Babuk Ransomware Activity Resurfaces - Copycat Campaigns and Legacy Threats

Overview

TL;DR

Babuk ransomware may have disbanded, but its code is still being used. One Aspire customer was recently impacted by activity linked to Babuk or its copycats.

The group is known for exploiting exposed services and using stolen credentials. New campaigns, some under the name Babuk2, are reusing old data and malware built on Babuk's leaked code.

Stay alert, block known IoCs, and patch exposed systems.

Babuk ransomware first appeared in 2021 as a Ransomware-as-a-Service (RaaS) operation, known for double extortion tactics. The Russian threat actor encrypts victim data before threatening to release the data to the public – pressuring victims into paying ransom demands. The group quickly gained notoriety after breaching the D.C. Metropolitan Police Department, stealing 250GB of sensitive files. Following internal disputes and law enforcement pressure, Babuk disbanded in mid-2021.

However, in September 2021, Babuk's source code was leaked on a Russian-language forum. That leak triggered a wave of new ransomware variants built off Babuk's original framework, including groups like Dark Angels. In 2025, a group calling itself Babuk2 resurfaced, claiming responsibility for new attacks, though investigations suggest they're simply repackaging old data. One campaign reportedly used a vulnerability in SentinelOne's EDR platform to deploy Babuk payloads.

Babuk has historically gained access by targeting exposed services like vulnerable VPNs, RDP, and other internet-facing systems. They've also used stolen credentials purchased from dark web markets. Aspire is sharing this notice so customers are aware of the renewed activity and can stay alert.

Aspire Protects

- Audit endpoint protections – Validate that EDR solutions are properly configured and patched.
- Harden backups – Ensure backups are offline, protected, and tested for restoration.
- Block known indicators – Apply IoCs to firewall, proxy, and EDR solutions.

- Report any suspicious behavior – Unusual service stops or command-line activity may signal ransomware staging.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Babuk-related actors have leveraged known vulnerabilities, such as flaws in endpoint detection tools, to deliver ransomware payloads.

Execution

- Command and Scripting Interpreter: Windows Command Shell [T1059.003] – Babuk uses the command line for execution on compromised hosts.

Discovery

- File and Directory Discovery [T1083] – The attacker enumerates files and folders across the target system.
- Network Share Discovery [T1135] – Network shares are identified to locate additional data for encryption or exfiltration.
- System Information Discovery [T1082] – Babuk collects details about disk volumes and service status to optimize its attack.

Impact

- Service Stop [T1489] – Backup services may be disabled to prevent recovery and increase ransom pressure.

IoCs

Older IoCs - These IoCs are tied to known Babuk ransomware payloads from earlier campaigns. See a complete list of older IoCs here.

MD5 Hashes

- 2b37963bad6d0f866235caf14c502b34
- 2e4c216c7d987e5c0655e5180f0c93d3
- 335577e59b4d5a62837d57654ba2d089
- 395249d3e6dae1caff6b5b2e1f75bacd
- 4601076b807ed013844ac7e8a394eb33
- 64b8e75e76283e034e134c128e9a405a
- ce73b00417464190d7fb9b36af74968a
- ce9fa2d78d2e4e8331956ae938232823
- cfb6d21ffe7c4279f761f2351c0810ee
- e56c97cb4f9df25845cda36e3cd7d597

Newer IoCs (Copycat Activity) - Associated with more recent Babuk2 or post-leak campaigns that are reusing Babuk's code. Stay updated with newer IoCs here.

- Bitcoin Wallets
  - 1JUToCyRL5UwgeucjnFAagKs4v1YqhjT1
  - bc1qvnk8xkw9esmujpjz00hs4706j3803s9nf5z2px
- Domain
  - Bitmain[.]shopping

Targeted Industries

Some environments are more at risk than others, especially those running exposed services, older endpoint tools, or widely deployed VPNs and RDP.

- Healthcare
- Transportation
- Education

Aspire Service Offerings

- **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 cyber attacks.
- **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.

Supporting Documentation

Babuk ransomware deployed via “Bring Your Own Installer” EDR evasion | SC Media

Fake Out: Babuk2 Ransomware Group Claims Bogus Victims

Babuk Ransomware Linux Variant Analysis – LMNTRIX Blog