IronNet

Quarterly Threat Intelligence Report

Q4

October - December

IRONNET'S QUARTERLY

Threat Intelligence Report

Insights into Q4 cyber threat trends drawn from IronNet Collective Defense platform detections and intelligence assessments by IronNet analysts from October 1, 2022 to December 31, 2022.

IronNet

EXECUTIVE SUMMARY

The IronNet Threat Research team is proud to present its Quarterly Threat Intelligence Report for the fourth quarter of 2022.

IronNet's Q4 2022 report includes a comprehensive assessment of the cyber threat landscape from October 1, 2022 to December 31, 2022, drawn from telemetry provided by IronNet's network detection and response (NDR) platform **IronDefense** and automated Collective Defense platform **IronDome**. We combine the telemetry provided by our detections and behavioral correlations with unique insights gleaned from our proactive threat intelligence feed **IronRadar**, as well as with intelligence from our partners, to help us in our investigations.

KEY FINDINGS

During that time, IronNet Threat Research observed:

- An increase in Sliver C2 servers, indicating the Sliver C2 framework may be growing in popularity amongst threat actors as a top alternative for Cobalt Strike.
- Commodity tools such as Racoon Stealer, IcedID, and Aurora Stealer remain popular among threat actors, which we often observe used in combination with vulnerability scanning tools like reNgine.
- Threat actors are increasingly devising ways to bypass traditional C2 detection mechanisms and make their infrastructure less detectable through tactics such as domain aging and domain recycling.

IronRadar

ADVERSARY INFRASTRUCTURE TRACKING

IronNet tracks the creation of new malicious infrastructure for numerous post-exploitation toolkits, vulnerability scanners, and remote access trojans (RATs) through a unique fingerprinting process developed by our analysts to track observable artifacts, such as server certificates, HTTP listeners, and management services, prior to the use of a command-and-control (C2) server in a cyber attack.

Between October and December, IronNet identified nearly 10,000 malicious indicators across more than 25 adversarial tools. In Q4 alone, IronRadar added detection capabilities for more than 15 additional tools, which expanded our detections beyond post-exploitation frameworks to include scanning engines, phishing frameworks, and popularly used loader malware. Due to the wide array of updates and added detection capabilities integrated into IronRadar this quarter, observed Q4 trends showed a very different distribution compared to last quarter.

In Q4, we observed an increase in Sliver C2 detections, which may indicate the Sliver C2 framework is gaining popularity as a top alternative to Cobalt Strike. Sliver is a free, open-source C2 framework that's updated almost daily with new capabilities, thus negating the need for a license or cracked version (like is the case with Cobalt Strike and Brute Ratel) and offering many other benefits to threat actors. Outside C2 frameworks, commodity tools like Racoon Stealer, IcedID, and Aurora Stealer remain popular and are often seen used in coordination with vulnerability scanning tools like reNgine. Also in Q4, it became apparent that threat actors are progressively devising ways to bypass traditional C2 detection mechanisms through tactics such as domain aging and domain recycling.

IronRadar℠

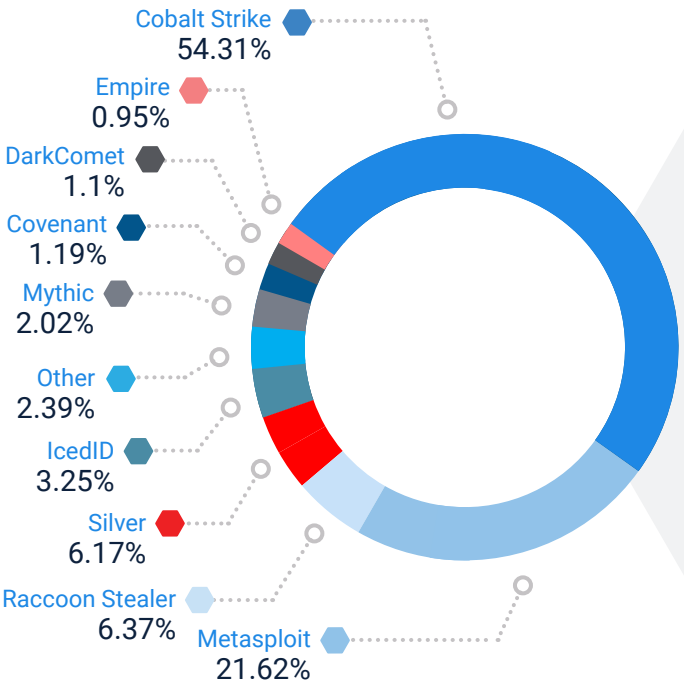
An automated threat intelligence feed for proactive threat intelligence on command-and control (C2) servers and adversary infrastructure. Delivered via a robust API, IronRadar can be consumed by a firewall, a SIEM, a threat intel platform, or any other threat hunting tools.

Learn More

TOP 5 MOST DETECTED TOOLS

Number of Malicious Indicators Detected

C2 Servers:
By the Numbers



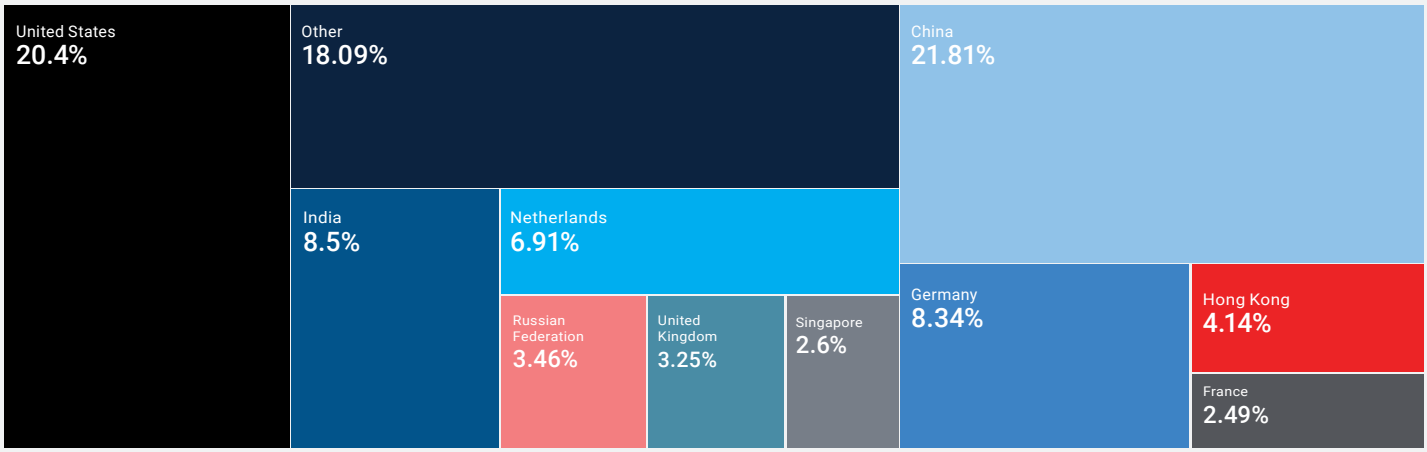
Top detected malicious C2 servers

It's no surprise that Cobalt Strike continued to rank at the top of total C2 detections over the quarter. IronRadar tracked nearly 4,000 malicious Cobalt Strike C2s in the last three months of 2022. But while Cobalt Strike still holds the largest market share, we do see a growing diversity in the C2 environment, with commodity tools such as Metasploit, Racoon Stealer, and Sliver also being popular amongst threat actors.

Though Brute Ratel is mentioned often in public reporting as a growing alternative to Cobalt Strike, it still makes up a very small percentage of total malicious C2 servers detected by IronRadar. However, we have noticed an increase in Sliver detections over the past several months, indicating Sliver and other frameworks like Mythic and Covenant may be favored substitutes of choice for cybercriminals.

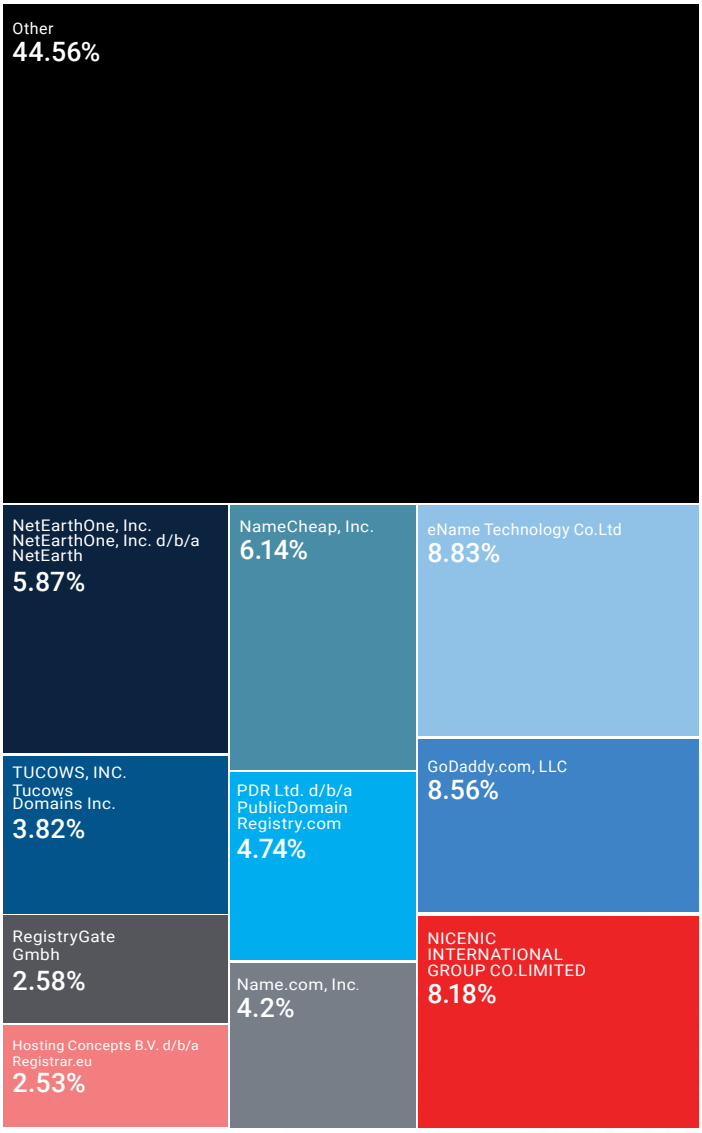
Top countries hosting unique C2s

As opposed to Q3 where IronRadar trends indicated China hosted the largest percentage of C2 servers (38.92%), IronRadar's added detection capability of new tools in Q4 diversified the data's geographical distribution. Since China hosts primarily Cobalt Strike servers – hosting only 4% of C2 servers outside of Cobalt Strike this quarter – the addition of new tools raised the proportion of IronRadar-detected C2s hosted in other countries.



IronNet

When looking at tools other than Cobalt Strike, we see the largest concentration of C2 servers hosted in the U.S. (23.3%), followed by India (13.9%), and Germany (13.8%). While some tools are relatively diverse in where their C2s are hosted, there are others that have large concentrations of C2 servers in specific countries. For example, more than 50% of detected Brute Ratel servers were hosted in the U.S., while 35% of Metasploit servers were hosted in India, and 33% of Raccoon Stealer servers were hosted in the Netherlands. This potentially indicates differing preferences and/or characteristics of threat actors using different tools and frameworks.



Top domain registrars of C2 domains

In Q4, domain registration for C2 servers remained distributed across various registrars. However, rather than seeing strong trends in who threat actors are registering C2 domains with, we've observed trends in how C2 domains are being registered and weaponized.

Many firewalls use domain age as a generic traffic filtering parameter, meaning they will flag, isolate, or block hosts associated with newly registered domains. This is because newly registered domains are commonly known to have a propensity for delivering malware. However, threat actors have caught on to this filtering method and started to try to evade detection through a tactic called domain aging, in which they use domains that were registered years ago and activate them just in time for their campaigns. Threat actors typically acquire aged domains by either buying them from reputation-building markets or waiting for previously registered domains to age, which can be an effective method of bypassing security systems that use registration timing as a detection parameter.[1] There are also observed trends of threat actors, including Russian state-sponsored APTs, re-registering expired domains that are either benign or previously associated with a widely distributed commodity malware to enable follow-on compromises.[2]

IRONNET DETECTION SPOTLIGHT

Defending the NOC at Black Hat Europe

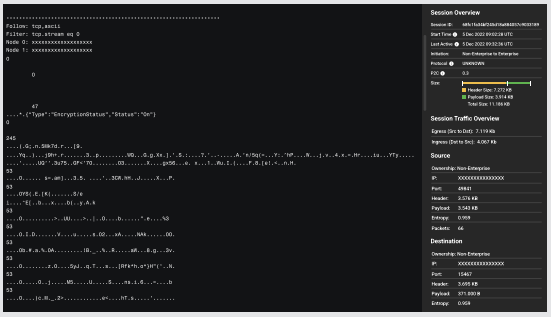
Overview

In early December, IronNet wrapped up another year of defending the Network Operations Center (NOC) at the Black Hat Europe cybersecurity conference. In addition to filling the critical role of providing network visibility for troubleshooting and hygiene in the Black Hat environment, IronNet lent its detection and threat hunting capabilities, which resulted in several malicious and suspicious findings on the network.

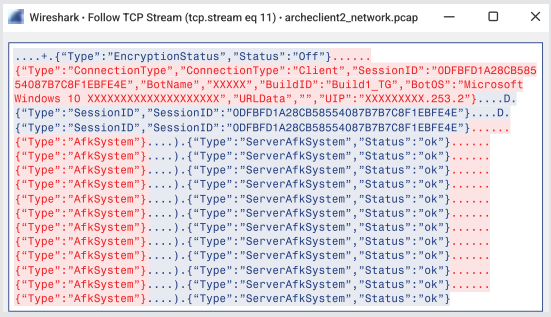
Read the article – Key Findings from Defending the NOC at Black Hat Europe 2022

Arechclient2 Info-Stealer

On the first day of the conference, IronNet hunters observed a user connecting to the network with a device that was already infected with the Arechclient2 info-stealer – a .NET remote access trojan (RAT) with numerous functionalities. Within 10 seconds the user joining the conference wifi, IronNet detected the malware calling out to the attacker-controlled C2, and we were later able to confirm the infection and help the user clean up their device.



IronNet PCAP sample of Arechclient2 encryption flag



PCAP sample of Arechclient2 encryption flag from Tampa Bay Tech

We were able to connect the observed activity to Arechclient2 (aka SectopRAT) based on the string "{"Type":"EncryptionStatus","Status":"On"}", which had been referenced only a few days prior by a Tampa Bay Tech[3] article on Arechclient2 (see comparison of PCAPs below). We also observed outbound C2 communications to a confirmed malicious destination IP (35.198.166[.]27) and Google Cloud hosts on port 15647, aligning with Arechclient2's historical TTPs and further confirming the presence of this malware on the user system.

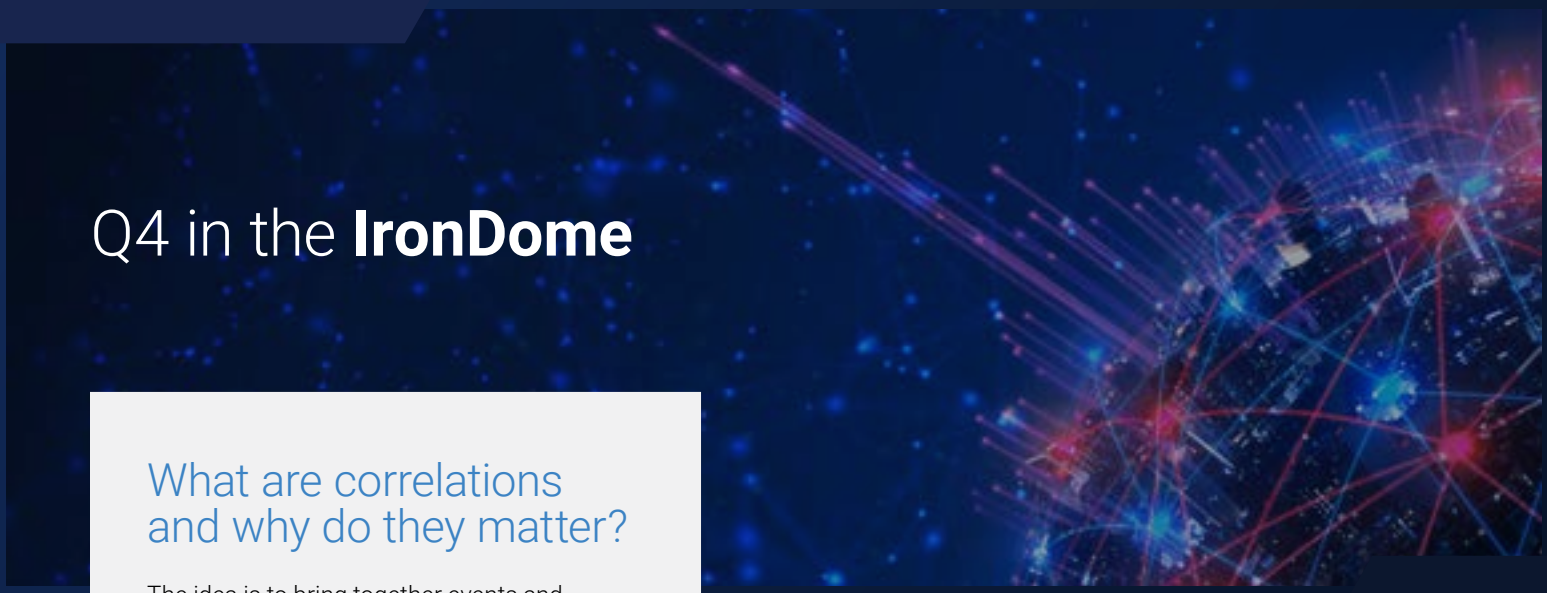
FBDown Chrome Browser Extension

During the conference, a user had a previously installed Chrome Extension called FBDown (Facebook Video Downloader/ Video Downloader Pro) on their laptop, which we observed sending all of the user's browser activity and history via a base64 encoded HTTP POST request to the external server owned by the extension (usage.fdown[.]net/pb). There's no evidence FBDown is malicious in itself, but it does pose a significant security risk. A threat actor could target the extension to access the information of all users who have it installed or try to purchase the extension from the original developer knowing the data it contains.

Following this detection, we rated the alert as malicious (given the sensitivity of the data being collected and high potential for compromise), which automatically pushed the related details to all organizations under IronNet's Collective Defense platform IronDome. As a result, the IronDome platform detected the presence of this extension and associated exfiltration activity across 9 different enterprises in the U.S., Asia, and the Middle East. In one instance, this activity was reported to a customer in the healthcare sector where more than 11 systems were determined to have the browser extension present.

IronNet

Q4 in the **IronDome**



What are correlations and why do they matter?

The idea is to bring together events and alerts from multiple customers' IronDefense deployments into a common data store, enabling similar behavior across networks (aka "correlations" to be identified. These correlations can be made on indicators such as domain and IP or on similarity across a wide variety of features available in event contexts, known as behavioral correlations.

IronDome's unique cross sector visibility grants the ability to analyze and correlate seemingly unrelated instances across enterprise networks, which is critical for identifying sophisticated attackers who leverage various infrastructures to evade detection.

What is IronDome?

IronDome is a Collective Defense platform that correlates similar traffic behavioral patterns across participants within an enterprise's business ecosystem, industry, or region.

How Does it Work?

When the indicator or the attributes of an alert match with an alert in another customer environment, the correlation is shown in the alert interface. There you can see how other customers rated the alert and what their comments were. This is a force multiplier that enables SOCs to work together.

4,100
Total alerts correlated

Data correlated from the IronDome

3,826
Correlated between more than 3 participants

IronNet

IronDome Visibility in the Middle East

Overview

Starting in early November, IronNet observed several malware infections and ongoing intrusions across multiple organizations in a Middle Eastern country. IronDome's visibility across the country enabled participating organizations to connect the dots between malware activity happening in their networks. At the moment, IronNet has ISP-level visibility into these environments, so further investigation into network activity is limited due to the status of our engagement. However, using IronDefense and IronDome in combination with IronRadar intelligence and proactive Threat Hunting queries, IronNet hunters were able to identify several high-fidelity indicators of compromise (IOCs) related to five separate malware variants across six enterprise environments.

Due to IronDefense's North-South visibility, we regularly see first-stage payloads downloading additional malware stages and communicating back to attacker-controlled C2 servers. Threat actors will most likely use this time to harvest credentials, move laterally, and begin to sell access to more sophisticated threat actors. In many cases, the targets were able to identify and remediate the threat in the early stages of the attack; however, post-infection activity has been observed in some environments, including active exfiltration.

The malware we have seen in these Middle East organizations' networks include (but are not limited to):

1. **Smoke Loader** - A modular malware often used to drop additional malware on infected systems, with added modules available for keylogging, credential theft, DDoS, and more.[4]
2. **Raccoon Stealer** - An information-stealing trojan distributed under a malware-as-a-service (MaaS) model that enables the theft of data such as passwords, cookies, crypto-wallet, and autofill data from browsers. A new variant of Raccoon Stealer (Raccoon Stealer v2) was released in early July 2022.[5]
3. **TrickBot** - A former banking trojan that has evolved over the years to add capabilities beyond stealing victim information. As a modular malware, it's able to move laterally within a network, copy itself, and drop additional malware, and it's popularly used in "big game hunting" ransomware attacks.[6]
4. **Powershell Empire** - A post-exploitation framework for Windows, Linux, and macOS with the ability to run PowerShell scripts in memory and make a connection back to a victim machine. It has rapidly deployable post-exploitation modules from key loggers to Mimikatz and sports adaptable communications to evade network detection.[7]
5. **SystemBC** - A proxy malware and remote access tool that leverages TOR to encrypt and hide C2 network traffic, often used by cybercriminals to maintain a foothold within a company's network and launch additional post-exploit tools.[8]

Indicator	Notes
45.144.29[.]18	Last seen being operated by REvil in Spring 2022
77.73.131[.]124	Still active as of November 2022 hosting malicious payloads for RedLineStealer and Smoke Loader
185.99.2[.]115	Weaponized in phishing campaigns by TrickBot threat actors since 2020
data-file-data-7[.]com	Attributed to Raccoon Stealer v2 hosting malicious payloads for various campaigns
uaery[.]top	Observed as a Filecoder ransomware C2 server as of October 2022
guluiiiimnstrannaer[.]net	Still active as of November 2022 hosting malicious payloads for Smoke Loader and Private Loader
simplyadvanced1[.]com	Smoke Loader C2 server
193.33.194[.]176	Attributed to Raccoon Stealer v2 hosting malicious payloads for various campaigns
45.144.29[.]18	Last seen being operated by REvil in Spring 2022 - Large outbound sessions observed to this C2 server

Significant Community Findings

Below you will find a sample of significant community findings from our customers collaborating in our platform. These are notable indicators found among participant environments in IronDome during Q4 that were deemed significant by our analysts due to the affiliation, severity, and/or frequency of the indicator.

Indicator	Details	Recommended Action
Indicator: bbdg[.]net SECTORS DETECTED Healthcare, Energy	This domain was created in 2009 and produces a 403 forbidden error. Associated URLS have been observed containing qakbot.zip in the path and delivering Qakbot payloads. **Associated Malware** Categorized as a Qakbot delivery domain (low-moderate confidence). Qakbot/Qbot is a form of malware/trojan used to exfiltrate data.	It's recommended that traffic analysis be conducted and the domain be blocked. Do not travel to URLs containing qakbot.zip in the path.
Indicator: fdown[.]net SECTORS DETECTED Education, Energy, Defense, Finance, Government, Healthcare, IT, Space, Telecommunications, Transportation	This domain is associated with a suspicious Chrome browser extension called FBDown (Facebook Video Downloader/Video Downloader Pro). This extension exfiltrates all of the user's browser activity and history via a base64 encoded HTTP POST request to this domain (usage.fdown[.]net/pb). **Associated Malware** Though not a confirmed malicious extension, FBDown presents significant security concerns and poses a high risk of compromise.	If seen, it's recommended to investigate POST requests to the URL fdown[.]net/pb. Ensure to only install extensions through trusted sources and closely review all browser extension permissions.
Indicator: progress.cashdigger[.]com SECTORS DETECTED Healthcare, Energy	This domain is indicative of a compromised Wordpress site, which can download malware to endpoints via an executable or a redirect. In this case, the compromised Wordpress sites were: ymcade[.]org, ccrstables[.]com.	It's recommended to block these domains. Take care when traveling to third-party sites and in downloading any files or applications from unverified sites.
Indicator: bongsking[.]com SECTORS DETECTED Finance	IronDome observed suspicious encoded subdomain queries following the same encoding pattern for the domains bongsking[.]com and acescustombuilds[.]com. **Associated Malware** May be related to phishing activity.	Domains could be legitimate, but compromised by a threat actor. If seen, it's recommended to investigate encoded subdomains.

Q4 IronNet Nation-State Analysis

IronNet

RUSSIA

CYBER STRATEGIC OBJECTIVES

- Testing out new tools and techniques for use in potential future attacks.
- Shifting tactical strategy to accommodate faster-pace cyber operations to aid war efforts

Russian APTs trying out new tools and tactics

As the war continues and Russia faces struggles on the battlefield, Russian state-sponsored APTs appear to be dabbling in new tools and tactics for future operations. In October, Microsoft Security Threat Intelligence[9] reported the Sandworm Group deployed a new ransomware called "Prestige" against transportation and logistics industries in Ukraine and Poland. The next month, ESET[10] reported Sandworm also deployed a new wave of ransomware called RansomBoggs against multiple Ukrainian organizations. It's our assessment that rather than having a financial motivation, it's likely these ransomware attacks are efforts to test out new deployment techniques.as Russia is known to deploy ransomware and wipers in tandem and to disguise wipers as ransomware.

In addition to these new ransomware deployments, there has also been an observed shift in tactics by GRU (Russian intelligence directorate) actors. According to Mandiant analysts, GRU cyber campaigns have adopted a faster operating rhythm since the beginning of the war and started focusing on exploiting "edge" devices such as firewalls, routers, and email servers to gain access to networks rather than their typical tactic of phishing. This "living on the edge" strategy allows the GRU to have constant ready-made access to target networks and enables faster-paced operations for disruption and spying.[11] However, this switch to a faster operating rhythm may demonstrate how Russian state hackers are racing (struggling, even) to keep up with the pace of physical war. This is exemplified not only by operational mistakes made by the actors, but also by their repeated use of CaddyWiper – a very simple, does-the-job wiper.

The growing sophistication of hacktivist groups

Since the beginning of the war, we have observed a gradual evolution in both the tactics and targeting of pro-Russian and pro-Ukraine hacktivists, which have come to have a larger operational impact on their targets. A primary example of this is the Cyber Army of Russia's cyber attack on the Slovak Parliamentary, which succeeded in jamming the parliament's entire computer network and forcing the Slovak Senate to cancel its vote on various bills and postpone it several days.[12] This real-world disruption beyond disabling a website was a notable escalation in the Russian hacktivist attacks seen previously during the war. However, we're also seeing the same gradual sophistication in Ukrainian hacktivist attacks – primarily by 'Team OneFist' who is increasingly targeting Russian OT infrastructure. Over the past few months, the group claims to have launched several attacks on Russian energy systems and succeeded at taking their SCADA systems offline. In some cases, they did not only take the SCADA devices offline, but damaged the systems beyond the point of repair.[13]

In light of Q4 trends in Russian cyber activity, organizations should:

1. Be vigilant and active in patching and updating systems, especially public-facing edge devices that may be taken advantage of by threat actors to gain and maintain access to an enterprise's network.
2. Be aware of hacktivist group tendencies to launch attacks on organizations in direct retaliation for expressed support of Ukraine and/or opposition against Russia. Accordingly, entities under heightened risk should increase their securities, especially in regard to DDoS attacks.

CHINA

CYBER STRATEGIC OBJECTIVES

- Securing its sphere of influence and positioning itself to further expand and progress its Belt and Road Initiative in key regions such as the Asia Pacific, Middle East, and Europe.
- Securing its sphere of influence and positioning itself to further expand and progress its Belt and Road Initiative in key regions such as the Asia Pacific, Middle East, and Europe.
- Securing its sphere of influence and positioning itself to further expand and progress its Belt and Road Initiative in key regions such as the Asia Pacific, Middle East, and Europe.

China and the Ukraine-Russia War

It's clear that China remains heavily influenced by the Ukraine-Russia War and has altered its cyber strategy and targeting to accommodate its increased interest in Eastern European affairs. Throughout the year, Chinese threat actors not only have demonstrated a burgeoning interest in Russian and Ukrainian targets, but they also have exploited the ongoing war in Ukraine to create more convincing phishing lures. One recent example of this is a Mustang Panda campaign that used "Political Guidance for the new EU approach towards Russia.rar" as a lure to deliver PlugX malware to European and Asia Pacific entities. The motivation behind this campaign was to steal data detailing those entities' relations with Western countries.[14]

Cyber espionage interest in Myanmar

One country appearing to be a particular focus of Chinese cyber espionage activity in Q4 was Myanmar. Q4 open-source reporting revealed Myanmar entities were the target of three focused and persistent campaigns by the Chinese APT Mustang Panda. Two of these Mustang Panda campaigns – reported on by BlackBerry[15] and Avast Threat Labs[16] – targeted only Myanmar organizations and were successful in stealing troves of data from Myanmar government, army, police, and private institutions, even including Myanmar embassies in other countries as well as opposition groups and NGOs in the country. The third campaign, reported on by Trend Micro[17], involved a wider victimology across the Asia Pacific, but involved several decoy documents linked to organizations working with Myanmar government entities.

These persistent campaigns indicate a very specific interest by China in Myanmar government affairs. This is significant given China's high level of support for the country's military, which staged a coup and ousted the democratically elected Aung San Suu Kyi and her parliament in February 2021.[18] Given China's desire for expansive influence in Southeast Asia, it likely saw this coup as an opportunity to pull the country away from Western and U.S. influence and step in as its closest partner. Focusing cyber espionage attacks on Myanmar entities serves a level of insurance for China to ensure it can maintain control over the government and keep tabs on actions that may oppose China's strategic or commercial interests.

In light of Q4 trends in Chinese cyber activity, organizations should:

1. Keep an eye out for phishing emails with geopolitically themed lures. Chinese APT Mustang Panda, who has been particularly active in cyber espionage campaigns this year, is well-known to conduct spear-phishing attacks using lures that mimic the targeted country or organization or relate to relevant geopolitical events.
2. Increase protections against webshells by employing regular updates to applications and operating systems to fix known vulnerabilities as well as implementing a least-privileges policy on web servers to reduce the ability of attackers to escalate privileges or pivot laterally.

IRAN

CYBER STRATEGIC OBJECTIVES

- Maintaining control over domestic opposition populations protesting against the Islamic Republic.
- Gaining advantage over dissidents, researchers, and civil society groups focused on the Middle East.
- Leveraging well-known exploits and unpatched systems to gain access to high-profile entities in the U.S.

Nationwide protests influence the focus of Iranian cyber operations

Domestic turmoil continued to dominate the Iranian political agenda in Q4 of 2022, as nationwide protests against the Islamic Republic surpassed their 100th day in December. In response to protests – sparked by the unjust detention and death of a young woman named Mahsa Amini for wearing her head covering incorrectly – the Islamic regime launched a brutal security crackdown that has led hundreds of people to be killed and thousands to be arrested.

In addition to scaling back internet and phone connectivity at the beginning of the protests, the Islamic regime has also begun targeting Middle East-focused researchers, civil society groups, and dissidents. The Human Rights Watch[19] reported that beginning in October, Iranian APT42 launched a sophisticated social engineering and credential harvesting campaign targeting two Human Rights Watch staff members and at least 18 other high-profile activists, journalists, researchers, academics, diplomats, and politicians focused on Middle East issues – reportedly succeeding in compromising the sensitive data of at least three of its targets. This is not outside the scope of previous APT42 targeting, who is well known to conduct social engineering and credential harvesting attacks against entities specializing in Middle Eastern affairs, including compromising a U.S. think tank in November.[20]

Using well-known exploits to gain access to high-profile targets

Even a year after it was first discovered and reported, Log4Shell remains a favorite of Iranian threat actors looking to gain initial access. Multiple reports in Q4 detailed Iranian APTs' use of Log4Shell in various campaigns this year to gain access to high-profile systems and conduct post-exploit activity. Specifically, there were several occasions where Iranian threat actors exploited Log4j vulnerabilities in unpatched VMware Horizon servers for initial access.

Q4 reports of this activity include a November alert by CISA[21] stating that from June through July, it investigated a cyber attack by Iranian state-sponsored actors on a Federal Civilian Executive Branch organization. In the attack, the actor exploited Log4Shell in an unpatched VMware Horizon server to gain access to the network, install the XMRig crypto-miner, and perform other post-exploitation activities. Additionally, SecureWorks[22] reported in December that Iranian APT Cobalt Mirage leveraged two Log4j vulnerabilities to compromise an unpatched VMware Horizon server in a U.S. local government network in February.

In light of Q4 trends in Iranian cyber activity, organizations should:

1. If updates or workarounds were not promptly applied following VMware's release of updates for Log4Shell in December 2021, organizations should treat those VMware Horizon systems as compromised. Follow incident response procedures prior to applying updates, but if no compromise is detected, immediately install updated builds to ensure affected VMware Horizon and UAG systems are updated to the latest version.

N.KOREA

CYBER STRATEGIC OBJECTIVES

- Drawing in financial profit through attacks targeting fintech and cryptocurrency companies, as well as ransomware operations.
- Asserting superiority and control over South Korea through cyber operations to support military provocations.

In the last three months of 2022, the North Korean regime continued to try to flex its muscles via artillery tests and assert itself as a dominant nuclear power – with Kim Jong Un himself stating in November that North Korea's ultimate goal is to possess the world's most powerful nuclear force.[23] North Korea's increasingly provocative missile and drone tests, which have crossed into both Japanese and South Korean territory and triggered a military response from South Korea on several occasions, demonstrates the country's desire to stoke tensions and establish itself as a premier threat on the international stage.[24][25]

Stealing Crypto Assets

It's commonly believed that North Korea funds these military tests through its cyber operations targeting cryptocurrency platforms and other fintech organizations, which have been successful in stealing a reported $626 million over the course of the year.[26] Cryptocurrency exchange platforms continue to be a favorite target of North Korean APTs, who use various methods like sophisticated social engineering tactics to steal credentials and siphon funds from crypto-wallets. For example, in October, Japan's National Police and Financial Services Agencies[27] released a joint statement stating the Lazarus Group impersonated Japanese crypto company executives in emails and on social media in order to trick the company's employees, gain access to internal systems, and steal cryptocurrency. Additionally, Volexity[28] researchers reported that from June through October, Lazarus developed and distributed trojanized cryptocurrency apps under the fake brand BloxHolder to infect systems with AppleJeus malware and gain access to networks to steal crypto assets.

Targeting South Korean Users

Apart from using cybercrime to generate revenue, North Korea also conducts cyber espionage operations to gather strategic intelligence from its geopolitical foes. The primary target of these is South Korea, who was not only a target of North Korea's military provocations in Q4, but also a victim of repeated cyberattack campaigns mainly targeting South Korean users. Google's Threat Analysis Group reported in December it observed North Korea's APT37 using the tragic incident that occurred during Halloween celebrations in South Korea as a lure to target South Korean users, with the goal of infecting them with an Internet Explorer 0-day embedded in a malicious document.[29] S2W Talon also published research on three new types of malware disguised as legitimate APKs, which were used by the North Korean APT Kimsuky to target Android devices of South Korean users.[30]

In light of Q4 trends in North Korean cyber activity, organizations should:

1. Be wary of sophisticated attacks targeting Android devices – North Korean APTs such as Kimsuky may use malware disguised as legitimate applications and other advanced methods to target Android devices and steal target information. We recommend avoiding or using special care when downloading viewer programs or document files from third parties on mobile devices.
2. Remain vigilant of highly advanced impersonation techniques used in spear-phishing attacks, where tactics such as thread hijacking and persistent communications via fraudulent accounts are used to target specific employees of interest and gain access to enterprise networks.

Featured Q4 IronNet Threat Research

IronNet analysts and hunters create high-quality content throughout the year to educate the cybersecurity community and contribute to our Collective Defense. These are some of the IronNet articles from Q4 (October - December) that stood out as particularly interesting and noteworthy.

2023 cybersecurity predictions by the IronNet team

As we wrap up a year marked by a global pandemic, a protracted war in Ukraine, soaring inflation, exorbitant gas prices, and relentless ransomware attacks, we look to 2023 and what we predict to see in cybersecurity next year. Read our analysts' 2023 cybersecurity predictions here.

Read the Article | Dec 16 | Threat Research

Key Findings from Defending the NOC at Black Hat Europe 2022

IronNet has wrapped up its second year of defending the NOC at Black Hat Europe. Our detections during the conference revealed not only several active malware infections – such as the Arechclient2 info-stealer – but also a series of poor security practices by attendees that could have led to severe follow-on compromises in both the Black Hat network and their respective enterprises.

Read the Article | Dec 21 | Threat Research

Robin Banks still might be robbing your bank (part 2)

This is the second part of a blog series on the Robin Banks phishing-as-a-service (PhaaS) platform. In this blog, we provide details on actions taken by the Robin Banks administrators following our publication on the platform in July 2022, as well as dive deeper into the infrastructure behind the phishing kit and what our findings may signify to the overall threat landscape.

Read the Article | Nov 3 | Threat Research

IronNet

Q1 2023 Threat Watch

THREAT ACTOR

Royal Ransomware

Royal Ransomware is a ransomware family that surfaced in September 2022 and overtook LockBit in November 2022 to be the most prolific ransomware in the cybercriminal landscape. Targeting healthcare, manufacturing, and energy companies worldwide (with a particular focus on North America), the Royal ransomware group is suspected to be composed of former members of other ransomware groups like Conti and DarkSide. Royal ransomware expands on the idea of partial encryption by configuring parameters that are used to determine the percentage of file content to be encrypted, thus allowing for quicker encryption and more challenges for anti-ransomware solutions.[32]

Mitre TTPs

T1490:
Inhibit System Recovery

T1563:
Remote Service Session Hijacking

T1001:
Data Obfuscation

Q4 Sample Targets

- Intrado Telecommunications (US)
- Queensland University of Technology (AU)
- Silverstone (GB)
- Northwest Michigan Health Services Inc. (US)
- Priority Power Management (US)

Threat Analyst Comment

Royal is often delivered through phishing or malvertising campaigns that use BatLoader and Qbot as malware loaders before dropping Cobalt Strike and the Royal ransomware payload. Researchers have identified groups acting as initial access brokers (IABs) for Royal ransomware affiliates, and the number of organizations compromised with this ransomware has skyrocketed in recent weeks.[31] It is highly likely this trend will continue and that Royal will continue to rival LockBit in both frequency and sophistication of attacks.

MALWARE

Raspberry Robin

Raspberry Robin first surfaced in September 2021 as a relatively low-profile threat known to spread to Windows systems through infected USB drives. Since then, Raspberry Robin – which is also known as QNAP Worm due to its use of compromised QNAP storage servers for C2 – has grown to become a highly active malware that often leads to follow-on hands-on-keyboard attacks and ransomware activity. Though first observed to deploy LockBit ransomware, Raspberry Robin is now also commonly deploying IcedID, Bumblebee, Truebot, Cobalt Strike, and Clop ransomware and has most recently been seen targeting financial and insurance sectors in Europe.[33]

Mitre TTPs

T1091:
Replication Through Removable Media

T1218:
Signed Binary Proxy Execution

T1059:
Command and Scripting Interpreter (Windows Command Shell)

Threat Analyst Comment

Raspberry Robin has evolved from being a widely distributed worm with no observed follow-on activity to one of the largest malware distribution platforms currently active. Given the interconnected nature of the cybercriminal ecosystem, it's likely that Raspberry Robin is purchased and leveraged by a range of cybercriminal actors to gain a foothold into target networks; thus, it poses a threat to organizations of all sectors and sizes.

IronNet

ENDNOTES

1 Yarochewsky. (2022). CashRewindo: How to age domains for an investment scam like fine scotch. Medium. https://blog.confiant.com/cashrewindo-how-to-age-domains-for-an-investment-scam-like-fine-scotch-a48d22788c84.

2 Hawley, Roncone, McLellen, Mattos, & Wolfram. (2023). Turla: A Galaxy of Opportunity. Mandiant. https://www.mandiant.com/resources/blog/turla-galaxy-opportunity.

3 TampaBayTech2. (2022). Arechclient2. Tampa Bay Tech. https://tampabay.tech/2022/11/30/arechclient2/.

4 MITRE ATT&CK. (2018). Smoke Loader. MITRE. https://attack.mitre.org/software/S0226/.

5 Misraa. (2022). Raccoon Stealer v2: The Latest Generation of the Raccoon Family. ZScaler. https://www.zscaler.com/blogs/security-research/raccoon-stealer-v2-latest-generation-raccoon-family.

6 MITRE ATT&CK. (2021). TrickBot. MITRE. https://attack.mitre.org/software/S0266/.

7 MITRE ATT&CK. (2022). Empire. MITRE. https://attack.mitre.org/software/S0363/.

8 BalaGanesh. (2022). SystemBC Malware Being Used by Various Threat Attackers – Initial access to Indicator of Compromise. SOC Investigation. https://www.socinvestigation.com/systembc-malware-being-used-by-various-threat-attackers-initial-access-to-indicator-of-compromise/.

9 Microsoft Security Threat Intelligence. (2022). New "Prestige" ransomware impacts organizations in Ukraine and Poland. Microsoft. https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

10 ESET Research. (2022). Twitter. https://twitter.com/ESETresearch/status/1596181925663760386.

11 Greenberg. (2022). Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless. Wired. https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

12 Reuters. (2022). Slovak parliament suspends voting due to suspected cyberattack. Reuters. https://www.reuters.com/world/europe/slovak-parliament-suspends-voting-due-suspected-cyberattack-2022-10-27/

13 Vedere Labs. (2022). The Increasing Threat Posed by Hacktivist Attacks. Forescout. https://www.forescout.com/resources/threat-report-the-increasing-threat-posed-by-hacktivist-attacks/

14 The BlackBerry Research & Intelligence Team. (2022). Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets. BlackBerry. https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets.

15 The BlackBerry Research & Intelligence Team. 2022. Mustang Panda Abuses Legitimate Apps to Target Myanmar Based Victims. BlackBerry. https://blogs.blackberry.com/en/2022/10/mustang-panda-abuses-legitimate-apps-to-target-myanmar-based-victims.

16 Threat Intelligence Team. (2022). Hitching a ride with Mustang Panda. Avast Threat Labs. https://decoded.avast.io/threatintel/apt-treasure-trove-avast-suspects-chinese-apt-group-mustang-panda-is-collecting-data-from-burmese-government-agencies-and-opposition-groups/.

17 Dai, Su, Lu. (2022). Earth Preta Spear-Phishing Governments Worldwide. Trend Micro. https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html.

18 Paddock. (2022). Myanmar's Coup and Its Aftermath, Explained. New York Times. https://www.nytimes.com/article/myanmar-news-protests-coup.html.

19 Human Rights Watch. (2022). Iran: State-Backed Hacking of Activists, Journalists, Politicians – Ongoing Phishing Campaign Imperils Independent Groups. Human Rights Watch. https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians.

20 Insikt Group. (2022). Suspected Iran-Nexus TAG-56 Uses UAE Forum Lure for Credential Theft Against US Think Tank. Recorded Future. https://www.recordedfuture.com/suspected-iran-nexus-tag-56-uses-uae-forum-lure-for-credential-theft-against-us-think-tank.

21 CISA. (2022). Alert (AA22-320A): Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa22-320a.

22 Counter Threat Unit Research Team. (2022). Drokbk Malware Uses GitHub as Dead Drop Resolver. Secureworks. https://www.secureworks.com/blog/drokbk-malware-uses-github-as-dead-drop-resolver.

23 Al Jazeera. (2022). N Korea aims to have 'world's strongest' nuclear force, Kim says. Al Jazeera. https://www.aljazeera.com/news/2022/11/27/north-korea-aiming-for-worlds-strongest-nuclear-force-kim-says

24 Sang-Hun. (2022). North Korea Launches 23 Missiles, Triggering Air-Raid Alarm in South. NY Times. https://www.nytimes.com/2022/11/01/world/asia/north-korea-missile-launch.html

25 Shin. (2022). South Korea scrambles jets as North Korea sends drones over border. Reuters. https://www.reuters.com/world/asia-pacific/south-korea-briefly-suspends-flight-departures-upon-military-request-official-2022-12-2

26 The Associated Press. (2022). North Korea has hacked $1.2 billion in crypto and other assets for its economy. NPR. https://www.npr.org/2022/12/22/1144996480/crypto-hacking-north-korea-billion.

27 Hakki. (2022). North Korea's Lazarus Group Attacks Japanese Crypto Firms. Decrypt. https://decrypt.co/112130/north-koreas-lazarus-group-attacks-japanese-crypto-firms.

28 Roxan, Rascagneres, Mora. (2022). Buyer Beware: Fake Cryptocurrency Applications Serving as Front for AppleJeus Malware. Volexity. https://www.volexity.com/blog/2022/12/01/buyer-beware-fake-cryptocurrency-applications-serving-as-front-for-applejeus-malware/.

29 Lecigne & Sevens. (2022). Internet Explorer 0-day exploited by North Korean actor APT37. Google Threat Analysis Group. https://blog.google/threat-analysis-group/internet-explorer-0-day-exploited-by-north-korean-actor-apt37/.

30 Sebin & Yeongjae. (2022). Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware. S2W Talon. https://medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-discovered-mobile-malware-280dae5a650f.

31 Microsoft Security Threat Intelligence. (2022). DEV-0569 finds new ways to deliver Royal ransomware, various payloads. Microsoft. https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/.

32 Cybereason Global SOC & Cybereason Security Research Teams. (2022). Royal Rumble: Analysis of Royal Ransomware. Cybereason. https://www.cybereason.com/blog/royal-ransomware-analysis.

33 Microsoft Security Threat Intelligence. (2022). Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity. Microsoft. https://www.microsoft.com/en-us/security/blog/2022/10/27/raspberry-robin-worm-part-of-larger-ecosystem-facilitating-pre-ransomware-activity/.

Transforming cybersecurity **through Collective Defense**

our mission Deliver the power of **collective cybersecurity** to defend companies, sectors, and nations

our vision People, companies, and nations can live and work with peace of mind in cyberspace

Collective attacks need Collective Defense

See it in action:

Request a Demo

Try IronRadar today:

Get a Free 14-day trial

IronNet

