Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

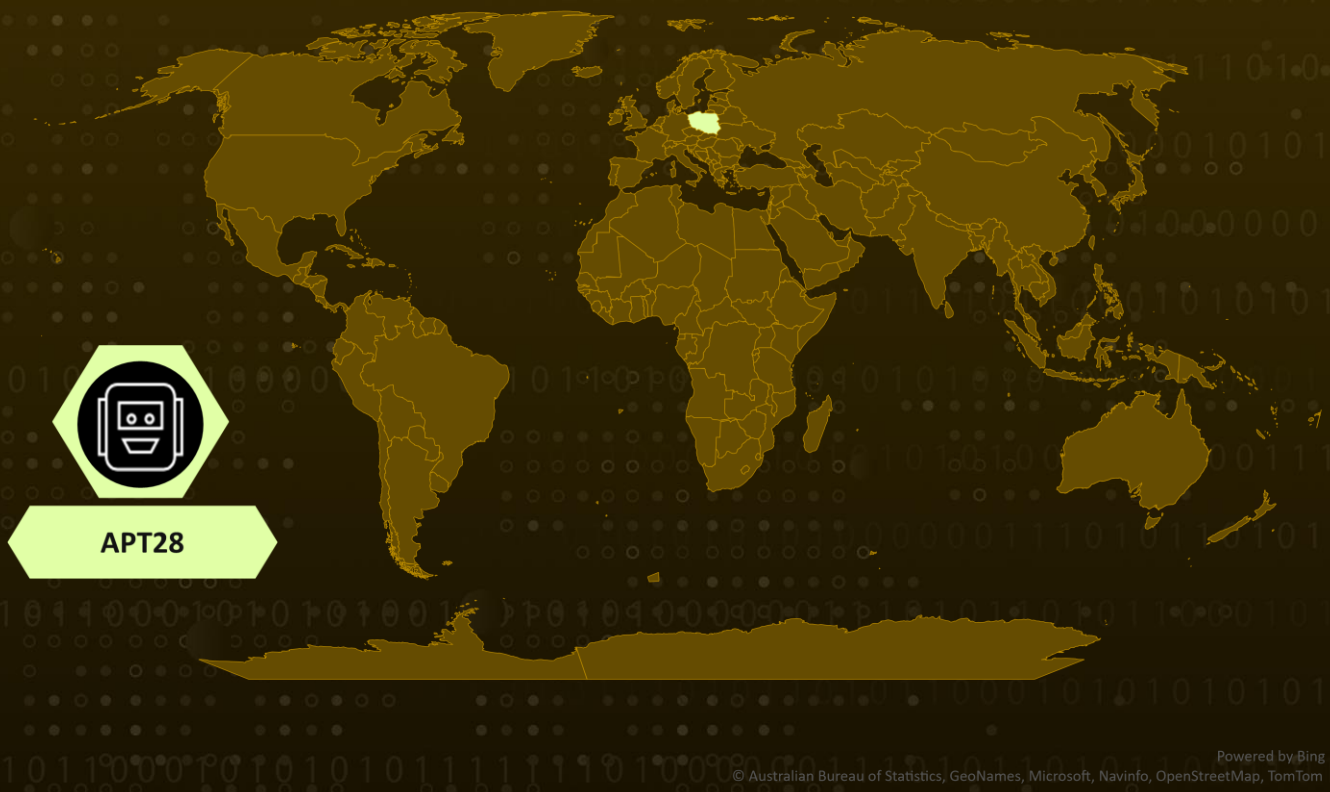
APT28's Intricate Email Campaign Against Poland

Date of Publication	Admiralty Code	TA Number
May 9, 2024	A1	TA2024180

Summary

Threat Actor: APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)
Targeted Industries: Government, Defense, Critical Infrastructure
Attack Region: Poland
Attack: The APT28 group, linked to the GRU, orchestrated a sophisticated email campaign targeting Polish government institutions.

Attack Regions



Attack Details

#1 A nefarious email campaign orchestrated by the APT28 group targeted Polish government institutions. The APT28 threat group associated with the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) employed deceptive tactics.

#2 The campaign utilized carefully crafted emails designed to intrigue recipients and encourage them to click on embedded links. These links directed users to a domain acting as a simple redirection point to another website, where a ZIP archive was available for download.

#3 Concealed within this archive were three files. Upon execution, a BAT script launched the Microsoft Edge browser, loading base64-encoded page content to facilitate the download of another batch script. This subsequent script then proceeded to collect information about the victim's computer before transmitting it to the designated C2 server.

Recommendations

- **Enhance Email Security Measures:** Given the sophisticated nature of APT28's email campaign, it's imperative to bolster email security protocols within Polish government institutions. Implement advanced email filtering and authentication systems to detect and block malicious emails effectively.
- **Implement Application Whitelisting:** Use application whitelisting to control the execution of unauthorized applications, thereby preventing the deployment of malicious payloads.
- **Continuous Monitoring and Analysis:** Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.
- **Enhance Firewall Restrictions:** Strengthen the firewall by adding a denylist that includes resources and IP addresses linked to cloud services used for traffic tunneling. This proactive step aids in blocking potential entry points exploited by threat actors such as APT28.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1204** User Execution	**T1033** System Owner/User Discovery
T1041 Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1082** System Information Discovery
T1204.002 Malicious File	**T1029** Scheduled Transfer	**T1007** System Service Discovery	**T1598.003** Spearphishing Link
T1562.004 Disable or Modify System Firewall	**T1564.001** Hidden Files and Directories	**T1053** Scheduled Task/Job	**T1055** Process Injection

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=2d07e34c-3dd3-45e8-865c-3888a65ab885, hxxps[:]//webhook[.]site/2d07e34c-3dd3-45e8-865c-3888a65ab885, hxxps[:]//webhook[.]site/4ba464d9-0675-4a7a-9966-8f84e93290ba, hxxps[:]//webhook[.]site/577b82c3-7249-44e9-9353-5eab106fead6, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=127df518-52be-46c5-bbb2-0479f4b9693b, hxxps[:]//webhook[.]site/127df518-52be-46c5-bbb2-0479f4b9693b, hxxps[:]//webhook[.]site/0ef0dcf7-f258-4d02-b274-cbf62a2000cf, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=c1112bb3-0e6e-4ba4-abe7-fb31388b47ad,

TYPE	VALUE
URLs	hxxps[:]//webhook[.]site/c1112bb3-0e6e-4ba4-abe7-fb31388b47ad, hxxps[:]//webhook[.]site/3f396db1-2016-4b69-9ec3-ffc417d5f3aa, hxxps[:]//webhook[.]site/66ea3bbc-29dc-4ece-b804-71c6ec7b77b6, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=efb79108-a2b5-4cba-844d-6352bb8fad8c, hxxps[:]//webhook[.]site/efb79108-a2b5-4cba-844d-6352bb8fad8c, hxxps[:]//webhook[.]site/9c87649c-220d-425d-8331-ffc8d9b94a38, hxxps[:]//webhook[.]site/c618ea32-2923-4c12-8151-8d0002b56af0, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=f97bcee0-0d91-4503-a30c-027f1b34820f, hxxps[:]//webhook[.]site/f97bcee0-0d91-4503-a30c-027f1b34820f, hxxps[:]//webhook[.]site/9a9cdaf8-120c-4de9-b17a-d6d8e2796a3b, hxxps[:]//webhook[.]site/e13d23aa-b6f8-4491-9adc-71f7f8c438df, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5e4c7949-30a2-4477-9e9b-e8828fc76a1b, hxxps[:]//webhook[.]site/5e4c7949-30a2-4477-9e9b-e8828fc76a1b, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5100fcc0-f6be-4b09-8c58-5a8a6706ec4f, hxxps[:]//webhook[.]site/5100fcc0-f6be-4b09-8c58-5a8a6706ec4f, hxxps[:]//webhook[.]site/7674f06b-e435-4470-a594-6d59578c552d, hxxps[:]//webhook[.]site/dee016bf-21a2-45dd-86b4-6099747794c4, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=508da0df-7ec9-420e-b1fe-958fbbe699d1, hxxps[:]//webhook[.]site/508da0df-7ec9-420e-b1fe-958fbbe699d1, hxxps[:]//webhook[.]site/bec23763-b8d9-4191-99ba-04a4a163b4de, hxxps[:]//webhook[.]site/90fea98f-fbdb-4847-be03-409d02a43caf, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=bc349b93-b047-42f8-a421-d45e3ec94dc5, hxxps[:]//webhook[.]site/bc349b93-b047-42f8-a421-d45e3ec94dc5, hxxps[:]//webhook[.]site/5a8758c6-5702-4fea-9d5e-4fbdb6dd795f, hxxps[:]//webhook[.]site/b10bd697-1a9f-4ec7-aa2f-1fa84ad916a1, hxxps[:]//run[.]mocky[.]io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=1658772a-4de8-4368-a604-980c90b0a1ed, hxxps[:]//webhook[.]site/1658772a-4de8-4368-a604-980c90b0a1ed, hxxps[:]//webhook[.]site/4fe5885c-f2f6-4905-8bc7-aef1a046a134, hxxps[:]//webhook[.]site/0d2dc90e-2d5e-49f8-8249-d7ab955c387a
SHA256	2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d, 52b8bfbd9ef8ecfd54e71c74a7131cb7b3cc61ea01bc6ce17cbe7aef14acc948, 4001498463dc8f8010ef1cc803b67ac434ff26d67d132933a187697aa2e88ef1, 158d49cce44968ddd028b1ef5ebc2a5183a31f05707f9dc699f0c47741be84db, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364,

TYPE	VALUE
SHA256	7c6689f591ce2ccd6713df62d5135820f94bdbf2e035ab70e6b3c6746865a898, c968f9dd1f16a435901d2b93a028a0ae2508e943c8f480935a529826deb3dbeb, 34cabc0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b, e1069c8677d64226f7881e8504ed7a13f79f43f143842ea6c1c8b2cc680ed6c2, 43ff178e428373512b83f85db32f364fc19c9a4ac7317835bd5089915b8727b5, ca700d44db08ad2ebd52278a3b303f8c13e44847a507fb317ea5dfb6cc924a76, bab7e81395e1e9ee1680c3bb702c44b1b13ee5e67fa893d765284ae168de8369, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 38ae06833528db02cb3a315d96ad2a664b732b5620675028a8c5e059e820514f, ee433ddd5988ab7325b92378c6d3cb736ddb7f1bad75b939e8c931f417660129, 9ddf5561562a62961a6fcac1dc49633cb79f5d3c8cc9b95fd9f87e7be70d2d35, dfd1f3229f903887f2474f361a26273dc63a6221883e86c5eea2dec9521dc081, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e, 642315d3091a3dfba6c0ed06f119fc40d21f3d84574b53e045baf8910e1fb38c, fb42a4e0f2dd293fd6e7acb8d67d67698a0ae7685bc5462685acf4c2f73d0b44, 07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 5d2675572e092ba9aece8c8d0b9404b3adbd27db1312cd659ba561b86301fe73, f348a0349fdec136c3ac9eaee9b8761da6bd33df82056e4dd792192731675b00, 351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f, 85f10d3df079b4db3a83ae3c4620c58a8362df2be449f8ce830d087ab41c7a52,

TYPE	VALUE
SHA256	939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587, 598a8b918d0d2908a756475aee1e9ffaa57b110d8519014a075668b8b1182990, ef67f20ff9184cab46408b27eaf12a5941c9f130be49f1c6ac421b546dac2bac, 96766dfbf6c661ee3e9f750696803824a04e58402c66f208835a7acebfab1cfc, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3, ae4e94c5027998f4ce17343e50b935f448e099a89266f9564bd53a069da2ca9a, d714fff643d53fdd56cf9dcb3bd265e1920c4b5f34a4668b584a0619703d8a3e, b3e60909036c4110eb7e3d8c0b1db5be5c164fcc32056885e4f1afe561341afd, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364, 5883842c87ca6b59236257e15db983cc88d4948cf0d649455f8f393899673fcc, 0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983, e826dc4f5c16a1802517881f32f26061a4cbc508c3f7944540a209217078aa11, 750948489ed5b92750dc254c47b02eb595c6ffcefded6f9d14c3482a96a6e793, 939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364
File Name	IMG-1030873974629655576.zip, WindowsCodecs.dll, bcpcn.bat, IMG-1030873974629655576.jpg, kpqsklcrdsonoknaote.css, IMG-7214532.zip, WindowsCodecs.dll, zdesdyf.bat, IMG-238279780.zip, WindowsCodecs.dll, hjpxswjdkayzwfphx.bat, IMG-238279780.jpg,

TYPE	VALUE
File Name	vngradn.css, IMG-810629002957075004.zip, WindowsCodecs.dll, yvrlqpkgngppjp.bat, IMG-810629002957075004.jpg, ovhupm.css, IMG-368912.zip, WindowsCodecs.dll, udkozfnsljmbpjs.bat, IMG-368912.jpg, wrkybdizscvb.css, IMG-451458326.zip, WindowsCodecs.dll, illgvjrfyevoqxk.bat, IMG-451458326.jpg, mzmtfylpywlyurkcd.css, IMG-0601181.zip, WindowsCodecs.dll, hzjtajjklr.bat, IMG-0601181.jpg, daukbpnawvkfcjcfzu.css, IMG-89848928.zip, WindowsCodecs.dll, jxfgibtfxiewsdvmeg.bat, IMG-89848928.jpg, cvywrkrhhfzza.css, IMG-3907894910429.zip, WindowsCodecs.dll, bmpxjphdzwommblflx.bat, IMG-3907894910429.jpg, qseybqanfkus.css

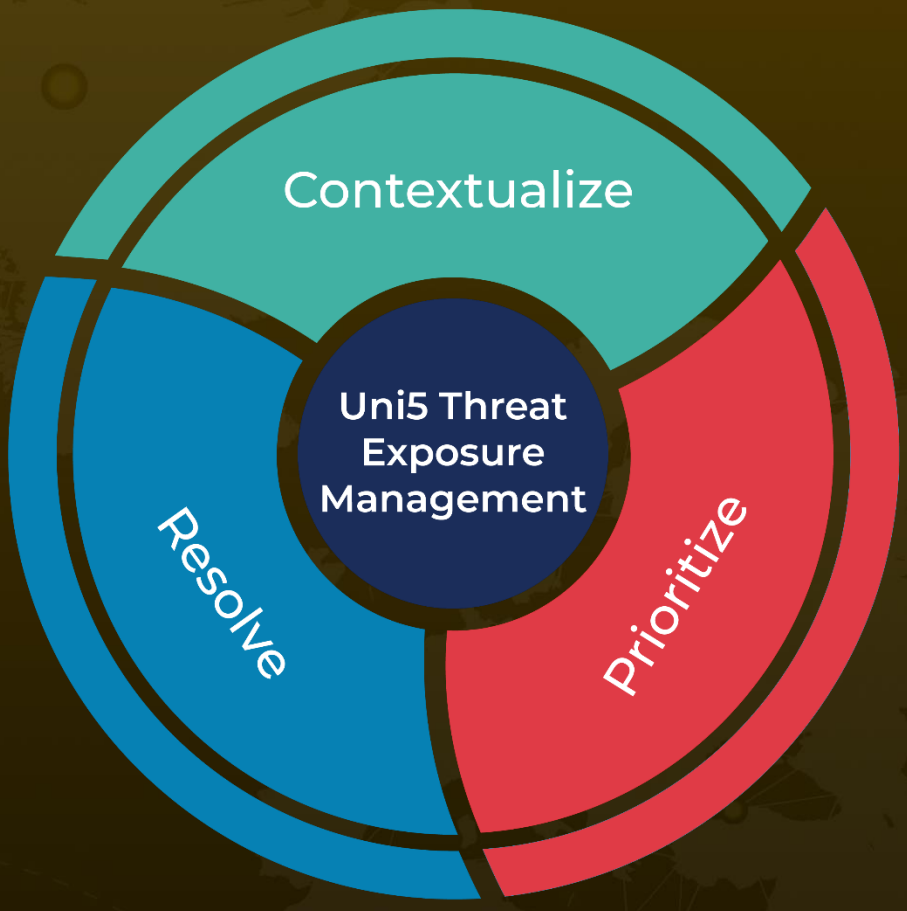
References

https://cert.pl/posts/2024/05/apt28-kampania/

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

May 9, 2024 • 6:00 AM

More at www.hivepro.com