Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

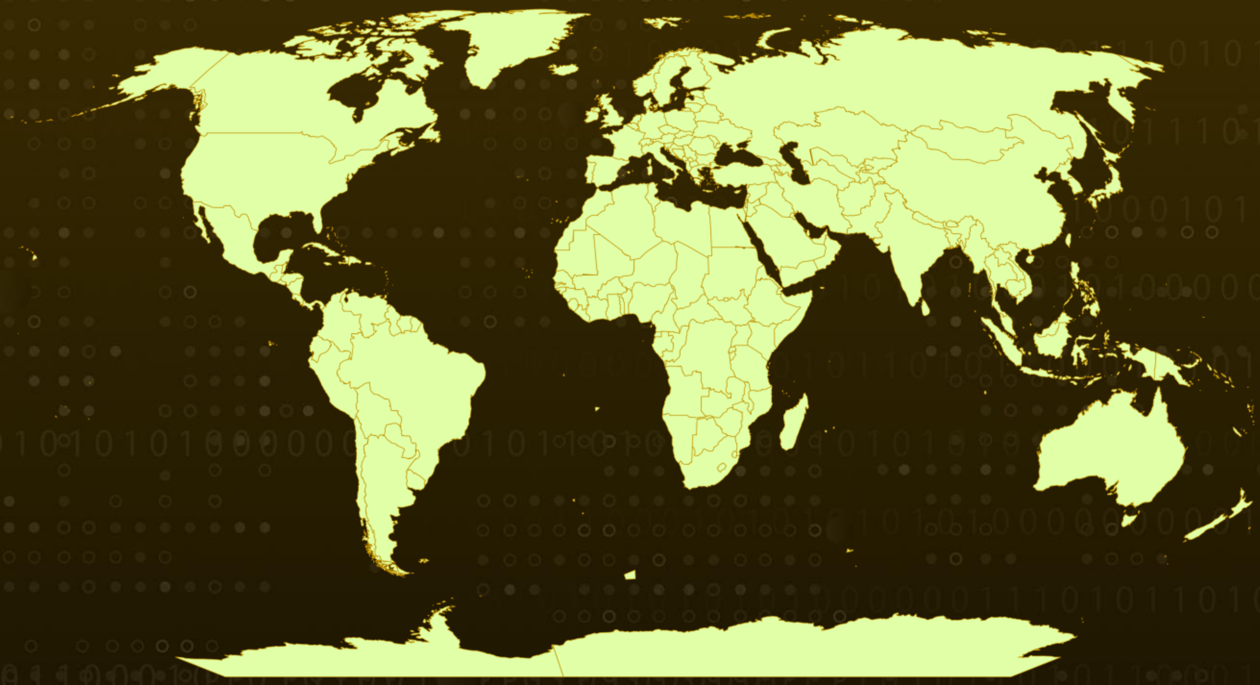
Bandook a 2007 Legacy Still Thriving in the Threat Landscape

Date of Publication	Admiralty Code	TA Number
December 22, 2023	A1	TA2023519

Summary

Active since: 2007
Malware: Bandook RAT (aka Bandok)
Attack Region: Worldwide
Affected Platform: Microsoft Windows
Attack: The Bandook malware is a persistent remote access trojan (RAT) that surfaced in 2007. Programmed in Delphi and C++, it has evolved through various iterations over the years and has historical associations with Dark Caracal. It featured prominently in a campaign dubbed 'Operation Manul'.

Attack Regions



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

Attack Details

#1

The Bandook malware also referred to as Bandok, is a remote access trojan (RAT) that first emerged in 2007, sustaining its malicious activities over numerous years. Programmed in both Delphi and C++, it originated as a commercial RAT created by PrinceAli, a Lebanese developer. As time progressed, various iterations of the Bandook malware surfaced online, resulting in its widespread availability for public download.

#2

In a recent campaign observed around October, a new variant of Bandook was distributed via a PDF file. The PDF document contained a shortened URL, guiding users to download a password-protected .7z file. Upon deployment, Bandook establishes a registry key embedded with control code, enabling the persistence of its payload and governing its behavioral functions. The injector component decrypts the payload, seamlessly integrating it into msinfo32.exe.

#3

A variant documented in 2021 required four control codes, producing four explorer.exe processes injected in a single execution. Initially, Bandook transmits victim information to its command-and-control (C2) server, followed by activities such as file manipulation, registry adjustments, downloads, information exfiltration, file execution, invocation of functions in DLLs from the C2, control over the victim's computer, process termination, and the uninstallation of the malware. Bandook has historical associations with Dark Caracal and featured prominently in a separate campaign known as "Operation Manul."

Recommendations

Email Security: Implement robust email filtering solutions to reduce the likelihood of spam and phishing emails reaching users' inboxes, thereby helping to filter out potentially harmful content.

Behavioral Analysis and Anomaly Detection: Incorporate behavioral analysis and anomaly detection tools to identify and stop processes initiated by the malware. Monitor for unusual system behavior, such as termination of specific processes or connections to unfamiliar websites.

Network Traffic Monitoring: Implement network traffic monitoring to detect unusual patterns or connections, especially those related to downloader URLs. Continuously monitor and analyze network activities for potential signs of a security threat.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1059 Command and Scripting Interpreter	T1005 Data from Local System	T1140 Deobfuscate/Decode Files or Information
T1083 File and Directory Discovery	T1070 Indicator Removal	T1070.004 File Deletion	T1105 Ingress Tool Transfer
T1056 Input Capture	T1027 Obfuscated Files or Information	T1566 Phishing	T1055 Process Injection
T1113 Screen Capture	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1041 Exfiltration Over C2 Channel
T1204 User Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	77[.]91[.]100[.]237, 45[.]67[.]34[.]219
SHA256	8904ce99827280e447cb19cf226f814b24b0b4eec18dd758e7fb93476b7bf8b8, d3e7b5be903eb9a596b9b2b78e5dd28390c6aadb8bdd4ea1ba3d896d99fa0057, 3169171e671315e18949b2ff334db83f81a3962b8389253561c813f01974670b,

TYPE	VALUE
SHA256	e87c338d926cc32c966fce2e968cf6a20c088dc6aedf0467224725ce36c9a525, 2e7998a8df9491dad978dee76c63cb1493945b9cf198d856a395ba0fae5c265a, 430b9e91a0936978757eb8c493d06cbd2869f4e332ae00be0b759f2f229ca8ce, cd78f0f4869d986cf129a6c108264a3517dbcf16ecfc7c88ff3654a6c9be2bca

References

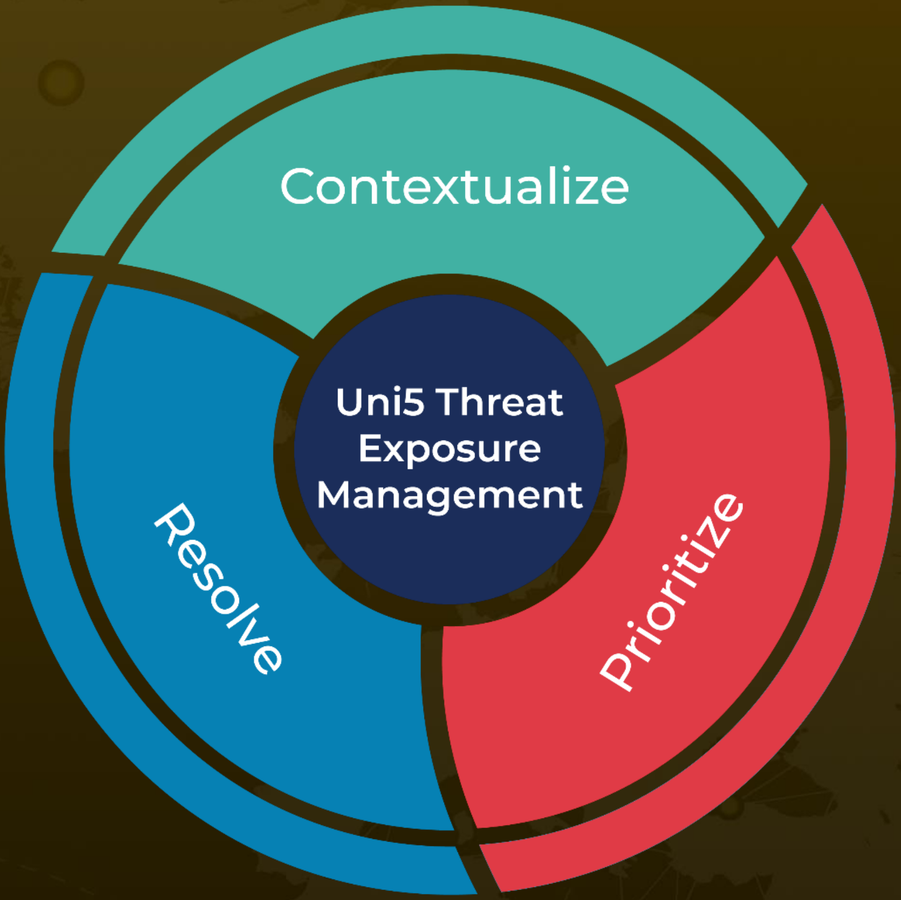
https://www.fortinet.com/blog/threat-research/bandook-persistent-threat-that-keeps-evolving

https://attack.mitre.org/software/S0234/

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

December 22, 2023 • 4:00 AM

More at www.hivepro.com