Severity

High

Analysis Summary

GhostWriter

GhostWriter is a state-sponsored threat group targeting individuals in Poland, Latvia, and Lithuania. The group has now been linked to UNC1151. The campaign by the threat group started in mid-2020 and now the actors responsible for these attacks are being associated with UNC1151. UNC1151 is a state-sponsored APT group partaking in malware campaigns and credential harvesting attacks. UNC1151 — a Minsk-based threat group — has been targeting Ukrainian government officials and military personnel with mass phishing emails. After the account is compromised, the attackers, by the IMAP protocol, get access to all the messages. Later, the attackers use contact details from the victim's address book to send the phishing emails.

APT28

APT28 is one of Russia's longest-running APTs and its operations date back to at least 2007. The group supports Russia in their strategic operations against the U.S, countries of the former Soviet Union, Europe, and now Asia. These attacks mostly involve cyber crimes against the defense and military of targeted countries. To support Russia's national interests, APT28 compromises the targeted country's operation, steals their data, and then leaks it to their government.

Going by the aliases Fancy Bear, Pawn Storm, Tsar Team, STRONTIUM, and Sofacy Group, APT28 performs their attacks using a spoofed website and phishing emails containing malicious links.

Recently, APT 28 (allegedly) has attacked Eastern European countries using Empire and Invoke-Obfuscation. The MSHTML Remote Code Execution vulnerability, CVE-2021-40444, is being used by their threat actors.

Other threat actors include Turla, COLDRIVER, and Curious Gorge.

Impact

- Information Theft
- Exposure of Sensitive Data
- Financial Loss
- Unauthorized Access

Indicators of Compromise

Domain Name

- wkoinfo[.]webredirect[.]org
- jadlactnato[.]webredirect[.]org
- cache-dns[.]com
- docs-shared[.]com
- documents-forwarding[.]com
- documents-preview[.]com
- protection-link[.]online
- webresources[.]live
- noreply[.]accountsverify[.]top
- microsoftonline[.]email-verify[.]top
- lt-microsoftgroup[.]serure-email[.]online
- facebook[.]com-validation[.]top
- lt-meta[.]com-verification[.]top
- lt-facebook[.]com-verification[.]top

MD5

- cf7eb797b63e8322269eb8281975af53
- 7df79de2f5e31263208ef83caca7b1f0

SHA-256

- 710faabf217a5cd3431670558603a45edb1e01970f2a8710514c2cc3dd8c2424
- 39d242660c6d5dbe97d5725bbfed0f583344d18840ccd902fffdd71af12e20ec

SHA-1

- beff0874841fc49e458f9fbfb04664143535bf32
- 670224a6b59827de20a93cbe754edfb510cf3cc3

Remediation

- Logging — Log your eCommerce environment’s network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.
- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets
- Security Best Practices — Do not open emails and attachments from unknown or suspicious sources.