Disrupting SEABORGIUM's ongoing phishing operations

8/15/2022

The Microsoft Threat Intelligence Center (MSTIC) has observed and taken actions to disrupt campaigns launched by SEABORGIUM, an actor Microsoft has tracked since 2017. SEABORGIUM is a threat actor that originates from Russia, with objectives and victimology that align closely with Russian state interests. Its campaigns involve persistent phishing and credential theft campaigns leading to intrusions and data theft. SEABORGIUM intrusions have also been linked to hack-and-leak campaigns, where stolen and leaked data is used to shape narratives in targeted countries. While we cannot rule out that supporting elements of the group may have current or prior affiliations with criminal or other nonstate ecosystems, MSTIC assesses that information collected during SEABORGIUM intrusions likely supports traditional espionage objectives and information operations as opposed to financial motivations.

This blog provides insights into SEABORGIUM's activities and technical methods, with the goal of sharing context and raising awareness about a significant threat to Microsoft customers. MSTIC would like to acknowledge the Google Threat Analysis Group (TAG) and the Proofpoint Threat Research Team for their collaboration on tracking and disrupting this actor. Microsoft's ability to detect and track SEABORGIUM's abuse of Microsoft services, particularly OneDrive, has provided MSTIC sustained visibility into the actor's activities and enabled us to notify impacted customers. As an outcome of these service abuse investigations, MSTIC partnered with abuse teams in Microsoft to disable accounts used by the actor for reconnaissance, phishing, and email collection. Microsoft Defender SmartScreen has also implemented detections against the phishing domains represented in SEABORGIUM's activities.

Who is SEABORGIUM?

SEABORGIUM is a highly persistent threat actor, frequently targeting the same organizations over long periods of time. Once successful, it slowly infiltrates targeted organizations' social networks through constant impersonation, rapport building, and phishing to deepen their intrusion. SEABORGIUM has successfully compromised organizations and people of interest in consistent campaigns for several years, rarely changing methodologies or tactics. Based on known indicators of compromise and actor tactics, SEABORGIUM overlaps with the threat groups tracked as Callisto Group (F-Secure), TA446 (Proofpoint) and COLDRIVER (Google). Security Service of Ukraine (SSU) has associated Callisto with Gamaredon Group (tracked by Microsoft as ACTINIUM); however, MSTIC has not observed technical intrusion links to support the association.

Since the beginning of 2022, Microsoft has observed SEABORGIUM campaigns targeting over 30 organizations, in addition to personal accounts of people of interest. SEABORGIUM primarily targets NATO countries, particularly the US and the UK, with occasional targeting of other countries in the Baltics, the Nordics, and Eastern Europe. Such targeting has included the government sector of Ukraine in the months leading up to the invasion by Russia, and organizations involved in supporting roles for the war in Ukraine. Despite some targeting of these organizations, Microsoft assesses that Ukraine is likely not a primary focus for this actor; however, it is most likely a reactive focus area for the actor and one of many diverse targets.

Within the target countries, SEABORGIUM primarily focuses operations on defense and intelligence consulting companies, non-governmental organizations (NGOs) and intergovernmental organizations (IGOs), think tanks, and higher education. SEABORGIUM has a high interest in targeting individuals as well, with 30% of Microsoft's nation-state notifications related to SEABORGIUM activity being delivered to Microsoft consumer email accounts. SEABORGIUM has been observed targeting former intelligence officials, experts in Russian affairs, and Russian citizens abroad. As with any observed nation-state actor activity, Microsoft directly notifies customers of Microsoft services that have been targeted or compromised, providing them with the information they need to secure their accounts.

Observed actor activity

Over many years of tracking, Microsoft has observed a consistent methodology from SEABORGIUM with only slight deviations in their social engineering approaches and in how they deliver the initial malicious URL to their targets. In this section, we provide detailed analysis of SEABORBIUM's operational tactics as well as several examples of their campaigns.

Impersonation and establishing contact

Before starting a campaign, SEABORGIUM often conducts reconnaissance of target individuals, with a focus on identifying legitimate contacts in the targets' distant social network or sphere of influence. Based on some of the impersonation and targeting observed, we suspect that the threat actor uses social media platforms, personal directories, and general open-source intelligence (OSINT) to supplement their reconnaissance efforts. MSTIC, in

partnership with LinkedIn, has observed fraudulent profiles attributed to SEABORGIUM being used sporadically for conducting reconnaissance of employees from specific organizations of interest. In accordance with their policies, LinkedIn terminated any account (including the one shown below) identified as conducting inauthentic or fraudulent behavior.

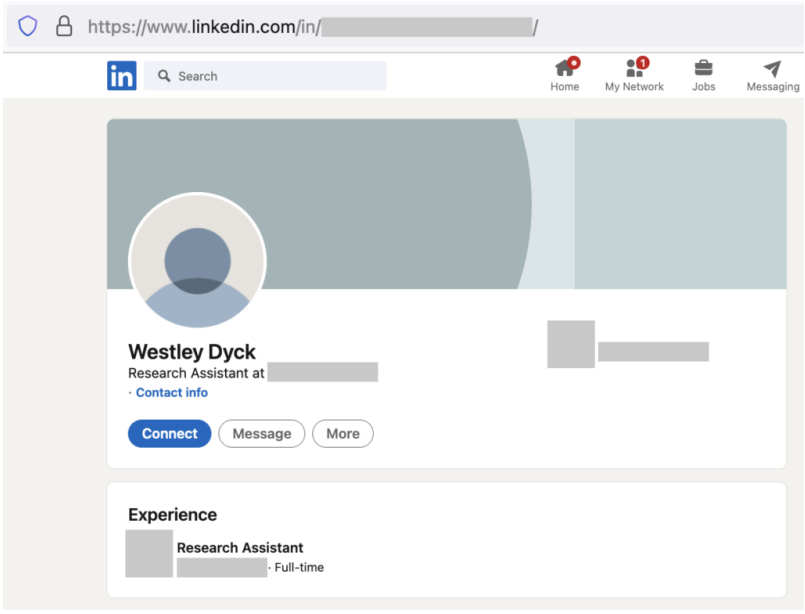

Figure 1: Example profile used by SEABORGIUM to conduct industry-specific reconnaissance

SEABORGIUM also registers new email accounts at various consumer email providers, with the email address or alias configured to match legitimate aliases or names of impersonated individuals. While the creation of new consumer accounts is common, we have also observed SEABORGIUM returning to and reusing historical accounts that match the industry of the ultimate target. In one case, we observed SEABORGIUM returning to an account it had not used in a year, indicating potential tracking and reusing of accounts if relevant to targets' verticals.

After registering new accounts, SEABORGIUM proceeds to establish contact with their target. In cases of personal or consumer targeting, MSTIC has mostly observed the actor starting the conversation with a benign email message, typically exchanging pleasantries before referencing a non-existent attachment while highlighting a topic of interest to the target. It's likely that this additional step helps the actor establish rapport and avoid suspicion, resulting in further interaction. If the target replies, SEABORGIUM proceeds to send a weaponized email.


I shared the paper. Did you get it?

Cheers,

From:
Sent:
To: @outlook.com>
Subject: Re: Wondering what you guys think

Please send the attachment

Get Outlook for iOS

From: @outlook.com>
Sent: Tuesday, June 8, 2021 8:53:41 AM
To:
Subject: Re: Wondering what you guys think

I know you have your hands full at the moment, but nevertheless thought this would interest you (attached).

Figure 2: Example email showing the multi-email approach and rapport building frequently used by the actors.

MSTIC has also documented several cases where the actor focuses on a more organizational approach to phishing. In these cases, the actor uses an authoritative approach in their social engineering and typically goes to directly sending malicious content.

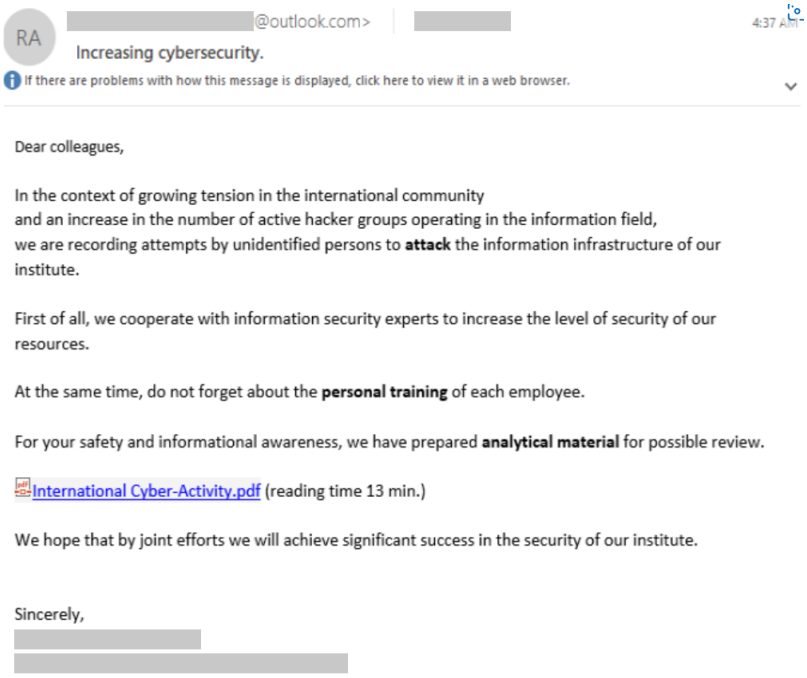

Figure 3: Example phishing email from 2022 where the actor impersonates the lead of an organization and emails select members of th

These examples serve to demonstrate the actors' capability to be dynamic and to adapt their social engineering approach to gain the trust of their victims.

Delivery of malicious content

Microsoft has identified several variations in the way that SEABORGIUM delivers a link that directs targets to their credential stealing infrastructure.

URL in body of email

In the simplest case, SEABORGIUM directly adds a URL to the body of their phishing email. Occasionally, the actor leverages URL shorteners and open redirects to obfuscate their URL from the target and inline protection platforms. The email varies between fake personal correspondence with a hyperlinked text and fake file sharing emails that imitate a range of platforms.

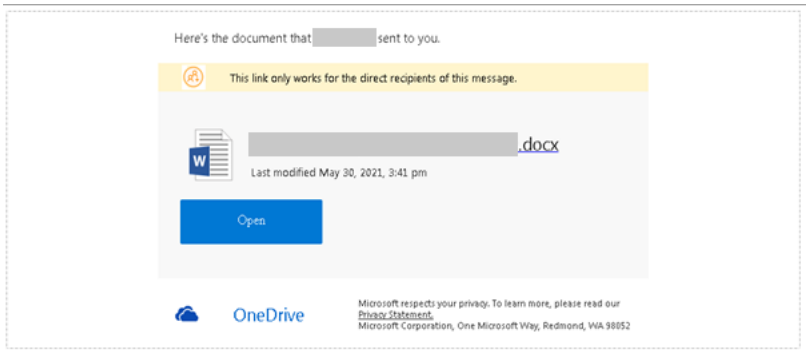

Figure 4: Example follow-up email impersonating a OneDrive share. The link embedded takes the user to actor-controlled infrastructure.

PDF file attachment that contains a URL

MSTIC has observed an increase in the use of attachments in SEABORGIUM campaigns. These attachments typically imitate a file or document hosting service, including OneDrive, and request the user to open the document by clicking a button.

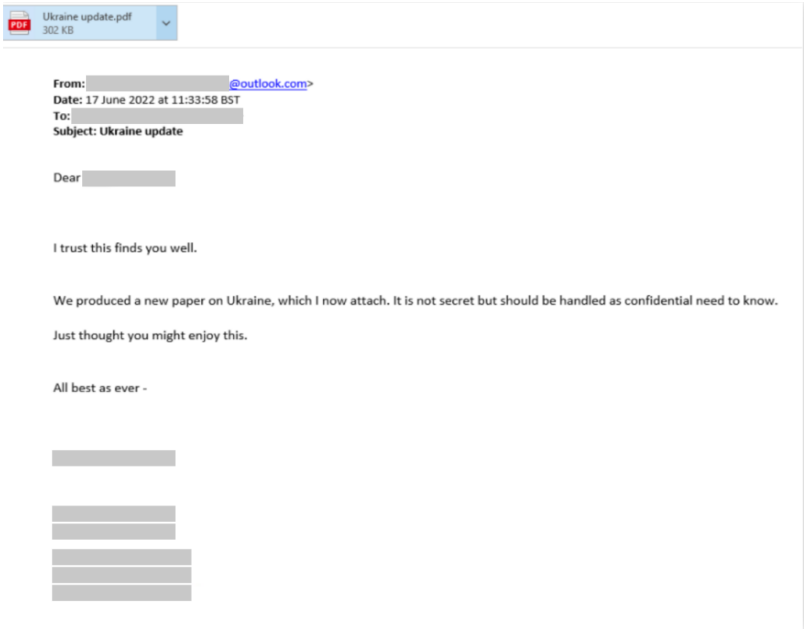

Figure 5: Campaign from 2022 using the war in Ukraine as a ruse. Example of SEABORGIUM directly attaching a PDF file to the email

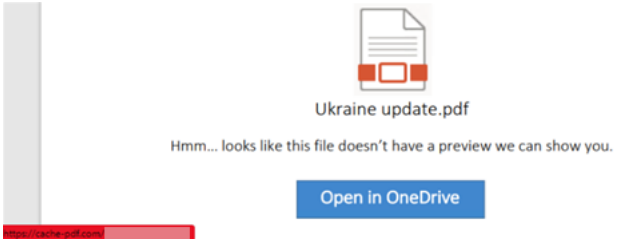

Figure 6: Example PDF file used in campaigns. The PDF files appear to be a failed preview, redirecting the users to click a link which takes the user to actor-controlled infrastructure.

OneDrive link to PDF file that contains a URL

SEABORGIUM also abuses OneDrive to host PDF files that contain a link to the malicious URL. This activity does not represent any security issues or vulnerabilities on the OneDrive platform. The actors include a OneDrive link in the body of the email that when clicked directs the user to a PDF file hosted within a SEABORGIUM-controlled OneDrive account. As seen in the previous example, the victim is presented with what appears to be a failed preview message, enticing the target to click the link to be directed to the credential-stealing infrastructure. Occasionally, SEABORGIUM makes use of open redirects within the PDF file to further disguise their operational infrastructure. In the example below, SEABORGIUM uses a Google URL for redirection.

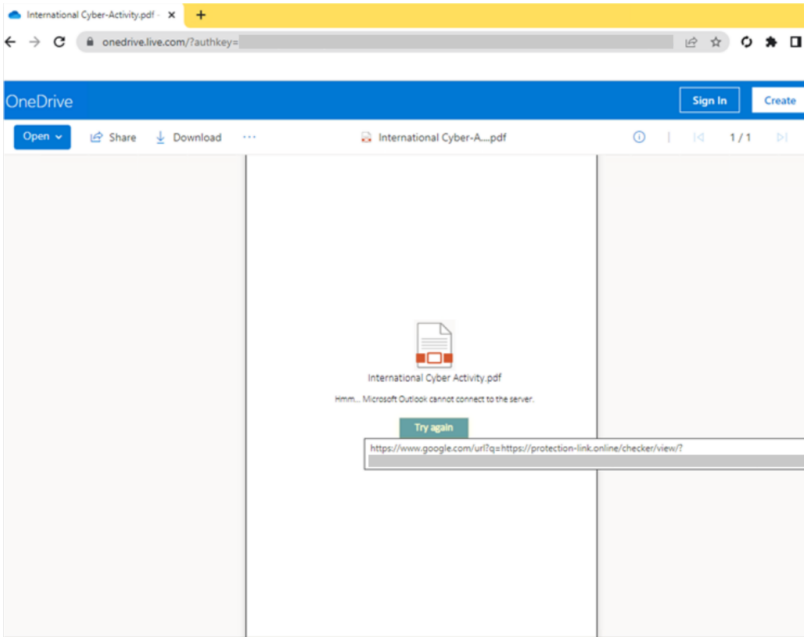

Figure 7: Example document hosted on OneDrive that uses a Google redirect link to send users to actor-controlled infrastructure.

Credential theft

Regardless of the method of delivery, when the target clicks the URL, the target is directed to an actor-controlled server hosting a phishing framework, most often EvilGinx. On occasion, Microsoft has observed attempts by the actor to evade automated browsing and detonation by fingerprinting browsing behavior. Once the target is redirected to the final page, the framework prompts the target for authentication, mirroring the sign-in page for a legitimate provider and intercepting any credentials. After credentials are captured, the target is redirected to a website or document to complete the interaction.

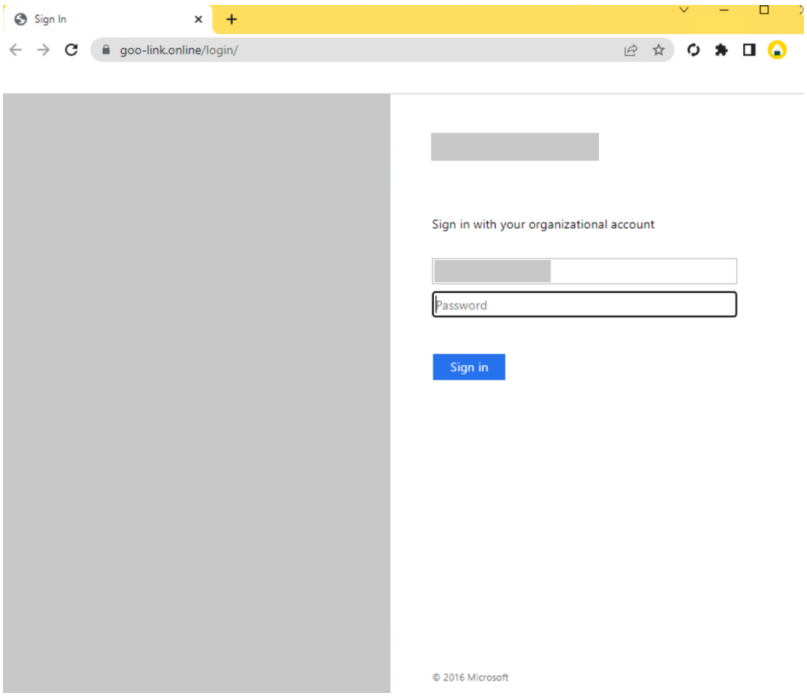

Figure 8: Example cloned phishing portal used by SEABORGIUM to directly impersonate a victim organization.

Data exfiltration and impact

SEABORGIUM has been observed to use stolen credentials and directly sign in to victim email accounts. Based on our experience responding to intrusions from this actor on behalf of our customers, we have confirmed that the following activities are common:

- **Exfiltration of intelligence data**: SEABORGIUM has been observed exfiltrating emails and attachments from the inbox of victims.
- **Setup of persistent data collection**: In limited cases, SEABORGIUM has been observed setting up forwarding rules from victim inboxes to actor-controlled dead drop accounts where the actor has long-term access to collected data. On more than one occasion, we have observed that the actors were able to access mailing-list data for sensitive groups, such as those frequented by former intelligence officials, and maintain a collection of information from the mailing-list for follow-on targeting and exfiltration.
- **Access to people of interest**: There have been several cases where SEABORGIUM has been observed using their impersonation accounts to facilitate dialog with specific people of interest and, as a result, were included in conversations, sometimes unwittingly, involving multiple parties. The nature of the conversations identified during investigations by Microsoft demonstrates potentially sensitive information being shared that could provide intelligence value.

Based on the specific victimology, documents stolen, conversations fostered, and sustained collection observed, we assess that espionage is likely a key motivation of the actor.

Sporadic involvement with information operations

In May 2021, MSTIC attributed an information operation to SEABORGIUM based on observations and technical overlaps with known phishing campaigns. The operation involved documents allegedly stolen from a political organization in the UK that were uploaded to a public PDF file-sharing site. The documents were later amplified on social media via known SEABORGIUM accounts, however MSTIC observed minimal engagement or further amplification. Microsoft was unable to validate the authenticity of the material.

In late May 2022, Reuters along with Google TAG disclosed details about an information operation, specifically using hack and leak, that they attributed to COLDRIVER/SEABORGIUM. Microsoft independently linked SEABORGIUM to the campaign through technical indicators and agrees with the assessment by TAG on the actor responsible for the operation. In the said operation, the actors leaked emails/documents from 2018 to 2022, allegedly stolen from consumer Protonmail accounts belonging to high-level proponents of Brexit, to build a narrative that the participants were planning a coup. The narrative was amplified using social media and through specific politically themed media sources that garnered quite a bit of reach.

While we have only observed two cases of direct involvement, MSTIC is not able to rule out that SEABORGIUM's intrusion operations have yielded data used through other information outlets. As with any information operation, Microsoft urges caution in distributing or amplifying direct narratives, and urges readers to be critical that the malicious actors could have intentionally inserted misinformation or disinformation to assist their narrative. With this in mind, Microsoft will not be releasing the specific domain or content to avoid amplification.

Recommended customer actions

The techniques used by the actor and described in the "Observed actor activity" section can be mitigated by adopting the security considerations provided below:

- 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.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- 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.

For Microsoft Defender for Office 365 Customers:

- Use Microsoft Defender for Office 365 for enhanced phishing protection and coverage against new threats and polymorphic variants.
- Enable Zero-hour auto purge (ZAP) in Office 365 to quarantine sent mail in response to newly acquired threat intelligence and retroactively neutralize malicious phishing, spam, or malware messages that have already been delivered to mailboxes.
- Configure Defender for Office 365 to recheck links on click. Safe Links provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages, other Office applications such as Teams, and other locations such as SharePoint Online. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Exchange Online Protection (EOP). Safe Links scanning can help protect your organization from malicious links that are used in phishing and other attacks.
- Use the Attack Simulator in Microsoft Defender for Office 365 to run realistic, yet safe, simulated phishing and password attack campaigns within your organization. Run spear-phishing (credential harvest) simulations to train end-users against clicking URLs in unsolicited messages and disclosing their credentials.

Indicators of compromise (IOCs)

The below list provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Confidence	Public References (if Applicable)
cache-dns[.]com	Domain name	High	Google TAG, Sekoia.io
cache-dns-forwarding[.]com	Domain name	High	
cache-dns-preview[.]com	Domain name	High	
cache-docs[.]com	Domain name	High	Sekoia.io
cache-pdf[.]com	Domain name	High	
cache-pdf[.]online	Domain name	High	
cache-services[.]live	Domain name	High	
cloud-docs[.]com	Domain name	High	Sekoia.io
cloud-drive[.]live	Domain name	High	
cloud-storage[.]live	Domain name	High	
docs-cache[.]com	Domain name	High	Sekoia.io
docs-forwarding[.]online	Domain name	High	
docs-info[.]com	Domain name	High	Sekoia.io
docs-shared[.]com	Domain name	High	Google TAG, Sekoia.io
docs-shared[.]online	Domain name	High	
docs-view[.]online	Domain name	High	
document-forwarding[.]com	Domain name	High	
document-online[.]live	Domain name	High	
document-preview[.]com	Domain name	High	
documents-cloud[.]com	Domain name	High	Sekoia.io
documents-cloud[.]online	Domain name	High	Sekoia.io
documents-forwarding[.]com	Domain name	High	Google TAG

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

NOTE: These indicators should not be considered exhaustive for this observed activity.

Detections

Intelligence gathered by the Microsoft Threat Intelligence Center (MSTIC) is used within Microsoft security products to provide protection against associated actor activity.

Microsoft Defender for Office 365

Microsoft Defender for Office offers enhanced solutions for blocking and identifying malicious emails. Signals from Microsoft Defender for Office inform Microsoft 365 Defender, which correlate cross-domain threat intelligence to deliver coordinated defense, when this threat has been detected. These alerts, however, can be triggered by unrelated threat activity. Example alerts:

- A potentially malicious URL click was detected
- Email messages containing malicious URL removed after delivery
- Email messages removed after delivery
- Email reported by user as malware or phish

Microsoft 365 Defender

Aside from the Microsoft Defender for Office 365 alerts above, customers can also monitor for the following Microsoft 365 Defender alerts for this attack. Note that these alerts can also be triggered by unrelated threat activity. Example alerts:

- Suspicious URL clicked
- Suspicious URL opened in web browser
- User accessed link in ZAP-quarantined email

Microsoft 365 Defender customers should also investigate any **"Stolen session cookie was used"** alerts that would betriggered for adversary-in-the-middle (AiTM) attacks.

Microsoft Defender SmartScreen

Microsoft Defender SmartScreen has implemented detections against the phishing domains represented in the IOC section above.

Advanced hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can run the following advanced hunting queries to locate IOCs and related malicious activity in their environments.

The query below identifies matches based on domain IOCs related to SEABORGIUM actor across a range of common Microsoft Sentinel data sets:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/SEABORGIUMDomainsAugust2022.yaml

Microsoft 365 Defender

Microsoft 365 Defender customers can run the following advanced hunting queries to locate IOCs and related malicious activity in their environments.

This query identifies matches based on domain IOCs related to SEABORGIUM against Microsoft Defender for Endpoint device network connections

https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/Microsoft%20365%20Defender/Campaigns/SEABORGIUMDomainIOCsAug2022.yaml