KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Russian-APT SEABORGIUM phishing to conduct Cyber-Espionage

Tracker ID: TN0824 **Date:** 24/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Europe, North America

Background

A persistent Russian state-sponsored threat actor identified as "SEABORGIUM " has been engaged in ongoing spear-phishing and credential theft operations against organizations and individuals linked with the Russian government. The threat actor appears to be primarily interested in cyberespionage. Several NGOs organizations, think tanks, universities, and multilateral organizations in the US and UK, as well as numerous entities in the defense and intelligence industries, are among its victims.

SEABORGIUM has repeatedly targeted the same organizations over time. Once accomplished, it gradually infiltrates the social networks of targeted organizations through repeated impersonation, rapport-building, and phishing to deepen its intrusion. For several years, it has successfully compromised organizations and people of interest in persistent campaigns, rarely changing methodology or tactics. SEABORGIUM overlaps with the threat groups listed as Callisto Group (F-Secure), TA446 (Proofpoint), and COLDRIVER based on known indicators of compromise and actor methods (Google).

The Ukrainian Security Service (SSU) has linked Callisto to the Gamaredon Group (tracked by Microsoft as ACTINIUM); however, MSTIC has found no technological infiltration links to justify the association. Since the beginning of 2022, researchers have observed SEABORGIUM campaigns targeting over 30 organizations, in addition to personal accounts of people of interest. According to the researchers, Ukraine is most certainly not the actor's primary focus; rather, it is most likely a reactive focus region for the actor and one of several distinct objectives.

SEABORGIUM predominantly uses phishing tactics to target individuals or groups of people to steal user credentials. It usually includes a URL in the body of the phishing email or PDF attachment. These attachments resemble files or documents from hosting services like OneDrive and require the user to click a button to view the attachment. Once the victim clicks the URL, they are directed to an actor-controlled server containing a phishing framework. By using URL shorteners and open redirection, the actor can sometimes mask their URL from the target and inline protection services.

Microsoft saw the perpetrator attempting to avoid automated surfing and detonation by fingerprinting browsing behavior. After redirecting the target to the final page, the framework prompts the target for authentication, replicating the sign-in page for a legitimate service and intercepting any credentials. Following the collection of credentials, the target is routed to a website or document to conclude the engagement.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Russian-APT SEABORGIUM phishing to conduct Cyber-Espionage

Tracker ID: TN0824 **Date:** 23/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Europe, North America

To thwart SEABORGIUM's activities, Microsoft has blocked accounts used for surveillance, phishing, and email gathering. It also revealed 69 sites that were reportedly linked to the threat actor's phishing attempts to get login information for Microsoft, ProtonMail, and Yandex accounts.

MITRE ATT&CK Tactics

Initial Access, Execution, Persistent, Defense Evasion, and Exfiltration.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Keep systems and products updated and patched as soon as possible after the patches are released.
- Avoid opening untrusted links and email attachments without first verifying their authenticity. Check the sender's email address to confirm its legitimacy.
- Be wary of or do not trust shortened URLs. Block them at the network gateway.
- Check your Office 365 email filtering settings to ensure you block spoofed emails, spam, and emails with malware. Configure Office 365 to disable email auto-forwarding.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Require multifactor authentication (MFA) for all users coming from all locations including perceived trusted environments, and all internet-facing infrastructure–even those coming from on-premises systems.
- Leverage more secure implementations such as FIDO Tokens, or Microsoft Authenticator with number matching. Avoid telephony-based MFA methods to avoid risks associated with SIM-jacking.
- Ensure employees are aware of the ongoing phishing campaigns and techniques.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Russian-APT SEABORGIUM phishing to conduct Cyber-Espionage

Tracker ID: TN0824 **Date:** 24/August/2022 **Category:** Threat Actor **Industry:** All **Region**: Europe, North America

References

- Jai Vijayan, Microsoft Disrupts Russian Group's Multiyear Cyber-Espionage Campaign, Dark Reading, 17th August 2022, External Link (www.darkreading.com).
- Microsoft, Disrupting SEABORGIUM's ongoing phishing operations, 15th August 2022, External Link (www.microsoft.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176 471 471

*

Domains			
cache-dns[.]com	documents-cloud[.]online	pdf-forwarding[.]online	onlinecloud365[.]live
cache-dns-forwarding[.]com	documents-forwarding[.]com	protection-checklinks[.]xyz	pdf-cloud[.]online
cache-dns-preview[.]com	document-share[.]live	protection-link[.]online	pdf-shared[.]online
cache-docs[.]com	documents-online[.]live	protectionmail[.]online	proton-pdf[.]online
cache-pdf[.]com	documents-pdf[.]online	protection-office[.]live	proton-view[.]online
cache-pdf[.]online	documents-preview[.]com	protect-link[.]online	office365-online[.]live
cache-services[.]live	documents-view[.]live	proton-docs[.]com	doc-viewer[.]com
cloud-docs[.]com	document-view[.]live	proton-reader[.]com	file-milgov[.]systems
cloud-drive[.]live	drive-docs[.]com	proton-viewer[.]com	office-protection[.]online
cloud-storage[.]live	drive-share[.]live	relogin-dashboard[.]online	documents-cloud[.]com
docs-cache[.]com	goo-link[.]online	safe-connection[.]online	pdf-docs[.]online
docs-forwarding[.]online	hypertextteches[.]com	safelinks-protect[.]live	cloud-mail[.]online
docs-info[.]com	mail-docs[.]online	secureoffice[.]live	docs-info[.]online
docs-shared[.]com	officeonline365[.]live	webresources[.]live	pdf-cache[.]online
docs-shared[.]online	online365-office[.]com	word-yand[.]live	document-preview[.]com
docs-view[.]online	online-document[.]live	yandx-online[.]cloud	docs-drive[.]online
document-forwarding[.]com	online-storage[.]live	y-ml[.]co	pdf-cache[.]com
document-online[.]live			