EuRepoC

ADVANCED PERSISTENT THREAT profile

APT29

Stealth at Scale

Associated APT designations

- **CozyDuke** (F-Secure)
- **UNC2452/APT29** (FireEye/Mandiant)
- **Cozy Bear** (CrowdStrike)
- **IRON HEMLOCK/IRON RITUAL** (Secureworks)
- **NOBELIUM** (Microsoft)
- **Dukes** (Kaspersky/CrySyS Lab Volexity/ESET)
- **Cloaked Ursa** (Palo Alto)
- **Fritillary** (Symantec)
- **G0016** (MITRE ATT&CK)

Sources [1] [2] [3] [9] [26] [27] [28] [29] [30] [42]

Country of origin

Time period of activity

Since at least 2008-today

Further industry reporting by SEKOIA.IO indicates the group may have started operations as early as 2004.

Sources: [1], [8], [9], [34]

Political affiliations

The US and UK governments attribute ATP29 to **Russia's Foreign Intelligence Service** (**SVR**), for which the responsibility of "political intelligence" and “economic intelligence” is even more important than for the domestic and military intelligence services, the FSB and GRU. The **Dutch General Intelligence and Security Service** (AIVD) also attributes ATP29 to the SVR, based on footage it obtained after compromising a security camera in ATP29’s presumed headquarters (HQ) in 2014. AIVD could identify several known SVR-members entering and leaving the HQ’s “hacking room.” Sources from the IT security industry, among them CrowdStrike in its initial reporting about the group, only confirmed APT29’s status as part of the **Russian intelligence apparatus,** without specifying a link to a particular agency. In subsequent years, however, CrowdStrike and Mandiant have supported judgments that identified APT29 as an SVR-operated entity. Similar to Turla's suspected general FSB affiliation, no specific SVR unit has been publicly linked to industry designations. This contrasts with more nuanced organisational connections established for other Russia-nexus actors, including APT28 (GRU Unit 26165), Sandworm (GRU Unit 74455), and Gamaredon (FSB 16th and 18th Centre). The more limited public information about the group's organisational place within Russian intelligence may reflect its comparatively higher level of operational security that may also influence an analytic reserve to disclose details that might jeopardise insight into the group's manoeuvring. Sources [4], [5], [6], [7], [31], [32], [33]

By Kerstin Zettl-Schabath, Jakob Bund, Timothy Gschwend and Camille Borrett

Agency type

State-integrated hacking group (foreign intelligence service/agency members):
The aforementioned industry and government sources characterise ATP29 as a direct agent of the Russian state, as part of the foreign intelligence service SVR. The operations are most often directed against Western societies labeled by the Russian government as "unfriendly states," with targets based in the US, UK, and across the EU. The technical sophistication and target selection of the group (see below) are strong indicators for its state integration (especially integration into secret services).

Sources [4], [7], [10]

Most frequent targets:

Sources [11], [12], [13]

Group composition and organisational structure

It can be assumed that ATP29 is either an SVR unit or a conglomerate of several groups or teams. Given its technical sophistication and well-prepared operations, both Mandiant and F-Secure assume that ATP29 is either itself a large actor or has access to resources of other (state) actors. In contrast to a report from the company in 2015, F-Secure analyst Artturi Lehtio assessed in 2020 that APT29 should not be designated as a "single organisation," but rather as a conglomerate of multiple operational groups and teams, using in part the same infrastructure and sometimes coordinating their efforts. Moreover, Lehtio emphasised that APT29's staff composition and, relatedly, many of its tools and tactics, also changed over the years, which is probably the case for all long-time operating APTs.

Sources [8], [11]

Impact type(s)

Direct

- **Political intelligence impact** (gathering information on political adversaries and allies to gain strategic and military advantage in potential conflict situations)

Indirect

- **Reputational impact** (2015 infiltration of the US Department of Defense email system; SolarWinds supply-chain compromise)

Sources [7], [14]

Incident type(s)

Data theft (Cyber espionage) against political/governmental targets (intrusion of networks at the Democratic National Committee (DNC) in 2015/2016).
Sources [10], [11]

Incident types documented by EuRepoC:
Data theft

Threat Level Index

13,5/24 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 APT29:

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	4,5 /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 APT29, on average attacks attributed to the group within the EuRepoC database, targeted 1.7 sectors per attack and 87% of all attacks were against political systems and/or critical infrastructure.
Geographical scope of attacks	3 /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 APT29, on average three countries were targeted per attack attributed to the group within the EuRepoC database.
Frequency of attacks	3 /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 APT29, the group was responsible for around 1 attack per year of activity (1.07).
Exploitation of Zero days	2 /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. 7% of attacks attributed to APT29 made use of zero-days.

→ Overall, the APT29 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 regarding their physical and socio-political effects, attacks by APT29 were frequent, targeting an above average number of countries and sectors, while sometimes exploiting zero-days.

TECHNICAL CHARACTERISTICS / PECULIARITIES / SOPHISTICATION

APT29 is a technically-highly sophisticated group that continues to evolve and improve its tactics, techniques, and procedures (TTPs) to better obfuscate its activities and thus avoid detection. Mandiant attests to the group's "exceptional operational security," e.g., via advanced tactics that target Microsoft 365. One of them is APT29's disabling of Purview Audit, a tool that can indicate if a threat actor has access to a certain mailbox, as reported by Mandiant in August 2022.

Basic attack pattern

Operations run a chain of spearphishing, deployment of backdoors and droppers (e.g., TEARDROP) to enable data exfiltration (mostly compromised servers and encrypted SSL connections). The group further employs HTTP/S and Twitter (backup) as command and control communications methods. APT29 uses social networks such as Twitter or GitHub, as well as cloud storage services, to forward commands and transfer data from infiltrated networks. To do this, the commands are encrypted and embedded in images (e.g., **GIFS**). The exfiltrated data is then uploaded to cloud storage services. APT29 also conducts "living-off-the-land-attacks," which utilise legitimate software and functions already available in the target system in order to execute their malicious operations. One more recent example of this tactic is the group's abuse of the Windows Credential Roaming feature, as reported by Mandiant in November 2022.

Zero-Day exploits

No explicit public reports exist about APT29's use of zero-day vulnerabilities, but the NCSC (UK GCHQ) - in collaboration with US counterparts at the National Security Agency (NSA), the Critical Infrastructure Security and Cybersecurity Agency (CISA), and the Department of Justice - warned that SVR actors, **including ATP29**, were actively scanning the internet for vulnerabilities. In May 2021, SolwarWinds acknowledged that the entry vector facilitating the infiltration of its networks had not been conclusively identified. The company ruled out the possibility that attackers developed access through known, unpatched vulnerabilities. Alongside a brute-force attack and social engineering, SolwarWinds considers the use of a zero-day in a third-party application or device as one of the three leading hypotheses. During investigations of the larger SolarWinds supply chain attack in December 2020, FireEye uncovered a separate compromise of SolarWinds' network monitoring platform Orion, further analysed by Microsoft, that used a zero-day vulnerability (CVE-2020-10148) to bypass authentication measures and install the SUPERNOVA web shell for remote access to servers of infected organisations. Secureworks linked this activity to the threat group SPIRAL, which it deems operates out of China.

Malware used (non-exhaustive)

HAMMERTOSS	TDISCOVER (alternative variant #1 to HAMMERTOSS)	UPLOADER (alternative variant #2 to HAMMERTOSS)
WellMESS + WellMail	**Cobalt Strike**	GoldMax
Sunburst (TEARDROP as dropper)		

Sources [2] [8] [11] [15] [16] [17] [18] [35] [43] [44] [45] [47]

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

MITRE Initial Access

Exploit public-facing application
External remote services
Phishing
Spearphishing attachment
Spearphishing link
Spearphishing via service
Supply chain compromise
Compromise software supply chain
Trusted relationship
Valid accounts
Domain accounts
Local accounts
Cloud accounts

MITRE Persistance

Account manipulation
Additional cloud credentials
Additional cloud roles
Additional email delegate permissions
Device registration
Boot or logon autostart execution
Registry run keys/startup folder
Create account
Cloud account
Event triggered execution
Windows management instrumentation event subscription
Accessibility features
External remote services
Modify authentication process
Hybrid identity
Scheduled task/job
Scheduled task
Server software component
Web shell
Valid accounts
Domain accounts
Local accounts
Cloud accounts

MITRE Defense Evasion

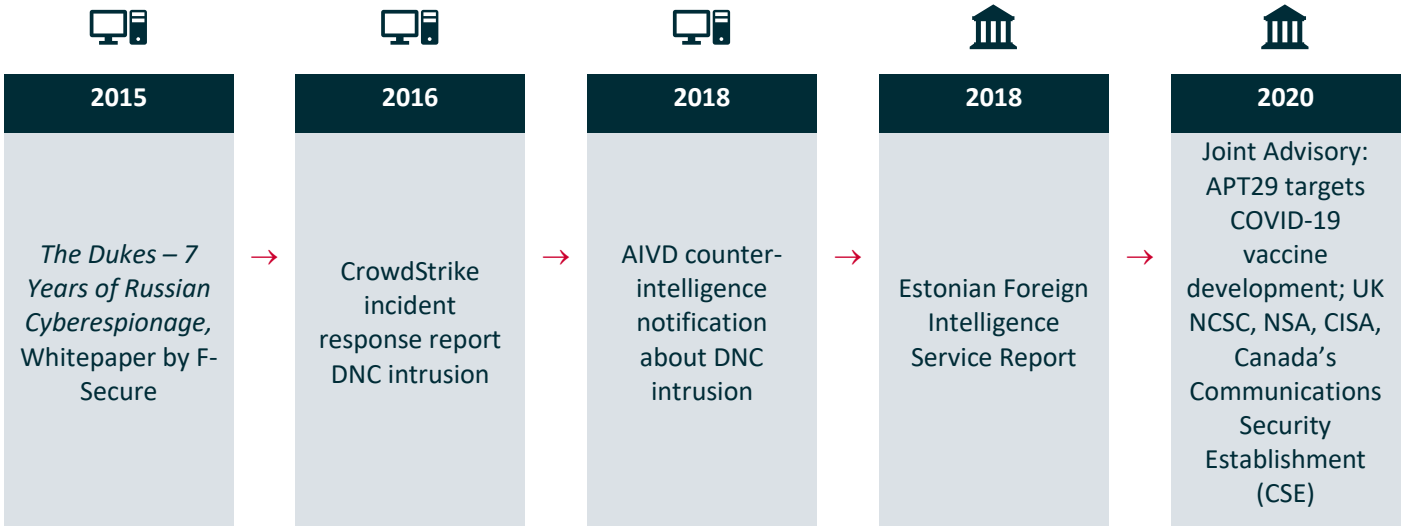
Deobfuscate/decode files or information
Domain policy modification
Domain trust modification
Impair defenses
Disable or modify tools
Disable Windows event logging
Disable or modify system firewall
Indicator removal
File deletion
Timestomp
Clear mailbox data
Masquerading
Masquerade task or service
Match legitimate name or location
Modify authentication process
Hybrid identity
Obfuscated files or information
Binary padding
Software padding
HTML smuggling
Subvert trust controls
Code signing
Mark-of-the-web bypass
System binary proxy execution
Mshta
Rundll32
Template injection
Use alternate authentication material
Application access token
Pass the ticket
Web session cookie
Valid accounts
Domain accounts
Local accounts
Cloud accounts

MITRE Exfiltration

Exfiltration over alternative protocol
Exfiltration over asymmetric encrypted non-C2 protocol

ATTRIBUTION

Attribution milestones



Sources [6] [7] [8] [10] [19] [20] [41]

Attribution ambiguities

DNC intrusion (2015/2016) - ATP 28 vs. ATP 29: While the two groups were both present in Democratic National Committee's servers at the same time, they appeared to be unaware of the other, each independently stealing the same passwords and otherwise duplicating their efforts. A **CrowdStrike forensic team determined that while APT29/Cozy Bear had been on the DNC's network for over a year (since 2015),** APT28/Fancy Bear had only broken in a few weeks prior to CrowdStrike's investigation. Internal Kremlin documents, disclosed in July 2021 to the wider public, indicate at least an internal "micromanagement" of the whole Russian undertaking from 2016 onwards. The report "No 32-04 \ vd" describes a high-level meeting on 22 January between Russian President Vladimir Putin and his intelligence agencies to develop a strategy for supporting candidate Donald Trump during the 2016 US presidential election. According to the document, which was assessed as being genuine by independent experts (source: The Guardian), Russian Defence Minister Shoigu was tasked with the supervision of the interagency endeavor. He was also tasked with the preparation of concrete hacking operations against US targets identified as sensitive and vulnerable by the SVR. If that information is accurate, it seems plausible that APT29 had already hacked the DNC in 2015 as part of its general "political intelligence mandate" and was then able to support APT28 in 2016 in the context of the hack-and-leak operation.

APT29 - an element of the SVR and/or FSB (?): Although more recent threat reports, as well as US and UK government statements in recent years, tend to view the SVR as the state entity directing APT29, the 2018 Estonian Foreign Intelligence Service's security report portrays the group as associated with, or part of, the SVR and FSB. F-Secure's observation of a small sample of APT29 targets in Russia that appear to be in the crosshairs of law enforcement over alleged criminal activity could be taken as an indicator that at least parts of APT29 are involved in interagency collaboration that aligns with the FSB's role as the domestic intelligence agency.

Revolving backdoors in the SolarWinds supply-chain attack (2019-2021) - Kazuar (Turla) connections in Sunburst (APT29): Kaspersky discovered several features in the Sunburst code that overlap with an advanced version of the Kazuar backdoor identified by Palo Alto in 2017. Researchers of the firm linked Kazuar to the APT group Turla. Sunburst is the centrepiece backdoor that APT29 pushed to SolarWinds customers through manipulated software updates. Kaspersky discusses multiple hypotheses explaining similarities between the two without weighting their probability. The most straightforward, though not necessarily most likely possibility is that Sunburst was developed by the same group as Kazuar, i.e. Turla. In graduations that move away from an institutionalised involvement of Turla, Kaspersky variously considers Kazuar may have served as indirect inspiration; both APT29 and Turla may have obtained their malware from the same source; Kazuar developers switched over to APT29 allowing for a transfer of tools and operational knowledge; or similarities to Kazuar have been purposefully built into Sunburst to distract from its origins as part of a false-flag operation. Palo Alto notes the iterative development of tools and code as typical for Turla operations. Components of Kazuar, specifically, trace back to as early as 2005. Sanction communications regarding the support function of Russian technology companies potentially shed further light on the theory about shared suppliers as the source for code overlaps. Two IT security firms designated by the US Treasury in April 2021, Neobit and AST (see section on sanctioned entities), provided technical assistance to both SVR- and FSB-conducted cyber operations. Kaspersky observed that later 2020 versions of Kazuar showed stronger parallels with Sunburst, suggesting an interface of recurring exchange between the groups deploying the tools. Use of shared contractors as go-betweens could fit in with this pattern**.**

APT29 - an umbrella designation for the SVR's cyber branch (?): Based on the US SolarWinds attribution, it is unclear to date whether APT29 is the only acting cyber unit associated with the SVR. The still-unsettled relationship between APT29 and Dark Halo - whether they are actually the same group or both parts of/subordinate to the SVR - further underscores this potential differentiation. The US threat intelligence company Volexity identified Dark Halo as responsible for the SolarWinds compromise on 14 December 2020, equating the group with FireEye's UNC2452, but not with APT29. Volexity instead tracks activity that it says overlaps with APT29 under the designation The Dukes. F-Secure researcher Artturi Lehtiö assessed in 2020 that APT29 is not a homogeneous "single organisation" but a conglomerate of various interacting/collaborating groups and teams. In this interpretation, APT29 might more accurately represent an umbrella term for the SVR's cyber branch, or at least comprises various operational teams.

Sources [4] [6] [8] [21] [22] [36] [37] [38] [39] [46]

Attribution and detection sensitivity

ATP29 is **highly sensitive to attribution and can quickly adapt to changes in the operational environment.** If their target started suspecting the malware HAMMERTOSS and thus monitored Twitter activity on their network, APT29 could easily switch to using the Uploader variant of HAMMERTOSS, which does not use Twitter and communicates directly to a specified URL. Due to their technical sophistication, APT29 can easily switch operational tactics. Mandiant reports conclude that ATP 29 places a **high emphasis on Operational Security (OPSEC)**. Nevertheless, they also have shown **consistent focus** on aggressively gaining and maintaining access to email accounts (government/diplomacy), easily switching tools/tactics if necessary. One more recent example for APT29's emphasis on detection evasion is the group's abuse of trusted cloud services, such as DropBox or Google Drive, which - in combination with encryption – makes it extremely difficult for targets to detect malicious activity, such as the deployment of malware using those services. As a reaction to F-Secure's report from 2015 on the group's activity, it seemed to go dark for at least half a year, indicating the setup of new infrastructure in the spring of 2016.

Sources [11], [16], [26]

LEGAL AND POLITICAL ACTIONS TAKEN AGAINST THE GROUP

Political/Legal/Law enforcement actions

The US Department of the Treasury sanctioned six Russian technology companies **in the context of the SolarWinds Hack on 15 April 2021, the same day the White House issued the "Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation" (E.O. 14024) and the related "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." The sanctioned entities not only included four Russian companies that are said to work for the SVR (Pasit, AO;** Neobit, OOO **[Neobit];** Advanced System Technology, AO **[AST]; and the Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation** [SVA]) but also other companies (e.g., Positive Technologies), which are associated with other Russian intelligence agencies, such as the FSB. The sanctions communication refers to the four companies as technical enablers of Russia's cyber operations, without stating explicitly whether the four companies are direct collaborators of APT29 or simply the SVR in general. The sanctions also set new restrictions on buying Russian sovereign debt. Reportedly, the US initiated the expulsion of ten Russian diplomats. The considerable scope and scale of the SolarWinds espionage campaign notwithstanding, the framing of the sanctions as a response to Russian harmful activity more broadly indicates a cumulative approach that places APT29 and the SVR in a wider context of malicious behaviour.

Sources: [17], [19], [22]

Indicted individuals / sanctioned (associated) entities

Sanctioned entities (15 April 2021):

Under new authorities established by E.O. 14024 designated with responding to Russian malign activities, the US Treasury Department designated six technology companies over their support of malicious cyber activities carried out by Russian intelligence services.

Among these companies, the Treasury identified the following four as offering support to the SVR:

- Pasit, AO
- Federal State Autonomous Scientific Establishment Scientific Research Institute Specialized Security Computing Devices and Automation (SVA)
- Neobit, OOO
- Advanced System Technology, AO (AST)

Two additional companies are listed under the sanctions regime for their assistance to other Russian intelligence services: ERA Technopolis, for its connections to the GRU; and Pozitiv Teknolodzhiz, AO (Positive Technologies), for its collaboration with the FSB and the GRU.

In addition to those actions pursuant to Executive Order 14024, the Treasury Department sanctioned 16 entities and 16 individuals for attempts "to influence the 2020 U.S. presidential election at the direction of the leadership of the Russian Government." One of the 16 designated entities, the Strategic Culture Foundation, operates under instructions from the SVR's Directorate MS, responsible for active measures.

Sources: [22], [40]

Landmark incidents

US Department of Defense email hacks 2015:
In 2015, ATP29 gained access to the unclassified email system used by the Department of Defense's Joint Chiefs of Staff. Consequently, the Pentagon had to replace both hardware and software, raising the question as to whether the attack was intended for intelligence and/or sabotage reasons.

DNC intrusion (starting in 2015):
APT29/Cozy Bear reportedly developed access to DNC systems in the summer of 2015. According to CrowdStrike, APT29 gained access via a backdoor and was able to exfiltrate an unknown amount of data, thereby presumably paving the way for APT28's subsequent hack-and-leak operation against the DNC.

SolarWinds compromise (starting in 2019): Supply chain attack against SolarWinds' Orion network monitoring tool through the Sunburst backdoor. APT29 subverted the software's maintenance function to distribute compromised updates to 18,000 of 33,000 Orion customers. While SolarWinds estimates only a significantly smaller subset of around 100 organisations were targeted in subsequent attack stages, the campaign compromised at least nine federal agencies in the US alongside high-value intelligence entities worldwide. From a software engineering perspective, Brad Smith, president of Microsoft, characterised the attack as the "largest and most sophisticated" to date. Microsoft assesses that 1,000 highly-trained engineers were involved in preparations of the campaign. For its investigations, the company itself assigned 500 analysts to dissect the activity. FireEye, which initially uncovered the compromise, had delegated 100 employees to make sense of suspicious behavior it first encountered in its own networks. Almost half of the 40 affected customers that Microsoft initially identified are active in the information technology sector, potentially paving the way for further cascades of vulnerability probing in products of downstream targets. Confirmed targets have also included security vendors Qualys, Fidelis Cybersecurity, Malwarebytes, Palo Alto Networks, and Cisco. CrowdStrike disclosed an attack attempt but concluded it was able to intercept the activity before it could achieve any impact. The cloud-based business email protection service Mimecast reported that a limited number of its source code repositories had been accessed. Microsoft disclosed similar, albeit isolated incidents, of accessed or downloaded source code components. In the breach of FireEye networks that led to the unraveling of SolarWinds' supply chain subversion, APT29 was able to collect the firm's red team toolkit, containing reconnaissance and penetration testing instruments. Part of the tools were specifically modified to circumvent security detection. In its assessment of the federal response to the SolarWinds incident, the US Government Accountability Office highlighted that CISA's incident support provides a baseline of confidence that the attackers have been locked out of infiltrated networks but also noted that the extended dwell-time may have allowed the threat actor to establish alternative means to perpetuate access.

Sources: [6] [11] [23] [24] [25] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57]

SOURCES

[1] Melissa Michael (2020), *039| Deconstructing the Dukes: A Researcher's Retrospective of APT29*, F-Secure Blog. Available at https://web.archive.org/web/20230213100918/https://blog.f-secure.com/podcast-dukes-apt29/ [Archived on: 13.02.2023].

[2] FireEye Threat Intelligence (2015), *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, FireEye. Available at https://web.archive.org/web/20221207170022/https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf [Archived on: 07.12.2022].

[3] Ryan McCombs (2016), *Bear Hunting: Tracking Down COZY BEAR Backdoors*, CrowdStrike Blog. Available at https://web.archive.org/web/20220529110050/https://www.crowdstrike.com/blog/bear-hunting-tracking-cozybear-backdoors/ [Archived on: 13.02.2023].

[4] The White House (2021), *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government*. Available at https://web.archive.org/web/20230203041243/https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ [Archived on: 13.02.2023].

[5] Foreign, Commonwealth & Development Office; The Rt Hon Dominic Raab (2021), *Russia: UK and US expose global campaign of malign activity by Russian intelligence services*. FCDO. Available at https://web.archive.org/web/20221015121127/http://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services [Archived on: 13.02.2023].

[6] 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].

[7] Eelco Bosch van Rosenthal (2018), *Dutch intelligence first to alert U.S. about Russian hack of Democratic Party*, NOS. Available at https://web.archive.org/web/20220922142638/https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party [Archived on: 13.02.2023].

[8] F-Secure Whitepaper (2015), *The Dukes: 7 Years of Russian Espionage*, F-Secure. Available at https://web.archive.org/web/20230128051344/http://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf [Archived on: 28.01.2023].

[9] Symantec Threat Hunter Team (2021), *Attacks Against the Government Sector*, Symantec. Available at https://web.archive.org/web/20221116160510/https://symantec.broadcom.com/hubfs/Attacks-Against-Government-Sector.pdf [Archived on: 16.11.2022].

[10] UK National Cyber Security Centre (2020), *UK and allies expose Russian attacks on coronavirus vaccine development*, National Cyber Security Centre (NCSC). Available at https://web.archive.org/web/20230213152334/https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development [Archived on: 13.02.2023].

[11] Mandiant (2022), *Assembling the Russian Nesting Doll: UNC2452 Merged into APT29*, Mandiant. Available at https://web.archive.org/web/20221227065208/https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29 [Archived on: 27 December 2022].

[12] CrowdStrike Adversary Universe, *Adversary: Cozy Bear*, CrowdStrike. Available at https://web.archive.org/web/20220901070815/https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/ [Archived on: 01.09.2022].

[13] Kaspersky Intelligence Reporting, *What's behind APT29?*, Kaspersky. Available at https://web.archive.org/web/20221225152021/https://www.kaspersky.com/enterprise-security/mitre/apt29 [Archived on: 25.12.2022].

[14] Evan Perez, Shimon Prokupecz (2015), *Sources: State Dept. hack the 'worst ever,'* CNN. Available at https://web.archive.org/web/20230213154641/https://edition.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/ [Archived on: 13.02.2023].

[15] FireEye, *Die Hackergruppen hinter Advanced Persistent Threats*, FireEye Deutschland. Available at https://web.archive.org/web/20230213160002/https://www.fireeye.de/current-threats/apt-groups.html#groups [Archived on: 13.02.2023].

[16] Mandiant Threat Research (2022), *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor*, Mandiant. Available at https://web.archive.org/web/20230116024834/https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor [Archived on: 16.01.2023].

[17] US Cybersecurity and Infrastructure Security Agency (2022), *Alert (AA22-011A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, CISA. Available at https://web.archive.org/web/20221217211912/https://www.cisa.gov/uscert/ncas/alerts/aa22-011a [Archived on: 17.12.2022].

[18] UK National Cyber Security Centre (2021), *Advisory: Further TTPs associated with SVR cyber actors*, GCHQ. Available at https://web.archive.org/web/20221218001943/https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf [Archived on: 18.12.2022].

[19] QuoIntelligence (2021), *US Sanctions Against Russia Unlikely to Limit Russian Cyber Espionage*, QuoIntelligence Blog. Available at https://web.archive.org/web/20221206115839/https://quointelligence.eu/2021/04/us-sanctions-against-russias-cyber-espionage/ [Archived on: 06.12.2022].

[20] Estonian Foreign Intelligence Service (2018), *International Security and Estonia: 2018*, Välisluureamet. Available at https://web.archive.org/web/20230202133006/https://www.valisluureamet.ee/doc/raport/2018-en.pdf [Archived on: 02.02.2023].

[21] Georgy Kucherin, Igor Kuznetsov, Constin Raiu (2021), *Sunburst backdoor – code overlaps with Kazuar*, Securelist/Kaspersky. Available at https://web.archive.org/web/20230213164540/https://securelist.com/sunburst-backdoor-kazuar/99981/ [Archived on: 13.02.2023].

[22] U.S. Department of the Treasury (2021), *Treasury Sanctions Russia with Sweeping New Sanctions Authority.* Available at https://web.archive.org/web/20230202161319/https://home.treasury.gov/news/press-releases/jy0127 [Archived on: 02.02.2023].

[23] Matthieu Faou, Mathieu Tartare, Thomas Dupuy (2019), *Operation Ghost: The Dukes aren't back – they never left*, ESET Research White Papers. Available at https://web.archive.org/web/20230213165605/https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf [Archived on: 13.02.2023].

[24] Saheed Oladimeji, Sean Michael Kerner (2022), *SolarWinds hack explained: Everything you need to know*, TechTarget. Available at https://web.archive.org/web/20230213165928/https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know [Archived on: 13.02.2023].

[25] Shaun Nichols (2022), *Russian cyber attacks on Ukraine driven by government groups*, TechTarget. Available at https://web.archive.org/web/20230212021017/https://www.techtarget.com/searchsecurity/news/252523950/Russian-cyber-attacks-on-Ukraine-driven-by-government-groups [Archived on: 12.02.2023].

[26] Mike Harbison, Peter Renals (2022), *Russian APT29 Hackers Use Online Storage Services, Dropbox and Google Drive*, Unit42. Available at https://web.archive.org/web/20230213170450/https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/ [Archived on: 13.02.2023].

[27] John Lambert (2021), *The hunt for NOBELIUM, the most sophisticated nation-state attacker in history*, Microsoft Security. Available at https://web.archive.org/web/20230201233601/https://www.microsoft.com/en-us/security/blog/2021/11/10/the-hunt-for-nobelium-the-most-sophisticated-nation-state-attack-in-history/ [Archived on: 01.02.2023].

[28] SecureWorks, *Threat Profile: Iron Ritual.* Available at https://web.archive.org/web/20230213202117/https://www.secureworks.com/research/threat-profiles/iron-ritual [Archived on: 13.02.2023].

[29] Damien Cash, et al. (2021), *Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns*, Volexity. Available at https://web.archive.org/web/20221208032006/http://www.volexity.com/blog/tag/dukes/ [Archived on: 08.12.2022].

[30] ESET, *Operation Ghost: The DNC hacking group "Dukes" still attacks government targets, ESET discovers*, ESET. Available at https://web.archive.org/web/20230213202243/https://www.eset.com/in/about/newsroom/press-releases/research/operation-ghost-the-dnc-hacking-group-dukes-still-attacks-government-targets-eset-discovers/ [Archived on: 13.02.2023].

[31] Douglas Bienstock (2023), *You Can't Audit Me: APT29 Continues Targeting Microsoft 365*, Mandiant. Available at https://web.archive.org/web/20230122005142/https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft [Archived on: 22.01.2023].

[32] Mark Galeotti (2016), *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations (ECFR). Available at https://web.archive.org/web/20230214105303/https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf [Archived on: 14.02.2023].

[33] 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].

[34] SEKOIA.IO, *APT29 aka Nobelium, Cozy Bear.* Available at https://web.archive.org/web/20230214110520/https://www.sekoia.io/en/resources/glossary/apt29-aka-nobelium-cozy-bear/ [Archived on: 14.02.2023].

[35] Thibault van Geluwe de Berlaere (2022), *They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming*, Mandiant. Available at https://web.archive.org/web/20230214111353/https://www.mandiant.com/resources/blog/apt29-windows-credential-roaming [Archived on: 14.02.2023].

[36] Damien Cash, et al. (2020), *Dark Halo Leverages SolarWinds Compromise to Breach Organizations*, Volexity Threat Research. Available at https://web.archive.org/web/20230214111654/https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/ [Archived on: 14.02.2023].

[37] Steven Adair (2016), *PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs*, Volexity. Available at https://web.archive.org/web/20230214111943/https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/ [Archived on: 14.02.2023].

[38] Joseph R. Biden (2021), *Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation*, The White House. Available at https://web.archive.org/web/20230214112214/https://www.whitehouse.gov/briefing-room/presidential-actions/2021/04/15/executive-order-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation/ [Archived on: 14.02.2023].

[39] Luke Harding, Julian Borger, Dan Sabbagh (2021), *Kremlin Papers appear to show Putin's plot to put Trump in White House*, The Guardian. Available at https://web.archive.org/web/20230214112545/https://www.theguardian.com/world/2021/jul/15/kremlin-papers-appear-to-show-putins-plot-to-put-trump-in-white-house [Archived on: 14.02.2023].

[40] U.S. Department of the Treasury (2021), *Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections.* Available at https://web.archive.org/web/20230214113212/https://home.treasury.gov/news/press-releases/jy0126 [Archived on: 14.02.2023].

[41] Dmitri Alperovitch (2016), *Bears in the Midst: Intrusion Into the Democratic National Committee*, 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].

[42] Kaspersky Global Research & Analysis Team (2013), *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor*, Kaspersky. Available at https://web.archive.org/web/20131217102330/https://www.securelist.com/en/blog/208194129/The_MiniDuke_Mystery_PDF_0_day_Government_Spy_Assembler_Micro_Backdoor [Archived on: 17.12.2013].

[43] US Cybersecurity and Infrastructure Security Agency (2021), *Malware Analysis Report (AR21-027A)*, CISA. Available at https://web.archive.org/web/20230222151224/https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-027a [Archived on: 22.02.2023].

[44] Microsoft 365 Defender Research Team and Microsoft Threat Intelligence Center (MSTIC) (2020), *Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers*, Microsoft. Available at https://web.archive.org/web/20230222151254/https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/ [Archived on: 22.02.2023].

[45] Secureworks Counter Threat Unit (2021), *SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group*, Secureworks. Available at https://web.archive.org/web/20220928153502/https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group [Archived on: 22.02.2023].

[46] Brandon Levene, Robert Falcone, and Tyler Halfpop (2021), *Kazuar: Multiplatform Espionage Backdoor with API Access*, Unit 42 Palo Alto Networks. Available at

https://web.archive.org/web/20230222152125/https://unit42.paloaltonetworks.com/unit42-kazuar-multiplatform-espionage-backdoor-api-access/ [Archived on: 22.02.2023].

[47] SolarWinds (2021), *Form 8-K Filing 7 May 2021*, US Securities and Exchange Commission. Available at https://web.archive.org/web/20230222152413/https://www.sec.gov/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm [Archived on: 22.02.2023].

[48] SolarWinds (2020), *Form 8-K Filing 14 December 2020*, US Securities and Exchange Commission. Available at https://web.archive.org/web/2/https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm [Archived on: 22.02.2023].

[49] US Government Accountability Office (2022), *Federal Response to SolarWinds and Microsoft Exchange Incidents*, GAO. Available at https://web.archive.org/web/20221217234133/https://www.gao.gov/assets/gao-22-104746.pdf [Archived on: 22.02.2023].

[50] CBS News 60 Minutes (2021), *Bill Whitaker interview with Brad Smith - SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments*, CBS News. Available at https://web.archive.org/web/20230222172324/https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/ [Archived on: 22.02.2023].

[51] Dustin Volz and Robert McMillan (2020), *Hack Suggests New Scope, Sophistication for Cyberattacks*, Wall Street Journal. Available at https://web.archive.org/web/20230222172723/https://www.wsj.com/articles/hack-suggests-new-scope-sophistication-for-cyberattacks-11608251360 [Archived on: 22.02.2023].

[52] Brad Smith (2020), *A moment of reckoning: the need for a strong and global cybersecurity response*, Microsoft. Available at https://web.archive.org/web/20230222172725/https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ [Archived on: 22.02.2023].

[53] Eduard Kovacs (2021), *More Cybersecurity Firms Confirm Being Hit by SolarWinds Hack,* SecurityWeek. Available at https://web.archive.org/web/20230222173054/https://www.securityweek.com/more-cybersecurity-firms-confirm-being-hit-solarwinds-hack/ [Archived on: 22.02.2023].

[54] Michael Sentonas (2020), *CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory,* CrowdStrike. Available at https://web.archive.org/web/20230222173139/https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/ [Archived on: 22.02.2023].

[55] Mimecast (2021), *SolarWinds Security Incident Report*. Available at https://web.archive.org/web/20230213162955/https://www.mimecast.com/incident-report/ [Archived on: 22.02.2023].

[56] Microsoft Security Response Center (2021), *Microsoft Internal Solorigate Investigation - Final Update,* Microsoft. Available at https://web.archive.org/web/20230222173123/https://msrc.microsoft.com/blog/2021/02/microsoft-internal-solorigate-investigation-final-update/ [Archived on: 22.02.2023].

[57] FireEye Threat Research (2021), *Unauthorized Access of FireEye Red Team Tools,* Mandiant. Available at https://web.archive.org/web/20230222173200/https://www.mandiant.com/resources/blog/unauthorized-access-of-fireeye-red-team-tools [Archived on: 22.02.2023].

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.
- **Jakob Bund** is an Associate at the German Institute for International and Security Affairs (SWP).
- **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: 02/03/2023