Mphasis
The Next Applied

Kremlin-Backed APT28 Targets Polish Institutions in Large-Scale Malware Campaign

Date: 12th May 2024 | Severity: Medium

Summary

The campaign sent emails with content intended to arouse the recipient's interest and persuade him to click on the link," the computer emergency response team, CERT Polska, said in a Wednesday bulletin.

The malicious DLL file is side-loaded by means of a technique called DLL side-loading to ultimately run the batch script, while images of an "actual woman in a swimsuit along with links to her real accounts on social media platforms" are displayed in a web browser to maintain the ruse.

Attack Vectors

- The campaign involved documents referencing a recent terrorist attack in New York in an attempt to trick victims into clicking on the malicious documents, which eventually infect their systems with malware. Since DDE is a Microsoft legitimate feature, most antivirus solutions don't flag any warning or block the documents with DDE fields.
- According to the journalists, they have experienced spear-phishing attacks for years in an attempt to hack networks and access sources and information
- The most notable APT28 presumed targets are the American Democratic National Committee, the German parliament, and the French television network TV5Monde. The group was also connected to the Hillary Clinton email leak among other campaigns and attacks.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• 64b0037dde987c78edf807a1bd7f09cdfac072ec2a59954cc4918828b7e608a3 • 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04 • 451f3d427ac21632f38619ef96dece25798918866d44fe82ff1ed30996f998dc • 40a7fd89b9e51b0a515ac2355036d203357be90a2200b9c506b95c12db54c7aa • 18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6 • f348a0349fdec136c3ac9eaee9b8761da6bd33df82056e4dd792192731675b00 • 54b14fc84f152b43c63babc46f2597b053e94627 • fcf03bf5ef4babce577dd13483391344e957fd2c855624c9f0573880b8cba62e

INDICATOR TYPE	INDICATORS
File Hash	• a1c73ce193ffa5323aaef73fbabbc2a984e10900f09cf9fcb0cb11606a23c402 • 4c49a17ee2f2dcd8041914110f362cd8 • 72227c531de0c8198399f712157d2039c9cb205b507dcc67c03f43b480e1f34c • 19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc • e9cd6bf375c2ff5b1f6baa2cf04b11c65f1472ed27302275f68445a17001a38b • 6fcf4592f9261d5734fb3b8534f6839ab65f68fd9ff14a9005225135e743226c • c78fcae030a66f388bf8cea569422f5a79b7b96c • 6bb7c33879c07d9e97b9f8b62466c1cf • 9a7d82ba55216defc2d4131b6c453f02 • 549726b8bfb1919a343ac764d48fdc81
IP Address	• 185.220.100.253 • 74.124.219.71 • 185.132.17.160 • 64.190.113.51 • 111.90.159.23 • 216.131.111.138 • 176.67.83.7 • 46.183.219.207 • 95.183.55.64 • 185.67.2.123 • 94.177.12.150 • 139.5.177.206 • 203.149.168.34 • 85.195.206.7 • 195.12.50.171 • 68.76.150.97

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

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://thehackernews[.]com/2024/05/kremlin-backed-apt28-targets-polish[.]html
- https://dashboard[.]ti[.]insight[.]rapid7[.]com/#/tip/cyber-term/57b972d86cdfe353001df88d