



| Brief |

The Underground Economist: Volume 4, Issue 13

B-2024-06-28a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web

June 28, 2024

Scope Note

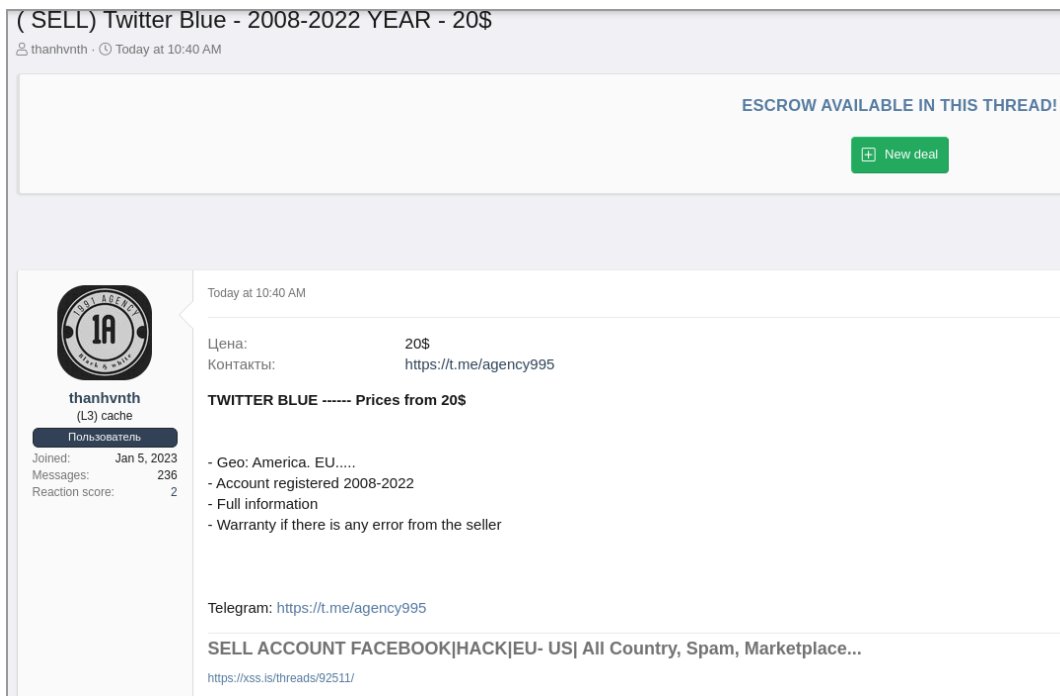
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 12:00 AM (EDT) on June 28, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | The Underground Economist: Volume 4, Issue 13

| Threat Actor Sells Blue X Accounts

On June 18, 2024, positive reputation actor “thanhvnth” announced the sale of verified X (formerly Twitter) “Blue” accounts on the Russian-speaking community xss Such services are widespread in deep and dark web (DDW) marketplaces, and ZeroFox has observed a significant uptick in the number of threat actors selling X accounts since the start of 2024.

- The actor stated that accounts for sale start at USD 20—an inflated price in comparison to ordinary X accounts purchasable from automated shops (often for less than one dollar).
- Thanhvnth claimed that the accounts come with a warranty and are designed to be identified as U.S. or European Union (EU)-based individuals registered between 2008–2022 with full information in order to appear to be legitimate individual users.
- Purchases are to be completed manually via the actor’s Telegram account.



Thanhvnth's post advertising blue X accounts for sale

Source: ZeroFox Intelligence

This service is almost certainly evidence of continuous threat actor interest in utilizing X accounts for malicious purposes. In this case, the accounts offered for sale are likely more convincing and come with capabilities beyond those of regular accounts, due to the X Blue subscription. It is likely the threat actor chose to promote U.S and EU account geolocation because such accounts may be more effective in targeting Western users with malicious activity, including—but not limited to—financial scams, disinformation campaigns, and impersonations.

X accounts are very likely favored amongst a wide array of threat actors, given the perceived benefits of operating on X versus other platforms. X accounts are almost certainly being increasingly implicated in various types of cybercrime that target individuals and organizations. This is enabled, to some extent, by:

- The allegedly lower levels of active internal regulation of accounts by X in comparison to its predecessor, Twitter. This results in fewer instances of accounts being suspended or banned for conveying controversial speech or otherwise violating the platform's user guidelines.

- The ability of threat actors to leverage licit as-a-service tools to bypass Know Your Customer (KYC) protocols, which are often associated with the creation of social media accounts. This aids the automated registration of large numbers of accounts for a small price and in a short period of time—accounts which are then used to conduct various nefarious activities without fear of reprisal.
- The inherent anonymity often associated with X in comparison to other social media platforms, where users expect profiles to contain overt links to other legitimate profiles as a display of authenticity. This enables and encourages antisocial behavior.
- The ability for users to engage with audiences far beyond their immediate following. This increases opportunities for malicious messages or services to be publicized.
- The payments from the platform to users that are part of the Creator Ads Revenue Sharing Program and receive at least 5 million organic impressions on a post. This encourages the posting of contentious or inflammatory language that may be more likely to be widely shared.

| New Malicious Tool Advertises Comprehensive Personal Information

On June 16, 2024, a positive-reputation actor known as “spam_assistant” announced a new tool called Data Fusion in the dark web forum Exploit. According to the advertisement, Data Fusion is capable of providing buyers with a significant amount of both personally identifiable information (PII) pertaining to individuals and organizational tax data. The service is currently available via spam_assistant’s Telegram channel.

- PII is easily monetized in DDW marketplaces due to a consistent demand from threat actors with various motivations. It is usually sold either in the form of a complete data breach or via automated tools able to offer the buyer specific information.

Spam_assistant alleged that they are in possession of data entries numbering in the billions pertaining to “all people in the world.” Three hundred fifty million of these records are purported to be U.S.-based, and the actor claims to have various tax data for “more

than half” of all U.S. organizations. Data Fusion can allegedly provide buyers with data such as:

- Social Security numbers (SSNs)
- Addresses, ZIP codes, and dates of birth (DOBs)
- Driver’s license numbers
- Taxpayer Identification Numbers (TINs) and Employer Identification Numbers (EINs)

spam_assistant

kilobyte



Paid registration

31 posts

Joined

07/10/20 (ID: 106192)

Activity

cnam / spam

Posted 34 minutes ago

We are happy to announce that we are launch Data Fusion! We created Automatized huge storebot marketplace for all.

We have billions of data - all people in the world. (In different countries)

We have a base of more than 100m SSN data, and we can also find any SSN/DL, even that we do not have - and all this for our lovely customers.

We have a database of almost 350m US and we create own BG. Data Fusion Reports.

We have ALL EINs/TINs more than half US companies.

WE HAVE API FOR RESELLERS! and we can create duplicate our bot in few minutes for each reseller!

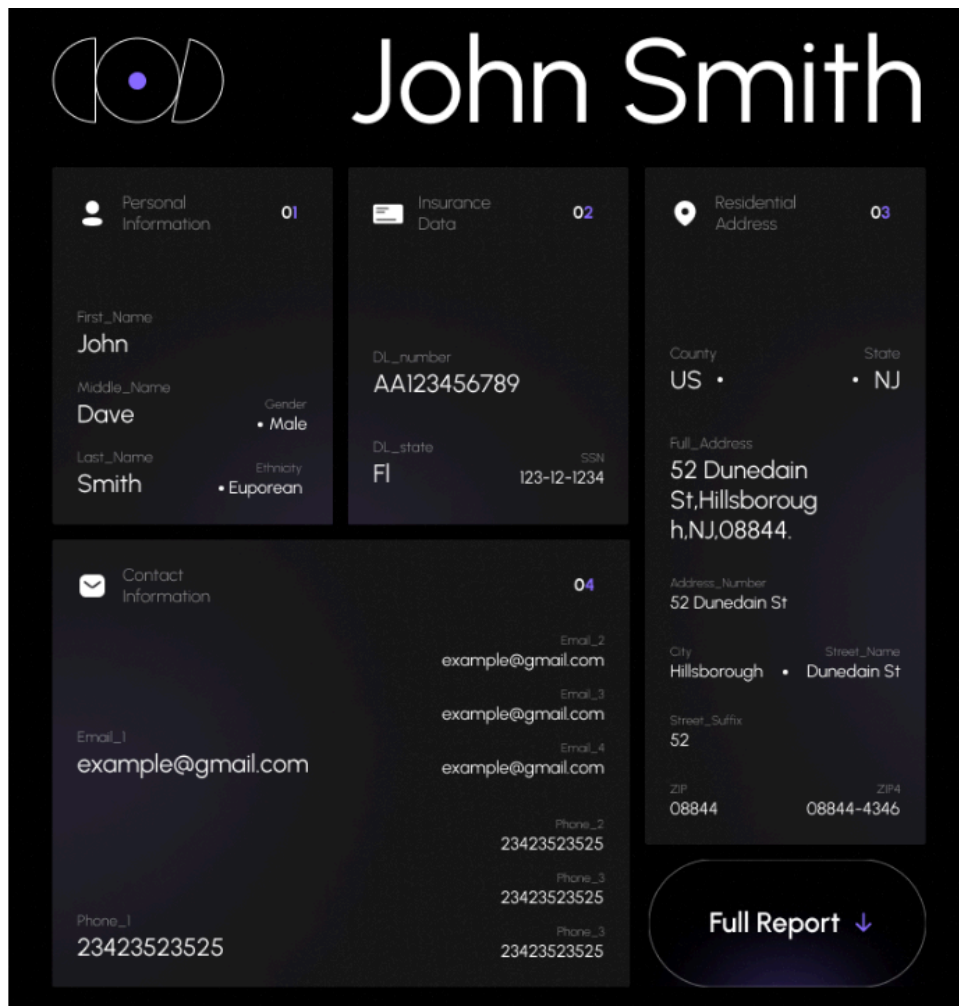
DataFusion - We find All info about everyone to anyone!

Exploit post advertising the the launch of Data Fusion

Source: ZeroFox Intelligence

Unlike similar DDW services offering the sale of PII, Data Fusion is allegedly capable of creating bespoke background reports that summarize the requested data. The price of these reports varies depending upon the type of information requested, and—though discounts are available for bulk sales—no subscription-based model is available. As a result, Data Fusion is almost certainly more expensive than other methods of purchasing PII, many of which offer partial results for free.

- Data Fusion also allows resellers to access its Application Programming Interface (API), where they can advertise the platform’s information. This is almost certainly intended to increase the service’s market reach.



Example of custom Data Fusion report

Source: ZeroFox Intelligence

The extent of information offered by Data Fusion is almost certainly exaggerated. Spam_assistant very likely leverages a large and diverse number of data sources, including those that are publicly available (such as various government resources and historic data breaches, many of which very likely contain incorrect or extant information) and contemporary data breaches (many of which carry a price tag). It is unlikely that comprehensive and accurate information can be provided at the advertised breadth.

- While spam_assistant claims that Data Fusion is an automated service, this is likely only partially true. The tool almost certainly requires a human element able to search for, compile, and supply the requested data.

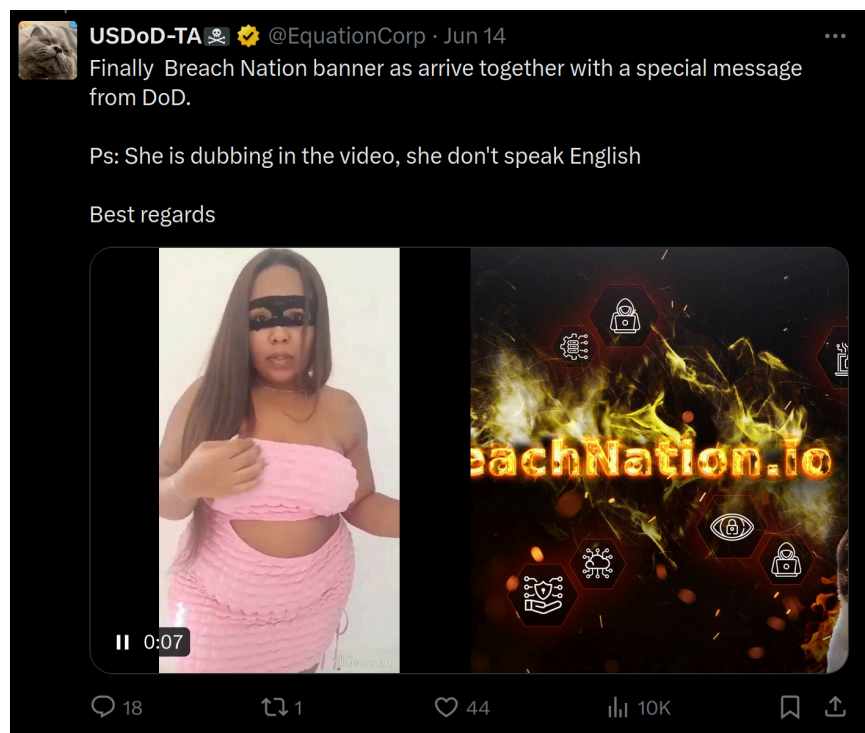
PII such as that advertised by spam_assistant is an integral aspect of many forms of cyberattack. Personal details are used to inform and enhance sophisticated social engineering attacks, such as spear phishing and business email compromise, or to enable fraudulent activity like identity theft and tax-related scams. PII is also regularly resold in other DDW forums, though—given the comparatively high price of Data Fusion—this is less likely.

Given the high and continuous demand for sensitive data such as PII, threat actors are almost certain to continue pursuing innovative, automated tools able to draw from an increasingly expansive repository of both publicly available information and illicit data leaks.

| Breach Nation Forum Continues to Gain Traction

On June 14, 2024, positive-reputation actor “USDoD” posted a thread on the social media platform X advertising a banner for their new hacking forum, “Breach Nation.” The thread also included the planned domain-breachnation[.]io, which ZeroFox can confirm was registered as of the writing of this report.

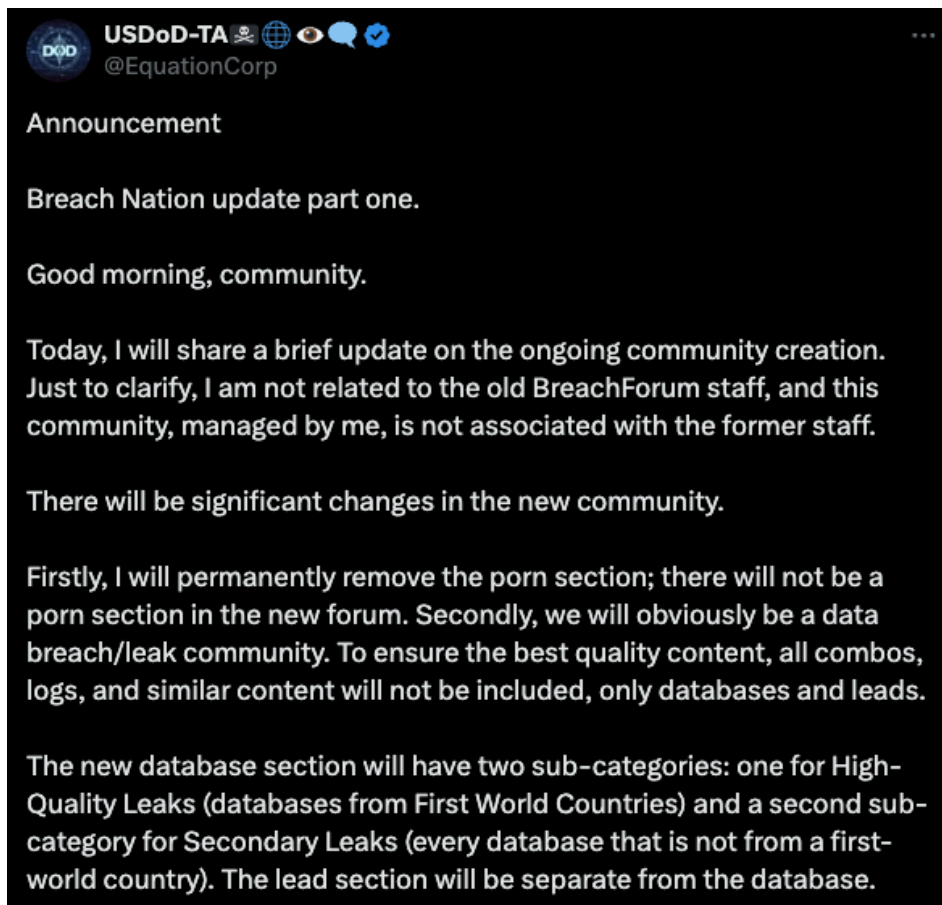
- Breach Nation was first announced by USDoD in an X thread on May 15, 2024. This coincided with the severe disruption of the popular hacking forum BreachForums, which occurred following a law enforcement (LE) operation that seized the forum’s clear web and dark web domains, as well as a Telegram channel.

**X post by USD0D advertising Breach Nation**

Source: ZeroFox Intelligence

BreachForums has made a significant resurgence in recent weeks, with actor “ShinyHunters”—who was suspected by some peers to be assisting an unspecified LE operation—rescinding their role as forum administrator. The actor “IntelBroker” also assisted in renewing BreachForums’ traction by returning to the forum with several high-profile leaks.

The revival of BreachForums had a very high chance of rendering Breach Nation (and other alternative, successor forums) obsolete due to its established reputation, user base, and infrastructure. Instead, on June 17, 2024, Breach Nation was the subject of significant discussion in a BreachForums thread.

**USDod provides insight as to intended Breach Nation features**

Source: [hXXps://x\[.\]com/EquationCorp/status/1792571853904511048](https://x[.]com/EquationCorp/status/1792571853904511048)

Many actors expressed positive expectations for Breach Nation, such as anticipating the platform including fewer paywalls than BreachForums. Users also very likely view Breach Nation as lower risk due to ongoing suspicion of BreachForums possible LE operations, and many are likely disgruntled with what is perceived as the inconsistent moderation of BreachForums in recent weeks.

06-17-2024, 10:38 PM

#1

So if you don't know back when baph was taken by a UFO on the water and Shiny took the site back and showed how the FBI didn't even fully take the site and then Shiny left (This shit will make a good movie)

A user who goes by USDoD made a post on twitter back when baph was taken on how he or she was gonna make a new better forum and it seems to be in full play and might come faster than we though since Shiny left

So as a user of BF I wanna know what do you think about this and do you support it as a person who belives in freedom I like this move as this gives people more sites to leak DB and more.

And as always have a wonderful day and I love you all @[@komi](#) ever you bbg 😊

 PM Find Reply Quote Report

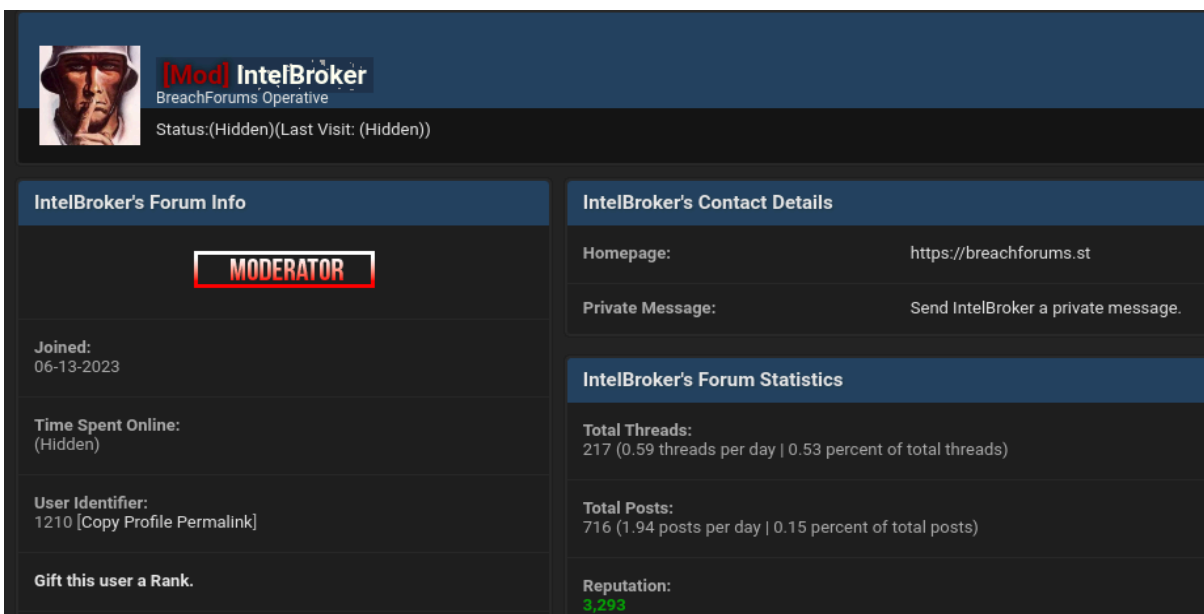
BreachForums post discussing Breach Nation

Source: ZeroFox Intelligence

While it is too early to predict if Breach Nation will be a success, its continued traction—despite the resurgence of BreachForums—is reflective of an appetite amongst the hacking community for a new, competitive option.

IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

On June 13, 2024, prominent and well-regarded threat actor IntelBroker registered an account on the popular illicit hacking forum BreachForums—one day after removing themselves from the platform. Shortly after rejoining, IntelBroker resumed publishing numerous high-profile data leaks.



The screenshot displays the profile of a user named IntelBroker on the BreachForums platform. The profile header includes a user avatar, the name [Mod] IntelBroker, the role BreachForums Operative, and a hidden status and last visit. The profile is divided into two main sections: IntelBroker's Forum Info and IntelBroker's Contact Details. The Forum Info section shows a Moderator badge, join date (06-13-2023), hidden time spent online, user identifier 1210 with a copy profile permalink, and a gift rank button. The Contact Details section shows the homepage (https://breachforums.st) and a private message button. A separate section, IntelBroker's Forum Statistics, shows 217 total threads (0.59 threads per day) and 716 total posts (1.94 posts per day). The reputation is 3,293.

IntelBroker's Forum Info	IntelBroker's Contact Details
MODERATOR	Homepage: https://breachforums.st
Joined: 06-13-2023	Private Message: Send IntelBroker a private message.
Time Spent Online: (Hidden)	IntelBroker's Forum Statistics
User Identifier: 1210 [Copy Profile Permalink]	Total Threads: 217 (0.59 threads per day 0.53 percent of total threads)
Gift this user a Rank.	Total Posts: 716 (1.94 posts per day 0.15 percent of total posts)
	Reputation: 3,293

IntelBroker's new BreachForums profile

Source: ZeroFox Intelligence

A subsequent spate of posts advertising numerous allegedly successful data breaches and illicit network accesses was very likely enabled in part by the exploitation of a zero-day vulnerability that targets Atlassian Jira software via remote code execution. On June 16, 2024, IntelBroker advertised this vulnerability for sale, which was then marked as "sold" between June 20 and June 24, 2024.

The vulnerability, which is allegedly capable of bypassing an Okta single sign-on credentials prompt, was advertised for a significant price of USD 800,000, though the final sale price was likely lower.

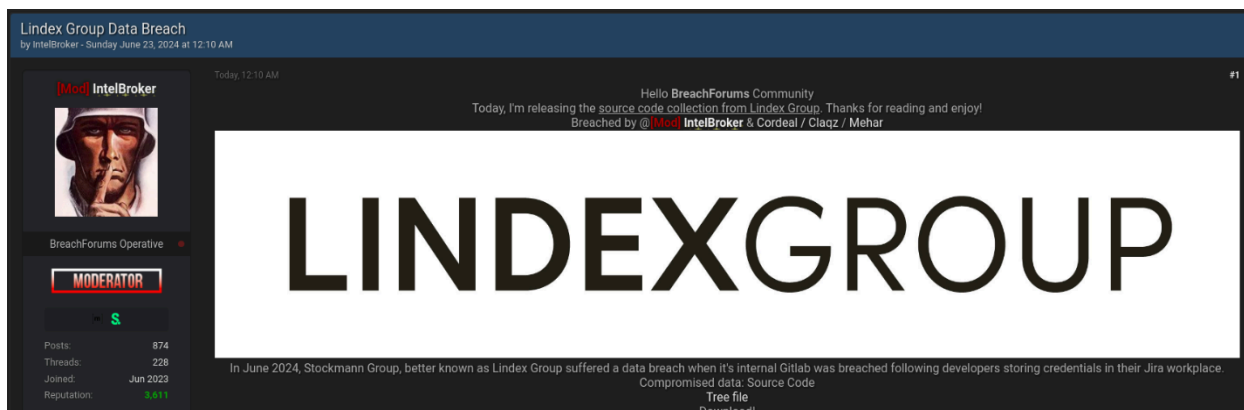


IntelBroker advertises Atlassian zero-day

Source: ZeroFox Intelligence

Between June 15 and June 23, 2024, IntelBroker posted three separate announcements on BreachForums that allude to an unspecified Atlassian Jira vulnerability, which is very likely the same as that advertised for sale on June 16, 2024.

- On June 23, 2024, IntelBroker allegedly released source code from unknown digital infrastructure belonging to the Swedish fashion organization Lindex Group. The post claimed that the information had been obtained via accessing developer credentials that were stored in Jira.



IntelBroker advertises access to Lindex Group source code

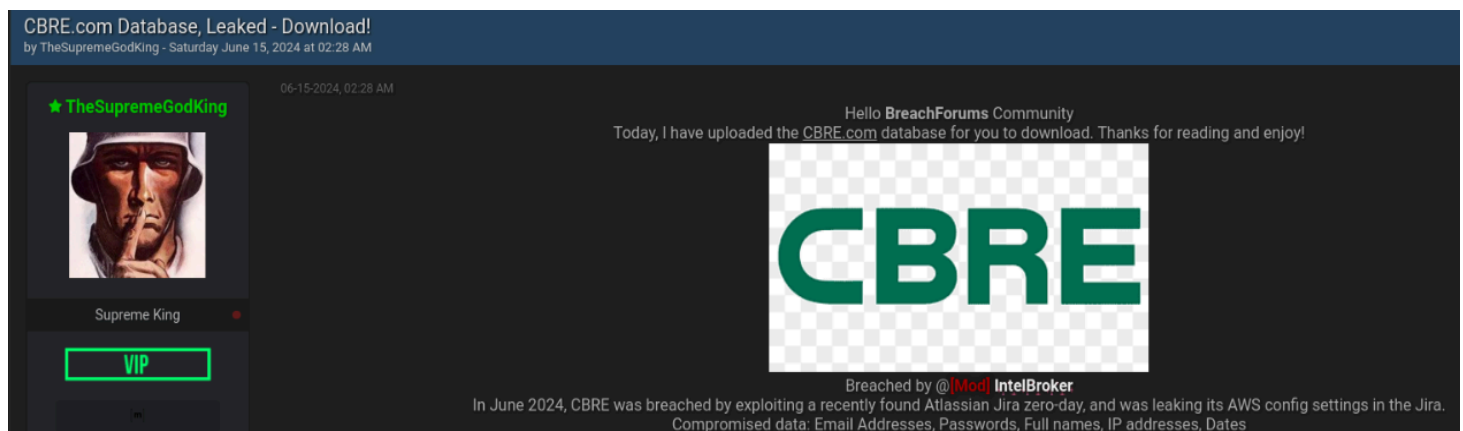
Source: ZeroFox Intelligence

- On June 15, 2024, Intelbroker advertised network access to over 400 “mostly all American-based” organizations, including Bitbucket, Bamboo, and Github (which had allegedly been obtained following the breach of an unknown company with which they are contracted). The nature of the network access and any associated privileges, as well as the price, was not detailed. Instead, IntelBroker invited those with a positive reputation to message him via the secure instant messaging platform Keybase.

The same advertisement had been posted the previous day by an actor named “TheSupremeGodKing”, who joined BreachForums in May 2024.

TheSupremeGodKing is very likely synonymous with IntelBroker.

- Also on June 15, 2024, IntelBroker announced and disclosed a breach of the real estate and investment organization Coldwell Banker Richard Ellis (CBRE). The data—which was offered for free and allegedly included PII such as email addresses, names, and passwords—was purportedly obtained via the exploitation of an Atlassian Jira zero-day.



IntelBroker discloses CBRE data breach

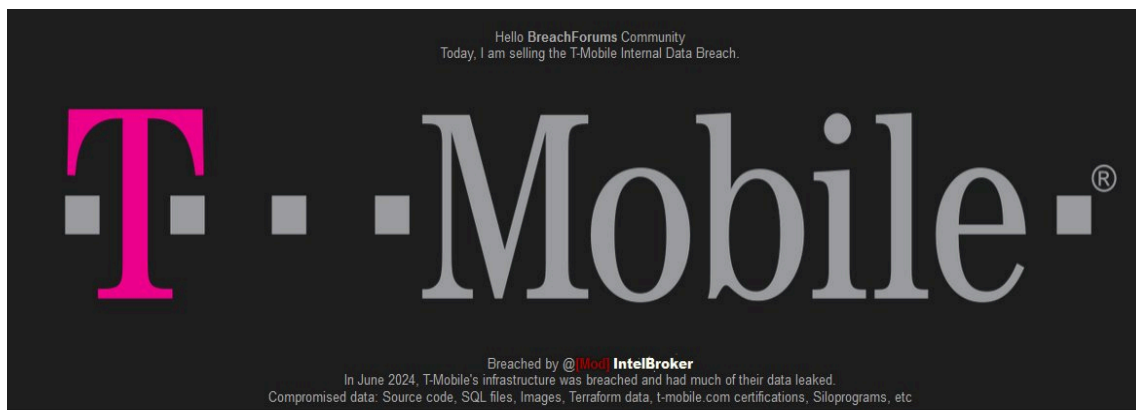
Source: ZeroFox Intelligence

It is rare for cybercriminals to publicly disclose the vulnerabilities leveraged or the threat vectors compromised in order to successfully breach a network. As such, the details provided in the announcement of these three incidents are almost certainly intended to serve as an advertisement or proof of concept for the zero-day vulnerability, with a likely

emphasis on justifying its exorbitant asking price. Despite the advertisement being updated as “sold”, there is a roughly even chance that further threat actors, threat researchers, and LE entities will enquire or purchase the vulnerability—likely for a reduced price.

During the same time period, IntelBroker advertised several other data breaches and network accesses pertaining to high-profile organizations from a multitude of sectors, which allegedly offer access to these entities’ Atlassian Confluence and Jira software. While there is a roughly even chance that the same zero-day vulnerability was leveraged in these attacks, it is not directly credited or advertised in the announcements.

- On June 19, 2024, IntelBroker published a data breach pertaining to international telecommunications organization T-Mobile. According to the post, data such as source code, SQL files, and website certifications are available for purchase, which—if legitimate—would very likely enable procuring threat actors to conduct further malicious activity. Several screenshots were attached to the post, allegedly showcasing administrative privileges to a Confluence server and T-Mobile’s internal Slack channel used by developers. No price was advertised, with potential buyers instead encouraged to “name their price.”

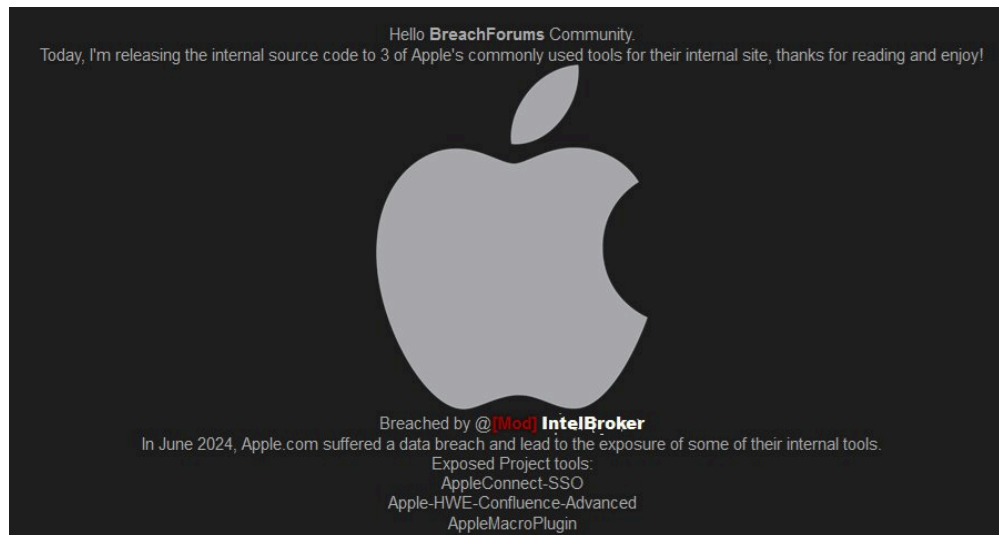


BreachForums post advertising T-Mobile breach

Source: ZeroFox Intelligence

- On June 18, 2024, IntelBroker announced their alleged compromise of tech organization Apple with a post advertising what is described as source code for three of the company’s internal web tools: AppleConnect-SSO, Apple-HWE-Confluence-Advanced, and AppleMacroPlugin. The information was

advertised for a price of eight BreachForums credits, which is equivalent to approximately USD 5-10. It is very unlikely that this data could be used to gain illicit access to either Apple's networks or endpoint devices, though it likely could enable further malicious activity if an active session was exploited.



BreachForums post advertising Apple breach

Source: ZeroFox Intelligence

- Also on June 18, 2024, IntelBroker advertised access to the network of an unspecified, Europe-based insurance organization with an annual revenue of USD 125 billion. The post did not mention Atlassian software, though it alluded to the exploitation of various other software solutions. This access was allegedly purchased for an unspecified, but likely significant, price shortly after it was advertised.

[Access] Insurance Agency Company

by IntelBroker - Tuesday June 18, 2024 at 03:34 PM

[Mod] IntelBroker

BreachForums Operative

44 minutes ago



Hello **BreachForums** Community.
Today, I'm selling the access to a company's infrastructure. Read below for the information:
Industry: Insurance
Revenue: \$125 Billion
Continent: Europe
Access type: Appstacks, Nodes, NetFlow & SolarWinds
Price: Message me for offers. I will be asking for a proof of funds.
Currency: XMR (ofc)
Remember: If you have no rank and or you have little to no reputation, don't bother talking to me.

BreachForums post advertising insurance company breach

Source: ZeroFox Intelligence

Other prominent IntelBroker posts made throughout June include numerous data breaches targeting U.S.-based semiconductor organization AMD and the U.S. Army Aviation and Missile Command, as well as network access to a Middle Eastern embassy.

There is a roughly even chance that IntelBroker had intentionally waited until the actor ShinyHunters relinquished their role as BreachForums' administrator before recommencing activity. IntelBroker is almost certain to continue conducting opportunistic, financially motivated malicious activity—primarily advertising data breaches and network accesses.

| Recommendations

- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Develop a comprehensive incident response strategy.
- Configure email servers to block emails with malicious indicators and deploy authentication protocols to prevent spoofed emails.
- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Proactively monitor for compromised accounts being brokered in DDW forums.
- Configure ongoing monitoring for Compromised Account Credentials.
- Ensure social media accounts are configured with organic security features, such as phishing-resistant multi-factor authentication and complex, unique passwords.
- Report accounts suspected as fake or those conducting malicious activity through the platform's internal report function.
- Be aware of the activity stemming from accounts with a recent creation date, limited activity, or those with seemingly nonsensical names.
- Ensure enterprise engagements taking place over social media platforms move to secure channels when appropriate, protecting internal and customer data.

| Appendix A: Traffic Light Protocol for Information Dissemination

WHEN SHOULD IT BE USED?

Red

Sources may use

TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

Amber

Sources may use

TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

HOW MAY IT BE SHARED?

Recipients may NOT share

TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Recipients may ONLY share

TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Note that

TLP:AMBER+STRICT restricts sharing to the organization only.

Green

WHEN SHOULD IT BE USED?

Sources may use

TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

Clear

Sources may use

TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

HOW MAY IT BE SHARED?

Recipients may share

TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.

Recipients may share

TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%