EuRepoC

ADVANCED PERSISTENT THREAT profile

APT28

Exploiting Democratic Vulnerabilities in Cyberspace

Associated APT designations

- **APT28** (FireEye/Mandiant)
- **Fancy Bear** (CrowdStrike)
- **SOFACY** (Kaspersky)
- **STRONTIUM** (Microsoft)
- **PawnStorm** (Trend Micro)
- **IRON TWILIGHT** (SecureWorks)
- **Sednit** (ESET)
- **Snakemackerel** (iDefense)
- **Tsar Team** (iSight)
- **G0007** (MITRE ATT&CK)

Sources [1], [2], [3], [4], [5], [37]

Country of origin

Time period of activity

2004-today

Sources: [2], [10]

Political affiliations

Today, APT28 is consistently attributed to **GRU Unit 26165**, **85th Main Special Service Centre (GTsSS)** of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). This attribution is mainly based on an indictment unsealed by the US Department of Justice (DoJ) in 2018. A **report by the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI)** from 2016 had previously attributed ATP28 with high confidence to the **Russian military or civilian intelligence services** without specifying the agency. In its 2018 security environment assessment, the **Estonian Intelligence Service** affirmed that ATP28 is consistent with observations for GRU Unit 26165. Later in 2018, the **UK National Cyber Security Center (NCSC)** assessed with "almost certainty" that APT28 operates as part of the GRU. Industry sources, such as FireEye, had already attributed APT28 as a Russian state-sponsored actor in 2014 without identifying any specific links to state institutions or agencies. In 2016, CrowdStrike was the first to publicly identify the GRU as the responsible state agency as a product of its investigations into the intrusions into the networks of the Democratic National Committee (DNC).

Sources [6], [7], [8], [9], [5], [34]

By Kerstin Zettl-Schabath, Timothy Gschwend and Camille Borrett

Agency type

State-integrated hacking group:

Based on the reports about the group's alleged political affiliations and several indictments against GRU agents, which claim to identify APT28 members, the group is considered a *de facto* **agent of the Russian state, more specifically its military intelligence branch (GRU)**. Furthermore, its extensive operations against defence ministries, NATO installations, and the defence sector **closely reflect the strategic and geopolitical interests of the Russian government.** With respect to aligning interests, **CrowdStrike** concluded that data stolen during intrusions by APT28 has been leaked **in support of Russian state information operation efforts** (see entries on **incident type** and **landmark incidents** below). Researchers from **Trend Micro** assessed that, in earlier stages, APT28 repeatedly carried out operations **against Russian citizens** who fit regime characterizations of **dissidents**. Targeting of the latter more typically fits in with patterns of Russia's domestic security services.

Sources [1], [5], [10], [11]

Most frequent targets:

Canada, China, France, Germany, Japan, South Korea, Switzerland, Turkey, United Kingdom, United States

The group focused mainly on state entities, international organisations, and security/military-related actors in general.

Sources [1], [5], [11], [12]

Group composition and organisational structure

The 2018 DoJ indictment discloses the names of 11 members of the group. According to public estimates, the GRU consists of around 12,000 people, so those indicted likely only represent a fraction of ATP28's force structure. As one of the service's main cyber groups, APT28 may also draw on personnel resources of the 6th Directorate, the GRU signal and electronic intelligence division. Operations of APT28 are often technically demanding and are maintained over a longer period, suggesting a substantial personnel capacity.

Impact type(s)

Direct

- **Intelligence impact** (Ukrainian military app hack 2014; German Parliament hack 2015; Norwegian Parliament hack 2019)
- **Disinformation impact** (DNC hack 2016; French Presidential election 2017)

Indirect

- **Reputational impact** (DNC hack 2016; WADA hack 2016)

Sources [5], [13], [14], [15], [35], [39]

Incident type(s)

Intelligence gathering (especially targeting political and defence-related entities, e.g., in EU and NATO member states. In 2022, targeting also included Ukrainian entities.)

Information operations (such as the hack-and-leak operation against the DNC during the US elections campaign in 2016; the false-flag attack against French TV station TV5 Monde in 2015, including disrupting and defacing the broadcast)

Sources [1], [12], [40], [41], [47]

Incident types documented by EuRepoC:

- Hijacking with misuse
- Data theft *(cyber-espionage)*
- Data theft & doxing
- Disruption

Threat Level Index

13/24 high 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 APT28:

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	3 /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 APT28, on average attacks attributed to the group within the EuRepoC database, targeted 1.5 sectors per attack and just under 70% of all attacks were against political systems and/or critical infrastructure.
Geographical scope of attacks	4 /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 APT28, on average five countries were targeted per attack attributed to the group within the EuRepoC database.
Frequency of attacks	4 /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 APT28, the group was responsible for close to 2 attacks per year of activity (1.94).
Exploitation of Zero days	1 /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. 3% of attacks attributed to APT28 made use of zero-days.

→ Overall, the APT28 group obtains a high-level threat score compared to other APT groups. Although the attacks analysed within the EuRepoC framework had a relatively low intensity in terms of their physical and socio-political effects, attacks by APT28 were frequent, targeted an above average number of countries and sectors, while sometimes exploiting zero-days, compared to the other APT groups analysed by EuRepoC.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

Basic attack pattern

According to FireEye, APT28 uses a flexible, modular framework that allows the group to consistently adapt and evolve their means of attack. The group most likely employs a conventional coding environment to develop these tools, which would allow the group to develop and deploy customized modules in their backdoors. According to CrowdStrike, APT28 has proven to be capable of running several, and often extensive, intrusion operations at the same time. APT28 combines vast use of Strategic Web Compromise (SWC) techniques with several checks to identify, prioritize, and then deploy malware only to specific targets of special importance. In cases where the group employs spear phishing techniques to deploy its malware, it uses lightweight reconnaissance tools to verify its targets before upgrading its hosts to more sophisticated malware capabilities at a later point in time.

Zero-Day exploits (non-exhaustive)

Java vulnerability (**CVE-2015-2590**) exploited by JHUHUGIT implant, type-confusion exploit in **Encapsulated PostScripts (EPS)** produced by Microsoft Office (**CVE-2017-0261**), Microsoft Word exploit (**CVE-2017-0262**), escalation of privilege (EOP) zero-day (**CVE-2017-0263**), Microsoft Office exploit (**CVE-2015-2424**), Windows EOP vulnerability (**CVE-2015-1701**), Adobe Flash exploit **(CVE-2016-7855)**, Adobe Flash exploit (**CVE-2015-3043**), Windows EOP zero-day (**CVE-2016-0167),** 'Follina' exploit in the Microsoft Windows Support Diagnostic Tool (MSDT) (**CVE-2022-30190).**

In a 2020 report, Trend Micro says APT28 has also begun conducting global scans of TCP ports 445 and 1433 in search of (zero-day) vulnerabilities in servers operating Microsoft SQL Server and Directory Services.

Malware used (non-exhaustive)

Sofacy (Trojan.Sofacy, Backdoor.SofacyX (also known as X-Agent)	CHOPSTICK	JHUHUGIT
KOMPLEX	XAGENTOSX	XTunnel
Zebrocy	Koadic	ADVSTORESHELL
Lojax	GAMEFISH	

Sources [1], [2], [3], [11], [15], [16], [17], [18], [19], [20], [21]

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

MITRE Initial Access

Drive-by compromise
Exploit public-facing application
External remote services
Phishing
Spearphishing attachment
Spearphishing link
Replication through removable media
Trusted relationship
Valid accounts
Cloud accounts

MITRE Persistance

Boot or logon autostart execution
Registry run keys/startup folder
Event-triggered execution
External remote services
Office application startup
Pre-OS boot
Bootkit
Server software component
Web shell
Valid accounts
Cloud accounts

MITRE Defense Evasion

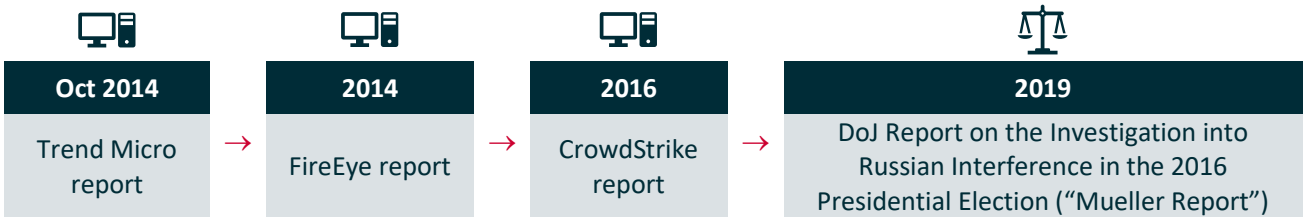
Access token manipulation
Deobfuscate/decode files or information
Exploitation for defense evasion
Hide artifacts
Hidden files and directories
Hidden window
Indicator removal
Clear Windows event logs
File deletion
Timestomp
Masquerading
Match legitimate name or location
Obfuscated files or information
Pre-OS boot
Bootkit
Rootkit
System binary proxy execution
Rundll32
Template injection
Use alternate authentication material
Application access token
Pass the hash
Valid accounts
Cloud accounts

MITRE Exfiltration

Data transfer size limits
Exfiltration over alternative protocol
Exfiltration over asymmetric encrypted non-C2 protocol
Exfiltration over web service
Network denial service

ATTRIBUTION

Attribution milestones



Sources [5], [13], [22], [23]

Attribution ambiguities

APT28 vs. Sandworm (generally): Since both Sandworm and APT28 allegedly work for the GRU, researchers point out that it has proven difficult to differentiate attacks between Unit 26165 and Unit 74455 (the field post number linked to Sandworm). Andy Greenberg, a US journalist, posited that Sandworm and Fancy Bear (APT28) are two names for the same group but has not been able to come to a clear conclusion. A CyberScoop article from 2017 cited two unnamed former US officials who claim that Sandworm acts as a subunit of APT28. Two of the six GRU officers named in a 2020 DoJ indictment (indictment CR 20-316 of 15 October 2020) for operations linked to Unit 74455, Petr Nikolayevich Pliskin and Anatoliy Sergeyevich Kovalev, apparently were also involved in the 2016 DNC hack, which was most likely carried out by APT28 (see below).

APT28 vs. Sandworm (Georgia 2008): It remains unclear whether Sandworm or APT28 is responsible for the DDoS/defacement operations carried out against Georgian government institutions during the Russo-Georgian War of 2008. Considering that both groups are attributed to the GRU, it is plausible that both were involved or, at the very least, resources were shared.

APT28 vs. Sandworm (BadRabbit 2017): Whereas the Security Service of Ukraine (SBU) blamed the international ransomware campaign BadRabbit on APT28, IT security company ESET indicated Sandworm as the responsible culprit. In a statement from 2018, the UK NCSC attributed the campaign to the Russian GRU but did not specify the responsible unit/hacking group.

APT28 vs. Sandworm (Olympic Destroyer 2018): To disguise Olympic Destroyer's origin, a disruptive malware used against the Pyeongchang Olympics, the attackers crafted some of the code as if it had originated from **Lazarus**, the North Korean APT group blamed for the global WannaCry campaign in 2017. The security company Intezer, in early code analysis, had identified overlaps with malware previously only observed in use by the China-aligned groups APT3, APT10 and APT12. Yet, Kaspersky research noted that, these isolated and transparent connections to Chinese tooling aside, the deployed code did not bear out these Chinese hallmarks. The 2020 DoJ indictment links Olympic Destroyer **to Sandworm**. However, researchers from Kaspersky believe that APT28 might be responsible. Sources [9], [24], [25], [26], [42], [48], [49]

Attribution and detection sensitivity

The group appears to possess effective counter-analysis capabilities, i.e., protection mechanisms. These include, for example, runtime checks to detect an analysis environment, unrecognizing strings that are unpacked during execution, and using unused machine instructions to slow down the analysis of deployed malware.

Despite direct attribution in 2018, technical signs of continued operational activity have been observed since then, suggesting that detection/attribution has not had a significant disruptive effect on APT28's operations. CrowdStrike argues that the group has increased their operational security (OPSEC) efforts after 2018, including toolkit diversification, loaders such as TrsLoader to deploy malware directly into memory to evade forensic analysis, and the use of short-lived command-and-control (C2) servers to complicate attribution.

Sources [1] [11] [15]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

Legal actions by Microsoft against APT28 (since **2016) :** In 2016, Microsoft took legal action against APT28 on account of an "Internet-based cyber-theft operation." As of 2022, the company has acted 15 times to seize control of more than a hundred APT28-controlled domains, also including infrastructure used against Ukrainian targets during the Russian invasion.

US DoJ Indictment against 11 GRU officers on the account of the 2016 DNC hack (2018): In 2018, the Grand Jury for the District of Columbia charged 11 officers from GRU Units 26165 and 74455 (among others) for Conspiracy to Commit an Offense Against the United States and on eight other counts (an overview of the indicted individuals affiliated with Unit 26165 is provided below).

EU sanctions against two individuals and one institution (based on EU Cyber Diplomacy Toolbox, 22 October 2020): The Council of the European Union imposed restrictive measures on Dmitry Badin and Igor Kostyukov (the head of the GRU), as well as GRU Unit 26165, who it deemed responsible for or involved in the cyber espionage campaign against the German Parliament in April and May 2015. The sanctions imposed include the freezing of the assets of all parties involved. The two designated GRU officers are also subject to an entry ban. In addition, EU persons and entities are prohibited from providing financial aid to the listed individuals and unit.

Arrest warrant by the Federal Public Prosecutor General of Germany (May 2020) for suspected Unit 26165 officer Dmitriy Badin over his alleged involvement in the 2015 cyberattack against the German Federal Parliament.

Arrest warrant for suspected Unit 26165 officer by the Federal Public Prosecutor General of Germany (2022): Nikolay Kozachek, a suspected member of APT28, allegedly penetrated a network of the NATO Joint Air Power Competence Centre in Kalkar, Germany, for espionage purposes in April 2017. He allegedly installed malware (X-Agent) with a keylogger function, facilitating the collection of an unknown amount of data.

As of July 2022, German authorities had not yet initiated a public search for either Badin or Kozachek. No corresponding entries had been listed in the Interpol search facility.

Sources: [5], [27], [28], [29], [30], [31], [43], [44]

Indicted individuals / sanctioned (associated) entities

US indictment of Russian intelligence officers for hacking offences related to the 2016 election (announced on 13 July 2018):

Viktor Borisovich Netyksho
Officer in command of Unit 26165

Boris Alekseyevich Antonov
Head of Department, leading sub-team within Unit 26165 focused on targeting military, political, governmental, and non-governmental organisations

Dmitriy Sergeyevich Badin
Assistant Head of Department under Antonov within Unit 26165

Ivan Sergeyevich Yermakov
Military officer assigned to Antonov's department within Unit 26165

Aleksey Viktorovich Lukashev
Senior Lieutenant assigned to Antonov's department within Unit 26165

Sergey Aleksandrovich Morgachev
Head of Department, leading sub-team within Unit 26165 dedicated to developing and managing malware (including X-Agent)

Nikolay Yuryevich Kozachek
Lieutenant Captain assigned to Morgachev's department within Unit 26165

Pavel Vyacheslavovich Yershov
Military officer assigned to Morgachev's department within Unit 26165

Artem Andreyevich Malyshev
Second Lieutenant assigned to Morgachev's department within Unit 26165

EU restrictive measures against Russian military intelligence officers and Unit 26165 (imposed on 22 October 2020):

Dmitriy Sergeyevich Badin
Assistant Head of Department of a sub-team within Unit 26165 focused on targeting military, political, governmental, and non-governmental organisations

Igor Olegovich Kostyukov
Head of the Main Directorate of the General Staff of the Armed Forces (GRU)

85th Main Centre for Special Service of the GRU/ Unit 26165

Arrest warrant by the Federal Public Prosecutor General of Germany in response to the 2015 cyberattack against the German Federal Parliament (issued in May 2020):

Dmitriy Sergeyevich Badin
Assistant Head of Department of a sub-team within Unit 26165 focused on targeting military, political, governmental, and non-governmental organisations

Arrest warrant by the Federal Public Prosecutor General of Germany in response to infiltrations of the NATO Joint Air Power Competence Centre (issued in 2022):

Nikolay Yuryevich Kozachek
Lieutenant Captain assigned to department within Unit 26165 dedicated to developing and managing malware

Sources: [6], [27], [29], [30], [31]

Landmark incidents

DNC hack 2016: APT28 penetrated the networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) via phishing attacks in April 2016. APT28 employed X-Agent malware, which enabled remote-command execution, transmissions of files, and keylogging, as well as the X-Tunnel malware. In March, the group had gained access to the email accounts of several staffers on Hillary Clinton's presidential campaign, including the campaign's chair, John Podesta. Material illicitly obtained as part of the hacks, including over 50,000 messages retrieved from Podesta's account, were subsequently leaked to WikiLeaks and posted online using fronts like DCLeaks and Guccifer 2.0.

German Federal Parliament/Bundestag hack 2015: During April and May 2015, APT28 penetrated the network of the German Bundestag by means of a large-scale phishing campaign. In total, an estimated 16 gigabytes of data, including emails from MPs, were exfiltrated to foreign servers.

Hack of Presidential Candidate Macron's Campaign 2017: On the eve of the French Presidential Election in 2017, presidential candidate Macron's campaign was targeted by a coordinated phishing campaign, with tens of thousands of emails and other internal documents being released online overnight as France's 'discretionary period' that halts campaigning and enforces an election-related media blackout came into effect. France, the EU, and the US blamed Russia, and APT28 in particular, for trying to influence the election in favour of Marine Le Pen, who is considered close to Russia.

Other notable incidents/campaigns: Ukraine military app hack (2014 – 2016), World Anti-Doping Agency (WADA, 2016), International Olympic Committee (IOC, 2018), French TV Station TV5 Monde (2015), Dutch ministries (2017), hack of NATO Joint Air Power Competence Centre (2017), Norwegian Parliament (2020), foiled attempt at hacking the Organisation for the Prohibition of Chemical Weapons (OPCW) and the OPCW-certified Spiez Laboratory in Switzerland, participation in the cyberwarfare campaign against Ukraine during the Russian invasion in 2022 (attempts at disruption and destruction of Ukrainian critical infrastructure/vulnerable systems; phishing campaigns against Ukrainian entities).

Sources: [6], [13], [14], [29], [32], [36], [45], [46]

SOURCES

[1] CrowdStrike Adversary Universe, *Adversary: Fancy Bear*, CrowdStrike. Accessed on 02.02.2023. https://web.archive.org/web/20230202113921/https://adversary.crowdstrike.com/en-US/adversary/fancy-bear/ [Archived on: 02.02.2023].
[2] MITRE (2022), *APT28*. Available at https://web.archive.org/web/20230202124339/https://attack.mitre.org/groups/G0007/ [Archived on: 02.02.2023.]
[3] Kaspersky (2015), *SoFacy APT hits high profile targets with upgraded toolset*, SecureList. Available at https://web.archive.org/web/20230202125430/https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/ [Archived on: 02.02.2023].
[4] Microsoft Defender Security Research Team (2015), *Microsoft Security Intelligence Report: Strontium*, Microsoft. Available at https://web.archive.org/web/20230202125806/https://www.microsoft.com/en-us/security/blog/2015/11/16/microsoft-security-intelligence-report-strontium/ [Archived on: 02.02.2023].
[5] FireEye (2014), *APT28: A Window into Russia's Cyber Espionage Operations?*, FireEye. Available at https://web.archive.org/web/20230202131524/https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf [Archived on: 02.02.2023].
[6] US Department of Justice (2018), *United States of America v. Victor Borisovich Netyksho [and 10 others]*, defendants: Case 1:18-cr-00215-ABJ. Available at https://web.archive.org/web/20230129052022/https://www.justice.gov/file/1080281/download [Archived on: 02.02.2023].
[7] Estonian Foreign Intelligence Service (2018), *International Security and Estonia 2018.* Available at https://web.archive.org/web/20221220095740/https://www.valisluureamet.ee/doc/raport/2018-en.pdf [Archived on: 02.02.2023].
[8] National Cybersecurity and Communications Integration Center (NCCIC), Federal Bureau of Investigation (2016), *Grizzly Steppe – Russian Malicious Cyber Activity*, Cybersecurity and Infrastructure Security Agency (CISA). Available at https://web.archive.org/web/20230103041149/https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [Archived on: 02.02.2023].
[9] National Cyber Security Centre (2018), *Reckless campaign of cyber attacks by Russian military intelligence service exposed*, NCSC. Available at https://web.archive.org/web/20230202133819/https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed [Archived on: 02.02.2023].
[10] Feike Hacquebord (2017), *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat*, TrendLabs. Available at https://web.archive.org/web/20221005233452/http://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf [Archived on: 02.02.2023].
[11] CrowdStrike (2019), *Who is FANCY BEAR (APT28)?*, CrowdStrike Blog. Available at https://web.archive.org/web/20230202134838/https://www.crowdstrike.com/blog/who-is-fancy-bear/ [Archived on: 02.02.2023].
[12] Symantec (2018), *APT28: New Espionage Operations Target Military and Government Organizations*, Symantec Enterprise Blogs. Available at https://web.archive.org/web/20221208122117/https://symantec-enterprise-blogs.security.com/blogs/election-security/apt28-espionage-military-government [Archived on: 08.12.2022].
[13] CrowdStrike (2020), *CrowdStrike's work with the Democratic National Committee: Setting the record straight*, CrowdStrike Blog. Available at https://web.archive.org/web/20230202135005/https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ [Archived on: 02.02.2023].
[14] FireEye (2017), *APT28: At the Center of the Storm: Russia Strategically Evolves Its Cyber Operations*, Mandiant. Available at https://web.archive.org/web/20221229204150/https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf [Archived on: 02.02.2023].
[15] Jochen Rummel (2017), *APT28: Steht auch Deutschland im Ziel russischer Hackergruppierungen?*, FireEye Blog. Available at https://web.archive.org/web/20230202141812/https://www.fireeye.com/blog/de-threat-research/2017/04/is-germany-the-target-of-russian-hacker-groups.html [Archived on: 02.02.2023].
[16] FireEye (2017), *Aktuelle Zero-Day-Exploits*, FireEye Blog. Available at https://web.archive.org/web/20230202142447/https://www.fireeye.de/current-threats/recent-zero-day-attacks.html [Archived on: 02.02.2023].
[17] Google (2016), *Disclosing vulnerabilities to protect users*, Google Security Blog. Available at https://web.archive.org/web/20230202142719/https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html [Archived on: 02.02.2023].
[18] FireEye Labs (2015), *Operation RussianDoll: Adobe Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack*, Mandiant Blog. Available at https://web.archive.org/web/20230202142947/https://www.mandiant.com/resources/blog/probable-apt28-useo [Archived on: 02.02.2023].

[19] Genwei Jiang, et al. (2022), *EPS Processing Zero-Days Exploited by Multiple Threat Actors*, Mandiant Blog. Available at https://web.archive.org/web/20230202143240/https://www.mandiant.com/resources/blog/eps-processing-zero-days [Archived on: 02.02.2023].
[20] Feike Hacquebord (2020), *Pawn Storm in 2019: A Year of Scanning and Credential Phishing on High-Profile Targets*, Trend Micro Research. Available at https://web.archive.org/web/20230105180201/https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf [Archived on: 02.02.2023].
[21] Ravie Lakshmanan (2022), *Russian Hackers Exploiting Microsoft Follina Vulnerability Against Ukraine*, The Hacker News. Available at https://web.archive.org/web/20221201105453/https://thehackernews.com/2022/06/russian-hackers-exploiting-microsoft.html [Archived on: 02.02.2023].
[22] Loucif Karouni, et al. (2014), *Operation Pawn Storm: Using Decoys to Evade Detection*, Trend Micro Research. Available at https://web.archive.org/web/20220427051328/https://documents.trendmicro.com/assets/wp/wp-operation-pawn-storm.pdf [Archived on: 02.02.2023].
[23] Robert S. Mueller, III (2019), *Report On The Investigation Into Russian Interference In The 2016 Presidential Election Volume I of II*, U.S. Department of Justice. Available at https://web.archive.org/web/20230129140646/https://www.justice.gov/archives/sco/file/1373816/download [Archived on: 02.02.2023].
[24] Andy Greenberg (2019), *US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit*, Wired. Available at https://web.archive.org/web/20230202145638/https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/ [Archived on: 02.02.2023].
[25] Rene Holt (2022), *Sandworm: A tale of disruption told anew*, ESET, WeLiveSecurity. Available at https://web.archive.org/web/20230202150152/https://www.welivesecurity.com/2022/03/21/sandworm-tale-disruption-told-anew/ [Archived on: 02.02.2023].
[26] Kaspersky Team (2018), *Olympic Destroyer: who hacked the Olympics?*, Kaspersky Daily. Available at https://web.archive.org/web/20230202151034/https://www.kaspersky.com/blog/olympic-destroyer/21494/ [Archived on: 02.02.2023].
[27] United States District Court, Eastern District of Virginia (2016), *Microsoft Corporation v. John Does 1-2, Controlling a Computer Network and Thereby Injuring Plaintiff and its Customers*, defendants: Civil Action No: 1:16-cv-00993 (GBL/TCB). Available at https://web.archive.org/web/20221130131507/https://noticeofpleadings.com/strontium/files/cmplt.pdf [Archived on: 02.02.2023].
[28] Tom Burt (2022), *Disrupting Cyber Attacks Targeting Ukraine*, Microsoft on the Issues. Available at https://web.archive.org/web/20230202152448/https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/ [Archived on: 02.02.2023].
[29] Council of the European Union (2020), *Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack*, European Council. Available at https://web.archive.org/web/20230202152835/https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/ [Archived on: 02.02.2023].
[30] Laurens Cerulus (2020), *EU sanctions Russian hackers for 2015 Bundestag breach*, Politico. Available at https://web.archive.org/web/20230202153546/https://www.politico.eu/article/eu-sanctions-russias-fancy-bear-hackers-for-2015-bundestag-breach/ [Archived on: 02.02.2023].
[31] Jörg Diehl, Matthias Gebauer, Fidelius Schmid (2022), *Wenn >>Blablabla1234565<< mitliest*, Spiegel Netzwelt. Available at https://web.archive.org/web/20230202154116/https://www.spiegel.de/netzwelt/hackerangriff-auf-nato-denkfabrik-in-deutschland-wenn-blablabla1234565-mitliest-a-3ac1abcb-4b5f-447f-8030-660784c8e704 [Archived on: 02.02.2023].
[32] BBC News (2018), *How the Dutch foiled Russian 'cyber-attack' on OPCW*, BBC. Available at https://web.archive.org/web/20230202155106/https://www.bbc.com/news/world-europe-45747472 [Archived on: 02.02.2023].
[33] Congressional Research Service (2021), *Russian Military Intelligence: Background and Issues for Congress*, version 7, CRS Report. Available at https://web.archive.org/web/20230126214625/https://sgp.fas.org/crs/intel/R46616.pdf [Archived on: 02.02.2023].
[34] Dmitri Alperovitch (2016), *Bears in the Midst: Intrusion into the Democratic National Committee*, CrowdStrike. Available at https://web.archive.org/web/20230202155836/https://cyber-peace.org/wp-content/uploads/2018/11/Bears-in-the-Midst_-Intrusion-into-the-Democratic-National-Committee-%C2%BB.pdf [Archived on: 02.02.2023].
[35] Euronews (2020), *Norway's Intelligence Service says Russian groups 'likely' behind Parliament attacks*, Euronews, with AP and AFP. Available at https://web.archive.org/web/20230202160142/https://www.euronews.com/2020/12/08/norway-s-intelligence-service-says-russian-groups-likely-behind-parliament-cyber-attack [Archived on: 02.02.2023].
[36] Shaun Nichols (2022), *Russian cyberattacks on Ukraine driven by government groups*, Techtarget. Available at https://web.archive.org/web/20230202160421/https://www.techtarget.com/searchsecurity/news/252523950/Russian-cyber-attacks-on-Ukraine-driven-by-government-groups [Archived on: 02.02.2023].

[37] Secureworks, *Threat Profiles: IRON TWILIGHT*. Available at https://web.archive.org/web/20230202160740/https://www.secureworks.com/research/threat-profiles/iron-twilight [Archived on: 02.02.2023].
[38] Andrei Soldatov, Irina Borogan (2022), *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*, CEPA. Available at https://web.archive.org/web/20230202161250/https://cepa.org/web/20230202161250/https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/ [Archived on: 02.02.2023].
[39] CrowdStrike Global Intelligence Team (2016), *Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units*, CrowdStrike. Available at https://web.archive.org/web/20221221184301/https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf [Archived on: 02.02.2023].
[40] Hossein Jazi, Roberto Santos (2022), *Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine*, MalwareBytes Labs. Available at https://web.archive.org/web/20230202162053/https://www.malwarebytes.com/blog/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine [Archived on: 02.02.2023].
[41] Shane Huntley (2022), *An update on the threat landscape*, Google Threat Analysis Group (TAG). Available at https://web.archive.org/web/20230202124356/https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ [Archived on: 02.02.2023].
[42] Chris Bing (2017), *Ukraine blames infamous Russian hackers for 'BadRabbit' ransomware attack*, CyberScoop. Available at https://web.archive.org/web/20221215183823/https://www.cyberscoop.com/fancy-bear-bad-rabbit-ransomware-security-service-of-ukraine/ [Archived on: 15.12.2022].
[43] Sopha Waterfield (2022), *Microsoft disrupts 'Russian nation-state' cyberattacks on Ukraine*, TechMonitor. Available at https://web.archive.org/web/20230202164651/https://techmonitor.ai/technology/cybersecurity-russia-gru-fancy-bear-sandworm-ukraine-explainer [Archived on: 02.02.2023].
[44] Florian Fade (2022), *Behörden suchen nach russischem Hacker*, Tagesschau. Available at https://web.archive.org/web/20230202164931/https://www.tagesschau.de/investigativ/wdr/russischer-hacker-101.html [Archived on: 02.02.2023].
[45] Joseph Menn (2022), *Belarus conducted widespread phishing campaigns against Ukraine, Poland, Google says*, Washington Post. Available at https://web.archive.org/web/20230202165344/https://www.washingtonpost.com/technology/2022/03/07/russia-belarus-conducted-widespread-phishing-campaigns-ukraine-google-says/ [Archived on: 02.02.2023].
[46] Cyware Alerts (2022), *Russian Hackers APT28 and UAC-0098 Target Ukraine Again*, Cyware Social. Available at https://web.archive.org/web/20230202165853/https://cyware.com/news/russian-hackers-apt28-and-uac-0098-target-ukraine-again-6fcda4cb [Archived on: 02.02.2023].
[47] Computer Emergency Response Team of Ukraine (CERT-UA) (2022), *Cyberattack by the APT28 group using CredoMap_v2 malware (CERT-UA#4622)*. Available at https://web.archive.org/web/20230202164555/https://archive.ph/nR51C [Archived on: 02.02.2023].
[48] Andy Greenberg (2019), The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History, Wired. Available at https://web.archive.org/web/20230206093159/https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/ [Archived on: 06.02.2023].
[49] Jay Rosenberg (2018), 2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang, Intezer. Available at https://web.archive.org/web/20191211163121/https://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/ [Archived on 11.12.2019].

Calculations for the Threat Level Index Indicator are based on version 1.0 of the EuRepoC Database downloadable 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.
- **Timothy Gschwend** 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: 03/02/2023