IronNet™

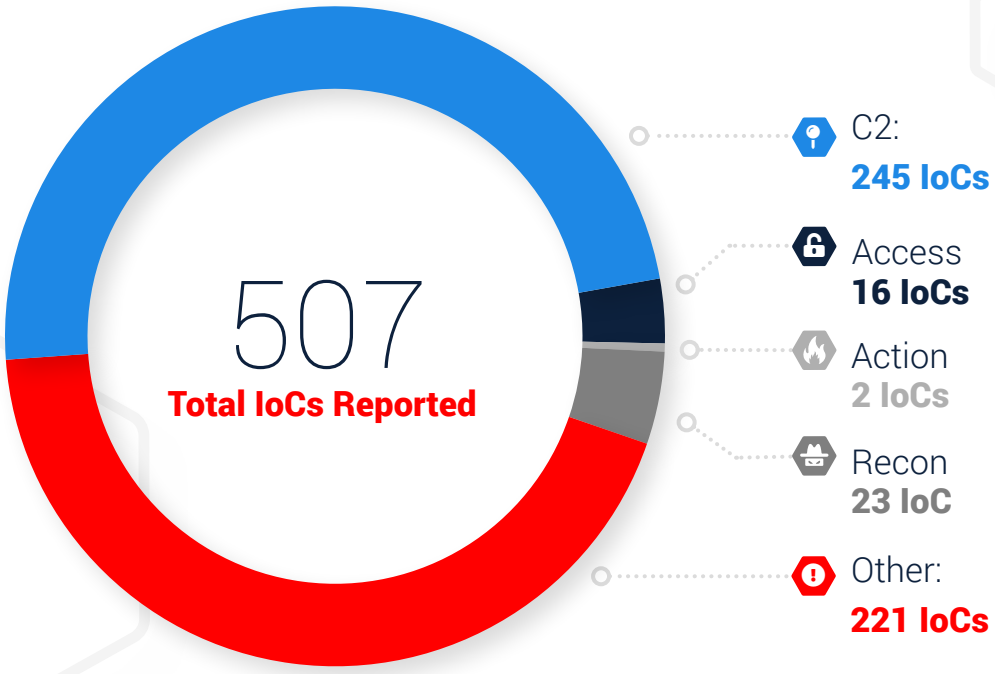
Edition #19: July 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
June 1 – June 30, 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
wcomhost[.]com	MALICIOUS	000knx1.wcomhost[.]com appears to host an insurance site; however, it is actually a copy of the legitimate insurance site www.aquidneckislandinsurance[.]com. In the past, this domain has hosted fake PayPal login pages to lure clients into inserting personally identifiable information (PII) and credentials into form fields of the page. Ensure no PII was entered into form fields and block the domain.
firstrepbn[.]us	MALICIOUS	This is a phishing site mimicking the First Republic Bank and attempting to harvest credentials and PII.
rsafrwdr[.]com	SUSPICIOUS	This is a pop-up adware redirector that may redirect the user to unwanted software. If seen in your network, block the domain.
witmorningmuscles[.]com	SUSPICIOUS	This is a TerraClicks-related domain for streaming content. If seen in your network, block the domain.
goo[.]io	SUSPICIOUS	This is a URL shortening service. If seen in your network, verify the URL destination, as many goo[.]io domains lead to unwanted sites.
carrelloamico[.]it	SUSPICIOUS	This domain is currently hosting suspicious links to APK (Android application package) files and ads. If seen in your network, ensure no downloads occurred around the time of the traffic.
teamviewer[.]com	SUSPICIOUS	Any attempts to download TeamViewer in an enterprise environment should be investigated. TeamViewer allows for remote connections to the system, bypassing the organization's firewall. If the user-agent \"Mozilla/4.0 (compatible; MSIE 6.0; DynGate)\" is seen, this indicates the application is running on the endpoint.
closemike[.]com	SUSPICIOUS	This URL is currently serving LNKR ad injections to website visitors via JavaScript, tracking GIFs, and JSONP. We recommend blocking the website.
crimeflare[.]net	SUSPICIOUS	This is a successful .zip file download (HTTP 200) from crimeflare[.]net. CrimeFlare is part of the CloudFail database, a tactical reconnaissance tool which gathers information about a target protected by CloudFlare to discover the server's location.
cpmstatsart[.]com	SUSPICIOUS	This is a potential scam domain. If seen in your network, block the domain and look for unwanted applications on the host.

Threat Rules Developed

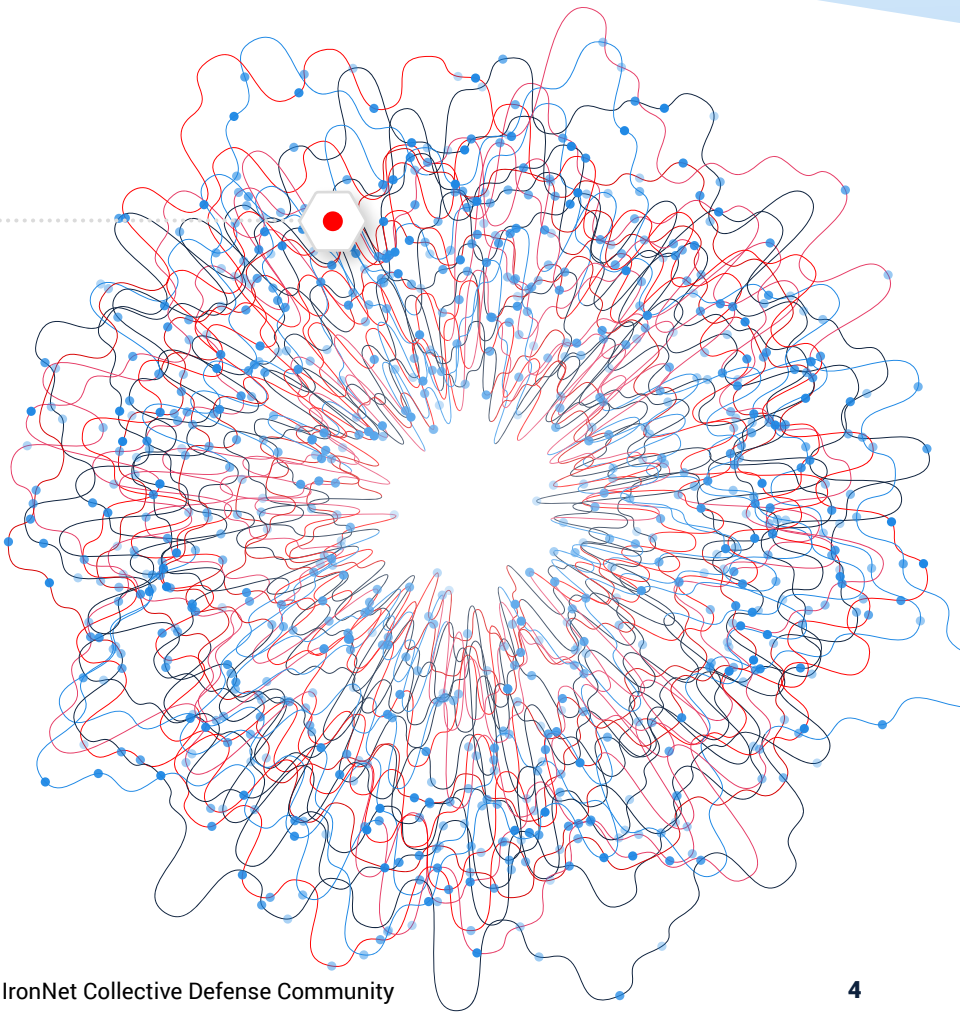
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

30,182

Threat Intel Rules Developed This Month

250,986

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 for the Hupigon backdoor
- C2 domains for Ramnit malware
- IoCs surrounding the NOBELIUM phishing campaign
- C2 domains for the Zeus Trojan
- IoCs related to Cobalt Strike beacon payload distribution and C2 activity
- C2 domains for Bebloh and Cerber malware
- IoCs surrounding the RedFoxtrot threat group, which has been tied to the Chinese military
- C2 domains for Banbra malware
- Malware delivery domains for the Gafgyt, AgentTesla, and Morila malwares
- C2 domains for FormBook malware

This Month in the IronDome

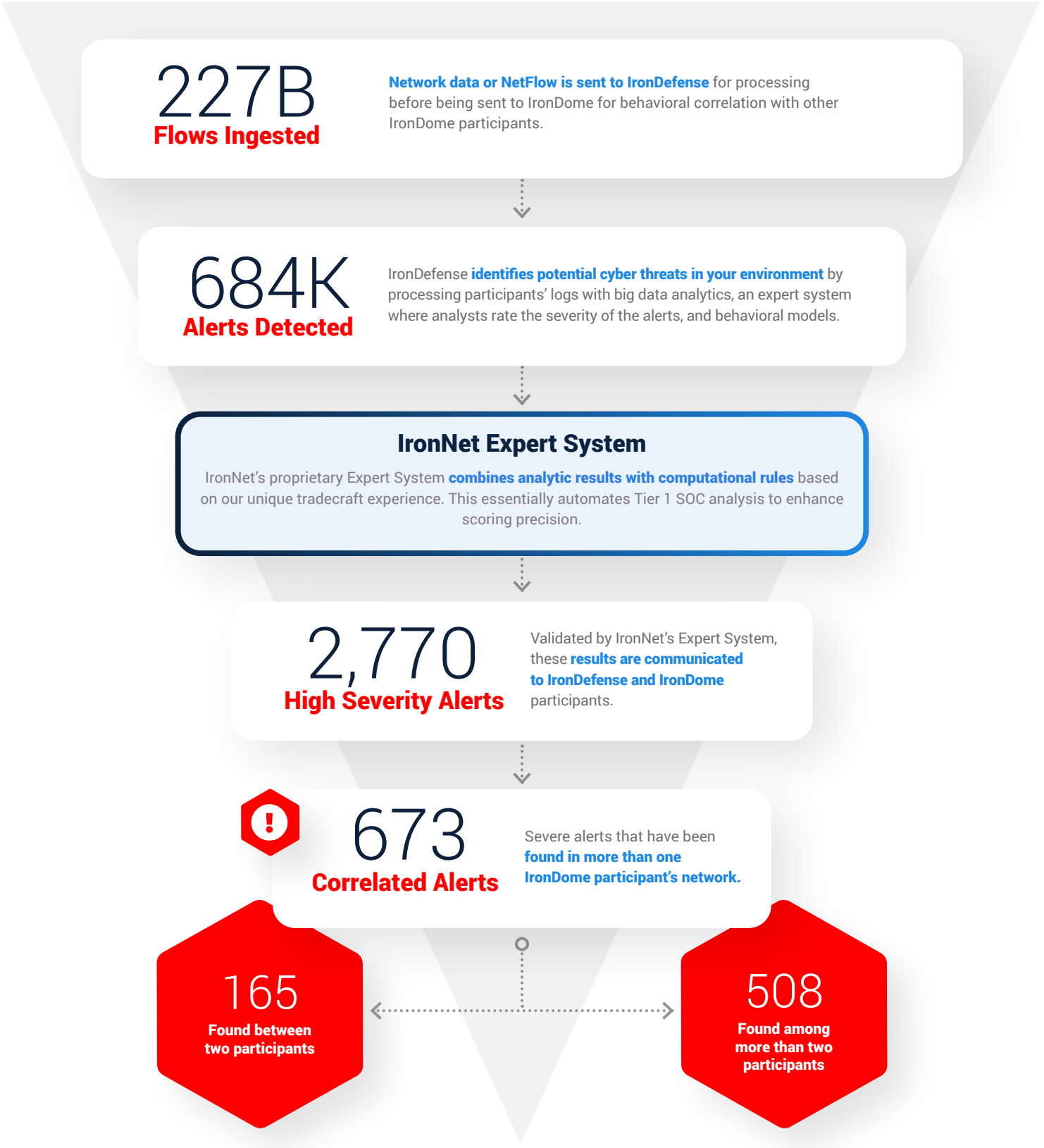
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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.

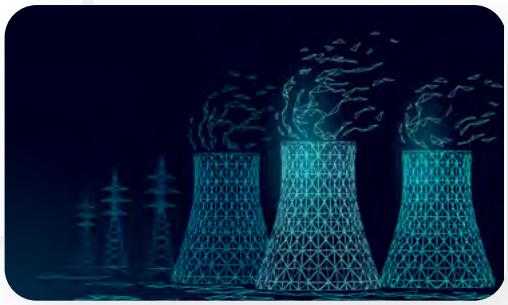
This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses.

On the following page is a snapshot of this month’s alerts.

Monthly Alert Snapshot



Tracking Industry Threats



REvil Continues to Create Headaches

The REvil ransomware gang was recently revealed to have targeted Sol Oriens, a U.S. federal nuclear contractor that consults for the U.S. Department of Energy's National Nuclear Safety Administration. Sol Oriens became aware of the attack in May 2021, but states no internal documents or sensitive information regarding U.S. nuclear programs was stolen. This latest ransomware attack by REvil adds to the group's recent attacks on meat producer JBS, Japanese technology corporation Fujifilm, foodservice supplier Edward Dawn, and Apple supplier Quanta Computer.

REvil has been increasingly observed using QBot malware as an initial access vector. Although it originated as a banking Trojan, QBot has evolved into a sophisticated botnet that can compromise sensitive data, typically exploiting hijacked email threads to instigate the spread of infection. REvil is not the only ransomware group to leverage QBot; ProLock and Egregor have also been known to partner with the QBot group.

Russia has garnered widespread condemnation for supposedly acting as a safe haven for infamous ransomware groups, including REvil and DarkSide. Russia is believed to be a breeding ground for young Russian cybercriminals, as it provides the education, internet access, and free reign that make cybercrime a low-cost, high-reward way to make money. Russia's harboring and fostering of criminal hackers was a key topic of discussion in the recent summit between Russian President Vladimir Putin and U.S. President Joe Biden. The publicity and government attention that recent ransomware attacks have attracted have led to a series of second- and third-order effects. Host countries are adding pressure and cracking down on cybercriminals, and the increased constraints and scrutiny from law enforcement may have influenced the latest shutdown of ransomware groups, such as Avaddon, who recently released the decryption keys for its victims and shut down its operations.

APT 28 - SkinnyBoy (SB)

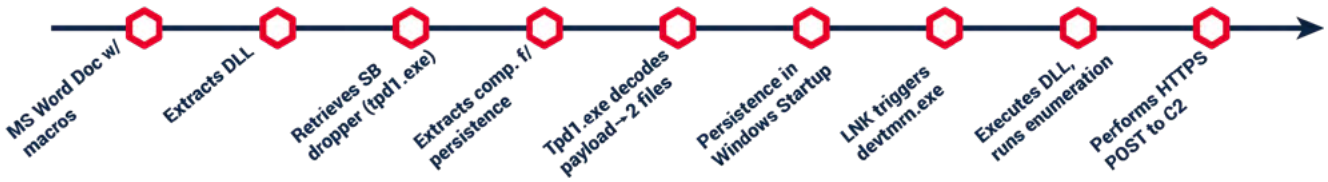
A new Cyber Threat Intelligence Research and Adversary Hunting Team, Cluster25, has discovered a new backdoor being used in a series of attacks conducted by APT 28 (also known as Fancy Bear, Strontium). APT 28 has been active since the mid-2000s and is believed to be a military unit of Russia's General Staff Main Intelligence Directorate (GRU). Tracked by Cluster25 as SkinnyBoy, this previously unreported malware is fully operational but lacks the sophistication normally expected of a nation-state tool, likely in an effort to evade attribution. This campaign reportedly began in March 2021, targeting military and government institutions mainly in the European Union (though it is possible U.S. organizations were affected as well). The infection chain used by APT 28 in this campaign is described below.

STAGE 1: The threat actors use a spearphishing email to deliver a Microsoft Word document that, when opened, triggers a macro function to extract the DLL (Dynamic Link Library) to download the SkinnyBoy dropper (tdp1.exe).

STAGE 2: Once the SkinnyBoy dropper is downloaded to the target's file system, it extracts components to establish persistence of the executable. The extracted payload is Base64 encoded and appended as an overlay. From there, the malicious process decodes the payload and writes two different files (devtmrn.exe and TermSrvClt.dll) on the filesystem, deleting itself afterward. The malware never executes the extracted files to avoid detection; instead, it creates persistence in Windows Startup (LNK file), which allows for delayed execution of the next stages.

STAGE 3: Upon reboot, the LNK file in the Startup folder triggers the execution of devtmrn.exe, which invokes the DLL executable, TermSrvClt.dll, the main implant of the infection chain.

STAGE 4: TermSrvClt.dll runs enumeration commands and exfiltrates information about the infected system, including a list of filenames from program files of interest. It then performs an HTTPS POST request to send the gathered information to the C2 (updaterweb[.]com). The POST body requests are XORED using two different keys in order to avoid static detection. After completing this, it contacts the C2 again to retrieve the next payload, to which the C2 replies with the next DLL to be executed, representing the final stage of the infection that most likely manifests backdoor behaviors.



LockBit Ransomware

Swiss cyber threat intelligence company PRODAFT recently released an in-depth analysis on LockBit Ransomware-as-a-Service (RaaS). Formerly known as ABCD ransomware, LockBit is relatively new and has become quite popular in the past few months, with use increasing dramatically in the last quarter of 2020 and peaking in early May 2021. As a RaaS platform, LockBit leases out its ransomware to affiliates who use it to carry out attacks. It has become one of the most popular ransomware variants, ranking third behind REvil and Conti, with 7.5% of the market share. Almost all of LockBit's victims are enterprise corporations, and actors using LockBit charge an average ransom of $85K. PRODAFT was able to gain access to some parts of the LockBit RaaS infrastructure, which consists of a management panel primarily used for managing victims and affiliate accounts, generating new ransomware builds, and serving the decryptor software if the demanded ransom is paid.

BREAKDOWN OF THE KILL CHAIN

Targets are typically selected through mass vulnerability scanning, phishing, credential stuffing, buying RDP accesses from underground shops, and Fortinet VPN exploits. After gaining initial access, the threat actors deploy LockBit ransomware. Once executed, LockBit will immediately begin trying to enumerate all accessible directories and network shares inside the victim system. When completed, the payload encrypts each file with a different random AES key. It also begins exfiltrating critical data, which the attackers upload to a free file upload service to use for extortion while negotiating with the victims. After files are encrypted and backups are deleted, the system wallpaper is replaced with an image stating all files are encrypted and to visit a specific .txt file that provides instructions on steps to restore the files.

The .txt file will lead the victims to a contact page that contains a "CHAT WITH SUPPORT" section, which they are expected to use to get in contact with the LockBit attacker regarding the purchase of the decryptor. It also contains a "TRIAL DECRYPT" section that allows the victims to "try out" the decryptor on a single encrypted file. This is necessary to receive the full decryptor, in addition to paying the agreed-upon ransom. Since ransomware groups often fail to hand over the decryptor once victims pay, this feature adds an additional level of protection and credibility, reassuring victims that LockBit attackers can successfully decrypt their files in an automated fashion. Given that LockBit was most active in May 2021, we expect to see activity increase from this ransomware family in the future and progressively see this name popping up in the news in coming months.

Kimsuky Targets South Korea

Kimsuky is a prolific North Korean advanced persistent threat whose primary target is the South Korean government. Active since 2012, Kimsuky's main goal is stealing high-value intelligence, carrying out attacks on a wide range of high-profile victims. Recently, Kimsuky was found to have breached the internal network of the South Korean Atomic Energy Research Institute (KAERI) in May 2021 by exploiting a VPN vulnerability. In late 2020, the group was identified as targeting at least six COVID-19 pharmaceutical companies in the U.S., the U.K., and South Korea, aligning with North Korea's concerns regarding the pandemic and interest in stealing intellectual property to manufacture a COVID vaccine for North Korea. Cybersecurity researchers also found Kimsuky to be responsible for a spearphishing campaign targeting high-profile South Korean officials in numerous government organizations using a backdoor dubbed AppleSeed. The Weibu Intelligence Agency published a report about its observations regarding Kimsuky through its threat-hunting system, finding that the Lazarus APT group is carrying out similar attacks against military targets, leading to speculation that the two groups are unitedly planning for targeted attacks.

Delivering documents in HWP format (Hangul Word Processor, a popular South Korean word processing application), Kimsuky uses topics related to "Korea-U.S. summit," Korean Ministry of Defense, and Korea Internet Security Agency (KISA) as lures to conduct targeted attacks. Disguising the Trojan in the HWP lure documents delivered through spearphishing emails, the threat actors use the Windows utility mshta.exe to execute malicious .hta files, which allow the adversary to proxy the execution of malicious code through a trusted utility (aka., living off the land). After copying malicious files to the TEMP directory and executing it, the threat actors maintain persistence via the registry under the name "WDFSync." The Remote Access Trojan (RAT) module then checks for Windows user account control (UAC). If the user is not in administrator mode, PowerShell will be run to escalate privileges. The group has upgraded its RAT module from its older version, and the module can now support multiple remote control functions, including remote shell, file upload/download/execution, keyboard logging, screen monitoring, and disk/USB monitoring. This indicates that Kimsuky is constantly enriching its spy functions and RAT capabilities.

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