Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

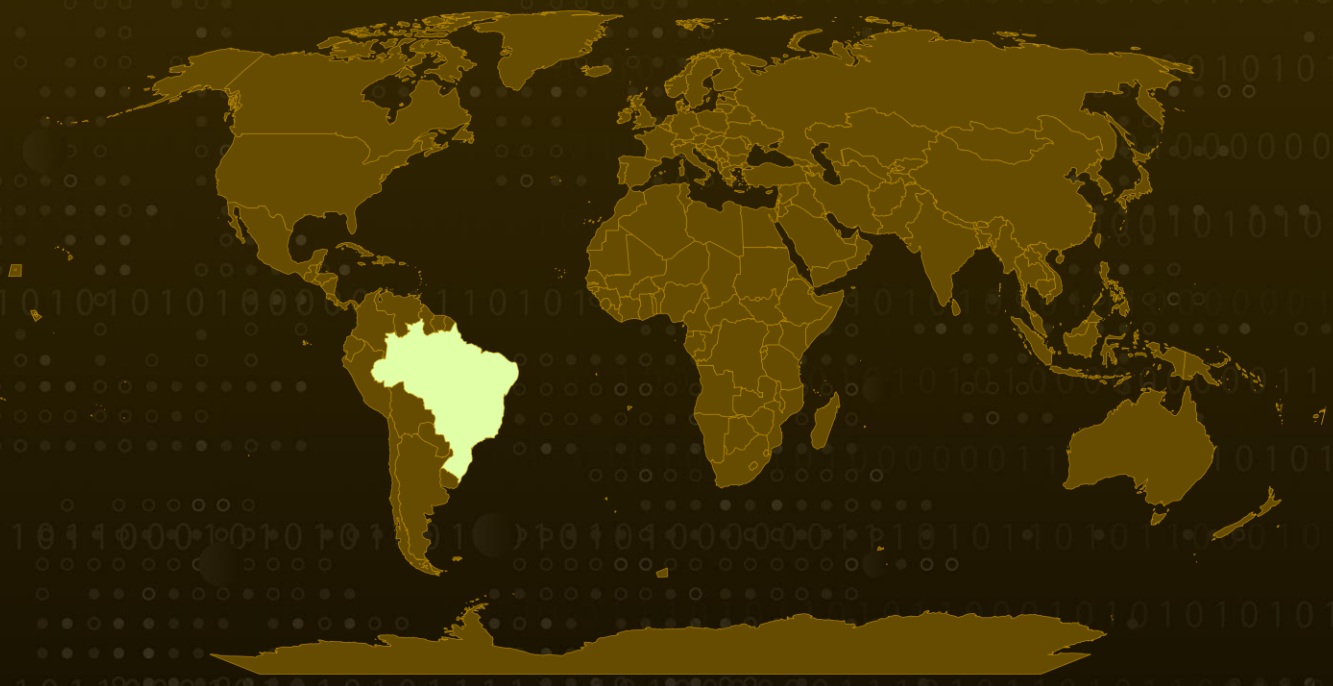
Coyote: A Sophisticated Banking Trojan Targeting Financial Information

Date of Publication	Admiralty Code	TA Number
February 12, 2024	A1	TA2024054

Summary

Attack Discovered: February 2024
Attack Region: Brazil
Affected Industries: Banking
Malware: Coyote
Attack: A new banking trojan called Coyote is currently targeting more than 60 banking institutions, primarily in Brazil. The malware distributes itself using the Squirrel installer and executes its infection process using Node.js and Nim, a relatively new multi-platform programming language.

Attack Regions



Attack Details

#1 The emergence of a new malware named Coyote is alarming, particularly due to its targeted focus on users of over 60 banking institutions, primarily located in Brazil. Of notable concern is the sophisticated infection chain employed by Coyote, utilizing various advanced technologies that distinguish it from conventional banking Trojan infections.

#2 Unlike typical banking Trojans, which often employ MSI installers or the Delphi programming language, Coyote demonstrates a unique approach in its development and deployment. The distribution method of this malware involves the Squirrel installer, while its infection process is completed using Node.js and Nim, a newer multi-platform programming language.

#3 Coyote follows a sequence involving the execution of complex JavaScript code by a Node.js application, a Nim loader unpacking a .NET executable, and ultimately, the launch of a Trojan. While Coyote skips code obfuscation, it employs string obfuscation with AES encryption to enhance its stealth. The Trojan's primary goal is consistent with typical banking Trojan behavior: monitoring access to specific banking applications or websites.

#4 Coyote malware monitors the applications open on a victim's computer. It can execute various commands, including capturing screenshots, logging keystrokes, terminating processes, displaying fake overlays, simulating mouse cursor movements, and initiating computer shutdowns. Additionally, it can perform malicious activities in the background and display a fake "Working on updates..." message to obstruct the user's access to the machine.

#5 The incorporation of Nim as a loader enhances the complexity of the trojan's architecture. This evolution highlights how threat actors are adapting and incorporating the latest languages and technologies into their malicious activities, emphasizing the increasing sophistication of the threat landscape.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Install apps from reliable sources: Ensure you install applications from reliable sources, it is crucial for maintaining the security and integrity of your devices.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact
T1113 Screen Capture	T1055 Process Injection	T1056 Input Capture	T1560 Archive Collected Data
T1140 Deobfuscate/Decode Files or Information	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1529 System Shutdown/Reboot	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1037 Boot or Logon Initialization Scripts	T1037.001 Logon Script (Windows)		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	03 eacccb664d517772a33255dff96020, 071b6efd6d3ace1ad23ee0d6d3eead76, 276f14d432601003b6bf0caa8cd82fec, 5134e6925ff1397fdda0f3b48afec87b, Bf9c9cc94056bcdae6e579e724e8dbbd
Domains	atendesolucao[.]com, servicoasso[.]com, dowfinanceiro[.]com, centralsolucao[.]com, traktinves[.]com, diadaacaodegraca[.]com, segurancasys[.]com

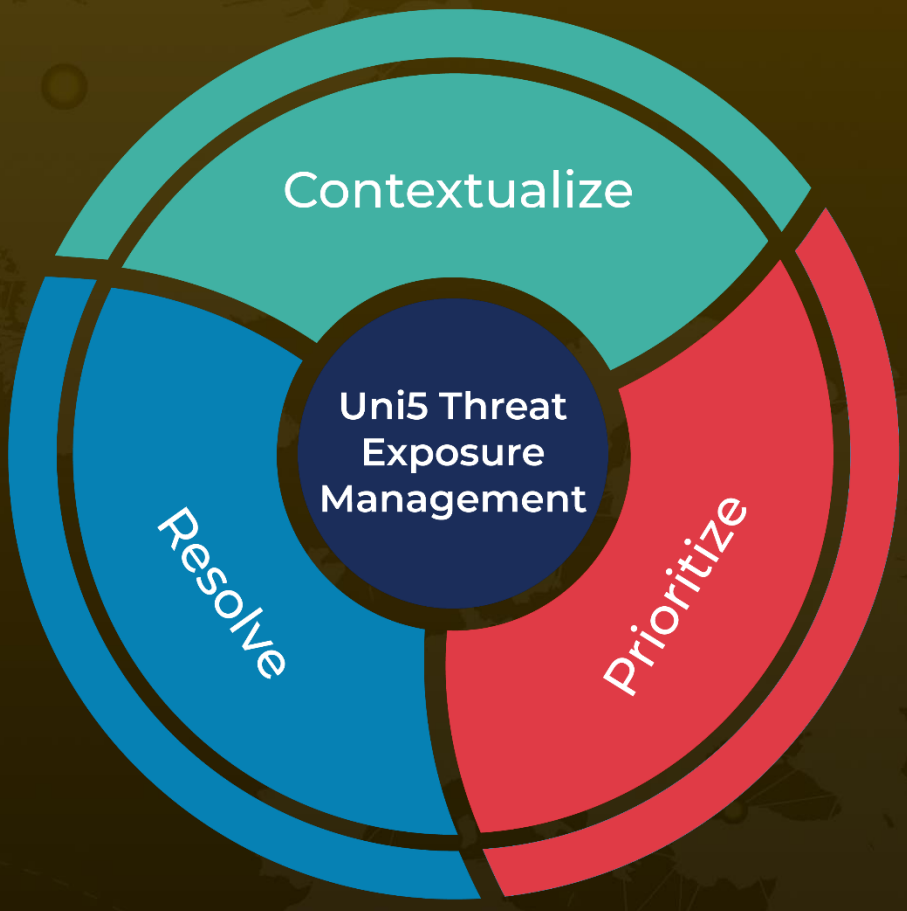
References

https://securelist.com/coyote-multi-stage-banking-trojan/111846/

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 12, 2024 • 3:20 AM

More at www.hivepro.com