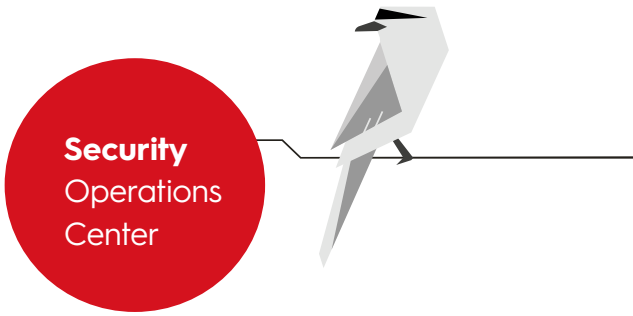
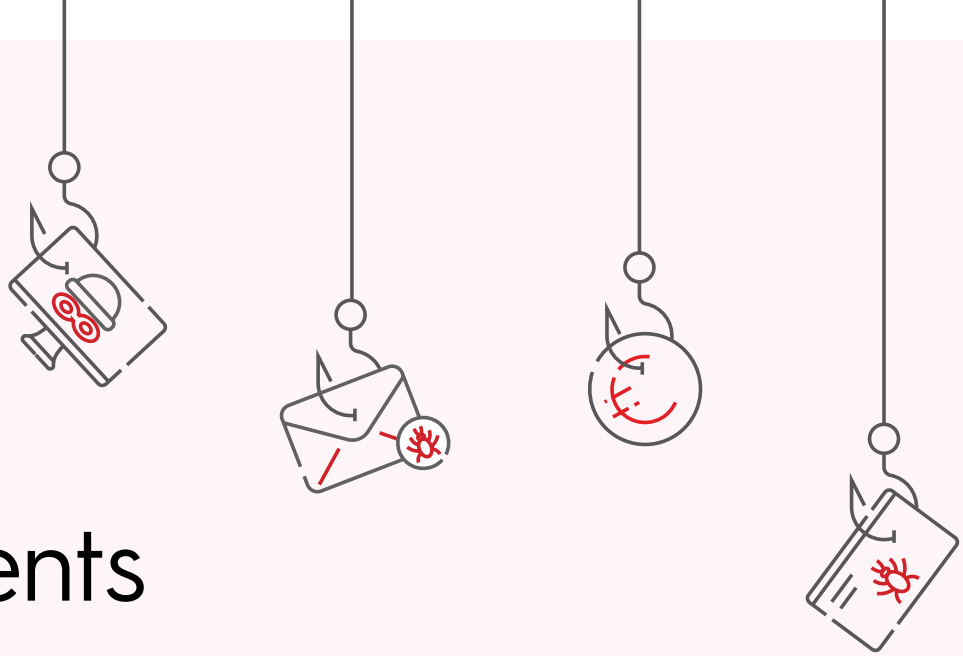


THREAT REPORT

Year in Review 2022

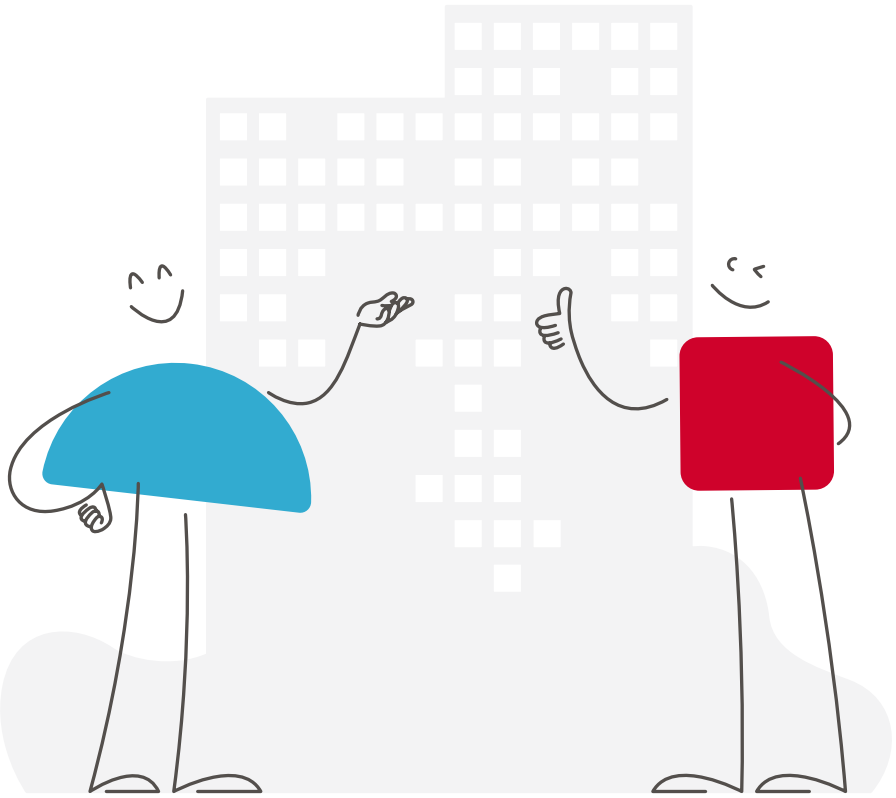
February 2023 • TLP: CLEAR

sopra steria



Contents

Please click on the desired heading for a direct link to the relevant page



About Sopra Steria

Sopra Steria Scandinavia is Norway's leading digital transformation and managed services provider and delivers managed services to enterprise customers in the Scandinavian market. Sopra Steria deliver managed services for Private and Public Cloud, Security, End user and Service Management, in multiple vertices including critical national infrastructure and public services.

Sopra Steria Security Operations Center (SOC) in Norway supports customers to reduce risk of data exfiltration, service disruption or regulatory non-compliance through managed security services.

Introduction

The Russian invasion of Ukraine was a defining moment in European Security and as with many of our peers, led to shifting intelligence requirements that required changes in collection, analysis, threat modelling, detection development and threat hunting. Although much work has been put into strategic planning and preparedness against Russian cyber operations, most of the incidents handled can be categorized as targeted and non-targeted cybercrime campaigns and vulnerability handling.

An important part of our company culture is Power of Sharing and as one of Norway's largest MSSPs, we want to share with our customers and broader public an excerpt of our observations and security incidents across our customer base. We are continuously striving to become more data-driven and future reports will be even more granular.

Phishing

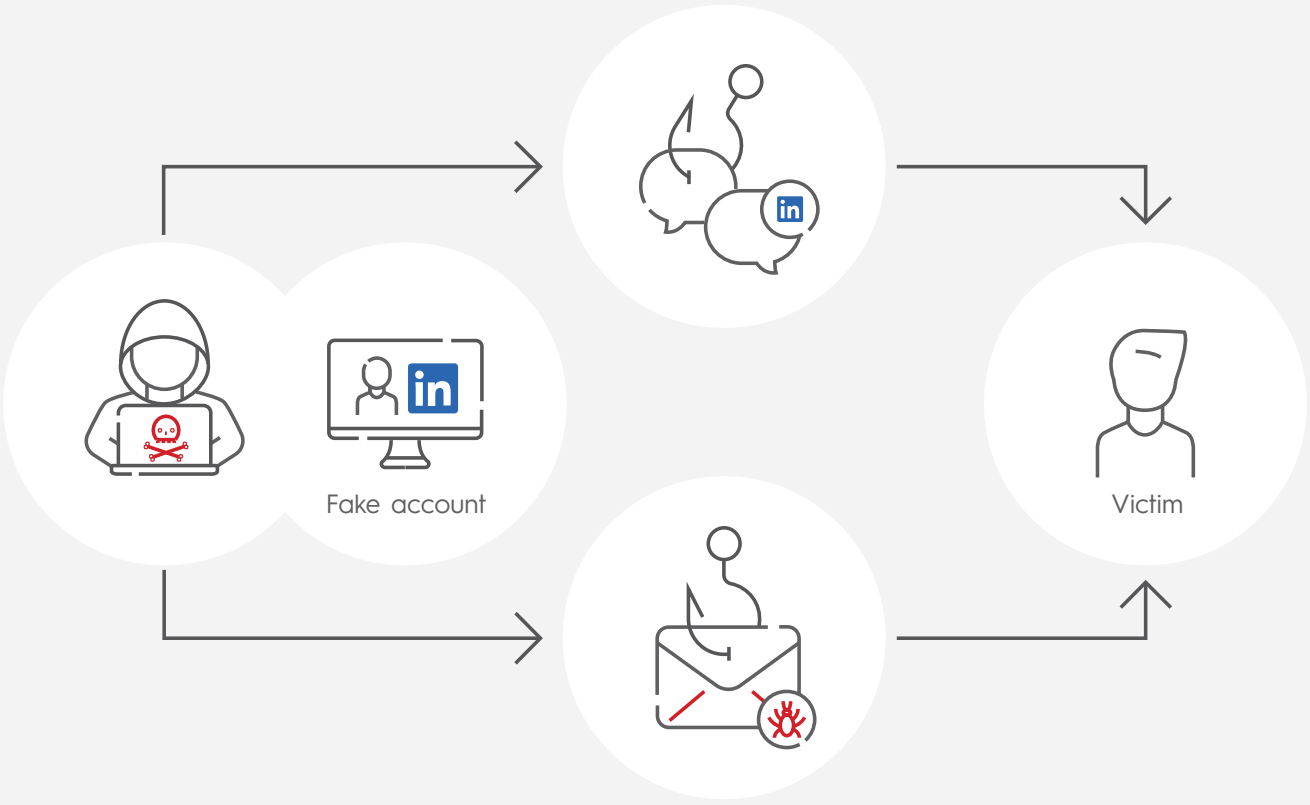
TRENDS

Phishing is an ever-evolving attack technique that has steadily increased year-on-year in phishing emails. Microsoft reports that on average 710 million emails are blocked every week by Microsoft's email security systems.

In the first half of 2022 phishing trends observed hitting Sopra Steria customers were mostly affected by world events. Phish operators are quick to adopt new e-mail templates using lures aligned with major world events such as the COVID-19 pandemic, the Beijing Olympics, and the war in Ukraine. Sopra Steria Nordics have observed examples of different lures being used such as:

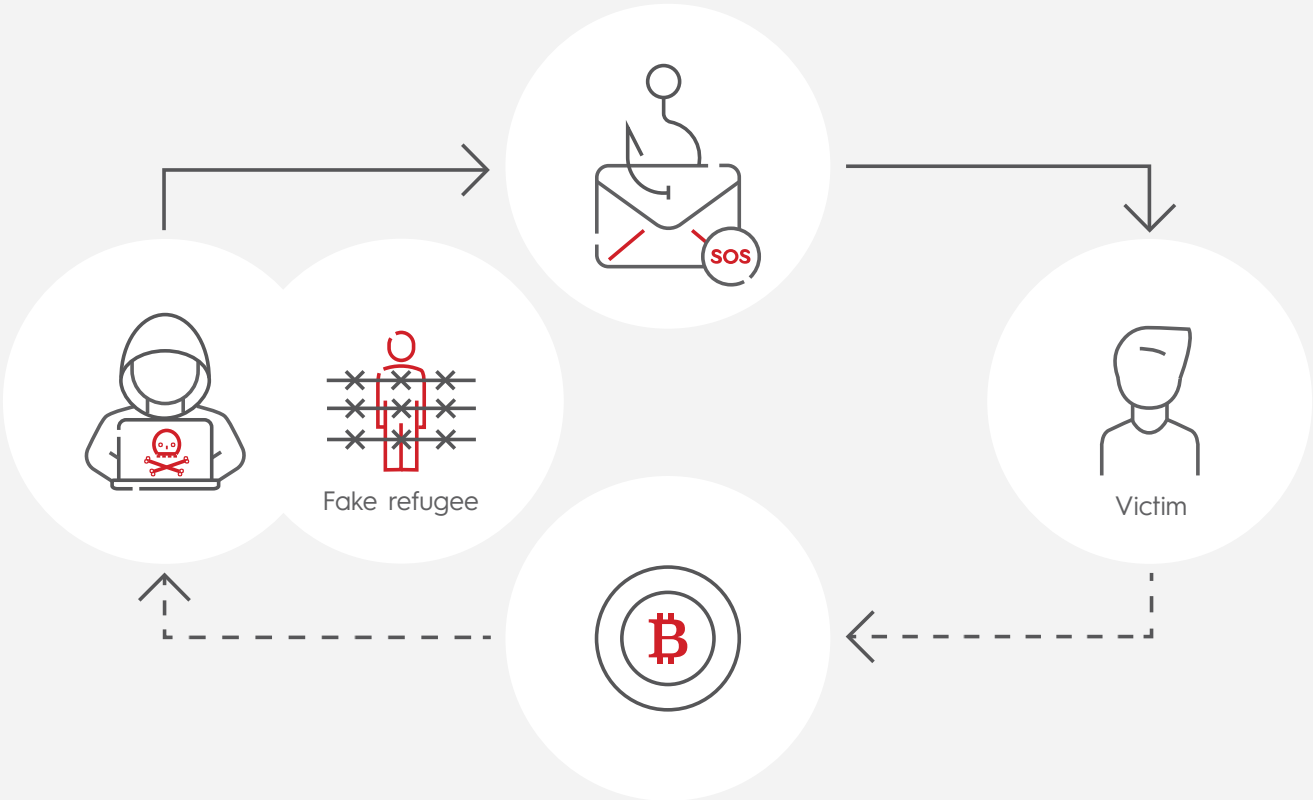
1

- A significant increase in the use of LinkedIn to masquerade phishing attacks. With both LinkedIn branded emails and with fake LinkedIn accounts to provide more credibility to the attack. These fake LinkedIn phishing attempts often claimed to have a job offer to the recipient and provide a link to a malicious site masquerading as a SharePoint site.



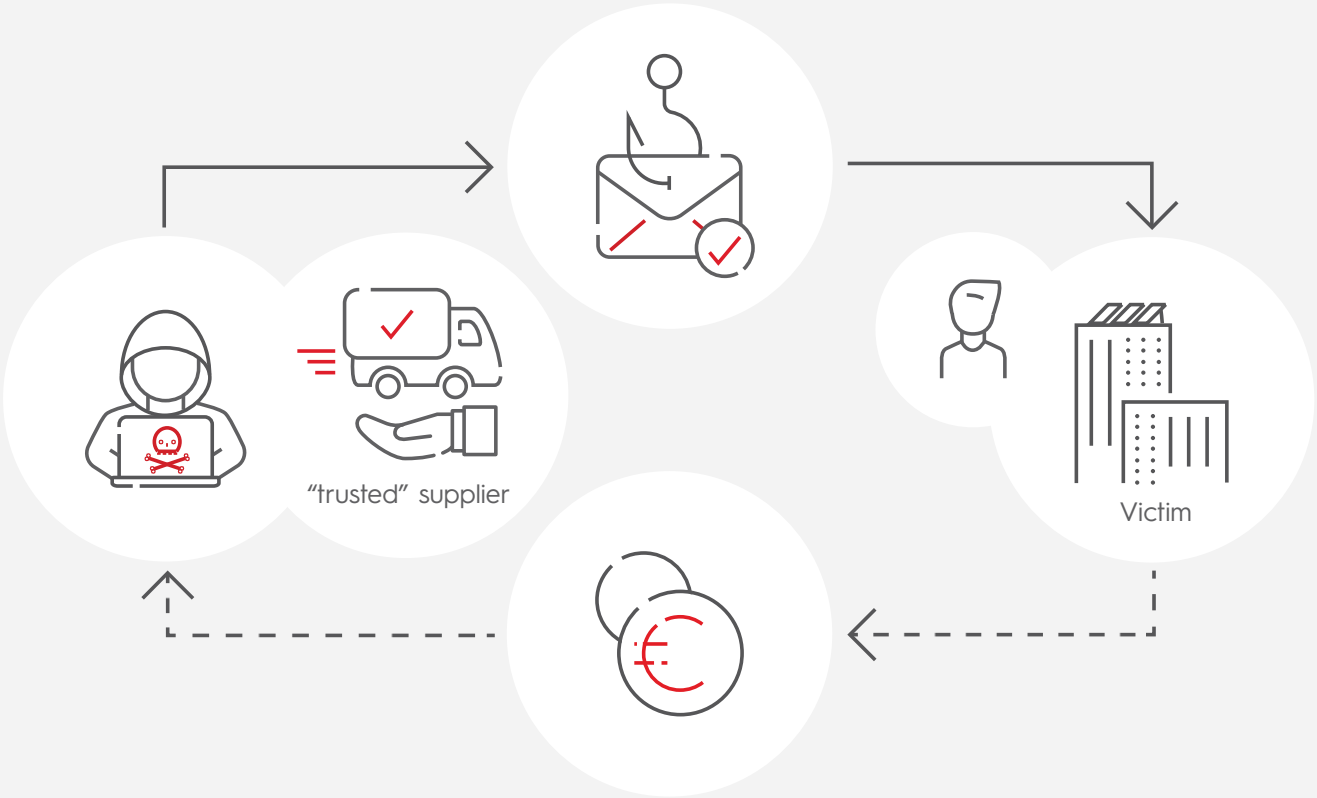
2

- Campaigns emerging with lures related to the situation in Ukraine. Multiple phishing attempts with the subject header “Help Ukraine” or similar. The threat actors were asking for donations to support Ukrainian people in need but kept any donations for themselves.
A common red flag characteristic of these phishing attacks was donation request in bitcoin.



3

- Invoice phishing lures targeting company's financial departments and private individuals in the company. The attackers often impersonate a trusted supplier, using their branding and logo, trying to make the fake invoice appear legitimate.

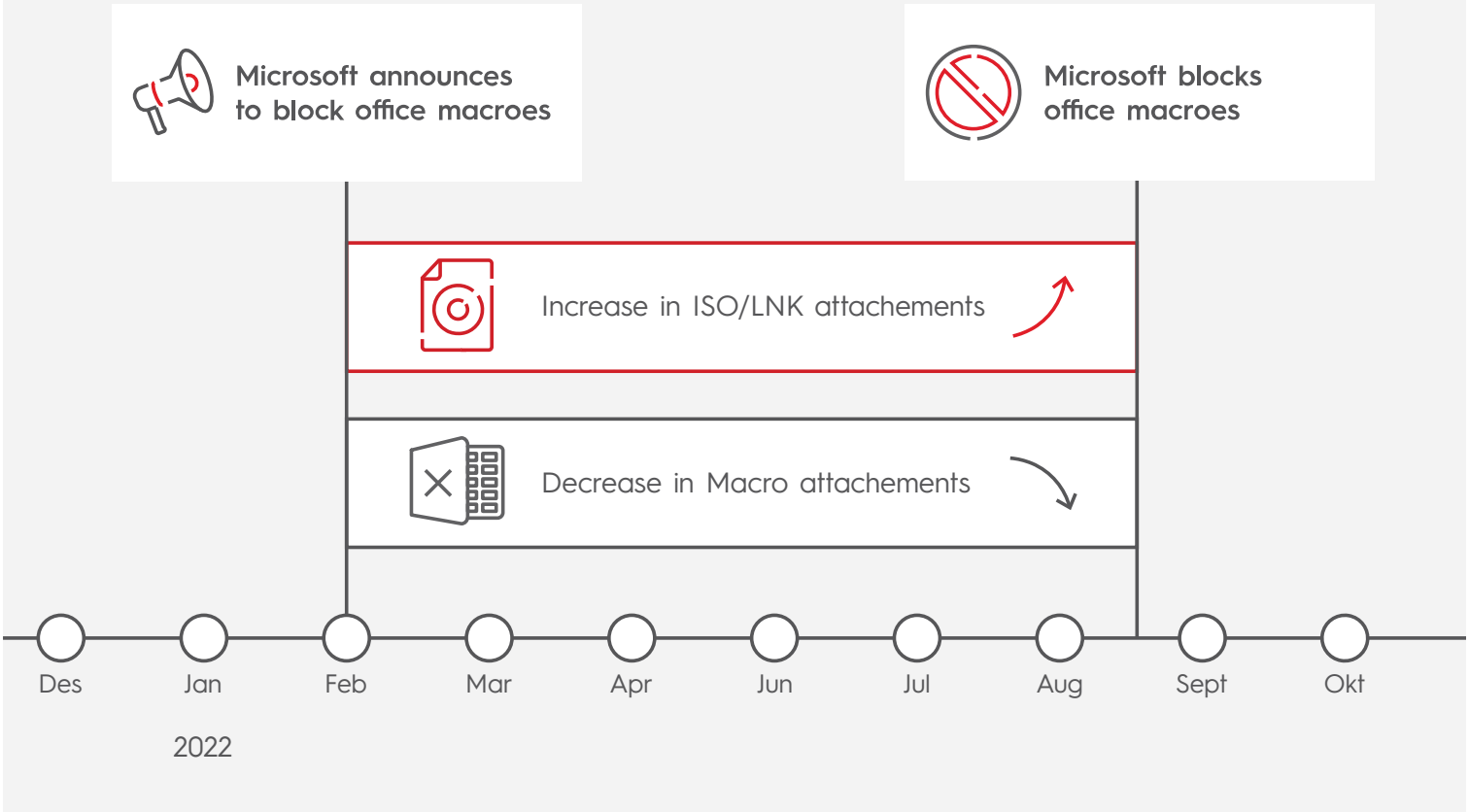


This is in addition to the steady stream of regular phishing emails containing links to fake Microsoft logins pages and malicious documents shared on well-known cloud platforms, with links attached in emails targeting end-users.

Sopra Steria Nordics customers also had their fair share of spear-phishing attempts. The most notable examples were emails that spoofed management in the company, asking staff to make a payment on their behalf with urgency. Companies most affected by these attempts are companies that share their organizational structure online, making the reconnaissance easier for any malicious actor.

MACROS AND BEYOND

In February, Microsoft announced their plans to disable macros by default to stop threat actors from abusing the feature to deliver malware via email attachments. Sopra Steria Nordics quickly observed a shift in threat actors' tactics, techniques, and procedures (TTPs).



The main difference being the obvious shift away from XLM and VBA macros in Office documents, instead we began to observe a shift to other delivery methods. The most notable example being excel documents with malicious add-ins, html attachments, zipped, and double-zipped attachments containing a variant of different files to avoid 'mark of the web' tag from Microsoft.

We have also observed an increase in malwares, such as trojans and stealers, being delivered through ISO files as mail attachments. These ISO files usually spawn LNK files (Windows shortcut files) disguised as folders that the user will open.

This method has been reported widely by the security community around the world.

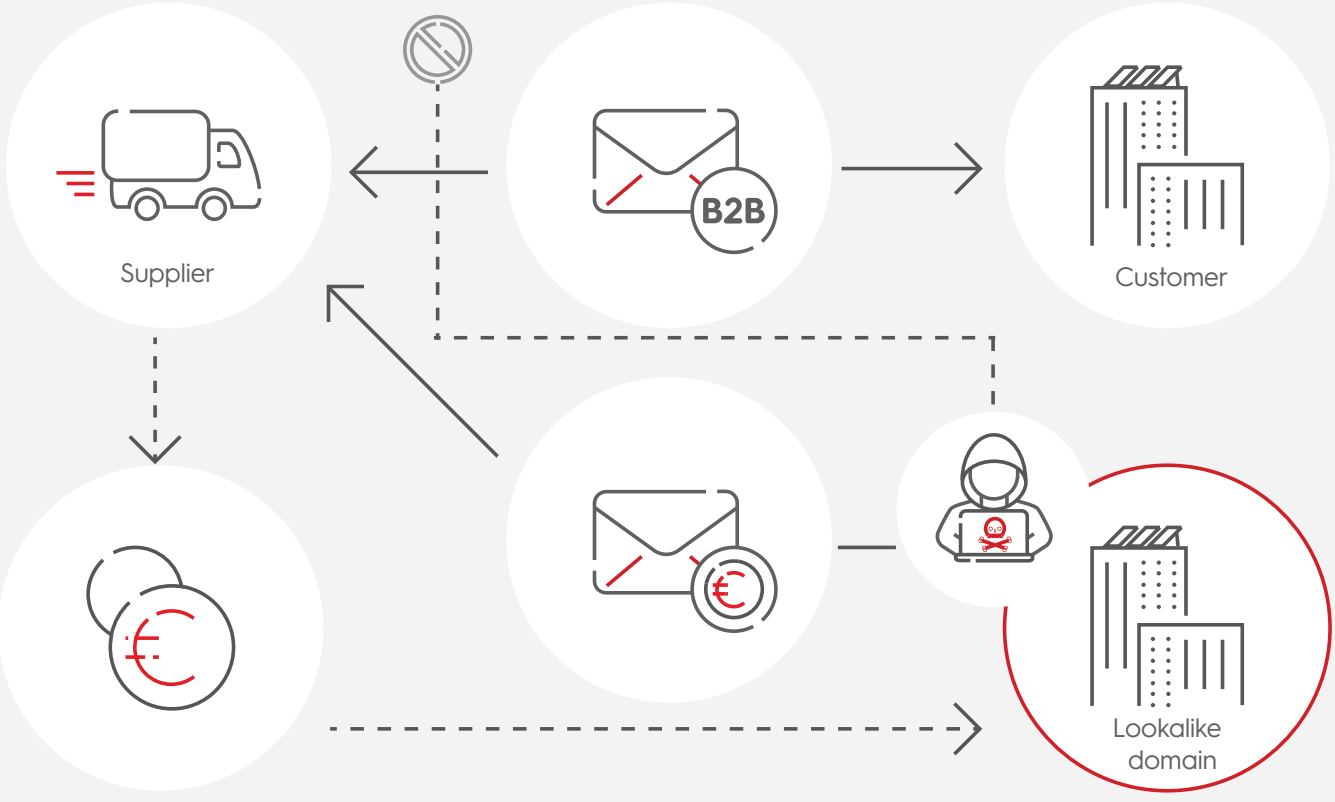
Based on number of observations, non-targeted global malicious spam campaigns continue to deliver attachments with html, zip and xls file format, and the vast majority is blocked and reported in the mail systems.

Malware delivery through ISO files is less common, but where we do observe ISO and IMG files being used is in campaigns being more targeted or at least narrower in its target selection. Phishing with malicious attachment is usually stopped in the email protection systems, but in a few cases, it has led to end-point compromise.

Business email compromise (BEC)

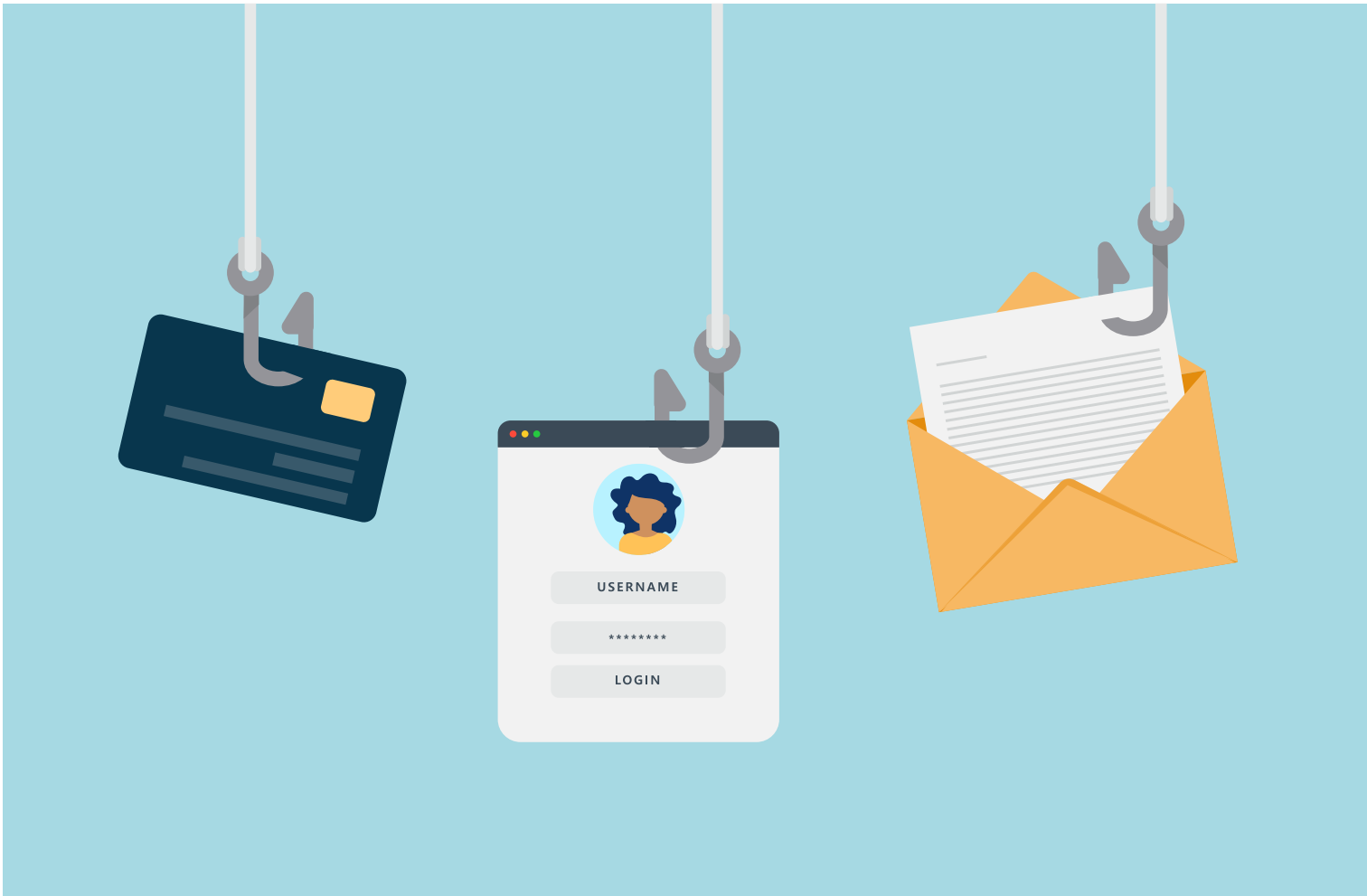
Business email compromise (BEC) is a type of cybercrime scam in which an attacker targets a business to defraud the company. As highlighted by Microsoft, BEC is the costliest financial cybercrime targeting organizations of all sizes across every industry around the world.

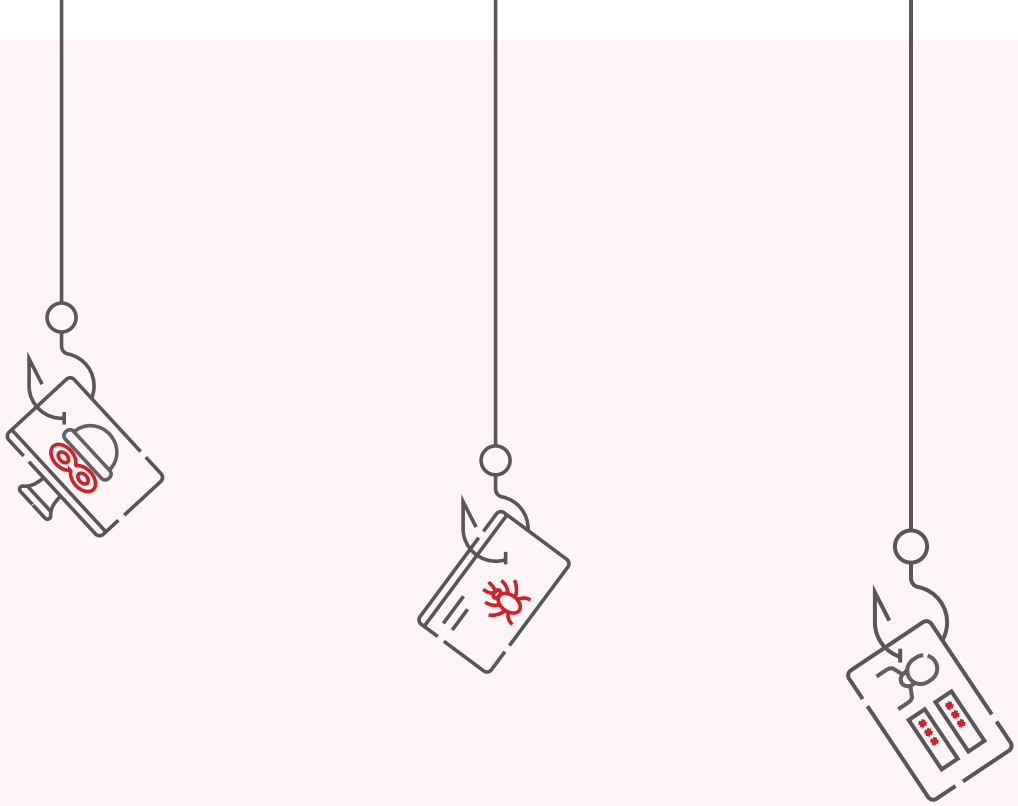
BEC attackers normally attempt to start a conversation with potential victims to build rapport. We observed an incident in November when a threat actor targeted a supplier of one of Sopra Steria Nordics customers. The threat actor managed to acquire an ongoing email correspondence between the supplier and the customer. Posing as our customer, the attacker continued the email dialogue with the supplier using a typosquatted



domain to give the appearance of key personnel being CCed in the correspondence managing to keep key staff out of the conversation. No traces of the scam were visible in our customer logs since they were out of the loop.

BEC attacks are difficult to detect because they do not use malware or malicious URLs that can be analyzed with standard cyber defenses. Instead, BEC attacks rely on impersonation and other social engineering techniques to trick people interacting with the threat actor. In this instance the threat actor additionally created several domains and emails using typosquatting to mimic our customer domain and email addresses to appear more legitimate.





Malware

Malware can be defined as software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [1]

During the last quarter of 2022, **55 percent of security incidents** handled by Sopra Steria SOC Nordics were malware related. Add potentially unwanted software (PUA) and the number is 76 percent.

A vast majority of the malware-infections are killed by EDR-tools or alerted for immediate investigation and subsequent remediation.

Throughout 2022, common malware such as WACATAC and CASUR have featured heavily across customers. They have predominantly been user-initiated after downloading malicious files.

More known malwares such as EMOTET and RASPBERRY Robin were also observed at several customers. The incidents coincided with open-source reporting on non-targeted large-scale campaigns.

[1] https://csrc.nist.gov/glossary/term/malware

Example:

In late October we reported on the Raspberry Robin malware being tracked by Microsoft as they observed Raspberry Robin being used in post-compromise activity attributed to actor DEV-0950. In July Microsoft identified samples detected as Fauppod that have similar process trees with DLLs written by Raspberry Robin LNK infections in similar locations and using similar naming conventions. Their infection chains also dropped the FakeUpdates malware. In this instance, Fauppod was delivered via GitHub, a fraudulent and malicious repository created by a cybercriminal actor that Microsoft tracks as DEV-0651. This activity was detected on endpoints belonging to customers of Sopra Steria during November. As this is a threat actor being tracked by Microsoft, the EDR agent was quick to stop and quarantine the payload before it was able to be unzipped and executed.

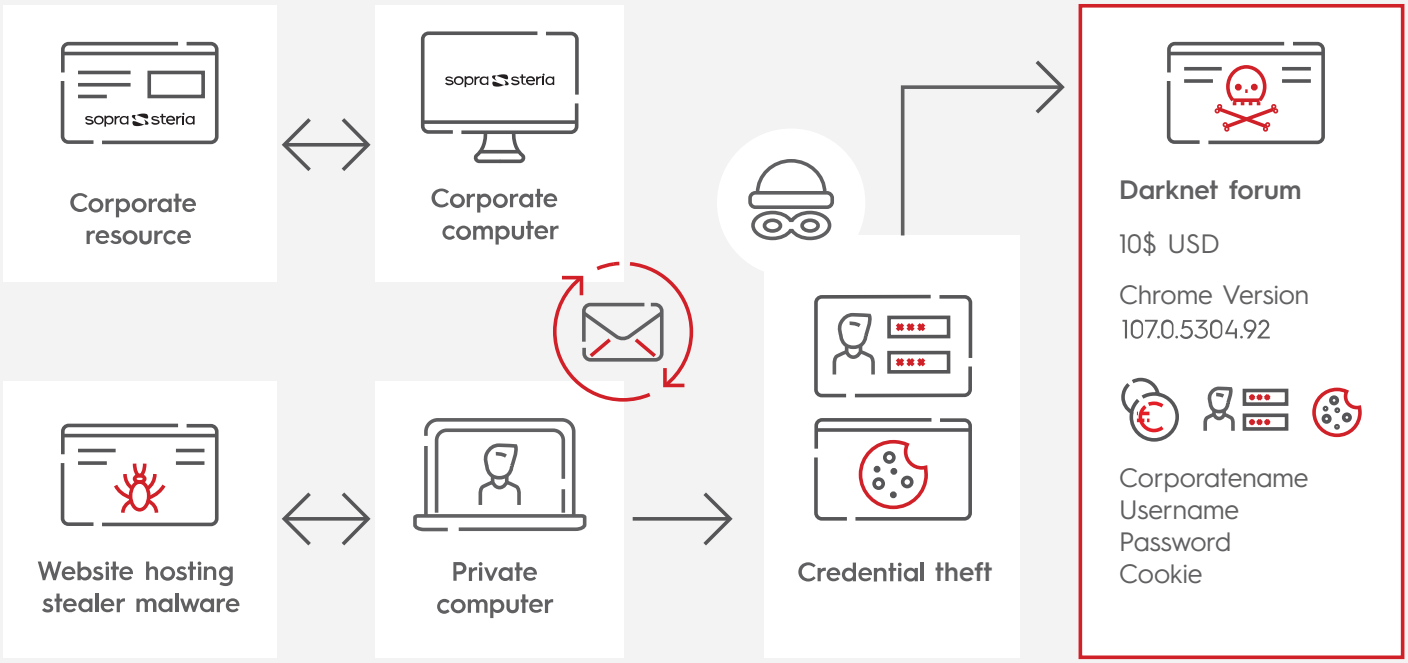
RISE OF STEALERS

Throughout 2022, Sopra Steria SOC has detected and remediated several instances of stealers found on endpoints for different customers, with the most observed being REDLINE stealer malware. Furthermore, our darknet monitoring service has alerted on multiple leaked credentials on corporate users and resources. The amount of credentials being sold on dark net forums and marketplaces is indicative of the high volume of stealer malware activity. What we typically observe in darknet forums is a post that advertise a leak with a Norwegian ISP with an updated version of chrome and a long list of credentials from what appears to be private websites, such as gaming, auctions, news, entertainment. Within a list of 100+ sites, we also observe 1-2 URLs for corporate resources.

Assessment

It is likely that most of these stealers are present on private devices where end-users have also stored corporate credentials. This becomes apparent when we look at what other credentials and URLs are bundled together with the work domain accounts. It is likely that browser sync between browser on corporate laptop and browser on private computer is the reason for data leak of corporate credentials, and that the presence of stealer on private computers is the credential theft method and subsequent listing on darknet forums.

Figure 1 The assessed theft of corporate credentials observed among customers.



THREAT ACTORS

In the annual Digital Defense Report, Microsoft highlights how the Ransomware-as-a-Service (RaaS) business-model has changed the relationship between developers of ransomware and operators, and how it makes more sense to track how the operators work in terms of tradecraft, tools and TTPs.

Throughout 2022, Sopra Steria Nordics have handled multiple incidents attributed to various affiliate threat actors. We had phishing incidents associated with DEV-0867 and their Caffeine Phishing-as-a-service (PhaaS) platform.

We also observed a case of DEV-0950 delivering Raspberry Robin. Microsoft associated DEV-0950 with an actor using Cl0p ransomware, preceded by second-stage payloads such as IcedID, Bumblebee and Truebot.

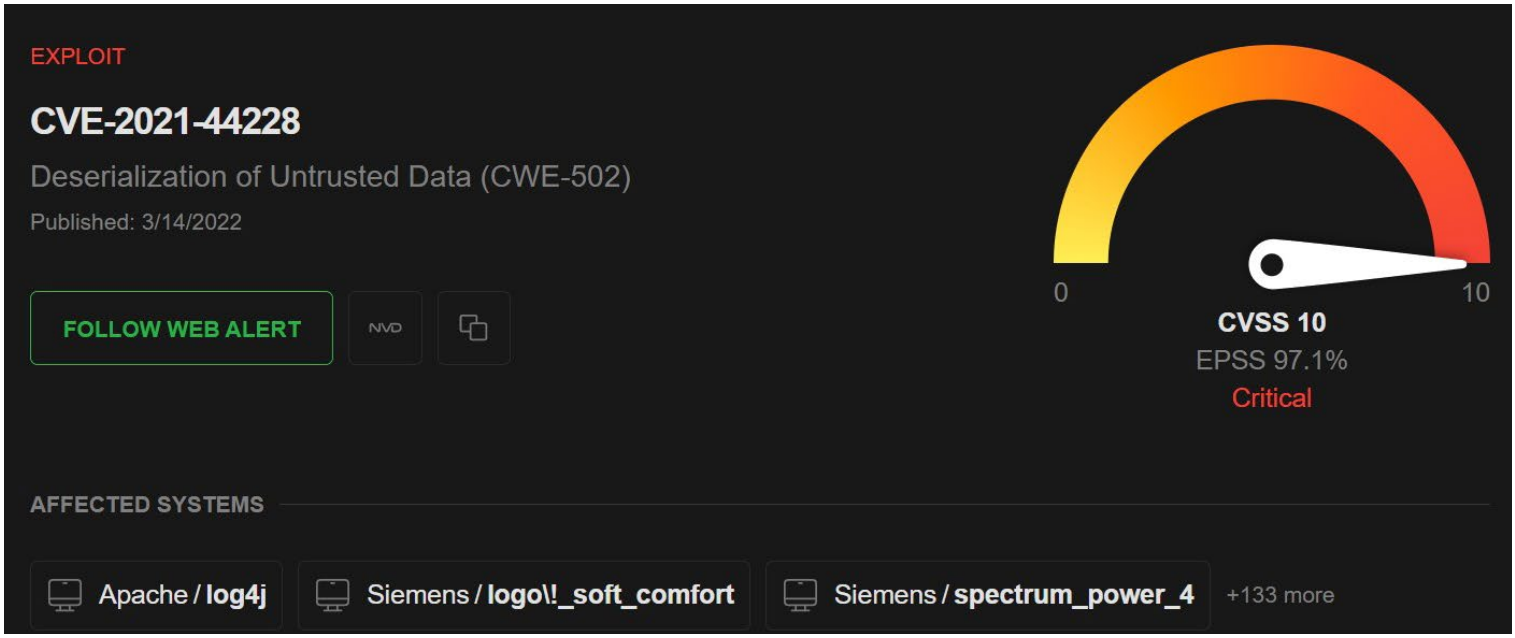
Vulnerabilities

Sopra Steria SOC Nordics continuously monitor the publication of vulnerabilities and patch releases. We use Feedly enterprise edition for open-source collection on current threats and vulnerabilities. With near real-time collection on vulnerabilities and forecast of CVSS and CWE using NLP models, we can become proactive in handling new vulnerabilities on technologies present in our customers' infrastructure.

When a new CVE emerges that is related to monitored technologies, we evaluate:

- Severity of a successful exploitation
- Proof-of-Concept available?
- Seen exploited in-the-wild?
- How exposed is the vulnerable system
- The base vulnerability metrics.
- Can it be mitigated without the patch (configuration settings, WAF and more)

Figure 2 Example of Feedly CVE insight card



Log4Shell activities dominated the first couple of months in 2022. Throughout the year, there were multiple vulnerabilities branded as "new Log4Shell", but none of them came close to the same impact as CVE-2021-44228. We continue to observe severe vulnerabilities on Exchange servers, and threat actors are quick to exploit if exposed to the internet.

Conclusion & Recommendations

Most of the cybercrime trends reported on in 2022 reflects Sopra Steria SOC observations and incidents. Malware constitute the largest category of security incidents handled by our SOC in 2022. Add potentially unwanted applications (PUA) and the number is well over two thirds of all incidents. Other featured categories include non-targeted phishing, Suspicious User Behavior and Spear-phishing. EDR-tools on servers and client are an absolute must for detecting and respond to malicious activity.

The threat from Business e-mail compromise continues to be challenging to detect due to the nature of social engineering versus the presence of malicious infrastructure or code that can be detected with standard cyber defenses.

It has been a year without any extreme vulnerabilities like Log4Shell, but it has still been important to have an efficient vulnerability management process, as critical vulnerabilities are exploited quicker than ever before. This emphasizes the importance of implementing patching or other mitigating actions shortly after the release of the vulnerability, especially if there is a proof-of-concept published.

We recommend all organizations to adhere to the NSM core principles for ICT-Security. We observe that those of our customers that operate with a high level of security maturity have fewer security incidents.

There are a couple of areas from the core principles that we would like to highlight:

Attack Surface Reduction

Several of our customers have worked diligently with attack surface reduction by implementing controls, such as preferred CIS benchmarks, best practice controls for malware/ ransomware prevention and setting ambitious targets for vulnerability management.

Once controls are in place, a successful attack surface reduction program should include capabilities and processes such as:

- Asset-based attack surface monitoring.
- External attack surface monitoring.
- Monitoring of the external vulnerability landscape, supplemented with threat intelligence and situational awareness from a Security Operations Center.
- Automated regular scanning of clients, servers and network components.
- Vulnerability telemetry categorized and followed up upon based on information from Configuration management database (CMDB) and prioritized based on exposure and criticality.

A strict policy for handling removable media

- Throughout 2022, we continued to observe malware incidents caused by infected USB-devices. Customers with stricter execution policy (such as properly configured ASR-rules in Defender) and mature processes for handling USB devices had fewer security incidents overall.

Automated detection and response of known threats

- Implementing a centralized XDR-solution such as Microsoft Defender for Endpoint or SentinelOne ensures processes, files, and network connections on endpoints (clients and servers) are monitored for malware and suspicious activity.
- A detection program should include support for both signature and heuristics-based detection.

Phishing awareness and reporting

Customers that have worked actively with security awareness and have implemented solutions for user-friendly reporting of malicious email have significant higher submission and detection rate on phishing campaigns.

Important capabilities:

- Responding to alerts on potentially malicious activity based on deployed tooling or based upon custom threat detection
- Ensure a user-friendly method for users to report suspicious e-mails that includes both verdict and feedback.

Security Operations Center

For feedback, comments orenquiries about our services, don't hesitate to contact us.

If you would like to subscribe to our weekly security newsletter, please click here.

sopra steria