Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

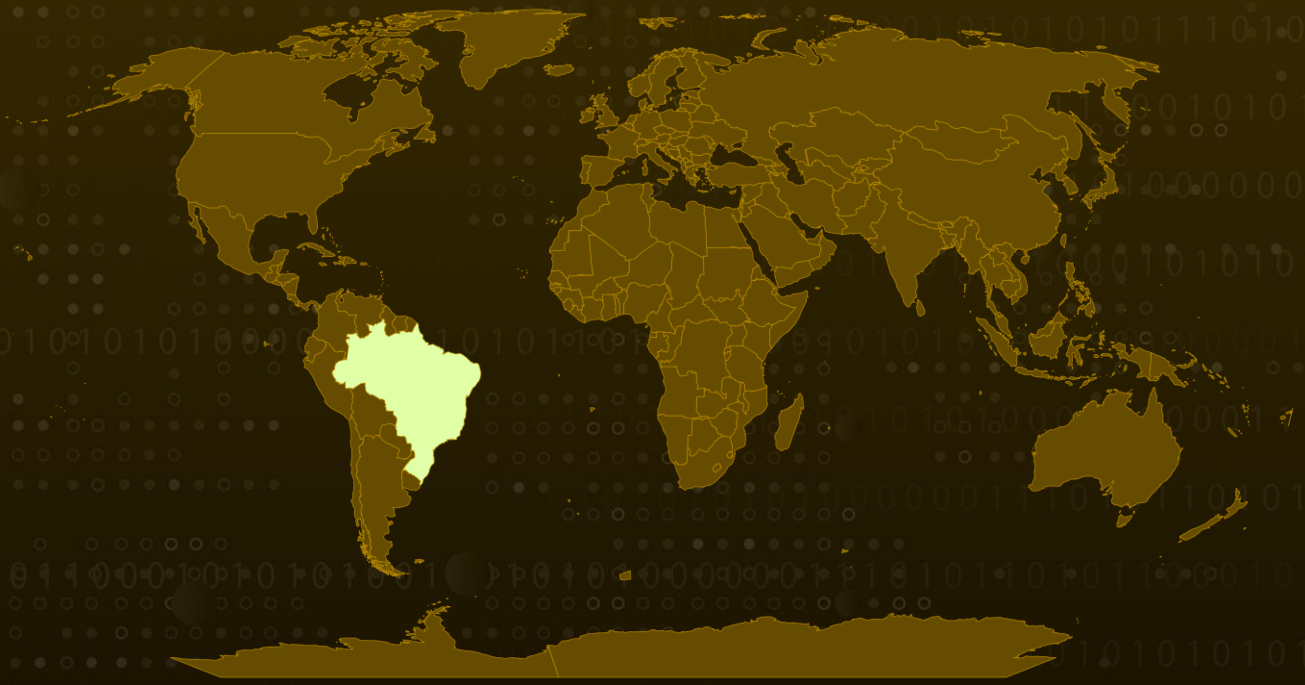
Attackers Exploit Brazil's PIX System with GoPIX Malware Campaign

Date of Publication	Admiralty Code	TA Number
October 26, 2023	A1	TA2023434

Summary

First appeared: December 2022
Attack Region: Brazil
Affected Platform: WhatsApp Web
Malware: GoPIX
Attack: The popularity of Brazil's PIX payment system has attracted cybercriminals using GoPIX malware, targeting users searching for "WhatsApp web" with malicious ads. This poses a threat to users' financial and personal information.

Attack Regions



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

Attack Details

#1

The PIX payment system in Brazil, known for its low acceptance cost due to minimal intermediaries, has become highly popular. However, this popularity has attracted cybercriminals using a new malware called GoPIX. These attackers use malicious ads that surface when users search for "WhatsApp web" on search engines, leading them to a malware-infested landing page.

#2

To evade detection, a cloaking service is employed, distinguishing between humans and bots using a fraud prevention solution. Legitimate users are then presented with a fake WhatsApp download page that conceals a malicious installer. The malware's download source varies based on the user's system configuration to bypass security measures.

#3

The installer's main purpose is to launch GoPIX using a technique called process hollowing, injecting the payload into the Windows system process svchost.exe. GoPIX functions as a clipboard stealer, replacing PIX payment requests with the attacker's controlled PIX string retrieved from a command-and-control server. The malware can also manipulate Bitcoin and Ethereum wallet addresses, although these are hardcoded.

#4

Similar attacks have targeted users searching for messaging apps like WhatsApp and Telegram, luring victims to fraudulent pages where they are prompted to scan QR codes. Furthermore, there is a growing trend of Latin American-focused malware expanding its reach to Europe.

#5

The cybercrime landscape is witnessing a surge in information stealers offered as malware-as-a-service (MaaS), enabling less skilled threat actors to conduct attacks. This campaign poses a significant threat to users in Brazil, potentially leading to financial losses and other serious consequences if infected with GoPIX.

Recommendations

Use Trusted Sources: Download applications and software only from official, trusted sources. Avoid downloading from third-party websites or clicking on links in unsolicited emails or ads.

Secure Browsing: Use secure browsing practices, and consider deploying ad-blockers or privacy-focused browsers to minimize exposure to malicious ads.

Software and System Updates: Keep your server's software, including the operating system and all applications, up-to-date with the latest security patches. Vulnerabilities in outdated software can be exploited by malware like GoPIX.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0004 Privilege Escalation	TA0040 Impact	T1055.001 Dynamic-link Library Injection	T1140 Deobfuscate/Decode Files or Information
T1055.012 Process Hollowing	T1055 Process Injection	T1036 Masquerading	T1583 Acquire Infrastructure
T1583.008 Malvertising	T1189 Drive-by Compromise	T1059.001 PowerShell	T1059 Command and Scripting Interpreter
T1204 User Execution	T1204.001 Malicious Link		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	EB0B4E35A2BA442821E28D617DD2DAA2, 6BA5539762A71E542ECAC7CF59BDDF79, 333A34BD2A7C6AAF298888F3EF02C186

References

https://thehackernews.com/2023/10/malvertising-campaign-targets-brazils.html

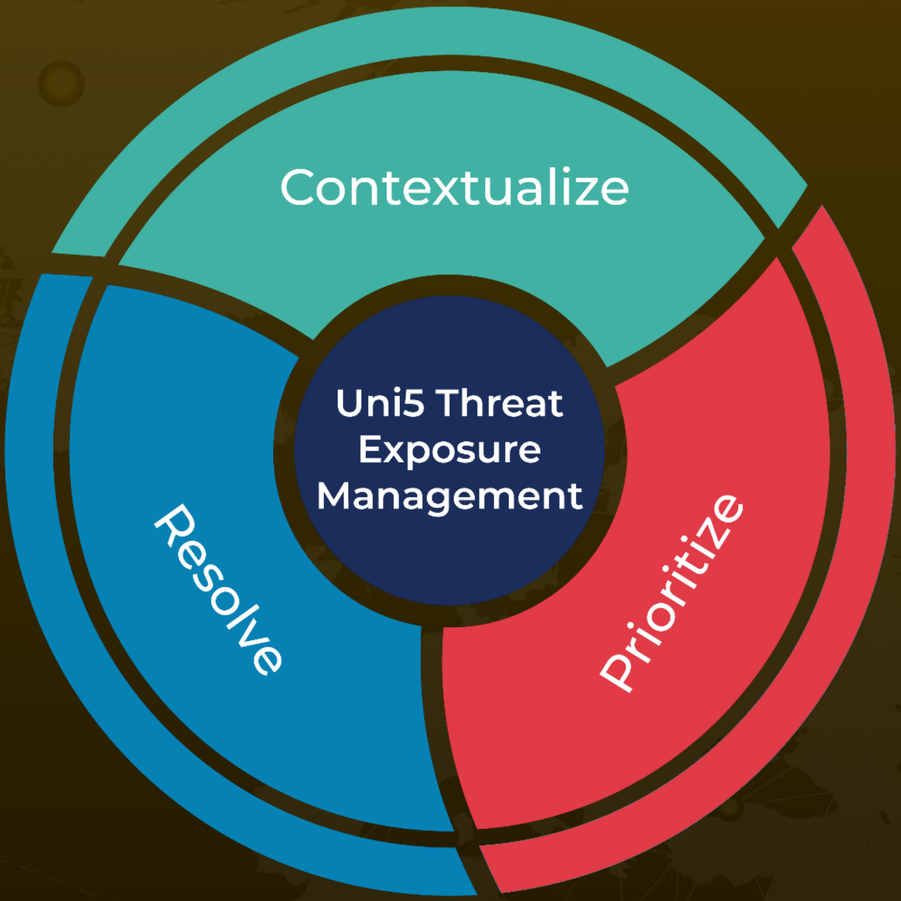
https://securelist.com/crimeware-report-gopix-lumar-rhysida/110871/

https://www.bcb.gov.br/en/financialstability/pix_en

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

October 26, 2023 • 5:00 AM

More at www.hivepro.com