Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

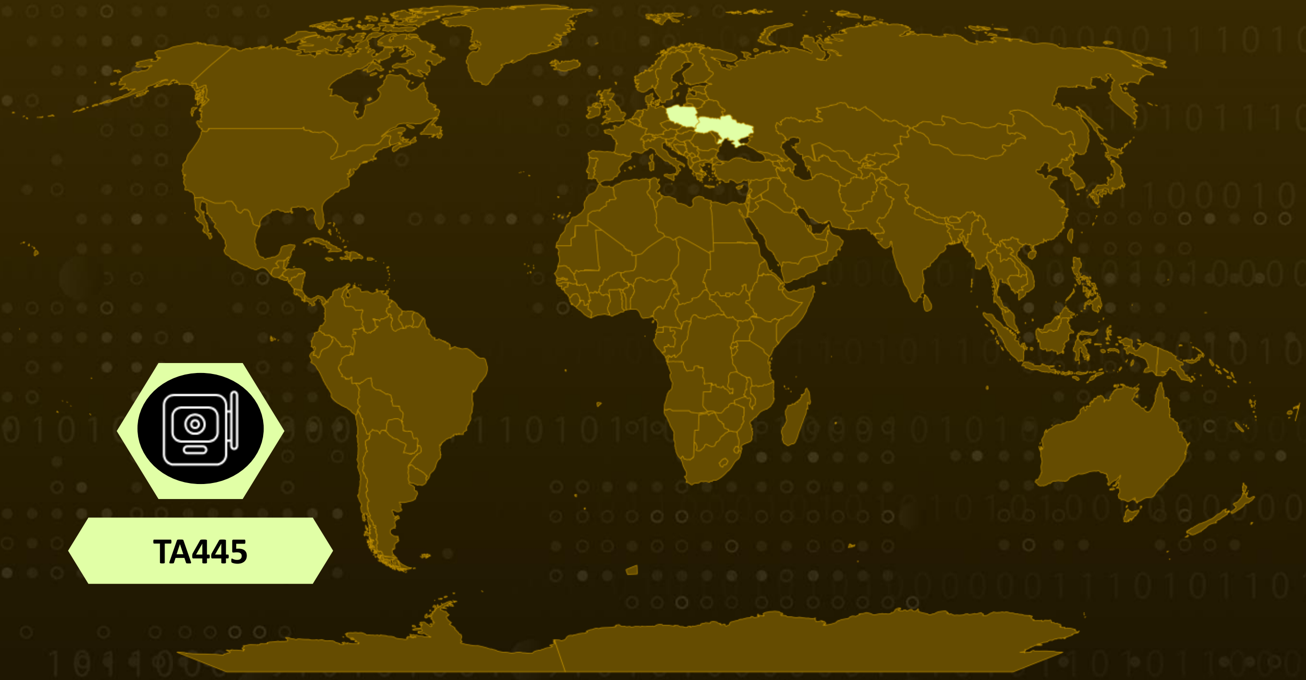
TA445 Targeting Government and Military Sectors in Ukraine and Poland

Date of Publication	Admiralty Code	TA Number
July 14, 2023	A1	TA2023299

Summary

First appeared: April 2022
Attack Region: Ukraine and Poland
Actor Name: TA445 (Operation Ghostwriter, UNC1151, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)
Affected Platform: Windows
Malware: PicassoLoader, AgentTesla, Cobalt Strike Beacon and njRAT
Targeted Industries: Government, Military, Business, Civilian
Attack: TA455 conducts ongoing campaigns targeting government entities, military organizations, and civilians in Ukraine and Poland to steal information and establish remote access, using multi-stage infection chains and payloads like AgentTesla RAT, Cobalt Strike, and njRAT.

Attack Regions



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

Attack Details

#1

A series of cyber-attacks targeting government entities, military organizations, and civilians in Ukraine and Poland. The threat actor, known as TA445 and allegedly linked to the Belarusian government, aims to steal information and gain remote access to systems.

#2

The campaigns, which have been ongoing since April 2022, utilize malicious Microsoft Office documents, particularly Excel and PowerPoint files, as the initial infection vector. The attacks involve multistage infection chains, including an executable downloader named PicassoLoader and payloads such as the AgentTesla remote access trojan (RAT), Cobalt Strike beacons, and njRAT.

#3

The actor primarily targets Ukrainian and Polish government and military organizations, employing socially engineered lures that mimic official documents and instructions to enable macros. The campaigns also encompass attacks on Ukrainian and Polish businesses and general users.

#4

The VBA code in the files is obfuscated, and the infection chain involves the creation of DLLs and shortcut files, as well as the use of image files to conceal the payloads. The downloader decrypts and loads the next-stage payload using AES encryption or simplified RC4 decryption techniques. The final payloads, including AgentTesla and Cobalt Strike, are used for information theft and remote control.

Recommendations

To prevent PicassoLoader malware, Utilize a robust endpoint protection solution enabling real-time protection against known and unknown threats.

Apply strong access controls, including multi-factor authentication and privileged access management, and implement continuous monitoring to detect and respond to suspicious activities promptly, reducing the potential impact of PicassoLoader or similar threats.

Regularly train employees on security best practices, emphasizing the risks of phishing attacks and malicious downloads, to minimize the likelihood of falling victim to attacks by the TA445 Group or other threat actors.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0003 Persistence	**T1574** Hijack Execution Flow	**T1140** Deobfuscate/Decode Files or Information	**T1574.001** DLL Search Order Hijacking
T1566 Phishing	**T1204** User Execution	**T1204.002** Malicious File	**T1059.005** Visual Basic
T1059 Command and Scripting Interpreter	**T1564** Hide Artifacts	**T1036** Masquerading	**T1027** Obfuscated Files or Information
T1218.010 Regsvr32	**T1218** System Binary Proxy Execution	**T1218.011** Rundll32	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d, 6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a, a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6, 1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac, 0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72, ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114, 5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e, a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363, 7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c, 27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3, c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558, aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e, 7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211, 0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4, 41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb, 1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af, e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945, 6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c, dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751, 40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df, d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9,

TYPE	VALUE
SHA256	f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0, 71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944, 00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e, a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9, 4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829, 4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65, 4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b, df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89, bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55, 00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87, 991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58, 2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104, 44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e, 30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa, 924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b, ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a, bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198, ea5a8f1052e40cb6bcebf384fe67a6920b3651fbd8f3a34a844f39789ebc4d5f, ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6, 3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9, 5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106, a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7,

TYPE	VALUE
SHA256	c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8, 0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32, 35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9, 5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14, c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990, e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411, 73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a, 7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
Hostname	everything-everywhere.at.ply[.]gg
IPV4	94.131.108[.]109
URLs	hxxps[://]wuzhenfestival[.]site/5109c46d40f801a862c96e628f83faca[.]png, hxxps[://]onyangdol[.]site/thumb_d_F3D14F4982A256B5CDAE9BD579429AE7[.]jpg, hxxps[://]kebhana[.]site/Believe-Me-Lyrics[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]ellechina[.]online/01_logo_HLW-300x168[.]jpg, hxxps[://]sellmyhousequickly[.]website/dangjiansigeyishibiaoyuxuanchuanguahua[.]jpg, hxxps[://]frivol[.]space/memnet-profiles/A10818[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]simplifymedia[.]pw/images/bnd/news/23908t5[.]png, hxxps[://]hssenglish[.]pw/fonini/pundit/leaf_background[.]jpg, hxxps[://]mingxing[.]pw/content/_processed_/f/a/_742fa0bbd1[.]jpg, hxxps[://]mingxing[.]pw/datastream/thumb_b/43950sec[.]jpg, hxxps[://]carpetmarker[.]pw/images/Carpet_Shop_3b09adf[.]jpg, hxxps[://]bourns[.]space/p/covers/assets/images/lee-leopard[.]jpg

References

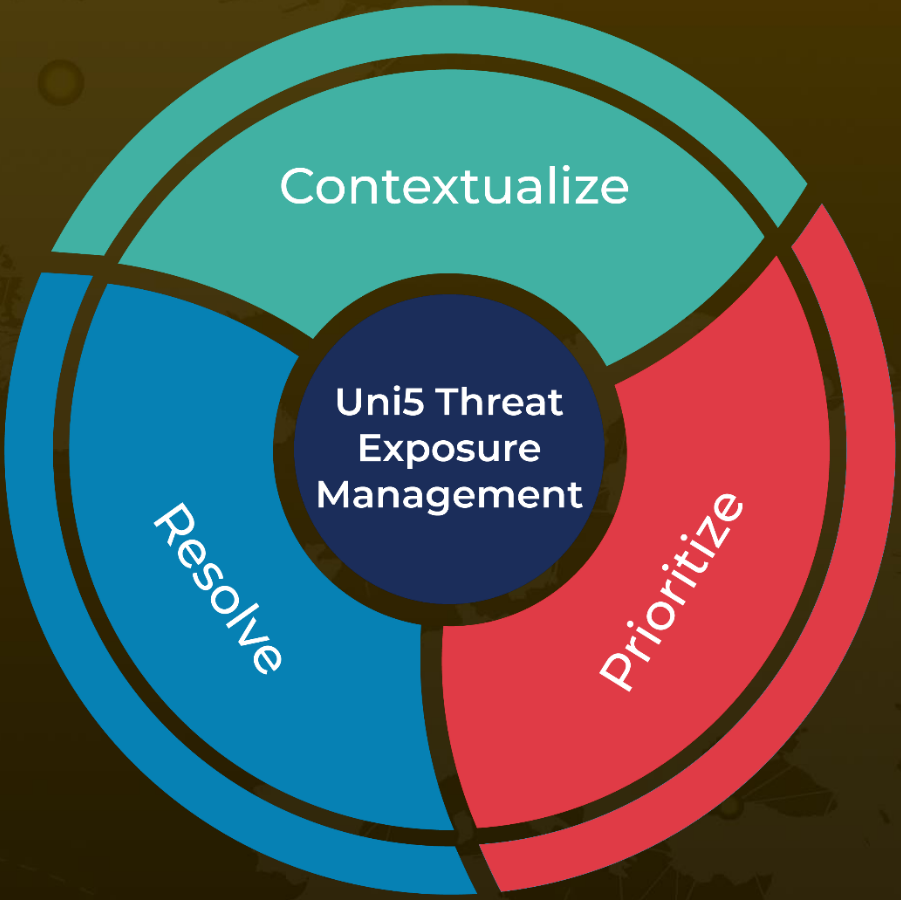
https://blog.talosintelligence.com/malicious-campaigns-target-entities-in-ukraine-poland/

https://raw.githubusercontent.com/Cisco-Talos/IOCs/main/2023/07/malicious-campaigns-target-entities-in-ukraine-poland.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

July 14, 2023 • 6:10 AM

More at www.hivepro.com