

The Intelbroker Data Leak Threat Actor

Date: 21th June 2024 | Severity: High

Summary

The threat actor, presumably from Serbia, is known for breaching high-profile organizations in various sectors, such as government, telecommunications, automotive, and technology. In addition, IntelBroker is the operator of the Endurance ransomware. IntelBroker claimed responsibility for attacks against numerous organizations, including Autotrader, Volvo, AT&T, and Verizon. As its name suggests, the threat actor acts as an intelligence broker, breaching organizations and selling their data on underground hacking forums.

Attack Vectors

- IntelBroker often uses a unique ransomware strain, Endurance, to extort organizations into paying a ransom to prevent the exposure of their data.
- The C#-based ransomware, acting more as a wiping malware, overwrites the content of the targeted files with random bytes, cleans it, renames the file using a random string, and then deletes the file. Endurance's source code is publicly available on the threat actor's GitHub repository.
- This statement comes after IntelBroker, a well-known threat actor linked to numerous breaches, claimed to have breached T-Mobile.
- IntelBroker has been rapidly releasing new data breaches, and if they all used this cloud provider, it could explain where all the data is coming from. The hacker had access to a Jira instance for testing applications as recently as this month.
- Hackers breached the provider, but one of the leaked images shows a search for critical vulnerabilities listing CVE-2024-1597, which affects Confluence Data Center and Server.
- T-Mobile denied that it was breached or that the source code came from its servers; however, it is possible that the threat actor compromised a third-party service provider for T-Mobile.

Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|----------------|--|
| URL | http[:]//h44jyyfomcbnnw5dha7zgwgkvpzbzbdyx2onu4fxaa5smxrgbjgq7had.onion/ olx.id7423[.]ru boxberry.id7423[.]ru avito-rent.id7423[.]ru 3inf[.]site |
| FileHash | 600be5ab7f0513833336bec705ca9bcfd1150a2931e61a4752b8de4c0af7b03a 8a3ca9efa2631435016a4f38ff153e52c647146e 285e0573ef667c6fb7aeb1608ba1af9e2c86b452 26727d5fceef79de2401ca0c9b2974cd99226dcb dc7cb3bfdc236c41f1c4bbac911daaa2 |

Recommendation

- Threat Intelligence and Monitoring:Stay informed about emerging threats and vulnerabilities. Use threat intelligence feeds to identify IOCs associated with known threat actors. Continuously monitor network traffic and logs for suspicious activity.
- Access Control and Least Privilege: Limit user privileges to the minimum necessary for their roles.
 Implement strong access controls, including two-factor authentication (2FA). Regularly review and revoke unnecessary access rights.
- Patch Management: Keep software and systems up to date with security patches. Vulnerabilities in outdated software can be exploited by hacker.
- Network Segmentation: Isolate critical systems from less secure areas of the network. Limit lateral movement for attackers.
- Endpoint Security: Deploy robust antivirus, anti-malware, and intrusion detection systems. Regularly scan endpoints for vulnerabilities.
- Incident Response Plan: Develop and test an incident response plan. Know how to respond to a breach promptly and effectively.
- Encryption and Data Protection: Encrypt sensitive data at rest and in transit. Use strong encryption protocols.
- Employee Training and Awareness: Educate employees about phishing, social engineering, and safe online practices. Regularly conduct security awareness training.

Reference Links

- https://en.as.com/latest_news/who-is-intelbroker-what-security-breaches-is-the-threat-actor-responsible-for-n/
- https://hackread.com/intelbroker-hacker-cybersecurity-firm-breach/