Block Sandworm Team Cyber Attack IOCs

Date: 21st April 2024 | Severity: High

Summary

The Sandworm Team (AKA Quedagh, VOODOO BEAR) is a group of Russian hackers that has initiated major cyber campaigns against foreign government leaders and institutions, primarily in Ukraine.

Attack Vectors

- In April 2024, cybersecurity researchers reported a novel backdoor, Kapeka, that has been used by Sandworm in attacks against entities in Eastern Europe since at least mid-2022.
- The new malware, first discovered in an attack against an Estonian logistics company, shares code similarities with two other malware, GreyEnergy and Prestige, that had been formerly linked to Sandworm. Kapeka is a Windows DLL, written in C++, that consists of a dropper component responsible for dropping, executing, and setting up persistence for the backdoor, before it removes itself from the disk.
- Once deployed, the malware collects information about the victim's machine and user through a set of WinAPI calls and registry queries, and then sends it to the attackers' C2 server.

Indicator of compromise

INDICATOR TYPE	INDICATORS
CVE ID	CVE-2014-4114
Domain	• ett.ddns.net • tgset.click • outlook.adfs.kyivstar.online • zpltcmgodhvvedxtfcygvbgjkvgvcguygytfigj.cc • cpcpipe.org • telegramweb.us • ufowdauczwpa4enmzj2yyf7m4cbsjcaxxoyeebc2wdgzwnhvwhjf7iid.onion.moe • darksea.ddns.net • ukroboronprom.com.ukr.pm • userarea.in • zdg.re

Url	• https://88.80.148.65/news/article • https://185.38.150.8/star/key • https://103.78.122.94/help/healthcheck • https://185.181.229.102/home/info • https://fex.net/s/bttyrz4 • https://fex.net/s/59znp5b
File Hash	• 97e0e161d673925e42cdf04763e7eaa53035338b • 9bbde40cab30916b42e59208fbcc09affef525c1 • d297281c2bf03ce2de2359f0ce68f16317bf0a86 • 587b6377a3e069c1f399cb480729bbc70665cdd25af95f859f4b0a767463b3d3 • 00af82a2676688bdefec49941b61b3df • 87f5d52c006400e17af08bd4f1cf3b5afd90f377caad723c2cc597f9f62478e6 • 1557e59985faab8ee3630641378d232541a8f6f9 • 50b990f6555055a265fde98324759dbc74619d6a7c49b9fd786775299bf77d26 • 8d379585e0a9db4c65450622ced26c108dc694ab • cc092f7b23c04b58adc94466bbd4408cfa440e473e7473fcd5324b21f25a797b • f9f3374d89baf1878854f1700c8d5a2e5cf40de36071d97c6b9ff6b55d837fca • b0df1c855db31dd29a1e9b40f8360e5036e848e023741e05114d46b7359ff6f6 • 0eec5a7373b28a991831d9be1e30976ceb057e5b701e732372524f1a50255c72 • a976d912122b80200c29b8a106f899ddf3103ceb76a403502b46c2507212f4bb • f080eec275f07aec6b7a617e215d034e67e011184e1de5b2e71e441a6dd8027f • 1b6b898c628279b9445515e3059e53577f3db46477351c316f646752f2f15177 • edbc90c217eebabb7a9b618163716f430098202e904ddc16ce9db994c6509310
IP	• 185.220.101.58 • 185.220.101.185 • 80.67.167.81 • 176.119.195.115 • 176.119.195.113 • 190.2.145.24 • 82.180.150.197 • 217.57.80.18 • 70.62.153.174 • 185.220.102.248 • 185.220.102.245 • 185.220.102.251 • 185.220.102.2507 • 107.182.129.219 • 96.80.68.193 • 151.0.169.250 • 24.199.247.222 • 103.150.187.121 • 195.230.23.19 • 80.78.24.14 • 78.134.89.167 • 212.202.147.10 • 85.206.161.94 • 77.91.123.136 • 45.154.98.225 • 103.27.202.12

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- To protect your organization from falling victim to attacks like the one involving the MadMxShell backdoor, implement a comprehensive, multi-layered security strategy.
- Establish and enforce strict download policies.
- Implement procedures for verifying the legitimacy of downloaded files.
- Implement execution policies to control application and script execution.
- Prevent the execution of unknown or malicious files.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.darkreading.com/ics-ot-security/-sandworm-group-is-russia-s-primary-cyber-attack-unit-in-ukraine
- https://www.cvedetails.com/cve/CVE-2014-4114/?q=CVE-2014-4114
- https://www.rapid7.com/blog/post/2014/10/14/sandworm/