Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

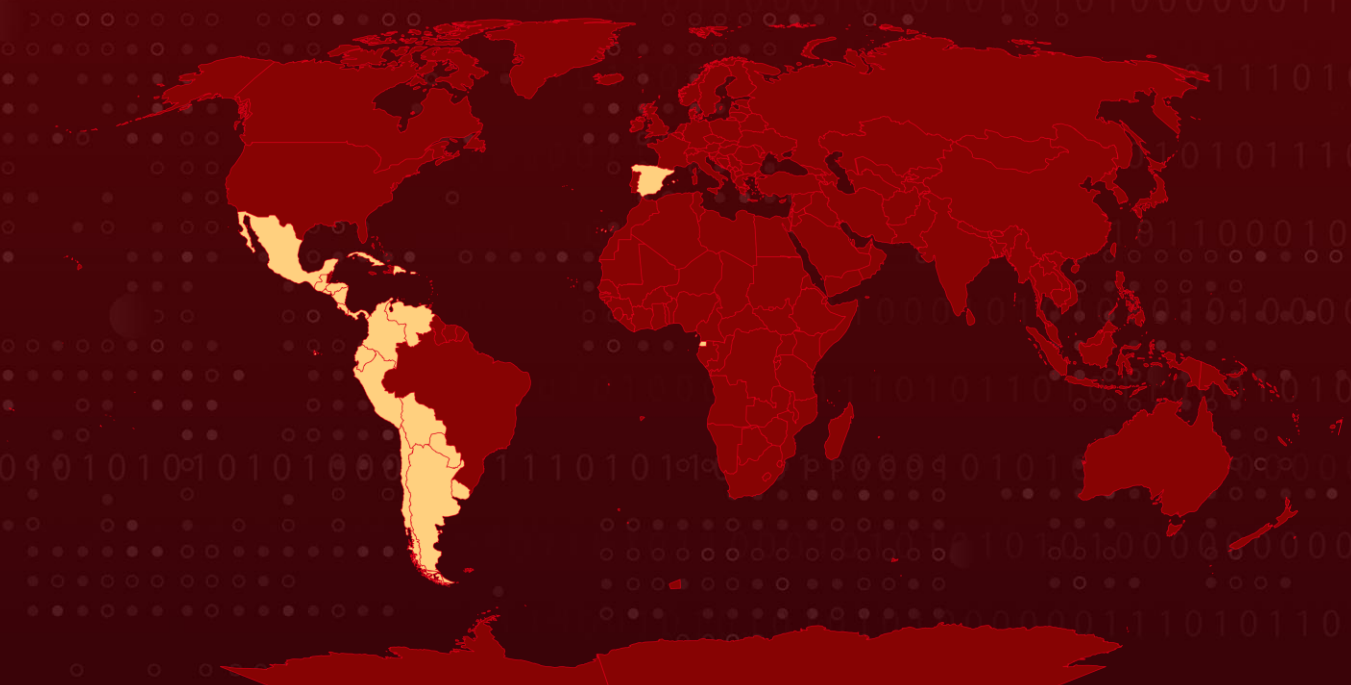
A New Horabot Botnet Threat Targeting Spanish-Speaking Users in the Americas

Date of Publication	Admiralty Code	TA Number
June 02, 2023	A1	TA2023250

Summary

First Appearance: November 2020
Malware: Horabot
Target Countries: Argentina, Bolivia, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Equatorial Guinea, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Puerto Rico, Uruguay, Venezuela, Spain
Affected Platforms: Windows
Attack: A new botnet program called "Horabot" being used by a threat actor to deploy a banking trojan and spam tool, targeting Spanish-speaking users in the Americas.

Attack Regions



Attack Details

#1 A new botnet program called "Horabot" deployed by a threat actor since November 2020. The botnet delivers a banking trojan and spam tool to victim machines. The attacker primarily targets Spanish-speaking users in the Americas, with a focus on Mexico.

#2 The campaign has also affected users in Uruguay, Brazil, Venezuela, Argentina, Guatemala, and Panama. The attacker controls the victim's Outlook mailbox, collects email addresses, and sends phishing emails with malicious attachments.

#3 The banking trojan steals login credentials, operating system information, and security codes. The spam tool compromises email accounts and sends spam emails. The attacker's infrastructure involves multiple hosts, including an Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instance. The attacker uses lookalike domains to evade detection.

#4 The attack chain includes phishing emails, PowerShell downloader scripts, and DLL sideloading. The payloads include a banking trojan and a spam tool. The banking trojan collects sensitive information and has remote desktop management capabilities. It also overlays fake windows to steal security codes. The spam tool compromises mailboxes and sends phishing emails.

Recommendations

Enhanced Email Security: Implement robust email security measures specifically designed to detect and block the malicious activities associated with the Horabot botnet. This includes advanced email filtering, attachment scanning, and domain reputation checks to prevent phishing emails and malicious attachments from reaching users' inboxes.

Network Monitoring and Intrusion Detection: Deploy robust network monitoring tools and intrusion detection systems to identify any signs of Horabot botnet activities within the network. Monitor outgoing traffic for unusual connections, communication with known malicious hosts, or the presence of specific botnet-related indicators. Actively investigate and respond to any alerts or anomalies detected during network monitoring.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0001 Initial Access	T1059 Command and Scripting Interpreter	T1059.001 Power Shell	T1584 Compromise Infrastructure
T1566.001 Spearphishing Attachment	T1566 Phishing	T1056.001 Keylogging	T1082 System Information Discovery
T1190 Exploit Public-Facing Application	T1204.001 Malicious Link	T1204 User Execution	T1584.005 Botnet
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1036 Masquerading	T1547.009 Shortcut Modification
T1027 Obfuscated Files or Information	T1547.001 Registry Run Keys / Startup Folder	T1115 Clipboard Data	T1113 Screen Capture
T1497 Virtualization/Sandbox Evasion	T1003 OS Credential Dumping	T1078 Valid Accounts	T1070.004 File Deletion
T1070 Indicator Removal	T1083 File and Directory Discovery	T1106 Native API	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	139[.]177[.]193[.]74 185[.]45[.]195[.]226 216[.]238[.]70[.]224 51[.]38[.]235[.]152 137[.]220[.]53[.]87 212[.]46[.]38[.]43 191[.]101[.]2[.]101
Domains	tributaria[.]website facturacionmarzo[.]cloud m9b4s2[.]site wiqp[.]xyz ckws[.]info amarte[.]store
SHA256	63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064 aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252 fd932d83965d20683ea7f99244dc672e0b4187c9e7588578b626b99d67ac71a6 39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611 474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76 07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da 74a7d13289029d8439e38e0acb4d3b526c63ae863a41218a511182d8f0e6ebef 26e06886d9dde7c9ecdc9b223e5f325d0af27cc9b470179a8e493ac300bd783e 294363039bf93d4c34c8769e581b9c47f8ea210e427fc1feed128bd9bf979a4a
URLs	hxxps[://]tributaria[.]website/ hxxps[://]tributaria[.]website/ESP/12/151222/UP/UP hxxps[://]tributaria[.]website/A/08/150822/AU/TST/INDEX[.]PHP?LIST hxxps[://]tributaria[.]website/a/09/01092022/au/tst/index[.]php?list hxxps[://]tributaria[.]website/a/08/150822/up/up hxxps[://]tributaria[.]website/esp/12/151222/up/up hxxps[://]tributaria[.]website/a/W_/X\\W_YY/au/au hxxps[://]tributaria[.]website/a/08/150822/au/au

TYPE	VALUE
URLs	hxxp[://]tributaria[.]website:443/ hxxps[://]tributaria[.]website/A/08/150822/AU/AU hxxps[://]tributaria[.]website/esp/12/151222/au/au hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0703[.]html hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/adjuntos_0703[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/logs/index[.]php?CHLG hxxp[://]139[.]177[.]193[.]74/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/tst/index[.]php?list hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/09/01092022/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]htm hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]html hxxp[://]139[.]177[.]193[.]74:443/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2012[.]html hxxp[://]139[.]177[.]193[.]74/A/08/150822/AU/ADJUNTOS_2012[.]HTML hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/gm/index[.]php?CHLG hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/documento-pdf[.]html hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/index[.]php?va hxxps[://]facturacionmarzo[.]cloud/m/archivos[.]pdf[.]html hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html hxxp[://]216[.]238[.]70[.]224/20/t/e/m.zip hxxp[://]ckws[.]info/ hxxps[://]ckws[.]info/a/310122/up/up hxxps[://]ckws[.]info/a/310122/au/au hxxp[://]ckws[.]info/a/07/080722/up/up hxxp[://]ckws[.]info/a/07/080722/au/au hxxps[://]ckws[.]info/A/07/080722/UP/UP hxxps[://]ckws[.]info/a/0511/ hxxp[://]ckws[.]info/a/0511 hxxps[://]ckws[.]info/a/0511/up/up hxxp[://]ckws[.]info/a/0511/au/au hxxp[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/a1/u hxxps[://]m9b4s2[.]site/a1/u/ hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html%20%20Servicio%20de%20Administraci%C3%B3n%20Tributaria hxxp[://]m9b4s2[.]site/2001525248/12457856[.]html hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html=0A= hxxps[://]m9b4s2[.]site/tst/index[.]php?list hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat hxxps[://]m9b4s2[.]site/a1/u/a/index[.]php hxxps[://]m9b4s2[.]site/a1/u/a/index[.]p[.]h[.]p hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat' hxxp[://]m9b4s2[.]site/N/I hxxp[://]m9b4s2[.]site/k/i

TYPE	VALUE
URLs	hxxp[://]m9b4s2[.]site/A/I hxxp[://]m9b4s2[.]site/k hxxp[://]m9b4s2[.]site/a/i hxxp[://]m9b4s2[.]site/K/I hxxp[://]m9b4s2[.]site/A/I' hxxp[://]m9b4s2[.]site/k/I hxxps[://]m9b4s2[.]site/i7_5_7_3_3_2E9Uogmx/i7_5_7_3_3_2E9Uog/i7_5_7_3_3_2E9Uogal/i7_5_7_3_3_2E9Uog hxxps[://]m9b4s2[.]site/M1S8823HSN34/?1538567474 hxxp[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/09/01092022/au/au hxxp[://]wiqp[.]xyz/09/01092022/up/up hxxps[://]amarte[.]store/ hxxps[://]amarte[.]store/a/08/150822/au/au hxxps[://]amarte[.]store/a/08/150822/up/up hxxp[://]51[.]38[.]235[.]152/20/a/m/m[.]zip hxxp[://]137[.]220[.]53[.]87/20/t/p/m[.]zip hxxp[://]212[.]46[.]38[.]43/m/1 hxxp[://]212[.]46[.]38[.]43/e/1 hxxp[://]191[.]101[.]2[.]101/m/1

References

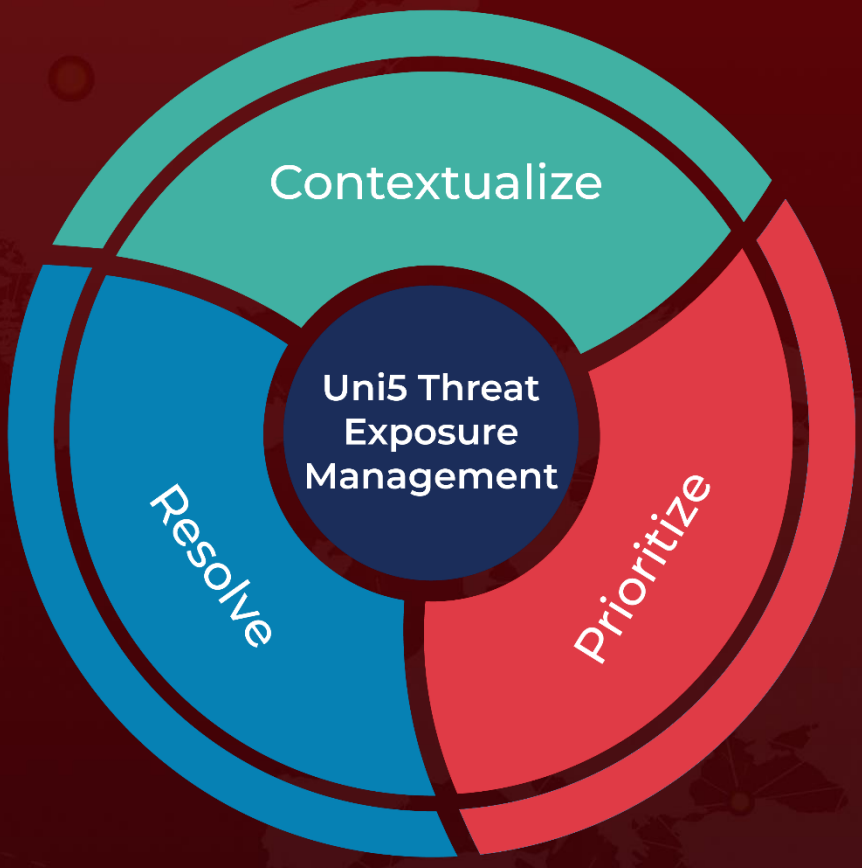
https://blog.talosintelligence.com/new-horabot-targets-americas/

https://github.com/Cisco-Talos/IOCs/blob/main/2023/05/new-horabot-targets-americas.txt

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

June 02, 2023 • 5:30 AM

More at www.hivepro.com