



| Flash |

IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

F-2024-06-27a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Deep and Dark Web, Data Breach, Zero-Day Vulnerability

June 27, 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 9:00 AM (EDT) on June 27, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

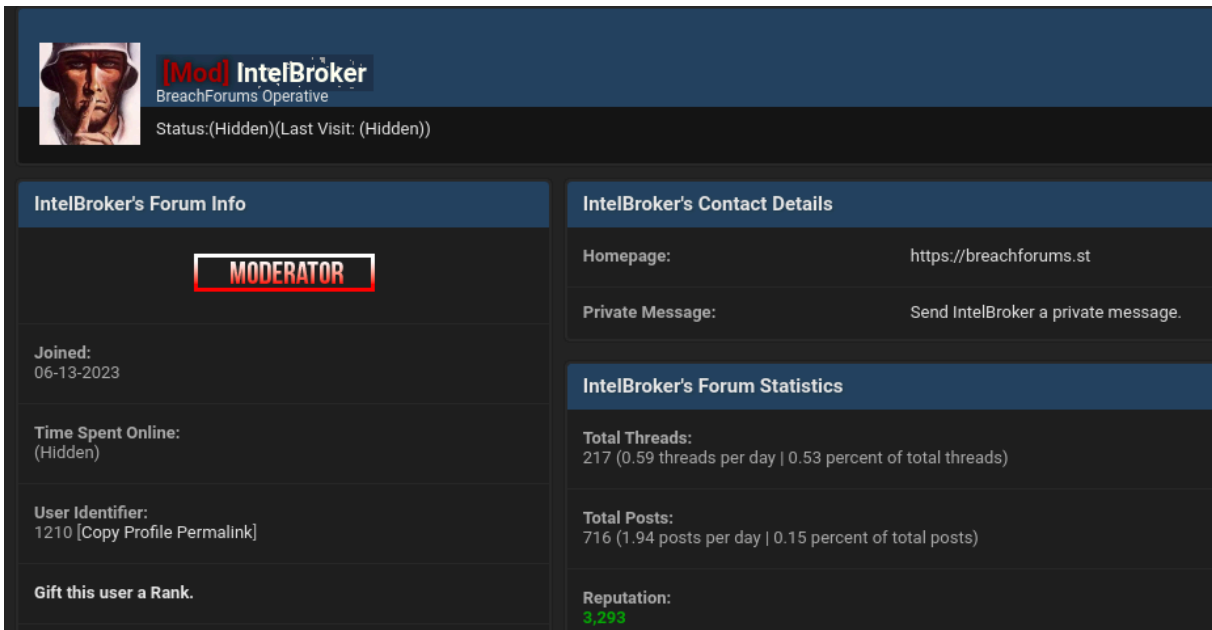
| Flash | IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

› Key Findings

- 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 returning to the forum, IntelBroker began advertising numerous illicit network accesses and data breaches targeting high-profile organizations from a multitude of industries. The majority of these attacks alluded to the exploitation of an unspecified vulnerability targeting Atlassian software.
- On June 16, 2024, IntelBroker advertised the sale of a zero-day vulnerability that targets Atlassian Jira software via remote code execution. This was purchased by an unknown actor between June 20 and June 24, 2024, though it is unlikely that IntelBroker received the exorbitant asking price of USD 800,000.
- The details provided in the announcement of the three attacks were almost certainly intended to serve as an advertisement or proof of concept for the zero-day vulnerability.

Details

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 user profile for IntelBroker on the BreachForums forum. The profile header includes a user avatar, the name [Mod] IntelBroker, the role BreachForums Operative, and status information (Hidden). Below the header, the profile is divided into two main sections: IntelBroker's Forum Info and IntelBroker's Contact Details. The Forum Info section features a Moderator badge, join date (06-13-2023), time spent online (Hidden), user identifier (1210), and a gift rank option. The Contact Details section lists the homepage (https://breachforums.st) and a private message link. A separate section, IntelBroker's Forum Statistics, shows 217 total threads, 716 total posts, and a reputation of 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)	
User Identifier: 1210 [Copy Profile Permalink]	
Gift this user a Rank.	

IntelBroker's Forum Statistics
Total Threads: 217 (0.59 threads per day 0.53 percent of total threads)
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.

Flash | IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

F-2024-06-27a

TLP:CLEAR

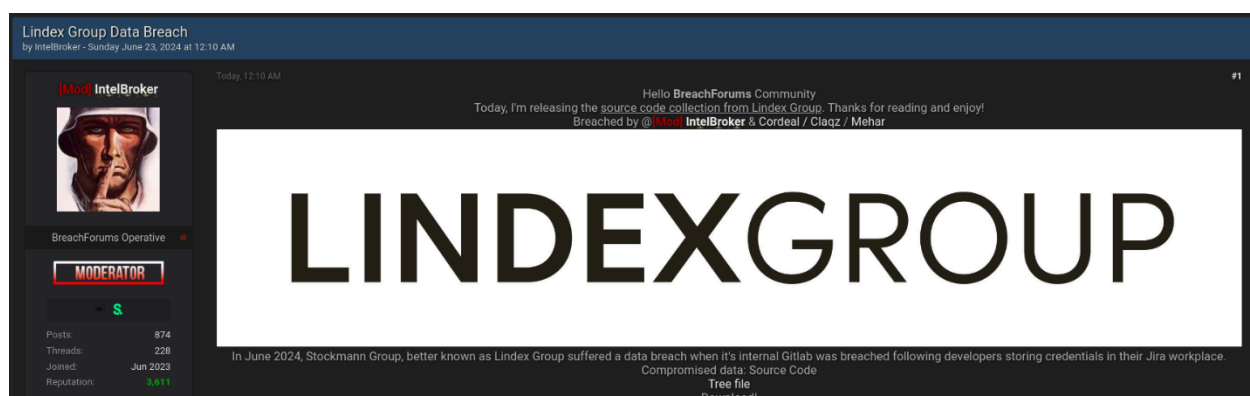


IntelBroker advertises Atlassian zero-day

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

Flash | IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

F-2024-06-27a

TLP:CLEAR

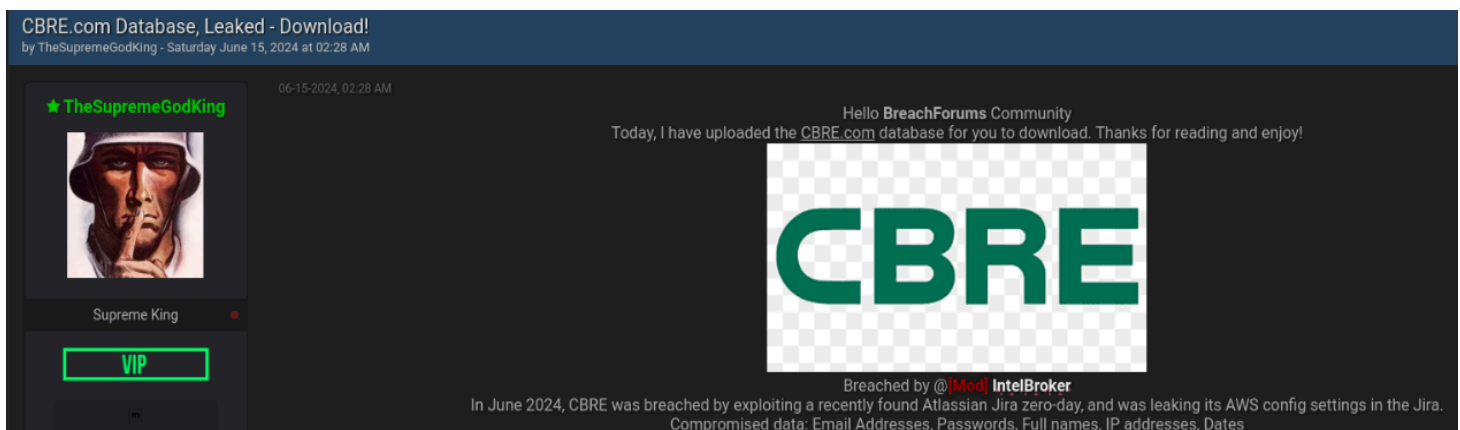


- On June 15, 2024, Intelbroker advertised network access to over 400 “mostly all American-based” organizations, including Bitbucket, Bamboo, and Github (which had allegedly been obtained following the breach of an unknown company with which they are contracted). The nature of the network access and 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 personally identifiable information (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

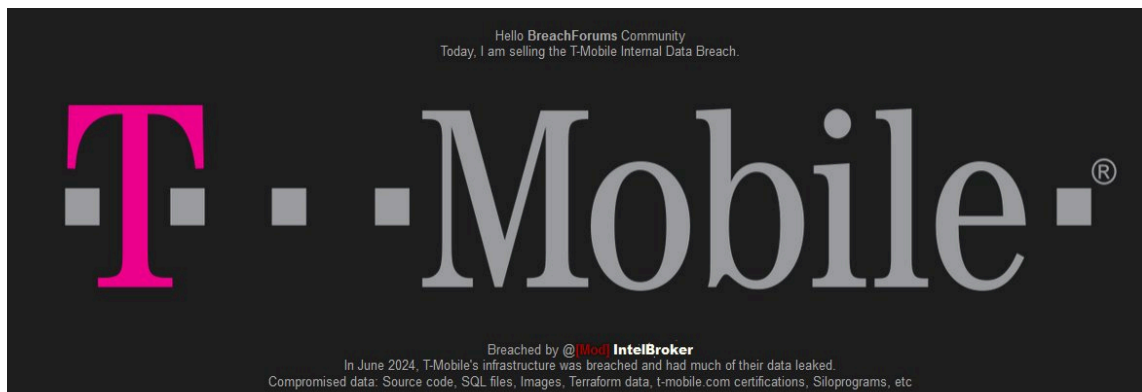
Source: ZeroFox Intelligence

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 law enforcement 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

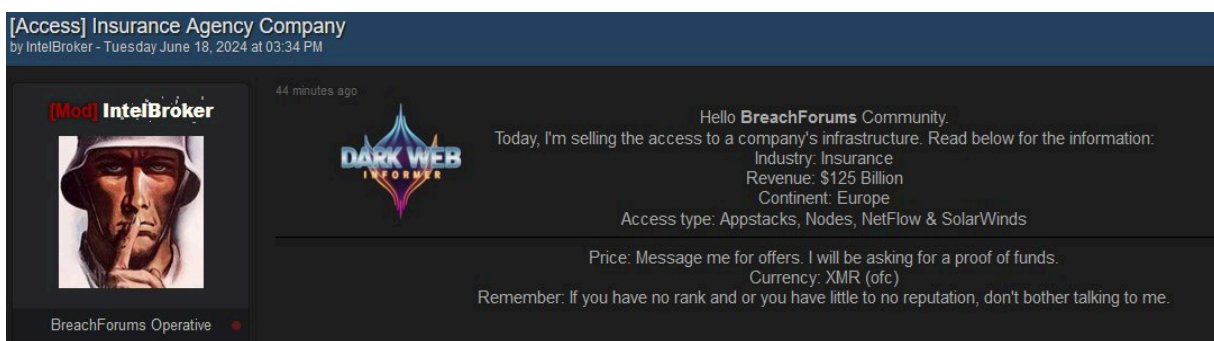
approximately USD 5-10. It is very unlikely that this data could be used to gain illicit access to either Apple's networks or endpoint devices, though it likely could enable further malicious activity if an active session was exploited.



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.



BreachForums post advertising insurance company breach

Source: ZeroFox Intelligence

| Flash | IntelBroker Sells Zero-Day Vulnerability Leveraged in Recent Attacks

F-2024-06-27a

TLP:CLEAR



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 known as “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

- Deploy a holistic patch management process and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Ensure Atlassian solutions are configured in accordance with official guidance and best practices.
 - [hXXps://confluence.atlassian\[.\]com/doc/configuring-confluence-security-151515.html](https://confluence.atlassian.com/doc/configuring-confluence-security-151515.html)
- Ensure Confluence and Jira products are updated with the latest manufacturer software patches.
 - [hXXps://www.atlassian\[.\]com/software/jira/download-archives](https://www.atlassian.com/software/jira/download-archives)
 - [hXXps://www.atlassian\[.\]com/software/confluence/download-archives](https://www.atlassian.com/software/confluence/download-archives)
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement secure password policies with phishing-resistant multi-factor authentication (MFA), complex passwords, and unique credentials.
- 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.
- Implement network segmentation to separate resources by sensitivity and/or function.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	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.	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	Clear
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.	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%