes a consistent effort to delete tools and any forensic artifacts from compromised systems and is assisted by a newly identified utility called FJORDOHELPER. FJORDOHELPER updates FOCUSFJORD configs and completely wipes FOCUSFJORD from the system.

As part of OPSEC, UNC215 also uses other victim networks to proxy its C2 instructions to evade detection and blend in with normal network traffic. Additionally, UNC215 actors incorporate false flags. For example, on at least three occasions, the threat actor employed a custom tool leaked from Iranian actors to deceive analysts.

Though UNC215 is evidenced to prioritize evading detection in a network, it has used the same malware and infrastructure against multiple victims and has reused the same SSL certificate [PDF], indicating a lack of concern about the possibility of their attacks being linked to each other.

These UNC215 operations have occurred against the backdrop of China's investment in its Belt and Road Initiative (BRI) and the billions of dollars invested by Chinese companies into Israeli technology startups. China has carried out multiple intrusion campaigns to monitor for possible obstructions to the BRI. It is suspected that UNC215's campaign is part of this and that the group will continue to target governments and organizations involved in these infrastructure projects in Israel and the wider Middle East.

# LockFile Ransomware

A new ransomware family called LockFile has surfaced to target victims in various industries around the globe. First seen on the network of a U.S. financial organization on July 20th, LockFile's latest activity was observed on August 20th. The new ransomware strain has already hit at least 10 corporations. Most of its victims are based in the U.S. and Asia in the sectors of manufacturing, financial services, engineering, legal, business, and tourism.

Two aspects of LockFile's attack chain are garnering attention: ProxyShell and PetitPotam. LockFile exploits ProxyShell vulnerabilities to gain access to Microsoft Exchange email servers, which threat actors use to pivot to companies' internal networks. ProxyShell is the name for three vulnerabilities that are chained together to accomplish unauthenticated remote code execution on Microsoft Exchange servers. LockFile uses the PetitPotam exploit to take over a company's Windows domain controller and deploy file-encrypting payloads to connected workstations. PetitPotam is an NTLM (New Technology LAN Manager) relay attack bug that low-privileged attackers can use to take over a domain controller, which allows them to have control over the entire Windows domain and run any command they want.

LockFile first exploits the ProxyShell vulnerabilities to gain access to Microsoft Exchange servers. Upon exploitation, the attacker executes a PowerShell command that downloads a file from a remote location. It is unknown exactly what is downloaded by the PowerShell command; however, it is known that the attackers maintain access in victim networks for at least several days before beginning the ransomware attack. Around 20 to 30 minutes before deploying the ransomware, the threat actors install a set of tools onto the compromised Exchange Server. These tools include the exploitation for PetitPotam contained in a folder named "efspotato.exe" and two additional files designed to download shellcode to help with the exploitation. Once activated, the PetitPotam exploitation file allows the threat actors to take over the domain controller. The final step is to copy the LockFile ransomware payload, along with a batch file and supporting executables, onto the local domain controller and push it across the network as client hosts authenticate to the server.

LockFile appears to be the newest threat in the very crowded ransomware landscape. The investigation into this group and whether it may have links to any known or retired ransomware threats continues. However, some connections to existing groups have been identified. The ransom note used by the LockFile gang is very similar to the one used by the LockBit ransomware [PDF] operators. Additionally, the group references the Conti gang in the contact email address left for 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, 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