



White Paper
TLP: WHITE

Overview of cyber threat trends to beware of in 2022

Key findings

- Ransomware attacks remain a priority threat to organizations worldwide. We continue to monitor the evolution of ransomware operations in 2022, while also anticipating an answer to the quantity versus quality debate as we observe future service developments.
- General operations for most organizations include third-party vendors and services, creating an environment primed for supply chain attacks. A prominent threat that increased in 2021, supply chain attacks likely will continue to remain a potential vulnerability for organizations in 2022.
- The market for compromised credentials is propagated by the frequent threat of data breach events. Private sellers and those that leverage credential marketplaces contribute to account takeover (ATO) and initial access attacks, requiring organizations to remain diligent when implementing credential security measures.
- Business email compromise (BEC) tops business cybersecurity priorities as a high profit yielding attack technique that leverages CEO impersonations to carry out phishing attacks on company employees. While not as prominent as other trending threat types, BEC likely will remain a risk to organizations in 2022.
- Smishing and malware operations showed persistence against changes to the threat landscape, preferences for more profitable offerings and law enforcement action. The evolution of such services indicate they likely will continue to adjust to unexpected challenges and operate with impunity.
- The use of deepfake technology could become an increasingly popular method for actors seeking to elevate their social engineering attack techniques. Although the current complexity of using this technology has limited its underground presence, deepfakes will remain an area of operations to monitor in 2022.

Introduction

Cybersecurity increasingly has become a priority for organizations across all sectors as technology continues to advance worldwide. Often plagued by similar cyberattacks, businesses seek an understanding of threat actor techniques and how to protect against them. While several attack strategies can be avoided by adhering to standard cybersecurity practices such as mandating regular password changes and providing education about device security, Intel 471 continued to observe the evolution of well-established threats in 2021 despite these protection efforts. This report aims to provide a high-level overview of these threats, which likely will remain prevalent and worthy of continued focus throughout 2022, including active and emerging ransomware operations, supply chain attacks, the theft and sale of compromised credentials, the maturation of BEC attacks, WhatsApp impersonations and subscriber identity module (SIM) card swapping, the return of the Emotet malware and the underground application of deepfake technology.

Our research

Information used to support assessments made in this report was gathered from Intel 471 reporting, along with common themes observed by our Intelligence Team and open source media outlets. While some activity may apply to a specific threat type, we also observed links between several common cybercrime tactics. These observations highlight threat actors' use of more than one – or the combination of several – attack methods to reach their overall objectives.

Ransomware operations remain highly impactful

Several high-profile ransomware events were observed over the course of 2021, such as the attack against the Georgia, U.S.-based Colonial Pipeline, where attackers allegedly exfiltrated about 100 GB of data from the compromised network. This event changed ransomware operations in the underground due to increased media attention and pressure from law enforcement against operators and affiliates of these services. After administrators shut down ransomware activity on their respective forums, the RAMP forum was created and became the go-to platform for threat actors to discuss ransomware-related operations. While we occasionally continue to see discussions of ransomware on the Exploit and XSS underground forums, there were no recent advertisements for these services at the time of this report.

We also observed threat actors claiming they would not target certain industries in order to reduce attention from high-profile attacks, including specific actors who stated their affiliates were prohibited from targeting government, health care and educational institutions. They largely kept their word, however, the BlackMatter ransomware-as-a-service (RaaS) was affiliated with an attack on an education center after previous claims of restraint against critical infrastructure. Although the group was not explicit in its definition of “critical infrastructure,” this subsequent attack on a public sector entity raised doubts about its claims and overall reduced the likelihood that other groups who had made similar adjustments would stand by their revised models.

Assessment

Ransomware attacks against organizations can cause a vast amount of damage and are considered a global threat. If a business falls victim to a ransomware attack, it can suffer from unpredictable downtime, reputational damage and financial repercussions when facing a ransom payment. Impacted entities likely will need to invest time and resources into recovery and remediation efforts, as well as increase security measures to protect against future incidents. Understanding the stages of a ransomware attack and tactics, techniques and procedures (TTPs) from threat actors who use ransomware as a primary attack method can assist organizations in these attempts (see: Figure 1).

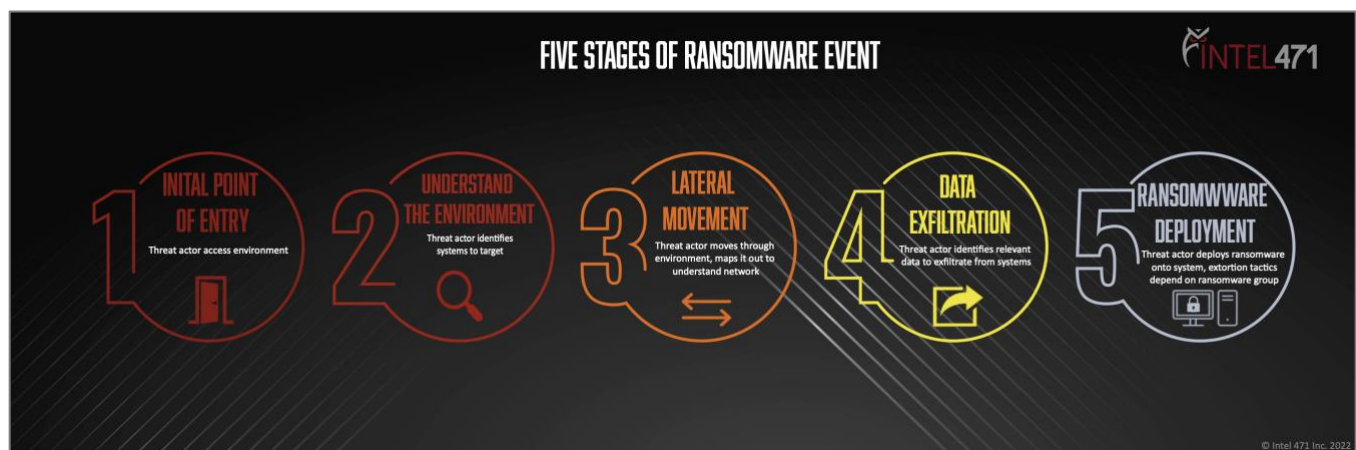


Figure 1: This graphic provides an overview of the different stages of a typical ransomware attack.

The evolution of ransomware has included the use of double-extortion tactics, such as the implementation of distributed denial-of-service (DDoS) attacks, making phone calls to an organization's management team and leveraging the media to add pressure to victim organizations to pay a ransom. The success of these tactics suggests ransomware operators likely will continue to diversify attack strategies and use modified extortion methods to increase payment outcomes in 2022. Additionally, we may see these tactics increase a RaaS group's reputation, which may inadvertently increase its negotiating power.

Analyst comment

Threat actors have endless opportunities to leverage ransomware services, and the number of services available has given attackers at all skill levels the ability to profit. Ransomware operators continue to adapt to new challenges, allowing their services to take on variable and sometimes novel characteristics. This means there is no single course of action to protect against all ransomware variants, but emphasizes the necessity for analysts and threat teams to study ransomware services holistically to implement strategies that protect their organizations effectively.

As we move through 2022, it will be insightful to observe ransomware attacks and respective operators' targeting methodology. The popular opportunistic approach that indiscriminately infects as many victims as possible likely will remain a large portion of all observed events. However, we likely also will see operators and affiliates conduct advanced research on potential victims and target those that will ensure a higher ransom payout. The question remains: Will we see quantity over quality take precedent in 2022?

Supply chain attacks leverage vulnerable third-party systems

The observed increase in the number of supply chain attacks in 2021 points to the popularity of this attack method and indicates a likely continuation of this technique in 2022. Supply chain attacks often are successful because they typically exploit legitimate services for concealment and allow threat actors to exploit an organization through a less secure third-party service. These types of compromises potentially can open access to multiple organizations while only requiring the attacker to exploit a single point of entry. For example, the July 2021 cyberattack on the U.S.-based information technology (IT) and management software company Kaseya led to ransomware attacks against managed service providers (MSPs) that serviced about 800 to 1,500 businesses worldwide.^[1] In this instance, Kaseya may not have been the intended target but acted as an initial access point for attackers to gain entry into and subsequently impact many networks and organizations that used the third-party service.

Assessment

Supply chain attacks likely will continue to surge as long as threat actors are able to find vulnerable entry points in third-party vendors of prominent organizations. Considering the possible ease at which an actor could exploit a single point of entry and navigate into networks of organizations the compromised vendor services, it is more likely we should think about when – not if – an attack will occur. This likelihood emphasizes the need for a detailed understanding of a company's corporate and digital footprint to ensure partnerships with vendors do not leave a business vulnerable to a supply chain attack. Additionally, it is vital to increase employee awareness

of common access techniques, as well as ensure security professionals remain prepared to respond quickly in the event a vendor is compromised.

Compromised credentials market enables persistent attack techniques

For underground actors focused on the sale of stolen credentials, reputation plays a large part in their success. While forum users can post lists of credentials that can be analyzed freely for authenticity, a prolific seller relies on an earned level of credibility to post an advertisement that allows private authentication only for serious buyers. In addition to advertising on underground forums, threat actors can sell stolen credentials on specialized marketplaces such as Genesis Store and Infinity Store. Corporate credentials in these shops can start at US \$10 to US \$50 and raw information-stealer logs can be priced as low as US \$5. On the higher end of advertised offers, prices can range from hundreds to thousands of dollars. Although these prices may seem like a steal compared to potential profits from putting the stolen credentials to work, there is a risk that the accounts may no longer be valid at the time of purchase.

Forums and marketplaces that enable the sale of stolen credentials allow purchases with the intent to repurpose the credentials for malicious activity. We typically observe threat actors who purchase credential sets or bots – machine identifiers, cookies and browsers used to bypass access control measures – use them to emulate genuine account holders. For example, in June 2021, threat actors reportedly purchased stolen cookies for US \$10 that subsequently were leveraged to access a Slack channel used by the video game company Electronic Arts Inc. (EA). The attacker used the access to message the company’s IT support, request a multifactor authentication (MFA) token and log in to EA’s corporate network.^[2]

Assessment

The sale of compromised credentials and the use of credential-specific marketplaces likely will continue to grow in popularity in 2022. On the seller side, these shops offer a quick and easy way to make a profit from small or large batches of stolen credentials. On the buyer side, stores like Genesis and Infinity operate as ideal environments for threat actors at any skill level. Less sophisticated attackers can purchase ready-made initial access to an organization that can be compromised further by a magnitude of other packaged tooling offered on underground forums.

With the advent of stronger security measures such as two-factor authentication (2FA), organizations may assume their systems, accounts and sensitive data are protected adequately, even if company credentials were to be compromised. However, threat actors observably are aware of increased measures organizations have taken and have adapted their strategies by adding additional attack techniques such as social engineering to help them gain access to networks. One way to combat this threat is to raise awareness related to password reuse and leaked credentials. Additionally, organizations can use free applications such as password safes that have built-in warnings to alert users when a weak password is created and/or notifies them if credentials or accounts have been compromised.

Analyst comment

The consistent threat of data breaches draws attention to the impact compromised credentials can have on an organization's security. Although several developments in cybersecurity have attempted to thwart the efficacy of stolen credentials, marketplaces for buying and selling compromised data sets still flourish. Several threat actors built strong reputations as consistent sellers of valid credentials, including prolific actors who received nominations on the Raid Forums underground forum announcement for a 2021 "leaker of the year" award. Prominent actors in the credentials ecosystem likely will remain in business and we also will be on the lookout for any possible newcomers offering paid or free valid credential sets throughout 2022.

Additionally, the EA breach was a prime example of how the ATO life cycle can pose a significant risk to organizations. Intel 471's Credential Intelligence platform provides coverage across underground marketplace offerings, allowing users to proactively monitor and mitigate the risk associated with compromised credentials. Credential monitoring can help support a company's awareness of identification theft, loss of employee data and potential damage to the brand's reputation.

Business email compromise reported as frequently observed threat type

The use of business email compromise (BEC) is a popular threat actor attack tactic and has remained an accessible means to gain access to victim accounts and networks over time. Those outside the information security community may be less aware of the potential threat associated with BEC, likely because it is not categorized as a traditional phishing method. BEC scams typically appear more sophisticated when compared to other well-known lures, using refined templates that have better grammar and more believable content. Interestingly, this attack technique is viewed as a high-profit scam. The U.S. FBI's 2020 Internet Crime Report stated BEC threats accounted for 43% of all cybercrime losses for the year – the highest of all threat types recorded – and caused more than US \$1.8 billion of monetary losses to impacted businesses.^[3]

We observed multiple deployment methods for BEC campaigns, typically defined by the actor's motivations. A common social engineering ploy for BEC attackers is impersonating CEOs in order to facilitate wire transfer fraud, which reportedly can solicit payments from US \$50,000 to US \$80,000 per transaction.^[4] However, the target pool for such an attack can be limited since many employees do not have the authorization to execute a wire transfer on behalf of their organization. Conversely, threat actors also used BEC to obtain gift cards, which could allow attackers to exploit more employees in a single attack. For example, one scammer impersonated an organization's management and requested employees purchase Amazon gift cards as a "thank you" for the team. This represents a less sophisticated use of BEC and consequently returns payouts as small as or smaller than US \$250, with an average profit of US \$1,627. Threat actors using BEC as their primary phishing attack method also were seen capitalizing on global events, such as Coronavirus Disease 2019 (COVID-19).^[5] Aligning with traditional phishing methods, the creation of targeted campaigns using trending topics as lures can appeal to users' interests and decrease skepticism regarding their interaction with the email content.

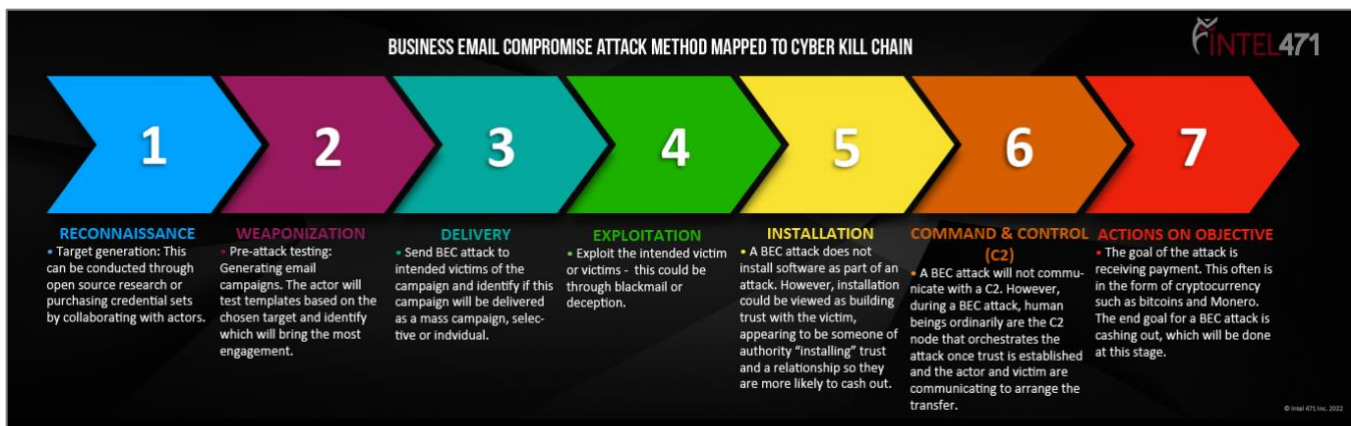


Figure 2: This graphic depicts the BEC attack method mapped to Lockheed Martin’s cyber kill chain.

Assessment

Attack statistic claims such as those in the FBI 2020 Internet Crime Report indicate that while threat actors wield many cybercrime tactics, BEC remains a consistently profitable option among the more “traditional” methods observed. The popularity could be based on alleged higher profit returns versus those seen in less refined phishing attacks.^[3] Additionally, BEC requires very little investment up-front compared to other types of attack techniques, which reduces overhead operational costs and generates more net profit. Intel 471 observed threat actors seeking partnerships to conduct BEC attacks and it is possible sophisticated threat actors could move to BEC to conduct targeted phishing attacks to increase their return on investment (ROI).

Many companies still rank BEC as one of their top cybersecurity priorities likely due to the potential impact these attacks can have. The use of email authentication protocols such as domain-based message authentication, reporting and conformance (DMARC) can assist in protecting senders and receivers from phishing, spam and spoofing attempts by filtering email services. However, one of the most effective ways to protect against BEC attacks is providing employee education and awareness of this phishing method. Education should target all levels of employees within an organization and explain what a BEC attack is, what to do if employees suspect a phishing attempt and how to report it.

Smishing, WhatsApp impersonations, subscriber identity module card-swapping techniques

Threat actors have evolved their short message service (SMS) phishing aka smishing campaigns to incorporate the use of SIM card swapping and messaging platforms such as WhatsApp. In smishing attacks, threat actors attempt to entice targeted recipients to click a link, download malware to their smartphone and/or send the attacker private information. Social engineering efforts are displayed in this tactic and can include created content mimicking news on recent events with a link for “important” or “more” information and curated messages implying potential delivery or transaction issues with a link to “resolve the issue.” The use of SMS to send these notifications is the more traditional route of attack observed, however, threat actors are adding other ways to reach potential victims.

WhatsApp appears to be a tool of high interest for cybercriminals, frequently is mentioned on underground forums and observably has been used as a vector to conduct smishing attacks. Scammers reportedly have used the messaging platform to request money by impersonating a victim’s close relative.^[6] There also was an

instance where attackers allegedly impersonated what appeared to be a legitimate financial business within a WhatsApp trading group to conduct a cryptocurrency scam. SIM card swapping enables a victim's telephone number to be used on another device but using this technique for smishing also requires the use of social engineering practices. These can include targeting telecommunications support operators or developing relationships with employees working in the cellular provider's organization.

Assessment

We assess there is a high probability impersonations and extortion attempts via smishing campaigns will continue to increase on nontraditional messaging services. Additionally, threat actors likely will continue to use social engineering to acquire the SMS code sent to a victim's number to activate a WhatsApp account on another device. We have observed service offerings using SIM card swapping to intercept text messages sent to a targeted phone number undetected. Paying close attention to the legitimacy of SMS sender details including the phone number, display name and time of SMS delivery can assist in limiting accidental interactions with potentially malicious links.

Return of Emotet malware depicts operators' resilience

The operators behind Emotet are known for their geographically targeted malspam campaigns and reply-chain email tactics. They deliver geo-targeted malspam campaigns to a specific region or country at a relevant time using local languages to appear more legitimate and increase the click-rate of spam recipients. In January 2021, a law enforcement joint task force took over the well known and prolific Emotet botnet. Due to the reliability and status of this malware, we assessed there likely would be a swift return of Emotet to the underground. The increasing demand from ransomware operators seeking to purchase quality malware-as-a-service (MaaS) also supported this assessment, as it is likely reputable ransomware operators would desire higher quality malware services to ensure high ransom payouts continued. It took several months for the threat actors behind Emotet to regroup and execute their return and on Nov. 14, 2021, Intel 471's Malware Intelligence Team observed instances of the Trickbot banking trojan downloading and executing updated Emotet malware binaries. Post-takedown, we observed Emotet with a Cobalt Strike module that could be loaded directly onto infected systems, indicating potential support for ransomware operations.

Assessment

Commodity malware campaigns are used as one of the primary ways to resell or to extend access, which makes it more than likely that Emotet will continue to develop their capabilities. Having observed Emotet operators directly deploying Cobalt Strike, it is likely they are acting solely as access brokers for ransomware operators. It also is possible the malware service will operate more exclusively, with fewer partners than before, to mitigate exposure to ongoing law enforcement investigations. We assess it will take time for the threat actors operating Emotet to build their spamming capacity back up to pre-takedown levels. Considering Emotet likely has not yet shown their full capabilities post-takedown, our Malware Intelligence Team continues to closely track the service's maturing activity and will report on relevant updates.

Deepfake technology makes cybercrime appearance

Originating from a Reddit social media platform user in 2017, the term “deepfake” typically refers to synthetic media that was edited using an algorithm to replace a person in the original with someone else. The use of deepfake technology has become increasingly popular and there are recent real-world use cases where threat actors leveraged deepfakes for voice phishing (vishing) campaigns.^[7] However, the current complexity of using this technology has limited its presence on underground forums. The hardware needed for this type of attack is comparatively expensive and the technology requires a high level of technical understanding as well as hundreds of images of the target to produce a basic deepfake.

Assessment

Although the concept of deepfakes is appealing to threat actors seeking to elevate their social engineering attack techniques, our consensus is the technology required to create a convincing deepfake remains in its infancy. Additionally, the means required to create the necessary content would have to be more affordable and accessible for underground actors to leverage the tools and still see a redeeming profit. Intel 471 assesses deepfakes likely will increase in popularity with cybercriminals and should remain an area of operations to monitor in 2022. If advancements in the technology lower the skill level needed to create deepfakes, it is likely the attack method will become more widely used.





Intent 	Capability 	Opportunity 
<i>Goals the adversary wants to achieve.</i>	<i>The adversary's ability to successfully achieve their goal(s).</i>	<i>The adversary's knowledge of the intended target environment.</i>
<ul style="list-style-type: none"> • Deceiving the victim into believing the content is real. • Gaining initial access into the intended target’s environment. • Circumventing security settings, such as video verification. 	<ul style="list-style-type: none"> • Vishing and video phishing campaigns. <p><i>*There are limitations in the technology used for deepfakes. Actors of a lesser skill level will be dependent on technological advancements to support their capabilities.</i></p>	<ul style="list-style-type: none"> • Using open source intelligence (OSINT) to identify relevant events and/or individuals to create campaigns around. • Leveraging publicly available personally identifiable information (PII) to create more convincing deep fakes. <p style="text-align: right;"> © Intel 471 Inc. 2022</p>

Figure 3: This image depicts a summary of the intent, capability and opportunity of actors seeking to use deepfake technology.

Summary

The impact of cyber attacks are costly, both in terms of time and money. In July 2021, an IBM Security Report highlighted a 10% increase in the average cost of a data breach from 2020 to 2021, which likely will increase in 2022.^[8] This report provided insight into what Intel 471 assesses to be relevant threats for 2022, but at the time of this report they remain predictions based on currently observed trends in the underground. The threats outlined potentially can evolve against security challenges and cause more damage to impacted organizations. Threat actors likely will continue to modify and refine their offers to keep up with developments in the threat landscape, and change or revamp existing products, services and goods to remain competitive and relevant in their respective markets. Underground services and operations are capricious, and while favored activity from 2021 likely will persist into 2022, we would be naive to think other profitable offerings will remain at bay (see: Figure 4).

Available data supports the importance of employee education – such as targeted education for different departments covering exploitation tactics utilized by attackers – to increase awareness of the types of threats an organization can face. Some facets of cybercrime remain unpredictable, making it prudent for security practitioners to monitor and be prepared for any critical shifts in activity that may occur. The range of Intel 471’s intelligence products can assist security teams in their efforts to defend against impending threats and mitigate risks from active cybercrime operations. Our Adversary Intelligence offers visibility into TTPs and motivations of threat actors, as well as relationships between services that might equip attackers with advanced attack capabilities. Users also can proactively monitor for compromised credentials via Intel 471’s Credential Repatriation, Enumeration and Disposition System (CREDS), track weaponized malware via our Malware Intelligence and determine patch prioritization of vulnerabilities via our Vulnerability Dashboard.

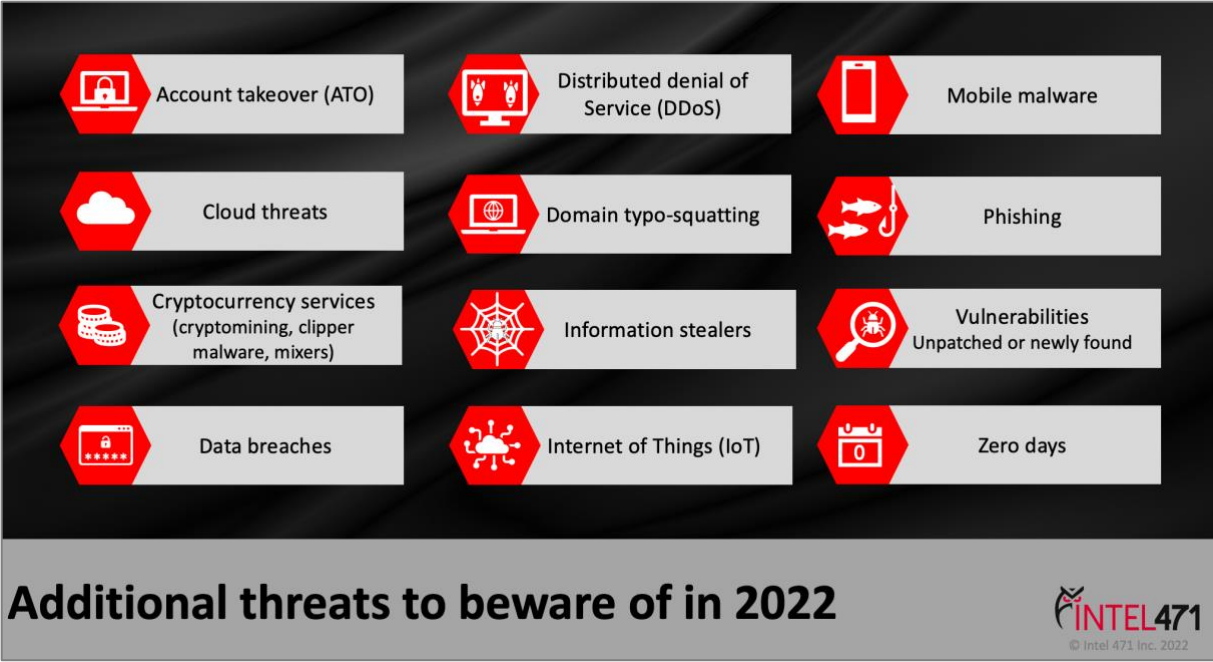


Figure 4: This image depicts additional persistent threats to beware of in 2022.

GIRs

- 1.1.1 Ransomware malware
- 1.1.2 Mobile malware
- 1.1.4 Banking trojan malware
- 1.1.5 Information-stealer malware
- 1.1.15 Cryptomining malware
- 1.2 Malware-as-a-service (MaaS)
- 1.2.2 Ransomware-as-a-service (RaaS)
- 1.3.8 Malware spamming
- 2.1 Vulnerabilities
- 4.1.1 Cashout
- 4.1.5 Prepaid or gift card fraud
- 4.1.9 Business email compromise (BEC)
- 4.1.10 Document fraud
- 4.2 Compromised data or access
- 4.3 Account takeover (ATO)
- 4.3.4 Subscriber identity module (SIM) swapping
- 4.4.1 Phishing
- 4.4.2 Spear-phishing
- 4.4.3 Vishing
- 6.1.2.1 Oil, gas and consumable fuels industry
- 6.1.8.1 Technology industry
- 6.1.8.2 Media and entertainment industry

Sources

- [1] 08Nov2021 MSSP alert: Kaseya REvil Ransomware Cyberattack: Hacker Charged
<https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/>
- [2] 11June2021 Vice Blog article: How Hackers Used Slack to Break into EA Games
<https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack>
- [3] 17March2021 FBI annual report: Internet Crime Report 2020
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- [4] 27Aug2020 Anti-Phishing Working Group (APWG)'s Phishing Activity Trends Report
https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf
- [5] 06April2020 FBI blog: FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic
<https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic>
- [6] 24Nov2021 Action Fraud article: 'Friend in need' message scam costs victims almost £50,000 in three months
<https://www.actionfraud.police.uk/alert/friend-in-need-message-scam-costs-victims-almost-50000-in-three-months>
- [7] 14Oct2021 Forbes article: Fraudsters Cloned Company Director's Voice In \$35 Million Bank Heist, Police Find
<https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=1610d5ad7559>
- [8] July2021 IBM Security report: Cost of a Data Breach Report 2021
<https://www.ibm.com/uk-en/security/data-breach>