NEWS

SEABORGIUM and TA453 continue their respective spear-phishing campaigns against targets of interest

Activity against targeted organisations and individuals in the UK and other areas of interest.

The Russia-based SEABORGIUM (Callisto Group/TA446/COLDRIVER/TAG-53) and Iran-based TA453 (APT42/Charming Kitten/Yellow Garuda/ITG18) actors continue to successfully use spear-phishing attacks against targeted organisations and individuals in the UK, and other areas of interest, for information gathering activity.

Industry has previously published details of SEABORGIUM and TA453 activity. This advisory draws on that body of information.

Throughout 2022, SEABORGIUM and TA453 targeted sectors included academia, defence, governmental organisations, NGOs, think-tanks, as well as politicians, journalists and activists.

Although there is similarity in the TTPs and targeting profiles, these campaigns are separate and the two groups are not collaborating.

This advisory aims to raise awareness of this activity for individuals and organisations in sectors known to be of interest to these actors. It helps identify the specifics of these actors' spear-phishing techniques.

Outline of the attacks

The activity is typical of spear-phishing campaigns, where an actor targets a specific individual or group, using information known to be of interest to the targets to engage them. In a spear-phishing campaign, an actor perceives their target to have direct access to information of interest, be an access vector to another target, or both.

Research and preparation

Using open-source resources to conduct reconnaissance, including social media and professional networking platforms, SEABORGIUM and TA453 identify hooks to engage their target. They take the time to research their interests and identify their real-world social or professional contacts. [T1589; T1593]

They have also created fake social media or networking profiles that impersonate respected experts [T1585.001], and used supposed conference or event invitations, as well as false approaches from journalists.

Both SEABORGIUM and TA453 use webmail addresses from different providers (including Outlook, Gmail and Yahoo) in their initial approach [T1585.002], impersonating known contacts of the target or eminent names in the target's field of interest or sector.

The actors have also created malicious domains resembling legitimate organisations to appear authentic [T1583.001]. Microsoft Threat Intelligence Center (MSTIC) provide a list of observed Indicators of Compromise (IOCs) in their SEABORGIUM blog, although this should not be considered as exhaustive.

Preference for personal email addresses

SEABORGIUM and TA453 have predominantly sent spear-phishing emails to targets' personal email addresses, although targets' corporate or business email addresses have also been used. The actors may use personal emails to circumvent security controls in place on corporate networks.

Building a rapport

Having taken the time to research their targets' interests and contacts to create a believable approach, SEABORGIUM and TA453 now start to build trust. They often begin by establishing benign contact on a topic they hope will engage their targets. There is often some correspondence between attacker and target, sometimes over an extended period, as the attacker builds rapport.

Delivery of malicious link

Once trust is established, the attacker uses typical phishing tradecraft and shares a link [T1566.002], apparently to a document or website of interest. This leads the target to an actor-controlled server, prompting the target to enter account credentials.

The malicious link may be a URL in an email message, or the actor may embed a link in a document [T1566.001] on OneDrive, GoogleDrive, or other file-sharing platforms.

TA453 has even shared malicious links disguised as Zoom meeting URLs, and in one case, even set up a Zoom call with the target to share the malicious URL in the chat bar during the call.

Industry partners have also reported the use of multi-persona impersonation (use of two or more actor-controlled personas on a spear-phishing thread) to add the appearance of legitimacy.

Exploitation and further activity

Whichever delivery method is used, once the target clicks on the malicious URL, they are directed to an actor-controlled server that mirrors the sign-in page for a legitimate service. Any credentials entered at this point are now compromised.

The SEABORGIUM and TA453 actors then use the stolen credentials to log in to targets' email accounts [T1078], from where they are known to access and steal emails and attachments from the victim's inbox [T1114.002]. They have also set-up mail-forwarding rules, giving them ongoing visibility of victim correspondence [T1113.003].

The actors have also used their access to a victim email account to access mailing-list data and victim's contacts lists. The actors then use this information for follow-on targeting and have also used compromised email accounts for further phishing activity [T1586.002].

Conclusion

Although spear-phishing is an established technique used by many actors, SEABORGIUM and TA453 continue to use it successfully and evolve the technique to maintain their success.

Individuals and organisations from previously targeted sectors should be vigilant of the techniques above. In the UK, **report activity consistent with that described above to the NCSC**.

Information on effective defence against spear-phishing is included in the 'Mitigation' section below.

MITRE ATT&CK®

This report has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	ID	Technique	Procedure

Reconnaissance	T1593	Search Open Websites/Domains	SEABORGIUM actors use open source research and social media to identify information about victims to be used in targeting. TA453 actors likely use professional networking sites and other open source resources to research their targets.
Reconnaissance	T1589	Gather Victim Identity Information	SEABORGIUM and TA453 actors use online data sets and open source resources to gather information about their targets.
Resource Development	T1585.001	Establish Accounts: Social Media Accounts	SEABORGIUM actors have been observed to establish fraudulent profiles on professional networking sites to conduct reconnaissance. TA453 actors have been observed to use fraudulent profiles on professional networking and other social media sites to approach their targets.
Resource Development	T1585.002	Establish Accounts: Email Accounts	SEABORGIUM and TA453 actors register consumer email accounts matching the names of individuals they are impersonating to conduct spear-phishing activity.
Resource Development	T1583.001	Acquire Infrastructure: Domains	SEABORGIUM actors register domains used to host their phishing framework. TA453 actors register domains to host fake login pages.
Resource Development	T1586.002	Compromise Accounts: Email Accounts	SEABORGIUM actors have been observed to use compromised victim email accounts to conduct spear-phishing activity against contacts of the original victim.
Initial Access	T1078	Valid Accounts	SEABORGIUM and TA453 actors use compromised credentials, captured from fake login pages, to log in to valid victim user accounts.
Initial Access	T1566.001	Phishing: Spear-phishing attachment	SEABORGIUM actors use malicious links embedded in an email attachment to direct victims to their credential stealing sites.
Initial Access	T1566.002	Phishing: Spear-phishing link	SEABORGIUM actors send spear-phishing emails with malicious links directly to credential stealing sites, or to documents hosted on a file sharing site which direct victims to credential stealing sites. TA453 actors send spear-phishing emails with malicious links directly to credential stealing sites and to malware hosted on a file sharing site.

Collection	T1114.002	Email Collection: Remote Email Collection	SEABORGIUM and TA453 actors interact directly with externally facing Exchange services, Office 365, or Google Workspace to access email and steal information using compromised credentials or access tokens.
Collection	T1113.003	Email Collection: Email Forwarding Rule	SEABORGIUM actors may abuse email-forwarding rules to monitor the activities of a victim, steal information, and maintain persistent access to victim's emails even after compromised credentials are reset.

Mitigation

- **Use strong passwords**
  Use a separate password for email accounts and avoid password re-use across multiple services. See NCSC Guidance.
- **Use multi-factor authentication**
  Also known as 2-step verification. Helps reduce the impact of password compromises. See NCSC Guidance for organisations and advice for small business, individuals and families
- **Protect your devices and networks by keeping them up to date**
  Use the latest supported versions, apply security updates promptly, use antivirus and scan regularly to guard against known malware threats. See NCSC Guidance.
- **Exercise vigilance**
  Spear-phishing emails are tailored to avoid suspicion. You may recognise the sender's name, but has the email come from an address that you recognise? Would you expect contact from this person's webmail address rather than their corporate email address? Has the suspicious email come to your personal/webmail address, rather than your corporate one? Can you verify that the email is legitimate via another means?
  See NCSC phishing guidance. CPNI's 'Think Before You Link' app, can help individuals identify malicious online profiles and reduce the risk of being targeted in the first instance.
- **Enable your email providers' automated email scanning features**
  These are turned on by default for consumer mail providers. See NCSC advice.
- **Disable mail-forwarding**
  Attackers have been observed to set up mail-forwarding rules to maintain visibility of target emails. If you cannot disable mail-forwarding, then monitor settings regularly to

ensure that a forwarding rule has not been set up by an external malicious actor.

PUBLISHED

26 January 2023

WRITTEN FOR

Small & medium sized organisations

Large organisations

NEWS TYPE

Alert