Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

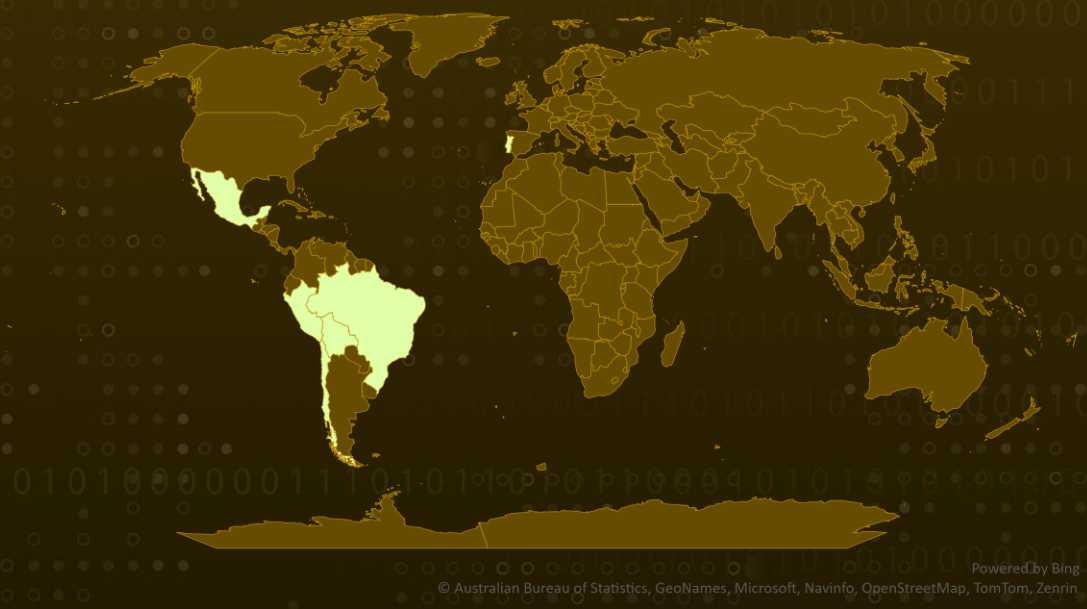
Mispadu Targets Latin America with MalSpamming

Date of Publication	Admiralty Code	TA Number
March 22, 2023	A1	TA2023153

Summary

Attack Began: August 2022
Attack Region: Chile, Mexico, Peru, Brazil, Bolivia and Portugal
Attack Industry: Online Banking, Schools, Government Services, Social Media, Gaming, E-commerce, Public Repositories
Malware: Mispadu
Attack: Mispadu has been linked to various spam campaigns, and it is capable of stealing both monetary and credential information while acting as a backdoor through keystroke and screenshot capture.

Attack Regions



Attack Details

#1

Mispadu is a banking trojan that was first documented in 2019 and has been linked to multiple spam campaigns targeting countries such as Bolivia, Chile, Mexico, Peru, and Portugal since August 2022. The trojan can cause financial and credential theft, operate as a backdoor by capturing keystrokes and taking screenshots, and target victims by commandeering legitimate websites and converting them into command-and-control servers to distribute malware.

#2

It delivers various types of malware depending on the region it infects and can discover installed antivirus software, extract login credentials from Google Chrome and Microsoft Outlook, and support the downloading of more malware. Mispadu implements deceptive overlay screens to steal sensitive data linked to online banking gateways and other information. Mispadu has bypassed detection by a wide range of security software and has harvested over 90,000 bank account credentials from over 17,500 unique websites. Mispadu is known for targeting Latin American countries through malvertising and spamming campaigns, and its modus operandi as malware-as-a-service.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

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	T1566 Phishing	T1566.001 Spearphishing Attachment	T1218 System Binary Proxy Execution
T1218.011 Rundll32	T1176 Browser Extensions	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1140 Deobfuscate/Decode Files or Information	T1036 Masquerading	T1059 Command and Scripting Interpreter	T1056 Input Capture
T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1552.002 Credentials in Registry	T1083 File and Directory Discovery
T1057 Process Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery	T1082 System Information Discovery
T1115 Clipboard Data	T1113 Screen Capture	T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	E903B37B1E42D0B8BF0514CB13A46233 E5967A8274D40E0573C28B664670857E 0ADB9B817F1DF7807576C2D7068DD931 2858CDF0B9FB6DDD18709909DF612063 3FB45296ABDC78792FB609C187B4A89D AB80D005BCC4641D5D1AE75FBB2723B9 0D8D82E1810F549F8645535C836D7AFD 293B9621798EE17005D1EFFE463A8989 618A60899AAE66EA55E5DC8374C7B828 B41E2B88FFF36FF4937DC19F2677EE84 72E83B133A9E4CECD21FDB47334672F6 A96125294AFA1C3F92AB7BE615DC1CBE

TYPE	VALUE
Domains	germogenborya[.]top germogenborya[.]at grintour[.]newdestuner[.]xyz russk22[.]icu
URLs	hxxps[:]//www.zairtaz[.]com/wp-content/plugins/license/inc/hydra/do/it.php?f=9&w=Windows%2010, hxxps[:]//imberform[.]com/img/?dew98fy348erf7i, hxxp[:]//vasuk[i].in/wp-content/img/do/it.php?f=9&w=Windows%207, hxxp[:]//luzca[.]com/img/do/it.php?f=2&w=Windows%207, hxxp[:]//nbviajesacapulco[.]com/pruc/it.php?f=9&w=Windows%207, hxxp[:]//nbviajesacapulco[.]com/pixel/it.php?f=2&w=Windows%207, hxxp[:]//www.castleblack[.]online/cfr/it.php?f=2&w=Windows%207, hxxps[:]//dicktres.com[.]br/pontecom/wp-content/img/do/it.php, hxxps[:]//bdadvisors[.]ma/img/do/it[.]php?f=2&w=Windows%2010, hxxp[:]//blog.traveldealsbd[.]com/images/arrow/do/it.php?b1=1&v1=1033&v2=1033&v3=Windows%207&v4=User&v5=X64, hxxp[:]//tripsapata[.]com/assets/images/swan/do/it.php, hxxps[:]//blablamap[.]net/images/arrow/do/it.php, hxxp[:]//facturacion.sat[.]gob.educationalwriters.com/do/it.php?f=2&w=Windows%207, hxxp[:]//aguiasoft.com[.]br/blog/hydra/do/it.php?b1=1&v1=3082&v2=2058&v3=windows%207&v4=admin&v5=x64, hxxp[:]//explanada2023[.]com/wp-includes/stylish/it.php?f=2&w=Windows%207, hxxp[:]//vaadiandkoh[.]com/ue/app/do/it.php?f=9&w=Windows%207, hxxp[:]//websylvania[.]com/psj/do/it.php?b1=1&v1=3082&v2=1034&v3=windows%207&v4=admin&v5=x64, hxxp[:]//publicpressmagazine[.]com/images/swan/do/it.php?b1=1&v1=1033&v2=1033&v3=Windows%207&v4=User&v5=X86, hxxps[:]//factura61[.]click/2/?CQ9OCKlYIQOSZqMxY43B80jdDceyL69GLzh6HNkZ, hxxps[:]//sxconstructions[.]com[.]au/wp-content/img/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%207&v5=User&v6=X%2086&v7=, hxxps[:]//kh7jv[.]store/?JDCE8IFt3QZJ2Ms4FQv8bp5q9KM6bFvMKUeE7QOLg7z4Kl9Oa48sMGRJDCE8IFt3QZJ2Ms4FQv8bp5q9KM6bFvMKUeE7QOLg7z4Kl9Oa48sMGR,

TYPE	VALUE
URLs	hxxps[:]//sxconstructions[.]com.au/wp-content/img/do/it.php?f=2&w=Windows%210, hxxps[:]//sxconstructions[.]com.au/wp-content/img/do/it.php?info2=DATOS, hxxp[:]//highlineadsl[.]com/ddd/it.php?f=3&w=Windows%207, hxxp[:]//germogenborya[.]top/rest/?h=CODE, hxxp[:]//vaadiandkoh[.]com/ue/app/do/it.php?f=9&w=Windows%207, hxxp[:]//grintour[.]newdestuner[.]xyz/g1, hxxp[:]//grintour.newdestuner[.]xyz/dhyhsh3a.php, hxxps[:]//facturaciones[.]click/?7kqhhbEE9Y1FiEBZ0Uc7izRLyJ2TWdZFK0qnXvXU, hxxp[:]//russk22[.]icu/brbr.txt, hxxps[:]//bola.com[.]au/images/hh/cfdi/do/it.php?f=2&w=Windows%2010, hxxps[:]//splendidgifts.com[.]my/hiway/ap2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=User&v6=X64, hxxps[:]//tequilamisorpresa[.]com/ytweshdg.php?id=, hxxp[:]//formas-mexico[.]com/formas.xls, hxxps[:]//retiro10[.]click/, hxxps[:]//facturaciones[.]click, hxxps[:]//facturasnet[.]store, hxxps[:]//facturaciones3[.]click/, hxxps[:]//retiro10[.]store/ hxxp[:]//grintour[.]newdestuner[.]xyz/g1 hxxp[:]//grintour.newdestuner[.]xyz/dhyhsh3a.php hxxps[:]//facturaciones[.]click/?7kqhhbEE9Y1FiEBZ0Uc7izRLyJ2TWdZFK0qnXvXU hxxp[:]//russk22[.]icu/brbr.txt hxxps[:]//bola.com[.]au/images/hh/cfdi/do/it.php?f=2&w=Windows%2010 hxxps[:]//splendidgifts.com[.]my/hiway/ap2/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%2010&v5=User&v6=X64 hxxps[:]//tequilamisorpresa[.]com/ytweshdg.php?id= hxxp[:]//formas-mexico[.]com/formas.xls hxxps[:]//retiro10[.]click/ hxxps[:]//facturaciones[.]click hxxps[:]//facturasnet[.]store hxxps[:]//facturaciones3[.]click/ hxxps[:]//retiro10[.]store/
IPV4:PORT	104[.]238[.]182[.]44:4000 104[.]238[.]182[.]44:4001 140[.]82[.]47[.]181:4000 140[.]82[.]47[.]181:4001

TYPE	VALUE
Filenames	%AppData%\Roaming\herman\a3x\herndon\Factura_Deuda_423534.cmd %AppData%\Roaming\herman\exe\vayala\jordan.exe %AppData%\Roaming\herman\a3x\Factura_Deuda_423534.a3x %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\DriverAudio.lnk %USER%\Downloads\sastreria.xls.exe %PUBLIC%\gnVzjGd.vbs
Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run:WinDriver

References

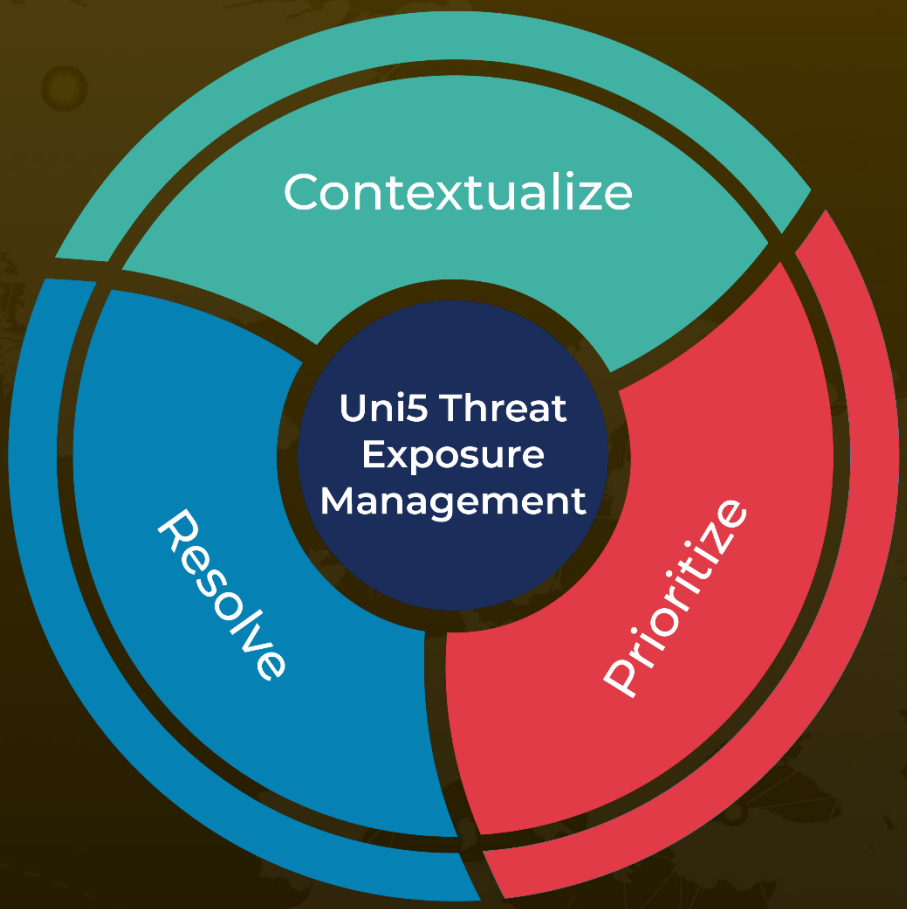
https://www.metabaseq.com/mispadu-banking-trojan/

https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

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

March 22, 2023 • 5:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com