Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

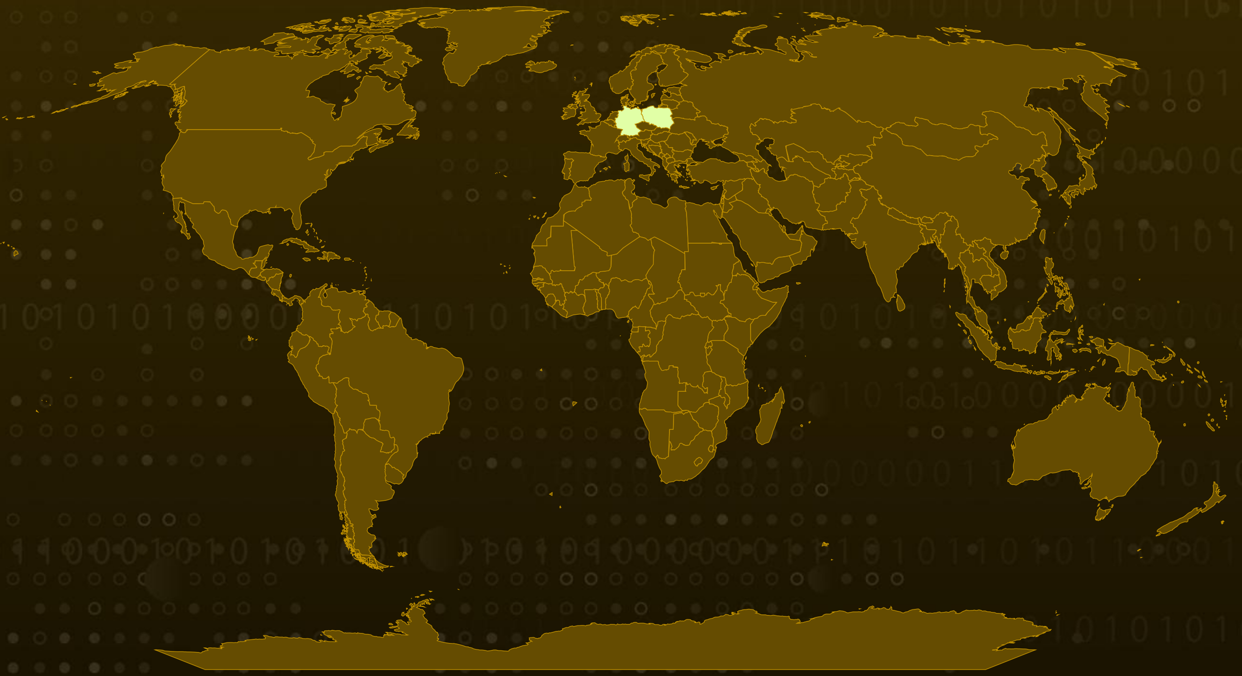
TorNet Backdoor: Stealthy Phishing Campaign Hits Poland and Germany

Date of Publication	Admiralty Code	TA Number
January 29, 2025	A1	TA2025024

Summary

Attack Discovered: July 2024
Targeted Countries: Poland and Germany
Malware: TorNet, PureCrypter
Attack: A financially motivated threat actor has been orchestrating a persistent phishing campaign since at least July 2024, primarily targeting users in Poland and Germany. The attacker employs various payloads, including a previously undocumented backdoor dubbed TorNet, which is deployed via the PureCrypter malware. Once executed, TorNet stealthily connects the victim's machine to the TOR network, enabling covert command-and-control (C2) communications while evading detection.

Attack Regions



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

Attack Details

#1 A financially motivated threat actor has been running a phishing campaign since at least July 2024. The attackers use phishing emails tricking victims into opening malicious attachments. These emails deliver various malware strains, including Agent Tesla, Snake Keylogger, and a newly discovered TorNet backdoor, which is installed using **PureCrypter** malware.

#2 The attack begins when a victim receives a phishing email impersonating a financial institution or manufacturing company. The email contains fake money transfer details or purchase invoices, primarily written in Polish and German, with some versions in English. The attachments use a ".tgz" extension, likely to bypass security scans by masquerading as compressed files.

#3 Once a victim unzips and opens the attachment, a .NET loader executes, downloading PureCrypter malware from a compromised server. This malware runs in system memory, making it harder to detect by security tools. It then installs TorNet, a backdoor that connects the infected machine to a hidden command-and-control (C2) server via the TOR network, allowing attackers to issue remote commands and maintain persistence.

#4 The .NET loader plays a critical role in deploying PureCrypter. It can either download additional malware or execute an encrypted malicious file embedded within itself. Once activated, PureCrypter takes multiple steps to evade detection and maintain access. It modifies Windows Defender settings to prevent security scans, detects if it is running in a security sandbox, and establishes persistence by adding itself to Windows startup settings and scheduled tasks. Additionally, it drops a Visual Basic script in the startup folder, ensuring the malware reloads even after a reboot.

#5 After securing its foothold, PureCrypter installs TorNet, which establishes a covert communication channel between the victim's machine and the attacker's C2 server via the TOR network. TorNet is a stealthy .NET-based backdoor that enables attackers to remotely control infected machines. Once it executes, it extracts a hidden C2 server address, connects using ports and performs anti-analysis checks to avoid detection. It then encrypts all communications with the attacker's infrastructure and can execute additional malware or commands as instructed.

#6 One of TorNet's most dangerous capabilities is its ability to download and install the TOR Expert Bundle, allowing it to route all communication through the TOR network. This provides the attackers with complete anonymity, making it extremely difficult to track or block their operations.

Recommendations

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.

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.

Network Segmentation and Traffic Monitoring: Limit outbound connections to the TOR network unless explicitly required for business operations. Implement strict firewall rules to block unauthorized TOR traffic and prevent malware from establishing stealthy communication channels. Additionally, continuously monitor network activity for unusual patterns, particularly connections to known TOR entry nodes and suspicious IP addresses, which may indicate potential compromise or malicious activity.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block PureCrypter malware and its associated loaders. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity, such as reflective DLL loading and process injection.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1566.001 Spearphishing Attachment	T1614 System Location Discovery	T1614.001 System Language Discovery
T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1656 Impersonation	T1560 Archive Collected Data

T1204 User Execution	T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1027 Obfuscated Files or Information
T1497 Virtualization/Sandbox Evasion	T1047 Windows Management Instrumentation	T1057 Process Discovery	T1589 Gather Victim Identity Information
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.005 Visual Basic	T1140 Deobfuscate/Decode Files or Information
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1036 Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	3b4e709768d7cd0cb895de74267f45a6ef6565ebed445393878f17ae02a983e3, 9d33726fc1d39fdc0426c70ed0cfb515e15f50d39c46d8ff38025b4faf8811dc, 75d2d368d735fca2bad0155510cb4a927f7f246ea72299395990027264056521, 84570dac910557d0d8217db746c9a8fd4a27cd3db89135731c7f3584b37df533, 7ce9af599857827317a444c5a63a08929ec97765bc2624076f4834f323a41da2, e9ab4772ba6de2db9add3d4bbd3ce0f2dd899f16399b57fd2a539769e6ee973a, 2f9c2e0bef460a7623954d65f10e6e5993c01d25e6f2905a5dc911639ca2ea75, dc513e35a6d96933e7af2b300782a32131d31445a6d1e2bbca9604128c92e7c6, 57543fd3673c9595a73c836b153faf68e23938662c5a4b6675205734b688ae95, 898d0451bd52c466d2284091be928f8ec1ced2184b205d903a04a747e67763ea, 53e7b3b72695a1eaea7146ec3cbd05d0ce2a1eba87f035ae07849feb4f59ec63 bff0ec65af8b2bb37fcc5202f823b5877ebdcc8efbd32e08f309cbcb4dc2570c, 6774a822d9c66951be95341d50c1f876a9373fefef52f68f29eaae4efc621817, c32d97fb9a1681a7bea3f417abde0264a2332221e317c8543e337baac9307c67,

TYPE	VALUE
SHA256	075737b17ba72aed5f45d227bf91dd5744914308e1468717a8f3100a0cca8156, a85423a1a37f604e492ee58920178080f0da306750a356ddfe1b695c12becd07, 4a5b8442dc2b34a270acdcd8a14cce573d59dc0922c9e49cda8fe2dd8e4a3862, 80b80e15f605f0b8740e1989e505280394d746e8a8ee37cdb9b009d745e42da0, 4280eb4cfa0445a40d8e1dfafdc0eb24613f3536c5959270ef0079034b30e653, 2f1cb29e47c5b07fba3070d6a5339b00d2f3075eb7717438cf5cf53679793919, 252d9ed583bbd2e5d75ae5167feb393bd50b44933594f9586aaf5d9987cf78ec, edac6216665f1c8b0a09158abdd5e7fab63a386a1c9ad31ddd5ee92a6aa811fc, 13ac538c8c6696a59f890677cf451db77b7c33539da1d380640ce549b2b70ca4
Domains	italzformendinggallores[.]duckdns[.]org, humblecrazeforeal8897[.]accesscam[.]org, sertiscoppersail432[.]freeddns[.]org, moristaetdfertal9002[.]ddnsgeek[.]com, paradoncalleke5689[.]camdvr[.]org, greeslieforreallcul5672[.]casacam[.]net, blissfulzerooooos690[.]ddnsfree[.]com, www[.]blissfulzerooooos690[.]ddnsfree[.]com
URLs	hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Sjydgbr[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Guwasd[.]dat, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Fwudzwsfsp[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Dyvfi[.]dat, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Iicivjzqdma[.]mp3, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Dewsmwflw[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Xlkythleoq[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Zerwfilj[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Sfrnotlay[.]mp3, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Jovjvwp[.]wav,

TYPE	VALUE
URLs	hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Vmoeykn[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Wyvmy[.]wav, hxxp[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Zafvlztxj[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Gikwomjv[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Zafvlztxj[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Qecvodcnuz[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Hlynogyqp[.]dat, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Uvkoiguq[.]dat, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Awtvbihi[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Oqjhea[.]mp3, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Ztpcwfowiiu[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Bonhowau[.]mp4, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Qcqvzdtpln[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Jlhwfgnnyms[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Otmaq[.]mp4, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Elxrh[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Rxmjavdc[.]mp3, hxxp[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Elxrh[.]vdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Cfyenm[.]mp4, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Bibyep[.]mp4, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Lcrakntjck[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Atcbgl[.]mp4, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Rspfqdltykq[.]mp3,

TYPE	VALUE
URLs	hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Fxsovxc[.]pdf, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Bnvqyotgu[.]mp3, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Rmtafnw[.]mp3, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Lmshcchh[.]wav, hxxps[://]sanel[.]net[.]pl/filescontentgalleries/pictorialcoversoffiles/Ibesc[.]wav, hxxps[://]cud-senegal[.]org/post-postlogin/Oojhwcym[.]wav, hxxps[://]cud-senegal[.]org/post-postlogin/Cpoewtupeck[.]mp4, hxxps[://]cud-senegal[.]org/post-postlogin/Nrileknnlgv[.]vdf, hxxps[://]cud-senegal[.]org/post-postlogin/Izevzxvwkpf[.]pdf

References

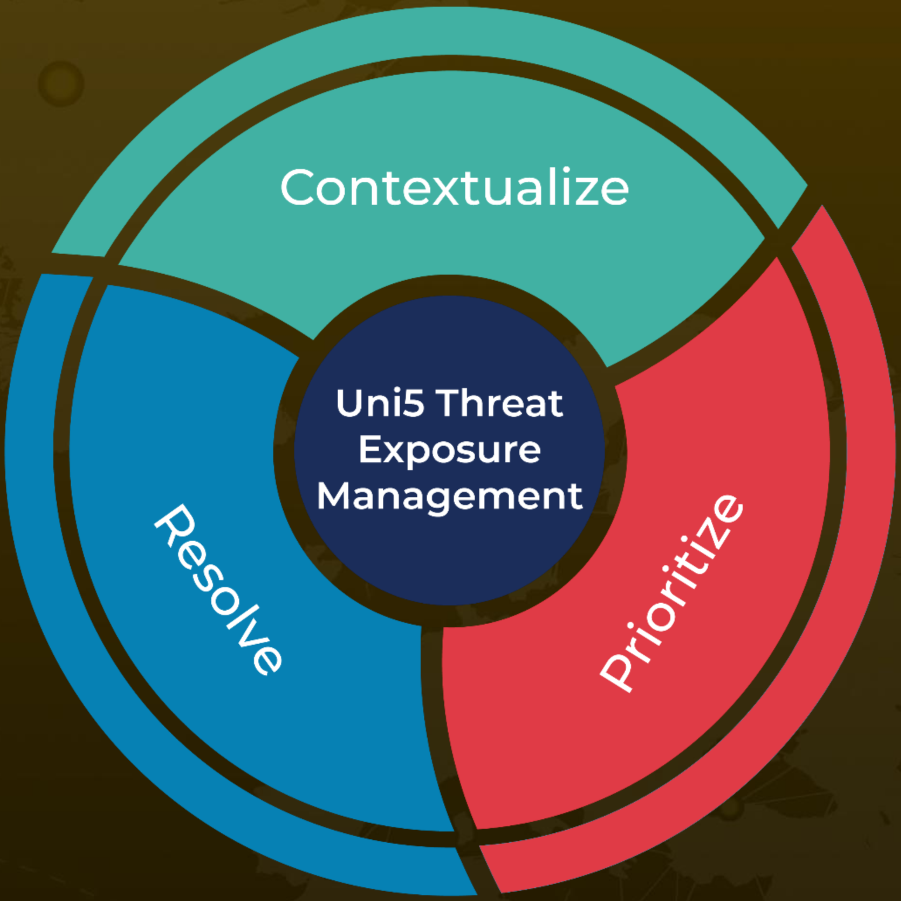
https://blog.talosintelligence.com/new-tornet-backdoor-campaign/

https://hivepro.com/threat-advisory/8220-gangs-heist-exploiting-oracle-weblogic-for-cryptomining/

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

January 29, 2025 • 3:40 AM

More at www.hivepro.com