Russian APT Operation: Star Blizzard

socradar.io/russian-apt-operation-star-blizzard/

26 Ocak 2024

[Update] January 30, 2024: "Official Attributions of Star Blizzard"

Within the continuously changing cyber threat landscape, the strategies of Star Blizzard unfold with a calculated precision, resembling a strategic orchestration. Spear-phishing, in this context, mirrors a carefully planned and executed maneuver. This elusive group, exhibiting a level of sophistication comparable to seasoned experts, systematically identifies specific individuals and groups as their targeted audience.

Threat actor card of Star Blizzard

By skillfully employing information tailored to captivate their targets, Star Blizzard executes the intricate steps of a spear-phishing campaign to identify individuals believed to have direct access to valuable information or serve as gateways to coveted assets.

This sophisticated adversary has targeted specific entities within academia, defense, governmental organizations, NGOs, and think-tanks.

As Star Blizzard's chilling maneuvers continue to unfold, the intricate dance of cyber warfare reveals a complex interplay of nation-state actors, each vying for supremacy in the ever-shifting landscapes of the cyber stage.

Who is Star Blizzard?

Star Blizzard, formerly recognized as **SEABORGIUM** and bearing alternative aliases like Callisto Group, TA446, COLDRIVER, TAG-53, and BlueCharlie, functions as a spear-phishing operation directly supported by the Russian government since 2019. This elusive group, akin to a digital phantom, employs a highly sophisticated approach that sets it apart in the realm of cyber threats.

The threat actor Star Blizzard exhibits a meticulous approach, utilizing social media and networking platforms to thoroughly stalk their victims. Taking the time to understand their targets, they craft **fake** email accounts and social media profiles, even going to the extent of creating deceptive websites and fake event invitations. This careful groundwork allows them to impersonate close contacts or experts convincingly.

How does the Star Blizzard Attack?

The group primarily relies on spear-phishing emails sent to personal email addresses, occasionally leveraging corporate addresses. Consequently, this fundamental approach has become emblematic of their operations as the tactic allows them to avoid the security controls on corporate networks.

The trap set by Star Blizzard involves drawing victims into a conversation through common interests. Once a rapport is established, they strategically introduce malicious links, often disguised as familiar platforms like Google Drive or OneDrive.

Reconnaissance

Leveraging openly available resources for information gathering, Star Blizzard employs reconnaissance techniques that involve scouring social media and professional networking platforms. Through this method, the hacking group identifies **entry points** to engage their targets, investing time in studying their interests and discerning their real-world social or professional connections.

Threat Actor Gathering Information (Forbes)

In an effort to maintain an air of legitimacy, Star Blizzard fabricates email accounts that mimic those of recognized contacts within the target's circle. Additionally, they craft deceptive social media and networking profiles, often posing as reputable experts. The group has been known to exploit the guise of conference or event invitations to lure their targets into their traps.

During their initial contact, Star Blizzard utilizes email addresses from various providers, such as Outlook, Gmail, Yahoo, and Proton Mail. These addresses are carefully selected to **impersonate** either known contacts of the target or well-established figures within the target's specific field or sector.

In a bid to further enhance their credibility, the threat actors go the extra mile by creating malicious domains that closely resemble legitimate organizations, adding an additional layer of authenticity to their deceptive tactics.

Evasion

As their primary strategy involves infiltrating through phishing emails, they also adapt their evasion maneuvers in accordance with this tactic. The actors deliberately opt for personal email addresses as a strategic move to bypass the security measures implemented on corporate networks.

Trust-Forging Tactics

Star Blizzard invests significant effort in researching the interests and connections of their targets to construct an approach that appears legitimate. Subsequently, the group initiates the process of cultivating trust by establishing seemingly harmless contact. This initial interaction usually revolves around a topic carefully chosen to engage the targets. Notably, during this phase, Star Blizzard refrains from engaging in any malicious activities, focusing solely on **building rapport** with their targets.


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).

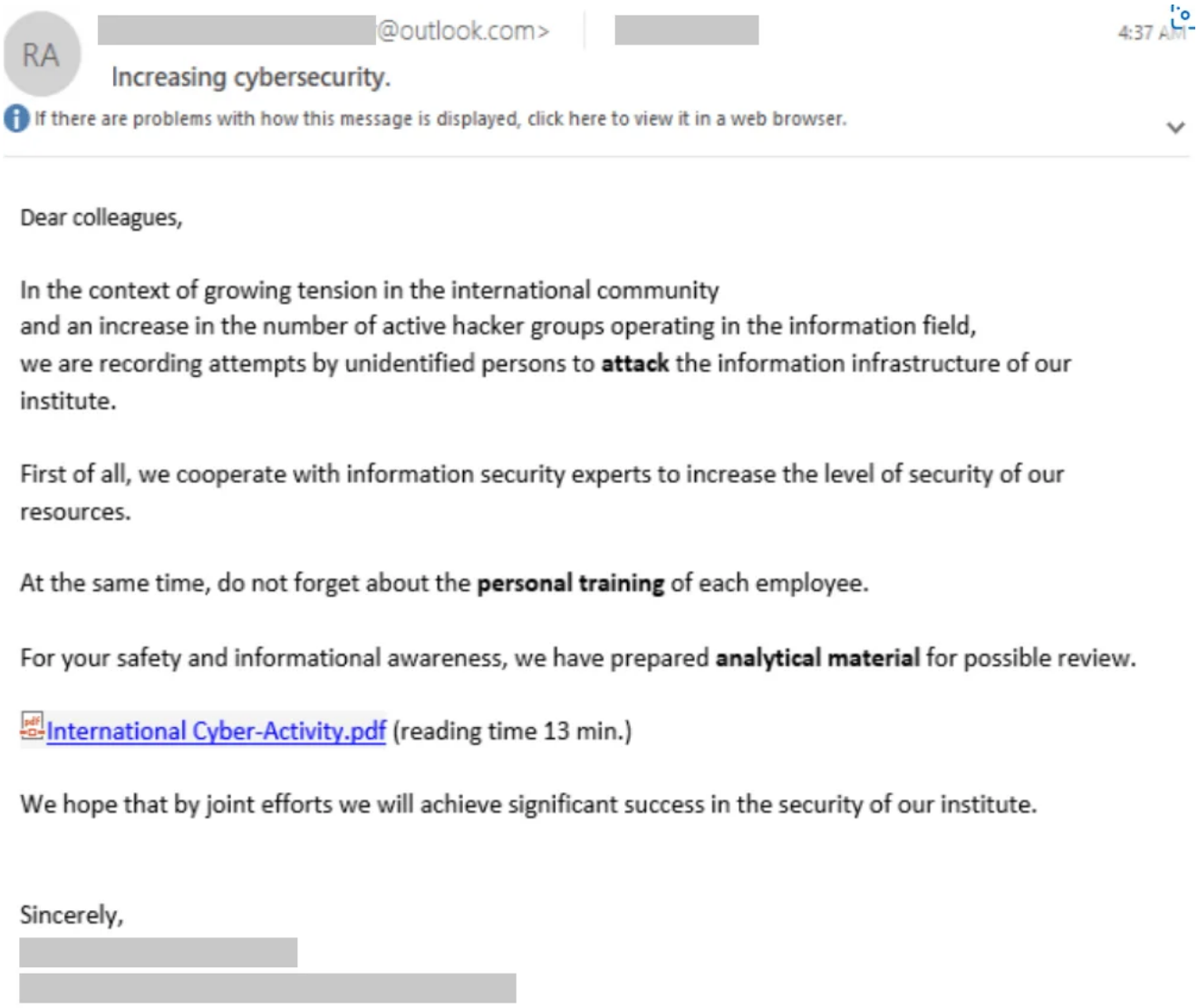
Contact by Threat Actors (Microsoft)

Once they are assured that the necessary rapport has been established, they proceed to launch their attacks. This method involves ongoing correspondence between the attackers and the targets, sometimes spanning an extended period to solidify the rapport.

The Delivery

After successfully building trust, Star Blizzard employs standard phishing techniques by sharing a link that seemingly directs the target to a document or website of interest. This link, however, leads to a server controlled by the attackers, coercing the target to input their account credentials.

The malicious link can manifest as a URL embedded in an email message, or the attacker might incorporate a link within a document hosted on platforms such as OneDrive, Google Drive, or other file-sharing services.



The Delivery of the Malicious File (Microsoft)

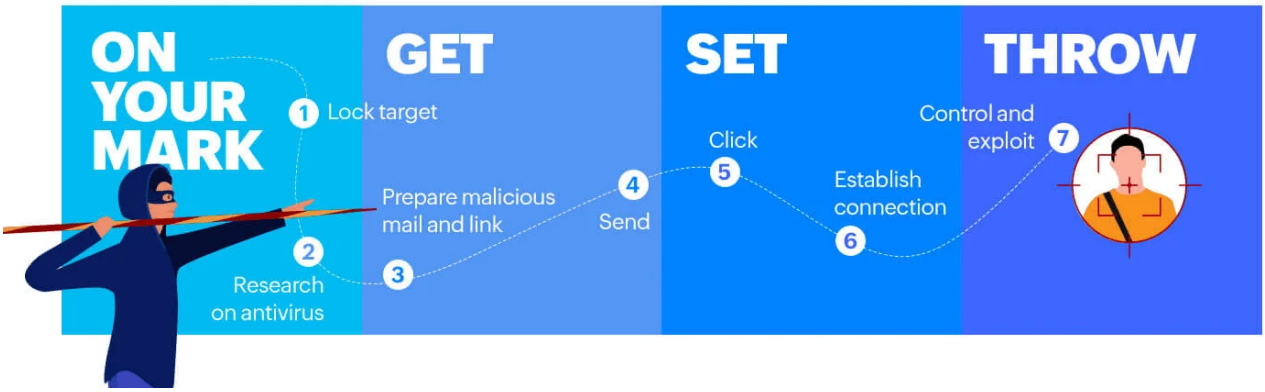
In their spear-phishing endeavors, Star Blizzard utilizes the open-source framework EvilGinx, enabling them to harvest credentials and session cookies. This strategic use of EvilGinx proves effective in circumventing the protective measures of **two-factor authentication**.

Exploitation

Regardless of the chosen delivery method, when the target clicks on the **malicious URL**, they are redirected to a server controlled by Star Blizzard. This server replicates the sign-in page of a legitimate service. Any credentials entered on this deceptive page become compromised at this stage.

Subsequently, Star Blizzard employs the obtained credentials to gain unauthorized access to the target's email account.

The actors have further utilized their access to a victim's email account to extract mailing-list data and the victim's contacts list. This acquired information is then exploited for subsequent targeted activities. Additionally, compromised email accounts have been employed by Star Blizzard for extended phishing campaigns.

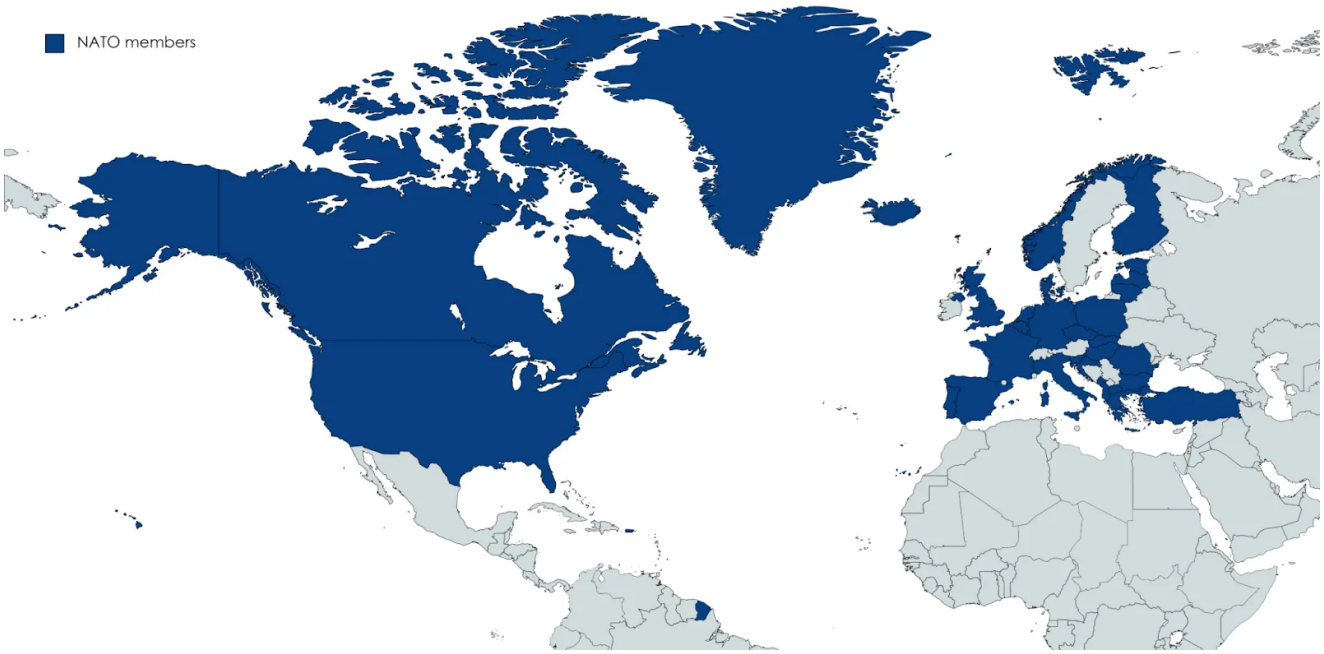


Stages of Spear-Phishing (ManageEngine)

Illustration of Threat Actors, Targeting Intergovernmental Organizations (Created with Pixlr)

Target Countries:

Star Blizzard has orchestrated campaigns with a geographical emphasis on **NATO** countries, particularly the United States and the United Kingdom. However, the threat actor's reach extends to other nations in the Baltics, the Nordics, and Eastern Europe. A notable instance involves targeting the government sector of Ukraine in the months leading up to the invasion by Russia. Despite engaging with organizations supporting the war in Ukraine, Microsoft's assessment suggests that Ukraine may not be the primary focus for Star Blizzard; rather, it appears to be a reactive focus area within a broader array of diverse targets.



NATO Member Countries, Targeted by Star Blizzard (Wikipedia)

Official Attributions of Star Blizzard

United States Government Reports

The U.S. Department of Justice (DOJ) indicted Ruslan Aleksandrovich Peretyatko and Andrey Stanislavovich Korinets for their global computer intrusion campaign involvement. Both individuals, working with Russia's Federal Security Service (FSB), have been charged with hacking into networks across several countries, including the USA, on behalf of the Russian government.

The Department of the Treasury and the UK have sanctioned these individuals for their role in an Advanced Persistent Threat (APT) group sponsored by the FSB. The National Security Agency (NSA) has released a **Cybersecurity Advisory** to raise awareness of the spear-phishing techniques used by Star Blizzard. The State Department's Rewards for Justice program has highlighted the involvement of Peretyatko and Korinets in spear-phishing campaigns targeting U.S. government networks and defense contractors.

United Kingdom's Response

The UK government also has exposed attempts by the FSB to interfere in its political processes, with Star Blizzard being a key player in these efforts. The Foreign, Commonwealth, and Development Office has sanctioned individuals involved in the group's activity, including Peretyatko and Korinets. The UK National Cyber Security Centre (NCSC) aligns with the U.S. in assessing Star Blizzard as subordinate to the Russian FSB Centre 18.

Conclusion

Star Blizzard stands as a formidable cyber adversary, employing a sophisticated spear-phishing strategy to strategically target diverse sectors and geographies. With a pronounced focus on **NATO** countries, particularly the US and the UK, and a reactive interest in Ukraine during geopolitical events, the threat actor's diverse range of targets includes defense companies, NGOs, IGOs, think tanks, and individuals with Russian affairs expertise. Vigilance is paramount for those previously targeted, as understanding Star Blizzard's tactics is crucial for fortifying defenses against their persistent cyber threats. The upcoming section will provide essential security recommendations to safeguard against Star Blizzard's multifaceted activities.

The next section will provide security recommendations to defend against Star Blizzard's activities.

Recommendations: Guarding Against Star Blizzard

Defensive strategies are crucial for effectively avoiding the malicious activities of threat actors like Star Blizzard. In this context, individuals and organizations should not only implement comprehensive cybersecurity measures but also be diligent in identifying potential threat elements and cultivating awareness of cybersecurity threats. This is essential to adapt to the dynamic changes in the cybersecurity landscape and internalize a proactive stance against threats posed by entities such as Star Blizzard.

Phishing Awareness: Raise cyber threat awareness, recognizing that spear-phishing emails are meticulously crafted to evade suspicion. Verify the legitimacy of emails by scrutinizing sender addresses, especially when they deviate from typical corporate email addresses. Be cautious if an email is directed to your personal/webmail address rather than your corporate one, and validate the email's authenticity through alternative means.

Password Creation: Utilize robust password practices by employing unique and strong passwords, particularly avoiding the reuse of passwords across various services.

Using MFA: Implement multi-factor authentication (MFA), also known as 2-factor authentication (2FA) or two-step verification, to mitigate the impact of potential password compromises.

Device and Network Protection: Safeguard your devices and networks by ensuring they are consistently updated with the latest supported versions. Promptly apply security updates, employ antivirus software, and conduct regular scans to fortify defenses against known malware threats.

Automated Email Scanning: Activate automated email scanning features provided by your email service providers, as these are typically enabled by default for consumer mail services. Check out our Email Threat Analyzer.

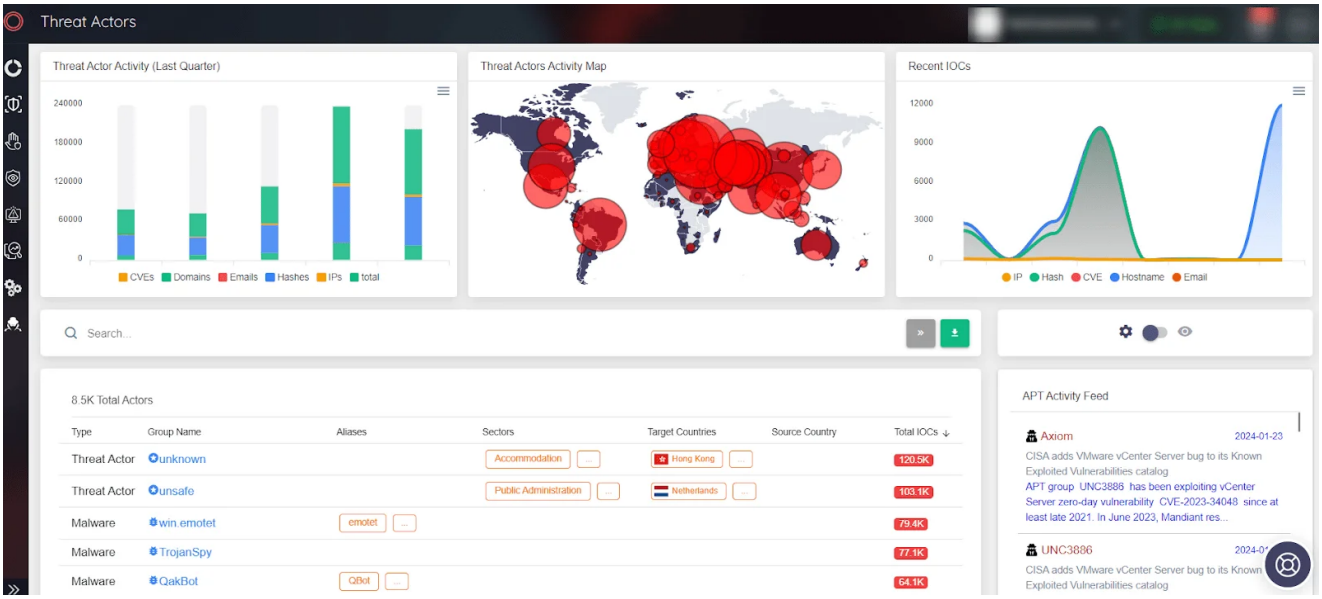
Mail Forwarding Rules: Disable mail-forwarding capabilities, as threat actors have been observed using this tactic to maintain visibility of target emails. Regularly monitor settings to ensure that external malicious actors have not established unauthorized mail-forwarding rules, or, if disabling is not feasible, take proactive measures to regularly assess and thwart potential forwarding rule setups by external entities.

Data Breach Protocols: Ensure that data breach protocols are in place and comply with legal and regulatory requirements pertaining to data exposure and leaks. For more information, you can visit our Account Breach Checker.

Notification Procedures: Establish procedures to notify affected parties and relevant authorities in the event of a data breach.

Utilize Threat Intelligence: Leverage cyber threat intelligence to gain insights into the Tactics, Techniques, and Procedures (TTPs) employed by Star Blizzard.

SOCRadar's Insights: Utilize SOCRadar Threat Actor/Malware to stay abreast of the latest developments and threats posed by threat actors like the Star Blizzard Group, ensuring that defenses are continually updated and fortified against emerging threats.



SOCRadar Threat Actor page

MITRE ATT&CK Tactic Table of Star Blizzard

TTP Table, as shared by NCSC:

MITRE ATT&CK Tactic	MITRE ATT&CK Technique	Description
Reconnaissance	T1593: Search Open Websites/Domains	Star Blizzard uses open-source research and social media to identify information about victims to use in targeting.
Reconnaissance	T1589: Gather Victim Identity Information	Star Blizzard uses online data sets and open-source resources to gather information about their targets.
Resource Development	T1585.001: Establish Accounts: Social Media Accounts	Star Blizzard has been observed establishing fraudulent profiles on professional networking sites to conduct reconnaissance.
Resource Development	T1585.002: Establish Accounts: Email Accounts	Star Blizzard registers consumer email accounts matching the names of individuals they are impersonating to conduct spear-phishing activity.
Resource Development	T1583.001: Acquire Infrastructure: Domains	Star Blizzard registers domains to host their phishing framework.
Resource Development	T1586.002: Compromise Accounts: Email Accounts	Star Blizzard has been observed using compromised victim email accounts to conduct spear-phishing activity against contacts of the original victim.
Initial Access	T1078: Valid Accounts	Star Blizzard uses compromised credentials, captured from fake log-in pages, to log in to valid victim user accounts.
Initial Access	T1566.001: Phishing: Spear-phishing Attachment	Star Blizzard uses malicious links embedded in email attachments to direct victims to their credential-stealing sites.
Initial Access	T1566.002: Phishing: Spear-phishing Link	Star Blizzard sends spear-phishing emails with malicious links directly to credential-stealing sites, or to documents hosted on a file- sharing site, which then direct victims to credential-stealing sites.
Defence Evasion	T1550.004: Use Alternate Authentication Material: Web Session Cookie	Star Blizzard bypasses multi-factor authentication on victim email accounts by using session cookies stolen using EvilGinx.

Credential Access	T1539: Steal Web Session Cookie	Star Blizzard uses EvilGinx to steal the session cookies of victims directed to their fake log-in domains. For more information visit our blog.
Collection	T1114.002: Email Collection: Remote Email Collection	Star Blizzard interacts directly with externally facing Exchange services, Office 365 and Google Workspace to access email and steal information using compromised credentials or access tokens.
Collection	T1114.003: Email Collection: Email Forwarding Rule	Star Blizzard abuses 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.

Star Blizzard IoCs

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

document-forwarding[.]com	Domain	High	
document-online[.]live	Domain	High	
document-preview[.]com	Domain	High	
documents-cloud[.]com	Domain	High	Sekoia.io
documents-cloud[.]online	Domain	High	Sekoia.io
documents-forwarding[.]com	Domain	High	Google TAG
document-share[.]live	Domain	High	
documents-online[.]live	Domain	High	
documents-pdf[.]online	Domain	High	Sekoia.io
documents-preview[.]com	Domain	High	Google TAG
documents-view[.]live	Domain	High	
document-view[.]live	Domain	High	
drive-docs[.]com	Domain	High	Sekoia.io
drive-share[.]live	Domain	High	Google TAG, Sekoia.io
goo-link[.]online	Domain	High	
hypertextteches[.]com	Domain	High	Sekoia.io
mail-docs[.]online	Domain	High	
officeonline365[.]live	Domain	High	
online365-office[.]com	Domain	High	
online-document[.]live	Domain	High	
online-storage[.]live	Domain	High	
pdf-cache[.]com	Domain	High	
pdf-cache[.]online	Domain	High	
pdf-docs[.]online	Domain	High	Sekoia.io
pdf-forwarding[.]online	Domain	High	
protection-checklinks[.]xyz	Domain	High	

protection-link[.]online	Domain	High	
protectionmail[.]online	Domain	High	Sekoia.io
protection-office[.]live	Domain	High	Google TAG, Sekoia.io
protect-link[.]online	Domain	High	Google TAG, Sekoia.io
proton-docs[.]com	Domain	High	Sekoia.io
proton-reader[.]com	Domain	High	
proton-viewer[.]com	Domain	High	Google TAG, Sekoia.io
relogin-dashboard[.]online	Domain	High	
safe-connection[.]online	Domain	High	
safelinks-protect[.]live	Domain	High	
secureoffice[.]live	Domain	High	
webresources[.]live	Domain	High	Google TAG
word-yand[.]live	Domain	High	
yandx-online[.]cloud	Domain	High	
y-ml[.]co	Domain	High	
docs-drive[.]online	Domain	Moderate	Sekoia.io
docs-info[.]online	Domain	Moderate	
cloud-mail[.]online	Domain	Moderate	
onlinecloud365[.]live	Domain	Moderate	
pdf-cloud[.]online	Domain	Moderate	Sekoia.io
pdf-shared[.]online	Domain	Moderate	Sekoia.io
proton-pdf[.]online	Domain	Moderate	
proton-view[.]online	Domain	Moderate	Sekoia.io
office365-online[.]live	Domain	Low	
doc-viewer[.]com	Domain	Low	
file-milgov[.]systems	Domain	Low	Sekoia.io

office-protection[.]online	Domain	Low	Sekoia.io

PROTECTION OF PERSONAL DATA COOKIE POLICY FOR THE INTERNET SITE

Protecting your personal data is one of the core principles of our organization, SOCRadar, which operates the internet site (www.socradar.com). This Cookie Usage Policy ("Policy") explains the types of cookies used and the conditions under which they are used to all website visitors and users.

Cookies are small text files stored on your computer or mobile device by the websites you visit.

Cookies are commonly used to provide you with a personalized experience while using a website, enhance the services offered, and improve your overall browsing experience, contributing to ease of use while navigating a website. If you prefer not to use cookies, you can delete or block them through your browser settings. However, please be aware that this may affect your usage of our website. Unless you change your cookie settings in your browser, we will assume that you accept the use of cookies on this site.

1. WHAT KIND OF DATA IS PROCESSED IN COOKIES?

Cookies on websites collect data related to your browsing and usage preferences on the device you use to visit the site, depending on their type. This data includes information about the pages you access, the services and products you explore, your preferred language choice, and other preferences.

2. WHAT ARE COOKIES AND WHAT ARE THEIR PURPOSES?

Cookies are small text files stored on your device or web server by the websites you visit through your browsers. These small text files, containing your preferred language and other settings, help us remember your preferences on your next visit and assist us in making improvements to our services to enhance your experience on the site. This way, you can have a better and more personalized user experience on your next visit.

The main purposes of using cookies on our Internet Site are as follows:

- Improve the functionality and performance of the website to enhance the services provided to you,
- Enhance and introduce new features to the Internet Site and customize the provided features based on your preferences,
- Ensure legal and commercial security for the Internet Site, yourself, and the Organization, and prevent fraudulent transactions through the Site,
- Fulfill legal and contractual obligations, including those arising from Law No. 5651 on the Regulation of Publications on the Internet and the Fight Against Crimes Committed Through These Publications, as well as the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet.

3. TYPES OF COOKIES USED ON OUR INTERNET SITE 3.1. Session Cookies

Session cookies ensure the smooth operation of the internet site during your visit. They are used for purposes such as ensuring the security and continuity of our sites and your visits. Session cookies are temporary cookies and are deleted when you close your browser; they are not permanent.

3.2. Persistent Cookies

These cookies are used to remember your preferences and are stored on your device through browsers. Persistent cookies remain stored on your device even after you close your browser or restart your computer. These cookies are stored in your browser's subfolders until deleted from your browser's settings. Some types of persistent cookies can be used to provide personalized recommendations based on your usage purposes.

With persistent cookies, when you revisit our website with the same device, the website checks if a cookie created by our website exists on your device. If so, it is understood that you have visited the site before, and the content to be presented to you is determined accordingly, offering you a better service.

3.3. Mandatory/Technical Cookies

Mandatory cookies are essential for the proper functioning of the visited internet site. The purpose of these cookies is to provide necessary services by ensuring the operation of the site. For example, they allow access to secure sections of the internet site, use of its features, and navigation.

3.4. Analytical Cookies

These cookies gather information about how the website is used, the frequency and number of visits, and show how visitors navigate to the site. The purpose of using these cookies is to improve the operation of the site, increase its performance, and determine general trend

directions. They do not contain data that can identify visitors. For example, they show the number of error messages displayed or the most visited pages.

3.5. Functional Cookies

Functional cookies remember the choices made by visitors within the site and recall them during the next visit. The purpose of these cookies is to provide ease of use to visitors. For example, they prevent the need to re-enter the user's password on each page visited by the site user.

3.6. Targeting/Advertising Cookies

They measure the effectiveness of advertisements shown to visitors and calculate how many times ads are displayed. The purpose of these cookies is to present personalized advertisements to visitors based on their interests.

Similarly, they determine the specific interests of visitors' navigation and present appropriate content. For example, they prevent the same advertisement from being shown again to the visitor in a short period.

4. HOW TO MANAGE COOKIE PREFERENCES?

To change your preferences regarding the use of cookies, block or delete cookies, you only need to change your browser settings.

Many browsers offer options to accept or reject cookies, only accept certain types of cookies, or receive notifications from the browser when a website requests to store cookies on your device.

Also, it is possible to delete previously saved cookies from your browser.

If you disable or reject cookies, you may need to manually adjust some preferences, and certain features and services on the website may not work properly as we will not be able to recognize and associate with your account. You can change your browser settings by clicking on the relevant link from the table below.

5. EFFECTIVE DATE OF THE INTERNET SITE PRIVACY POLICY

The Internet Site Privacy Policy is dated The effective date of the Policy will be updated if the entire Policy or specific sections are renewed. The Privacy Policy is published on the Organization's website (www.socradar.com) and made accessible to relevant individuals upon request.

SOCRadar
Address: 651 N Broad St, Suite 205 Middletown, DE 19709 USA
Phone: +1 (571) 249-4598
Email:
Website: www.socradar.com