Threat Highlights Report

July 2022

WITH secure

Contents

Foreword

This month’s threat highlights report contains a look at the ongoing war in Ukraine and how the Trickbot group is systematically attacking the nation, most likely under the direction of Russian intelligence services. We also look at the use of the adversary attack simulation tool Brute Ratel by threat actors, as well as the capability and victimology of ransomware newcomers Black Basta.

The ransomware section this month longer than in recent times due to a large uptick in ransomware activity, especially from newcomers BlackCat and Black Basta, and a noticeable shift in the use of Rust as a programming language.

We also take a brief look at a number of issues, including a targeted campaign of DDoS attacks on Norway and an attack impersonating cybersecurity companies.

1 Monthly highlights

1.1 Trickbot group attack Ukraine

Researchers from Security Intelligence tracked a campaign that appears to show the Trickbot group targeting the people, military, and government of Ukraine. The group, which is a cybercrime outfit, with strong connections to ransomware groups such as Ryuk, Conti, and Diavol is known to be sympathetic to Russia and may have stronger connections to the nation.

Since April 2022 the group has been attributed carrying out attacks on Ukraine, only a couple of months after the start of the invasion. These attacks involve common Trickbot tactics, techniques and procedures (TTPs) such as the use of phishing, malicious office documents, the use of .ISO files, and delivery of malware such as IcedID and AnchorMail, accompanied by usage of attack frameworks such as CobaltStrike and Metasploit.

WithSecure™ Insight

While the name Trickbot is used to identify a specific trojan, it is also the name of the organization and criminal network behind the malware's development and deployment. The group are tracked by various other identities including WIZARD SPIDER, UNC2727, Gold Ulrick and ITG23, and are best described as a highly sophisticated and eminent financially motivated cybercriminal network. From the ContiLeaks incident, we know that there is a strong connection between Trickbot and other threat actors, including Conti, Diavol, Emotet and Karakurt, all of whom appear to be Russian-language groups who are sympathetic to the Russian-state.

The campaign tracked by Security Intelligence demonstrates a shift in the group's behavior, as the group previously avoided attacks in Ukraine and other former Soviet nations. Other than the shift in victimology, these attacks fall well within the known TTPs of Trickbot, with a focus on gaining initial access through phishing, malicious office documents and more recently the use of alternative malicious file types such as .ISO files. Later stages of the attack-chain include deployment of malware known to be in the Trickbot arsenal, including IcedID and AnchorMail (AnchorDNS). Of note, the lures used in these attacks are related to the war in Ukraine or nexus-topics, and this is likely an opportunistic tactic designed to improve victim engagement.

Trickbot are ordinarily financially motivated and in recent years were focused on the deployment of ransomware. These attacks are clearly influenced by the war in Ukraine, and are instead focused on causing disruption, damage and chaos for Ukrainian citizens, organizations and authorities. It is highly likely that these attacks have been carried out pursuant to the interests of the Russian intelligence services and military, whether this is via direct request or because of patriotic duty, is unknown.

The TTPs utilized by Trickbot are well-known and defenses include the use of antivirus and endpoint protection products, as well as providing users with education surrounding common initial access vectors such as phishing, and common malicious file types.

1.2 Brute Ratel being abused by threat actors

On July 5th, researchers from Palo Alto's Unit 42 published a threat advisory on the malicious usage of a new red team and adversary attack simulation tool called Brute Ratel created by former Mandiant and CrowdStrike employee Cheten Nayak under his brand Dark Vortex.

Dark Vortex describe Brute Ratel as:

"...the most advanced Red Team & Adversary Simulation Software in the current C2 Market. It can not only emulate different stages of an attacker killchain, but also provide a systematic timeline and graph for each of the attacks executed to help the Security Operations Team validate the attacks and improve the internal defensive mechanisms.

Functionality of Brute Ratel is listed as including:

- SMB and TCP payloads provide functionality to write custom external C2 channels over legitimate websites such as Slack, Discord, Microsoft Teams and more
- Built-in debugger to detect EDR userland hooks
- Ability to keep memory artifacts hidden from EDRs and AV
- Direct Windows SYS calls on the fly
- Patching Event Tracing for Windows (ETW)
- Patching Anti Malware Scan Interface (AMSI)

Unit 42's analysis focuses on an ISO file that was likely delivered to a target through phishing. When mounted this ISO file contains a LNK files disguised as a MS Office Word document, and hidden executable and .dll files. This technique has been adopted by a number of threat actors but is commonly associated with tradecraft linked to the Russian intelligence services.

Sophos have also released a report regarding an investigation into 5 instances of BlackCat ransomware being deployed, with Brute Ratel being installed by the attackers as a Windows service named "wewe". An alarming development considering BlackCat is already a high-profile and sophisticated ransomware group, despite its infancy.

WithSecure™ Insight

Red-team and adversary attack simulation tools like Cobalt Strike and Metasploit have long been abused by threat actors, seeking to streamline and simplify their attack process. It provides them with a well-designed system to embed in a network and issue C2 commands over long periods, often in a very covert way. As a result, defenders and cybersecurity companies have developed detection rules and defenses to detect these tools, making them less effective and hampering threat actors' attacks. It is no surprise then, that new tools like Brute Ratel, which is designed from the outset to bypass antivirus and endpoint protection are being used by threat actors seeking to gain the upper hand.

While the attacks using Brute Ratel analyzed by Unit 42 and Sophos are alarming, they are currently a very small proportion of what occurs across the threat landscape, which typically involves more traditional tooling. These incidents should be viewed as opportunities to gain intelligence and a better understanding of these novel threats, allowing the cybersecurity community the opportunity to better improve our products and improve our clients' defenses.

1.3 Black Basta on the rise

Relative newcomers Black Basta, who started operations in April and have quickly proven themselves to be capable, are believed to be expanding their TTPs by making use of the QBot trojan and exploiting the PrintNightmare vulnerability in Windows. Trend Micro is reporting on the group's activities and the group's new use of QBot, a malware family previously associated with other ransomware operators such as Egregor and REvil. While QBot is a veteran cyber threat, existing since 2007, it has been continually updated and recently added the Follina (CVE-2022-30190) exploit to its initial access arsenal. Despite this, QBot is still primarily delivered via phishing, and standard phishing mitigations remain the best line of defense.

WithSecure™ Insight

Black Basta has only recently emerged as a threat but has quickly dominated the ransomware landscape, quickly becoming the third most prevalent ransomware variant in Q2. This has led to some speculation that the group is a rebrand or evolution of a former one, most notably Conti. This is due to some similarities between the group's onion website and their language/behavior. Evidence also shows that the group's infrastructure has been in development since at least February, the same month ContiLeaks occurred and Conti began plans to dismantle and rebrand its operations. Despite this, Conti directly disputed the claim, stating "Black Basta are f****** kids", it is possible that Black Basta is made up of a few former Conti members, while others have gone on to other groups such as Diavol, Karakurt, and Black Matter a theory that is backed up by covert intelligence gained in May.

On the surface Black Basta is operating a standard double-extortion ransomware operation, infiltrating targets, stealing data and encrypting everything, and then demanding ransom. However, the group's recent shift to using QBot for initial access and as a dropper for other tools/malware indicates their standing in the cybercriminal underworld. QBot is normally associated with former big players like Egregor and REvil, and its usage by Black Basta is indicative of their substantial infrastructure and sophistication. Analysis of Black Matter has provided insight into their attack process:

Tactic	Technique
Initial Access	T1566 Phishing
	T1078 Valid Accounts
Lateral Movement	T1021 Remote Services
	T1080 Taint Shared Content
Execution	T1059 PowerShell
	T1053 Scheduled Task/Job
Persistence	T1053 Scheduled Task/Job
Defence Evasion	T1562 Impair Defenses
Credential Access	T1555 Password Stores
Discovery	T1087 Account Discovery
	T1082 System Info Discovery
	T1083 File & Directory Discovery
	T1614 System Location Discovery
Collection	T1005 Data from System
Exfiltration	T1020 Automated Exfiltration
Impact	T1490 Inhibit System Recovery
	T1486 Data Encrypted for Impact

Black Basta have already proven themselves a formidable threat and their switch to utilizing QBot shows their motivation to attack as many targets as possible. It is highly likely that Black Basta will continue to grow throughout the coming weeks and months, with further victims targeted.

A post by Black Basta on Russian Language hacker forums indicates their victimology is limited to companies in the USA, Canada, UK, Australia, and New Zealand, but not limited to a specific sector.

Pre-existing detections for QBot, as well as training surrounding phishing and malicious file types, are likely to thwart the initial access stage of Black Basta attacks, except for in instances of access via valid accounts. Once in, Black Basta makes use of common hands-on attack methodologies, including the use of PowerShell, and common tools like Cobalt Strike and Coroxy which can often be detected by endpoint protection systems. In cases of compromise, prompt isolation of the host is paramount, as well as commencing incident response playbooks as appropriate.

2 Ransomware: Trends and notable reports

2.1 BlackCat under the spotlight

BlackCat (aka ALPHV) are relative newcomers to the ransomware-as-as-service (RasS) landscape but have quickly become a prevalent threat. With a locker written in Rust and TTPs and toolkits which rarely overlap with their ransomware brethren, the group shows resourcefulness and a unique approach that has landed them several high-profile victims, but also a lot of attention, from both the cybersecurity community and government/law enforcement. AdvIntel has recently released a report on BlackCat which looks at the group's history, attack methodologies, and code, which provides a good insight into how the group operates. Microsoft has also recently released an analysis on BlackCat providing defenders a close look at the group's TTPs and capabilities. Further analysis by Resecurity has also examined the group's infrastructure, TTPs, and ransom demand history, which it notes has recently increased in value to around $2.5 million Sophos have also released a report on 5 BlackCat attacks, with some involving the use of Brute Ratel.

2.2 Vice Society

Despite being barely a year old, the ransomware group Vice Society has become a prolific threat actor, positing victim data to their leak site on an almost weekly basis, suggesting the group is proactive and consistently attacking organizations. Sekoia released a blog post on the group's activities, with a specific focus on victimology, which is limited to the Americas and West Europe. But also includes some IoCs and YARA rules, which may prove useful to defenders.

2.3. A closer look at LockBit 3.0

It seems that each month we have an update or further analysis on the LockBit group, which post-Conti could be described as the market leader in ransomware. LockBit is a highly sophisticated group, who have recently updated its locker and branding to version 3.0. Cluster 25 has released an analysis of this new version, drawing comparisons between this new variant and BlackMatter, LockBit is calling its new version “LockBit Black” giving further evidence of a connection between those groups.

2.4 Hive joins BlackCat in using Rust

Hive, whose locker was previously written in Go has switched to a variant written in the Rust programming language. The majority of ransomware is written in C-languages, but some have recently shifted to more exotic languages like Rust, likely as a defense evasion tactic. Microsoft's Threat Intelligence Centre (MSTIC) has taken a look at this new Hive variant, along with an analysis of some samples, and provides some advice regarding mitigation and a list of IOCs. This switch means Hive is joining BlackCat and newcomers Luna in using Rust. We are also likely to see more malware being written in exotic languages to avoid detection and allow easier porting to target other platforms.

Unfortunately for the group, excellent work has been carried out by analysts and researchers, and a keystream decryptor has been publicly released for this Rust-based variant via GitHub.

2.5 CISA produce alert on MedusaLocker

CISA has produced an alert on the ransomware variant MedusaLocker. The alert contains a wealth of technical details surrounding the group and their TTPs, as well as a long list of IOCs and general mitigation advice. MedusaLocker is known to gain initial access through the exploitation of vulnerable RDP instances and operate a standard RaaS model.

2.6 HavanaCrypt, a new group with novel tactics

Researchers from Trend Micro have uncovered and analyzed a new ransomware variant called HavanaCrypt. The malware is a .NET-compiled application disguised as a Google software update and uses a Microsoft web hosting service as its C2, a tactic designed to prevent detection of malicious traffic, as this IP is unlikely to be blacklisted. The team at Trend Micro also notes how the ransomware abuses legitimate tools provided by KeePass as part of its encryption phase and predicts that the locker is still in its development phase.

2.7 Q2 statistics from Digital Shadows

Digital Shadows have produced a Q2 report on the ransomware landscape, the content looks at the most prevalent ransomware groups, and their victimology, including the sectors and nations, attacked most often. It’s noteworthy that veterans such as LockBit and Conti led the activity leaderboard in Q2 but were chased by relative newcomers such as BlackCat (ALPHV) and Black Basta, showing the prevalence and capability of these new groups.

3 Other notable highlights in brief

3.1 Microsoft delay VBA macro block

Back in February Microsoft announced that they would begin to block VBA macros in office documents by default, with the change planned for between April and June. The decision was welcomed across the IT and cyber industry, as VBA macros are a common delivery route for executing malware contained within malicious office documents. Unfortunately, Microsoft is rolling back this plan, quoting "user feedback" as the reason and describing this stall as "temporary".

This is unfortunate, as the action would have likely resulted in a noticeable decrease in initial access attack vectors and forced threat actors to change their TTPs; as they could no longer rely upon VBA macros, and were instead using other file types and infection vectors to gain initial access/execute code. At the time of writing, there is no word from Microsoft of when the plan will be reimplemented, but for now, we recommend organizations block VBA macro usage across their estate, as appropriate, using group policy settings, as well as educating users regarding the dangers that macros can present. This change has not altered Microsoft's decision to block XLM macros by default.

3.2 Denial of service attack targets Norwegian websites

At the end of June, Norwegian authorities reported a coordinated DDoS attack on several websites, noting that defenses were quickly raised and normal operations quickly resumed. The NSM is blaming pro-Russian criminal groups for the attacks and a group calling themselves DeaDNet claimed responsibility, who join a growing list of so-called hacktivist groups of questionable provenance such as Killnet and Xaknet. These groups have carried out similar attacks against Lithuania, Germany, Italy, and Romania in what is likely a proxy campaign carried out by Russia.

3.3 Attack impersonates cyber security companies

Researchers at CrowdStrike uncovered a campaign that involves the impersonation of prominent cybersecurity companies. The attacks involve fake communications, which include an attacker-controlled phone number requesting the target to call them urgently. CrowdStrike suspects that these phishing attempts are followed up with complex social engineering tactics, over-the-phone, requesting a target employee to install a remote access tool or malware, allowing the attacker access to the host.

Currently, the attacker has not been identified, but similar TTPs were previously attributed to Trickbot (WIZARD SPIDER), though complex social engineering is a tactic used by a myriad of threat actors from both financially motivated and nation-state backgrounds.

WithSecure™ (or F-Secure) are not believed to be a part of this campaign but would never contact customers in this way. All communications between our customers occurs through pre-organized channels. If you doubt the authenticity of any communication you receive, please contact your security provider directly.

3.4 1 billion records of Chinese citizens are leaked

A suspected hacker going by the username “ChinaDan” has reportedly offered the records of around 1 billion Chinese citizens for sale on a criminal marketplace. The post states that the records come from a leaked database belonging to the Shanghai National Police and consists of around 23TB of data. Zhao Changpeng of Binance suggested that the leak could be a result of a developer accidently leaking credentials as part of a blog post/research piece, highlighting the importance of sanitization when publicly publishing content. Whilst the leak itself is alarming, perhaps the larger issue is the fact that the police were storing data on so many of China’s citizens, highlighting the far reach of the surveillance state.

3.5 FBI issues warning over deepfake tactics

The US Department of State, Department of Treasury and FBI previously reported on the TTPs used by North Korean threat actors, in order to embed covert human assets within western organizations. This activity is alleged to be a campaign designed to generate revenue for the nation, as well as being a useful tool for gaining initial access into targeted organizations.

A further publication issued by the FBI discussed a tactic used by threat actors to gain unlawful employment in target organizations, which includes the use of deepfake videos and voice spoofing. While North Korea is not mentioned in this report, the activity is likely related due to the overlap in TTPs involved. The alert states the bureau received a number of complaints regarding applicants using stolen PII to apply for jobs, and video/voice interviews being conducted using deepfake video or overdubbing of voices, in an effort to fool panelists as to the identity/nationality of the candidate.

This activity is certainly unusual and particularly brazen, and something employers should be mindful of when carrying out remote interviews. As deepfake technology improves and becomes more widely available, it is highly likely that similar tactics will be used for similar objectives and may become more convincing and harder to detect.

4 Threat data highlights

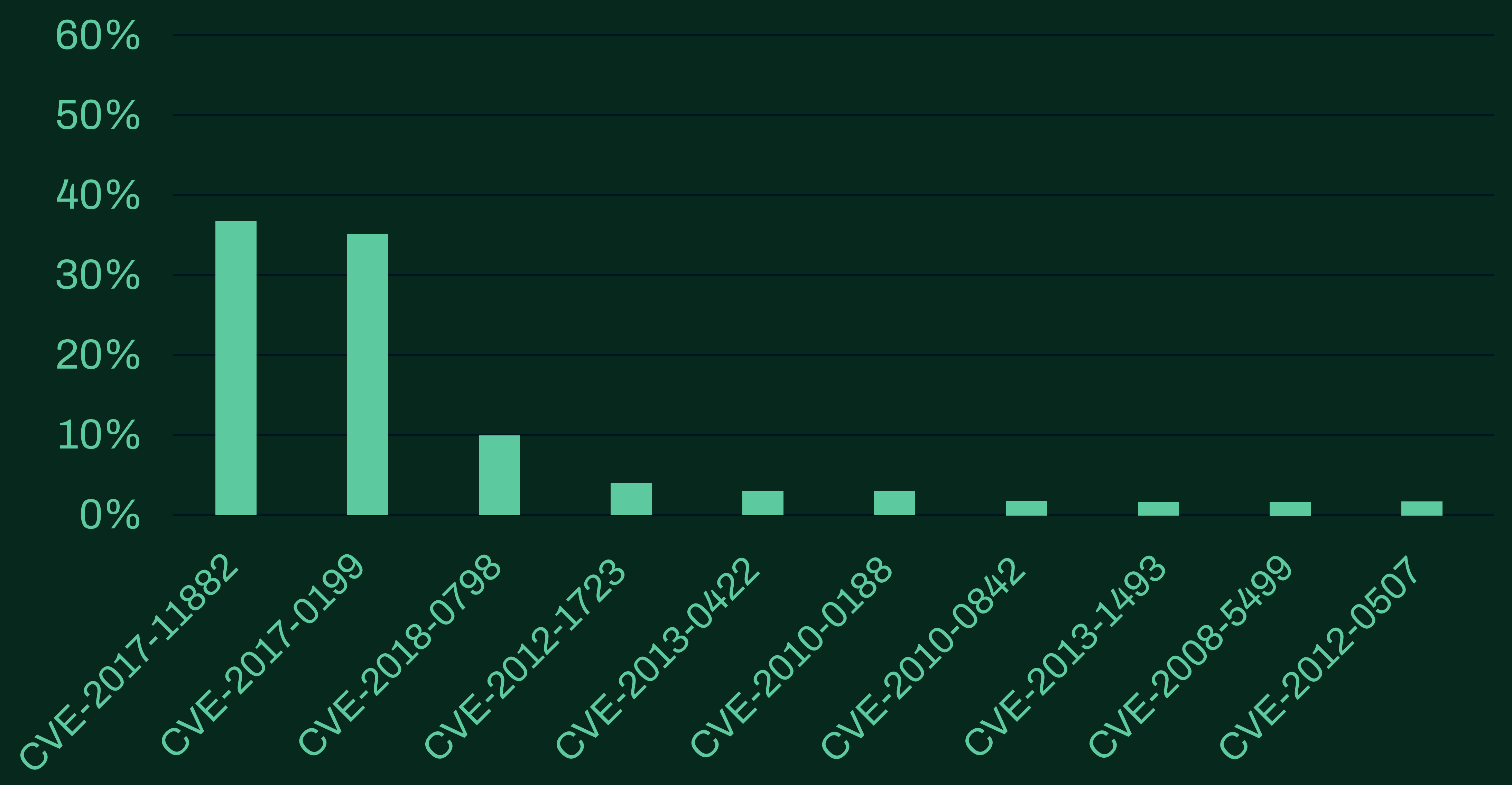
4.1 Exploits

CVE-2017-11882 is a vulnerability in MS office products and provides remote code execution for the attacker, it is exploited by malicious office documents.

CVE-2017-0199 is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted RTF document.

CISA have added 2 new vulnerabilities to their known exploitation list this month, CVE-2022-22047 and CVE-2022-2625, which both exist in Microsoft Windows.

Exploits in the wild



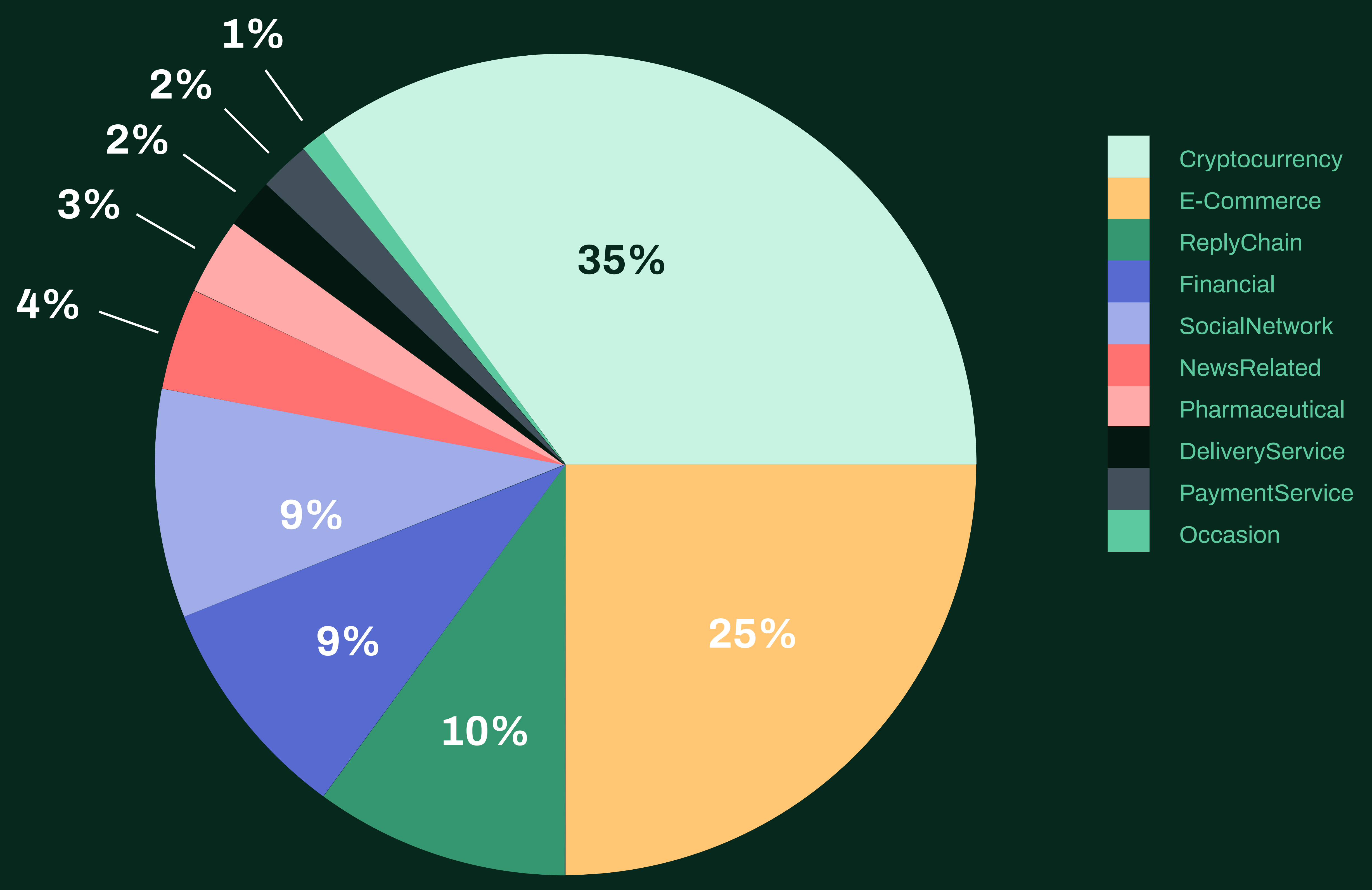
WithSecure™ endpoint protection

4.2 Email threats

Cryptocurrency-themed emails continue to dominate the spam landscape this month, likely due to the continued volatility of the crypto markets.

E-Commerce and ‘reply-chain’ (where attackers insert themselves into legitimate conversation with stolen credentials) style email threats also continue to score highly.

Spam Email themes



WithSecure™ spam data collection

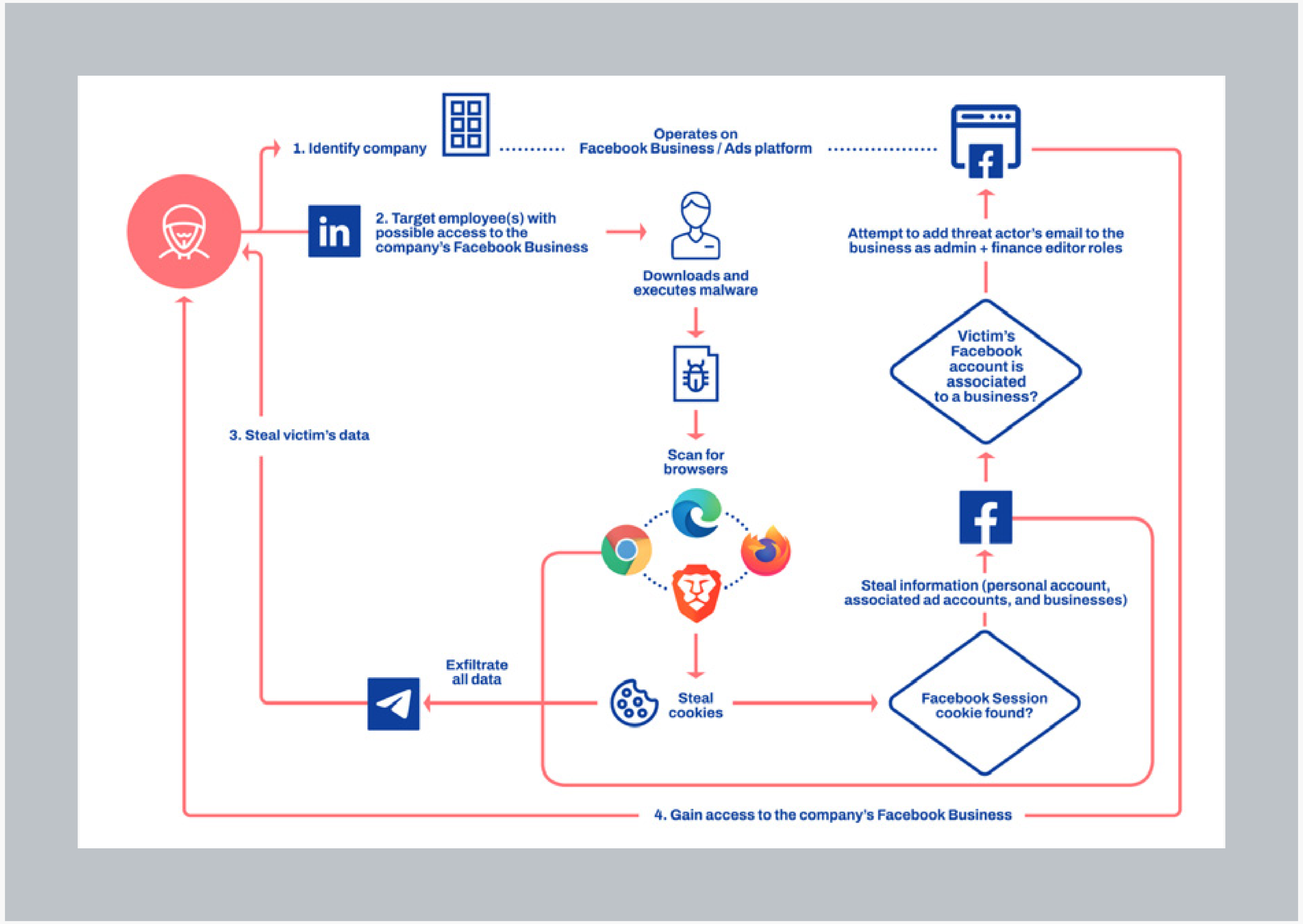
5 Research highlights

5.1 Ducktail: An infostealer malware targeting Facebook business accounts

WithSecureTM Intelligence tracked an operation dubbed "DUCKTAIL" that targets individuals and organizations that operate on Facebook's Business/Ads platform.

The operation consists of a malware component, which performs information stealing as well as Facebook Business hijacking. Based upon analysis and gathered data, we have determined that the operation is conducted by a Vietnamese threat actor.

Our investigation reveals that the threat actor has been actively developing and distributing malware linked to the DUCKTAIL operation since the latter half of 2021. Evidence suggests that the threat actor may have been active in the cybercriminal space as early as late 2018.


1. Identify company
Operates on Facebook Business / Ads platform
2. Target employee(s) with possible access to the company's Facebook Business
Downloads and executes malware
Scan for browsers
Steal cookies
Exfiltrate all data
3. Steal victim's data
Facebook Session cookie found?
Steal information (personal account, associated ad accounts, and businesses)
Victim's Facebook account is associated to a business?
Attempt to add threat actor's email to the business as admin + finance editor roles
4. Gain access to the company's Facebook Business

The full research on Ducktail, by Mohammad Kazem Hassan Nejad is available here

Delivery mechanism and victimology

Based on telemetry and investigation conducted by WithSecure™, one approach employed by the threat actor is to scout for companies that operate on Facebook's Business/ Ads platform and directly target individuals within the company/business that might have high-level access to the Facebook Business. We have observed individuals with managerial, digital marketing, digital media, and human resources roles in companies to have been targeted. The WithSecure™ Countercept Detection and Response team identified instances where the malware was delivered to victims through LinkedIn. These tactics would increase the adversary's chances of compromising the respective Facebook Business all the while flying under the radar.

The malware

Since late 2021, samples associated with the DUCKTAIL operation were exclusively written in .NET Core and were compiled using its single file feature. This feature bundles all dependent libraries and files into a single executable, including the main assembly. The usage of .NET Core and its single-file feature is not commonly seen in malware.

The purpose of the malware is to scan the victim's machine for browsers (Chrome, Edge, Brave, Firefox) and extract stored cookies, including any Facebook session cookies.

The full research on Ducktail, by Mohammad Kazem Hassan Nejad is available here

Motivation

The information stolen by Ducktail includes personal account information (name, email, birthday, user ID) and also any information relating to any Facebook business pages associated with the personal account (name, verification status, ad account limit, users, clients, etc), along with the associated ad account data.

One of the unique features of the malware is its ability to hijack Facebook Business accounts associated with the victim's Facebook account. It attempts to grant the threat actor's emails access to the business with the highest privilege roles.

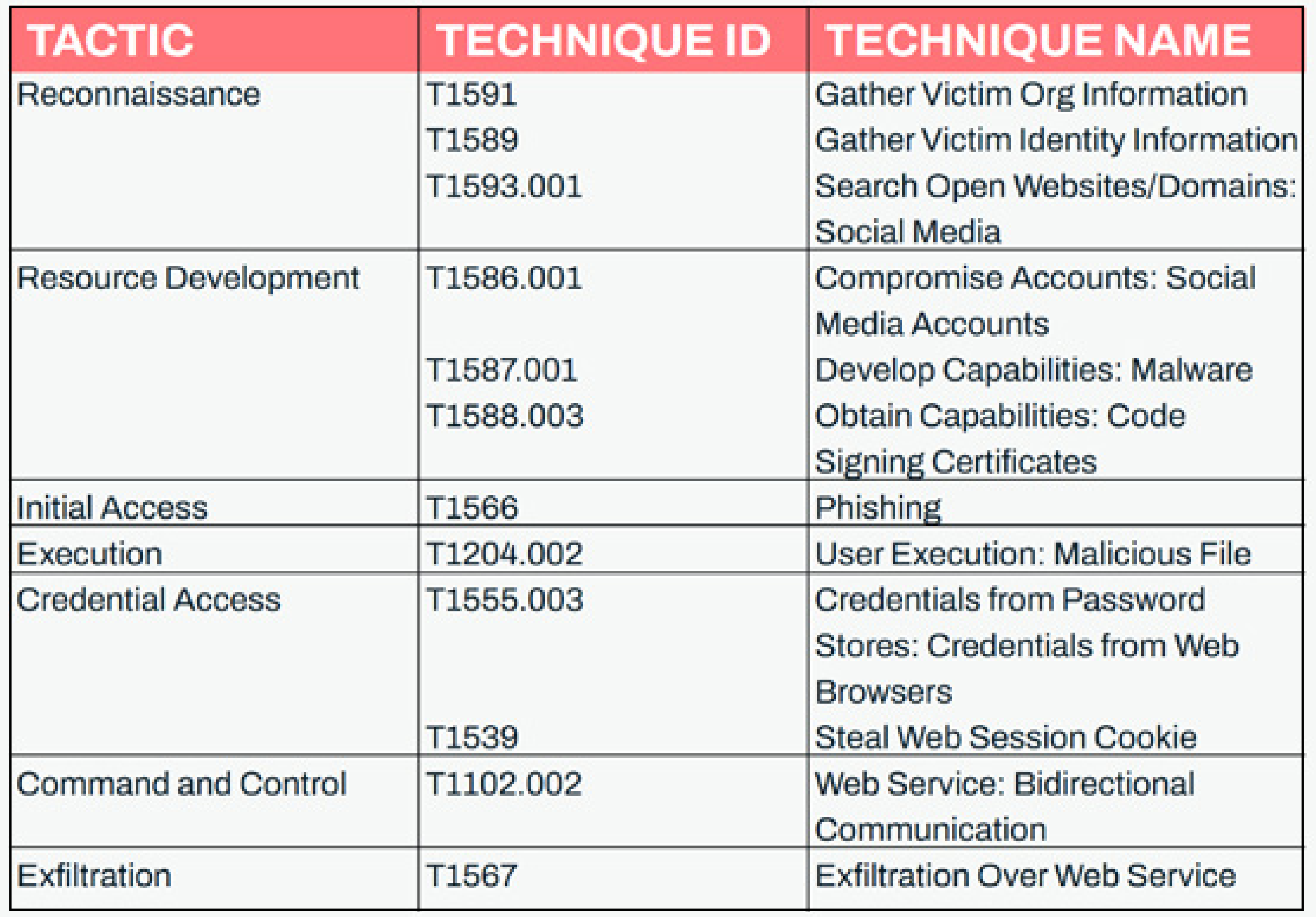
Mitigation

WithSecure™ Endpoint protection offers multiple detections that detect the malware and its behavior.

Our products currently offer the following detections for the malware:

- Trojan:W32/DuckTail.*
- Trojan:W32/SuspiciousDownload.A!DeepGuard
- Trojan:W32/WindowsDefenderExclusion.A!DeepGuard
- Malicious certificate blocking

MITRE ATT&CK Techniques



TACTIC	TECHNIQUE ID	TECHNIQUE NAME
Reconnaissance	T1591 T1589 T1593.001	Gather Victim Org Information Gather Victim Identity Information Search Open Websites/Domains: Social Media
Resource Development	T1586.001 T1587.001 T1588.003	Compromise Accounts: Social Media Accounts Develop Capabilities: Malware Obtain Capabilities: Code Signing Certificates
Initial Access	T1566	Phishing
Execution	T1204.002	User Execution: Malicious File
Credential Access	T1555.003 T1539	Credentials from Password Stores: Credentials from Web Browsers Steal Web Session Cookie
Command and Control	T1102.002	Web Service: Bidirectional Communication
Exfiltration	T1567	Exfiltration Over Web Service

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure