IronNet

Annual **Threat Report** 2022

Events and trends that have impacted the cybersecurity landscape in the past year

Foreword

Keith Alexander

GEN (Ret) Keith Alexander
IronNet Founder, Chairman, & CEO

▶ When we created IronNet in 2014, our mission was to bridge the gap between the public and private sectors. The government could not see active threats against the private sector, and as a consequence, could not defend against real-time attacks. At the same time, the private sector did not have the ability to share unknown, real-time threats with the government at network speed. The energy sector specifically came up with the phrase: "We need to be able to shoot the archers." IronNet has created the capability to share real time threats between the public and private sectors, enabling the energy sector's vision.

Our story is part of a larger Collective Defense story - one that we saw play out both physically and in cyberspace this year. As Russia invaded Ukraine, we saw the bonds of NATO grow stronger and technology companies from around the globe unite to defend Ukrainian infrastructure. We saw multiple law enforcement task forces work hand-in-hand to take down cybercrime actors and shut down several prolific ransomware groups. Through IronNet's Collective Defense platform IronDome, we had unique visibility into equitable collaboration, where smaller companies alert larger organizations of emerging attacks, and large organizations with more resources provide context to the activity targeting both organizations.

Our 2022 Annual Threat Report not only provides insight into emerging cyber trends and efforts by threat actors to evade detection, but also demonstrates how we collectively worked together to defend our businesses and our nations.

Anthony Grenga

VP of IronNet's Cyber
Operations Center (CyOC)

▶ IronNet's Annual Threat Report paints a picture showing how threat actors are constantly trying new tactics to evade detection, whether it be changing their infrastructure, testing bypasses for mitigations, or targeting assets that may have been overlooked in a M&A. To combat this evolution, IronNet launched IronRadar, our purpose built threat feed that uniquely identifies and tracks attacker infrastructure while it's being stood up, keeping us one step ahead. Additionally this year, we leveled up IronDome's capabilities through continuous automated threat hunting and detection engineering via IronPredator.

Our Annual Threat Report shares unique observations and analysis from our Threat Research Team, combined with intelligence drawn from the vast telemetry of the IronNet ecosystem and the services we offer. This provides crucial insight into the ever-evolving cyber threat landscape so security teams can be more proactive in their defenses while we continue to move the community together to collectively defend against cyber threats.

IronNet's Annual
Threat Report

This report provides an overview of the events and trends that impacted the cybersecurity landscape in 2022, as seen by IronNet analysts and hunters.

Report Highlights

Nation-state Analysis: Threats from the Big Four

Assessments of the largest geopolitical developments for Russia, China, Iran, and North Korea – with special analysis on the Ukraine-Russia War. Includes explanations of the countries' strategic objectives in cyber with examples of corresponding attacks, as well as actionable recommendations for avoiding compromise by these countries' APTs.

Adversary Infrastructure: By the Numbers

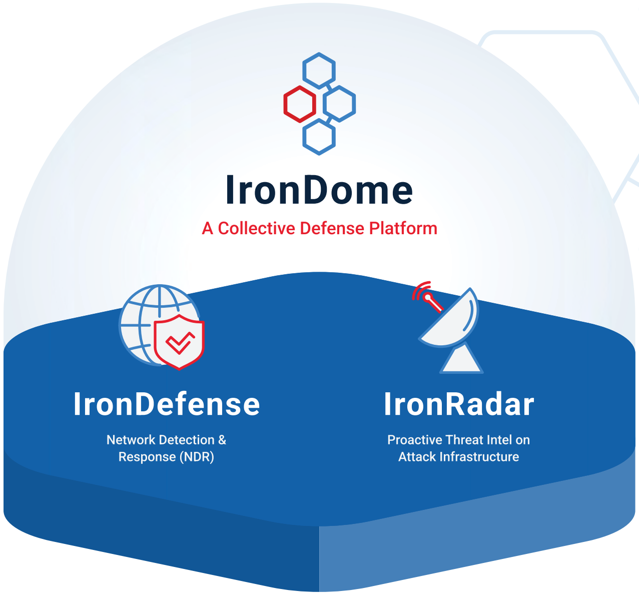
Insight into adversary infrastructure trends, including breakdowns of the top countries, cloud providers, and domain registrars hosting IronRadar-detected C2 servers, as well as new evasive tactics by threat actors.

A Spotlight on Sliver Research

Analysis of recent increases in IronRadar-detected Sliver C2 servers and details into characteristics that make Sliver likely to rival Cobalt Strike as the preferred post-exploitation framework for threat actors.

Detecting a MUMMY SPIDER campaign and Emotet infection

Observations from our investigation of a new MUMMY SPIDER campaign testing a new bypass for Microsoft disabling macros by default and discussion of trends observed while tracking Emotet infrastructure activity via IronRadar.


IronDome
A Collective Defense Platform
IronDefense
Network Detection & Response (NDR)
IronRadar
Proactive Threat Intel on Attack Infrastructure

THE IRONNET ECOSYSTEM

The IronNet ecosystem works together to provide organizations with the most comprehensive coverage to identify threats in their networks. **IronRadar** acts as an early warning system of adversary infrastructure that enables organizations to proactively block malicious C2 activity. **IronDefense** is a Network Detection & Response (NDR) platform with sensors positioned around the world to help paint a real-time view of cyber activity. **IronDome** is an intelligence collaboration platform that aims to improve the way organizations share attack intelligence in order to provide sectors and communities with a Common Operating Picture (COP) of the cyber threat landscape.

The analysis in IronNet's 2022 Annual Threat Report is drawn from telemetry provided by IronNet's network detection and response (NDR) platform IronDefense and automated Collective Defense platform IronDome. The telemetry from our detections and behavioral correlations is combined with unique insights granted from our proactive threat intelligence feed IronRadar, as well as with intelligence from our partners, to help us in our investigations.

2022 IronNet **Nation-State** Analysis

2022 was busier than ever for nation-state actors, who consistently used cyber operations to achieve their strategic goals. In this section, IronNet analyzes the geopolitical and cyber activity of the Big 4 (Russia, China, Iran, & North Korea) and provides actionable recommendations to avoid compromise by these countries' APTs.

RUSSIA

Most active groups APT29, Cold River, Gamaredon

Popular targets

Government	Ukraine
Defense	NATO
Telecommunications	U.S.
Energy & Utilities	Poland
NGOs	Estonia

Snapshot: Russia in 2022

When Russia invaded Ukraine in February 2022, it had a historical impact on world order, globalization, and international collaboration. Russia's invasion inspired an unprecedented wave of economic sanctions and diplomatic severances, which fundamentally changed the role Russia plays within the global economy. In all situations, Russia has tried to maintain the upper hand through tactics such as cutting off oil supplies, threatening nuclear warfare, directing missile attacks on Ukrainian critical infrastructure and civilians, and waging offensive cyber operations.

Strategic Objectives in Cyber

Causing disruption and discord within and between Ukraine and NATO countries

In Russia's initial invasion, it leveraged various wiper variants in an effort to disrupt critical systems in Ukraine and its allies. While some attacks caused more damage than others, many failed to accomplish their goal.

- In February 2022, Russian state-sponsored threat actors used the AcidRain wiper to wipe SATCOM modems at Viasat's KA-SAT satellite broadband service, impacting 5,800 German wind turbines and thousands of European satellite internet users.[1]
- In April 2022, Russian APT Sandworm targeted Ukrainian electrical substations using a new variant of Industroyer malware, but the attack was detected and mitigated before a blackout impacting roughly two million people occurred.[2]

Targeting Ukraine and NATO countries in cyber espionage operations to collect information from strategic sectors such as diplomatic missions, government, NGOs, and think tanks.

After falling short in its disruptive attacks, Russia pivoted its efforts to cyber espionage as it realized information on strategic plans by the Ukrainian government and NATO could provide it with more of an advantage in its war operations than temporary disruptions.

- APT29 targeted several Western diplomatic missions between May and June 2022 in a new phishing campaign using online storage services to evade detection.[3]
- In August 2022, APT29 conducted multiple highly targeted and concurrent campaigns against government organizations, NGOs, IGOs, and think tanks in the U.S., Europe, and Central Asia.[4]

Recommendations

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.

Identify the attack surface of the organization by mapping and accounting all external-facing assets (applications, servers, IP addresses) that are vulnerable to DDoS attacks or other cyber operations.

CYBER IN THE Ukraine-Russia WAR

As the largest military conflict in the age of cyber began, many prepared for the cyber domain to be as much of a battleground as in Ukraine. However, the war has played out much differently than most expected – instead of being the architect of a debilitating cyber campaign, Russia's operations were faced with resistance as Ukraine's defenses continually repelled attacks and Russian cyber weaknesses began to show. **With the cyber domain creating a whole new war front, the Ukraine-Russia War instigated one of the largest displays of collective cybersecurity in history, as not only governments jumped in to assist Ukraine in its cyber defenses, but also technology companies from around the world.**

Collective Defense Actions that Changed the War

Hunt forward operations

The U.S. deployed its largest "hunt forward" team in history to hunt for malicious cyber activity on Ukrainian networks – enabling Ukrainian and Western cyber experts to sit side-by-side as they meticulously hunted for any threats or vulnerabilities that may compromise Ukrainian organizations.[5]

Digitizing government services and increasing digital resilience

The private sector aided Ukraine in migrating its data and services to distributed cloud servers. They also provided automated defense of networks and threat intelligence that gave Ukraine more resilience than what it could have achieved alone.

Threat intelligence sharing

U.S. agencies and various cybersecurity groups began establishing mechanisms and processes for bidirectionally sharing intelligence with Ukrainian partners, including indicators of compromise, adversary TTPs, strategic assessments, and more.

Cyber "boots-on-the-ground"

System and Network Administrators are not only defending cyber attacks but are working tirelessly to keep systems up from bombed-out network infrastructure. Engineers are motivated by ensuring that vital information is provided to Ukrainians, remembering that "networks allow families to stay in touch, [and] internet and phone connections often mean human connection."[6]

Utilizing digital platforms for humanitarian assistance and civil defense

Throughout the war, Ukraine has creatively used various forms of technology to aid its war efforts. This includes leveraging Russian soldiers' use of open cell phone lines to track force positions and get inside information; creating apps to allow civilians to report sightings of incoming strikes; and using social media to mobilize hackers around the world to join Ukraine's IT Army.

A Collective Defense Effort

Unfortunately, the current state of geopolitics suggests the conflict in Ukraine will not be the last time entities need to work together to provide cyber assistance to a nation under attack. For this reason, it's important to learn from the effort in Ukraine as Russia's invasion has given impetus for governments to institutionalize and scale new approaches mitigate future cyber conflicts. Though the collective cyber defense assistance to Ukraine has been remarkably effective, one element that's created complications is that none of the entities assisting Ukraine have a complete picture of cyber attacks targeting the country. This exemplifies the need for countries and companies to set up the foundations for collective defense by investing in platforms and tools that can coordinate activity and intelligence between organizations to reinforce better collaboration.

CHINA

Most active groups Mustang Panda, APT41, APT10

Popular targets

Government
Defense
Technology
Human Rights Activists
Research

Ukraine
Russia
Taiwan
U.S.
Japan

Snapshot: China in 2022

In 2022, the People's Republic of China (PRC) struggled to maintain an upper hand in the international arena while focusing its domestic efforts on recovering from the pandemic and quelling opposition to its strict zero-COVID policy. After Russia invaded Ukraine, it wasn't long before eyes turned to China in fear it would follow Russia's lead. As a result, China's threat to Taiwan and the South China Sea became the center of attention for surrounding nations as they began to increase their defenses. Beyond navigating the ramifications of Russia's invasion, China's top priorities continued to be expanding global influence through infrastructure investment and boosting the economic success of its commercial sector.

Strategic Objectives in Cyber

Remain a step ahead in the Ukraine-Russia conflict and the international response to the war

It's clear that China has been heavily influenced by the Ukraine-Russia War and altered its cyber strategy and targeting to accommodate its increased interest in Eastern Europe. Throughout the year, Chinese threat actors not only demonstrated a burgeoning interest in Russian, Ukrainian, and Belarusian targets, but also exploited the war to create more convincing phishing lures.

- In January 2022, Chinese APT TA428 carried out a targeted cyber espionage campaign against numerous military industrial enterprises and public institutions in Russia, Ukraine, Belarus, and Afghanistan.[7]
- In April 2022, Ukrainian intelligence accused China of targeting more than 600 websites belonging to Ukrainian government, military, and critical infrastructure leading up to Russia's invasion.[8]

Keep an edge of intimidation over Taiwan

Throughout the year, China consistently ran invasive military drills around Taiwan and violated its air defense zone. In cyberspace, China's intimidation tactics were no different. In addition to numerous cyber espionage campaigns against Taiwanese entities, China also launched DDoS attacks to intimidate the Taiwanese government.

- In February 2022, Taiwanese researchers reported that APT10 conducted a series of large-scale supply chain attacks targeting financial software systems in Taiwan.[9]
- In August 2022, Taiwanese government websites were targeted in DDoS attacks and experienced intermittent outages just ahead of U.S. Speaker Pelosi's arrival.[10]

Recommendations

Immediately patch network devices. Chinese actors like to use common vulnerabilities to gain access to target networks, like those in Small Office/Home Office (SOHO) routers and Network Attached Storage (NAS) devices, as well as well-known vulnerabilities like Log4Shell in VMware Horizon servers.[11, 12]

Keep an eye out for phishing emails with geopolitically themed lures. Chinese APT Mustang Panda is well-known to conduct spear-phishing attacks using lures that mimic the targeted country or organization or relate to relevant geopolitical events.

IRAN

Most active groups

MuddyWater, Charming Kitten, Cobalt Mirage

Popular targets

- Government
- Journalism/media
- Human rights activists
- Civilians
- Telecommunications

- Israel
- Saudi Arabia
- U.S.
- Turkey
- Armenia

Snapshot: Iran in 2022

As the Iranian government drew international ire for supplying weapons and drones to Russia in its attacks on Ukraine, the Iranian public's dissatisfaction with the country's leadership became increasingly clear. After national protests broke out in May in response to cuts on state subsidies on food, the nation rose up again in September following the unjust detention and death of 22-year-old woman Mahsa Amini by Iran's morality police. The protests, which are still ongoing, have been met with a brutal security crackdown by the Islamic Republic that led hundreds of people to be killed and thousands to be arrested.

Strategic Objectives in Cyber

Maintaining control over domestic populations

Violence wasn't the only tactic the Iranian government used to quell protests, as they heavily restricted internet and mobile access to multiple parts of the country during the uprisings. Additionally, the Islamic Republic also tried to monitor the activities of Iranian citizens to stay ahead of any plans of dissent.

- Amid protests over the death of Mahsa Amini in September 2022, sources confirmed a near-total disruption to internet service in parts of the country, as well as a nation-scale shutdown of mobile networks and curbed access to social media.[13]
- In October 2022, Iranian APT Domestic Kitten (APT-C-50) used a new version of the Android malware FurBall in a long-running mobile surveillance campaign targeting Iranian citizens.[14]

Showing strength through retaliation

Iran is well-known for its retaliatory attack strategy, and it doesn't hesitate to turn to cyber to respond to a variety of perceived transgressions. Retaliatory cyber attacks and making diplomatic threats, like refusing to sign the JCPOA, serve as Iran's way of showing it has the capabilities to strike back against perceived threats and insults.[15]

- In retaliation for an Israeli airstrike in Syria in March 2022, Iranian threat actors launched a DDoS attack on Israeli telecom providers, taking down several Israeli government websites.
- Shortly after Albania cut diplomatic relations with Iran in September 2022, Iranian state actors launched a second cyber attack on Albania's national police computer systems, impacting control systems at seaports, airports, and border posts.[16]

Recommendations

Prioritize patching well-known and critical vulnerabilities that allow for remote code execution on internet-facing systems. Exploiting Log4Shell was one of the most popular initial access methods among Iranian actors in 2022. If updates were not applied following VMware's release of updates for Log4Shell in December 2021, organizations should treat those systems as compromised. Follow incident response procedures prior to applying updates, but if no compromise is detected, immediately install updated builds to VMware Horizon and UAG systems.

N.KOREA

Most active groups

The Lazarus Group, Kimsuky, APT37

Popular targets

- Cryptocurrency
- Finance
- Defense
- Research
- Journalism/Media

- South Korea
- U.S.
- Japan
- Europe

Snapshot: North Korea in 2022

In 2022, North Korea carried out an unprecedented number of missile and weapons tests in an effort to 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.[17] North Korea's increasingly provocative artillery tests, which have crossed into both Japanese and South Korean territory and triggered a military response from South Korea on several occasions, clearly demonstrate North Korea's desire to stoke tensions and establish itself as a premier threat on the international stage.[18, 19]

Strategic Objectives in Cyber

Funding missile and weapons program through cyber operations

It's commonly believed that North Korea funds its military tests through its cyber campaigns targeting cryptocurrency organizations, which have been successful in stealing a reported $626 million over the course of the year. [20] These compromises typically include persistent social engineering campaigns, often targeting employees at cryptocurrency companies.

- In March 2022, The Lazarus Group used a fake job scheme to hack the play-to-earn Axie Infinity game to steal a total of $540 million (at the time of theft). [21]
- In October 2022, The Lazarus Group targeted Japanese crypto firms by impersonating company executives to trick employees, gain access to internal systems, and steal cryptocurrency. [22]

Stealing IP to bolster weapons development

To support its weapons programs, North Korea also used cyber espionage to try to steal intellectual property (IP) from defense industrial base organizations. It's likely North Korea is trying to collect confidential information that may help in its research and development of advanced weapons and machinery.

- In February 2022, a new campaign by The Lazarus Group used employment phishing lures to target U.S. defense sector job applicants, including those at Lockheed Martin. [23]
- Silent Chollima exploited Log4Shell in February 2022 to breach an engineering firm working in the energy and military sectors with the likely goal of stealing sensitive IP. [24]

Recommendations

Educate employees on social engineering tactics on social media and spear-phishing emails. Employees of fin-tech and defense organizations should be especially cautious, as North Korea launched numerous attacks this year impersonating organizations to lure employees with fake job opportunities.

Be cautious with third-party downloads—especially cryptocurrency applications. North Korean actors have repeatedly demonstrated the ability to trojanize applications and gain a foothold on host devices, so it's important for users to always verify file downloads and ensure the application is from a primary or reputable source.

KEY TRENDS IN Ransomware 2022

Law enforcement and international collaboration have changed the ransomware game

Following a series of large ransomware attacks in 2021, like those on Colonial Pipeline and Kaseya, several ransomware groups were forced underground because of law enforcement measures. Through the end of 2021 and into 2022, the strong government response to ransomware included:

- Law enforcement "Hack-Back" operations to shut down attack infrastructure and recover stolen/paid funds
- National and international law enforcement task forces dedicated to ransomware investigations
- Stricter regulations on cyber attack reporting
- Sanctions on ransomware groups (making it illegal for companies to pay them)
- Arrests and indictments of cybercriminal group members

The large-scale ransomware attacks also led to greater cybersecurity awareness and motivated many companies to put in place mitigations in case of an attack. As a result, it's become riskier for cybercriminals to target large organizations, leading them to alter their targeting and tactics.

1 A shift from "big game hunting" to targeting vulnerable prey

As opposed to 2021, which was characterized by attacks on large, high-profile organizations, 2022 has seen ransomware groups shift their attention on more small- and medium-sized businesses (SMBs). As cybercriminals realized that disrupting larger organizations can provoke investigations, they began to focus their attacks on SMBs that typically generate less attention, have less cyber resources, and are more vulnerable to exploitation.

2 Out with the Conti, in with the influx of replacements

In what's now referred to as the "Conti Leaks," retaliatory attacks on Conti infrastructure in early 2022 led the ransomware group's operations and secrets to be exposed on a global scale. As Conti went underground, a surge of new ransomware groups like Black Basta, Black Cat (ALPHV), and BianLian began to flood the market. While Conti may have moved its operations into other ransomware brands, it's likely many groups used Conti's exposed tactics to jumpstart their own operations in an opportunistic effort to fill the new market gap.

3 A rise in extortion without ransomware

In late 2021, we began to see a rise in extortion incidents not involving ransomware. While cybercriminals commonly employ double-extortion (encryption + data theft), several groups in 2022 – such as Karakurt, Lapsus$, and RansomHouse – chose to skip over the encryption step and only steal data for ransom. By not deploying ransomware, the actors can still ransom companies while avoiding any operational disruptions that would result from encryption.[25]

2022 Adversary Infrastructure Trends

This analysis of adversary infrastructure trends is drawn from data produced by IronNet's proactive threat intelligence feed IronRadar.

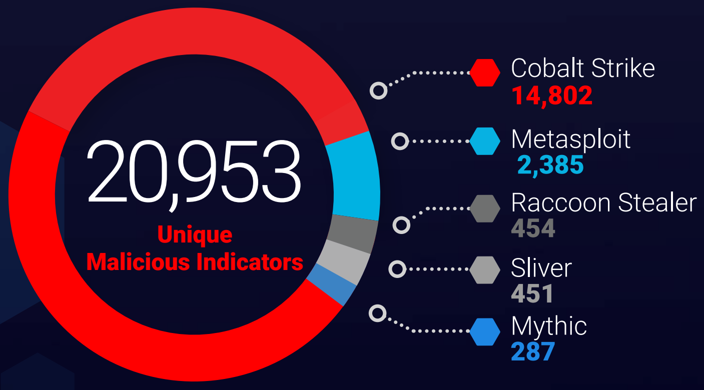
IronRadar

ADVERSARY INFRASTRUCTURE TRACKING

IronNet tracks the creation of new attack infrastructure for numerous post-exploitation toolkits, vulnerability scanners, and remote access trojans (RATs) through a unique fingerprinting process to track observable artifacts, such as server certificates, HTTP listeners, and management services. Our expert scanning and probing techniques allow us to detect and identify malicious infrastructure as it's being stood up and weaponized, before it's used in an attack. This intelligence is generated via IronNet's proactive threat intelligence feed **IronRadar**, which automatically equips organizations with the intelligence they need to proactively block adversary infrastructure before it can be used against them. IronRadar's advanced detection coverage provides us with unique insight into many characteristics of C2 infrastructure and allows us to map the techniques, tools, and procedures (TTPs) of how threat actors are setting up their malware infrastructure for attacks.

TOP 5 MOST DETECTED TOOLS

Number of Malicious Indicators Detected



TRENDS IN C2 INFRASTRUCTURE

- While Cobalt Strike remains the top C2 framework abused by threat actors, IronRadar data shows an increase in Sliver C2 servers in the second half of 2022, indicating Sliver may match or even overtake Cobalt Strike as the most popular C2 framework this year.
- Threat actors are adopting more evasive tactics to bypass traditional C2 detection mechanisms and make their infrastructure less detectable, including discarding, aging, reusing, and recycling domains.
- Because of the heavy use of vulnerability scanners by threat actors, IronRadar often detects scanners like reNgine used in combination with various C2 frameworks and commodity tooling, such as Racoon Stealer, IcedID, and Aurora Stealer.

DEBUTING

IronRadar℠

In September of 2022, IronNet debuted its new threat intelligence solution **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

What is adversary infrastructure?

Adversary/Attack infrastructure are the tools, services, and processes threat actors use to stage, launch, and execute an operation. Most often, this includes the use of a command-and-control (C2) server, which allows an attacker to drop malware, communicate with compromised systems, and exfiltrate data.

IronRadar
Infrastructure TTP Mapping

When it comes to cyber defense, we talk about how actors breach and move around a network via TTPs (Tactics, Techniques, and Procedures). Well, what if we could define and track the TTPs and patterns a threat actor exhibits when setting up their infrastructure?

IronRadar detects adversary infrastructure as it's being stood up and weaponized, allowing us to map the infrastructure TTPs of various APTs and cybercriminal groups.

IronRadar detected a cluster of Cobalt Strike servers linked to Chinese APT41 subgroup 'Earth Longzhi' in December 2021 - 11 months prior to public attribution.[26]

We also located additional Cobalt Strike servers with similar infrastructure characteristics which we believe are connected to threat groups under APT 41.

INFRASTRUCTURE TTPS

- **Hosting:** DigitalOcean data center in Singapore
- **Redirection:** Cloudflare
- **Domain registrar:** Tucows and GoDaddy
- **TLS certificates:** Let's Encrypt

IronRadar detected several Cobalt Strike servers targeting Ukraine up to almost a year before CERT-UA reported the indicators.[27]

Months before Russia's invasion, IronRadar discovered multiple Metasploit and Cobalt Strike servers being stood up. We were not aware of their targets at the time, but they all followed similar patterns in the malleable profiles they used and some other infrastructure details. As the war progressed, we observed the attributes of the payload change on a weekly basis, such as the domains rotating to domains that were bought weeks instead of months prior.

INFRASTRUCTURE TTPS

- **Hosting:** Hostkey
- **Domain registrar:** Eranet
- **TLS certificates:** Let's Encrypt

IronRadar detected a Cobalt Strike server linked to MUMMY SPIDER, the actor behind Emotet, about three months prior to the server being reported by open sources.

We observed this Cobalt Strike server go on- and off-line several times over the following months, each time coming online with new malicious C2 domains. We also noticed an overlap between these C2 domains and Wizard Spider (aka TrickBot) infrastructure we had recently identified. Given reports in November 2021 that Emotet rebuilt its botnet using TrickBot's infrastructure, this is significant as it shows continued overlap between the two families.

INFRASTRUCTURE TTPS

- **Hosting:** Hostkey
- **Domain registrar:** NiceNIC
- **TLS certificates:** Let's Encrypt

Adversary Infrastructure:

By the Numbers

Top countries hosting unique C2s

China	29.54%
United States	22.01%
Germany	5.82%
Netherlands	5.57%
India	5.31%

- Together, China and the United States hosted more than 50% of all C2 servers detected by IronRadar in 2022. China's top spot in C2 server hosting, however, primarily stemmed from hosting C2s of one specific framework: Cobalt Strike. In fact, China hosted only 6% of C2 servers outside Cobalt Strike over the course of the year.

- While some tools are relatively diverse in where their C2s are hosted, there are others with large concentrations of servers in specific countries – potentially indicating differing preferences among threat actors using different tools.

  For example:

  40% of detected Brute Ratel C2 servers were hosted in the U.S.;

  33% of Responder C2 servers were hosted in Ireland;

  25% of Metasploit C2 servers were hosted in India.

Top cloud providers hosting unique C2s

Amazon AWS	33.32%
Tencent Cloud	25.72%
Digital Ocean	19.5%
Vultr	5.06%
Alibaba Cloud	4.53%

- On a month-to-month basis, there was a consistency amongst the top cloud providers hosting detected C2 servers, with Amazon, Tencent Cloud, and DigitalOcean holding the top three spots respectively. Cobalt Strike and Metasploit accounted for a large percentage of C2 servers hosted by the top cloud providers, but Sliver C2 servers began to make up a larger percentage of detected servers in the last three months of the year.

- More than 92% of detected C2s hosted by Tencent Cloud were Cobalt Strike Servers. Given Tencent Cloud is located in Shenzen, China, this is likely why we see a large concentration of Cobalt Strike C2s hosted in the country and why China consistently ranks at the top of countries hosting detected C2s.

Adversary Infrastructure: By the Numbers

CONTINUED

Top domain registrars of C2 domains

eName	22.47%
GoDaddy	9.51%
Eranet	7.31%
NiceNIC	6.41%
NameCheap	5.93%

In 2022, domain registration for C2 servers was distributed across various registrars. While we saw continued popularity among large registrars, we noticed a trend of threat actors favoring registrars that value privacy, accept cryptocurrencies, and have a lax review process of abuse reports. For example, this year, we observed a steady decrease in the use of NameCheap by threat actors following changes to Namecheap's abuse reporting process in June 2021.

We've also observed threat actors try to evade detection by being more strategic in how they set up and use their attack infrastructure. Many firewalls use domain age as a generic traffic filtering parameter, meaning they will flag, isolate, or block hosts associated with newly registered domains. To bypass this filtering method, threat actors are using a tactic called domain aging, where they use domains registered years ago and activate them just in time for their campaigns. Threat actors also commonly go to resellers to buy domains that have a prior history as a benign site (e.g. domain categorization), while others re-register expired domains previously associated with a commodity malware.[28]

For these reasons, we advise analysts and researchers to remain vigilant when analyzing domain registration information. By comparing whois created and updated dates, along with historical whois data, a user can gain valuable insights into possible ownership changes that may reveal the current purpose of the domain.

A SPOTLIGHT ON

IronNet Sliver Research

Advertised as an "open-source alternative to Cobalt Strike," Sliver was created by lead researchers Joe DeMesy and Ronan Kervella from Bishop Fox to be an adversary emulation/red team framework that allows organizations of all sizes to perform security testing.[29] Since its creation in late 2019, Sliver has repeatedly been seen used in the wild by nation-state APTs and ransomware-as-a-service (RaaS) affiliates.[30]

There are many attributes that make Sliver a prime alternative to Cobalt Strike, and in many ways, Sliver has features that present it as an even more attractive option to cybercriminals. As a framework written in Golang and available via GitHub, Sliver includes many common C2 framework features, such as multiple C2 channels, multi-user operation, user-developed extensions, and payload generation.

Other benefits of Sliver include:

- Being free and open-source, negating the need for a license or cracked version such as with Cobalt Strike.
- Being developed by top-tier developers and frequently updated with new capabilities.
- Incorporating operational security around its C2 listeners with procedural C2, JARM and Certificate randomization, and mutual authentication.
- Having native support for Let's Encrypt Certificates.
- Supporting dynamic code generation and compile-time obfuscation for implants and supports MacOS, Windows, and Linux.
- Supporting a malleable C2 profile, which is one of the key advantages of Cobalt Strike.

Alternatives to Cobalt Strike: Sliver v. Brute Ratel

Though Brute Ratel is often mentioned in reporting as a growing alternative to Cobalt Strike, it still makes up a small percentage of malicious C2 servers detected by IronRadar. Brute Ratel has certain advantages as a C2 framework, like also supporting malleable C2 profiles, but there's only one cracked version, making its accessibility and use more limited. Instead, we've observed an increase in Sliver detections over the past several months, including a nearly 25% increase in December 2022 alone. This increase supports the assessment that Sliver will likely match Cobalt Strike as the fastest growing C2 framework among threat actors this year.

2022 Sliver Servers Usage

(observed by IronRadar)

Digital Ocean as primary **hosting provider**

Let's encrypt as primary **TLS cert provider**

Name.com as primary **domain registrar**

Sliver to rival Cobalt Strike as fastest growing C2 framework among threat actors?

IronNet has observed an increase in Sliver detections over the past several months, including a nearly **25% increase in December 2022 alone.**

IRONNET DETECTION SPOTLIGHT

Defending the **Black Hat Conference** Networks

Overview

For the past two years, IronNet has played a critical role in defending the Network Operations Center (NOC) at the Black Hat security conferences in Asia, the U.S., and Europe. At the conferences this year, IronNet's detections revealed not only several active malware infections, but also a series of poor security practices by attendees that could have led to severe follow-on compromises.

A Key Partner in Defending the NOC at the Black Hat Cybersecurity Conferences

2	Number of years IronNet has defended the Black Hat NOC
20,000+	Number of attendees at Black Hat USA
6	Number of companies defending the NOC

> ***Having the opportunity to defend one of the world's leading cybersecurity conferences has been incredibly rewarding*** *and provided exposure to a wide range of cyber threats. From detecting North Korean campaign domains at BH USA to discovering Shlayer malware at BH EU, I've been able to assist in protecting the BlackHat ecosystem for the past two years.* ***After the events, taking the discovered IOCs and distributing them throughout the IronDome to protect our customers with the threat intel gained from BH brings everything full circle.***

Blake Cahen
Senior Threat Hunter, IronNet

Defending the NOC at Black Hat USA

Suspected North Korean SHARPEXT malware detection

During the Black Hat USA conference, we observed repeated callouts from multiple unique hosts to three C2 domains associated with SHARPEXT malware. SHARPEXT has been linked to the North Korean APT Kimsuky, and given North Korea's demonstrated interest in security researchers, the discovery of SHARPEXT on the Black Hat network is significant due to its potential access to hundreds of security employees.[31, 32]

However, the activity surrounding the DNS queries to the SHARPEXT C2 domains was peculiar. The domains successfully resolved to IP addresses, but there was no outbound traffic to the resolved IPs. Successful resolution is unexpected in itself, but often there's some kind of communication to the IPs, so it's unclear why these hosts were simultaneously making successful DNS queries and not performing any subsequent activity.

Read the blog – Defending in a hostile environment: Key findings from the BlackHat NOC

Defending the NOC at Black Hat Asia

Detecting a WordPress Infection Campaign

While supporting the Black Hat Asia NOC in Singapore, IronDefense generated an alert for encrypted communications when a user navigated to an infected WordPress site (96bspinadvisor[.]com). Based on traffic flows, the user was redirected to the URIs print.legendarytable[.]com and local.drakefellow[.]com, which were likely embedded links on the site. Attackers regularly exploit vulnerable plugins to compromise WordPress websites, and infected users can be redirected to sites that are spam laden, fraudulent, or host malware. In this case, we observed additional redirects to multiple suspicious and malicious domains, which were linked to a WordPress infection campaign.[33]

The Power of
Collective Defense

IronNet hunters rated the alert and associated domains as malicious and pushed the related details to all organizations in IronDome. As a result, IronNet hunters quickly identified the same attack being leveraged in at least two other customer environments and worked with them to rapidly respond to the threat.

Read the blog – Protecting the network at the 2022 Black Hat Asia Network Operations Center (NOC)

Defending the NOC at Black Hat Europe

Arechclient2 Info-Stealer

On the first day of the conference, IronNet hunters observed a user connecting to the network with a device infected with the Arechclient2 info-stealer – a .NET remote access trojan (RAT) with numerous functionalities. Within 10 seconds of the user joining the conference wifi, IronDefense detected the malware calling out to the attacker-controlled C2.

We connected the activity to Arechclient2 (aka SectopRAT) based on an encryption string that had been referenced only a few days prior by a Tampa Bay Tech article.[34] 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's system.

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

IRONNET DETECTION SPOTLIGHT

Detecting a MUMMY SPIDER campaign and Emotet infection

Actors: MUMMY SPIDER

Sectors targeted: Logistics

TTPs: T1071: Application Layer Protocol
T1586: Compromise Accounts
T1046: Network Service Discover

Overview

At the start of the Eid Al-Fitr (Islamic holiday) weekend in early May 2022, IronNet's NDR platform IronDefense, in combination with our cybersecurity experts, detected a thread hijacking attack carrying Emotet malware against an organization located in the Asia Pacific. This cyber attack was likely part of a new campaign by the MUMMY SPIDER threat group designed to test a new bypass for Microsoft disabling macros by default for use in future large-scale campaigns.

MUMMY SPIDER (also known as TA542) is a threat group that utilizes various malicious spam (malspam) email campaigns to deploy Emotet malware in combination with other payloads like Cobalt Strike. After initial triage, IronNet analysts were able to categorize this as a thread hijacking attack, where the threat actor injected themselves into an email thread to trick the user into thinking it's legitimate. In this instance, the actors leveraged an existing email chain to ask the target to update a spreadsheet of delivery information, thus providing a legitimate use case for the victim to open the attached file.

Read the blog – Detecting a MUMMY SPIDER campaign and Emotet infection

IronRadar-observed Emotet C2 Trends

IronNet Threat Research also tracks MUMMY SPIDER and Emotet activity via IronRadar. In 2022, some trends we observed include:

- In early 2022, we observed Emotet moving to 64-bit modules and then later in the year change to password-protected zip files.
- In the month of December alone, IronRadar tracked 20+ Emotet botnet servers all being hosted by DigitalOcean and using the same TLS subject fields.
- Cobalt Strike servers used in a MUMMY SPIDER campaign against critical infrastructure in Ukraine leveraged Hostkey as its main hosting provider, Let's Encrypt for its TLS cert, and NiceNIC as its domain registrar.

Digital Ocean as primary **hosting provider**

Global Security as primary **TLS cert provider**

GoDaddy as primary **domain registrar**

Around the same time IronDefense detected the Emotet thread hijacking campaign in late May, IronRadar picked up a Cobalt Strike server with the IP address of 139.60.161[.]52, which was later publicly attributed to MUMMY SPIDER in an OTX pulse published by BinaryDefense on August 19th. According to intelligence sources, this infrastructure was used in cyber attacks against critical infrastructure in Ukraine. In the following months, we saw this Cobalt Strike server go on- and off-line with the most recent occurrence in mid-October. Interestingly, we also found overlap between the domains hosted by this Cobalt Strike server and infrastructure we discovered when hunting for Wizard Spider (aka TrickBot) indicators shared by CISA. Given reports in November 2021 that Emotet rebuilt its botnet using TrickBot's infrastructure, this is significant as it demonstrates continued overlap between the two malware families.[35]

IRONNET DETECTION SPOTLIGHT

China Chopper Discovered in M&A Infrastructure of U.S. Security Software Company

Threat actor: Suspected China-based threat actor

Sectors Targeted: Technology

TTPs: T1087: Account Discovery
T1071: Application Layer Protocol
T1016: System Network Config. Discovery
T1505: Server Software Component
T1046: Network Service Discovery
T1021: Remote Services

Overview

In late August 2022, IronNet Threat Research discovered a malicious cyber intrusion by a sophisticated, likely China-based threat actor in the network of a U.S.-based security software company. Specifically, we observed the threat actor target a compartmentalized segment in the network that was acquired in a company acquisition several years earlier and contained outdated and unpatched systems.

Read the blog – The security risk of M&A: Are Chinese cyber threats lurking in legacy infrastructure?

Infection Chain

The threat actor gained initial access to the compartmentalized network segment via compromised VPN credentials. The authentication attempts included various naming combinations of a company acquired by the targeted organization in 2014, indicating the threat actors were targeting legacy systems in an acquired network segment likely forgotten about by the victim enterprise. In the infection chain, we observed the threat actor attempt to circumvent security controls implemented in the system's version of MS SQL using a unique MS SQL bypass technique that closely overlapped with tactics detailed in a Chinese blog breaking down the steps necessary to infect and escalate privileges on MS SQL servers.

Additionally, we saw the threat actor deploy several different webshells. After the MS SQL bypass technique, the threat actor appeared to upload an aspx webshell, but the attempt was unsuccessful, which is likely why they continued system enumeration. After various port scanning and access attempts, an HTTP POST session succeeded, and the threat actor uploaded a file soon categorized as the shack2 JSP webshell. It was after this we observed the format for the webshell in the sap_door.jsp file change to the China Chopper webshell.

Following the swap from shack2 to China Chopper, we began to observe more targeted enumeration scans and system commands. The last activity observed was outbound activity to remote Chinese IPs, encrypted over 443.

Motivation and Attribution

While this network segment and its devices were outdated, the attacker's continued persistence and level of target knowledge suggest it was targeted for a reason. The threat actor may have chosen this time to be active in preparation for the upcoming Labor Day weekend, where they likely assumed cybersecurity response would be lower. We believe the goal behind this intrusion may have been to exfiltrate data or to find a pivot point to production environments.

The use of China Chopper, as well as the use of Chinese language in the code and the tight alignment to the Chinese blog detailing MS SQL exploitation, indicate a China-based actor is responsible for the attack. The attacker exhibited a high level of sophistication and target knowledge, evidenced through quickly bypassing security controls and conducting all observed activity in under two hours. For these reasons, IronNet Threat Research asserts with low-moderate confidence a sophisticated China-based actor – possibly a state-sponsored Chinese APT – is responsible for the attack.

2022 in the IronDome

Collective Defense aims to correct fundamental problems in the way we share cyber attack intelligence.

Intel-sharing groups aim to enable similar organizations to share intelligence on the malicious activity targeting their networks. Though this is a positive step in cybersecurity collaboration, these groups often fall short of their desired intent. In many cases, companies struggle deciding when and what information to share with others and indicators are only shared after an incident response (IR) is complete. This slow and manual process leads to an inefficient collaboration system where the intelligence shared is often no longer actionable by the time it reaches others.

As a Collective Defense platform, IronDome bypasses the latency and bureaucracy faced by typical intel-sharing groups by anonymously sharing real-time attack intelligence to participant organizations. Rather than sharing specific IOCs and intelligence on an ad hoc basis, **IronDome** automatically shares all malicious and suspicious activity in organizations' networks and generates alerts when similar activity is detected in another environment. In this way, IronDome enables analysts at different organizations to instantaneously collaborate on shared threats and equips them with the proactive intelligence they need to stop intrusions in their tracks.

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.

What are correlations and why do they matter?

IronDome brings together events and alerts from multiple IronDefense deployments into an anonymized central data store, enabling detections of similar behavior (or "correlations") to be identified. These correlations can be made on indicators or on similarities across a wide range of event context features, known as behavioral correlations. IronDome's unique cross-sector visibility and ability to correlate seemingly unrelated instances across networks is critical for identifying sophisticated attackers who use various tools and tactics to evade detection.

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. This brings attention to the alert as particularly suspicious and allows analysts to see how other participants rated the alert and what their comments were. It works as a force multiplier that enables SOCs to work together.

17,367
Total alerts correlated

Data correlated from the IronDome

15,455
Alerts correlated between 3+ participants

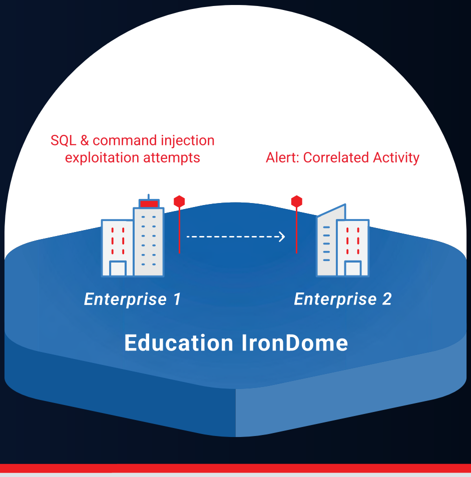
2022 in the IronDome

Collective Defense Spotlights

Targeted Attacks on EU Colleges

During a Proof-of-Value (POV) with multiple EU universities and colleges, IronDefense detected suspected data exposure of log-on activity to an enterprise login server. After reviewing the alert, IronNet hunters identified this activity as external SQL and command injection exploitation attempts against the college's public infrastructure and pushed the intelligence to both the education and EU IronDomes.

Upon reviewing alerts in a second college's environment, the same activity was identified. Both attacks involved an external host that had not previously been seen performing vulnerability or exploitation attacks. We determined this to be a targeted attack against multiple colleges, and the Irondome correlation enabled reduced triage time.

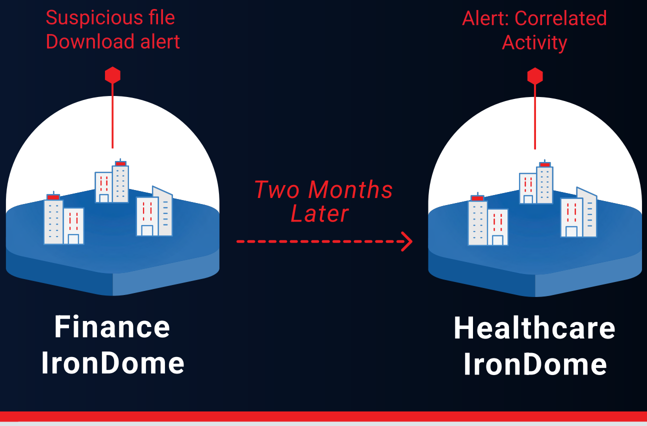

SQL & command injection exploitation attempts
Alert: Correlated Activity
Enterprise 1
Enterprise 2
Education IronDome

Impact

Discovery of a targeted attack against multiple European colleges through correlated alert activity in the Education and EU IronDomes.

Malicious File Download from a Fraudulent Zoom installer

In June 2022, IronDefense generated a Suspicious File Download alert in the environment of a Finance IronDome participant, firing on a download of a malicious file from a domain masquerading as a legitimate Zoom installer. This activity was escalated to the participant's Security Operations Center (SOC), and the intelligence was automatically pushed to organizations in IronDome. Approximately two months later, this same activity was identified in a Healthcare IronDome participant. Because this correlation was highlighted to be severe, the time to triage was greatly reduced as it enabled the analyst to quickly prioritize the alert.



Impact

Detection of malicious file download from a fraudulent Zoom installer in Finance IronDome led to the quick identification of the same activity in the network of a Healthcare organization two months later.

Collective Defense Spotlights

A High-Risk Chrome Extension at Black Hat Europe

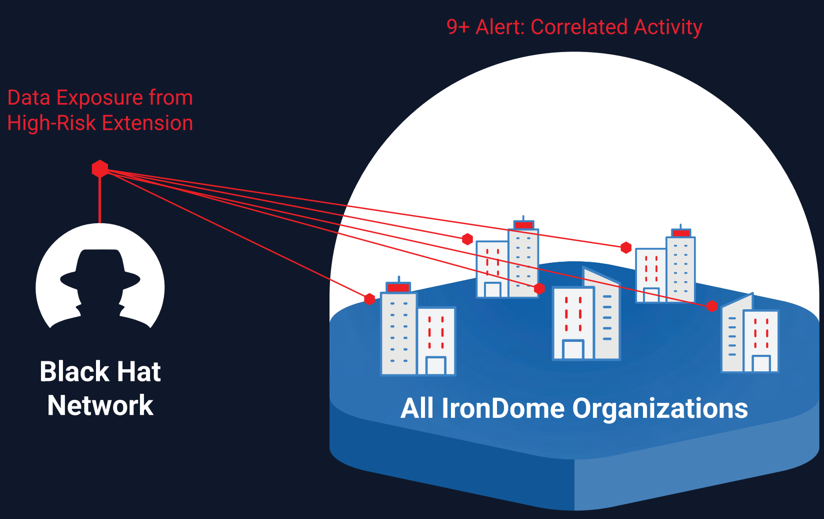
While supporting the Black Hat EU NOC, IronDefense generated an alert related to data exposure from numerous devices present at the conference. After thorough review, IronNet hunters identified a previously installed Chrome extension called FBDown (Facebook Video Downloader/Video Downloader Pro) on a user's computer that was exfiltrating all of their browser activity and history to an extension-owned server.

Though there's no evidence FBDown is malicious in itself, it does pose a significant security risk as a threat actor could target the extension to access user information or someone could try to purchase the extension from the original developer knowing the data it contains.

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

Impact

Malicious alert detected while defending the NOC at Black Hat Europe 2022 led to the identification of the same activity across at least nine different enterprises in the U.S., Asia, and the Middle East.


9+ Alert: Correlated Activity
Data Exposure from High-Risk Extension
Black Hat Network
All IronDome Organizations

IronPredator

New Proactive Detection Engineering Platform in IronDome

Overview

When discovering threats, there are many ways to detect malicious activity via network traffic. In the past, we have added several capabilities to IronDome to help us "connect-the-dots" when discovering a malicious threat in multiple sectors. Our latest addition to these capabilities is IronPredator - a detection engineering platform with a SIGMA-like capability that allows hunters to develop rules to detect specific malware traffic and hunt on broader threat actor TTPs that may not appear as immediately malicious. Consider Microsoft BITS traffic to an external service that wasn't Microsoft, or a download of a file with just 3 characters.

Though it wouldn't be efficient to have customer-facing alerts on these attributes, we can hunt on these broad queries to discover threats or on granular characteristics to uncover specific malware. Furthermore, IronNet's proactive threat intelligence feed IronRadar helps add context to the hunt and remove false positives so that hunters are only alerted when something truly seems off.

How Does it Work?

1. Analyst reads a report or thinks of a behavior that they want to capture
2. Analyst begins crafting rule to capture the intended traffic
3. Rule is run against a live set of data and fine tuned
4. Depending on the scope, rule is either set to alerting or informational
5. Hits are analyzed 24/7, in near real time, and sent to customers post triage

This new global capability is an incredible addition to our IronDome toolset. We can use these rules to observe suspicious behavior in customer networks and tailor specific rules for certain environments. The indicators from these rules are immediately fed into our internal intelligence lifecycle that kicks off additional analysis for our Intelligence Analysts.

Spectrum of Rules

IronNet analysts commonly deploy both broad and specific Hunt Rules. We can write a rule looking for a vague technique that would be beneficial to hunt on but not necessarily suitable to create an alert, or we can write a rule searching for a very specific behavior.

MOST BROAD **SPECIFIC**

Suspicious 3 character limit

- Designed to catch the download of 3 character EXE files, which is something commonly used by malware frameworks like Mozi

BITSadmin user agent to external IP address

- Designed to catch threat actors abusing Microsoft BITS to reach out to an external IP, a technique seen frequently by threat actors to avoid detection

Raccoon Stealer

- Designed to detect all forms of Raccoon Stealer C2s by searching for specific characteristics and path strings that indicate in the Download, GET request, and POST (exfil).

59
rules created in 3 months

21
findings in 3 months

2022 Must-Read Articles

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 2022 that stood out as particularly interesting and noteworthy.

Tracking Cobalt Strike servers used in cyberattacks on Ukraine

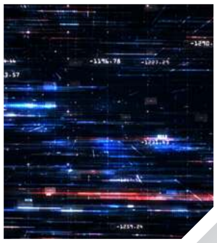
This article provides an in-depth analysis of IronRadar's longitudinal dataset of C2 servers hosted on the IP addresses and domains referenced in a CERT-UA report (#4490).

Read the Article | May 08 | Threat Research

Detecting a MUMMY SPIDER campaign and Emotet infection

IronNet Threat Research outlines its detection of MUMMY SPIDER using a new bypass to deploy Emotet malware against an Asian Pacific organization at the start of Eid Al-Fitr (Islamic holiday) in early May 2022.

Read the Article | May 11 | Threat Research



The security risk of M&A: Are Chinese cyber threats lurking in legacy infrastructure?

This article discusses IronNet's detection of a sophisticated, China-based actor targeting the acquired infrastructure of a U.S. software company from an M&A to deploy the China Chopper webshell.

Read the Article | Oct 18 | Threat Research

Robin Banks still might be robbing your bank

This two-part blog series discusses IronNet's discovery and analysis of a new phishing-as-a-service (PhaaS) platform called Robin Banks selling ready-made phishing kits to cybercriminals.

Read the Article (Part 1) | Read the Article (Part 2) | Threat Research

Defending in a hostile environment: Key findings from the Black Hat NOC

IronNet Hunters detail notable observations from defending the Black Hat USA network, including North Korean-attributed SHARPEXT malware, Shlayer malware, and NetSupport RAT malware.

Read the Article | Aug 24 | Threat Research

Key Findings from Defending the NOC at Black Hat Europe 2022

IronNet Hunters break down the findings from defending the NOC at Black Hat Europe, including several active malware infections like the Arechclient2 info-stealer and an insecure Chrome extension with suspicious exfiltration activity.

Read the Article | Nov 03 | Threat Research

Predictions for 2023

Raj Sivasankar
Vice President of Product Management
IronNet

"The cyber insurance industry will prompt all to rethink the security perimeter from a cyber risk perspective."

▶ Rethinking the security perimeter is going to become even more fundamental from a risk perspective for CIOs and CISOs, especially because cyber insurance is becoming about ten times more expensive in 2023 (as well as the **Lloyd's of London announcement** that nation-state attacks will not be covered starting in March 2023). There will be great concern and fear of the cyber insurance fine print and an organization's ability to afford it.

Anthony Grenga
Vice President of Cyber Operations
IronNet

"2023 will be the year of Identity Access Management (IAM)."

▶ Keeping up with who has access to your network will be crucial to prevent insider threats and data breaches, particularly as the tech industry continues to lay off hundreds of thousands of people. Organizations will have to recognize that some former employees may still have user access to some systems, so scrutinizing what IAM means to an organization will be essential as companies contend with off-boarding layoffs — while at the same time moving to SaaS applications.

Peter Rydzynski
Principal Threat Analyst
IronNet

"Expect to see a rise in canaries."

▶ Given that we continue to observe sophisticated attackers such as China, Iran, and Russia moving rapidly with little care for the traces left on the network, I think there will be an increase in the use of canaries as an opportunity to get ahead of these really rapid threats. Furthermore, comparatively speaking, canaries provide a very cost-effective solution for small organizations that may not be able to staff a full operations team to monitor the network.

Joey Fitzpatrick
Threat Analysis Team Lead
IronNet

"As-a-service type offerings for threat actors will gain more popularity (PhaaS, MaaS, etc.)."

▶ From Robin Banks (PhaaS) to the latest DuckLogs malware (MaaS), cybercriminals are continuing to become more niche in their development. Gone are the days of having to develop end-to-end attack chains from initial access to full compromise for low- to mid-tier actors. Just as modern society has progressed through specialization of the labor force, threat actors too will become increasingly more successful via specialization. The division of labor enables higher quality malware used by a range of actors and lowers the price-to-play in regard to entering the world of cybercrime.

Morgan Demboski
Threat Intelligence Analyst
IronNet

"We are likely to see more abuse of M&As."

▶ In 2022, We saw a lot of cases where threat actors were specifically looking for companies going through the merger and acquisition (M&A) process because they knew that in all of that craziness, they would have a better chance of slipping by and gaining access to companies' networks undetected. IronNet saw this M&A abuse in the case of a **Chinese threat actor infiltrating a software company** by targeting a network segment integrated from a prior acquisition. There's a lot that can be overlooked when integrating one company's technical infrastructure into another, and I think it's very likely that threat actors will increasingly exploit M&As to compromise organizations for espionage or ransomware in 2023.

CONCLUSION

The cyber activity and strategic objectives of nation-state threat actors continues to show the interrelationship between the geopolitical and cyber threat landscapes, highlighting the importance of tracking government actions and international relations to assess their potential implications in the cyber domain. This is especially important as the Ukraine-Russia War continues into its second year, which IronNet closely monitors to assess the risk of destructive, disruptive, and cyber espionage attacks against Ukraine and its allies.

In 2022, the barrier-to-entry to cybercrime continued to lower as "as-a-service" offerings made cyber attack tools available to actors with minimal hacking experience. IronNet's discovery of the **Robin Banks** phishing-as-a-service platform in July 2022 found the platform's phishing kits to be heavily reliant on open-source code and off-the-shelf tools, exemplifying not only the growing accessibility of cybercriminal attacks, but also the growing capability of low-sophistication actors to create platforms to sell as-a-service offerings for additional profit. Meanwhile, improved cyber defenses continually motivate threat actors to adopt more evasive tactics – from testing bypasses for Microsoft disabling macros by default to targeting assets that may have been overlooked in a M&A.

Looking forward, we remain vigilant in tracking threat actors' efforts to shield their infrastructure from being detected. As C2 detection capabilities improve, threat actors will be pressured to find more ways to stay undetected, which could include using a legitimate external web service such as DropBox or Telegram as a mechanism for C2 or setting up a redirector or proxy for basic operational security.

Our mission at IronNet is to deliver the power of collective cybersecurity to defend companies, sectors, and nations. IronNet Threat Research will continue to share our metrics and analysis to assist organizations in their cyber defense efforts, contribute proactive intelligence to the cybersecurity community, and improve our collective security.

ENDNOTES

1 Guerrero-Saade. (2022). AcidRain | A Modern Wiper Rains Down on Europe. SentinelLabs. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

2 CERT-UA. (2022). Cyber attack of the Sandworm group (UAC-0082) on the energy facilities of Ukraine using malicious programs INDUSTRO ER2 and CADDYWIPER (CERT-UA#4435). CERT-UA. https://cert.gov.ua/article/39518.

3 Harbison & Renals. (2022). Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive. Unit42. https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

4 MSTIC, DART, Microsoft 365 Defender Research Team. (2022). MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone. Mi rosoft. https://www.microsoft.com/en-us/security/blog/2022/08/24/magicweb-nobeliums-post-compromise-trick-to-authenticate-as-anyone/

5 Cyber National Mission Force Public Affairs. (2022). Before the Invasion: Hunt Forward Operations in Ukraine. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

6 Brewster. (2022). Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them. Forbes. https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/?sh=774f85885a4c

7 Kaspersky ICS CERT. (2022). Targeted attack on industrial enterprises and public institutions. Kaspersky. https://ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/

8 Tucker. (2022). China accused of hacking Ukraine days before Russian invasion. The London Times. https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

9 Aoyi Wisdom Technology Powered by CyCraft. (2022). In-depth analysis of Operation Cache Panda organizational supply chain attacks targe ing Taiwan's financial industry. Medium. https://medium.com/cycraft/supply-chain-attack-targeting-taiwan-financial-sector-bae2f0962934

10 Collier. (2022). Taiwanese websites hit with DDoS attacks as Pelosi begins visit. CBS News. https://www.nbcnews.com/tech/security/taiwanese-websites-hit-ddos-attacks-pelosi-begins-visit-rcna41144

11 CISA. Alert (AA22-158A): People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

12 Lakshmanan. (2022). Chinese Hackers Target VMware Horizon Servers with Log4Shell to Deploy Rootkit. The Hacker News. https://thehackernews.com/2022/04/chinese-hackers-target-vmware-horizon.html

13 Netblocks. (2022). Internet disrupted in Iran amid protests over death of Mahsa Amini. Netblocks. https://netblocks.org/reports/internet-disrupted-in-iran-amid-protests-over-death-of-mahsa-amini-X8qVEwAD

14 Stefanko. (2022). Domestic Kitten campaign spying on Iranian citizens with new FurBall malware. ESET. https://www.welivesecurity.com/2022/10/20/domestic-kitten-campaign-spying-iranian-citizens-furball-malware/

15 Bracken. (2022). Cyberattacks Against Israeli Government Sites: 'Largest in the Country's History'. ThreatPost. https://threatpost.com/cyberattacks-israeli-government-sites-largest/178927/

16 AlJazeera. (2022). Albania blames Iran for second cyberattack since July. AlJazeera. https://www.aljazeera.com/news/2022/9/10/albania-blames-iran-for-second-cyberattack-since-july

17 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

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

19 Shin. (2022). South Korea scrambles jets as North Korea sends drones over border. Reuters. https://www.reuters.com/world/asia-pacifisouth-korea-briefly-suspends-flight-departures-upon-military-request-official-2022-12-26/

20 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

21 Ronin Network. (2022). Community Alert: Ronin Validators Compromised. Ronin Blackchain. https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r

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

23 Pradhan. (2022) LolZarus: Lazarus Group Incorporating Lolbins into Campaigns. Qualys. https://blog.qualys.com/vulnerabilities-threat-research/2022/02/08/lolzarus-lazarus-group-incorporating-lolbins-into-campaigns

24 Threat Hunter Team. (2022). Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets. Symantec. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage

25 CISA. (2022). Alert (AA22-152A): Karakurt Data Extortion Group. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa22-152a

26 Hiroaki & Lee. (2022). Hack the Real Box: APT41's New Subgroup Earth Longzhi. Trend Micro https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html

27 CERT-UA. (2022). Cyber attack on state organizations of Ukraine using the "Azovstal" theme and the Cobalt Strike Beacon malware (CERT UA#4490). https://cert.gov.ua/article/39708

28 Hawley, et al. (2023). Turla: A Galaxy of Opportunity. Mandiant. https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

29 BishopFox. (2023). sliver. GitHub. https://github.com/BishopFox/sliver

30 U.K. NCSC. (2021). Advisory: Further TTPs associated with SVR cyber actors. U.K. GCHQ. https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf

31 Rascagneres, Lancaster, Volexity Threat Research. (2022). SharpTongue Deploys Clever Mail-Stealing Browser Extension "SHARPEXT." Volex ty. https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/

32 Weidemann. (2021). New campaign targeting security researchers. Google Threat Analysis Group (TAG). https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

33 Numen Cyber Labs. (2022). Thousands of WordPress sites were hacked to inject malicious JavaScript — Full detail. Medium. https://medium.com/numen-cyber-labs/thousands-of-wordpress-sites-were-hacked-to-inject-malicious-javascript-full-detail-32e478f08b21

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

35 Abrams. (2021). Emotet malware is back and rebuilding its botnet via TrickBot. Bleeping Computer. https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

Take back the power from cyber attackers

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

Request a Demo

to see Collective Defense in action

Collective attacks need **Collective Defense**

IronNet