Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

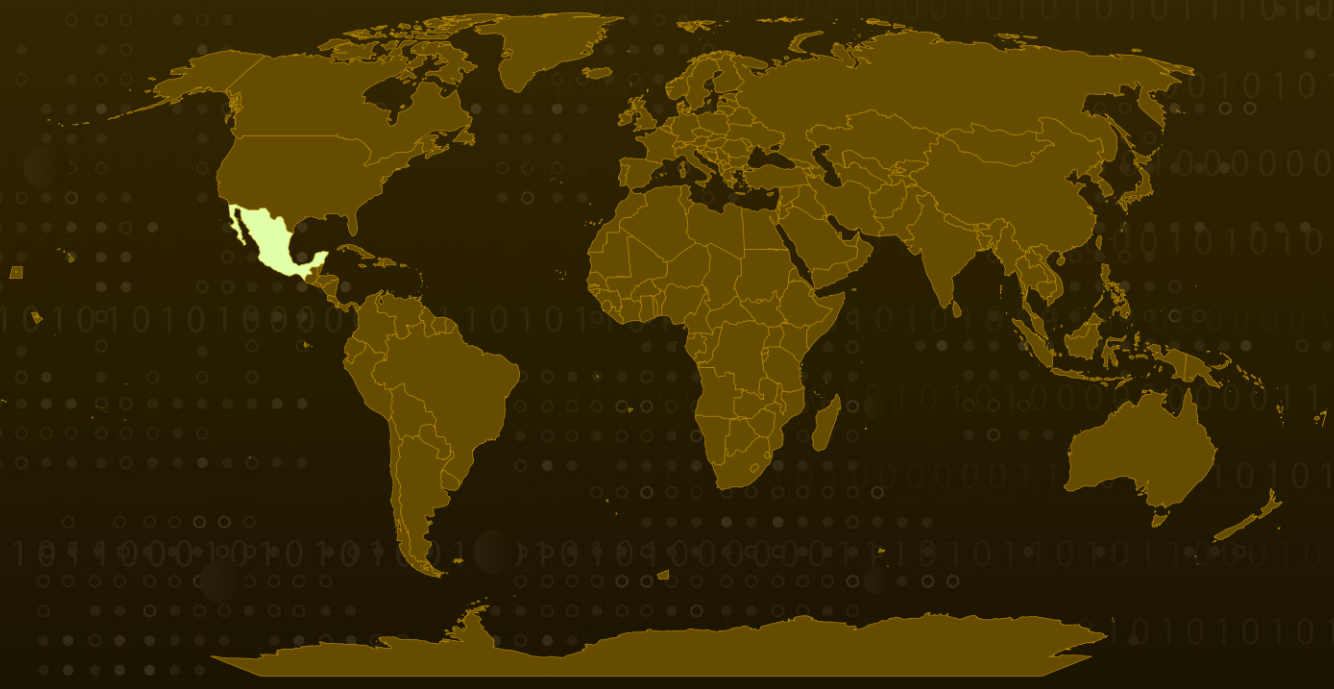
TimbreStealer Focuses On Mexico With Social Engineering

Date of Publication	Admiralty Code	TA Number
March 14, 2024	A1	TA2024101

Summary

Attack Began: November 2023
Attack Region: Mexico
Malware: TimbreStealer
Attack: Since at least November 2023, there has been a persistent phishing spam campaign targeting potential victims in Mexico. The campaign entices users to download TimbreStealer, a new information stealer that has been disguised. This campaign use financial-themed phishing emails to lure consumers into running the malicious application by taking them to a compromised website hosting the payload.

Attack Regions



Attack Details

#1 Since November 2023, there has been an ongoing phishing spam campaign in Mexico, aimed at enticing users to download TimbreStealer. The campaign utilizes geofencing tactics and phishing emails with financial themes. If users try to access the compromised website from a location other than Mexico, they will receive a blank PDF file, as the payload is hosted elsewhere. The campaign predominantly exploits the CDFI digital tax receipt standard in Mexico.

#2 TimbreStealer is an advanced malware designed to Collect credential information from the victim's machine, Search for Files, Collect OS information, Search for file extensions, Look for URLs Accessed, Disable System Protections, Look for Remote Desktop Software, POST data to remote site. It employs several sophisticated techniques including the use of custom loaders, the Heaven's Gate technique that executes 64-bit code within a 32-bit process, and direct system calls to bypass API monitoring mechanisms.

#3 TimbreStealer is designed to extract data from targeted systems through a three-stage process. These stages include the orchestrator layer, which identifies systems of interest, and the decryption layer, which extracts subsequent modules. The malware conducts various checks, such as verifying that the system language is Russian, if time zone is within a Latin American region and counting desktop child windows. Additionally, it performs checks for mutexes, searches for files and registry keys associated with previous infections, and scans system browsers for indications of legitimate user activity.

#4 The malware has an intricate decryption procedure that includes modules kept in the ".data" folder, a central orchestration DLL, and a global decryption key. By searching Ntdll for Zw* exports, the loader component generates an ordered hash table of functions. Following decoding, the orchestrator DLL is started by means of a modified PE loader, and the MZ header and PE signature are deleted.

#5 Orchestrator DLL further deploys installed DLL which has additional safeguards to deactivate user mode Event Tracing for Windows data collection and does the replacement of all loaded DLLs with clean copies. It also incorporates TLS callbacks and an additional encryption round to hinder analysis on external systems.

#6 This threat actor has been involved in distribution activities since at least September 2023. Initially, they used geofenced WebDAV servers to distribute a version of the **Mispadu** banking trojan, but later changed to TimbreStealer. Upon switching to this stealer, the threat actor drastically reduced employing Mispadu, we can speculate that TimbreStealer is a revamp of Mispadu.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	TA0040 Impact
T1566 Phishing	T1566.002 Spearphishing Link	T1566.001 Spearphishing Attachment	T1204 User Execution
T1204.002 Malicious File	T1105 Ingress Tool Transfer	T1190 Exploit Public-Facing Application	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1568 Dynamic Resolution
T1568.002 Domain Generation Algorithms	T1027 Obfuscated Files or Information	T1027.009 Embedded Payloads	T1027.010 Command Obfuscation

T1027.002 Software Packing	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1497 Virtualization/Sandbox Evasion
T1497.003 Time Based Evasion	T1497.001 System Checks	T1497.002 User Activity Based Checks	T1055 Process Injection
T1055.002 Portable Executable Injection	T1055.001 Dynamic-link Library Injection	T1055.012 Process Hollowing	T1140 Deobfuscate/Decode Files or Information
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1082 System Information Discovery	T1486 Data Encrypted for Impact
T1070 Indicator Removal	T1070.001 Clear Windows Event Logs	T1012 Query Registry	T1140 Deobfuscate/Decode Files or Information
T1053 Scheduled Task/Job	T1053.003 Cron	T1053.005 Scheduled Task	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1112 Modify Registry		

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://hamster69[.]senac2021[.]org/~armadillo492370/, hxxps://snapdragon50[.]crimsondragonemperor[.]com/~aster963249/, hxxps://69[.]64[.]35[.]1/~route649289/, hxxp://folio24[.]spacefordailyrituals[.]com/facdigital/55ae12184283dc, hxxp://folio47[.]marcialledo[.]com/seg_factura/e6bab6d032e282, hxxp://pdf43[.]marcialledo[.]com/factura/50e1e86db86ff2, hxxp://suscripcion95[.]servicioslomex[.]online/cfdi/0faa4a21fff2bb, hxxps://0[.]solucionegos[.]top/timbreDigital/e99522f778ea6a,

TYPE	VALUE
URLs	hxxps://auditoria38[.]meinastrohoroskop[.]com/factura/b5b0c16b999573, hxxps://auditoria42[.]altavista100[.]com/factura/b20569ae393e7e, hxxps://auditoria67[.]mariageorgina[.]com/cfdi/bb743b25f5c526, hxxps://auditoria7[.]miramantolama[.]com/factura/d84d576baf1513, hxxps://auditoria82[.]taoshome4sale[.]com/seg_factura/efebfc104991d4, hxxps://auditoria84[.]meinastrohoroskop[.]com/timbreDigital/8f7b2f8304d08e, hxxps://auditoria88[.]mariageorgina[.]com/factura/3db4832ada4f80, hxxps://auditoria89[.]venagard[.]com/timbreDigital/f6a5f34123d980, hxxps://auditoria92[.]venagard[.]com/factura/2c6652a143f815, hxxps://auditoria93[.]serragrandreunion[.]com/timbreDigital/a2e79b61ac4635, hxxps://comprobante14[.]miramantolama[.]com/seg_factura/fb0b02b2d41b12, hxxps://comprobante2[.]marcialledo[.]com/factura/3ce069ac2b865e, hxxps://comprobante27[.]mariageorgina[.]com/timbreDigital/eada68119275aa, hxxps://comprobante27[.]serragrandreunion[.]com/facdigital/bca7513c9e00b9, hxxps://comprobante27[.]servicioslocomer[.]online/factura/2003b3fe7ae6f4, hxxps://comprobante45[.]altavista100[.]com/cfdi/d13011c95ba2b0, hxxps://comprobante51[.]meinastrohoroskop[.]com/facdigital/121c0388193ba5, hxxps://comprobante63[.]serragrandreunion[.]com/facdigital/3c45bca741d4f6, hxxps://comprobante68[.]portafoliocfdi[.]com/seg_factura/58c0146a753186, hxxps://comprobante70[.]miramantolama[.]com/timbreDigital/18665ae0a7b9e1, hxxps://comprobante75[.]meinastrohoroskop[.]com/timbreDigital/bfa30824f1120b, hxxps://comprobante80[.]serragrandreunion[.]com/timbreDigital/bf4a8735ed3953, hxxps://comprobante91[.]servicioslocomer[.]online/timbreDigital/adb6403b186182, hxxps://comprobante93[.]venagard[.]com/cfdi/57880f98ef2b70, hxxps://cumplimiento19[.]altavista100[.]com/timbreDigital/dd141e683a3056, hxxps://cumplimiento35[.]solucionegos[.]top/factura/bde64155cabbe5, hxxps://cumplimiento39[.]meinastrohoroskop[.]com/seg_factura/d4e9d7823adff2, hxxps://cumplimiento43[.]commerxion[.]buzz/facdigital/1ac5acb1a5525b,

TYPE	VALUE
URLs	hxxps://cumplimiento47[.]solucionegos[.]top/seg_factura/7fa6018dc9b68f, hxxps://cumplimiento48[.]callarlene[.]net/seg_factura/c19a0dd4addc3e, hxxps://cumplimiento56[.]timbradoelectronico[.]com/facdigital/dd37434dcde7ad, hxxps://cumplimiento72[.]serragrandreunion[.]com/seg_factura/92cd2425a6c150, hxxps://cumplimiento81[.]paulfenelon[.]com/cfdi/20149ee8e1d3b2, hxxps://cumplimiento91[.]miramantolama[.]com/seg_factura/e907d32bf0d056, hxxps://cumplimiento94[.]meinastrohoroskop[.]com/cfdi/bd56529f9d1411, hxxps://cumplimiento98[.]serragrandreunion[.]com/factura/3f209bc16cbb9a, hxxps://factura10[.]miramantolama[.]com/factura/039d9cbaeec9b5, hxxps://factura20[.]facturascorporativas[.]com/seg_factura/9622cf8c695873, hxxps://factura20[.]solunline[.]top/cfdi/6401eac16211b2, hxxps://factura34[.]changjiangys[.]net/facdigital/52490c838bd94f, hxxps://factura4[.]servicioslocomer[.]online/cfdi/f2369d09a54ad9, hxxps://factura40[.]miramantolama[.]com/cfdi/9318466130e6af, hxxps://factura44[.]servicioslocales[.]online/cfdi/25e8a6f5393e1f, hxxps://factura46[.]facturasfiel[.]com/factura/021bd5fa122bb2, hxxps://factura49[.]marcialledo[.]com/factura/fc2cc5bf671dd0, hxxps://factura50[.]callarlene[.]net/cfdi/867d138f26fb23, hxxps://factura59[.]altavista100[.]com/seg_factura/0179ae05a51830, hxxps://factura7[.]taoshome4sale[.]com/factura/eebf49f810a0a6, hxxps://factura71[.]servicioslomex[.]online/timbreDigital/5de7db415c7e8e, hxxps://factura72[.]serragrandreunion[.]com/seg_factura/728423dceff50c, hxxps://factura73[.]mariageorgina[.]com/cfdi/71deea8cdbcb10, hxxps://factura81[.]altavista100[.]com/factura/8421cd5cb1c8e4, hxxps://factura90[.]changjiangys[.]net/timbreDigital/029a6531330379, hxxps://factura91[.]servicioslocomer[.]online/timbreDigital/2952b54a9542f1, hxxps://folio24[.]serragrandreunion[.]com/seg_factura/548b685f48dd30, hxxps://folio24[.]spacefordailyrituals[.]com/facdigital/55ae12184283dc, hxxps://folio47[.]marcialledo[.]com/seg_factura/e6bab6d032e282, hxxps://folio53[.]mariageorgina[.]com/seg_factura/ca2fd939c046fa, hxxps://folio60[.]callarlene[.]net/seg_factura/367b377baf47e5, hxxps://folio75[.]taoshome4sale[.]com/cfdi/7482bf3f2690af, hxxps://folio75[.]venagard[.]com/cfdi/7718efe0fd3952,

TYPE	VALUE
URLs	hxxps://folio76[.]miramantolama[.]com/cfdi/a74b25b75c7182, hxxps://folio83[.]altavista100[.]com/factura/20f00b7d569c85, hxxps://folio89[.]changjiangys[.]net/factura/b645784e80f71a, hxxps://folio90[.]servicioslocomer[.]online/facdigital/d1950dc8f24757, hxxps://folio99[.]solunline[.]top/facdigital/b7928d4e0eade5, hxxps://pdf21[.]changjiangys[.]net/cfdi/2f99e7adf61c47, hxxps://pdf33[.]venagard[.]com/timbreDigital/91849e7d9fe4ad, hxxps://pdf34[.]solucionpiens[.]top/seg_factura/2dfed5bc7fcbf6, hxxps://pdf39[.]facturasonlinemx[.]com/seg_factura/66971f3669145a, hxxps://pdf49[.]marcialledo[.]com/factura/729c18972d690c, hxxps://pdf50[.]changjiangys[.]net/factura/cdb5ed3876c4bf, hxxps://pdf57[.]visual8298[.]top/factura/5239e15a8324ab, hxxps://pdf59[.]venagard[.]com/cfdi/5791bf23c6929e, hxxps://pdf63[.]paulfenelon[.]com/timbreDigital/3ae250718da0ca, hxxps://pdf65[.]verificatutramite[.]com/facdigital/e1ec8098e50a0b, hxxps://pdf70[.]mariageorgina[.]com/cfdi/fab1264f158f44, hxxps://pdf81[.]photographyride[.]com/seg_factura/4eb3832fe6d1bd, hxxps://pdf85[.]miramantolama[.]com/factura/74f871b7ca1977, hxxps://pdf93[.]venagard[.]com/factura/f24a53f8932b3f, hxxps://pdf98[.]solunline[.]top/timbreDigital/f57e558c31a86e, hxxps://portal27[.]marcialledo[.]com/timbreDigital/f8a5f05b3c1651, hxxps://portal34[.]solunline[.]top/cfdi/a068bb0da7eea1, hxxps://portal48[.]solucionpiens[.]top/timbreDigital/15ec5fc2aaf26a, hxxps://portal50[.]solucionegos[.]top/factura/8d4c6f7e2a4c7f, hxxps://portal55[.]solucionegos[.]top/seg_factura/f5f59070b20629, hxxps://portal63[.]paulfenelon[.]com/seg_factura/77907fa76c7c59, hxxps://portal70[.]solunline[.]top/timbreDigital/92b380d91a67a0, hxxps://portal80[.]changjiangys[.]net/cfdi/2224782a3b7f1d, hxxps://portal86[.]serragrandreunion[.]com/facdigital/68da4282591283, hxxps://portal90[.]meinastrohoroskop[.]com/factura/64f247c6238c38, hxxps://portal92[.]solucionpiens[.]top/timbreDigital/34893de446d532, hxxps://suscripcion0[.]venagard[.]com/timbreDigital/5c86c63ca1ffda, hxxps://suscripcion10[.]solunline[.]xyz/facdigital/ebe0cb51090e51, hxxps://suscripcion24[.]facturasonlinemx[.]com/factura/d6a6f8208ed508, hxxps://suscripcion24[.]venagard[.]com/timbreDigital/50c6f1fad17f5e, hxxps://suscripcion32[.]servicioslocomer[.]online/facdigital/22ccd8880c217e, hxxps://suscripcion38[.]eagleservice[.]buzz/cfdi/6dadfe1a18cffc, hxxps://suscripcion38[.]mariageorgina[.]com/factura/9c787623800b5e, hxxps://suscripcion57[.]changjiangys[.]net/factura/22ad73593f724a, hxxps://suscripcion65[.]g1ooseradas[.]buzz/factura/9f03d9ef3d73b5, hxxps://suscripcion84[.]taoshome4sale[.]com/cfdi/e4af3e6e22a8a6, hxxps://suscripcion95[.]servicioslomex[.]online/cfdi/0faa4a21fff2bb, hxxps://timbrado0[.]meinastrohoroskop[.]com/cfdi/515c9b9087c737, hxxps://timbrado11[.]verificatutramite[.]com/facdigital/f7640878ebc0f9,

TYPE	VALUE
URLs	hxxps://timbrado17[.]marcialledo[.]com/factura/2ea580ee99d5f1, hxxps://timbrado17[.]mariageorgina[.]com/seg_factura/95a6c2c0e004d8, hxxps://timbrado2[.]serviciosna[.]top/facdigital/c5cb33d68be323, hxxps://timbrado2[.]solucionegos[.]top/seg_factura/7c867709e85c67, hxxps://timbrado33[.]meinastrohoroskop[.]com/timbreDigital/aaf2cc575db42c, hxxps://timbrado42[.]mariageorgina[.]com/facdigital/f0f82ab0c87b32, hxxps://timbrado54[.]changjiangys[.]net/cfdi/04e4e38338d82a, hxxps://timbrado6[.]meinastrohoroskop[.]com/cfdi/5290b37e80850a, hxxps://timbrado73[.]mariageorgina[.]com/timbreDigital/ff862f9245e8b6, hxxps://timbrado74[.]callarlene[.]net/timbreDigital/eb52e334a2c0b3, hxxps://timbrado74[.]mexicofacturacion[.]com/factura/14fcb6e3eaf351, hxxps://timbrado80[.]paulfenelon[.]com/timbreDigital/684bc3f7d7e7f9, hxxps://timbrado84[.]miramantolama[.]com/cfdi/18864dcecc9e9c, hxxps://timbrado90[.]porcesososo[.]online/factura/cde31eb6fcac1d, hxxps://timbrado96[.]paulfenelon[.]com/facdigital/ef18828525a8fb, hxxps://validacion22[.]hb56[.]cc/seg_factura/8f845f6ba70820, hxxps://trilivok[.]com/2ysz0gghg/cbt0mer/it.php?f=2&w=Windows%2010, hxxps://trilivok[.]com/3s9p2w9yy/bvhcc5x/it.php?f=9&w=Windows%2010, hxxps://chidoriland[.]com/1r49ucc73/hs4q07q/it.php?f=2&w=Windows%2010, hxxps://manderlyx[.]com/cruto/it.php?f=2&w=Windows%2010, hxxps://bailandolambada[.]com/5iplivg7q/gn4md5c/it.php?f=2&w=Windows%2010
Domains	trilivok[.]com, chidoriland[.]com, manderlyx[.]com, bailandolambada[.]com, 0[.]solucionegos[.]top, auditoria38[.]meinastrohoroskop[.]com, auditoria42[.]altavista100[.]com, auditoria67[.]mariageorgina[.]com, auditoria7[.]miramantolama[.]com, auditoria82[.]taoshome4sale[.]com, auditoria84[.]meinastrohoroskop[.]com, auditoria88[.]mariageorgina[.]com, auditoria89[.]venagard[.]com, auditoria92[.]venagard[.]com, auditoria93[.]serragrandreunion[.]com, comprobante14[.]miramantolama[.]com, comprobante2[.]marcialledo[.]com, comprobante27[.]mariageorgina[.]com, comprobante27[.]serragrandreunion[.]com, comprobante27[.]servicioslocomer[.]online, comprobante45[.]altavista100[.]com,

TYPE	VALUE
Domains	comprobante51[.]meinastrohoroskop[.]com, comprobante63[.]serragrandreunion[.]com, comprobante68[.]portafoliocfdi[.]com, comprobante70[.]miramantolama[.]com, comprobante75[.]meinastrohoroskop[.]com, comprobante80[.]serragrandreunion[.]com, comprobante91[.]servicioslocomer[.]online, comprobante93[.]venagard[.]com, cumplimiento19[.]altavista100[.]com, cumplimiento35[.]solucionegos[.]top, cumplimiento39[.]meinastrohoroskop[.]com, cumplimiento43[.]commerxion[.]buzz, cumplimiento47[.]solucionegos[.]top, cumplimiento48[.]callarlene[.]net, cumplimiento56[.]timbradoelectronico[.]com, cumplimiento72[.]serragrandreunion[.]com, cumplimiento81[.]paulfenelon[.]com, cumplimiento91[.]miramantolama[.]com, cumplimiento94[.]meinastrohoroskop[.]com, cumplimiento98[.]serragrandreunion[.]com, factura10[.]miramantolama[.]com, factura20[.]facturascorporativas[.]com, factura20[.]solunline[.]top, factura34[.]changjiangys[.]net, factura4[.]servicioslocomer[.]online, factura40[.]miramantolama[.]com, factura44[.]servicioslocales[.]online, factura46[.]facturasfiel[.]com, factura49[.]marcialledo[.]com, factura50[.]callarlene[.]net, factura59[.]altavista100[.]com, factura7[.]taoshome4sale[.]com, factura71[.]servicioslomex[.]online, factura72[.]serragrandreunion[.]com, factura73[.]mariageorgina[.]com, factura81[.]altavista100[.]com, factura90[.]changjiangys[.]net, factura91[.]servicioslocomer[.]online, folio24[.]serragrandreunion[.]com, folio24[.]spacefordailyrituals[.]com, folio47[.]marcialledo[.]com, folio53[.]mariageorgina[.]com, folio60[.]callarlene[.]net, folio75[.]taoshome4sale[.]com, folio75[.]venagard[.]com, folio76[.]miramantolama[.]com,

TYPE	VALUE
Domains	folio83[.]altavista100[.]com, folio89[.]changjiangys[.]net, folio90[.]servicioslocomer[.]online, folio99[.]solunline[.]top, pdf21[.]changjiangys[.]net, pdf33[.]venagard[.]com, pdf34[.]solucionpiens[.]top, pdf39[.]facturasonlinemx[.]com, pdf43[.]marcialledo[.]com, pdf49[.]marcialledo[.]com, pdf50[.]changjiangys[.]net, pdf57[.]visual8298[.]top, pdf59[.]venagard[.]com, pdf63[.]paulfenelon[.]com, pdf65[.]verificatutramite[.]com, pdf70[.]mariageorgina[.]com, pdf81[.]photographyride[.]com, pdf85[.]miramantolama[.]com, pdf93[.]venagard[.]com, pdf98[.]solunline[.]top, portal27[.]marcialledo[.]com, portal34[.]solunline[.]top, portal48[.]solucionpiens[.]top, portal50[.]solucionegos[.]top, portal55[.]solucionegos[.]top, portal63[.]paulfenelon[.]com, portal70[.]solunline[.]top, portal80[.]changjiangys[.]net, portal86[.]serragrandreunion[.]com, portal90[.]meinastrohoroskop[.]com, portal92[.]solucionpiens[.]top, suscripcion0[.]venagard[.]com, suscripcion10[.]solunline[.]xyz, suscripcion24[.]facturasonlinemx[.]com, suscripcion24[.]venagard[.]com, suscripcion32[.]servicioslocomer[.]online, suscripcion38[.]eagleservice[.]buzz, suscripcion38[.]mariageorgina[.]com, suscripcion57[.]changjiangys[.]net, suscripcion65[.]g1ooseradas[.]buzz, suscripcion84[.]taoshome4sale[.]com, suscripcion95[.]servicioslomex[.]online, timbrado0[.]meinastrohoroskop[.]com, timbrado11[.]verificatutramite[.]com, timbrado16[.]taoshome4sale[.]com, timbrado17[.]marcialledo[.]com,

TYPE	VALUE
Domains	timbrado17[.]mariageorgina[.]com, timbrado2[.]serviciosna[.]top, timbrado2[.]solucionegos[.]top, timbrado33[.]meinastrohoroskop[.]com, timbrado42[.]mariageorgina[.]com, timbrado54[.]changjiangys[.]net, timbrado6[.]meinastrohoroskop[.]com, timbrado73[.]mariageorgina[.]com, timbrado74[.]callarlene[.]net, timbrado74[.]mexicofacturacion[.]com, timbrado80[.]paulfenelon[.]com, timbrado84[.]miramantolama[.]com, timbrado90[.]porcesososo[.]online, timbrado96[.]paulfenelon[.]com, validacion22[.]hb56[.]cc
SHA256	600d085638335542de1c06a012ec9d4c56ffe0373a5f61667158fc63894dde9f, 883674fa4c562f04685a2b733747e4070fe927e1db1443f9073f31dd0cb5e215, b1b85c821a7f3b5753becbbfa19d2e80e7dcbd5290d6d831fb07e91a21bdeaa7, e04cee863791c26a275e0c06620ea7403c736f8cafbdda3417f854ae5d81a49f, aa187a53e55396238e97638032424d68ba2402259f2b308c9911777712b526af, 66af21ef63234c092441ec33351df0f829f08a2f48151557eb7a084c6275b791, b3f4b207ee83b748f3ae83b90d1536f9c5321a84d9064dc9745683a93e5ec405, e87325f4347f66b21b19cfb21c51fbf99ead6b63e1796fcb57cd2260bd720929, 103d3e03ce4295737ef9b2b9dfef425d93238a09b1eb738ac0e05da0c6c50028, a579bd30e9ee7984489af95cffb2e8e6877873fd881aa18d7f5a2177d76f7bf2, b01e917dd14c780cb52cafcd14e4dd499c33822c7776d084d29cf5e0bb0bddb6, 795c0b82b37d339ea27014d73ad8f2d28c5066a7ceb6a2aa0d74188df9c311c9, 07521bd6acf725b8a33d1d91fd0cc7830d2cff66abdb24616c2076b63d3f36a8, 71ce48c89b22e99356c464c1541e2d7b9419a2c8fe8f6058914fc58703ba244f, ba7bc4cff098f49d39e16c224e001bd40a5d08048aeec531f771a54ee4a5ecef,

TYPE	VALUE
SHA256	010b48762a033f91b32e315ebcefb8423d2b20019516fa8f2f3d54d57d221bdb, 024f3c591d44499afb8f477865c557fc15164ab0f35594e0cfdfa76245459762, 03cd17df83a7bdf459f16677560e69143d1788ce1fc7927200a09f82859d90ea, 075910c802f755d3178a8f1f14ee4cd7924fd4463c7491277bdf2681b16e593c, 12bff33da7d9807252bb461d65828154b9b5b1dca505e8173893e3d410d40dd0, 1aaa4fb29a88c83495de80893cd2476484af561bb29e8cdfc73ce38f6cd61a84, 23b9e4103141d6a898773b1342269334e569bcf576cdcb4a905f24e26320cdab, 27c1e41fde9bc0d5027a48ccada1af8c9c8f59937bf5f77edd21e49bd28f29a2, 2a225784289f31adbaa8be0b8770495fa8950fce2b7352a0c7a566fc79067547, 2a38b75e88f91f9cd28ef478e82c3b44f50e57cb958ba63e58f134d8bd368812, 2a3f869e9e78b4d7945a60ceec27586c07bc8b0770be64463358fffe3b6b7395, 2e04c36b7ddd6939b7bef258bfeba6f91a5c37a43389dd6d9a88eff5863df5ed, 43e99539e4b966dde2f9de8dc1ffb4a22bc560e54c01de9aef6b15fac1412714, 46226d4fb7ffe15ba8167e3724f991c543731672e19ef40bb43fddc6df648d0a, 46cc07a9287da26e238a74734d87e0aae984f4648a80a26547afa0de8c850afb, 51be3a3b4ebd15c305c0f9b57388c449f88f0d6d2d46a0a838f046f0fd21b78f, 55b0247b9b574978a4c9abd19c3bcc04ea78598398b9f8aeb35bd51cbd877576, 56612bb0ab00cbb7af24326b027a55ff25852ddab1f1c8e24471b7ce97003505, 5831f4f8ce715d4a021284e68af1b6d8040a2543484ac84b326eea20c543552e, 58562e49c1612f08e56e7d7b3ca6cd78285948018b2998e45bd425b4c79ce1f4, 62495620b0d65d94bc3d68dec00ffbe607eacd20ab43dc4471170aa292cc9b1a, 682546addb38a938982f0f715b27b4ba5cda4621e63f872f19110d174851c4e9, 69019b7b64deb5cc91a58b6a3c5e6b1b6d6665bd40be1381a70690ba2b305790,

TYPE	VALUE
SHA256	6bf082f001f914824a6b33f9bdd56d562c081097692221fb887035e80926d583, 7923d409959acffab49dda63c7c9c15e1bdd2b5c16f7fcfe8ef3e3108e08df87, 7ac22989021082b9a377dcc582812693ce0733e973686b607e8fc2b52dcf181d, 8420d77ba61925b03a1ad6c900a528ecacbb2c816b3e6bc62def40fc14e03b78, 850dd47a0fb5e8b2b4358bf3aa1abd7ebaae577b6fc4b6b4e3d7533313c845b8, 96363b2b9e4ed8044cb90b6619842ba8897b4392f9025cbfdccfda1ea7a14a58, 97157c8bbeb8769770c4cb2201638d9ad0103ba2fdfed9bdbd03c53bd7a5fcb9, a103b0c604ef32e7aabb16c2a7917fd123c41486d8e0a4f43dcf6c48d76de425, a82fb82f3aa2f6123d2c0fb954ae558ac6e8862ef756b12136fbe8d533b30573, a92934c014a7859bd122717f4c87f6bd31896cb87d28c9fac1a6af57ff8110f6, ab2a2465fccd7294580c11492c29a943c54415e0c606f41e08ce86d69e254ee4, ababe815e11b762089180e5fb0b1eaffa6a035d630d7aaf1d8060bd5d9a87ea5, b04a0a4a1520c905007a5d370ed2b6c7cb42253f4722cc55a9e475ae9ece1de7, c29b9f79b0a34948bde1dfca3acecca6965795917c7d3444fcacba12f583fb98, c99237a5777a2e8fa7da33460a5b477d155cc26bc2e297a8563516a708323ead, ca652fc3a664a772dbf615abfe5df99d9c35f6a869043cf75736e6492fbd4bea, b5a272acd842154b2069b60aab52568bbfde60e59717190c71e787e336598912, 5efa99b3cb17bec76fec2724bcfcc6423d0231bba9cf9c1aed63005e4c3c2875, ce135a7e0410314126cacb2a2dba3d6d4c17d6ee672c57c097816d64eb427735, d3ff98b196717e66213ccf009cbeed32250da0e2c2748d44f4ee8fb4f704407c, 35b7dd775db142699228d3e64ee8e9a02c6d91bb49f7c2faf367df8ba2186fd6, e65e25aee5947747f471407a6cce9137695e4fee820f990883b117726195988c,

TYPE	VALUE
SHA256	e8ed09b016ea62058404c482edf988f14a87c790d5c9bd3d2e03885b818ef822, febf9c5ede3964fdb3b53307a3d5ef7b0e222705a3bb39bef58e28aaba5eed28, ff3769c95b8a5cdcba750fda5bbbb92ef79177e3de6dc1143186e893e68d45a4
IPs	24[.]199[.]98[.]128, 159[.]89[.]50[.]225, 104[.]131[.]169[.]252, 104[.]131[.]67[.]109, 137[.]184[.]108[.]25, 137[.]184[.]115[.]230, 138[.]197[.]34[.]162, 142[.]93[.]50[.]216, 143[.]244[.]144[.]166, 143[.]244[.]160[.]115, 146[.]190[.]208[.]30, 157[.]230[.]238[.]116, 157[.]245[.]8[.]79, 159[.]223[.]96[.]160, 159[.]89[.]226[.]127, 159[.]89[.]90[.]109, 162[.]243[.]171[.]207, 167[.]71[.]24[.]13, 167[.]71[.]245[.]175, 167[.]71[.]246[.]120, 192[.]241[.]141[.]137, 24[.]144[.]96[.]15, 45[.]55[.]65[.]159, 64[.]225[.]29[.]249

References

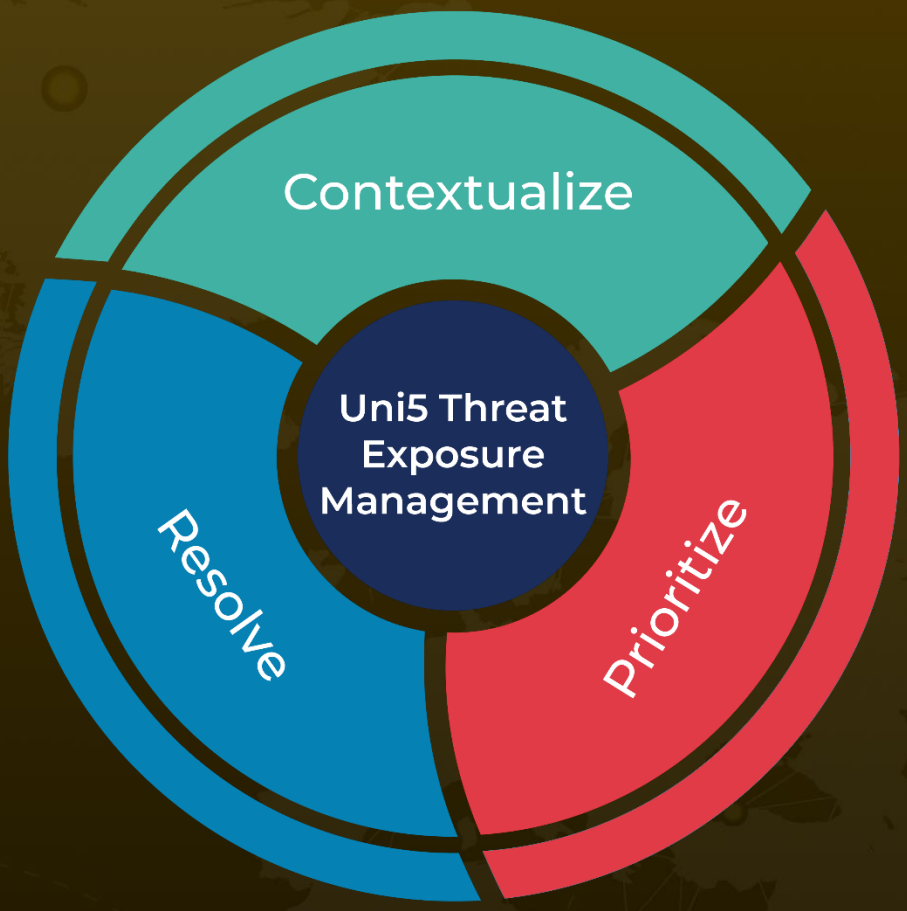
https://blog.talosintelligence.com/timbrestealer-campaign-targets-mexican-users/

https://www.hivepro.com/threat-advisory/mispadu-leverages-cve-2023-36025-vulnerability-in-latest-attack/

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 14, 2024 • 5:30 AM

More at www.hivepro.com