ZEROFOX® | REPORT

2022 Threat Intelligence Forecast

Security Predictions & Recommendations

February 2022

zerofox.com

Table of Contents

Introduction

ZeroFox Intelligence strives every day to produce complete, accurate, relevant, and timely intelligence reports our customers need to reduce risk and uncertainty against a constantly evolving threat landscape. This paper reflects the collective insights of the experts dedicated to that mission.

Information available as of January 20, 2022, was used in the preparation of this forecast.

We have gone further than telling you what we think will happen. We also offer recommendations to counter the threats described in the latter part of this forecast.

Please take our four question survey after reading this forecast. Your feedback is critical to ensuring ZeroFox Intelligence is delivering insights you need to gain a decision advantage over the threat landscape.

KEY FORECASTS FOR 2022

- ZeroFox anticipates that ransomware will continue to thrive at an accelerated pace throughout 2022. Organizations in the financial, manufacturing, retail, and healthcare sectors will remain at heightened risk. Ransomware developers are likely to focus on achieving persistence and evolving extortion tactics, including directing threats towards high-profile individuals.
- ZeroFox forecasts a surge in data kidnapping attacks—extortion without the encryption of victim data—in 2022.
- ZeroFox expects more cyber criminals to shift from Bitcoin to Monero as their cryptocurrency of choice in the coming year.
- ZeroFox predicts third-party compromises will continue on an upward trajectory in terms of frequency, scale, and sophistication; threat actor targeting is likely to focus on smaller, third-party vendors within larger supply chains and key events in 2022.
- ZeroFox assesses that remittance-heavy economies will move towards digital currencies in 2022 at an accelerated pace. Because of that trend, more states will continue to attack the cryptocurrency industry in the coming year to generate funds for governments seeking to circumvent various economic sanctions.
- ZeroFox expects competition among infostealer developers to increase in 2022, encouraging innovation aimed at building better, more sophisticated, and easier-to-use services.
- ZeroFox assesses with high confidence that the demand for Initial Access Brokers services will continue to thrive in 2022, with more threat groups or individual actors attempting to sell access given the relatively low risk and high demand from various malicious groups.
- ZeroFox predicts that threat actors will look for and use new Java-based vulnerabilities to recreate the success of Log4j in the coming year.
- ZeroFox anticipates that cyber criminals will continue to use automation to fuel the growth of sophisticated Phishing-as-a-Service kits for sale and license.

EXECUTIVE SUMMARY

Threat actors around the world made 2021 an extremely stressful year for security teams—perhaps the most challenging year on record. The year began with the community still cleaning up the SUNBURST supply chain compromise and ended with a widespread and easy-to-exploit vulnerability in a common open source tool. In between, ZeroFox Intelligence observed record-setting ransomware incidents, more supply chain compromises, and increased geopolitical tensions in Europe and Asia. ZeroFox also was the first threat intelligence firm to discover a variant of ransomware called Colossus whose operators appeared to be at least highly familiar if not directly associated with other existing ransomware-as-a-service groups.

While law enforcement around the world have made progress at tracking and interdicting criminal cryptocurrency activity, and governments have debated new basic security requirements and regulation of cryptocurrencies, ZeroFox Intelligence does not forecast these achievements will result in a decrease in cyber crime for 2022. Software Bills of Material (SBOMs) should improve our visibility into the components and libraries embedded in enterprise software, and attack surface management programs will help reduce data breaches due to “shadow IT.” However, the threat landscape continues to find ways to exploit emerging technologies and business processes in our multi- and hybrid-cloud environments. Cyber criminals will also evolve their techniques for laundering the proceeds of their activities. We are confident 2022 will be another taxing year for security teams around the world.

At ZeroFox, we completed the integration of the former Cyveillance team and acquired Vigilante. The new ZeroFox Intelligence team, led by VP of Intelligence AJ Nash, is now poised for continued growth and delivery of intelligence across the physical and cyber domains. Our ability to detect threat infrastructure and activities increased dramatically as a result of these integrations and acquisitions, allowing ZeroFox to go further and disrupt threat actor infrastructure at a scale unmatched in the industry. Throughout 2022, ZeroFox Intelligence will continue to expand capabilities and improve our collection and analytical tradecraft to answer even more requirements for our customers.

Happy Threat Hunting!

ZeroFox Intelligence

2021 IN REVIEW

Ransomware

The frequency and scale of ransomware attacks globally reached an all-time high in 2021, impacting organizations of all sizes and across all geographic regions and verticals. Attacks also hit victims harder than in previous years, with reports indicating that average downtime reached a high of 23 days in 2021—up from 16 days in 2019.[1] The average cost of remediating ransomware attacks reached USD 1.85 million in 2021, up from approximately USD 750,000 in 2020.[2] The last year also saw the highest ransomware demands ever made, including the initial demand of USD 70 million by REvil to victims of the Kaseya ransomware attack in July.[3] The rise in Ransomware-as-a-Service (RaaS) offerings in 2021 lowered the barriers to entry for threat actors and put highly-effective malware in the hands of more operators. We also saw an increased proliferation of successor variants—malicious code developed from older, well-established ransomware strains.

High-profile ransomware attacks aimed at the Colonial Pipeline and a series of ransomware attacks targeting multinational companies spurred retaliatory action from law enforcement agencies against DarkSide operators and REvil, respectively, and was highly likely a driving factor in multiple threat actor collectives taking a break from activity—or closing down operations and restarting under a different name. This also likely contributed to the drop in "big game" hunting towards the end of 2021, with threat actors instead targeting small and medium-sized businesses.

Third-Party Compromises

Third-party compromises (TPC) continued to increase in frequency and scale throughout 2021. Remote-working solutions and the adoption of cloud infrastructure have necessitated that organizations utilize equipment produced by third parties and grant those third parties trusted access to sensitive information through platforms they produce. This has created a web of interdependent supply-chain companies and has massively expanded the cyber attack surface; one intrusion can create a platform from which threat actors can compromise the systems of hundreds—or thousands—of end users. Several high-profile attacks against software solutions in 2021 provided examples of the threat posed and damage inflicted by TPC attacks, such as those on SolarWinds (the fallout from which continued into 2021), Kaseya, and Accellion FTA, all of which were exploited and then used to pivot to targeting their partners.[4]

ZeroFox also observed an apparent rise in targeting of cloud computing solutions, remote working infrastructure, and managed software service providers (MSSPs) in 2021. These are targeted because of the trusted access afforded to vendors; when accessed, threat actors can easily pivot to other vulnerable targets within the software environment. One notable example of such an attack was the novel technique of ransomware being distributed via a fake software update.[5] Another notable TPC was the Colonial Pipeline attack in May 2021 carried out by Darkside, which reportedly leveraged compromised virtual private network (VPN) credentials to access and distribute ransomware. VPNs have been increasingly targeted in 2021; multiple vendors reported dramatic surges in attack volume, similar to that of attacks directed towards MSSPs.[6]

Malware-as-a-Service

In 2021, the cyber crime landscape continued to evolve to support a mature ecosystem of variously-motivated actors that specialize in the distribution of tools and methods for system and account compromises. ZeroFox ingested 19,460,794 account credentials harvested from information stealer logs out of the total volume of 1,424,411,700 compromised account credentials we collected in 2021.

The top five information stealers observed by ZeroFox in 2021 were Redline[7], Raccoon[8], Vidar[9], Dendevil, and Taurus; the first three are responsible for the majority of leaked credentials found in the ZeroFox botnet dataset. Unsurprisingly, given the subscription model, these strains of malware have a strong following among various bad actors and are readily deployed as-a-service against inadequately protected systems and users.

Chart 1: Top Five Botnet Families in 2021 / Source: ZeroFox Intelligence

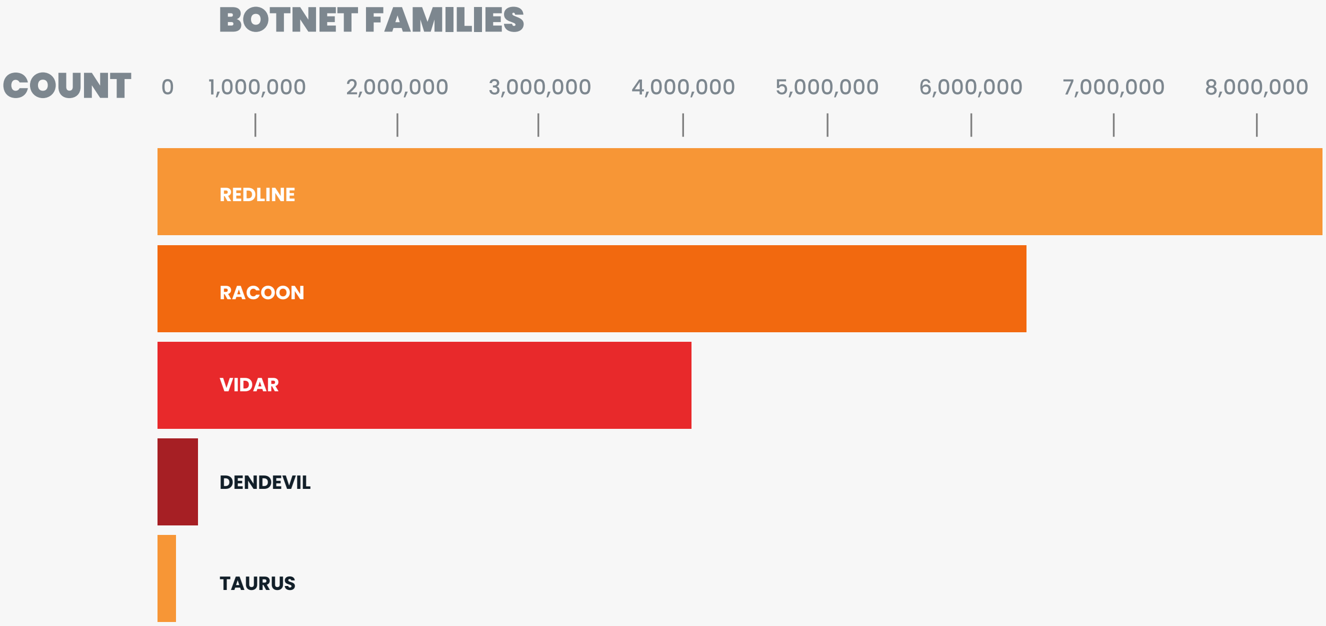
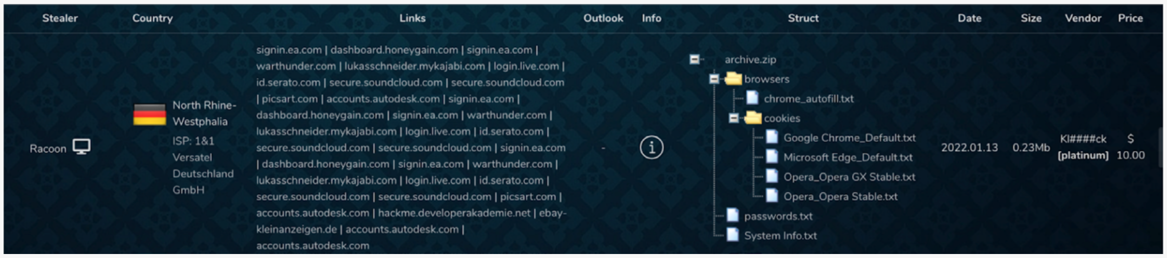


Figure 1: Example of sale of credentials obtained from Raccoon stealer / Source: ZeroFox Intelligence



Stealer	Country	Links	Outlook	Info	Struct	Date	Size	Vendor	Price
Racoon	North Rhine-Westphalia ISP: 1&1 Versatel Deutschland GmbH	signin.ea.com | dashboard.honeygain.com | signin.ea.com | warthunder.com | lukasschneider.mykajabi.com | login.live.com | id.serato.com | secure.soundcloud.com | secure.soundcloud.com | picsart.com | accounts.autodesk.com | signin.ea.com | dashboard.honeygain.com | signin.ea.com | warthunder.com | lukasschneider.mykajabi.com | login.live.com | id.serato.com | secure.soundcloud.com | secure.soundcloud.com | signin.ea.com | dashboard.honeygain.com | signin.ea.com | warthunder.com | lukasschneider.mykajabi.com | login.live.com | id.serato.com | secure.soundcloud.com | secure.soundcloud.com | picsart.com | accounts.autodesk.com | hackme.developerakademie.net | ebay-kleinanzeigen.de | accounts.autodesk.com | accounts.autodesk.com	-	ⓘ	archive.zip browsers chrome_autofill.txt cookies Google Chrome_Default.txt Microsoft Edge_Default.txt Opera_Opera GX Stable.txt Opera_Opera Stable.txt passwords.txt System Info.txt	2022.01.13	0.23Mb	Kl####ck [platinum]	$ 10.00

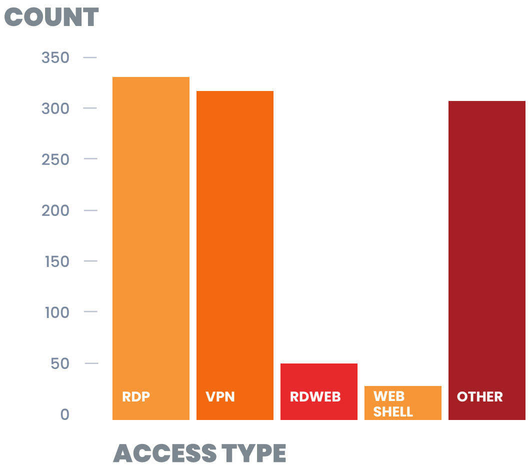
Initial Access Brokers

In 2021, ZeroFox observed a continued increase in the professionalization of the cybercriminal underground, as serious threat actors worked to establish their reputations as trustworthy and formidable brokers of access and data across various forums. Commonly known as "Initial Access Brokers" (IABs), these actors serve as intermediaries by targeting vulnerable organizations and selling access to them to the highest bidder—including ransomware groups across cyber criminal underground environments. Cyber criminals and ransomware operators are increasingly dependent on purchased initial access to gain a foothold into victims' networks, move laterally to advance their privileges, and deploy ransomware or conduct some other type of attack. Using IABs enables threat actors to avoid the time-consuming, laborious process of finding and compromising victims.

In 2021, ZeroFox analyzed 848 advertisements selling internal access to organizations across multiple industries posted by IABs to various underground forums. Our research revealed that Remote Desktop Protocol (RDP) and VPN access continued to be the leading commodities within the IAB market in 2021. In many cases, however, IABs were selling nondescript access to a victim company, and discussions about the vector of compromise typically took place through private chats.

Number of initial access broker by type

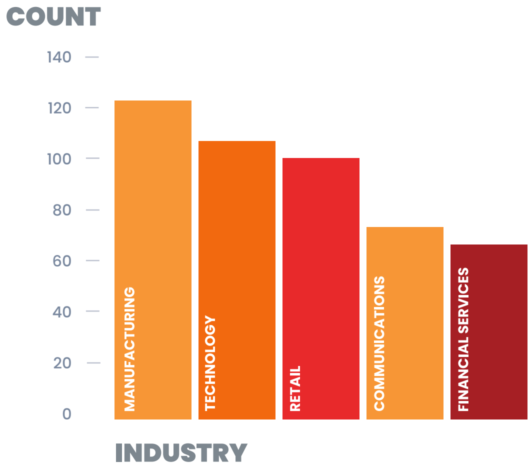
Chart 2: initial access brokers by Type / Source: ZeroFox Intelligence



Accesses obtained from IABs resulted in various corporations across multiple verticals being infected by ransomware in 2021. (See Chart 3 below.)

IAB total by industry

Chart 3: Initial access brokers by Industry / Source: ZeroFox Intelligence



ZeroFox observed the rise of ransomware and its financial returns parallel the services being offered by IABs. In 2021, prices for access varied between USD 1,000 and USD 30,000 depending on the type and level of access being sold and the organization's revenue, number of employees, and devices accessible. However, buying access still costs a fraction of the expected profit from a successful ransom payment. Additionally, some IABs worked to develop long-term relationships with certain ransomware groups, affiliates, or intermediaries and offered them the first right of refusal before making accesses available to others. As a result, ZeroFox observed that most conversations surrounding access, negotiations, and transactions typically occurred through private communication via Jabber, Telegram, or forum messages.

Vulnerabilities and Exploits

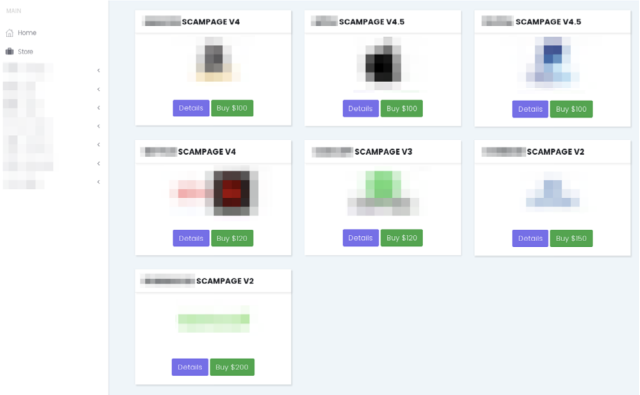
ZeroFox observed several significant, newly-disclosed vulnerabilities and powerful exploits in 2021 that resulted in major cybersecurity incidents that directly or indirectly impacted networks across the globe. This increase in reported vulnerabilities was partly due to the COVID-19 pandemic, which forced many organizations to hastily shift resources online without recommended security planning.

In light of the large volume and severity of the identified vulnerabilities, security professionals and IT teams had to work quickly in 2021 to patch and update vulnerable systems and software. The rapid weaponization of newly-discovered vulnerabilities by ransomware collectives or state-sponsored groups, as observed with Log4j and PrintNightmare, placed extra pressure on organizations.[10, 11] For instance, within weeks of the mid-December discovery of Log4j, reporting indicated that nation-state actors, botnets, and ransomware collectives had already created toolkits for mass-exploiting the vulnerability.

Phishing-as-a-Service

Phishing remained one of the most popular cyber crime threats in 2021, continuing the trend seen in the last several years. As such, ZeroFox researchers analyzed distribution of phishing kits from the perspective of the criminal underground and the phishing ecosystem, specifically focusing on the 16Shop and FreakzBrothers phishing kit distribution networks.[12] Threat actors within these groups developed kits utilizing a Phishing-as-a-Service framework (PhaaS)—which is similar to the Software-as-a-Service (SaaS) market in that it allows them to develop phishing kits for sale and to license these kits to operators for a cost—and advertised them for popular brands in the finance and retail spaces.

Figure 2. 16 Shop advertises phishing kits targeting multiple brands and platforms / Source: ZeroFox Intelligence



Cryptocurrency

Cryptocurrency adoption soared by nearly 900 percent in 2021, with emerging economies and global institutional investors adding cryptocurrencies to their balance sheets, more companies accepting cryptocurrency payments, and traditional fintech firms rolling out policies to accept crypto payments. [13]

The soaring popularity of cryptocurrency, the value of the digital currency, and the ease of use make cryptocurrency exchanges an attractive target for cyber criminals and suspected nation-state actors, who steal or manipulate the value of cryptocurrencies. The most prominent cryptocurrency theft took place in 2021, with the attack on a decentralized finance “DeFi” project named PolyNetwork, resulting in a loss of over USD 600 million. While more than 99 percent of the stolen money was returned to the firm, the attack surpassed the 2018 Coincheck theft of over USD 534 million.

2022 FORECAST & RECOMMENDATIONS

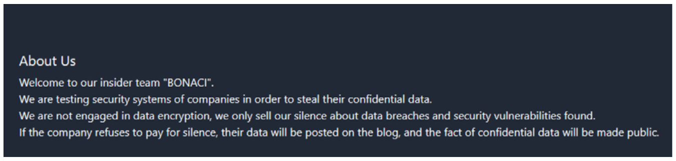
Ransomware

It is highly likely that ransomware will continue at an accelerated pace throughout 2022. Without substantial changes to security practices to prevent intrusion or changes in international laws preventing threat actors operating in bulletproof jurisdictions, the ransomware industry is highly likely to continue to thrive, targeting organizations of all sizes across all sectors. ZeroFox anticipates that the financial, manufacturing, retail, and healthcare sectors in particular will remain at increased threat from ransomware operators. While it is likely the early months of 2022 will see continued focus on the targeting of small and midsize businesses, it is anticipated that "big game hunting" will begin to re-emerge in later months. This may manifest in the targeting of MSSPs and other third-party services afforded privileged access to multiple customers' systems because these targets enable threat actors to infect numerous downstream organizations with a single intrusion.

Disruptive activity from law enforcement agencies is unlikely to have a sustained impact on ransomware operations. ZeroFox expects that groups targeted by such activity may temporarily halt operations or continue the cycle of shutting down and reemerging under a different name. The threat actors behind the most prevalent ransomware strains in 2021—Conti, REvil, LockBit, and BlackMatter—will likely continue to operate throughout 2022.

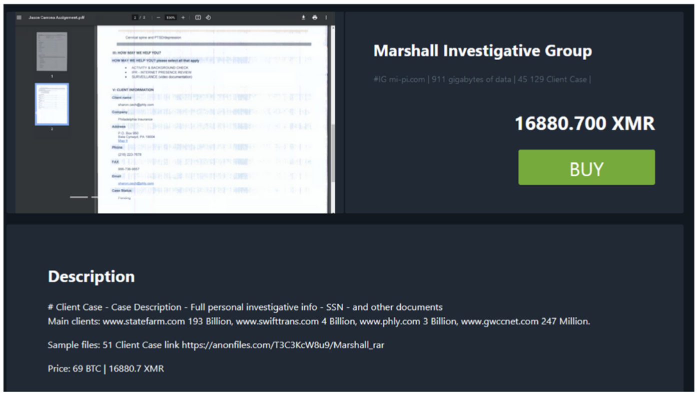
Following an emerging trend towards the latter half of 2021, ZeroFox anticipates threat actors will become increasingly focused on the information searched for, encrypted, and exfiltrated after the intrusion. This will involve conducting search strings to identify and exfiltrate business-critical information, the impact of which organizations cannot mitigate with simple security practices such as establishing offline backups. Targeted information is likely to include legal or insurance documents, business financial information, intellectual property, or market-sensitive information such as details of acquisitions or mergers. Such information can be leveraged by threat actors to demand a larger ransom payment and exert greater pressure on victims to pay. Ransomware developers are also likely to focus more on persistence, enabling threat actors to hit victims a second time even after security teams believe they have eliminated the initial threat.

Figure 3: Example of data offered by data kidnapping group "Bonaci" / Source: ZeroFox Intelligence



About Us

Welcome to our insider team "BONACI".
We are testing security systems of companies in order to steal their confidential data.
We are not engaged in data encryption, we only sell our silence about data breaches and security vulnerabilities found.
If the company refuses to pay for silence, their data will be posted on the blog, and the fact of confidential data will be made public.



Marshall Investigative Group

#IG mi-pi.com | 911 gigabytes of data | 45 129 Client Case |

16880.700 XMR

Description

Client Case - Case Description - Full personal investigative info - SSN - and other documents
Main clients: www.statefarm.com 193 Billion, www.swifttrans.com 4 Billion, www.phly.com 3 Billion, www.gwccnet.com 247 Million.

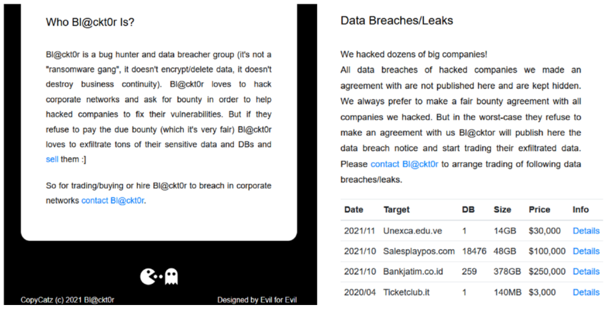
Sample files: 51 Client Case link https://anonfiles.com/T3C3KcW8u9/Marshall_rar

Price: 69 BTC | 16880.7 XMR

Aggressive law enforcement actions against ransomware groups in 2021 spurred some to move away from ransomware attacks in favor of data kidnapping schemes, which the groups judge as less risky. During a data kidnapping operation, the actor or group obtains the data by phishing, dumping of a misconfigured server, or other means and then threatens the victim company with leaking the data if payment is not made (see Figures 3 and 4). This differs from a ransomware attack in that the victim's files are not encrypted, and the victim has full control of its servers and operations but may want to avoid the embarrassment or fines associated with a known data breach.

Extortion tactics are likely to evolve as threat actors seek more effective means to coerce victims into paying ransoms. In addition to exfiltrating and leveraging sensitive business information, threat actors may also move towards targeting high-profile individuals to elicit payment. Threats to C-level executives and their families, or embroiling executives in illegal activity, are feasible scenarios.

Figure 4: Data kidnapping group "Bl@ckt0r" information and example of data offered on their website / Source: ZeroFox Intelligence



Who Bl@ckt0r Is?

Bl@ckt0r is a bug hunter and data breacher group (it's not a "ransomware gang", it doesn't encrypt/delete data, it doesn't destroy business continuity). Bl@ckt0r loves to hack corporate networks and ask for bounty in order to help hacked companies to fix their vulnerabilities. But if they refuse to pay the due bounty (which it's very fair) Bl@ckt0r loves to exfiltrate tons of their sensitive data and DBs and sell them :]

So for trading/buying or hire Bl@ckt0r to breach in corporate networks contact Bl@ckt0r.

CopyCatz (c) 2021 Bl@ckt0r

Designed by Evil for Evil

Data Breaches/Leaks

We hacked dozens of big companies!
All data breaches of hacked companies we made an agreement with are not published here and are kept hidden. We always prefer to make a fair bounty agreement with all companies we hacked. But in the worst-case they refuse to make an agreement with us Bl@cktor will publish here the data breach notice and start trading their exfiltrated data. Please contact Bl@ckt0r to arrange trading of following data breaches/leaks.

Date	Target	DB	Size	Price	Info
2021/11	Unexca.edu.ve	1	14GB	$30,000	Details
2021/10	Salesplaypos.com	18476	48GB	$100,000	Details
2021/10	Bankjatim.co.id	259	378GB	$250,000	Details
2020/04	Ticketclub.it	1	140MB	$3,000	Details

Intelligence Recommendations

Move from a **defense-in-depth** strategy to a **zero trust security** strategy.

- Segregate crown jewels and administrative accounts.
- Enforce multi-factor authentication (MFA) on remote access and administrative accounts.
- Monitor threat actor channels for compromised credentials.

Use **threat intelligence** to focus vulnerability management on **vulnerabilities being exploited.**

Reduce your attack surface.

- Disable admin and scripting tools (e.g., PowerShell) for users that do not need them to deny threat actors "living off the land binaries" (AKA LOLBins).
- Disable unnecessary or obsolete Windows and Linux components (e.g., SMB, macros from the Internet)
- Decommission remote access solutions that are no longer needed.

Prepare for a breach.

- Build relationships with law enforcement.
- Conduct tabletop exercises of incident response plans with law enforcement, legal, PR, etc.

Third-Party Compromises

ZeroFox assesses that TPC attacks are highly likely to continue on an upward trajectory in terms of frequency, scale, and sophistication during 2022. This assessment is underpinned by widespread reporting outlining the potential impact they can have and providing proof-of-concept for threat actors that may have previously deemed such attacks beyond their capability. [14, 15, 16]

The use of TPC as a means to distribute ransomware is likely to increase, driven in part by RaaS offerings lowering the barriers to entry for threat actors while putting effective malware in the hands of more operators. Ransomware-related attacks are likely to generate significant media coverage, possibly acting as a mitigating factor as threat actors look to avoid attention from authorities.

The continued expansion of software supply chains will also likely contribute to a rise in TPC attacks. ZeroFox expects smaller, third-party vendors within larger supply chains to be seen as weak links through which threat actors can target high-value, security-conscious organizations. As a result, organizations cannot focus solely on securing their own defenses and must ensure the security of their supply chain. Attacks that target vulnerabilities within remote working and cloud infrastructures are likely to increase, including those used in software modules and off-the-shelf packages.

There is also likely to be an increase in non-nation state and non-state-linked threat actors seeking to conduct TPC attacks. It is possible these could be directed at key events in 2022, such as the 2022 Winter Olympics in China, to cause disruption and reputational damage to event sponsors. Furthermore, as with the 2020 U.S. presidential election, the 2022 mid-term elections are likely to highlight the risks associated with third-party vendors. Election officials have focused on shoring up cybersecurity around the nation's voting systems because nation-states previously probed for vulnerabilities and, in a small number of cases, breached voter registration systems.

Intelligence Recommendations

Move from a **defense-in-depth strategy** to a **zero trust security strategy.**

- Disallow network connections except for those necessary for network and security tools to function (e.g., allow list for only the OEM and organization's assets).
- Monitor cyber threat communications channels for chatter regarding breaches to your third parties.
- Use attack surface management practices and netflows to detect probable ransomware breaches at your third parties.

Develop and maintain security contacts at key third parties for incident response planning.

Supply chain **incidents should be disclosed** with accurate and timely information provided to customers.

Malware-as-a-Service

ZeroFox assesses that, in 2022, underground criminal markets will continue to provide a lucrative outlet for various cyber criminals to peddle stolen credentials from various stages of an organization's network compromise. Given the increased prevalence and longevity of marketplaces, ZeroFox asserts that the increased usage of information stealers like Redline, Raccoon, and Vidar will continue to fuel widespread support from their developers and community. Moreover, given their efficacy and growing popularity, the already-multidimensional capabilities of these information stealers will likely expand and grow in 2022. ZeroFox predicts that competition among infostealer developers to gain consumers will increase, which will invariably encourage innovation among developers to build better, more sophisticated, and easier-to-use services as they try to distinguish themselves from competitors.

As infostealers significantly lower barriers to entry for low-level threat actors, ZeroFox does not see a downtrend in the use of these malicious tools.

Botnet logs provided from these information stealers aid in gaining additional access to other services through credential harvesting, obtaining sensitive information, or assisting in deploying additional payloads.

> *The versatile nature of information stealers and their capability to steal such a variety of sensitive data makes them a threat to all organizations across all industries.*

ZeroFox recommends limiting employees utilizing personal devices for work-related activities and encouraging them to not reuse personal passwords for corporate accounts.

Intelligence Recommendations

Provide company devices for **business activities** rather than BYOD.

Discourage password reuse between personal and business accounts and encourage using business email for business purposes only.

Enforce MFA for all remote access to company assets.

Create access policies informed by **continuous, contextual, and risk-based verification** across users and their associated devices.

Initial Access Brokers

ZeroFox predicts with high confidence that the demand for IAB services will likely continue to thrive in 2022, as the evolving symbiotic relationship between access brokers and ransomware operators continues at an accelerated pace given the return on investment that IABs provide. Such relationships will continue to facilitate persistent targeting of entities across multiple industries and streamline the network compromise process, allowing threat actors to act quickly and more efficiently. ZeroFox projects that more groups or various insidious individuals will participate and attempt to sell access to various organizations, given the relatively low risk and high demand from various malicious groups.

Intelligence Recommendations

Continually audit remote access accounts and disable those no longer necessary.

Develop an attack surface management program that continually monitors for exploitable assets exposed on the internet.

Enforce MFA on remote access accounts.

Leverage a trusted vendor to monitor threat actor channels (forums, marketplaces, messaging platforms) for compromised credentials.

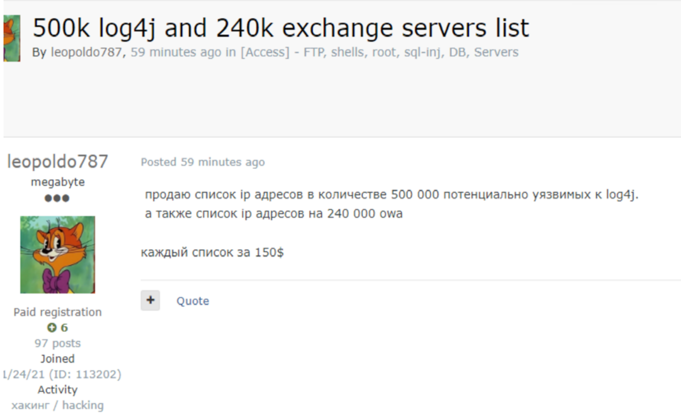
Vulnerabilities and Exploits

Based on the trends observed in 2021, ZeroFox judges that Log4j showcased a critical problem in today's software ecosystem that will likely carry over into 2022. Namely, vulnerabilities that exist in packages that are bundled and imported in a wide range of applications will likely continue to appeal to attackers looking to maximize the effect of their work. Threat actors are likely to take the time to find consistent inputs from a diversity of applications that ultimately lead to the same vulnerable functions within very popular libraries. This could potentially allow attackers to develop a working exploit for a wide variety of applications, increasing the amount of potential targets while reducing the level of effort.

> *ZeroFox predicts that nefarious actors will research more Java-based exploit avenues, focusing on common libraries exposed to attacker control content.*

ZeroFox also forecasts that threat actors—pivoting off of access obtained from exploiting the Log4j vulnerability—will compromise systems, extract personally identifiable information (PII), and conduct data extortion schemes. As of early January 2022, threat actors had already begun to tout and sell access to hundreds of thousands of unpatched servers vulnerable to the Log4j exploit (see Figure 4).

Figure 4: Post by threat actor "leopoldo787" advertising 500,000 unpatched servers / Source: ZeroFox Intelligence



500k log4j and 240k exchange servers list

By leopoldo787, 59 minutes ago in [Access] - FTP, shells, root, sql-inj, DB, Servers

leopoldo787
megabyte
●●●
Paid registration
6
97 posts
Joined
1/24/21 (ID: 113202)
Activity
хакинг / hacking

Posted 59 minutes ago

продаю список ip адресов в количестве 500 000 потенциально уязвимых к log4j.
а также список ip адресов на 240 000 owa

каждый список за 150$

Intelligence Recommendations

Develop an attack surface management program that continually monitors for company assets and integrate that data into your **vulnerability management tools.**

Use **vulnerability intelligence** to focus remediation efforts on known exploited vulnerabilities rather than critical and high CVSS scores.

Use SBOMs to discover and inventory software components and libraries.

Phishing-as-a-Service

In 2022, ZeroFox expects cyber criminals to continue to use sophisticated phishing kits and automation to take cyber crime to a new level, fueling the growth of PhaaS. These types of kits may vary in complexity and sophistication and can be purchased via criminal underground networks, covert channels, and sometimes clear web platforms.

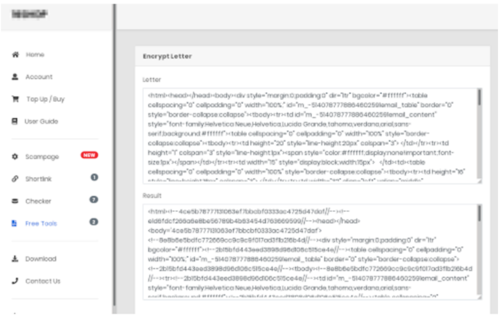
This type of cyber crime business model presents a few major benefits to the kit creators:

- Kit deployments have to be validated, and unauthorized users (or those that have not paid) will be unable to fully deploy the phishing kit.
- Lower skilled actors have a turn-key approach to phishing kit deployment at their fingertips.
- Kit creators charge licenses and can receive regular monthly payments, not unlike legitimate business models for SaaS applications.
- The use of obfuscated code or digital rights management (DRM) in these kits reduces the risk of kits being taken and resold to other threat actors.

Operators that purchase kits from these platforms are often supplied with most (if not all) necessary resources by the kit creator. This can include tools to rapidly deploy landing pages, detection evasion tools, and even interfaces to generate obfuscated HTML templates that will bypass anti-spam or phishing email checks and arrive successfully in the recipient's inbox.[17]

ZeroFox specializes in tracking how threat actors monetize victim data and fraud, as well as how they distribute compromised credentials from phishing attacks. Threat actors that partake in phishing kit distribution can benefit from using criminal underground networks and covert channels to advertise their kits and even automate transactions by using bots to sell compromised data.[18] Because of improving and evolving security technologies designed to detect phishing kits and websites, threat actors are constantly changing their TTPs to evade detection and continue their lucrative operations. ZeroFox assesses that PhaaS will continue in 2022 with evolved tactics and sophisticated techniques to conduct credential phishing attacks.

Figure 5: Storefront of a well-known phishing kit provide / Source: ZeroFox Intelligence



Encrypt Letter

Letter

```
<html><head></head><body><div style="margin:0;padding:0" dir="ltr" bgcolor="#ffffff"><table
cellspacing="0" cellpadding="0" width="100%;" id="m_-5140787778864602591email_table" border="0"
style="border-collapse:collapse"><tbody><tr><td id="m_-5140787778864602591email_content"
style="font-family:Helvetica Neue,Helvetica,Lucida Grande,tahoma,verdana,arial,sans-
serif;background:#ffffff"><table cellspacing="0" cellpadding="0" width="100%" style="border-
collapse:collapse"><tbody><tr><td height="20" style="line-height:20px" colspan="3"> </td></tr><tr><td
height="1" colspan="3" style="line-height:1px"><span style="color:#ffffff;display:none!important;font-
size:1px"></span></td></tr><tr><td width="15" style="display:block;width:15px"> </td><td><table
cellspacing="0" cellpadding="0" width="100%" style="border-collapse:collapse"><tbody><tr><td height="16"
```

Result

```
<html><!--4ce5b78777131063ef7bbcbf0333ac4725d47daf//--><!--
eld6fdcf266a6e8be56789b4b63454d763669599//--><head></head>
<body='4ce5b78777131063ef7bbcbf0333ac4725d47daf>
<!--8e8b6e5bdfc772669cc9c9c9f017ad3f1b216b4d//--><div style="margin:0;padding:0" dir="ltr"
bgcolor="#ffffff"><!--2bl5bfd443eed3898d96d106c515ce4e//--><table cellspacing="0" cellpadding="0"
width="100%;" id="m_-5140787778864602591email_table" border="0" style="border-collapse:collapse">
<!--2bl5bfd443eed3898d96d106c515ce4e//--><tbody><!--8e8b6e5bdfc772669cc9c9c9f017ad3f1b216b4d
//--><tr><!--2bl5bfd443eed3898d96d106c515ce4e//--><td id="m_-5140787778864602591email_content"
style="font-family:Helvetica Neue,Helvetica,Lucida Grande,tahoma,verdana,arial,sans-
```

Intelligence Recommendations

Integrate tactical threat intelligence into your email security gateways, SOC, and phishing reporting processes.

Enforce MFA on remote access accounts.

Retain phishing samples in your threat intelligence platform for metrics, analysis, and enrichment of new phishing alerts.

Use **external threat intelligence service** to continually identify domains and websites impersonating your brand and automatically disrupt that criminal infrastructure.

Cryptocurrency

ZeroFox expects remittance-heavy economies to move towards digital currencies in 2022 at a faster pace, especially in the Middle East and Central Europe. Crypto's threat to long-established currencies, like the U.S. dollar and the Euro, could result in further efforts to regulate the industry. Since enforcing its crypto mining ban in mid-2021 in light of concerns over heavy energy usage associated with mining Bitcoin, China went from mining about two-thirds of all Bitcoin to none within a month. Iran and Venezuela are also notable Bitcoin mining hotspots relative to their population and economic power, as crypto has a reputation of being used by dictators to evade sanctions, launder money, and disrupt the U.S. dollar-based economic system. Further regulation of the sector is likely to come from the traditional economic powers, with the United States rolling out new tax reporting requirements last year that will continue into 2022[19] and the EU exploring a digital Euro to compete with cryptocurrencies in the coming years.

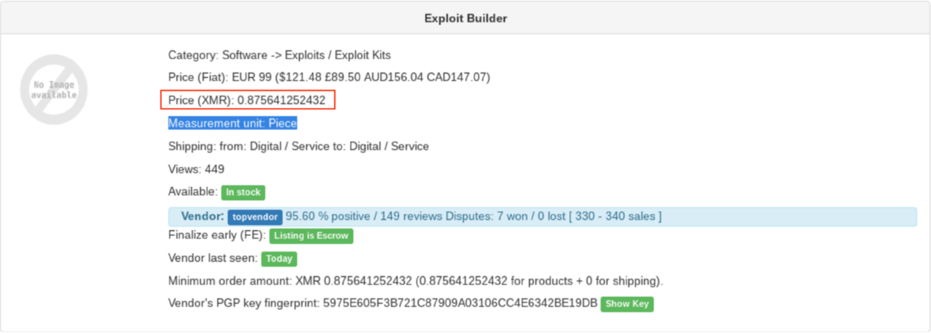
ZeroFox predicts continued attacks on crypto exchanges in 2022. In addition to causing financial damage, threat actors may seek to exploit blockchain companies, which collect a vast amount of data from their customers for security reasons, with the aim of stealing customer PII.

While attacks on crypto exchanges will continue, a hack on a crypto exchange does not necessarily mean users will lose their money. Nevertheless, ZeroFox recommends basic security measures when accessing any crypto account, including enabling two-factor authentication or using hardware keys.

As cyber criminals find new methods to steal investors' financial assets and as cryptocurrency attacks become more targeted, digital currency exploits will not be reserved for cyber criminals. Nation-states will also likely continue to attack the cryptocurrency industry at a higher rate in 2022 as a way to generate funds for governments circumventing various economic sanctions.

Cyber criminals are likely to expedite their transition from Bitcoin to Monero[20] as the preferred cryptocurrency to facilitate transactions in response to more aggressive law enforcement operations and government scrutiny. Careful and more reputable actors are making the switch, and ZeroFox assesses it is likely that Monero use will increase more broadly in 2022 amongst the threat actor community, as observed on Dark Web marketplaces White House Market and AlphaBay (see Figures 6 and 7).

Figure 6: Criminal marketplace White House Market illustrating Monero as the only accepted cryptocurrency on the site / Source: ZeroFox Intelligence



Exploit Builder

Category: Software -> Exploits / Exploit Kits

Price (Fiat): EUR 99 ($121.48 £89.50 AUD156.04 CAD147.07)

Price (XMR): 0.875641252432

Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 449

Available: In stock

Vendor: topvendor 95.60 % positive / 149 reviews Disputes: 7 won / 0 lost [330 - 340 sales]

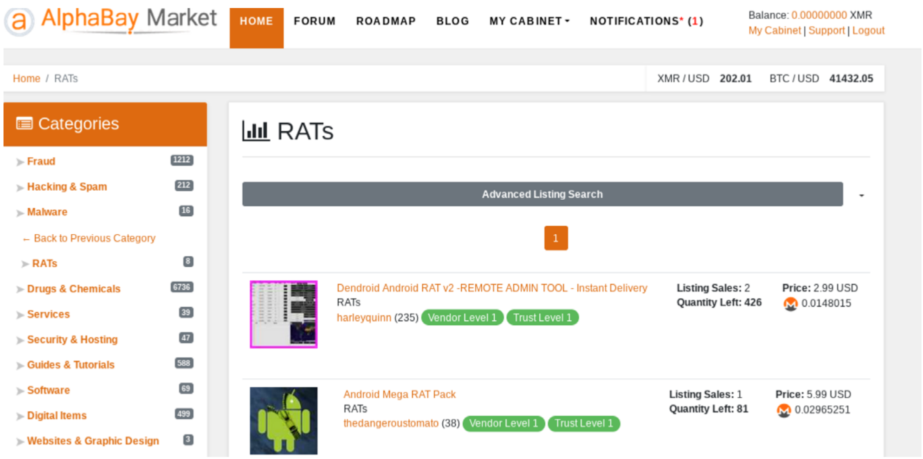
Finalize early (FE): Listing is Escrow

Vendor last seen: Today

Minimum order amount: XMR 0.875641252432 (0.875641252432 for products + 0 for shipping).

Vendor's PGP key fingerprint: 5975E605F3B721C87909A03106CC4E6342BE19DB Show Key

Figure 7: Criminal marketplace AlphaBay with Monero as the preferred cryptocurrency / Source: ZeroFox Intelligence



Balance: 0.00000000 XMR

XMR / USD 202.01 BTC / USD 41432.05

Fraud	1212
Hacking & Spam	212
Malware	16
RATs	8
Drugs & Chemicals	6736
Services	39
Security & Hosting	47
Guides & Tutorials	588
Software	69
Digital Items	499
Websites & Graphic Design	3

RATs

Dendroid Android RAT v2 -REMOTE ADMIN TOOL - Instant Delivery
RATs
harleyquinn (235) Vendor Level 1 Trust Level 1
Listing Sales: 2
Quantity Left: 426
Price: 2.99 USD
0.0148015

Android Mega RAT Pack
RATs
thedangeroustomato (38) Vendor Level 1 Trust Level 1
Listing Sales: 1
Quantity Left: 81
Price: 5.99 USD
0.02965251

Intelligence Recommendations

Report criminal cryptocurrency wallets to law enforcement as soon as possible to increase the likelihood of interdicting cryptocurrency laundering.

Leverage external threat intelligence services to **monitor** criminal usage of cryptocurrencies.

SUMMARY OF RECOMMENDATIONS

Move from a **defense-in-depth strategy** to a **zero trust security strategy.**

- Segregate crown jewels and administrative accounts.
- Enforce multi-factor authentication (MFA) on remote access and administrative accounts.
- Create access policies informed by continuous, contextual, and risk-based verification across users and their associated devices.
- Disallow network connections except for those necessary for network and security tools to function (e.g., allow list for only the OEM and organization's assets).
- Continually audit remote access accounts and disable those no longer necessary.

Reduce your attack surface.

- Develop an attack surface management program that continually monitors for company assets and integrate that data into your vulnerability management tools.
- Disable admin and scripting tools (e.g., PowerShell) for users that do not need them to deny threat actors "living off the land binaries" (AKA LOLBins).
- Disable unnecessary or obsolete Windows and Linux components (e.g., SMB, macros from the internet).
- Decommission remote access solutions that are no longer needed.

Use threat intelligence to improve SOC and DFIR metrics.

- Integrate tactical threat intelligence into your email security gateways, SOC, and phishing reporting processes.
- Monitor cyber threat communications channels for compromised credentials and chatter from the criminal underground.
- Use vulnerability intelligence to focus remediation efforts on known exploited vulnerabilities rather than critical and high CVSS scores.
- Leverage external threat intelligence services to monitor criminal usage of cryptocurrencies.
- Use an external threat intelligence service to continually identify domains and websites impersonating your brand and automatically disrupt that criminal infrastructure.

Prepare for a breach.

- Build relationships with law enforcement.
- Conduct tabletop exercises of incident response plans with law enforcement, legal, PR, etc.
- Develop and maintain security contacts at key third parties for incident response planning.
- Use threat intelligence and attack surface management programs to support third-party risk management.
- Supply chain incidents should be disclosed with accurate and timely information provided to customers.

Use attack surface management practices and netflows to detect probable ransomware breaches at your third parties.

- Leverage your attack surface management program to monitor for third party risks to your company.
- Use threat intelligence to identify likely abuses of your third parties people and trademarks.

Conclusion

Threats will not abate in 2022. Security teams must resource their teams and employ strategies to address emerging threat tactics, techniques, and procedures—not last year's TTPs. Security leaders should monitor geopolitical fluctuations and macroeconomic trends to provide indications and warnings of state-nexus and criminal threat actors' next targets.

Threat intelligence can help overburdened security teams struggling to keep pace with breaches, vulnerability disclosures, and the media cycle of attacks by focusing their attention on relevant threats. ZeroFox Intelligence will continue to grow and expand our visibility into the threat landscape to ensure our customers have the predictive intelligence needed to protect their customers, employees, and intellectual property.

Please take our four question survey after reading this forecast. Your feedback is critical to ensuring ZeroFox Intelligence is delivering insights you need to gain a decision advantage over the threat landscape.

TAKE SURVEY

RESOURCES

1. hxxps://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
2. hxxps://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
3. hxxps://www.bleepingcomputer.com/news/security/revil-ransomware-asks-70-million-to-decrypt-all-kaseya-attack-victims/
4. hxxps://www.zdnet.com/article/asic-reports-server-breached-via-accellion-vulnerability/
5. hxxps://www.risk based security.com/2021/07/12/the-kaseya-attack-everything-to-know/
6. hxxps://www.helpnetsecurity.com/2021/06/15/vpn-attacks-up/
7. Redline harvests credentials, targets individual crypto wallets, and steals system information. See hxxps://any.run/malware-trends/redline for additional details.
8. Raccoon harvests credentials and personally identifiable information and is leveraged to install other pieces of malware; it is observed in a multitude of entry points or is bundled with other software from non-reputable sources. See hxxps://any.run/malware-trends/raccoon for additional details.
9. Vidar stealer is mainly bundled with cracked commercial software or distributed via malvertising and attempts to harvest credentials, device information, and browser history. This collection is exfiltrated to the attackers' command and control servers, with exfiltrated log data being sold in the dark web. See hxxps://malware.news/t/deep-analysis-of-vidar-stealer/49591 for additional details.
10. hxxps://www.zdnet.com/article/ransomware-now-attackers-are-exploiting-windows-print nightmare-vulnerabilities/
11. hxxps://www.bleepingcomputer.com/news/security/translated-conti-ransomware-playbook-gives-insight-into-attacks/
12. https://www.zerofox.com/blog/16shop-cash-app-phishing-kit/
13. hxxps://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/
14. hxxps://security boulevard.com/2021/06/third-party-data-breaches-a-rising-threat/
15. hxxps://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html
16. hxxps://www.kaspersky.com/about/press-releases/2021_partnership-costs-third-party-incidents-became-most-costly-enterprise-data-breaches-in-2021
17. https://www.zerofox.com/blog/phishing-kit-lure-distribution/
18. https://www.zerofox.com/blog/phishing-kit-victim-workflow-and-data-exfiltration/
19. hxxps://www.natlawreview.com/article/infrastructure-bill-contains-new-cryptocurrency-reporting-requirements
20. Monero (XMR) has been around since 2014 and is harder to trace than Bitcoin because Monero uses ring signatures and stealth addresses to hide the identities of the sender and the receiver.

About ZeroFOX

ZeroFOX provides enterprises protection, intelligence and disruption to dismantle external threats to brands, people, assets and data across the public attack surface in one, comprehensive platform. With complete global coverage across the surface, deep and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFOX Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more. The patented ZeroFOX Platform technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email and more.