TIR-20241105 IntelBroker Unmasked

11/5/2024

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

Table of Contents

Executive Summary

In October 2024, Cisco announced that it was looking into reports of a potential data breach after a hacker claimed to be selling stolen data from the company on a dark web forum. The group claiming responsibility for the breach was identified as IntelBroker, which shared samples of the supposedly stolen information.

The shared samples included a database, customer details, various documents related to customers, and images of customer management portals. However, IntelBroker did not disclose how they accessed the data. Let's take a look at IntelBroker's claims, their tactics and techniques, as well as what really happened with the alleged Cisco breach.

TIR Snapshot

Threat Actor – IntelBroker

Targeted Industries

- Semiconductors and Technology - AMD, Cisco, Hewlett Packard Enterprise
- Government and Federal Agencies - U.S. Department of State, Department of Defense, National Security Agency
- Retail - Shoprite, an African retail giant
- Healthcare and Insurance - DC Health Link, covering U.S. House members and staff
- Telecommunications - T-Mobile
- Food Services - Weee! grocery delivery service

Targeted Software

- Atlassian Confluence - Exploited using CVE-2024-1597 in attacks on T-Mobile and others
- Jenkins - Used CVE-2023-23897 to breach an IT service provider
- SonarQube - Breached via default credentials to access third-party contractor systems
- Microsoft Exchange Server - IntelBroker is associated with exploits targeting Exchange vulnerabilities
- BitBucket - Accounts and SSH keys targeted for data exfiltration

Countries Targeted

- United States - Various federal agencies, tech companies, healthcare organizations
- South Africa - Shoprite, a major African retailer
- Global - Multinational corporations with headquarters in the U.S. but operations worldwide, including tech and retail sectors

Malware Used

- Endurance Ransomware, a ransomware strain written in C#. This malware not only encrypts files but can act as a wiper, corrupting and deleting data to maximize disruption.

Motive

- Financial gain and influence

IntelBroker

Originally from Serbia, IntelBroker is a well-known cybercriminal group that has made a name for itself through a series of high-profile data breaches. The group has been active since October 2022 and is driven by money and influence. Operating primarily on dark web forums, they have a reputation for boasting about their exploits and selling stolen data to the highest bidder. IntelBroker is also known for developing the open-source, C#-based ransomware called "**Endurance**," as well as for its involvement in malware creation and the sale of access to compromised systems.

IntelBroker serves as the administrator of the cybercriminal forum **BreachForums** and targets major companies, including tech giants like AMD and Apple. The group uses various tactics to infiltrate organizations and access sensitive information, often focusing on internal databases, source code, and customer data.

What sets IntelBroker apart is their practice of sharing samples of the stolen data they acquire. By showcasing snippets of their attacks, they successfully market their capabilities while instilling fear in potential victims. This tactic not only elevates the perceived severity of their breaches but also highlights the ongoing battle organizations face in protecting their data from such relentless adversaries.

Tactics and Techniques

IntelBroker's tactics and techniques highlight their capabilities in exploiting vulnerabilities, exfiltrating sensitive data, and effectively utilizing the dark web for their operations. Their focus on third-party vendors establishes a strategic approach to bypass traditional security measures and access valuable information without direct confrontation. Here is a break down of the group's tactics and techniques.

Initial Access

- **Exploitation of Vulnerabilities** - IntelBroker has been known to exploit weaknesses in third-party vendors' systems, often utilizing default credentials to gain access to sensitive data. For example, the group reportedly accessed a third-party contractor's SonarQube server using default logins.

Credential Dumping

- **Harvesting Credentials** - The threat actor has engaged in credential dumping, which involves extracting usernames and passwords from compromised systems. This technique allows them to maintain access and move laterally within networks.

Data Exfiltration

- **Stealing Sensitive Information** - IntelBroker steals sensitive data, including source code, customer databases, employee information, and internal documents. Their

recent activities involved exfiltrating data from well-known companies like Cisco, AMD, and Nokia.

Data Sale and Distribution

- **Marketplace Transactions** - Once data is stolen, IntelBroker uses dark web forums to sell this information. They share samples of the compromised data to entice potential buyers, demonstrating the value of what they have acquired.

Targeting Third-Party Vendors

- **Supply Chain Attacks** - By targeting third-party vendors that service larger organizations, IntelBroker can compromise a company's security indirectly. This strategy has been evident in their breaches where they accessed data through a contractor.

Use of Insider Information

- **Leveraging Internal Knowledge** - IntelBroker's attacks sometimes indicate an understanding of internal company processes, suggesting they might have insider knowledge or have studied their targets closely.

IntelBroker finds potential targets by collecting publicly accessible information and scanning for vulnerabilities within organizations. They may even be using social engineering techniques to gain deeper insights into organizational hierarchies and employee specifics. According to security researchers, IntelBroker takes advantage of both known and zero-day vulnerabilities in software and hardware to compromise systems. They have been linked to several notable exploits, including:

- **CVE-2024-1597** - This vulnerability in Confluence data centers was used in an attack on T-Mobile.
- **CVE-2024-21894** - Exploiting this vulnerability allowed IntelBroker to steal data from multiple U.S. government agencies.
- **CVE-2023-23897** - This critical unauthenticated local file inclusion vulnerability in Jenkins was leveraged to breach an IT service provider.

Following an initial breach, IntelBroker installs backdoors to ensure ongoing access and facilitate data exfiltration. They gather credentials from legitimate accounts to elevate their access privileges and move laterally within the network.

IntelBroker and the Cisco Breach

In October 2024, IntelBroker announced on BreachForums that they attacked Cisco. The group claimed that they stole a large volume of data and that over dozens of organizations were impacted. The alleged data included API tokens, hard-coded credentials, confidential internal documents, API tokens, source code, and storage buckets.

While the group shared samples of this alleged stolen data, they did not disclose specific details about how the breach was executed, leaving many questions regarding the security measures in place at Cisco. Cisco's response to the incident included a public acknowledgment of the claims and the initiation of an internal investigation to assess the validity of IntelBroker's claims.

A few days after the breach was made public, Cisco confirmed that the company was the victim of a security incident where threat actors obtained data from a public-facing DevHub environment. DevHub is a platform designed for content management and marketing, and Cisco referred to the compromised area as a resource center that provided source code, scripts, and other content for its customers.

Cisco reported that they found a small set of files, not intended for public distribution, may have been made available during the breach. However, the company made it clear that no sensitive data, such as financial or personal information, was part of the stolen files. As a precautionary measure, Cisco disabled public access to the affected website in response to the incident. Cisco's internal systems were not impacted in any way.

Other Attacks

U.S. Government (April 2024) – In the spring, the U.S. State Department initiated an investigation into claims that a threat actor stole government data from a contractor. IntelBroker claimed that they had accessed sensitive information pertaining to several U.S. agencies, including the State Department, Defense Department, and National Security Agency, after breaching Acuity, a Virginia-based technology consulting firm that collaborates with federal agencies. Neither Acuity nor the agencies mentioned in the IntelBroker's post provided comments, and the Cybersecurity and Infrastructure Security Agency (CISA) also refrained from commenting.

However, a State Department spokesperson acknowledged the situation, stating that they were aware of the alleged cyber incident and were looking into it. The spokesperson also said that the department's commitment to protecting its information and improving its cybersecurity measures but did not disclose specific details about the claims. Additionally, a researcher who

reviewed the threat actor's post noted that they had to obscure numerous legitimate U.S. government email addresses from the State Department, FBI, Department of Homeland Security, and Justice Department that were included in the leak. The hacker promoted the breach on social media, offering to share the full leak with interested parties, and had previously made claims of other hacks, including a reported breach of UberEats.

AMD (June 2024) – During the summer of 2024 IntelBroker claimed responsibility for a significant data breach involving Advanced Micro Devices (AMD), claiming that they accessed a wide range of sensitive information from the company's databases. IntelBroker shared details of the alleged breach on BreachForums, including samples of the stolen data, which reportedly encompassed specifications for upcoming AMD products, customer databases, financial records, and extensive employee information.

In response to these claims, AMD announced it was investigating the matter in collaboration with law enforcement and a third-party hosting partner. Although AMD's officials did not confirm the breach, the potential severity of the situation raised concerns about the company's cybersecurity measures, particularly in light of previous cyber incidents involving IntelBroker, which had targeted other organizations and government contractors.

Jenkins (July 2024) - In the Jenkins attack, IntelBroker exploited a critical unauthenticated local file inclusion vulnerability (CVE-2023-23897) affecting the open-source automation server. The group leveraged this flaw to breach an IT service provider, gaining unauthorized access to sensitive systems. Once inside, IntelBroker was able to exfiltrate valuable data, including internal files and credentials, while evading detection. This attack highlighted the risks that come with leaving systems unpatched or improperly configured.

Nokia (November 2024) - Currently, Nokia is investigating a potential data breach involving a third-party vendor, after IntelBroker claimed to have stolen and is attempting to sell Nokia's source code. The hacker stated that the data was obtained from a vendor's server used to support Nokia's internal development tools. IntelBroker allegedly accessed the vendor's SonarQube server using default credentials and extracted a variety of sensitive data, including SSH keys, source code, RSA keys, BitBucket logins, and other credentials. Nokia responded by stating that, as of now, there is no evidence suggesting its systems were compromised, but the company is continuing to monitor the situation closely.

Conclusion

IntelBroker's claims about breaching Cisco made waves, especially with their bold bragging about obtaining sensitive company data. However, with Cisco confirming there was no evidence that their internal systems were compromised, IntelBroker's claims appeared to be overstated, likely for publicity.

The group has a tendency to exaggerate their exploits on dark web forums, a tactic that not only spreads fear but boosts their reputation within cybercriminal circles. Their history of attempting to sell stolen data and access further indicates they are invested in making a name for themselves, often prioritizing notoriety over proven success.

Looking ahead, it's likely that IntelBroker will continue targeting high-profile companies and releasing information that may or may not be fully accurate. The group's approach of publicly posting samples and boasting about intrusions may signal a continued pattern of exaggerated claims. This tactic—while effective in building their reputation—can also serve as a smokescreen, making it harder for organizations to assess the legitimacy of their threats. Given their pattern of mixing real breaches with bold claims, organizations should monitor IntelBroker closely, expect future attempts to exploit known vulnerabilities, and prepare for the possibility of both credible threats and exaggerated publicity stunts.

Aspire's Recommendations

Patch Management and Vulnerability Remediation

- **Apply Patches for High-Impact CVEs** - Ensure timely patching of vulnerabilities IntelBroker has exploited, including Confluence (CVE-2024-1597), Jenkins (CVE-2023-23897), and government-focused software often targeted in their campaigns. Prioritize patching all known exploited vulnerabilities with critical and high-severity scores.
- **Regular External Scanning** - Continuously monitor external-facing systems for vulnerability exposure. Use tools that identify weak configurations or default credentials on cloud infrastructure and CI/CD platforms.

Account and Access Management

- **Enforce MFA for All Access Points** - Require multi-factor authentication (MFA) on all accounts with privileged access and external access, especially for third-party vendor accounts that could be used as entry points.
- **Limit Third-Party Vendor Access** - Restrict third-party vendors to only necessary resources and verify permissions regularly. Vendors like Acuity should undergo regular security assessments, especially if they access sensitive data repositories.

Behavioral Threat Detection and Monitoring

- **Monitor for Credential Dumping Techniques (T1003)** - Deploy tools that can detect and alert on attempts to dump credentials, as IntelBroker often seeks credentials for deeper access.

- **Anomaly Detection in Web Traffic** - Use network monitoring and anomaly detection for signs of encrypted exfiltration over unusual web protocols (T1048). Monitor for large outbound data transfers and encrypted communications to detect potential exfiltration attempts.
- **Set Alerts for Unusual Repository Access** - Implement logging and alerting for unusual access to repositories containing source code and sensitive data.

Strengthen Endpoint Security Against IntelBroker's Ransomware and Wipers

- **Deploy EDR with Strong Wiper Detection** - Ensure endpoint detection and response (EDR) tools are capable of detecting wiper malware behaviors, as IntelBroker has used destructive tools like Endurance, which can corrupt or delete files.
- **Control Scripting and Execution on Endpoints** - Disable or restrict scripting capabilities on endpoints, particularly PowerShell and C#-based scripts, which IntelBroker has been known to use for ransomware execution.
- **Backup Data and Test Restores Regularly** - Maintain offline, encrypted backups and routinely test recovery processes. IntelBroker's ransomware tactics may involve data encryption and wiper malware, so having effective backups is essential.

Enhanced Incident Response and Remediation

- **Implement a Rapid Incident Response Plan** - Prepare for potential ransomware or data exfiltration incidents with an established IR plan that includes containment, eradication, and forensic investigation capabilities.
- **Engage Threat Intelligence and Analysis**: Actively monitor threat feeds and intelligence platforms to stay informed about IntelBroker's evolving TTPs. IntelBroker frequently targets specific sectors and vulnerabilities; tracking these indicators will help prevent future breaches.

Training and Awareness Focused on Social Engineering

- **Educate on Social Engineering Tactics** - Provide training on social engineering methods, as IntelBroker has been known to exploit public information and trick employees into revealing details that assist with reconnaissance.
    - Regularly conduct phishing simulations and awareness training. IntelBroker's social engineering focus on gathering internal details suggests that user awareness can be a critical defense layer.

Aspire Protects

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

MITRE Map

Initial Access	T1190 – Exploit Public Facing Application T1078 – Valid Accounts
Execution	T1059 – Command and Scripting Interpreter
Persistence	T1543 – Create or Modify System Process T1098 – Account Manipulation
Privilege Escalation	T1548 – Abuse Elevation Control Mechanism
Defense Evasion	T1027 – Obfuscated Files or Information
Credential Access	T1003 – Credential Dumping
Discovery	T1016 – System Network Configuration Discovery
Lateral Movement	T1021 – Remote Services T1550.002 – Pass Hash
Collection	T1213 – Data from Information Repositories
Exfiltration	T1048 – Exfiltration Over Alternative Protocol T1567 – Exfiltration Over Web Service
Impact	T1486 – Date Encrypted for Impact T1485 – Data Destruction

Indicators of Compromise (IoCs)

MD5

- dc7cb3bfdc236c41f1c4bbac911daaa2

SHA1

- 26727d5fceef79de2401ca0c9b2974cd99226dcb
- 285e0573ef667c6fb7aeb1608ba1af9e2c86b452
- 8a3ca9efa2631435016a4f38ff153e52c647146e

SHA256

- 600be5ab7f0513833336bec705ca9bcfd1150a2931e61a4752b8de4c0af7b03a

Domain

- 3inf[.]site

Hostname

- avito-rent[.]id7423[.]ru
- boxberry[.]id7423[.]ru
- olx[.]id7423[.]ru

Email

- intelsales@protonmail[.]com
- brokerdata@riseup[.]net

Known aliases for IntelBroker on underground forums

- DataHunter77
- LeakSource

Supporting Documentation

Warnings of SharePoint Flaw After Exploit | SC Media UK

Intelbroker Advertises Massive AMD Data Breach On Dark Web

june-21-12-the-intelbroker-data-leak-threat-actor.pdf

Cisco takes DevHub portal offline after hacker publishes stolen data

BORN Group Supply Chain Breach: In-Depth Analysis of Intelbroker's Jenkins Exploitation | CloudSEK

Who is IntelBroker? What security breaches is the threat actor responsible for? - AS USA

DC healthcare exchange breach leaked sensitive data of Congress members, staff

State Department investigating reports of data theft allegedly involving federal tech consulting firm

Cisco Confirms Security Incident After Hacker Offers to Sell Data - SecurityWeek

5 Critical Threat Actors You Need to Know About - ReliaQuest

Nokia investigates breach after hacker claims to steal source code

Cisco launches investigation into IntelBroker's cyber attack - Cyber Daily

Threat actor IntelBroker claims alleged breaches of Apple, AMD | Cybernews

Exclusive IntelBroker Interview: Inside The Mind Of A Hacker

BORN Group Supply Chain Breach: In-Depth Analysis of Jenkins Exploitation - LevelBlue - Open Threat Exchange

Chinese ecommerce giant PandaBuy hit by cyberattack, data breach | TechRadar

AMD working with law enforcement after reports of massive data breach — hack may have uncovered future product details | Tom's Hardware

Appendix II: Disclaimer

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.