EuRepoC

ADVANCED PERSISTENT THREAT profile

Gamaredon

Russian Intelligence Preparation of the Battlefield in Ukraine

Associated APT designations

- **Gamaredon Group** (LookingGlass, ESET)
- **ACTINIUM/ DEV-0157** (Microsoft)
- **BlueAlpha** (Recorded Future)
- **Dancing Salome** (Kaspersky)
- **G0047** (MITRE ATT&CK)
- **Iron Tilden** (Secureworks)
- **Primitive Bear** (CrowdStrike)
- **Shuckworm** (Symantec)
- **Trident Ursa** (UNIT 42/Palo Alto)
- **UAC-0010** (CERT-UA)
- **Winterflouder** (iDefence)

Sources: [1] [2] [3] [4] [5]

Country of origin

Time period of activity

June 2013-today

Industry reporting traces the group's operations back to June 2013, only months before the Russian annexation of the Crimean Peninsula.

Sources: [6]

Political affiliations

The Ukrainian Security Service (SSU) has tied Gamaredon Group to the Russian domestic security service FSB, more specifically to its 16th Centre, which comprises the agency's primary electronic and signals intelligence assets, and the 18th Centre, which operates as the Information Security Centre. The first public industry reporting on the group by LookingGlass aligned with these findings. A Cybersecurity Advisory jointly released by the cybersecurity authorities of Australia, Canada, New Zealand, the UK, and the US in April 2022 acknowledged links of Gamaredon Group to the FSB identified by industry. However, states of the Five Eyes intelligence alliance have not publicly directly associated the group with the Russian government.

Sources [2] [6] [7] [20] [26]

By Kerstin Zettl-Schabath, Jakob Bund, Lena Rottinger and Camille Borrett
January 2023

Agency type

State-integrated hacking group (intelligence service/agency members). Government and industry reporting has identified Gamaredon as Russia-nexus agent that operates in close alignment with Russian state interests in Ukraine. Ukraine's main intelligence agency SSU explicitly linked the group to the FSB, personally identifying five members known to be officers of Russia's security service.

Sources [2] [7]

Most frequent targets:

 **Ukraine** Sources [2] [3]

Group composition/organisational structure

In detailed revelations about the group's operational structure in November 2021, the SSU characterised the group as being coordinated by the FSB's 18th Centre and composed of regular service officers stationed in the occupied Autonomous Republic of Crimea and Sevastopol that had been joined by former Ukrainian law enforcement members. Based on this account, the unit forms part of the 4th Section of the Counterintelligence Operations Service within the FSB field office in occupied Crimea. The SSU report identifies five FSB officers presumed to form part of Gamaredon by name and function, including the group's leadership:

- Sklianko Oleksandr Mykolaiovych
  Deputy Chief, 4th Section of the Counterintelligence Operations Service (SCO), FSB Department in occupied Crimea and Sevastopol
- Chernykh Mykola Serhiiovych
  Head of the unit identified as responsible for conducting Gamaredon operations, 4th Section of the SCO, FSB Department in occupied Crimea and Sevastopol
- Starchenko Anton Oleksandrovych
  Officer within the unit identified as responsible for conducting Gamaredon operations, 4th Section of the SCO, FSB Department in occupied Crimea and Sevastopol
- Miroshnychenko Oleksandr Valeriiovych
  Officer within the unit identified as responsible for conducting Gamaredon operations, 4th Section of the SCO, FSB Department in occupied Crimea and Sevastopol
- Sushchenko Oleh Oleksandrovych
  Officer within the unit identified as responsible for conducting Gamaredon operations, 4th Section of the SCO, FSB Department in occupied Crimea and Sevastopol

Sources [7] [16]

Impact type(s)

Direct

Intelligence and military/geopolitical impact (gathering sensitive information to gain strategic advantages for conventional operations in a military conflict)

Sources [2] [9] [10]

Incident type(s)

Data Theft (cyber espionage against military targets, as well as political and government institutions, especially in Ukraine).

Sources [1] [8]

Threat Level Index

11/24 moderate threat level

Index scoring scale

Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the **sectorial** and **geographical scope** of the APT's attacks, the **intensity** of the attacks, the **frequency** of attacks and the **use of zero-days**. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here and here.

Breakdown of the scores for Gamaredon:

Sub-indicator	Score	Explanation
Intensity of attacks	1 /5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	8 /8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. In the case of Gamaredon, on average attacks attributed to the group within the EuRepoC database, targeted three different sectors per attack. In addition, all attacks were against political systems and/or critical infrastructure.
Geographical scope of attacks	1 /4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of Gamaredon, the only targeted country was Ukraine.
Frequency of attacks	1 /4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. In the case of Gamaredon, the group was responsible for less than 1 attack per year of activity (0,33).
Exploitation of Zero days	0 /3	This indicator calculates the percentage of attacks attributed to the APT that make use of one or multiple zero days. The obtained score is then converted to a three-level scale. Gamaredon has not made use of zero-days.

→ Overall, the Gamaredon group obtains a moderate-level threat score compared to other APT groups. The attacks analysed within the EuRepoC framework, were of relatively low intensity, infrequent and only targeted Ukraine. However, Gamaredon attacks affected multiple critical sectors and political institutions at the same time.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

Industry reporting describes Gamaredon Group as less sophisticated than other Russian APTs known for targeting infrastructure systems, such as Sandworm. The group seeks to compensate for this through a high frequency of attacks. After largely relying on off-the-shelf tools, the group started to deploy custom-developed malware in 2017. While the group has been observed to use false-flag tactics at times, their degree of operational security is described as deficient in other instances.

Basic attack pattern

The group primarily initiates attacks with **spearphishing emails** containing malicious attachments and links, which activate macros that employ **remote templates to infiltrate victim networks** and gather sensitive information. The group mainly employs their customised backdoors **Pterodo/Pteranodon** in modified versions, presumably with the goal to maintain operational continuity in case the command-and-control infrastructure of one variant is blocked. In early 2022, at least four iterations of this malware were leveraged against targets in Ukraine.

Sources [4] [5] [11] [12] [13] [14] [16] [21]

Zero-Day exploits

No use of zero days reported.

Malware used (non-exhaustive)

DinoTrain	DesertDown	DilongTrash
Evil Gnome	ObfuBerry	ObfuMerry
PowerPunch	Pterodo/Pteranodon	

Sources [4] [5] [11] [12] [13] [15] [21]

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework

MITRE Initial Access

Phishing
Spearphishing attachement
Spearphishing link
Trusted relationship

MITRE Persistence

Boot or logon autostart execution
Office application startup
Scheduled task/job

MITRE Defense Evasion

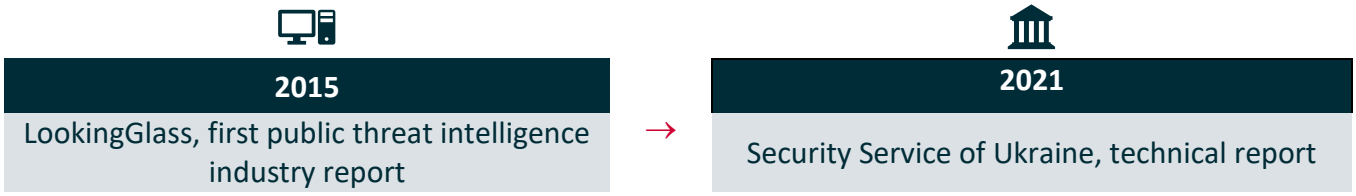
Deobfuscate/decode files or information
Hide artifacts
hidden window
Impair defenses
disable or modify tools
Indictor removal
file deletion
Masquerading
match legitimate name or location
Modify registry
Obfuscated files or information
binary padding
compile after delivery
System binary proxy execution
Mshta
Rundll32
Template injection
Virtualization/sandbox evasion
user activity based checks

MITRE Exfiltration

Automated exfiltration
Exfiltration over command-and-control channel
Data destruction
Defacement
internal defacement

ATTRIBUTION

Attribution milestones



Sources [2] [7]

Attribution ambiguities

Possible hijacking of infrastructure operated by Iranian APTs: In 2019, Recorded Future reported an overlap in attack infrastructure between several Iranian state-nexus groups and BlueAlpha, the identifier given by the company to an activity cluster with close operational resemblance to Gamaredon. Researchers traced malicious activity involving a domain impersonating the Saudi International Petrochemical Company to operational infrastructure of BlueAlpha. The same bogus domain had previously been leveraged by two threat actors associated with Iran's Islamic Revolutionary Guards Corps (APT33/Elfin and APT35/Charming Kitten) and a group suspected to be subordinate to the Iranian Ministry of Intelligence and Security (MUDDYWATER). Against the backdrop of parallel reporting on other Russia-based threat actors seizing control of Iranian APT tooling (most notably Turla operating on FSB tasking), these intersections suggest BlueAlpha may have infiltrated Iranian-run attack platforms or reclaimed decommissioned infrastructure.

Developing access for InvisiMole: In 2018, ESET discovered a previously-unknown cyberespionage tool on systems in Ukraine and Russia. The initial access vectors of the threat activity (tracked by ESET as "InvisiMole") remained unclear, as did any potential state links. Resumed campaign activity against a cluster of defence organisations and diplomatic delegations in Eastern Europe conducted by the same actor in late 2019 revealed a staged infiltration process. Intrusion patterns showed InvisiMole tooling being deployed via Gamaredon's signature Pterodo backdoor, suggesting the group turned over access to InvisiMole for pin-pointed and stealthier exploitation of a select subset of targets. Using Gamaredon's simpler and easier-to-rebuild tools for reconnaissance, this mode of target acquisition has allowed InvisiMole to maintain a lower profile in the shadow of one of the most prolific Russian threat actors. ESET traces coordination between the two groups back to 2018, while assessing that both actors remain organisationally separate and leverage distinct TTPs.

Sources [13] [16] [22] [23] [24] [27]

Attribution-/detection sensitivity

Since around 2016/2017, the group has increasingly shown technical aptitude through the development of customised malware in what may be a bid to obfuscate its tooling and slow down analysis. To what extent these operational adjustments are motivated by SSU and industry disclosures of the group's activities cannot be conclusively assessed at this stage. The group's continued interest in false-flag tactics may, however, indicate an increased level of attribution sensitivity. Reporting by the Microsoft Threat Intelligence Center in April 2022 attested the group the use of variegated techniques to avoid scrutiny, highlighting the role of flexible changeovers of infrastructure in thwarting detection efforts.

Sources [4] [16]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

On 4 November 2021, the SSU announced that it had notified five members of Gamaredon about their suspected involvement in high treason and the alleged breach of Article 111 of the Criminal Code of Ukraine.

Sources: [7]

Indicted individuals / sanctioned (associated) entities

In its November 2021 disclosures, the SSU revealed the identity of five FSB officers serving in the unit deemed responsible for Gamaredon operations and their immediate superiors.

To date, no public records exist about further law enforcement actions or indictments against these designated individuals. The breakdown reproduced in the section on the group's suspected composition of this report merely serves as an overview of the group's operational structure.

Sources: [7]

Landmark incidents

Operation Armageddon: Gamaredon has been engaged in a long-term cyber espionage campaign against Ukrainian government and military officials dating back to 2013. This campaign is in support of Russia's military offensives against Ukraine, reaching back to the invasion of Crimea.

Sources [2] [4] [5] [14] [17] [18]

Targeting of EU government agencies:
In March 2022, in the context of Russia's invasion of Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA) for the first time spotted Gamaredon targeting government entities outside Ukraine with established spearphishing techniques to gain access to victim networks and data. In one confirmed case, the attackers, posing as the Deputy Commander for Armaments of Ukraine's armed forces, delivered a malicious message to a Latvian government agency under the disguise of a request for military assistance. The cover narrative employed may indicate an interest in other European government entities that might have been targeted as part of the same campaign.

Sources: [19] [25]

SOURCES

[1] Unit 42 Team (2017), The Gamaredon Group Toolset Evolution, Unit 42. Available at: https://web.archive.org/web/20230117170227/https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/ [Archived on: 17.01.2023].

[2] Lookingglass Cyber Threat Intelligence Group (2015), Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare, LookingGlass Cyber Threat Intelligence Group (CTIG). Available at: https://web.archive.org/web/20230118121545/https://7412038.fs1.hubspotusercontent-na1.net/hubfs/7412038/Operation_Armageddon_Final.pdf [Archived on: 18.01.2023].

[3] Unit 42 Team (2022), Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine, Unit 42, Palo Alto Networks. Available at: https://web.archive.org/web/20230117193312/https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/ [Archived on: 17.01.2023].

[4] Microsoft Threat Intelligence Center (MSTIC) and Microsoft Digital Security Unit (2022), ACTINIUM targets Ukrainian organizations, Microsoft Security Blog. Available at: https://web.archive.org/web/20230117190312/https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/ [Archived on: 17.01.2023].

[5] Symantec Threat Hunter Team (2022), Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine, Symantec Enterprise Blogs/Threat Intelligence. Available at: https://web.archive.org/web/20230117193839/https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine [Archived on: 17.01.2023].

[6] Cimpanu (2021), Ukraine discloses identity of Gamaredon members, links it to Russia's FSB, The Record from Recorded Future News. Available at: https://web.archive.org/web/20230117194110/https://therecord.media/ukraine-discloses-identity-of-gamaredon-members-links-it-to-russias-fsb/ [Archived on: 17.01.2023].

[7] SSU (2021), SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine (video), Security Service of Ukraine (SSU). Available at: https://web.archive.org/web/20230117194324/https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy [Archived on: 17.01.2023].

[8] Ji (2022), Russian APT Group Gamaredon Launches Phishing Campaign Against Ukrainian Ministry of Foreign Affairs, NSFocus. Available at: https://web.archive.org/web/20230117194807/https://nsfocusglobal.com/russian-apt-group-gamaredon-launches-phishing-campaign-against-ukrainian-ministry-of-foreign-affairs/ [Archived on: 17.01.2023].

[9] Tucker (2018), Russia Launched Cyber Attacks Against Ukraine Before Ship Seizures, Firm Say, Defense One. Available at: https://web.archive.org/web/20230117195032/https://www.defenseone.com/technology/2018/12/russia-launched-cyber-attacks-against-ukraine-ship-seizures-firm-says/153375/ [Archived on: 17.01.2023].

[10] Lakshmanan (2022), Microsoft Documents over 200 Cyberattacks by Russia Against Ukraine, The Hacker News. Available at: https://web.archive.org/web/20230117195228/https://thehackernews.com/2022/04/microsoft-documents-over-200.html [Archived on: 17.01.2023].

[11] Ananin and Semenchenko (2019), The Gamaredon Group: A TTP Profile Analysis, Fortinet. Available at: https://web.archive.org/web/2/https://www.fortinet.com/blog/threat-research/gamaredon-group-ttp-profile-analysis [Archived on: 17.01.2023].

[12] Rapid7 (2022), The Top 5 Russian Cyber Threat Actors to Watch, Rapid7. Available at: https://web.archive.org/web/20230117195554/https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/ [Archived on: 17.01.2023].

[13] Insikt Group (2019), Operation Gamework: Infrastructure Overlaps Found Between BlueAlpha and Iranian APTs, Recorded Future. Available at: https://web.archive.org/web/20210714143430/https://go.recordedfuture.com/hubfs/reports/cta-2019-1212.pdf [Archived on: 17.01.2023].

[14] Toulas (2022), Russian State Hackers Hit Ukraine With New Malware Variants, Bleeping Computer. Available at: https://web.archive.org/web/2/https://www.bleepingcomputer.com/news/security/russian-state-hackers-hit-ukraine-with-new-malware-variants/ [Archived on: 17.01.2023].

[15] MITRE ATT&CK (2022), Gamaredon Group, MITRE ATT&CK. Available at: https://web.archive.org/web/2/https://attack.mitre.org/groups/G0047/ [Archived on: 17.01.2023].
[16] SSU (2021), Gamaredon/Armageddon Group, Security Service of Ukraine (SSU). Available at: https://web.archive.org/web/20230101093143/https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armageddon.pdf [Archived on: 17.01.2023].
[17] Lakshmanan (2022), Ukraine Continues to Face Cyber Espionage Attacks from Russian Hackers, The Hacker News. Available at: https://web.archive.org/web/20230117200900/https://thehackernews.com/2022/02/ukraine-continues-to-face-cyber.html [Archived on: 17.01.2023].
[18] Vicens (2022), Russia-linked Gamaredon shows signs of possible recent activity in Ukraine, researchers say, CyberScoop. Available at: https://web.archive.org/web/20230117201159/https://www.cyberscoop.com/gamaredon-russian-hacker-cyber-attack-ukraine/ [Archived on: 17.01.2023].
[19] Toulas (2022), Ukraine: Russian Armageddon phishing targets EU govt agencies, BleepingComputer. Available at: https://web.archive.org/web/20230117201405/https://www.bleepingcomputer.com/news/security/ukraine-russian-armageddon-phishing-targets-eu-govt-agencies/ [Archived on: 17.01.2023].
[20] Bowen (2022), Russian Cyber Units, Congressional Research Service. Available at: https://web.archive.org/web/20230118100841/https://sgp.fas.org/crs/row/IF11718.pdf [Archived on: 18.01.2023].
[21] Boutin (2020), Gamaredon group grows its game, ESET, Welivesecurity. Available at: https://web.archive.org/web/20230117180249/https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/ [Archived on: 17.01.2023].
[22] SOCRadar Research (2023), Dark Web Profile: MuddyWater APT Group, SOCRadar. Available at: https://web.archive.org/web/20230117190708/https://socradar.io/dark-web-profile-muddywater-apt-group/ [Archived on: 17.01.2023].
[23] Hromcová and Cherepanov (2020), Digging up InvisiMole's hidden arsenal, ESET, Welivesecurity. Available at: https://web.archive.org/web/20230117191046/https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal [Archived on: 17.01.2023].
[24] Hromcová (2018), InvisiMole: Surprisingly equipped sypware, undercover since 2013, ESET, Welivesecurity. Available at: https://web.archive.org/web/20220701133217/https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/ [Archived on: 17.01.2023].
[25] CERT-UA (2022), *Кібератака групи UAC-0010 (Armageddon) на державні інституції країн Європейського Союзу (CERT-UA#4334)*, Computer Emergency Response Team of Ukraine (CERT-UA). Available at: https://web.archive.org/web/20220404221031/https://cert.gov.ua/article/39086 [Archived on: 04.04.2022].
[26] CISA (2022), Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, Cybersecurity & Infrastructure Security Agency (CISA). Available at: https://web.archive.org/web/20230110030415/https://www.cisa.gov/uscert/ncas/alerts/aa22-110a [Archived on: 17.01.2023].
[27] EuRepoC (2022), Advanced Persistent Threat Profile: Turla, European Repository of Cyber Incidents (EuRepoC). Available at: https://web.archive.org/web/20230117192521/https://strapi.eurepoc.eu/uploads/Eu_Repo_C_APT_profile_Turla_c9c7d8ed38.pdf [Archived on: 17.01.2023].

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database the full dataset, calculations and methodology can be downloaded here: https://doi.org/10.7802/2494

About the authors :

- **Kerstin Zettl-Schabath** is a researcher at the Institute of Political Science (IPW) at Heidelberg University.
- **Jakob Bund** is an Associate at the German Institute for International and Security Affairs (SWP). He is currently a fellow with the European Cyber Conflict Research Initiative (ECCRI).
- **Lena Rottinger** is a political science student at the Institute for Political Science (IPW) at Heidelberg University and a former research intern for EuRepoC.
- **Camille Borrett** is a Data Analyst at the German Institute for International and Security Affairs (SWP).

Last updated: 23.01.2023