Hive Pro®

Threat Level
Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Albabat Ransomware Infiltrates via Counter-Strike Cheat Utility

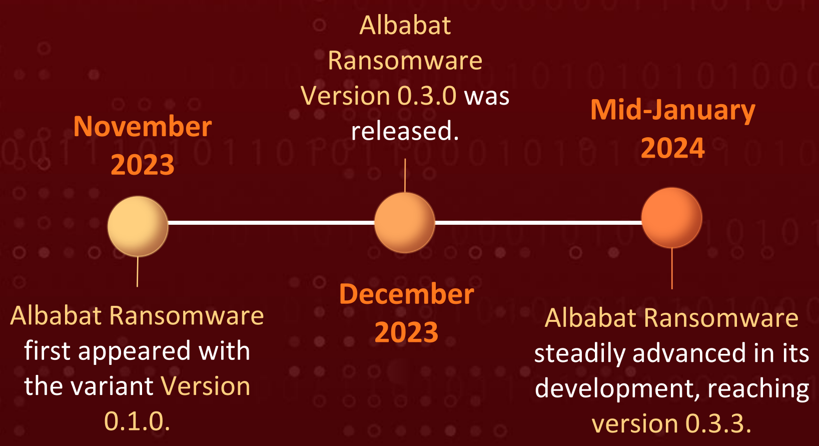
Date of Publication	Admiralty Code	TA Number
February 9, 2024	A1	TA2024052

Summary

First Seen: November 2023
Malware: Albabat Ransomware (aka White Bat)
Ransom: 0.0015 Bitcoin (worth 69.89 USD at the time of writing)
Attack Region: Argentina, Brazil, Czech Republic, Germany, Hungary, Kazakhstan, Russia, and the United States.

Attack: Albabat ransomware, made its debut in November 2023, emerging as a financially motivated threat crafted in Rust. This ransomware has targeted both corporate entities and individual consumers across diverse geographical regions.

Attack Timeline



November 2023

Albabat Ransomware first appeared with the variant Version 0.1.0.

December 2023

Albabat Ransomware Version 0.3.0 was released.

Mid-January 2024

Albabat Ransomware steadily advanced in its development, reaching version 0.3.3.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 Making its debut in November 2023, Albabat ransomware, also known as White Bat, emerges as a financially motivated threat crafted in Rust, boasting Version 0.1.0. Subsequent iterations, such as Version 0.3.0 in late December and Version 0.3.3 in mid-January 2024, have been observed. Notably, Albabat Ransomware targets both corporate entities and individual consumers across diverse geographical regions.

#2 This strain of Albabat ransomware appears to propagate through means masquerading as legitimate software offerings, including a counterfeit Windows 10 digital activation tool and a purported cheat utility for the popular Counter-Strike 2 game. Upon execution, Albabat ransomware diligently searches for files to encrypt, appending a ".abbt" extension to its victims' data.

#3 Moreover, the Albabat ransomware takes control over the victim's desktop background, asserting its presence with distinct imagery. Victims are then directed to a ransom note, README.html, instructing them to initiate contact with the perpetrator, who demands a ransom of 0.0015 Bitcoin.

#4 Notably, the ransom note features a translation option leveraging the capabilities of Google Translate, facilitating communication in over 100 languages. Interestingly, the default translation setting points to Portuguese, possibly indicating the primary language of the ransomware developer.

#5 Given that Albabat is developed using the Rust programming language, renowned for its cross-platform compatibility, speculation arises regarding the potential release of a Linux-compatible version in the foreseeable future.

Recommendations

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	TA0040 Impact	T1059 Command and Scripting Interpreter
T1566 Phishing	T1055 Process Injection	T1562.001 Disable or Modify Tools	T1027 Obfuscated Files or Information
T1036 Masquerading	T1010 Application Window Discovery	T1083 File and Directory Discovery	T1105 Ingress Tool Transfer
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	%USERPROFILE%\Albabat\Albabat.ekey, %USERPROFILE%\Albabat\Albabat_Logs.log, %USERPROFILE%\Albabat\personal_id.txt, %USERPROFILE%\Albabat\readme\README.html, %USERPROFILE%\Albabat\readme\assets\banner.jpg, %USERPROFILE%\Albabat\readme\assets\script.js, %USERPROFILE%\Albabat\readme\assets\style.css, %USERPROFILE%\Albabat\readme\pages\faq.html, %USERPROFILE%\Albabat\wallpaper_albabat.jpg, %USERPROFILE%\Albabat\Albabat.log, %USERPROFILE%\Albabat\README.html,

TYPE	VALUE
File Path	%USERPROFILE%\Albabat\www\banner.jpg, %USERPROFILE%\Albabat\www\faq.html, %USERPROFILE%\Albabat\www\script.js, %USERPROFILE%\Albabat\www\style.css, %USERPROFILE%Albabat\readme\README.html, %USERPROFILE%Albabat\readme\assets\style.css, %USERPROFILE%Albabat\readme\assets\script.js, %USERPROFILE%Albabat\readme\assets\banner.jpg, %USERPROFILE%Albabat\readme\pages\faq.html, %USERPROFILE%\Albabat\credits.txt, %USERPROFILE%\Albabat\Encryption_DBG.log, %USERPROFILE%\Albabat\assets\banner.jpg, %USERPROFILE%\Albabat\assets\script.js, %USERPROFILE%\Albabat\assets\style.css, %USERPROFILE%\Albabat\pages\faq.html
SHA256	e1c399c29b9379f9d1d3f17822d4496fce8a5123f57b33f00150f287740049e9, ce5c3ec17ce277b50771d0604f562fd491582a5a8b05bb35089fe466c67eef54, 483e0e32d3be3d2e585463aa7475c8b8ce254900bacfb9a546a5318fff024b74, 614a7f4e0044ed93208cbd4a5ab6916695e92ace392bc352415b24fe5b2d535c, bfb8247e97f5fd8f9d3ee33832fe29f934a09f91266f01a5fed27a3cc96f8fbb

References

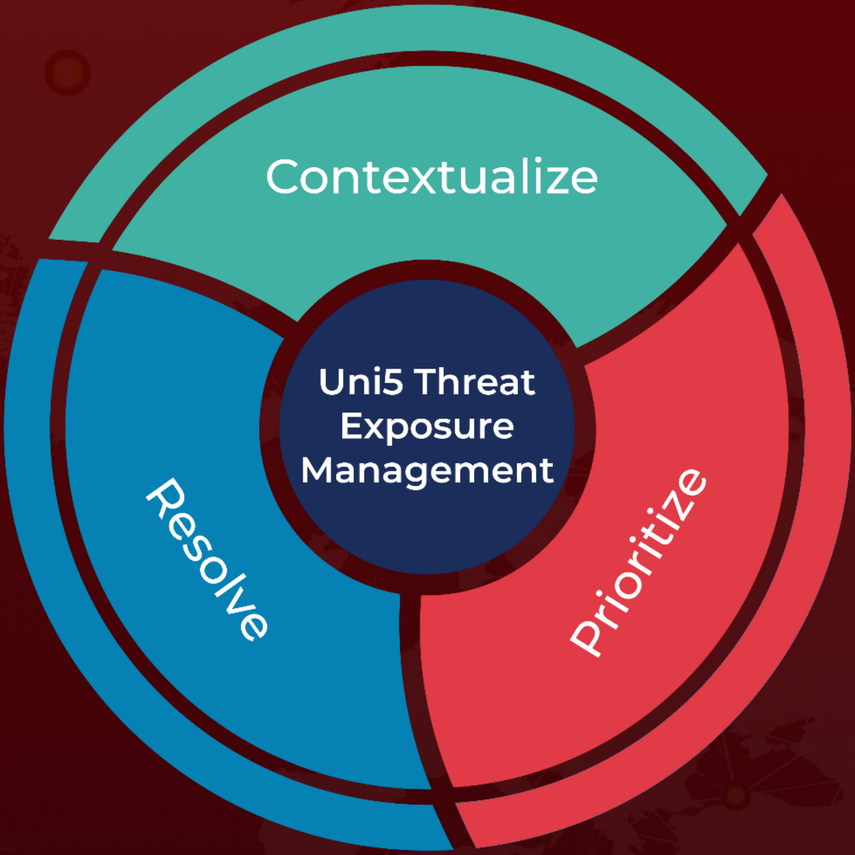
https://www.fortinet.com/blog/threat-research/ransomware-roundup-albabat

https://www.broadcom.com/support/security-center/protection-bulletin/albabat-ransomware-aka-white-bat

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 9, 2024 • 4:30 AM

More at www.hivepro.com