RAPID7

JANUARY 2022

Cyberthreat Intelligence Banking Report for XYZ

Executive Summary

In Q1 of 2022, we saw active chatter in Telegram channels regarding malicious tools and methods that are used to target XYZ and their customers. We identified the sale of banking web injects, banking Trojans, and also phishing kits that use uAdmin panels. In addition, we saw threat actors offering bank account credit cards and login credentials for sale.

Searching for the XYZ name, brand, and logos on more than 20 third-party Android app stores revealed that most of the links related to XYZ are down. We found several applications that contain XYZ's name, brand, or logo.

It is essential to say that although these third-party vendors are unofficial application stores, most of them mirror legitimate app stores.

In a survey of the threat landscape to find the most relevant and active threat actors targeting the banking and financial sectors, we identified the following:

- Anonymous
- ALPHV
- Conti
- Hive
- Lockbit 2.0

Besides the most active TA ("Top 5 Threat Actors"), we listed an additional five threat actors that constantly target organizations in the relevant sectors, even though they have no specific reported attacks in the past quarter.

Methodology

The research results that are presented in this report are a combination of several methodologies: IntSights proprietary investigation tools, open-source intelligence (OSINT) search tools, deep and dark web searches, and social media profile content investigation.

This report covers the first three months of 2022.

Chatter: Clear, Deep and Dark Web Research

As part of our research on threats against XYZ, we carried out extensive research using different sources, such as social networks, forums, markets and messaging applications on the clear, deep and dark web. We identified several threats targeting XYZ including stolen bank login credentials and credit card numbers, phishing pages, web injections, and fake banking Trojans.

Also, we searched more than 20 unofficial app stores for the XYZ brand, name, or logo. Those stores are listed in the appendix.

Bank Login Credentials

Threat actors know that customer systems are not usually as well protected as are banking systems. This makes it more beneficial to obtain customer bank login credentials than to try to infiltrate the bank.

We identified several dark web locations where one can purchase account login credentials to XYZ bank accounts.

We found a few Telegram channels where threat actors sell XYZ bank account credentials. These bank accounts have a balance ranging from 10 to 100 thousand Euros, including bank documents and identification certificates (Figures 1 and 2).

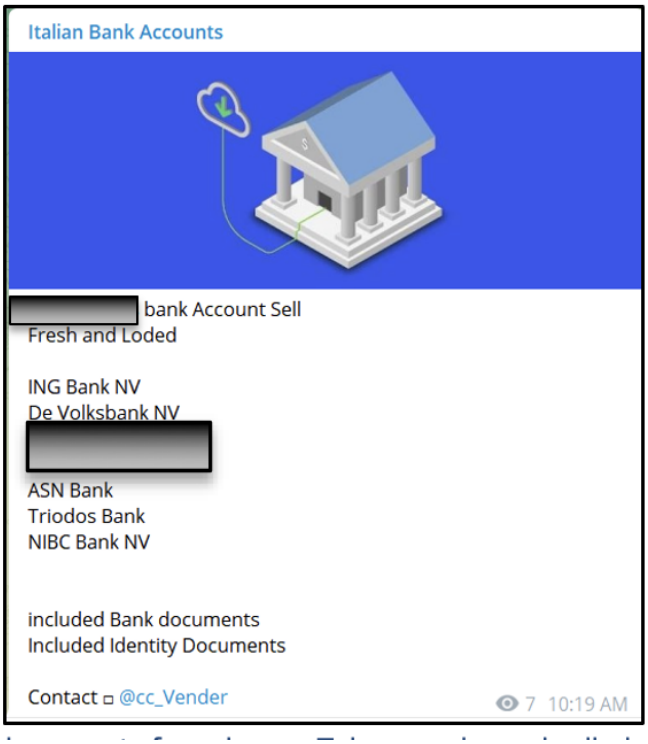


Figure 1 - XYZ bank accounts for sale on a Telegram channel called "Italian Bank Accounts"

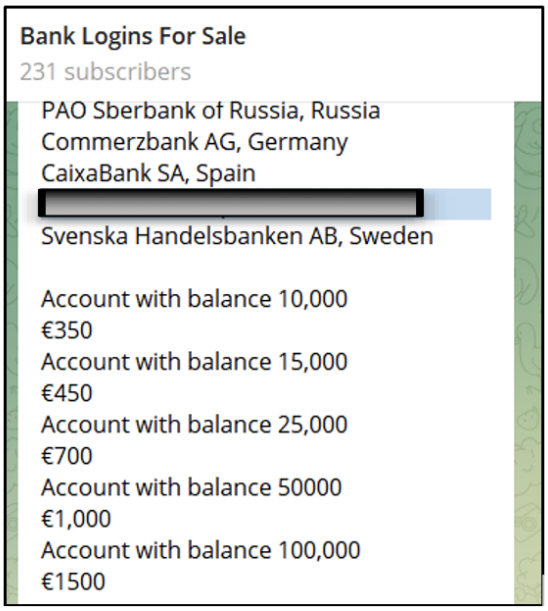


Figure 2 XYZ bank accounts for sale published on a Telegram channel called "Bank Logins for Sale"

Apart from Telegram, we have also recently identified several **** bank accounts for sale on a dark web market named “bitify” (Figures 3, 4, and 5).

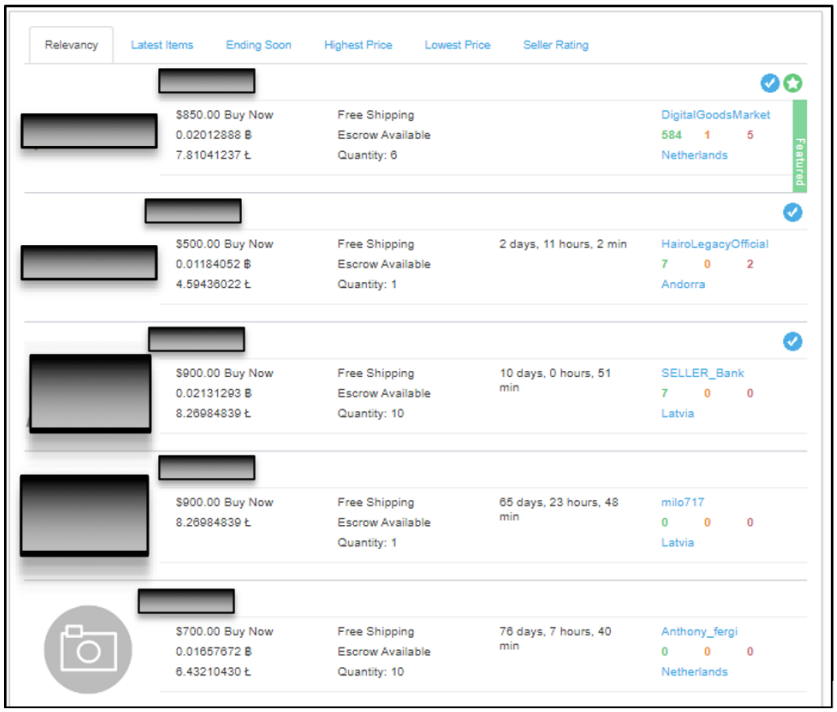


Figure 3 - A list of XYZ bank accounts for sale on a dark web market

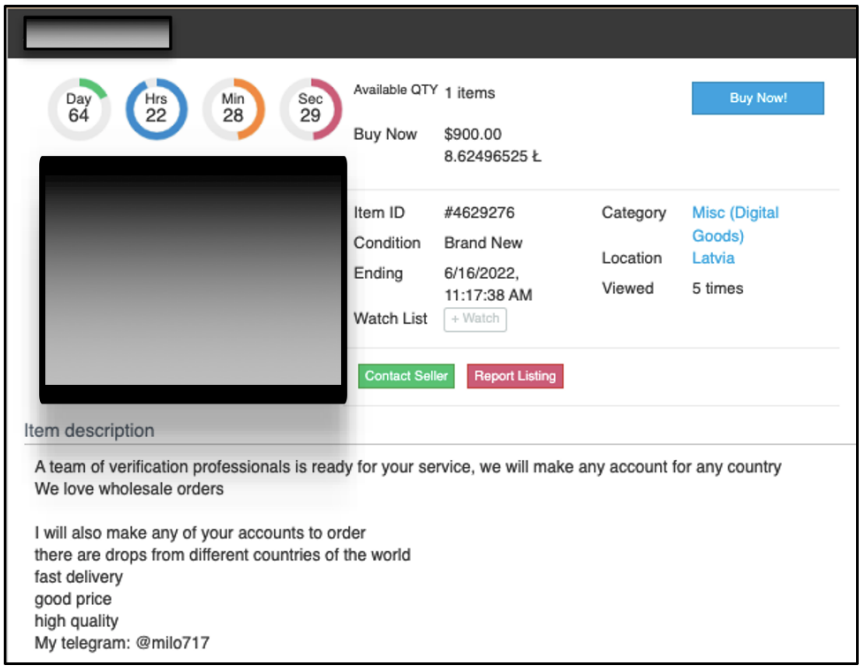


Figure 4 -Details of an XYZ bank account for sale on a dark web market

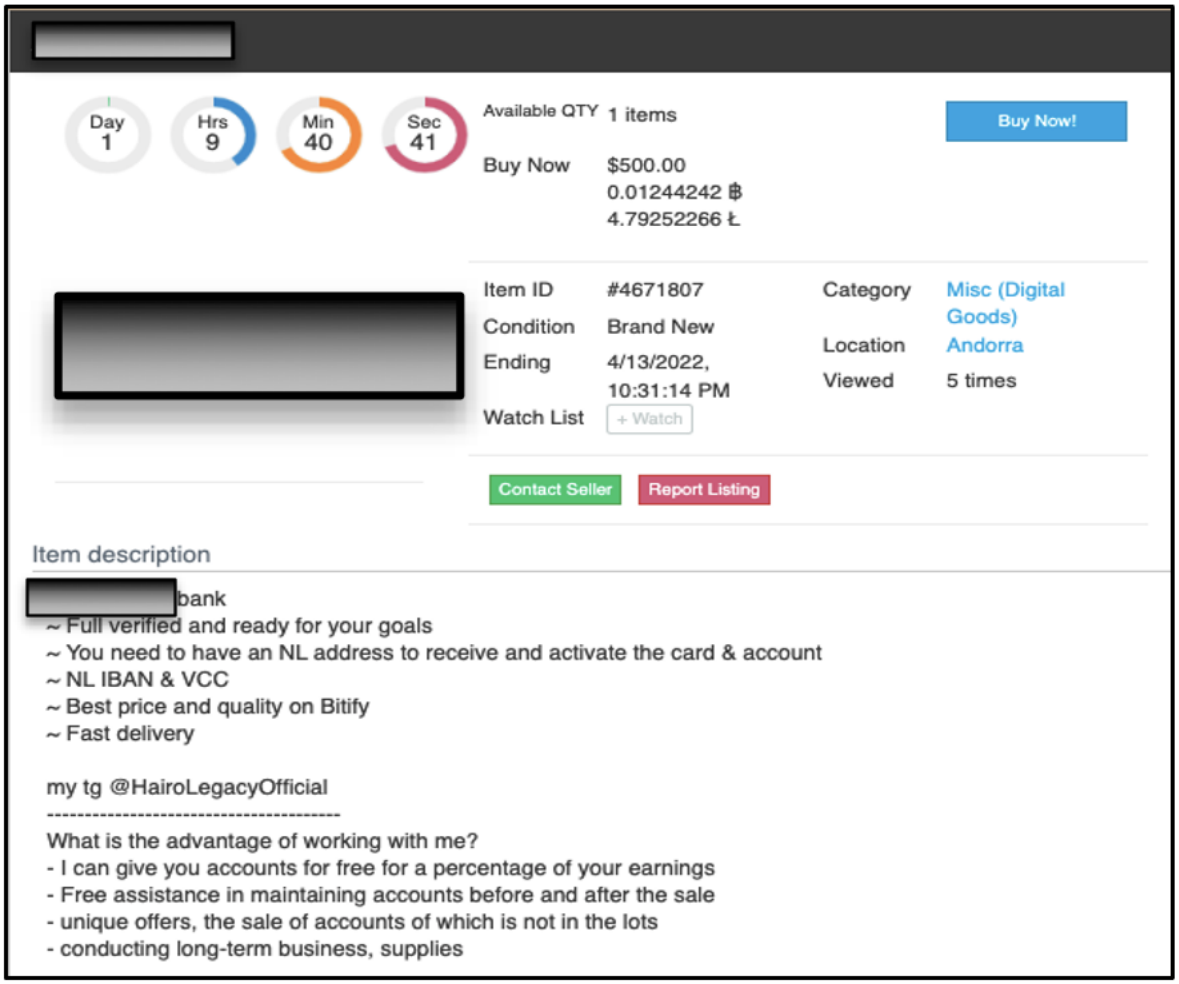


Figure 5 - Details of an XYZ bank account for sale on a dark web market

Credit Cards and Cash Out

Banks and credit card companies constantly face the issues of stealing and selling credit card numbers and cashing out from corrupt or illegal bank accounts. We conducted deep research and identified several Dutch Telegram groups where threat actors sell stolen credit cards from different banks, including XYZ (Figure 6). In addition, we identified a threat actor looking for people who own stolen credit cards to collaborate in cashing out services on bank accounts including XYZ (Figure 7).

Figure 6 - A Dutch Telegram group with XYZ credit cards for sale

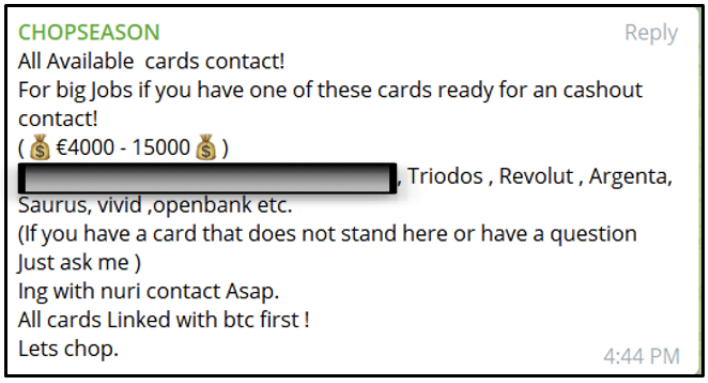


Figure 7 - A Dutch Telegram group with a threat actor looking for people to cash out XYZ accounts

Phishing and Leads

Like credit cards and bank logins, phishing and spear phishing attacks are constant threats employed against bank customers. We thoroughly analyzed these threats targeting XYZ and identified some of them on Telegram. We identified some Telegram groups in which threat actors sell uAdmin pages, as well as leads for phishing, including for the XYZ bank (Figures 8 and 9).

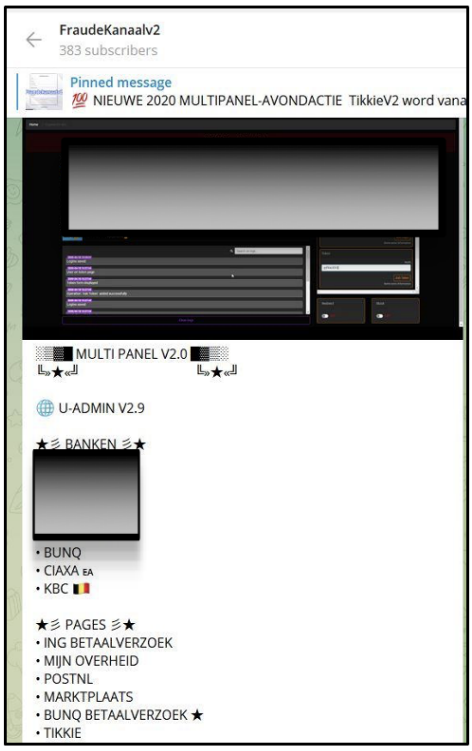


Figure 8 - A Dutch Telegram group where a threat actor is selling uAdmin for XYZ phishing page

Figure 9 - A Dutch Threat actor selling XYZ leads for phishing

Banking Web Injects

Banking web injects, a malicious tool that is usually integrated with banking Trojans, enable threat actors to bypass the two-factor authentication (2FA) security measure and compromise a users' bank accounts. Web injects pose a real security issue for banks and customers. During our threat research, we identified a dark web market that sells banking web injects, including those of XYZ (Figure 10).

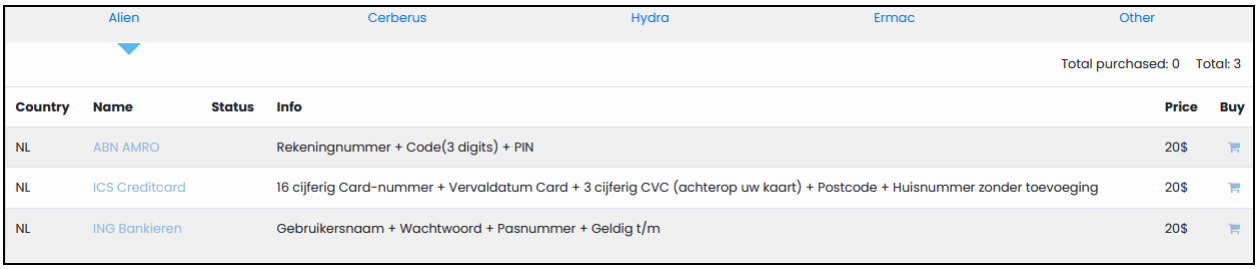


Figure 10 - An XYZ web inject for sale on a dark web market

Banking Trojans

Banking Trojans are among the most common types of malware and are responsible for a large proportion of attacks against banks. The primary function of a banking Trojan is to compromise online banking credentials that are stored on compromised devices and use this unauthorized access for fraudulent purposes. The access can be abused by the attackers themselves or sold on underground black markets. We searched various hacking forums for the current, most popular banking Trojans. The following is a list of the most relevant (in Q1 of 2022) banking Trojans, in alphabetical order.

- **Ares V2** - A variant of Kronos that surfaced in spam campaigns targeting German speakers. Ares is designed to install a stealer that collects login credentials from various VPN clients and web browsers, exfiltrates cryptocurrency wallets' private keys, and downloads arbitrary files. The banking Trojan has been recently modified with new features and is currently identified as Ares V2 (Figure 11).

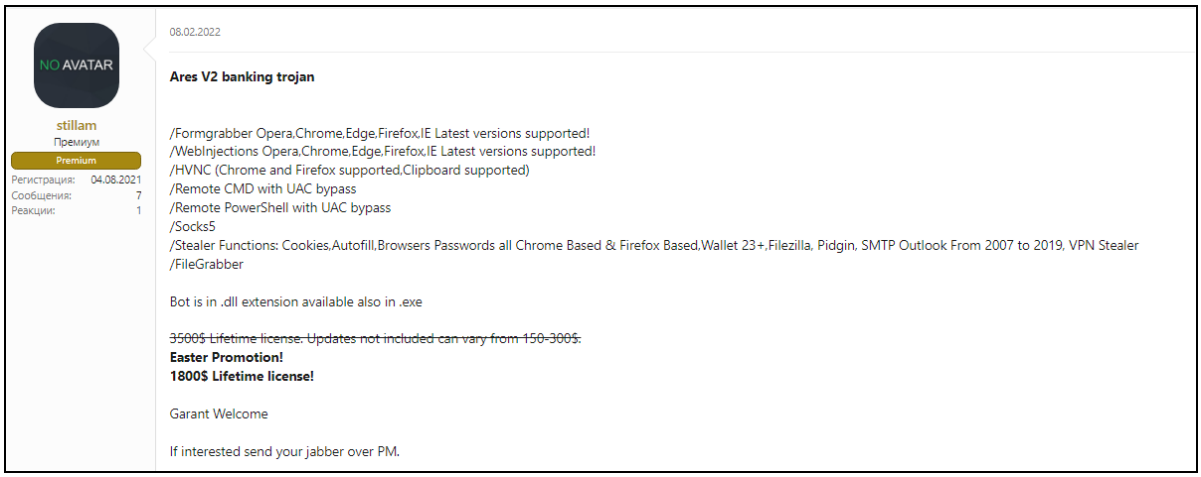


Figure 11- Kronos for sale on a cybercrime forum

- **Alien** - This Android banking Trojan is a descendant of the Cerberus banking Trojan, active since January 2020. The Trojan primarily targets banking applications in countries such as the United States, the United Kingdom, France, Italy, Spain, Germany, and Australia. It has also targeted other apps, such as email messaging providers (e.g., Gmail), social media services (e.g., Facebook, Twitter), instant messaging platforms (e.g., Telegram), and cryptocurrency apps (e.g., BitPay).

- **BRATA** - This Brazilian-developed Android banking Trojan was first reported by Kaspersky researchers in August 2019 and has been active since January 2019. The malware initially targeted users in Brazil, but its distribution seems to be expanding with time, as it was observed infecting users in other countries, such as the United States, Spain, and Italy. The name BRATA is an abbreviation for "Brazilian RAT Android."

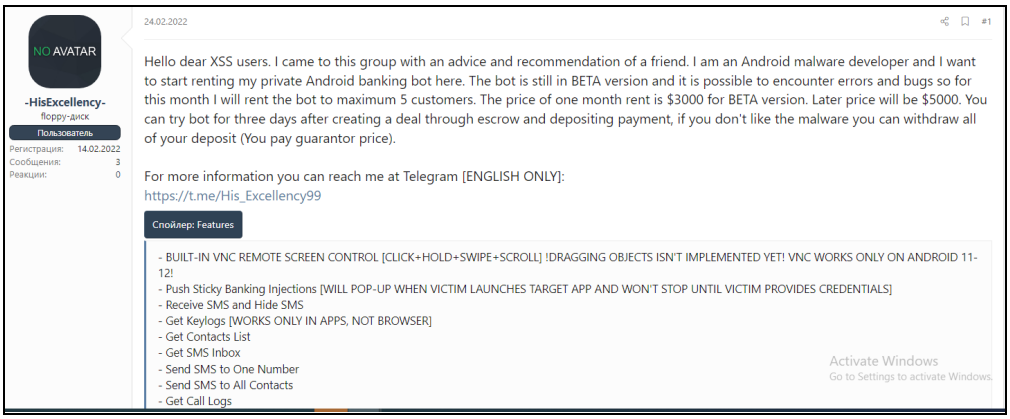
- **Dridex (AKA Bugat)** - Was first observed in 2011. It is famous for stealing banking and payment card credentials. The malware is a further evolution of the earlier banking trojan Cridex. In December 2021, threat actors were reported to exploit the critical Log4j vulnerability (CVE-2021-44228) to infect their victims with the Dridex malware.

- **DanaBot** - This banking Trojan targets users in Australia via email messages containing malicious URLs written in Delphi (Figure 12).

Figure 12 - DanaBot for sale on a cybercrime forum

- **ERMAC** - An Android banking Trojan that was first observed in July 2021. The malware initially targeted only users in Poland, but its distribution seems to be expanding with time, as it was observed infecting users from other countries as well, such as the United States. ERMAC is considered a descendant of the BlackRock banking Trojan, both developed by a threat actor nicknamed "DukeEugene."

- **Escobar (AKA Aberebot)** - This Android banking Trojan was first observed by cybersecurity researchers in July 2021. The Trojan primarily targets banking and cryptocurrency applications in countries such as the United States, the United Kingdom, France, Italy, Spain, Germany, India, Japan, and Australia. In March 2022, a new Aberebot variant named Escobar started to be distributed among Android users (Figure 13).



- **Flubot** (AKA Cabassous, FedEx Banker) - An Android banking malware discovered by PRODAFTon November 10, 2020. The malware was dubbed Flubot due to its ability to spread rapidly with infection vectors that resemble the common flu.

- **Hydra** - An Android-based malware, first used around 2018-2019, initially as a dropper and then as an Android bankbot. At the beginning of its distribution, the malware targeted exclusively Turkish banks and crypto wallet applications; however, since early 2020, the targets have expanded to central banks around the globe (e.g., ING Australia Banking, AXA Banque France, Deutsche Bank Mobile, Wells Fargo Mobile, and many more).

- **Medusa (AKA Gorgona)** - An Android banking Trojan that was first observed by cybersecurity researchers in July 2020. The Turkish-created malware targets banking applications, primarily from the United States, Spain, and Turkey.

- **Oscorp** - An Android Trojan developed to attack multiple financial targets, including banks and cryptocurrency applications. First observed at the beginning of 2021, Oscorp can send, intercept, and delete SMS messages, make phone calls, and perform overlay attacks on more than 150 mobile applications. In May 2021, new samples of Oscorp were identified with some modifications that paralleled the appearance of another Android malware known as UBEL. There are several indicators that link Oscorp and UBEL to the same malicious code base.

- **Octo (AKA ExobotCompact.D)** - an Android banking Trojan that was first reported by cybersecurity researchers in April 2022, after its name surfaced on underground hacking forums in January 2022. Octo is a rebrand of the ExobotCompact malware (AKA ExoCompact) that targets banking, financial, and instant messaging apps mainly in Europe, in countries such as the United Kingdom, Germany, Italy, Spain, and Portugal. The malware is being offered for sale by a threat actor using the aliases "Architect" and "Goodluck."

- **SharkBot** - An Android banking Trojan that was first observed in October 2021. The malware targets banking applications and cryptocurrency exchanges in the United States, the United Kingdom, and Italy. Its name originates from multiple strings found in its code, containing the word "sharked." Currently, SharkBot is believed to be in its early stages of development.

- **TeaBot (AKA Anatsa, Toddler)** - An Android banking Trojan that was first observed in January 2021. The Trojan targets banking apps mainly in Europe, in countries such as the United Kingdom, Belgium, Italy, Spain, Germany, and the Netherlands. It supports six languages: Spanish, English, Italian, German, French, and Dutch. The TeaBot banking Trojan was sometimes distributed alongside other banking malware, such as FluBot (AKA Cabassous).

- **Xenomorph** - an Android banking Trojan that was first reported in February 2022. The malware targets banking applications from countries like Spain, Portugal, Italy, and Belgium and also general applications like email services and cryptocurrency wallets. It shares some coding similarities with the Alien Android malware, indicating that the same developers created both malware.

- **Nameless Private Malware** - We also identified other unnamed banking malware for sale on Russian underground hacking forums (Figures 14 and 15).

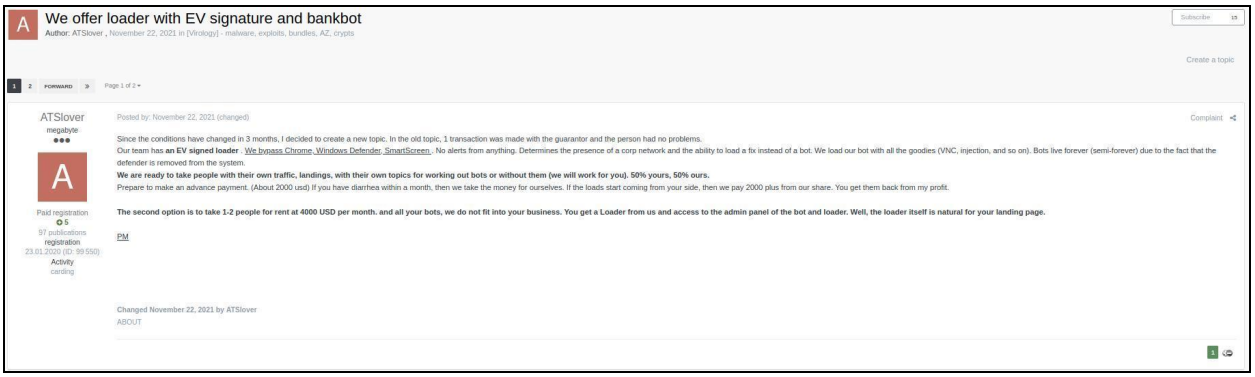


Figure 14 - Start of auction for unnamed banking malware

Figure 15 - Halt of partner drafting for unnamed banking malware

XYZ Banking app

We searched for **** APK files on some of the biggest, unofficial online application stores. These stores usually mirror the official app stores (Google Play Store, Galaxy Store, etc.), but some also allow the uploading of unverified apps.

Unverified apps can be infected by threat actors with different Trojans to target the bank's customers and steal their credentials. Some of these stores contain links presenting the XYZ brand by its name or logo; however, most of these links do not work. This may be due to a takedown of the hosted app or a broken link. We did not download or examine any APK files during this research process.

We searched in 26 different unofficial app stores (the complete list appears in the Appendix), but only found mentions for XYZ in the following stores:

Figure 21 - Files related to **** on VirusTotal

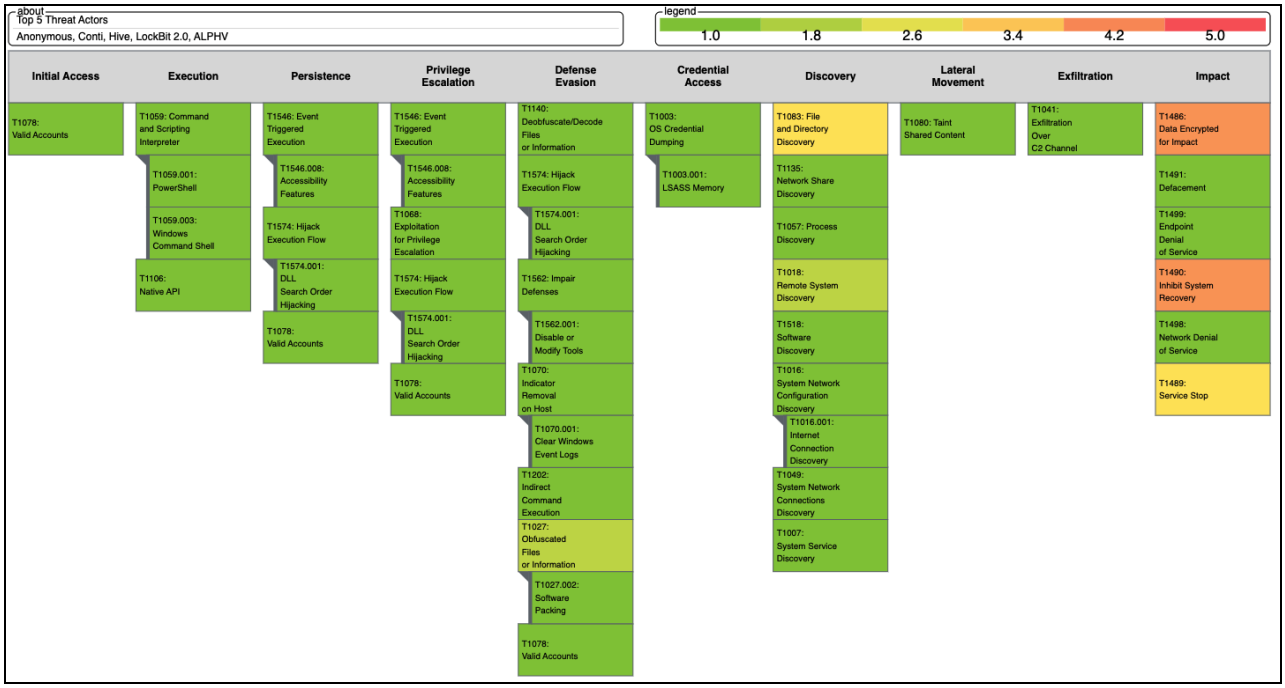
Threat Actors

This section describes threat actors that actively targeted organizations in the banking and financial sectors in the past year.

We first specify the most active threat actors targeting the above sectors during Q1 of 2022 (Top 5 Threat Actors) and then elaborate on other active threat groups operating in these sectors in the past year.

Notably, this section only includes threat actors that are still active. In addition, there may be threat actors that targeted the above industries but were not actively observed in a specific attack against them during the discussed time frame.

A list of relevant tactics, techniques, and procedures (TTP) for each threat actor appears in the Appendix. The TTP of the Top 5 threat actors also includes detective and protective measures as specified on the MITRE ATT&CK website (attack.mitre.org).



Top 5 Threat Actors

Anonymous

Anonymous is an international network of activists and hacktivists. The group became known for a series of well-publicized publicity stunts and distributed denial-of-service (DDoS) attacks on government, religious, and corporate websites. Current active Anonymous affiliated groups include Network Battalion 65' (NB65), AgainstTheWest (ATW), AnonGhost, and The Black Rabbit World.

Recent activity related to the banking and financial sectors

- On March 1, 2022, amidst the Russo-Ukrainian War, the Anonymous-affiliated group AgainstTheWest claimed to hack the Russian state-owned Sberbank bank and leaked its data, including DNS infrastructure, private keys for SSL, Sberbank API, CLI, and SDKs.

ALPHV

The ALPHV ransomware-as-a-service provider (AKA BlackCat) was first observed by cybersecurity researchers in November 2021. The ransomware operators are Russian speakers, as it is promoted in Russian hacking forums. In February 2022, one of the group members confirmed that ALPHV consists of former members of the BlackMatter (formerly DarkSide) and REvil ransomware groups.

Some cybersecurity researchers believe it is a rebrand of BlackMatter/DarkSide. The group uses the double-extortion method of stealing the data before encryption and threatening to publish it if the ransom is not paid. The extortion method can also be tripled where the threat actors threaten to perform DDoS attacks until the ransom is paid.

Recent activity related to the banking and financial sectors

- At the beginning of February 2022, ALPHV uploaded files allegedly belonging to Albany Bank and Trust Company. The mainstream media did not cover the attack, but it is safe to assume that the group refused the ransom demands, as its files were publicly exposed.

Conti

The Conti ransomware-as-a-service (RaaS) has been active since December 2019, increasing its activity since June 2020. The group is suspected to be operated by the Russian criminal enterprise known as "Wizard Spider." The threat actor's targets are very diverse and attacks were initiated against major corporations and government agencies, particularly in North America and Western Europe. Due to similarities found in the malware code and ransom notes of the Conti and Ryuk ransomware, the first is considered a successor of Ryuk, both building on TrickBot infrastructure. Conti is also associated with the financially-motivated threat group TA551 (AKA Shatak).

Recent activity related to the banking and financial sectors

- On January 20, 2022, Bank Indonesia (BI) suffered a ransomware attack in December, in which employee data was stolen. Although the bank did not attribute the attack to any specific threat actor, the Conti operators claimed responsibility for uploading some stolen files to their leak site. The threat actors threatened to leak 13.88 GB of documents if the bank did not pay the ransom. The bank representatives stated that the attack was stopped before affecting its public services and that the stolen data was not critical.

Hive

The Hive ransomware group was discovered on June 26, 2021, when security researchers stumbled upon their leak site named HiveLeaks. The group operators employ the double-extortion technique as they exfiltrate their targets' data before they encrypt it. The ransomware payload appends encrypted files with the .hive extension. Although there are no details on the origin of the

malware and its operators, their leak site uses the infrastructure of a known Russian cybercriminal community.

Recent activity related to the banking and financial sectors

- On March 23, 2022, Hive created a leak site entry for Banco Caribe of the Dominican Republic. The threat actors claimed to breach the bank on January 22, 2022, however the allegedly stolen information was not released yet, which may indicate that the victim paid the ransom.

LockBit 2.0

The LockBit ransomware group emerged from Russian darknet forums on January 17, 2020. The group first used a preliminary ransomware strain, dubbed ABCD Ransomware, active in mid-October 2019. LockBit's distribution model is based on an affiliate program, allowing users to share their income with the malware's author. In mid-July 2021, the operators of LockBit ransomware relaunched their affiliate program under the name LockBit 2.0. The announcement was promoted via the group's Tor leak site, inviting cybercriminals and insiders to take part in the malware's new and advanced capabilities, claiming that LockBit 2.0 has the "fastest encryption all over the world."

Recent activity related to the banking and financial sectors

- On January 17, 2022, LockBit announced that it breached the Central Bank of Florida. The threat actors gave the bank 24 hours to agree to the ransom demands and then published the allegedly stolen data on the group's leak site. The files are currently not available for download, so either the bank agreed to the ransom demands or the threat actors lost interest.

Other Threat Actors

APT10

The APT10 threat group (AKA Stone Panda, MenuPass, Red Apollo, and Cicada) has been active since at least 2006. The Chinese state-sponsored group globally targets organizations from various sectors, such as finance, healthcare, defense, biotechnology, energy, and government, focusing on Japanese organizations. In 2016-2017, APT10 became well-known for orchestrating a

global campaign dubbed "Operation Cloud Hopper," targeting managed IT service providers (MSPs). Experts believe that the goals behind APT10's hacking campaigns support the Chinese national security goals, acquiring valuable military and intel and stealing confidential business data to support Chinese corporations.

Recent activity related to the banking and financial sectors

- In February 2022, CyCraft researchers reported on an APT10 campaign initiated in November 2021 and targeted financial organizations in Taiwan. In the campaign, dubbed "Operation Cache Panda," the threat actors leveraged a web service vulnerability in the system management interface of unnamed security software to upload the ASPXCSharp web shell and control the website host. In addition, they used the Impacket penetration tool to scan computers within the network and eventually deploy the .NET-based Quasar RAT on as many computers as possible to steal sensitive information.

AvosLocker

The AvosLocker ransomware group emerged in late June 2021 (although according to its Tor website, the first announcement was on January 1, 2021). One of the ransomware operators, "Avos," posted on two major Russian cybercrime forums that they seek partners with specific requirements and skills (pentesters/access brokers). In addition, the ransomware operators announced on the dark web discussion forum, Dread, that they are willing to collaborate through an affiliate program, offering their ransomware-as-a-service (RaaS) model to handle the negotiation, extortion, and the leak publication. AvosLocker has a dedicated Tor leak website where they release data of the victims who have not responded or refused to pay the ransom demand which varies between $50,000 to $75,000 in Monero (XMR).

Recent activity related to the banking and financial sectors

- On September 4, 2021, AvosLocker claimed to breach Pacific City Bank and publish screenshots of the allegedly stolen data, including various business documents. The Pacific City Bank was removed from the group's leak site, probably due to obsolescence.

Grief

The Grief ransomware group (AKA PayOrGrief) emerged around the end of May 2021. Researchers believe that Grief is a rebrand of the DoppelPaymer ransomware group. The threat actors operate an active leak site, in which they add additional pressure to pay the ransom by publishing the European Union's General Data Protection Regulation (GDPR) and systems downtime statistics costs. In addition, they use anti-crawl protection to prevent attempts of indexing the leak site.

Recent activity related to the banking and financial sectors

- On May 26, 2021, Naz Financial Services suffered a ransomware attack conducted by Grief. The threat actors leaked approximately 5 GB of the Canadian company's data, including tax and accounting documents and customer records.

Lazarus

The Lazarus Group has been active since at least 2009. The North Korean state-sponsored group established its dominance that year, setting several significant cyberattacks against the financial industry, especially via the secure transactions platform SWIFT. Lazarus overlaps with other North Korean threat groups, such as the Guardians of Peace, Hidden Cobra, and Zinc. It is considered a highly sophisticated threat group that is responsible for numerous worldwide cyber campaigns, such as the 2017 WannaCry ransomware attack, Operation Blockbuster, Operation Dream Job, and Operation GhostSecret.

Recent activity related to the banking and financial sectors

- In February 2021, the US Department of Justice indicted three North Korean military hackers associated with Lazarus. According to the indictment, the defendants participated in multiple cyber campaigns compromising the systems of financial organizations worldwide and stealing more than $1.3 billion.

TA505

The TA505 threat group (AKA Hive0065) has been active since 2014. The financially-motivated group targets financial institutions and retail companies by using malicious spam campaigns and frequently-changing malware. It is known for leading global trends in terms of malware distribution.

Among the malware previously used by TA505: the Dridex banking Trojan, Locky ransomware, and the TrickBot banking Trojan.

Recent activity related to the banking and financial sectors

- In October 2021, cybersecurity researchers reported on a TA505 campaign, dubbed MirrorBlast, targeting financial organizations in various countries, such as the United States, Canada, and Hong Kong. The threat actors used phishing email messages that contained macro-embedded Excel documents. Once the macro codes were enabled, an MSI package was dropped, deploying the REBOL and KiXtart malware for data collection and exfiltration.

Conclusion

In Q1 of 2022, we observed active chatter in Telegram channels and underground crime forums related to XYZ Most of the chatter on these channels was regarding XYZ login credentials and uAdmin phishing pages that were offered for sale.

We also found different versions of a few banking apps related to XYZ on unofficial app stores. Threat actors can use these app stores to upload a malicious copy of the bank app to target the bank's customers.

On the threat actors side, we identified 10 active threat groups that target the banking and financial sectors. Out of those, 5 were observed in specific attacks in the last quarter. Most of the identified threat actors are ransomware groups and the mitigation measures against such attacks are detailed in the Recommendations section.

It should be noted that the attack against the Russian state-owned Sberbank bank by the Anonymous-affiliated group AgainstTheWest is not typical of Anonymous and was conducted amidst the Russo-Ukrainian War. With that said, Anonymous are known for their fickle and whimsical character and thus might target Western entities as well if it suits their agenda.

Recommendations

These are the common TTPs of the Top 5 Threat Actors. We provided the detection and mitigation controls regarding these TTPs as they appear on MITRE:

T1486 Data Encrypted for Impact

- Detection
    - Use process monitoring to track the execution and command line parameters of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.
    - Monitor for the creation of suspicious files as well as unusual file modification activity. In particular, look for large quantities of file modifications in user directories.
- Mitigation
    - Behavior Prevention on Endpoint - On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware.
    - Data Backup - Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. Ensure that backups are stored off system and are protected from common methods used by adversaries to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.

T1490 - Inhibit System Recovery

- Detection
    - Use process monitoring to track the execution and command line parameters of binaries involved in inhibiting system recovery, such as vssadmin, wbadmin, and bcdedit. The Windows event logs, ex. Event ID 524 indicating a system catalog was deleted, may contain entries associated with suspicious activity.
    - Monitor the status of services involved in system recovery. Monitor the registry for changes associated with system recovery features.
- Mitigation
    - Data Backup - Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups used to restore organizational data. Ensure backups are stored off system and are protected from common methods used by adversaries to gain access and destroy the backups to prevent recovery.

    - Operating System Configuration - Consider technical controls to prevent the disabling of services or deletion of files involved in system recovery.

T1489 - Service Stop

- Detection
    - Monitor processes and command-line arguments to see if critical processes are terminated or stop running.
    - Monitor for edits or modifications to services and startup programs that correspond to services of high importance.
    - Look for changes to services that do not correlate with known software, patch cycles, etc. Windows service information is stored in the Registry at HKLM\SYSTEM\CurrentControlSet\Services. Systemd service unit files are stored within the /etc/systemd/system, /usr/lib/systemd/system/, and /home/.config/systemd/user/ directories, as well as associated symbolic links.
    - Alterations to the service binary path or the service startup type that are changed to disabled might be suspicious.
    - Remote access tools with built-in features may interact directly with the Windows API to perform these functions outside of typical system utilities. For example, ChangeServiceConfigW may be used by an adversary to prevent services from starting.
- Mitigation
    - Network Segmentation - Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.
    - Restrict File and Directory Permissions - Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services.
    - Restrict Registry Permissions - Ensure proper registry permissions are in place to inhibit adversaries from disabling or interfering with critical services.
    - User Account Management- Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.

T1083 - File and Directory Discovery

- Detection
    - System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as collection and exfiltration, based on the information obtained.
    - Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.
- Mitigation
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

T1018 - Remote System Discovery

- Detection
    - System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.
    - Normal, benign system and network events related to legitimate remote system discovery may be uncommon, depending on the environment and how they are used. Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.
    - Monitor for processes that can be used to discover remote systems, such as ping.exe and tracert.exe, especially when executed in quick succession.
- Mitigation
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Appendix

3rd party app stores

- Apkpure
- ApkMiror
- APKSFree
- Aptoide
- Uptodown
- F-Droid
- APK-DL
- apkmonk
- APKHERE
- APKCombo
- APKBeasts
- dlandroid
- ANDROIDTOP
- APPSAPK
- Soft112
- MODMAFIA
- an1
- ACMarket
- RevD1
- rexdl
- TECHYLIST
- APK4Free
- apkbuilds
- APK4Fun
- AndroPalace
- APKWHALE

Threat Actors TTP

Top 5 Threat Actors

Anonymous

- T1083 - File and Directory Discovery
  Detective controls:
  - DS0017 - Command Execution
  - DS0009 - OS API Execution, Process Creation

  Protective controls:
  - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1489 - Service Stop
  Detective controls:
  - DS0017 - Command Execution
  - DS0022 - File Modification
  - DS0009 - OS API Execution, Process Creation, Process Termination
  - DS0019 - Service Metadata
  - DS0024 - Windows Registry Key Modification

  Protective controls:
  - M1030 - Network Segmentation
  - M1022 - Restrict File and Directory Permissions
  - M1024 - Restrict Registry Permissions
  - M1018 - User Account Management
- T1491 - Defacement
  Detective controls:
  - DS0015 - Application Log Content
  - DS0022 - File Creation, File Modification
  - DS0029 - Network Traffic Content

  Protective controls:
  - M1053 - Data Backup
- T1498 - Network Denial of Service
  Detective controls:
  - DS0029 - Network Traffic Flow
  - DS0013 - Host Status

  Protective controls:
  - M1037 - Filter Network Traffic
- T1499 - Endpoint Denial of Service
  Detective controls:
  - DS0015 - Application Log Content
  - DS0029 - Network Traffic Flow

    - DS0013 - Host Status

  Protective controls:
    - M1037 - Filter Network Traffic

ALPHV

- T1486 - Data Encrypted for Impact

  Detective controls:
    - DS0010 - Cloud Storage Metadata, Cloud Storage Modification
    - DS0017 - Command Execution
    - DS0022 - File Creation, File Modification
    - DS0009 - Process Creation

  Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1053 - Data Backup
- T1083 - File and Directory Discovery

  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1018 - Remote System Discovery

  Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Access
    - DS0029 - Network Connection Creation
    - DS0009 - Process Creation

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1490 - Inhibit System Recovery

  Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Deletion
    - DS0009 - Process Creation
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

  Protective controls:
    - M1053 - Data Backup
    - M1028 - Operating System Configuration

Conti

- T1059.003 - Command and Scripting Interpreter: Windows Command Shell

  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - Process Creation

  Protective controls:

    - M1038 - Execution Prevention
- T1486 - Data Encrypted for Impact
  Detective controls:
    - DS0010 - Cloud Storage Metadata, Cloud Storage Modification
    - DS0017 - Command Execution
    - DS0022 - File Creation, File Modification
    - DS0009 - Process Creation

  Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1053 - Data Backup
- T1140 - Deobfuscate/Decode Files or Information
  Detective controls:
    - DS0022 - File Modification
    - DS0009 - Process Creation
    - DS0012 - Script Execution

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1083 - File and Directory Discovery
  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1490 - Inhibit System Recovery
  Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Deletion
    - DS0009 - Process Creation
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

  Protective controls:
    - M1053 - Data Backup
    - M1028 - Operating System Configuration
- T1106 - Native API
  Detective controls:
    - DS0011 - Module Load
    - DS0009 - Process Creation

  Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1038 - Execution Prevention
- T1135 - Network Share Discovery
  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation

  Protective controls:
    - M1028 - Operating System Configuration
- T1027 - Obfuscated Files or Information
  Detective controls:

    - DS0017 - Command Execution
    - DS0022 - File Creation, File Metadata
    - DS0009 - Process Creation

  Protective controls:
    - M1049 - Antivirus/Antimalware
    - M1040 - Behavior Prevention on Endpoint
- T1057 - Process Discovery

  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1055.001 - Process Injection: Dynamic-link Library Injection

  Detective controls:
    - DS0022 - File Metadata, File Modification
    - DS0011 - Module Load
    - DS0009 - OS API Execution, Process Access, Process Modification

  Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1026 - Privileged Account Management
- T1021.002 - Remote Services: SMB/Windows Admin Shares

  Detective controls:
    - DS0017 - Command Execution
    - DS0028 - Logon Session Creation
    - DS0011 - Module Load
    - DS0033 - Network Share Access
    - DS0029 - Network Connection Creation, Network Traffic Flow
    - DS0009 - Process Creation

  Protective controls:
    - M1032 - Multi-factor Authentication
    - M1018 - User Account Management
- T1018 - Remote System Discovery

  Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Access
    - DS0029 - Network Connection Creation
    - DS0009 - Process Creation

  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1489 - Service Stop

  Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Modification
    - DS0009 - OS API Execution, Process Creation, Process Termination
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

  Protective controls:
    - M1030 - Network Segmentation

    - M1022 - Restrict File and Directory Permissions
    - M1024 - Restrict Registry Permissions
    - M1018 - User Account Management
- T1016 - System Network Configuration Discovery
  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation
    - DS0012 - Script Execution
  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1049 - System Network Connections Discovery
  Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Creation
  Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
- T1080 - Taint Shared Content
  Detective controls:
    - DS0022 - File Creation, File Modification
    - DS0033 - Network Share Access
    - DS0009 - Process Creation
  Protective controls:
    - M1038 - Execution Prevention
    - M1050 - Exploit Protection
    - M1022 - Restrict File and Directory Permissions

Hive

- T1574.001 – Hijack Execution Flow: DLL Search Order Hijacking
  Detective controls:
    - DS0022 - File Creation, File Modification
    - DS0011 - Module Load
  Protective controls:
    - M1047 - Audit
    - M1038 - Execution Prevention
    - M1044 - Restrict Library Loading
- TA0005 – Defense Evasion
- TA0004 – Privilege Escalation
- T1486 - Data Encrypted for Impact
  Detective controls:
    - DS0010 - Cloud Storage Metadata, Cloud Storage Modification
    - DS0017 - Command Execution
    - DS0022 - File Creation, File Modification
    - DS0009 - Process Creation
  Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1053 - Data Backup
- T1027.002 – Obfuscated Files or Information: Software Packing

Detective controls:
    - DS0022 - File Metadata

Protective controls:
    - M1049 - Antivirus/Antimalware

- T1003.001 – OS Credential Dumping: LSASS Memory

Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution, Process Access, Process Creation

Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1043 - Credential Access Protection
    - M1028 - Operating System Configuration
    - M1027 - Password Policies
    - M1026 - Privileged Account Management
    - M1025 - Privileged Process Integrity
    - M1017 - User Training

- T1007 – System Service Discovery

Detective controls:
    - DS0017 - Command Execution
    - DS0009 - Process Creation

Protective controls:
    - This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

- T1059 – Command and Scripting Interpreter

Detective controls:
    - DS0017 - Command Execution
    - DS0011 - Module Load
    - DS0009 - Process Creation
    - DS0012 - Script Execution

Protective controls:
    - M1049 - Antivirus/Antimalware
    - M1040 - Behavior Prevention on Endpoint
    - M1045 - Code Signing
    - M1042 - Disable or Remove Feature or Program
    - M1038 - Execution Prevention
    - M1026 - Privileged Account Management
    - M1021 - Restrict Web-Based Content

- T1059.001 – Command and Scripting Interpreter: PowerShell

Detective controls:
    - DS0017 - Command Execution
    - DS0011 - Module Load
    - DS0009 - Process Creation
    - DS0012 - Script Execution

Protective controls:
    - M1049 - Antivirus/Antimalware
    - M1045 - Code Signing
    - M1042 - Disable or Remove Feature or Program
    - M1038 - Execution Prevention
    - M1026 - Privileged Account Management

- T1059.003 - Command and Scripting Interpreter: Windows Command Shell

Detective controls:
    - DS0017 - Command Execution
    - DS0009 - Process Creation

Protective controls:
    - M1038 - Execution Prevention

- T1490 - Inhibit System Recovery

Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Deletion
    - DS0009 - Process Creation
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

Protective controls:
    - M1053 - Data Backup
    - M1028 - Operating System Configuration

LockBit 2.0

- T1078 - Valid accounts

Detective controls:
    - DS0028 - Logon Session Creation, Logon Session Metadata
    - DS0002 - User Account Authentication

Protective controls:
    - M1013 - Application Developer Guidance
    - M1027 - Password Policies
    - M1026 - Privileged Account Management
    - M1017 - User Training

- T1562.001 - Impair defenses - disable or modify tools

Detective controls:
    - DS0017 - Command Execution
    - DS0009 - Process Termination
    - DS0013 - Host Status
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Deletion, Windows Registry Key Modification

Protective controls:
    - M1022 - Restrict File and Directory Permissions
    - M1024 - Restrict Registry Permissions
    - M1018 - User Account Management

- T1546.008 - Event-triggered execution - accessibility features

Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Creation, File Modification
    - DS0009 - Process Creation
    - DS0024 - Windows Registry Key Modification

Protective controls:
    - M1038 - Execution Prevention
    - M1035 - Limit Access to Resource Over Network
    - M1028 - Operating System Configuration

- T1070.001 - Indicator removal on host - clear Windows Event Logs

Detective controls:
    - DS0017 - Command Execution
    - DS0009 - OS API Execution

Protective controls:
    - M1041 - Encrypt Sensitive Information
    - M1029 - Remote Data Storage
    - M1022 - Restrict File and Directory Permissions

- T1041 - Exfiltration Over C2 Channel

Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Access
    - DS0029 - Network Connection Creation, Network Traffic Content, Network Traffic Flow

Protective controls:
    - M1057 - Data Loss Prevention
    - M1031 - Network Intrusion Prevention

- T1486 - Data Encrypted for Impact

Detective controls:
    - DS0010 - Cloud Storage Metadata, Cloud Storage Modification
    - DS0017 - Command Execution
    - DS0022 - File Creation, File Modification
    - DS0009 - Process Creation

Protective controls:
    - M1040 - Behavior Prevention on Endpoint
    - M1053 - Data Backup

- T1489 - Service Stop

Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Modification
    - DS0009 - OS API Execution, Process Creation, Process Termination
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

Protective controls:
    - M1030 - Network Segmentation
    - M1022 - Restrict File and Directory Permissions
    - M1024 - Restrict Registry Permissions
    - M1018 - User Account Management

- T1490 - Inhibit System Recovery

Detective controls:
    - DS0017 - Command Execution
    - DS0022 - File Deletion
    - DS0009 - Process Creation
    - DS0019 - Service Metadata
    - DS0024 - Windows Registry Key Modification

Protective controls:
    - M1053 - Data Backup
    - M1028 - Operating System Configuration

Other Threat Actors

APT10

- T1087.002 - Account Discovery: Domain Account
- T1583.001 - Acquire Infrastructure: Domains
- T1560 - Archive Collected Data
- T1560.001 - Archive via Utility
- T1119 - Automated Collection
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1005 - Data from Local System
- T1039 - Data from Network Shared Drive
- T1074.001 - Data Staged: Local Data Staging
- T1074.002 - Data Staged: Remote Data Staging
- T1140 - Deobfuscate/Decode Files or Information
- T1568.001 - Dynamic Resolution: Fast Flux DNS
- T1190 - Exploit Public-Facing Application
- T1210 - Exploitation of Remote Services
- T1083 - File and Directory Discovery
- T1574.001 - Hijack Execution Flow: DLL Search Order Hijacking
- T1574.002 - Hijack Execution Flow: DLL Side-Loading
- T1070.003 - Indicator Removal on Host: Clear Command History
- T1070.004 - Indicator Removal on Host: File Deletion
- T1105 - Ingress Tool Transfer
- T1056.001 - Input Capture: Keylogging
- T1036 - Masquerading
- T1036.003 - Rename System Utilities
- T1036.005 - Match Legitimate Name or Location
- T1106 - Native API
- T1046 - Network Service Scanning
- T1027 - Obfuscated Files or Information
- T1588.002 - Obtain Capabilities: Tool
- T1003.002 - OS Credential Dumping: Security Account Manager

- T1003.003 - OS Credential Dumping: NTDS
- T1003.004 - OS Credential Dumping: LSA Secrets
- T1566.001 - Phishing: Spearphishing Attachment
- T1055.012 - Process Injection: Process Hollowing
- T1090.002 - Proxy: External Proxy
- T1021.001 - Remote Services: Remote Desktop Protocol
- T1021.004 - Remote Services: SSH
- T1018 - Remote System Discovery
- T1053.005 - Scheduled Task/Job: Scheduled Task
- T1218.004 - Signed Binary Proxy Execution: InstallUtil
- T1553.002 - Subvert Trust Controls: Code Signing
- T1016 - System Network Configuration Discovery
- T1049 - System Network Connections Discovery
- T1199 - Trusted Relationship
- T1204.002 - User Execution: Malicious File
- T1078 - Valid Accounts
- T1047 - Windows Management Instrumentation

AvosLocker

- T1486 - Data Encrypted for Impact
- T1083 - File and Directory Discovery
- T1018 - Remote System Discovery
- T1490 - Inhibit System Recovery

Grief

- T1486 - Data Encrypted for Impact
- T1083 - File and Directory Discovery
- T1018 - Remote System Discovery
- T1543.003 - Create or Modify System Process: Windows Service

Lazarus

- T1134.002 - Access Token Manipulation: Create Process with Token
- T1098 - Account Manipulation

- T1583.001 - Acquire Infrastructure: Domains
- T1583.006 - Acquire Infrastructure: Web Services
- T1071.001 - Application Layer Protocol: Web Protocols
- T1010 - Application Window Discovery
- T1560 - Archive Collected Data
- T1560.002 - Archive via Library
- T1560.003 - Archive via Custom Method
- T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1547.009 - Boot or Logon Autostart Execution: Shortcut Modification
- T1110.003 - Brute Force: Password Spraying
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1543.003 - Create or Modify System Process: Windows Service
- T1485 - Data Destruction
- T1132.001 - Data Encoding: Standard Encoding
- T1005 - Data from Local System
- T1001.003 - Data Obfuscation: Protocol Impersonation
- T1074.001 - Data Staged: Local Data Staging
- T1491.001 - Defacement: Internal Defacement
- T1587.001 - Develop Capabilities: Malware
- T1561.001 - Disk Wipe: Disk Content Wipe
- T1561.002 - Disk Wipe: Disk Structure Wipe
- T1189 - Drive-by Compromise
- T1573.001 - Encrypted Channel: Symmetric Cryptography
- T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
- T1041 - Exfiltration Over C2 Channel
- T1203 - Exploitation for Client Execution
- T1008 - Fallback Channels
- T1083 - File and Directory Discovery
- T1564.001 - Hide Artifacts: Hidden Files and Directories
- T1562.001 - Impair Defenses: Disable or Modify Tools
- T1562.004 - Impair Defenses: Disable or Modify System Firewall
- T1070.004 - Indicator Removal on Host: File Deletion
- T1070.006 - Indicator Removal on Host: Timestomp

- T1105 - Ingress Tool Transfer
- T1056.001 - Input Capture: Keylogging
- T1036.005 - Masquerading: Match Legitimate Name or Location
- T1571 - Non-Standard Port
- T1027 - Obfuscated Files or Information
- T1588.004 - Obtain Capabilities: Digital Certificates
- T1566.001 - Phishing: Spearphishing Attachment
- T1542.003 - Pre-OS Boot: Bootkit
- T1057 - Process Discovery
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1090.002 - Proxy: External Proxy
- T1012 - Query Registry
- T1021.001 - Remote Services: Remote Desktop Protocol
- T1021.002 - Remote Services: SMB/Windows Admin Shares
- T1489 - Service Stop
- T1218.001 - Signed Binary Proxy Execution: Compiled HTML File
- T1082 - System Information Discovery
- T1016 - System Network Configuration Discovery
- T1033 - System Owner/User Discovery
- T1529 - System Shutdown/Reboot
- T1124 - System Time Discovery
- T1204.002 - User Execution: Malicious File
- T1047 - Windows Management Instrumentation

TA505

- T1087.003 - Account Discovery: Email Account
- T1071.001 - Application Layer Protocol: Web Protocols
- T1059.001 - Command and Scripting Interpreter: PowerShell
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1059.005 - Command and Scripting Interpreter: Visual Basic
- T1059.007 - Command and Scripting Interpreter: JavaScript
- T1555.003 - Credentials from Password Stores: Credentials from Web Browsers
- T1486 - Data Encrypted for Impact
- T1568.001 - Dynamic Resolution: Fast Flux DNS

- T1105 - Ingress Tool Transfer
- T1559.002 - Inter-Process Communication: Dynamic Data Exchange
- T1027 - Obfuscated Files or Information
- T1027.002 - Software Packing
- T1069 - Permission Groups Discovery
- T1566.001 - Phishing: Spearphishing Attachment
- T1566.002 - Phishing: Spearphishing Link
- T1055.001 - Process Injection: Dynamic-link Library Injection
- T1218.007 - Signed Binary Proxy Execution: Msiexec
- T1218.011 - Signed Binary Proxy Execution: Rundll32
- T1553.002 - Subvert Trust Controls: Code Signing
- T1553.005 - Subvert Trust Controls: Mark-of-the-Web Bypass
- T1552.001 - Unsecured Credentials: Credentials In Files
- T1204.001 - User Execution: Malicious Link
- T1204.002 - User Execution: Malicious File
- T1078.002 - Valid Accounts: Domain Accounts

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 10,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on LinkedIn or Twitter.