IronNet™

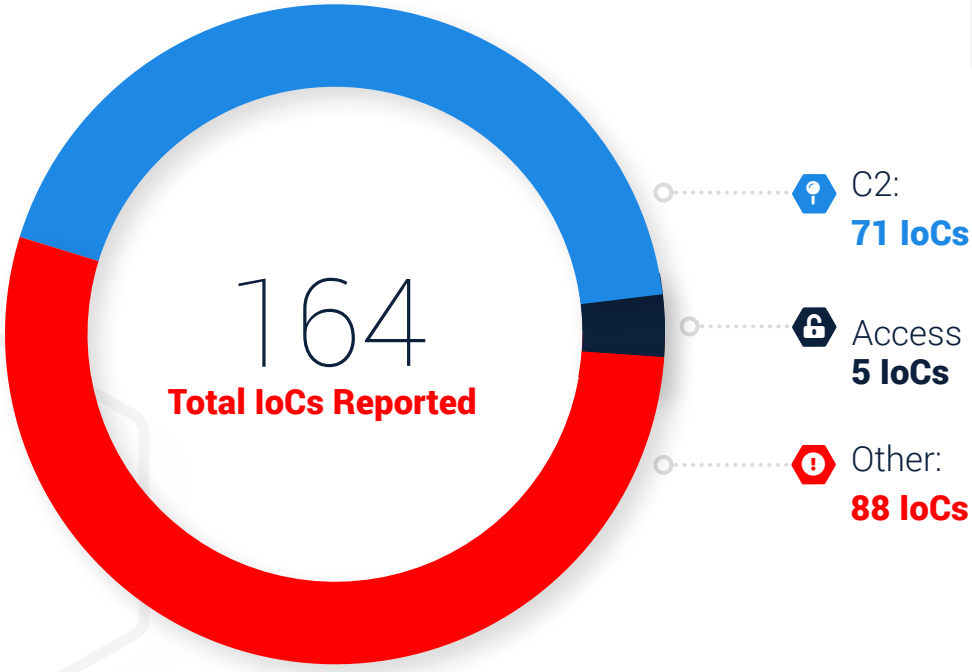
Edition #18: June 2021

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
May 1 – May 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
googlemanagerapi[.]com	MALICIOUS	This domain is involved with MageCart hacking of payment card information. If seen in your network, verify any traffic to checkout pages for possible compromised payment information. Other IoCs related to MageCart are tag-manager[.]net and tags-manager[.]com.
utmostsecond[.]com	SUSPICIOUS	This is a TerraClicks domain associated with adware that could lead to unwanted connections, downloads, and pop-ups. We recommend blocking the domain.
agagaure[.]com	SUSPICIOUS	This is a script used on hacked WordPress sites to load ads.
applewatchstoreusa[.]com	SUSPICIOUS	This is a fake online store claiming to sell Apple Watches. Interacting with the site could lead to compromised payment credentials.
customer-help[.]us	SUSPICIOUS	This is a fake tech support website masquerading as McAfee, Epson, Webroot, and HP support, among others. If this domain is seen in your network, ensure users do not enter data into any subdomain.
hotmail-account[.]email	SUSPICIOUS	This domain appears to be a how-to guide for logging into a Hotmail account. However, the site prompts the user to download a browser plug-in that is likely Suspicious or Malicious.
googie-anaiytlcs[.]com	SUSPICIOUS	The user arrived at this domain via POST from a compromised podcast website. The redirect may have ties to the MageCart credit card stealing campaign.
security-hsb-cancelpayees[.]com	SUSPICIOUS	This is a phishing page targeting HSBC Bank. This is a near-perfect clone of the bank's U.K. page looking to harvest customer credentials. If seen in your network, verify all GET and POST requests and ensure no information was submitted. The site has since been taken down.
mindactual[.]com	SUSPICIOUS	This domain appears to be related to TerraClicks because streaming content was found in the traffic. If seen in your network, block the domain.
betterprovokesap[.]com	SUSPICIOUS	This domain may be related to TerraClicks. If seen in your network, block the domain.

Threat Rules Developed

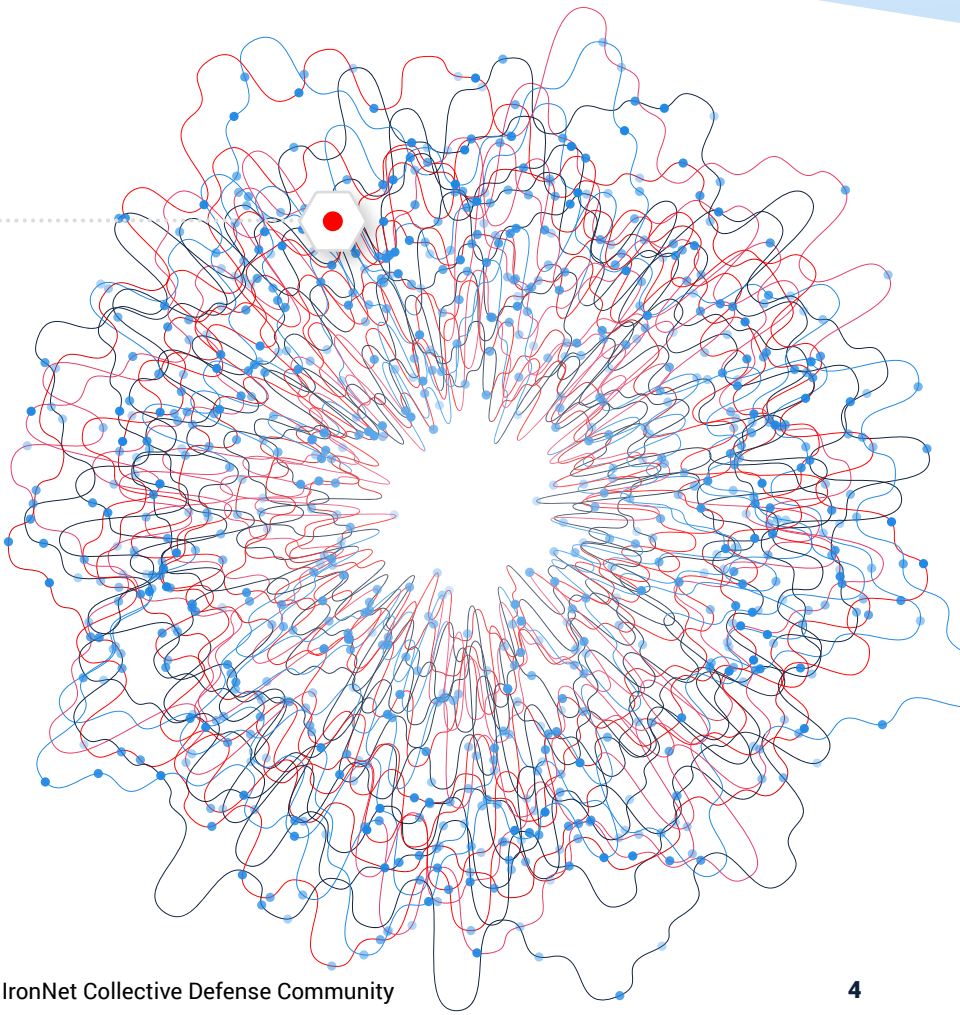
Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants.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

12,746

Threat Intel Rules Developed This Month

220,804

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 Win32.Esfury.T malware
- C2 domains for the Cerber Ransomware-as-a-Service (RaaS) malware
- IoCs surrounding the UNC2529 phishing campaign
- Creation of TIRs for the IoCs surrounding the Colonial Pipeline ransomware attack
- C2 domains for DarkComet malware
- Malware delivery domains for Gafgyt, AgentTesla, Heuristic, BazarLoader, and WifiGrab
- C2 domains for Ramnit malware
- C2 domains for FTCode malware
- C2 domains for the FormBook Malware-as-a-Service program
- C2 domains for Win32.Scarsi malware
- IoCs related to Cobalt Strike beacon payload distribution and C2

This Month in the IronDome

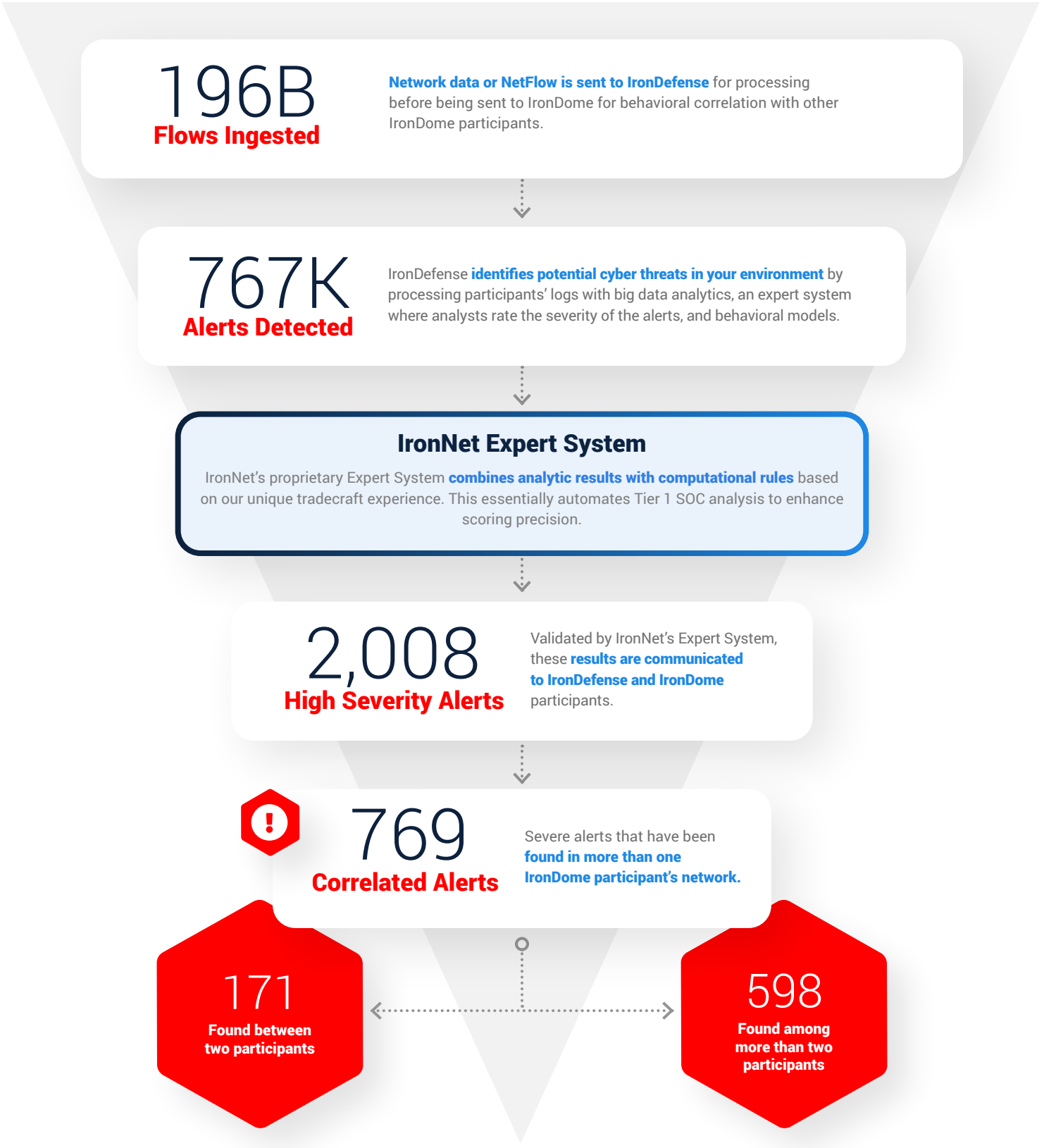
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- 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**

Colonial Pipeline Attack

On May 7th, Colonial Pipeline learned it was the victim of a ransomware attack that infected its corporate IT network. Colonial Pipeline is a major gasoline distributor that supplies 45% of the U.S. East Coast's fuel through its 5,500 miles of pipeline. According to *Bloomberg*, the attackers stole approximately 100GB of data from Colonial Pipeline on Thursday, May 6th before locking some of the company's computers and servers and demanding a ransom. The attackers reportedly threatened to leak the stolen data to the internet and hold the encrypted information hostage inside the network unless the company paid a ransom. At this time, it does not appear that the operational network that controls the company's pipelines and distributes fuel was infected, but Colonial temporarily shut down the pipelines as a precautionary measure to prevent the infection from spreading. Sources have attributed the attack to DarkSide, a "professional organized hacking organization" composed of veteran cybercriminals who are focused on squeezing out as much money as they can from their targets. Colonial has hired FireEye to manage the incident response investigation, and the company is working together with law enforcement and other federal agencies to investigate and deal with the fallout of the attack. IronNet is monitoring this incident as further details of the compromise and its impact continue to emerge.

GCHQ and NSA Joint Advisory

On May 7th, the Government Communications Headquarters (GCHQ) and the NSA released a joint advisory on the tactics, techniques, and procedures (TTP) of SVR, Russia's civilian foreign intelligence service. The U.S. and U.K. governments recently attributed a series of cyber attacks, including the SolarWinds compromise and the targeting of COVID-19 vaccine developers, to SVR (also known as APT29, Cozy Bear, and the Dukes). According to the advisory, SVR often uses publicly available exploits, including vulnerabilities in Pulse Secure VPN, Citrix, VMware, and most recently Microsoft Exchange zero-days, as initial intrusion vectors. SVR is also known to target software providers to gain initial access to a large number of organizations, but typically selects a much smaller number of targets, often in line with intelligence priorities, for follow-on compromise. This was seen in the supply chain attacks on SolarWinds and Mimecast acknowledged earlier this year.

SVR's post-compromise activity typically includes the use of open-source Red Team tools and custom malware to maintain persistent access or conduct further operations. In the SolarWinds attack, SVR's post-compromise activity included the use of the C2 framework Cobalt Strike, as well as the deployment of custom malware, such as GoldFinder, GoldMax, and Sibot. In attacks targeting COVID-19 vaccine developers, the U.K. observed SVR actors deploying custom malware dubbed WellMess and WellMail and utilizing another open-source Red Team C2 framework known as Silver to maintain access to victims after the malware was discovered.

SVR actors are also known to target administrator mailboxes to gain further network access, searching for credentials in company mailboxes for persistence and/or lateral movement. In one incident, SVR actors were able to gain access to the Mimecast Azure app and abuse its permissions with Microsoft Exchange (O365) to extract emails from any mailbox used by the victim organization. As a result, the actors did not need any further privilege escalation or lateral movement to access emails of interest.

Ireland HSE and Conti Ransomware

On the morning of May 14th, Ireland's publicly funded healthcare system Health Service Executive (HSE) was notified of a Conti ransomware attack on its network. As a precaution, HSE shut down all of its IT systems to assess the situation and further protect its infrastructure. This IT outage has widely disrupted the country's healthcare, limiting access to medical records and diagnostics, causing transcription errors, and leading to slow response times on healthcare visits. The Conti ransomware group claims to have been in the HSE network for at least two weeks before encrypting files and SQL servers and stealing 700GB of unencrypted files. The group demanded a ransom of almost €20 million ($24,282,400) to provide a decryptor and delete the stolen data, but HSE and the Prime Minister of Ireland have stated they will not be paying any ransom. at the time of reporting, only emergency services are up, and HSE IT is working to map out what sections can be brought back online safely.

Conti ransomware operations are reportedly conducted by a Russia-based cybercriminal group known as Wizard Spider. The group often uses phishing attacks to deliver a ZIP file loaded with a malicious JavaScript file as the initial intrusion vector. Wizard Spider then installs the TrickBot and BazarLoader Trojans to gain remote access to infected machines. Leveraging this remote access, the attackers move laterally through the network using SMB to transfer and execute a Cobalt Strike beacon while harvesting unencrypted data and stealing credentials. Once the threat actors have stolen everything of interest and accessed Windows domain credentials, they deploy the ransomware on the network to encrypt all devices. Wizard Spider is known for its double extortion tactics, in which it encrypts victims' servers and leverages stolen data to force the victim into paying a ransom by threatening to release sensitive information online if they do not pay.

Nobelium Strikes Again

On May 27th, Microsoft announced that Nobelium, the threat actor behind the SolarWinds attacks, hacked into the Constant Contact account of the United States Agency for International Development (USAID). Impersonating USAID, the Russian threat actors used the legitimate mass-mailing service to send out phishing emails containing malicious URLs to approximately 3,000 individual email accounts across over 150 organizations, including government entities, human rights organizations, and international development organizations. Nobelium employed a unique infection chain, utilizing four tools to gain a foothold in various entities' networks. These tools—EnvyScout, BoomBox, NativeZone, and VaporRage—have been observed in the wild as early as February 2021 and are designed for flexibility, allowing Nobelium to adapt to operational challenges over time.

EnvyScout (NV.html) is a malicious HTML/JS attachment that is deployed in the spearphishing emails to steal Windows New Technology LAN Manager (NTLM) credentials and drop a malicious ISO file. When the HTML file is opened, it will attempt to load an image using the file:// protocol handler. It is likely that the adversary is running a credential capturing service and that the remote server will attempt to capture sensitive NLTM information sent by the infected host. The adversary can then brute force them for future campaign use. The NV.html attachment is also used to turn an embedded text blob into a malicious ISO that is saved to the local file system. When opened, the ISO image executes the hidden BOOM.exe that is part of the malware family BoomBox.

The purpose of BoomBox (BOOM.exe) is to download two encrypted malware files from DropBox to the victim's device. After downloading and decrypting the files, it will save them as DLLs and execute them using rundll32.exe. In its final stage, the BoomBox malware performs reconnaissance by conducting an LDAP query to gather data about the Windows domain, encrypt the collected information, and send it back to a remote server that is controlled by Nobelium.

BoomBox drops and configures the NativeZone malware (NativeCacheSvc.dll) to start automatically when a user logs into Windows. When NativeZone is started via rundll32.exe, it launches the CertPKIProvider.dll malware known as VaporRage. When VaporRage is launched, it connects back to and registers itself with the remote C2 server, from which it will then call back to the remote site for shellcodes to download to deploy Cobalt Strike beacons.

Codecov, DarkSide, and Conti Updates

CODECOV

A software supply chain attack targeting the customers of software auditing company Codecov was discovered in April. Codecov's software, which helps test code for vulnerabilities, is used by over 29,000 customers, and more information is surfacing about which customers were affected by the attack. Multiple companies have announced that their private repositories were impacted by the Codecov attack, including (but not limited to) cloud communications platform Twilio, workflow management platform Monday.com, U.S. cybersecurity firm Rapid7, and software manufacturer HashiCorp.

The latest company to disclose a major breach due to exposure from the Codecov attack is Mercari, a Japanese publicly traded e-commerce platform. A week after Codecov's initial disclosure of the breach, GitHub notified Mercari of suspicious activity on the company's repositories related to the incident. After investigating, Mercari discovered that some customer information and source code stored in its GitHub repos were accessed by external actors, leading to the compromise of tens of thousands of customer records, including personal financial information. In addition to conducting an intensive investigation and purging its GitHub repositories from using Codecov anywhere, Mercari has notified customers whose information might have been compromised and alerted relevant authorities of the breach.

DARKSIDE

DarkSide, the same ransomware gang that staged an attack on the Colonial Pipeline, was confirmed to have also targeted the North American division of a world-leading chemical distribution company at the beginning of May. In the attack, DarkSide encrypted devices on the Brenntag network and stole 150GB of unencrypted files, demanding $7.5 million in bitcoin as ransom. Brenntag was able to negotiate with DarkSide to bring the ransom demand down to $4.4 million, which the company paid to receive a decryptor for the encrypted files and prevent the criminal group from leaking the stolen data. DarkSide is a Ransomware-as-a-Service (RaaS) operation, in which it shares the ransom profit with external affiliates who deploy the ransomware in target environments. As part of this arrangement, DarkSide earns around 30% of the ransomware payment while the rest goes to the affiliate who carried out the attack. The DarkSide affiliate behind this attack has stated that they gained access to the network after buying stolen credentials, illustrating the importance of enforcing MFA (multi-factor authentication) for all logins and placing all remote desktop servers behind a VPN.

CONTI TTP UPDATE (FBI)

The FBI released a Flash Report on May 20th regarding Conti ransomware attacks and associated tactics, techniques, and procedures (TTP). The FBI identified Conti as having targeted at least 16 U.S. healthcare and first responder networks, which are among the over 400 organizations around the world that have been victimized by Conti. Conti often gains initial access through malicious email links/attachments or stolen RDP (Remote Desktop Protocol) credentials, staying inside victim networks on average between four days to three weeks before deploying the ransomware payload. Conti actors are known to use remote access tools, which beacon to VPS (virtual private server) infrastructure over ports 80, 443, 8080, and 8443. They also often use port 53 for persistence. Conti's large HTTPS transfers go to MegaNZ and pCloud servers, which are cloud-based data storage providers. Other Conti activity indicators include installing Sysinternals, disabling endpoint detection, and constant HTTP and DNS beacons. The FBI report emphasizes the importance of reporting ransomware incidents to the FBI's 24/7 Cyber Watch or local field offices and lists a number of recommended mitigations to protect against Conti ransomware attacks.

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