Threat Highlights Report

August 2022

WITH secure

Contents

Foreword

This month's threat highlights report contains a look at the top malware strains of 2021 according to CISA, a look at supply chain attacks with incidents at Twilio and Mailchimp highlighting the danger of third-party providers, and Microsoft's observations of a threat actor called Callisto, who were first observed by WithSecure™ back in 2015.

As always we examine the ransomware threat landscape, including an excellent report by ENISA which maps out a year's worth of ransomware data, as well as covering research on initial access brokers, newcomers SolidBit and also SANS' ransomware summit.

We also take a brief look at a number of issues, including a new attack framework called Manjusaka, the theft of one-time passes, a private-sector offensive actor called DSIRF and the collation and analysis of multiple blockchain/crypto incidents by SlowMist.

1 Monthly highlights

1.1 Top malware strains of 2021

The United States (US) Cybersecurity and Infrastructure Security Agency (CISA) have released a joint security advisory outlining the top malware strains from 2021. In a general overview, CISA describes the top malware types as being:

- Remote Access Trojans (RATs)
- Banking Trojans
- Information Stealers, and
- Ransomware

The advisory goes on to provide specific insight into the malware strains, which it assesses as being the top for 2021, the list includes:

- Agent Tesla
- AZORult
- Formbook
- Ursnif
- Lokibot
- MOUSEISLAND
- Nanocore
- Qakbot
- Remcos
- Trickbot,
- Gootloader

CISA points out that these malware variants have all been in use and development for at least 5 years, with Ursnif and Qakbot having been around for over a decade. CISA comments that threat actors' preference for well-known malware "*offers organizations opportunities to better prepare, identify, and mitigate attacks from these known malware strains*".

The advisory provides detail on each of the identified malware strains, including an overview, the common delivery methods utilized by threat actors, as well as further resources, such as MITRE ATT&CK frameworks. CISA have also included a list of mitigations that are valuable to defenders, regardless of the type of threat they may face, which includes:

- Updating software
- Enforcing multi-factor authentication (MFA)
- Securing and monitoring Remote Desktop Protocol (RDP) and other "risky" services
- Making offline backups of data
- Providing end-user awareness and training

The report also includes an appendix of Snort detection signatures for each of the identified malware strains which may be valuable to defenders.

WithSecure™ Insight

CISA is recognized as an excellent source of information and intelligence, and their reports regularly appear within WithSecure's monthly Threat Highlight Report's. This advisory is co-authored with the Australian Cyber Security Centre (ACSC), but unusually there is no detail on how CISA or ACSC assessed which malware strains were the "top" in 2021, such as prevalence, harm, or a matrix/combination of factors. Regardless, the highlighted strains were indeed prevalent throughout 2021 and continue to be so and the overview, methods of delivery and mitigations provided are accurate and valuable.

Of note is CISA's observation that the major users of the highlighted malware strains are financially motivated cyber-criminals, rather than state-back threat actors. An important point, because this accounts for the overwhelming majority of hostile activity which defenders will face, and should be a priority for all organizations, though state-backed threats are indeed a real risk for many, especially those dealing with intellectual property, critical national infrastructure, and military/political interests.

WithSecure's proprietary data suggests the top malware strains of 2020-2021, based purely on prevalence were:

1. Lokibot
2. Formbook
3. Remcos
4. Trojans (generic)
5. Agent Tesla
6. Emotet
7. Ave Maria
8. Trickbot
9. Ransomware (all variants)
10. Qakbot

1.2 Mailchimp and Twilio incidents highlight the supply chain issue

On the 7th of August automated communications provider Twilio reported that some of its employee's credentials had been compromised by what it described as a "complex social engineering attack", which had then been abused to access internal Twilio tools and further access customer data. It is believed that the initial attack involved SMS-phishing (smishing) which led to credential harvesting pages.

Twilio are a third-party service provider for a vast array of clients, and Okta, Signal, Cloudflare and DoorDash have all reported follow-up activity related to the Twilio breach. This includes their customers being contacted via smishing, theft of one-time passes (discussed later in this report), and the addition of attacker-controlled devices to trusted device lists.

Twilio have said:

"*Trust is paramount at Twilio, and we recognize that the security of our systems and network is an important part of earning and keeping our customers' trust. As we continue our investigation, we are communicating with impacted customers to share information and assist in their own investigations. We will update this blog with more information as it becomes available*".

On the 12th of August the marketing and email automation provider Mailchimp announced that it had been the target and victim of a "social engineering" attack which had led to the compromise of one of its internal tools and that the resultant malicious activity had affected 214 Mailchimp accounts.

Mailchimp have stated that the attack was a targeted campaign against their "crypto-related users", with no mention of specific clients. One Mailchimp user who has gone public is cloud infrastructure provider DigitalOcean, who released a public statement regarding the compromise of their Mailchimp account. DigitalOcean state that some of their customers email addresses were exposed, and accounts had been attacked through threat actor initiated password reset attempts, with DigitalOcean stating:

"*Our internal logging indicated the attacker IP address X[.]213[.]155[.]164 had successfully changed the password, but in the case below, failed to access the account due to the second-factor authentication on the account. The attacker did not attempt to complete the second factor"*.

DigitalOcean's incident response capability was able to secure the targeted accounts and contacted the relevant customers. Following the attack, DigitalOcean has dropped Mailchimp as a third-party service provider, switching to an unnamed alternative.

WithSecure™ Insight

These incidents against Twilio and Mailchimp, which provide services to a large customer base once again highlight the issue with attacks on the supply chain. By attacking a supplier like Twilio or Mailchimp, an adversary is able to pivot and target their client/customer base, resulting in a larger issue and wider compromise. The supply chain is often an overlooked part of an organization's attack surface and presents a challenge for defenders. While you can bolster your own defenses and have robust security practices, if you're reliant on third parties for services/products it's important to consider the impact if the CIA (Confidentiallity, Integrity, Availability) of your data in your supply chain is affected, and consider this when constructing your incident response playbooks.

On this occasion, both Twilio and Mailchimp have described the initial access vector as involving a "complex social engineering attack" on their employees, resulting in the theft of legitimate credentials which have then been abused. This tactic is well-known and is becoming increasingly used against crypto-adjacent sectors, and is utilized by both cybercriminals and nation-state threat actors alike. While Mailchimp has not provided specific details regarding the attack, it is likely to have involved catfishing and well-crafted phishing/smishing lures designed to steal credentials, which appears to be what happened at Twilio.

Mailchimp has been met with criticism due to its lack of communication in the early stages, with many clients losing services and being locked out of their accounts, unaware of what was occurring. Communication is a vital part of incident response and without it, confusion and disruption are highly likely.

Mailchimp has since suggested that this attack was an effort to compromise their "crypto-related users" and this sector has been heavily targeted in recent months. A recent report by Slowmist has analyzed 15 such incidents that have occurred in 2022, with billions in crypto-assets being stolen. Crypto is heavily targeted due to the vast sums of money involved and comparatively lax security when compare to traditional banking and payment organizations/networks. This activity is often attributed to financially motivated cyber criminals, as well as nation-state groups such as Lazarus, who are DPRK-backed group focused on revenue generation.

1.3 Microsoft disrupt Callisto Group

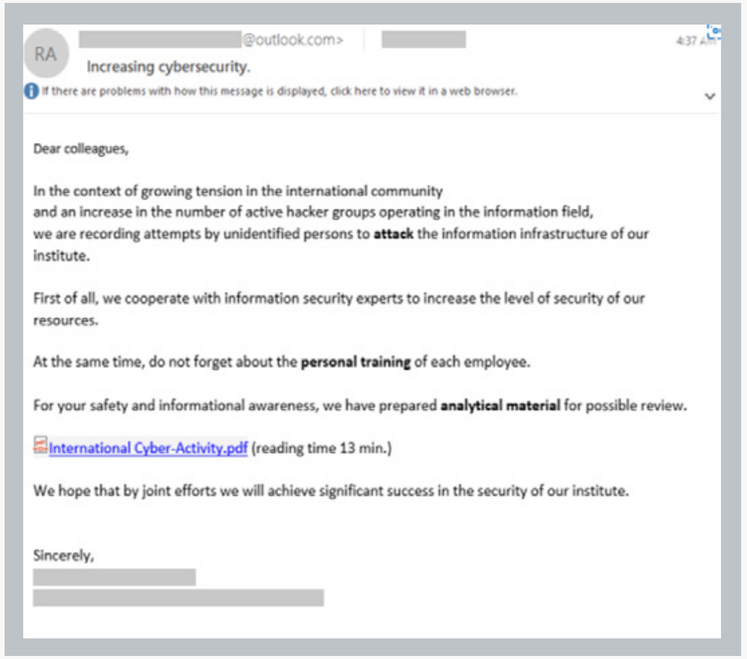
Microsoft's Threat Intelligence Center (MSTIC) have released a blog on a threat actor first observed by WithSecure™ (F-Secure at the time) back in 2015 called 'Callisto' (SEABORGIUM). Microsoft have attributed activity to Callisto since 2017 and believes them to be Russian-based and acting in the interests of the Russian state, and while the Security Service of Ukraine has linked the group to Gamaredon (Russian state-backed group) Microsoft is not linking the two.

Microsoft notes that Callisto has attacked at least 30 organizations in 2022, with their victimology being limited to member nations of NATO, and in particular the United States and the UK, and goes on to say…

"*Within the target countries, SEABORGIUM primarily focuses operations on defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, and higher education. SEABORGIUM has a high interest in targeting individuals as well, with 30% of Microsoft's nation-state notifications related to SEABORGIUM activity being delivered to Microsoft consumer email accounts. SEABORGIUM has been observed targeting former intelligence officials, experts in Russian affairs, and Russian citizens abroad*".

Microsoft details Callisto's current tactics, techniques and procedures (TTPs) which begin with the creation of fake profiles on social media, in order to perform reconnaissance and identify specific VIP/low-hanging targets. MSTIC have worked with social media platform LinkedIn to purge the profiles identified as being involved in Callisto's campaigns. MSTIC have observed Callisto interacting with targets, and building rapport with targets via the platform and comment:

"*SEABORGIUM proceeds to establish contact with their target. In cases of personal or consumer targeting, MSTIC has mostly observed the actor starting the conversation with a benign email message, typically exchanging pleasantries before referencing a non-existent attachment while highlighting a topic of interest to the target. It's likely that this additional step helps the actor establish rapport and avoid suspicion, resulting in further interaction. If the target replies, SEABORGIUM proceeds to send a weaponized email*".



MSTIC have witnessed Callisto use 3 methods of malicious link delivery, these include:

- A malicious URL in the email body, that is often obfuscated through URL shortening services.
- Attachments that imitate a file or document hosting service, including OneDrive, and request the user to open the document by clicking a button.
- OneDrive to host PDF files that contain a link to the malicious URL.

Regardless of the method used to deliver the URL the result is the same, with the target navigating to a credential harvesting page, often based on the EvilGinx phishing kit, which is designed to steal credentials and session tokens, allowing an attacker to potentially bypass MFA.

Callisto is then able to log in using those stolen credentials, and MSTIC has observed follow up activity which includes:

- Exfiltration of intelligence data
  - SEABORGIUM has been observed exfiltrating emails and attachments from the inbox of victims.
- Setup of persistent data collection
  - In limited cases, SEABORGIUM has been observed setting up forwarding rules from victim inboxes to actor-controlled dead drop accounts where the actor has long-term access to collected data. On more than one occasion, we have observed that the actors were able to access mailing-list data for sensitive groups, such as those frequented by former intelligence officials, and maintain a collection of information from the mailing-list for follow-on targeting and exfiltration.
- Access to people of interest
  - There have been several cases where SEABORGIUM has been observed using their impersonation accounts to facilitate dialog with specific people of interest and, as a result, were included in conversations, sometimes unwittingly, involving multiple parties. The nature of the conversations identified during investigations by Microsoft demonstrates potentially sensitive information being shared that could provide intelligence value.

MSTIC notes that the information stolen has on occasion been leaked and used as part of disinformation campaigns, designed to create false narratives and spread mistrust, but does not mention specific the material involved, as to not amplify the issue.

MSTIC have provided the following mitigation advice, based on the observable attack TTP's, as well as an exhaustive list of IOCs and Sentinel hunting queries:

- Check your Office 365 email filtering settings to ensure you block spoofed emails, spam, and emails with malware.
- Configure Office 365 to disable email auto-forwarding.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single-factor authentication, to confirm authenticity and investigate any anomalous activity.
- Require multifactor authentication (MFA) for all users coming from all locations including perceived trusted environments, and all internet-facing infrastructure–even those coming from on-premises systems.
- Leverage more secure implementations such as FIDO Tokens, or Microsoft Authenticator with number matching. Avoid telephony-based MFA methods to avoid risks associated with SIM-jacking.

In an effort to disrupt Callisto MSTIC has partnered with abuse teams in Microsoft to disable accounts used by the actor for reconnaissance, phishing, and email collection.

WithSecure™ Insight

Callisto has been observed and tracked by WithSecure™ since 2015, and in 2017 we released a whitepaper on the group, which discussed the group's TTPs from that period and provided relevant mitigation advice. This recent analysis by MSTIC serves as an update on the group's TTPs and is interesting because it demonstrates that the group's general modus operandi and motivations have not changed, and only some specific tooling/TTPs have developed.

Callisto's shift to targeted social engineering by abusing social media platforms is a common trend amongst threat actors, who are responding to hardened phishing defenses and greater user awareness of common phishing TTPs.

Callisto's activity is strongly linked to the geopolitical landscape and current affairs, with the group acting in the interests of the Russian state, as noted by their alleged involvement in the invasion of Ukraine.

MSTIC has provided excellent mitigation advice regarding Callisto-related activity, but on a more personal level, we would highly recommend that users undergo training to raise their awareness of social engineering attack tactics and techniques, which includes being suspicious of unsolicited contact on social media platforms such as LinkedIn. The Centre for the Protection of National Infrastructure (CPNI) has excellent training materials on the topic. WithSecure's security products including our endpoint detection capabilities provide coverage of the TTPs used by Callisto.

2 Ransomware: Trends and notable reports

2.1 ENISA's ransomware threat landscape

The European Union Agency for Cyber Security (ENISA) has released a report on the Ransomware landscape covering May 2021 to June 2022.

The main highlights of the report include the following:

- A novel LEDS matrix (Lock, Encrypt, Delete, Steal) that accurately maps ransomware capabilities based on the actions performed and assets targeted;
- A detailed and in-depth analysis of the ransomware life cycle: initial access, execution, action on objectives, blackmail, and ransom negotiation;
- Collection and in-depth analysis of 623 ransomware incidents from May 2021 to June 2022;
- More than 10 terabytes of data stolen monthly by ransomware from targeted organizations;
- Approximately 58.2% of all the stolen data contains GDPR personal data based on this analysis;
- In 95.3% of the incidents it is not known how threat actors obtained initial access into the target organization;
- It is estimated that more than 60% of affected organizations may have paid ransom demands;
- At least 47 unique ransomware threat actors were found.

The report is high quality and comprehensive, and the introduction of the LEDS matrix presents a novel way of tracking and highlighted ransomware functionality and capability.

2.2 A history lesson on Ransomware

The think tank Atlantic Council has released a report titled "Behind the rise of ransomware" which takes a detailed look at the following topics:

- The rise of ransomware
  - Which examines the history of ransomware since 1989 and looks at the shift in tactics that occurred around 2016 to more targeted attacks, as well as the move to big game hunting and the double-extortion model.
- Why ransomware isn't going away
  - An analysis of the current efforts to combat ransomware, including diplomatic, legal, and financial efforts.
- Addressing ransomware into the future
  - Three recommendations on helping combat ransomware, which include legislative steps which would make the reporting of ransomware incidents mandatory and suggestions on how to improve the cybersecurity capabilities of small and medium businesses within the US.

This report does a great job of examining the history of ransomware over time and its continual development and highlighting the difficulties of dealing with ransomware, especially when it comes to tracking threat actors, incidents, and crypto-assets, while offering excellent, albeit difficult to implement suggestions on tackling the rise of ransomware.

2.3 A look at Initial Access Brokers

Recorded Future has released a report on Initial Access Brokers (IABs) and their role in the rise of ransomware attacks. While ransomware operators can gain access to networks in several ways, such as the use of Remote Access Trojans (RATs) deployed through phishing, or the exploitation of vulnerabilities, the purchase of previously stolen valid credentials is a growing tactic and is a highly profitable market.

The report analyzes the extensive market for credentials on dark web sources and provides two key judgments:

- To conduct a successful ransomware attack, threat actors require remote access to compromised networks. The most common method by which threat actors obtain access is through the use of compromised valid credential pairs, which are often obtained via infostealer malware and sold on the dark web and special-access sources.

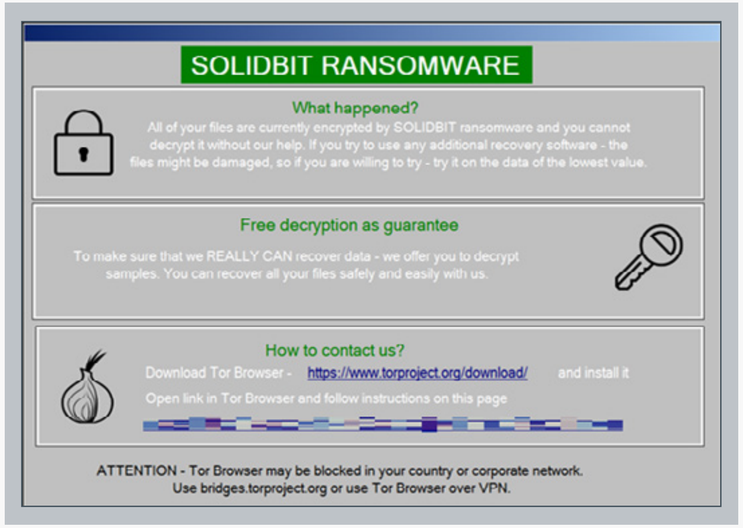
- Compromised credentials are often sold on the dark web and special-access forums and shops to ransomware affiliates, who use such access to move laterally through systems, escalate privileges and use malware loaders to deploy ransomware.

Recorded Future examines the different marketplaces which are selling credentials for services like VPN and RDP, as well as accompanying session cookies, which could enable an attacker to bypass MFA by using a pass-the-cookie style technique. Examples of credentials for sale are prevalent, thanks to the rise of highly capable infostealer malware families like Vidar, Redline, and Racoon Stealer, as well as a large appetite from ransomware groups to purchase them. The report also includes case studies on both Conti and BlackMatter, two of the most prolific ransomware groups in recent times, both known to use IABs to gain initial access.

2.4 Newcomers: SolidBit

Researchers from Trend Micro have analyzed a sample of a new ransomware variant called SolidBit. This group appears to be focused on targeting users of popular video games and social media platforms, with payloads being disguised as fake tools for League of Legends and Instagram.

These fake applications are hosted on GitHub, and when executed drop further payloads, which firstly launch Powershell commands that disable security services and then perform folder checks and begin encryption and delete shadow volumes, hampering recovery.



2.5 SANS ransomware summit

The 2022 SANS Ransomware Summit brought together infosec and cybersecurity experts from multiple organizations and fields, providing them an opportunity to present topics relevant to the threat of ransomware.

SANS have made the presentations from the event public, and they are available to view on Youtube

3 Other notable highlights in brief

3.1 Manjusaka framework

The intelligence team at Cisco Talos have uncovered a new attack framework called Manjusaka, which is freely available on GitHub and is an imitation of the venerable Cobalt Strike. The framework utilizes Go for its C2 and has implants written in Rust, languages which are seeing a steady rise in malicious usage.

Versions of the framework exist for both Windows and Linux based systems, with implants that are highly capable and exhibit common RAT functionality, such as:

- Execution of arbitrary commands
- Gathering file information
- Gathering information of current network connections (TCP and UDP)
- Collecting browser credentials
- Collecting Wi-fi SSID information
- Harvesting Navicat credentials
- Taking screenshots
- Obtaining comprehensive system information
- As well as numerous file management capabilities

Cisco Talos have assessed that the frameworks developer is likely a Chinese resident from GuangDong, and the C2 interface is written in simplified Chinese and has been linked to a maldoc distribution campaign which targeted residents of the Haixi Mongol and Tibetan Autonomous Prefecture, suggesting a geopolitical motivation. However, Cisco Talos is keen to mention that malicious usage of the framework is not necessarily attributable to the developer, as anyone can download and misuse it from GitHub, and that wider adoption across the criminal underground is likely.

3.2 Bots that steal OTP

One-time passes (OTP) are a form of multi-factor authentication (MFA) that is used to protect accounts. OTPs are dynamic passwords or phrases that normally consist of 4-8 characters, which change with each login attempt, and are delivered to the user through SMS, email or on authenticator applications like Authy, Duo and Okta Verify.

OTPs are problematic for threat actors, as they hamper initial access and credential theft, but a recent report by Recorded Future has looked at the growing trend and market for OTP bots, which are capable of stealing OTPs, making it cheaper and easier for threat actors to bypass MFA.

Recorded Future's key findings are:

- The increased use of OTPs by a variety of legitimate services (particularly for authenticating online account logins, money transfers, and 3-Domain Secure-enabled [3DS] purchases) creates parallel cybercriminal demand for methods of obtaining and bypassing OTPs.
- Dark web forum activity related to OTP bypassing (measured by volume of posts and views of posts related to the topic) rose sharply in 2020 and has remained high since.
- Traditional methods of OTP bypassing (performing SIM card swaps, brute-forcing, abusing poorly configured authentication systems, and manual social engineering) have become time-consuming and more technically challenging.
- OTP bypass bots combine social engineering and voice phishing (vishing) techniques with simple-to-use interfaces to provide a partially automated, affordable, and scalable method of obtaining victims' OTPs.

In related news, the compromise of automated communications provider Twilio, has also led to OTP compromises in several organizations and companies that utilized them as a third-party, including Okta, Cloudflare, Signal, DoorDash and Twilio's own Authy application.

3.3 Microsoft take a close look at DSIRF

The Microsoft Threat Intelligence Center (MSTIC) and the Microsoft Security Response Center (MSRC) are reporting on a private-sector offensive actor (PSOA) using multiple Windows and Adobe 0-day exploits, in limited and targeted attacks against European and Central American customers.

The PSOA, which Microsoft are tracking as KNOTWEED is an Austrian based organization called DSIRF who...

"*...provide services to multinational corporations in the technology, retail, energy and financial sectors" and have "a set of highly sophisticated techniques in gathering and analyzing information." They publicly offer several services including "an enhanced due diligence and risk analysis process through providing a deep understanding of individuals and entities" and "highly sophisticated Red Teams to challenge your company's most critical assets*".

This all sounds legitimate doesn't it? Well according to Microsoft and other news reports, DSIRF are linked to the development, sale and distribution of a malicious toolset called Subzero, which according to one of their sources, was used illegally.

Microsoft go on to examine Subzero's capability and methods of deployment, with known exploits including:

- CVE-2022-22047
- CVE-2021-31199
- CVE-2021-31201
- CVE-2021-28550
- CVE-2021-36948

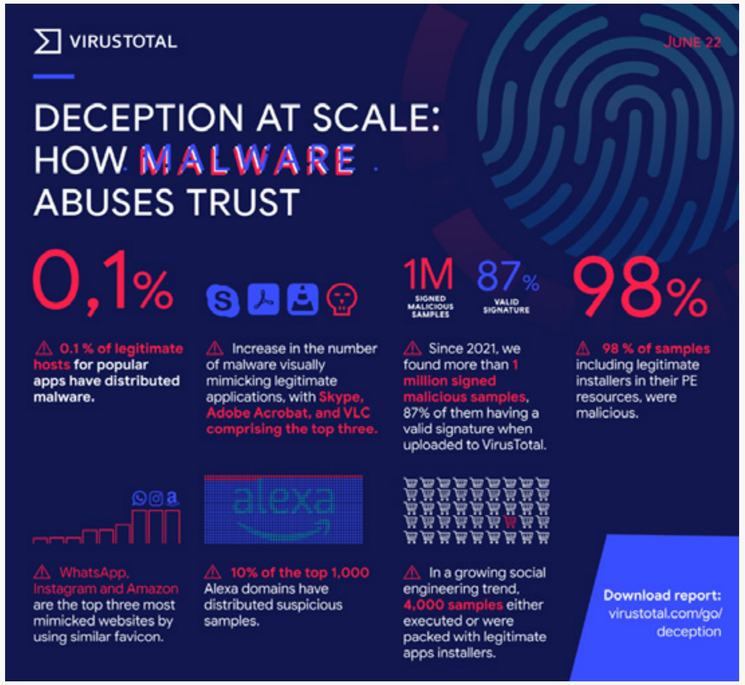
Microsoft have also include an excellent breakdown of Subzero's TTPs and provided mitigation advice, hunting queries and a comprehensive list of IOCs.

3.4 VirusTotal: Deception at scale

VirusTotal have produced a report that looks at the different methods used by malware developers to bypass defenses.

The main findings include:

- 10% of the top 1,000 Alexa domains have distributed suspicious samples.
- 0.1%of legitimate hosts for popular apps have distributed malware.
- 87% of the more than one million signed malicious samples uploaded to VirusTotal since January 2021 have a valid signature.
- In a growing social engineering trend, 4,000 samples either executed or were packed with legitimate apps installers.
- There has been a steady increase in the number of malware visually mimicking legitimate applications, with Skype, Adobe Acrobat, and VLC comprising the top three.
- 98% of samples, including legitimate installers in their PE resources, were malicious.

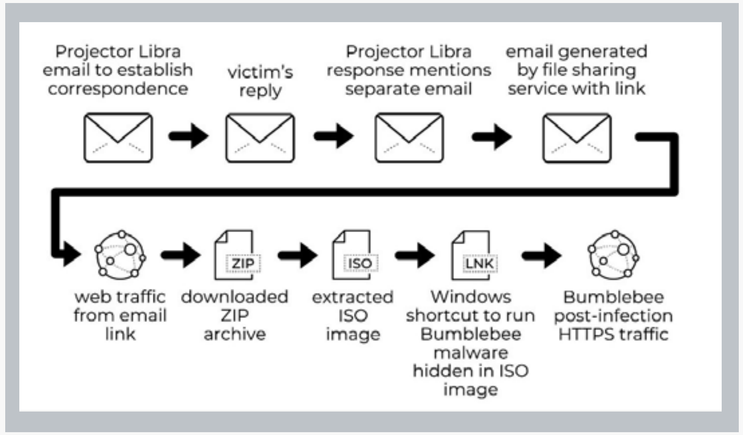


3.5 EXOTIC LILY spreading Bumblebee

Exotic Lily (Projector Libra) are a group who specializes in gaining initial access through complex social-engineering, and act as IABs for other threat actors, and who had previously been connected to the ransomware group Conti.

Researchers from Palo Alto's Unit 42 have been tracking an EXOTIC LILY campaign, in which the group have been distributing the malware Bumblebee, and following-up with Cobalt Strike. Bumblebee, which is a malware loader, has been around since early 2022 and has essentially replaced Trickbot's BazarBackdoor/BazarLoader tools.

Google's Threat Analysis Group (TAG) have previously reported on EXOTIC LILY's attack chain, and Unit 42 have provided an updated look at the group's process:



EXOTIC LILY go to a lot of effort to make their lures convincing and the first stages of their attack chain, which often includes correspondence and impersonation, can be considered social-engineering, and increases the likelihood of target interaction and subsequent infection.

3.6 A collation of crypto-heists

Blockchain security firm SlowMist have released their mid-year Blockchain Security and AML Analysis Report for 2022. The report looks at topics including; an overview of blockchain security, know security incidents and analysis related to money laundering activity.

Notably, the report highlights that there were 187 blockchain related security incident in the first half of 2022, which totaled losses/damages of nearly $2 billion. The report analyzes 15 high-profile incidents, which includes the Ronin ($610 million loss) and Wormhole ($326 million loss) breaches. As well as looking at the role of mixers such as Tornado, in the transfer and laundering of stolen and illicit funds on the blockchain.

Interestingly, SlowMist data also concludes that the vast majority (>75%) of incidents are caused by vulnerabilities, rather than scams, phishing or other activity. Highlighting the need for better vulnerability detection and management within the blockchain/crypto sector.

4 Threat data highlights

4.1 Exploits

WithSecure™ telemetry shows that threat actors continue to favor older but proven exploits, with exploits for CVE-2017-0199 and CVE-2017-11882 continuing to top the board. In fact, there are no 2022 exploits in the top-ten, showing threat actors preference for exploits with some history and track record. If it isn't broke, don't fix it?

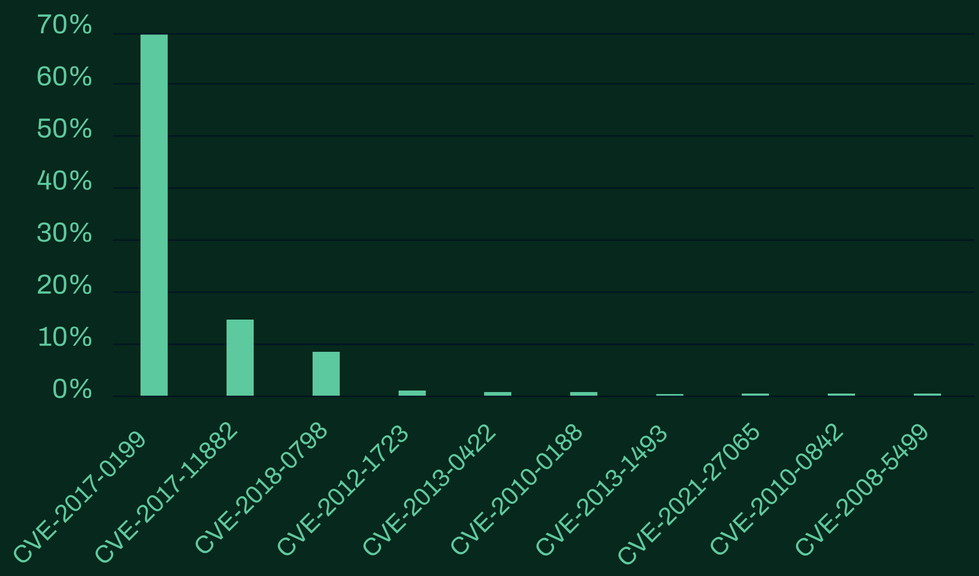
CVE-2017-0199 was the most prevalent vulnerability exploited at endpoints during August. It is a remote code execution vulnerability in MS Office and Wordpad exploited by a specially crafted RTF document.

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.

In August, CISA added 23 new vulnerabilities to their known exploited list. These include vulnerabilities in various applications such as **UNRAR** on linux & unix, windows components, **Grafana** authentication bypass and **WebRTC** heap buffer overflow.

Nearly all applications listed have patches available which should be applied. **DopSoft2** with improper input validation vulnerability is end of life and use should be discontinued.

Exploits in the wild

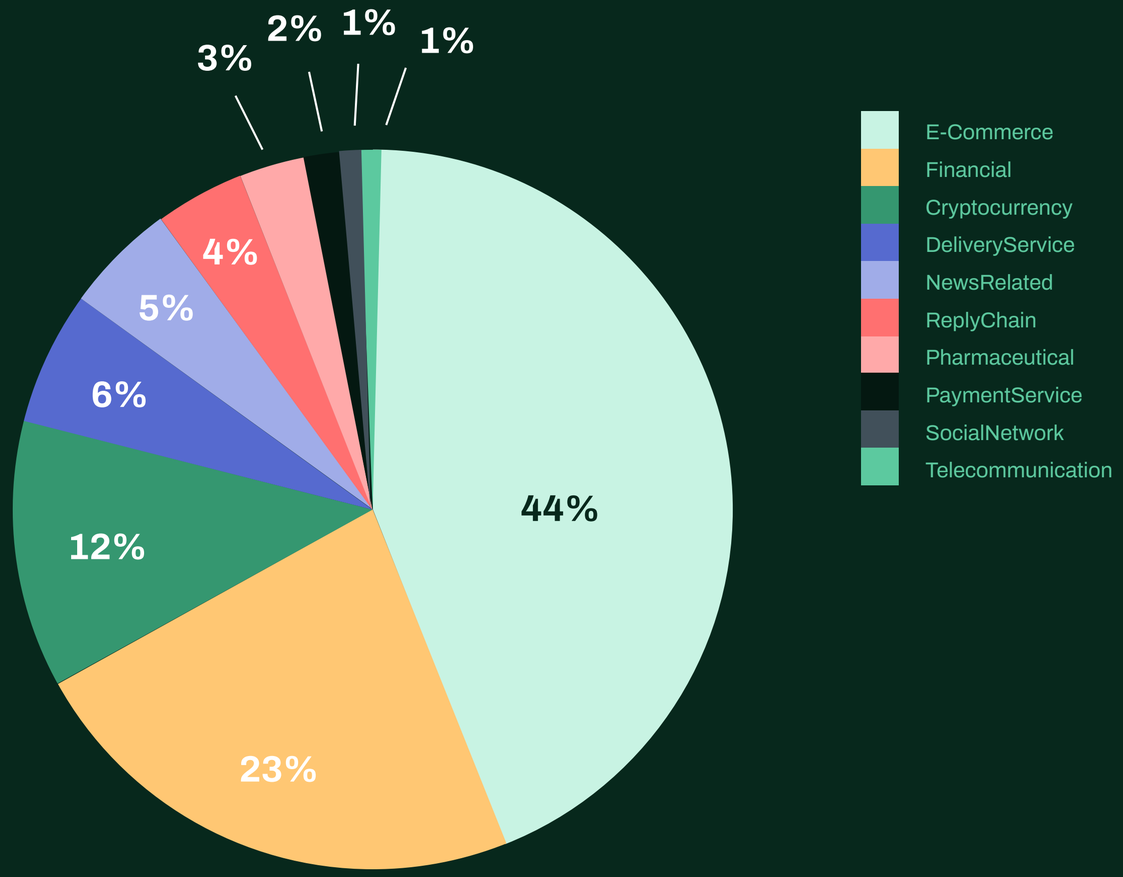


WithSecure™ endpoint protection

4.2 Email threats

In August, cryptocurrency has dropped in popularity among the spam email traffic. E-commerce dominates the spam-landscape followed by the financial theme.

Spam Email themes



WithSecure™ spam data collection

5 Research highlights

WithSecure™ researcher Connor Morley has recently spoke at DefCon 30, with their presentation “Malicious memory techniques on Windows and how to spot them”.

The full presentation is available on Youtube, and examines how malicious actors are trying to find new ways to avoid detection by evermore vigilant EDR systems and deploy their payloads.

Morley says...

“Over the years, the scope of techniques used has branched from relatively simplistic hash comparison and sandbox avoidance to low level log dodging and even direct circumvention of EDR telemetry acquisition. By examining some of the techniques used on Windows systems this talk will highlight the range of capabilities defensive operators are dealing with, how some can be detected and, in rare cases, the performance and false-positive obstacles in designing detection capability.

My research covers some of the more well known to more obscure malicious memory techniques on the Windows operating system. These span from relatively simple in-line hooking techniques used to jump to malicious code or circumvent legitimate code execution, all the way to manipulation of exception handling mechanisms. The research will also outline problematic situations which occur when designing detection mechanisms for such activities in the real world where cost-balancing is required for resource management.

An in depth explanation on in-line hooking, Kernel patching (InfinityHook, Ghost_in_the_logs), Heaven-Gate hooking and Vectored Exception Handler (VEH) manipulation techniques (FireWalker) and how they can be detected will be provided. In-line hooking and Heavens-Gate hooking involves the practice of manipulating the loaded memory of a module within a specific processes memory space. Kernel Patching involves injecting a hook into the Kernel memory space in order to provide a low level, high priority bypassing technique for malicious programs to circumvent ETW log publication via vulnerable kernel driver installation. VEH manipulation is the use of the high priority frameless exception mechanism in order to circumvent memory integrity checks, manipulate flow control and even run malicious shellcode. Understanding of the detection methods for all these techniques will involve advancing from the explanation of its execution to the telemetry sources that can be leveraged for detection purposes and what to look for within these data sets. In all cases this involves the examination of volatile memory, however as each technique targets a different native functionality, the mechanisms required to analyze the memory differ greatly. The deviations can be relatively simple, but in some cases an understanding of undocumented mechanisms and structures is required to affect detection capability

Examination of un-tabled module function modifications will also provide insight into some of the difficulties involved in this detection development work. This section will provide an understanding at a technical low level of how these techniques are targeted, developed and used by malicious actors and some possible solutions for detection, with an explanation of the inherent caveats in such solutions (primarily around resource availability or accuracy trade-offs).

A full explanation on devised detection methodology and collectable telemetry will be provided for each malicious technique. This will cover the overall detection capabilities as well as exploring the low level mechanisms used to collect this data from the monitored system such as OP code heuristics and memory location attribution crossing CPU mode boundaries. Included in this explanation will be an explanation on issues encountered with collection, typically related to OS architecture choices, and how these can also be circumvented to enable effective monitoring.

The core objective of my research is to provide details on the fundamentals of all the techniques outlined and why attackers may choose to employ them in different scenarios. Along with a functional understanding of the malicious technique, readers should be supplied with a working understanding of detection options for these techniques and clear examples of how monitoring can be deployed and integrated into their solutions".

Who We Are

WithSecure™, formerly F-Secure Business, 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 and response are 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™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure