



Quarterly Threat Intelligence Report

Q3

July - September

Threat Intelligence Report

Insights into Q3 cyber threat trends drawn from IronNet ecosystem detections and intelligence assessments by IronNet analysts from July 1, 2022 to September 30, 2022.

Executive Summary	3
Q3 Threat Landscape Overview	3
IronRadar	4
Detection Breakdown	4
C2 Servers: By the Numbers	5
Top countries hosting unique C2s	5
Top domain registrars of C2 domains	5
Top cloud providers hosting unique C2s	6
TLS server x509 certificate analysis	6
Case Studies	7
Robin Banks Phishing-as-a-Service Platform	7
BlackCat Ransomware	8
China Chopper Detection	9
Q3 in the IronDome	10
What is IronDome?	10
What are correlations and why do they matter?	10
How Does it Work?	10
Significant Community Findings	11
IronNet Nation-State Analysis	12
Russia Attack Trends	13
China Attack Trends	14
Iran Attack Trends	15
North Korea Attack Trends	16
Featured Q3 IronNet Threat Research	17
Q4 Threat Watch	18
Conclusion	19
Endnotes	20

EXECUTIVE SUMMARY

The IronNet Threat Research team is proud to present its first Quarterly Threat Intelligence Report.

IronNet's Q3 2022 report includes a comprehensive assessment of the cyber threat landscape from **July 1, 2022 to September 30, 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 granted from our new proactive threat intelligence feed **IronRadar**, as well as with intelligence from our partners, to help us in our investigations.

Q3 THREAT LANDSCAPE OVERVIEW

In Q3, the cyber threat landscape was characterized by persistent hacktivist threats from the Ukraine-Russia War, targeted nation-state attacks for commercial and political advantage, and low barrier-to-entry cybercrime.

During that time, IronNet Threat Research observed:

- » A potential Chinese threat actor in the network of a U.S. software company, specifically targeting legacy systems in an acquired network segment from a company acquisition several years prior.
- » A continued rise in low-cost phishing kits on the market to generate personal profit and to supplement initial access broker (IAB) activity.
- » A heavy reliance of cybercriminal platforms on open-source code and off-the-shelf tools, exemplifying the growing accessibility of not only cybercriminal attacks but the capability to create platforms and to sell as-a-service offerings for additional profit.

IronRadar

ADVERSARY INFRASTRUCTURE TRACKING

IronNet tracks the creation of new malicious infrastructure for numerous post-exploitation frameworks through a unique fingerprinting process developed by our analysts to detect C2 servers as they are being stood up and before they are used in an attack.

Between July and September, IronNet identified nearly 10,000 malicious indicators across more than 10 C2 frameworks. According to our detections, Cobalt Strike continued to top the list of most common C2 frameworks used by adversaries, followed by Metasploit and Dark Comet.

In open-source reporting, we observed a growing trend in threat actors swapping out the well-known and more noticeable Cobalt Strike for lesser known red team tools that won't draw as much attention. We have also observed adversaries using multiple C2 frameworks in a singular attack chain to achieve their objectives¹. These trends exhibit the growing importance of detection coverage across a range of frameworks in addition to Cobalt Strike, as we predict the malicious use of other frameworks to increase over the next year.

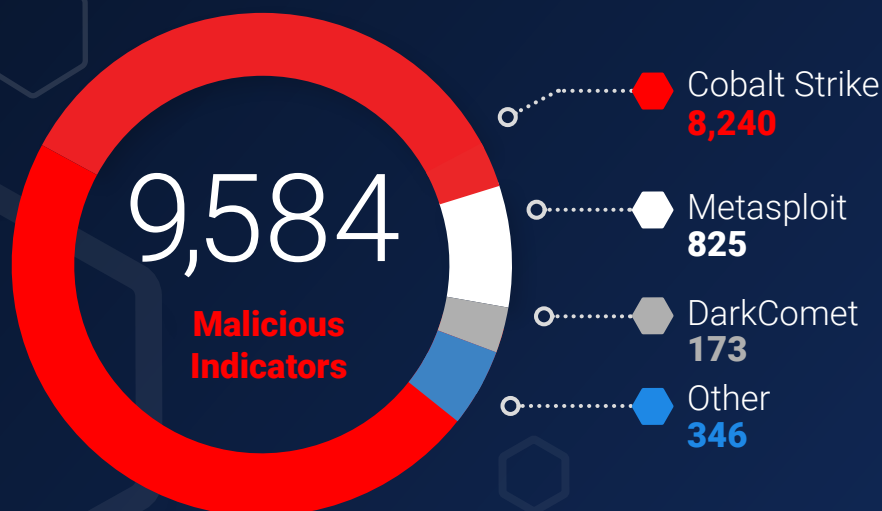
DEBUTING



In Q3, IronNet debuted its new threat intelligence solution IronRadar – an automated threat intelligence feed that tracks adversary infrastructure via proactive threat intelligence (PTI). This feed is delivered via a REST API and integrates easily with cyber security products such as Firewalls, SIEMs, SOARs, EDRs, and other tools that accept third party feeds.

[Learn More](#)

DETECTION BREAKDOWN

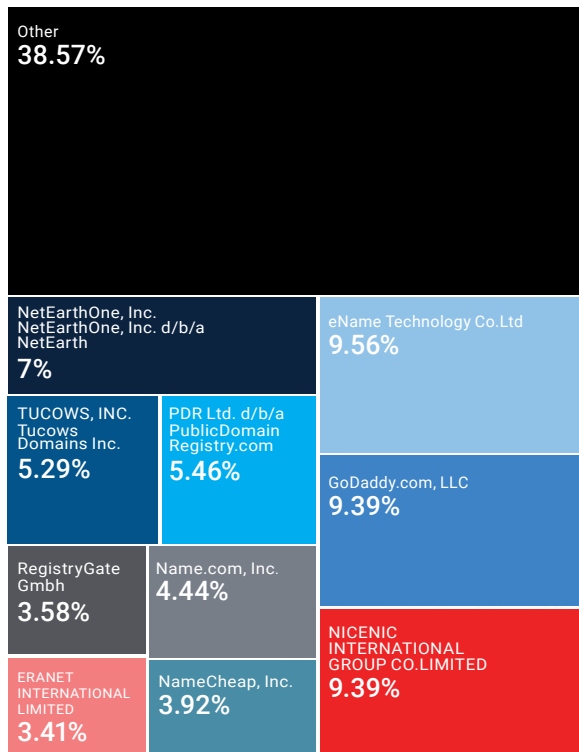
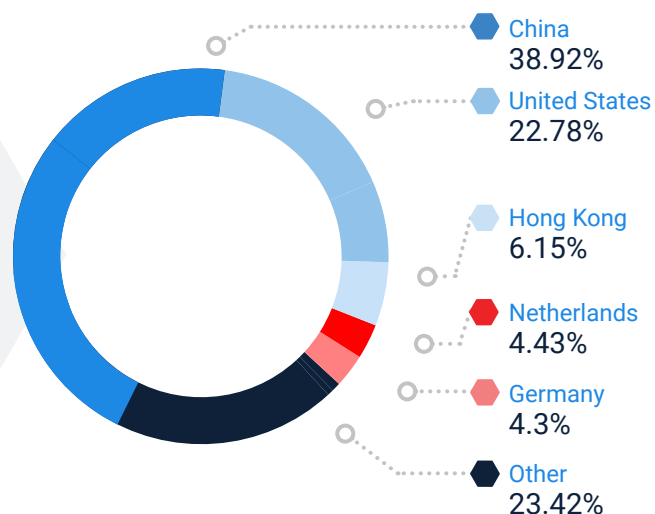


C2 Servers:

By the Numbers

Top countries hosting unique C2s

In Q3, almost 40% of all unique C2 servers detected by IronNet were hosted in China, almost doubling the number of C2 servers hosted by the next highest country: the United States. After the U.S., which hosted roughly 23% of detected servers, there was a large drop-off as the remaining servers were distributed across a variety of different countries. Hong Kong (6.1%), the Netherlands (4.4%), and Germany (4.3%), hosted the next largest concentrations of detected C2 servers, largely mimicking the same distribution as our detections in Q2.

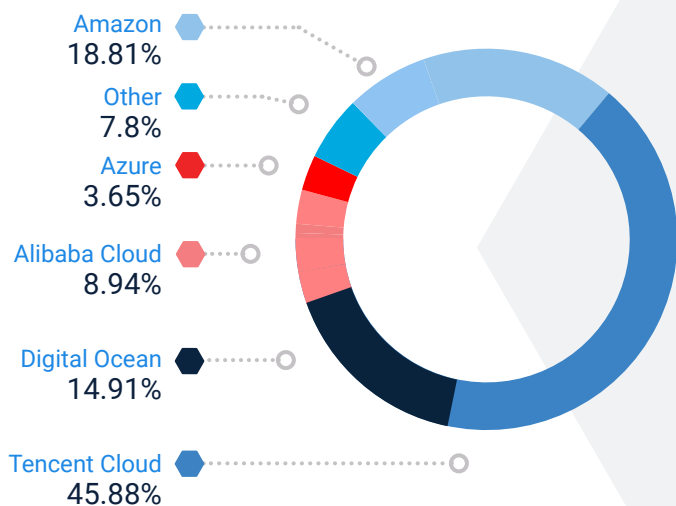


Top domain registrars of C2 domains

Domain registrars remained diverse in Q3. Continuing with the existing trend, threat actors are sticking to registrars that value privacy, accept cryptocurrencies, and have a protracted review process of abuse reports.

Notably, in June of 2021, Namecheap significantly revamped its abuse reporting process after public outcry from security researchers and analysts. Since then, we have observed a steady decrease in usage of this registrar by threat actors².

Furthermore, threat actors are continuing to acquire domains from resellers that have a prior history as a benign site (e.g. domain categorization) to further legitimize the appearance of their infrastructure. Analysts and researchers are advised to remain vigilant when analyzing domain registration info. Comparing whois created and updated dates, along with historical whois data, can provide valuable insights into possible ownership changes.



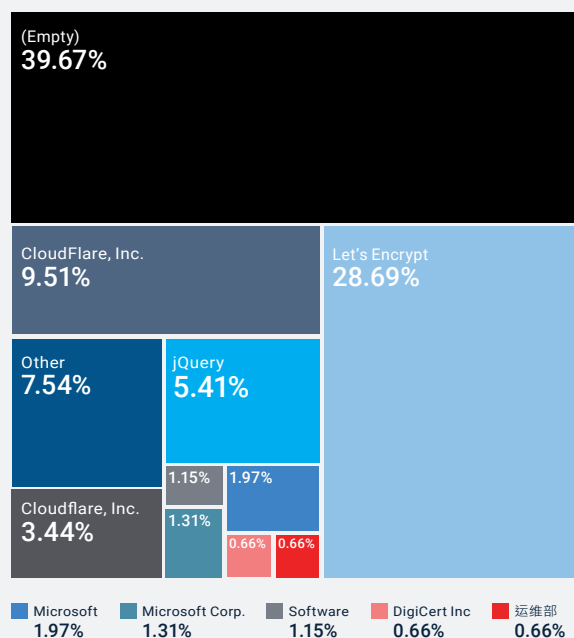
Top cloud providers hosting unique C2s

Tencent Cloud, operating out of China, is the top cloud provider for hosting unique C2 servers observed by IronNet, hosting close to half (45.9%) of all detected C2 servers. The second top cloud provider was Amazon (18.8%), followed by DigitalOcean (14.9%). Notably, the number of unique IronNet-detected C2 servers hosted by Amazon increased nearly 68% compared to Q2 (April-June), while the number of unique IronNet-detected C2 servers hosted by Tencent Cloud decreased slightly by 2.6%.

TLS server x509 certificate analysis

In Q3, IronNet began parsing TLS server x509 certificates that were acquired during analysis. Preliminary analysis indicates that threat actors are generating self-signed certificates in 40% of cases. However, when they do choose to use valid TLS certificates, they unsurprisingly favor free TLS/SSL certificate providers like Let's Encrypt and CloudFlare.

Furthermore, threat actors continue to abuse legitimate cloud services in their architectural deployments. These cloud services tend to provide managed certificates with no customer-attributable features outside of the subject common name and alternative names. Observed abused services include, but are not limited to, AWS Api Gateway, ngrok, Azure Web Apps, GCP Cloud Storage and CloudFlare Workers. IronNet recommends that SOCs keep a working list of known corporate cloud services to aid analysts when inspecting network communications to these destinations.



IRONNET DETECTION SPOTLIGHT

Robin Banks Phishing as-a-Service Platform



Actors: Multiple



Sectors targeted:

Multiple, with focus on financial



TTPs: T1566: Phishing

Overview

During Q3, IronNet Threat Research published a two-part blog series on a newly discovered phishing-as-a-service (PhaaS) platform called Robin Banks that sells ready-made phishing kits to cybercriminals aiming to gain access to the financial information of the customers of well-known banks and online services.

In the first blog, IronNet researchers provided details about the Robin Banks platform, the phishing kits it offers, and the use of the platform by threat actors. In addition to discussing the kit, we also detailed IronNet's discovery of a large-scale campaign using the Robin Banks platform to target victims via SMS and email, with the goal of accessing credentials and financial information pertaining to Citibank, as well as Microsoft account credentials.



Read the articles – [Part 1](#) & [Part 2](#)

A deeper dive into the Robin Banks kit

Following our initial discovery and reporting on Robin Banks in late July, we conducted a deeper dive into the infrastructure behind the kit and the platform itself. Through our analysis, we determined that the Robin Banks kit platform serves as a prime example of the growing trend of using different web tools and open-source code to host cybercriminal platforms.

For example, through deeper analysis of Robin Banks' phishing kit infrastructure, we learned Robin Banks uses an open-source obfuscation script called PHP obfuscator to obfuscate its code³. Once we deobfuscated this code, we realized much of the obfuscated base code within the core constructs of the kit relate to a third party tool: Adspect⁴. PhaaS providers like Robin Banks often leverage platforms such as Adspect to ensure targeted victims are redirected to malicious sites, while scanners and unwanted traffic are redirected to benign websites.

However, Robin Bank's use of open-source code does not end there. After IronNet published its first blog on Robin Banks in July, the platform admins debuted a new feature advertising its "own methodology" to bypass two-factor authentication (2FA) via the stealing of login session cookies. However, the binary files reveal Robin Banks admins may have taken their "own methodology" from the well-known pentesting tool evilginx2 that has a pre-built framework for phishing login credentials and authentication tokens (cookies)⁵.

Robin Banks' heavy reliance on open-source code and off-the-shelf tooling showcases just how low the barrier to entry is to not only conducting phishing attacks, but also to creating a PhaaS platform for others to use. The use of different web tools to host cybercriminal platforms is growing, thus posing concerns as cybercrime becomes more accessible and a low-effort option to drawing in a quick profit.

BlackCat Ransomware

**Actors:** BlackCat (ALPHV) Ransomware**Sectors targeted:** Education**TTPs:** T1046: Network Scanning Service
T1219: Remote Access Software
T1071: Application Layer Protocol

Overview

On June 18th, an IronNet customer in the education sector was targeted in a BlackCat ransomware attack. In this attack, the threat actors gained access to the victim environment using compromised credentials – a very common mode of initial access. The first indications of malicious activity were observed surrounding the C2 domain `dnsresolverconf[.]com`, in which the initial C2 activity did exhibit itself as very bursty beaconing at 1 second intervals.

After establishing a foothold through an independent C2, the threat actors were detected conducting second-stage activity. BlackCat was observed downloading and executing AnyDesk to the network, which is a legitimate remote desktop application. However, even though AnyDesk itself was legitimate, the victim did not have AnyDesk already present in their network, making the activity distinctly anomalous and suspicious. Additionally, the AnyDesk client made internet requests over TLS in a way that was novel and we were able to detect its unique TLS fingerprint.

C2 / Attacker IOCs	Description
dnsresolverconf[.]com	Believed to be adversary C2
107.175.123.236	IP for dnsresolverconf[.]com
172.245.6.115	AnyDesk C2. Interestingly, this IP is hosted on the same provider as the dnsresolverconf[.]com
213.152.162.84	Initiated RDP to a compromised host
80.66.76.145	Initiated RDP to a compromised host

Potential Adversary Infrastructure

Tactics	Technique	IronDefense Analytics	Analyst Comments
Discovery	T1046: Network Service Scanning	External Port Scanning Internal Port Scanning Knowledge Based Detection	Spike in scanning before compromise
Command & Control	T1219: Remote Access Scanning	Suspicious File Download TLS Invalid Cert Chain	Attacker downloaded and used AnyDesk
Command & Control	T1071: Application Layer Protocol	Consistent Beaconing TLS TLS Invalid Cert Chain Novel JA3	Persistent C2 over TLS Unknown framework used with novel JA3/JA3S

Observed MITRE ATT&CK TTPs & IronNet

IronDefense also detected RDP sessions inbound from the internet, and though we did not detect a high volume of data being exfiltrated from the network, we did see some use of megasync and believe there may have been some exfiltration over that. However, we do not believe the threat actors were able to extract victim information as we did not see any outbound flows large enough to be exfiltration.

BlackCat (aka ALPHV) was first observed in November 2021, when it garnered attention for being one of the first ransomware families written in the programming language Rust. Able to encrypt both Windows and Linux devices, and even VMWare instances, BlackCat operates under the ransomware-as-a-service (RaaS) model, and its deployments have varying entry vectors depending on the affiliate conducting the attack.

China Chopper Detection



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 software company. Specifically, the activity was observed in a compartmentalized segment of the company's network that contained legacy infrastructure from a company acquisition several years prior.



Read the article – 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. 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. Following 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 & Attribution

While this network segment and its devices are 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 may have assumed cybersecurity response to be lower. The goal behind this intrusion may have been to exfiltrate data to sell 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. Given these reasons, IronNet Threat Research asserts with moderate confidence a sophisticated China-based actor – possibly a state-sponsored Chinese APT – is responsible for the attack.

Q3 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 trends of similar behavior (or "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 and Collective Defense capabilities highlight the most frequent behaviors seen across multiple organizations, enabling us to track trends over time. This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses.

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.

7,586

Total alerts
correlated

6,773

Correlated between
more than 2 participants

*Data correlated
from the IronDome*

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 Q3 that were deemed significant by our analysts due to the affiliation, severity, and/or frequency of the indicator. We recommend blocking these domains and investigating further traffic.

Domain/IP	Rating	Comment
pcapp[.]store	MALICIOUS	Download of Zoom-Setup-PCAppStore.exe from pcapp[.]store - This file creates a Scheduled Task on the host upon execution for persistence. We recommend looking for HTTP GET requests for pcapp[.]store/cpg_fa.php with an Internet Explorer user-agent, which will indicate successful execution.
user-shield-check[.]com	MALICIOUS	Domain has been observed hosting various phishing campaigns that change based upon the HTTP Path requested. We recommend blocking this domain and investigating the parent domain, which may be making calls to this domain via embedded pop-ups.
cmovies[.]vc	MALICIOUS	Domain was created April 11, 2022 and streams copyrighted material. Suspicious/Malicious pop-ups were seen on various pages on this domain. OSINT sources have flagged this domain as malicious as well.
pgusgyzdfpj[.]ru	MALICIOUS	Domain was created Jan 19th, 2022 and appears to be an ad-redirect domain that redirects to suspicious websites. Multiple Russian media sites are using scripts from this domain; one of the scripts can be found at hxxps://pgusgyzdfpj[.]ru/pixels/b286ae57[.]js.
6bf0923c-2447-4d17-8428-51012c86466d.htmlcomponentservice[.]com	SUSPICIOUS	Domain returns 404. OSINT investigation shows other similar subdomains have been flagged for a fake paypal login screen. It has also been reported subdomains of htmlcomponentservice[.]com have been flagged for phishing scams and potential malicious activity.
duplicatepowerquay[.]com	SUSPICIOUS	Domain was created August 6th, 2022 and is an ad-redirect domain related to effectivedisplaycontent[.]com that contains multiple communicating javascript adware.
cleaner-update.cmdz35pvhcde[.]top	SUSPICIOUS	Domain appears to be a stage one phishing domain related to mobile phishing scams. The domain hosts a pop-up suggesting to the user that their software is out-of-date and they need to download an update. Potential stage three download domains may end with "phkr."
initiatepreciseoverlytheproduct[.]vip	SUSPICIOUS	Domain currently returns a 403 error code. OSINT investigation found it is part of an ad-redirect chain that leads to the download page for a suspicious chrome extension. This extension has been reported to push browser ads and to install other unwanted programs, as well as a browser hijacker.
kzeaa[.]com	SUSPICIOUS	Domain was created May 21st, 2022 and currently redirects to other DGA domains with a TLD of [.]top. The domain contains two malicious communicating files that have been reported as trojans and ransomware.
havanese[.]top	SUSPICIOUS	Domain was created June 29, 2022 and is related to spam push notifications. One file referring the domain is a potentially malicious javascript file and has been found as a source on suspicious download sites.



Q3 IronNet Nation-State Analysis



RUSSIA

5 CAMPAIGNS
REPORTED

CYBER STRATEGIC OBJECTIVES

-  Targeting NATO countries in cyber espionage operations to collect information from strategic sectors such as diplomatic missions, government agencies, NGOs, and think tanks.
-  Supporting non-state groups in carrying out disruptive attacks against the websites of various Western and Ukrainian organizations.

Ukraine-Russia War cyber activity

There are three main cyber actors in the Ukraine-Russia War: APTs, cybercriminals, and hacktivists. In the beginning months of the war, Russian state-sponsored APTs were relatively active in targeting Ukrainian and allied entities, but have been less active as of late as cybercriminal and hacktivist groups have become responsible for the majority of malicious cyber activity related to the war.

In Q3, this came to be especially evident as groups like the pro-Russian hacktivist group KillNet came to prominence launching DDoS attacks against high-profile entities supporting Ukraine, such as the Lithuanian government, LockHeed Martin, Polish law enforcement and healthcare, U.S. government targets, and more^{6, 7, 8}.

Using hacktivist groups as a front?

Historically, the Russian government has been known to maintain a certain level of plausible deniability in its operations to distance itself from retaliation, which has led it to partner with non-state threat groups to conduct cyber operations in support of its objectives. These efforts have been corroborated by sources linking the Russian government to Russia-based ransomware groups, and even more importantly, by recent research identifying at least three pro-Russian hacktivist groups that are believed to be a front for or working in coordination with the Russian government since the invasion of Ukraine in February^{9, 10}.

To avoid the retaliation that could result from openly targeting critical infrastructure outside of Ukraine, such as in a NATO country, it is very likely the Russian government would not hesitate to order a non-state actor to target NATO critical infrastructure through the facade of a ransomware attack or hacktivist operation. Instead, it would use its APT resources to conduct cyber espionage operations that tend to stay under the radar and generate less noise.

As the war continues, organizations need to be wary of:

1. Possible spillover or direct targeting by these threat actors looking to support their own personal interests or the wider interest of the Kremlin, and
2. Cyber espionage operations by Russian state-sponsored APTs looking to stay undetected and siphon valuable information from critical sources.




CHINA



CYBER STRATEGIC OBJECTIVES

13

CAMPAIGNS
REPORTED

-  Maintaining control over “dissident” populations in the country, such as Uyghur Muslims and opposition activists.
-  Suppressing Taiwanese and Tibetan pro-democracy movements.
-  Stealing information from military, research, and other strategic organizations to supplement commercial and political advantages.

China’s campaigns of control

China’s cyber activity in Q3 demonstrated the Chinese Communist Party’s (CCP) continued determination to maintain control of all the “dissident” populations that oppose it, both inside and outside the country.

In Q3, it came to light that China had been targeting the country’s Uyghur Muslims in a persistent cyber attack campaign. Researchers discovered a seven year mobile campaign targeting Uyghur Muslims, in which the Chinese Scarlet Mimic threat group leveraged more than 20 variations of MobileOrder malware, disguised in multiple Uyghur-related baits such as books, pictures, and even an audio version of the Quran, to surveil and spy on the Uyghur community since 2015¹¹.

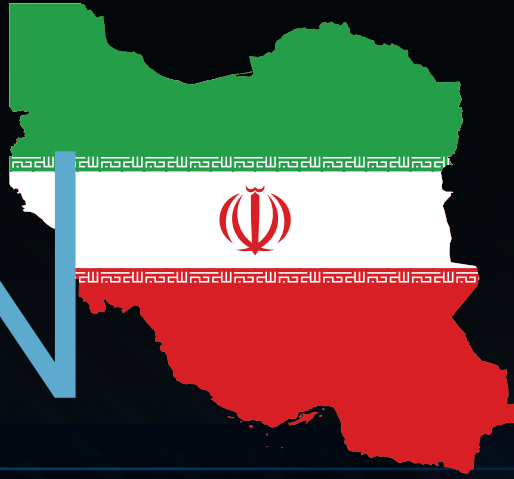
But the Uyghur population wasn’t the only group the CCP was trying to keep an eye on, it also was trying to maintain its campaign of control over two of its largest territorial opponents – Tibet and Taiwan. In September, a report was released detailing activity by TA413 targeting the Tibetan community for intelligence-gathering purposes over the past several years, using custom capabilities shared across other known Chinese state-sponsored groups, such as a shared zero-day exploit in Sophos Firewall (CVE-2022-1040)¹².

Additionally, China has become increasingly aggressive against Taiwan in recent months, particularly in August as U.S. House Speaker Nancy Pelosi visited Taiwan on a diplomatic visit – marking the highest ranking U.S. official to visit Taiwan in 25 years. Showing its opposition, China began invasive military drills surrounding the island and also launched DDoS attacks against Taiwanese government websites shortly before Pelosi’s visit, likely as an intimidation tactic^{13,14}. The Ukraine-Russian War has provoked fears that China may follow Russia’s lead to invade Taiwan, making their provocative tactics stir more concern from international parties.

Gaining strategic advantages

The CCP also continued to target international organizations to gain political and financial advantages, evidenced by the many long-running attack campaigns that were revealed in Q3. The targeting of some of these attack campaigns have exemplified China’s strategic interest in the Ukraine-Russia War since even before Russia invaded, such as TA428’s highly targeted cyber espionage campaign that was uncovered in August targeting over a dozen military industrial complex enterprises and public institutions in Russia, Ukraine, Belarus, and Afghanistan in January 2022¹⁵. Reported Chinese cyber operations also demonstrate the CCP’s continued interest in strategic organizations in the South China Sea, including a Leviathan cyber espionage campaign targeting entities in the region, including organizations involved in an offshore wind farm in the Taiwan Strait¹⁶.

IRAN



CYBER STRATEGIC OBJECTIVES

10

CAMPAIGNS
REPORTED



Maintaining control over domestic opposition populations protesting against the Islamic Republic.



Sustaining advantage over international opponents, such as Albania and Israel.

The Iranian government faced both external and internal conflicts in Q3, as it aggressively targeted Albania with a series of persistent cyber attacks and tried to quell domestic uprisings in the country by cutting internet service and social media access in late September. It also generated negative international attention for providing weapons such as drones and missiles to Russia in its war against Ukraine.

A sustained campaign against Albania

In July, Iranian state cyber actors – identifying as “HomeLand Justice” – launched a destructive cyber attack against the government of Albania, rendering certain websites and services unavailable. An FBI investigation later uncovered that the threat actors had gained initial access to the victim’s network approximately 14 months before launching the destructive cyber attack, which included a ransomware-style file encryptor and ZeroCleare wiper malware. In September, Albania severed diplomatic relations with Iran and expelled Iranian diplomats in response to the attack¹⁷. Shortly after, Iranian threat actors launched another wave of cyber attacks against the government of Albania, using similar TTPs and malware as the cyber attacks in July¹⁸. These were likely done in retaliation for public attribution of the cyber attacks in July and severed diplomatic ties between Albania and Iran.

Quelling domestic strife

At the end of Q3, the Islamic Republic was facing nationwide protests over the death of Mahsa Amini, a 22-year-old Iranian woman who died in police custody after being arrested by morality police for allegedly not complying with strict rules on head coverings. The multi-week protests that began on September 17 were met with violent repression by Iranian authorities, with over 130 people being killed and thousands being arrested by the beginning of October¹⁹. Violence was not the only tactic the Iranian government used to quell protests however, as citizens reported 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 Instagram and WhatsApp, two of the last remaining social networks in Iran²⁰. Another campaign was revealed in September 2022 demonstrating the Iranian government’s efforts to surveil citizens suspected of engaging in “immoral and illegal activities.” This campaign involved a previously unseen RAT called CodeRAT that exploits a bug in Microsoft’s data communications technology to target Farsi-speaking code developers in Iran²¹.

Tit-for-tat with Israel continues

Iranian cyber attack campaigns against Israel were also revealed in Q3, reflecting Iran’s consistent interest in gaining an edge on Israel in any way it can. This includes a UNC3890 campaign conducting ongoing cyber espionage attacks against Israeli shipping, government, energy, and healthcare organizations since at least late 2020²². And it also includes observed activity by Muddy Water, which has been associated with Iran’s MOIS, exploiting Log4j vulnerabilities in SysAid applications against Israeli organizations²³.


N.KOREA



12

CAMPAIGNS
REPORTED

CYBER STRATEGIC OBJECTIVES

-  Drawing in financial profit through ransomware operations and attacks targeting fintech and cryptocurrency companies.
-  Supplementing strategic sectors in North Korea by stealing intellectual property from energy, defense, research, and academic organizations abroad.

Consistent campaigns to steal cryptocurrency

North Korean APTs clearly showed their commitment to generating illegal revenue through persistent social engineering campaigns, often targeting employees at cryptocurrency companies and luring victims in with fake job positions. Not only were North Korean threat actors trying to obtain remote jobs at cryptocurrency companies by plagiarizing resumes and pretending to be from other countries, they were also targeting employees in the fintech industry by luring them in with fake job offers²⁴. The threat actors would impersonate companies such as Coinbase and Crypto.com and go through an extensive manipulation process to establish trust and trick victims into opening a malicious file disguised as a fake job offer^{25, 26}.

In July, it was discovered that North Korea used these social engineering tactics to gain access to the Sky Mavis Axie Infinity Ronin bridge in March, from which they stole nearly \$600 million in cryptocurrency²⁷. Specifically, the threat actors posed as job recruiters on LinkedIn and tricked a senior engineer at Sky Mavis into going through “multiple rounds of interviews” and opening an offer letter for a non-existent position to gain access²⁸.

Strategic cyber espionage attacks

But in addition to North Korea’s financially motivated attacks, which also included some suspected ransomware attacks with H0lyGh0st and Maui ransomware variants, the government also led cyber operations that were more geopolitically strategic^{29,30}. For example, researchers reported in August that they uncovered a Kimsuky campaign using the GoldDragon cluster to target professors, researchers, and politicians in South Korea focused on issues related to the Korean peninsula³¹. Shortly after, researchers also discovered a new RAT called MagicRAT used in attacks by the Lazarus Group to access the corporate networks of energy providers in the U.S., Canada, and Japan between February and July 2022³².


Featured Q3 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 Q3 (July-September) that stood out as particularly interesting and noteworthy.

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

IronNet's second year of defending the Black Hat Network Operations Center (NOC) is now in the books, where our NOC threat hunters worked tirelessly throughout the conference to monitor Black Hat network activity and investigate detections, which led to several findings of malicious behavior and malware on the network.

 [Read the Article](#)

 Aug 24

 Threat Research




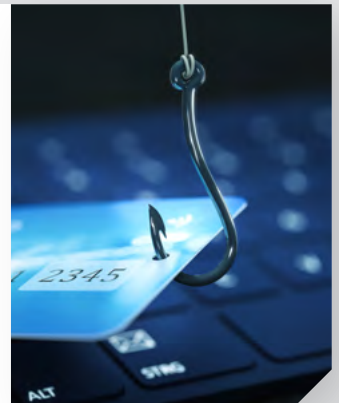
Robin Banks might be robbing your bank: A new phishing-as-a-service platform

In July, IronNet researchers observed a new PhaaS platform called Robin Banks selling ready-made phishing kits to cybercriminals aiming to gain access to the financial information of individuals in several countries.

 [Read the Article](#)

 July 26

 Threat Research



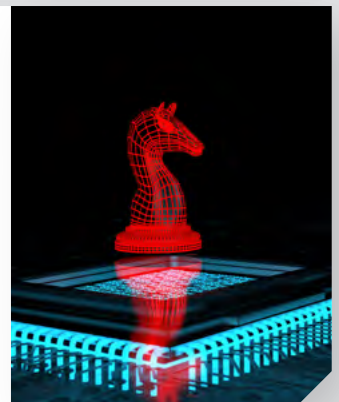
The security risk of M&A: Are Chinese cyber threats lurking in legacy infrastructure?

In late August 2022, IronNet Threat Research discovered a malicious cyber intrusion by a highly sophisticated, likely China-based threat actor in the network of a U.S. software company, specifically targeting a segment of the network absorbed from a prior company acquisition.

 [Read the Article](#)

 Oct 18

 Threat Research



Q4 Threat Watch

THREAT ACTOR

Bianlian Ransomware

BianLian³⁴ is a ransomware family that has been active since December 2021, but has had a massive uptick in activity in August. In August, BianLian had a three-fold increase in C2 server infrastructure. And in September, BianLian began ramping up attacks and skyrocketing the number of victims posted on its data leak site. Given this noticeable increase in attack infrastructure and campaign frequency, we will likely see BianLian pose a continued threat throughout Q4 to organizations in all sectors.

Mitre TTPs

T1046:

Network Service Scanning

T1219:

Remote Access Software

T1071:

Application Layer Protocol

Q3 Sample Targets

- » Spading Grammar School (GB)
- » WWAYTV3 (US)
- » Community Dental Partners (US)
- » Infinitely Virtual (US)
- » Baer's Furniture (US)
- » Ramada Hervey Bay (AU)

Threat Analyst Comment

This threat actor poses a large risk to healthcare and manufacturing organizations, and shows sophistication in its network penetration efforts through evasive techniques. The business side of BianLian operations is still developing, however, and is noted to show amateur tendencies.

MALWARE

Shikitega Malware

Shikitega³³ is a recently discovered malware targeting endpoints and IoT devices running Linux OS. The malware is known to avoid detection by hosting its C2 servers on legitimate cloud services and by slowly delivering partial payloads with numerous decoding loops. Delivered in a multistage infection chain, Shikitega exploits system vulnerabilities to gain high privileges, establish persistence, and execute a crypto miner.

Mitre TTPs

T1059:

Command & Scripting Interpreter

T1569:

System Service

T1543:

Create or Modify System Process

T1569:

System Service

Sample Network IOCS

- » dash[.]cloudflare[.]ovh
- » main[.]icloudfronts[.]net

Sample CVEs exploited:

- » CVE-2021-4034
- » CVE-2021-3493

CONCLUSION

In the constantly evolving cyber threat landscape, threat actors of all types and sophistication levels are exploiting weaknesses in organizations' defenses and leveraging open-source tools and red teaming frameworks to carry out malicious intrusions.

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 rages on and escalates, which IronNet closely monitors to assess the risk of destructive, disruptive, and cyber-espionage attacks against Ukraine and its allies.

In terms of tactics, compromised VPN credentials remain a top mode of initial access, evidenced by multiple intrusions detected by IronNet in Q3. It is of utmost importance to ensure inactive accounts are deleted, to enforce multi-factor authentication (MFA), and to closely monitor VPN credentials and usage. Identifying and securing all IT assets within an organization's environment is also increasingly vital, as we frequently see older, sometimes forgotten, infrastructure being exploited by threat actors for both initial access and evasion in post-intrusion activity. Additionally, we advise organizations and individuals to remain vigilant in the face of opportunistic phishing attacks by low-level cybercriminals trying to steal credentials and financial information. This has been and will proceed to be a threat for the foreseeable future, especially as more as-a-service platforms arise and the barrier to cybercrime lowers as a result.

ENDNOTES

- 1 Kenefick, Silva, & Hernandez. (2022). Black Basta Ransomware Gang Infiltrates Networks via QAKBOT, Brute Ratel, and Cobalt Strike. Trend Micro. https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html.
- 2 Kirkendall. (2021). Our fight against fraud is just getting started. NameCheap. <https://www.namecheap.com/blog/namecheaps-fight-against-fraud-is-just-getting-started/>.
- 3 Namdevel. (2020). scrapeBinary/php-obfuscator. GitHub. <https://github.com/scrapeBinary/php-obfuscator>.
- 4 Adspect. (2021). Adspect Documentation. <https://docs.adspect.ai/en/latest/>
- 5 Kgretzky. (2021). Kgretzky/evilginx2. GitHub. <https://github.com/kgretzky/evilginx2>
- 6 Townsend. (2022). Killnet Releases ‘Proof’ of Its Attack Against Lockheed Martin. Security Week. <https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin>.
- 7 Freed. (2022). Russian hacking group targets state-government websites in DDoS campaign. Statescoop. <https://statescoop.com/russia-ukraine-killnet-ddos-state-governments/>.
- 8 Montalbano. (2022). ‘Killnet’ Adversary Pummels Lithuania with DDoS Attacks Over Blockade. ThreatPost. <https://threatpost.com/killnet-pummels-lithuania/180075/>.
- 9 Demboski. (2021). Russia, ransomware, and the REvil shutdown – what does it all mean? IronNet. <https://www.ironnet.com/blog/russias-ransomware-and-revil-shutdown>.
- 10 Mandiant Intelligence. (2022). GRU: Rise of the (Telegram) MinIONS. Mandiant. <https://www.mandiant.com/resources/blog/gru-rise-telegram-minions>.
- 11 Checkpoint Research. (2022). 7 Years of Scarlet Mimic’s Mobile Surveillance Campaign Targeting Uyghurs. Check Point. <https://research.checkpoint.com/2022/never-truly-left-7-years-of-scarlet-mimics-mobile-surveillance-campaign-targeting-uyghurs/>
- 12 Insikt Group. (2022). Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets. Recorded Future. <https://www.recordedfuture.com/chinese-state-sponsored-group-ta413-adopts-new-capabilities-in-pursuit-of-tibetan-targets>.
- 13 New York Times. (2022). Nancy Pelosi Taiwan Visit As Pelosi Departs Taiwan, China Gears Up for Military Drills. <https://www.nytimes.com/live/2022/08/02/world/pelosi-taiwan>.
- 14 Paganini. (2022). Taiwan government websites suffered DDoS attacks during Nancy Pelosi visit. Security Affairs. <https://securityaffairs.co/wordpress/133997/breaking-news/taiwan-hit-cyberattacks.html>.
- 15 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/?utm_source=press-release&utm_medium=email&utm_campaign=targeted-attack-on-industrial-enterprises-and-public-institutions.
- 16 Raggi & Scenarelli. (2022). Rising Tide: Chasing the Currents of Espionage in the South China Sea. Proofpoint. <https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea>
- 17 Reuters. (2022). Albania cuts Iran ties over cyberattack, U.S. vows further action. <https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/>
- 18 FBI & CISA. (2022) Alert (AA22-264A): Iranian State Actors Conduct Cyber Operations Against the Government of Albania. CISA. <https://www.cisa.gov/uscert/ncas/alerts/aa22-264a>.
- 19 Iran Human Rights. (2022). Iran Protests: Death Toll Rises to 133 / 40+ Killed in Zahedan’s “Bloody Friday.” <https://iranhr.net/en/articles/5506/>.
- 20 Netblocks. (2022). Internet disrupted in Iran amid protests over the death of Mahsa Amini. <https://netblocks.org/reports/internet-disrupted-in-iran-amid-protests-over-death-of-mahsa-amini-X8qVEwAD>.
- 21 Black. (2022). RAT in the cyber-kitchen: new breed of trojan deployed against Iranian coders. Cybernews. <https://cybernews.com/news/rat-in-the-cyber-kitchen-new-breed-of-trojan-deployed-against-iranian-coders/>.
- 22 Mandiant Israel Research Team. (2022). Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors. Mandiant. <https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping>.
- 23 Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Research Team, & Microsoft Defender Threat Intelligence. (2022). MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations. Microsoft. <https://www.microsoft.com/en-us/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/>
- 24 Stone. (2022). North Koreans Steal LinkedIn Resumes in Crypto Job Search Scam. Bloomberg. <https://www.bloomberg.com/news/articles/2022-08-01/north-koreans-suspected-of-using-fake-resumes-to-steal-crypto-xj4y7vzkq>.
- 25 Toulas. (2022). North Korean hackers target crypto experts with fake Coinbase job offers. Bleeping Computer. <https://www.bleepingcomputer.com/news/security/north-korean-hackers-target-crypto-experts-with-fake-coinbase-job-offers/>.
- 26 Devadoss & Stokes. (2022). Lazarus ‘Operation In(ter)ception’ Targets macOS Users Dreaming of Jobs in Crypto. Sentinel One. <https://www.sentinelone.com/blog/lazarus-operation-interception-targets-macos-users-dreaming-of-jobs-in-crypto/>.
- 27 Ronin Network. Community Alert: Ronin Validators Compromised. Ronin Blockchain. <https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r>.
- 28 Towey. (2022). Hackers pulled off a \$620 million crypto heist by tricking an engineer into applying for a fake job and opening an offer letter containing spyware, report says. Business Insider. <https://www.businessinsider.com/axie-infinity-crypto-hack-fake-job-offer-letter-spyware-phishing-2022-7>
- 29 FBI & CISA. Alert (AA22-187A). North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector. CISA. <https://www.cisa.gov/uscert/ncas/alerts/aa22-187a>.
- 30 MSTIC & Microsoft Digital Security Unit (DSU). (2022). North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware. Microsoft. <https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/>.
- 31 Park. (2022). Kimsuky’s GoldDragon cluster and its C2 operations. SecureList. <https://securelist.com/kimsuky-golddragon-cluster-and-its-c2-operations/107258/>.
- 32 An, Malhotra, & Ventura. (2022). MagicRAT: Lazarus’ latest gateway into victim networks. Cisco Talos. <https://blog.talosintelligence.com/2022/09/lazarus-magicrat.html>.
- 33 Caspi. (2022). Shikitega – New stealthy malware targeting Linux. AT&T. <https://cybersecurity.att.com/blogs/labs-research/shikitega-new-stealthy-malware-targeting-linux>.
- 34 Armstrong, Pearce, Pittack, & Quist. (2022). BianLian Ransomware Gang Gives It a Go! Redacted. <https://redacted.com/blog/bianlian-ransomware-gang-gives-it-a-go/>.

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



Request a Demo

to see Collective Defense in action

Collective attacks
need **Collective Defense**

