Cozy Bear

By Contributors to Wikimedia projects

Published: 2015-08-07 · Archived: 2026-04-05 17:54:17 UTC

From Wikipedia, the free encyclopedia

"Office Monkeys" redirects here. For the 2003 British hidden camera television programme, see Office Monkey.

Cozy Bear

Formation	c. 2008[1]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Region	Russia
Methods	Spearphishing, malware
Official language	Russian
Parent organization	SVR (confirmed), FSB (tentative)[2][3][4]
Affiliations	Fancy Bear
Formerly called	APT29, CozyCar, CozyDuke, Dark Halo, The Dukes, Grizzly Steppe (when combined with Fancy Bear), NOBELIUM, Office Monkeys, StellarParticle, UNC2452, YTTRIUM (possibly)

Cozy Bear, also known as **APT29**, is a Russian advanced persistent threat hacker group believed to be associated with Russian foreign intelligence by United States intelligence agencies and those of allied countries.[4][5] Dutch signals intelligence (AIVD) and American intelligence had been monitoring the group since 2014 and were able to link the hacker group to the Russian foreign intelligence agency (SVR) after compromising security cameras in their office.[6] CrowdStrike and Estonian intelligence[7] reported a tentative link to the Russian domestic/foreign intelligence agency (FSB).[2] Various groups designate it **CozyCar**,[8] **CozyDuke**,[9][10] **Dark Halo**, **The Dukes**,[11] **Midnight Blizzard**,[12] **NOBELIUM**,[13] **Office Monkeys**,[14] **StellarParticle**, **UNC2452**[15] with a

tentative connection to Russian hacker group YTTRIUM.[16] Symantec reported that Cozy Bear had been compromising diplomatic organizations and national governments since at least 2010.[17] Der Spiegel published documents in 2023 purporting to link Russian IT firm NTC Vulkan to Cozy Bear operations.[18]

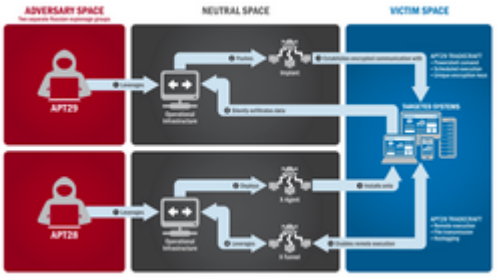

Diagram outlining Cozy Bear and Fancy Bear's process of using of malware to penetrate targets

APT29 has been observed to utilize a malware platform dubbed "Duke" which Kaspersky Lab reported in 2013 as "MiniDuke", observed in 2008 against United States and Western European targets.[1] Its initial development was reportedly in assembly language.[19] After Kaspersky's public reporting, later versions added C/C++ components and additional anti-analysis features which were dubbed "Cozyduke", "Cosmicduke", "SeaDuke" and "OnionDuke"[1][19]

Cozy Bear has been observed using an initial exploit or phishing email with malicious attachments to load a dropper which installs a Duke variant as a persistent trojan onto the target computer. It then gathers and sends data to a command and control server based on its configuration and/or live operator commands. Cozy Bear has been observed updating and refining its malware to improve cryptography, interactive functionality, and anti-analysis (including virtual machine detection).[19][20]

CosmicDuke was observed in 2013 as an updated version of MiniDuke with a more flexible plugin framework.[21] In 2014 OnionDuke leveraged the Tor network to conceal its command and control traffic and was distributed by infecting binary executables on the fly if they were transmitted unencrypted through a Russia-based Tor exit node.[22][23] "SeaDuke" appears to be a specialized trojan used in conjunction with other tools to compromise high-value targets.[17]

The group reportedly developed the 'HAMMERTOSS' trojan in 2015 to evade detection by relaying commands over covert channels on Twitter and GitHub.[24]

Intrusion campaigns

[edit]

Cozy Bear has been observed targeting and compromising organizations and foreign governments worldwide (including Russian opposition countries such as NATO and Five Eyes) and the commercial sector (notably financial, manufacturing, energy and telecom).[19] Targeting also included South America, and Asia (notably China and South Korea).[25] The United States is a frequent target, including the 2016 Clinton campaign, political parties (DNC, RNC), various executive agencies, the State Department and the White House.[20]

Intrusion into U.S. government agencies (2014)

[edit]

Cozy Bear malware was discovered on a Washington, D.C.–based private research institute in March 2014. Using compromised accounts at that organization, they sent phishing emails to other US government targets leveraging a malicious Flash file purporting to show "funny office monkeys".[17][1] By July the group had compromised several government networks.[17]

Exposure by Dutch intelligence (2014)

[edit]

In the summer of 2014, the Dutch General Intelligence and Security Service (AIVD) infiltrated the camera network used by Cozy Bear's physical office. This footage confirmed targeting of the US Democratic Party, State Department and White House and may have been used in the FBI investigation into 2016 Russian election interference.[6][26]

Intrusion into Pentagon email servers (2015)

[edit]

In August 2015 Cozy Bear was linked to a spear phishing campaign against the Pentagon, which the resulting investigation shut down the entire Joint Chiefs of Staff unclassified email system.[27][28]

Intrusion into the U.S. Democratic National Committee (2016)

[edit]

Cozy Bear and fellow Russian hacking group Fancy Bear (likely the GRU) were identified as perpetuating the Democratic National Committee intrusion.[2] While the two groups were both present in the DNC's servers at the same time, they appeared to operate independently.[29] Further confirming their independent operations, computer forensics determined that Fancy Bear had only compromised the DNC for a few weeks while Cozy Bear had done so for over a year.[30]

Attempted intrusion into US think tanks and NGOs (2016)

[edit]

After the 2016 United States presidential election, Cozy Bear was linked to spear phishing campaigns against multiple U.S.-based think tanks and non-governmental organizations (NGOs) related to national security, defense, international affairs, public policy, and European and Asian studies. Some emails were sent from compromised Harvard accounts.[31]

Attempted intrusion into Norwegian government (2017)

[edit]

On 3 February 2017, the Norwegian Police Security Service (PST) reported that Cozy Bear had launched spear phishing campaigns against at least nine individuals across the Ministry of Defence, Ministry of Foreign Affairs, and the Labour Party in January 2017.[32] Other targets included the Norwegian Radiation Protection Authority and members of the Norwegian Police Security Service, including section chief Arne Christian Haugstøyl. Norwegian Prime Minister Erna Solberg called the acts "a serious attack on our democratic institutions."[33]

Attempted intrusion into Dutch ministries (2016-2017)

[edit]

Reported in February 2017, both Cozy Bear and Fancy Bear had been attempting to compromise into Dutch ministries since 2016. Targets included the Ministry of General Affairs. Then-head of the Dutch intelligence service AIVD Rob Bertholee, stated on *EenVandaag* television that the Russian intrusion had targeted government documents.[34]

In response, Dutch Minister of the Interior and Kingdom Relations Ronald Plasterk announced that the March 2017 Dutch general election would be counted by hand.[35]

Duke variants and Operation Ghost (2019)

[edit]

In 2019 ESET reported that three malware variants had been attributed to Cozy Bear: PolyglotDuke, RegDuke and FatDuke. The malware had reportedly improved its anti-analysis methods and had been observed being used in intrusion campaigns dubbed "Operation Ghost".[36]

Attempted theft of COVID-19 vaccine data (2020)

[edit]

In July 2020 Five Eyes intelligence agencies NSA, NCSC and CSE reported that Cozy Bear had attempted to obtain COVID-19 vaccine data via intrusion campaigns.[37][38][39][40][4]

SUNBURST malware supply chain attack (2020)

[edit]

On 8 December 2020, U.S. cybersecurity firm FireEye disclosed that their internal tools had been stolen by a nation-state.[41][42] Later investigations implicated an internal compromise of software deployments of SolarWinds Orion IT management product to distribute a trojan that FireEye dubbed SUNBURST.[43] SolarWinds later confirmed that it had been compromised by a foreign nation state.[44] and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to issue an emergency directive that U.S. government agencies rebuild the affected software from trusted sources. It also attributed the intrusion campaign to the Russian SVR.[45]

Approximately 18,000 SolarWinds clients were vulnerable to the compromised Orion software.[46] Estimates based on DNS C2 activity indicate that around one percent of these SolarWinds clients were selected for stage-two operations, where the perpetrators installed backdoors to remotely control the vulnerable SolarWinds installations.[47] The *Washington Post* cited anonymous sources that attributed Cozy Bear as the perpetrator.[48][4]

According to Microsoft,[49] the hackers compromised SolarWinds code signing certificates and deployed a backdoor that allowed impersonation of a target's user account via a malicious Security Assertion Markup Language definition.[50]

Intrusion into U.S. civilian agencies (2020)

[edit]

On 20 December 2020 the U.S. Government reported that Cozy Bear was responsible for compromising the networks of civilian agencies Department of Commerce and Department of the Treasury.[51]

Intrusion into the U.S. Republican National Committee (2021)

[edit]

In July 2021, Cozy Bear breached systems of the Republican National Committee.[52][53] Officials said they believed the attack to have been conducted through Synnex, a compromised third-party IT vendor.([52])

Active Directory authentication bypasses (2021–2022)

[edit]

In 2021 Microsoft reported that Cozy Bear was leveraging the "FoggyWeb" tool to dump authentication tokens from compromised Active Directory instances. This was performed after they gained access to a machine on the target network and were able to obtain AD administrator credentials.[54] On 24 August 2022, Microsoft reported the group has deployed a similar tool "MagicWeb" to bypass user authentication on affected Active Directory Federated Services servers.[55]

Intrusion into Microsoft (2024)

[edit]

In January 2024, Microsoft reported having recently discovered and ended a breach beginning the previous November of the email accounts of their senior leadership and other employees in the legal and cybersecurity teams using a "password spray", a form of brute-force attack. This hack conducted by Midnight Blizzard appears to have aimed to find what the company knew about the hacking operation.[56]

Intrusion into TeamViewer (2024)

[edit]

German technology company TeamViewer SE reported on June 28, 2024, its corporate IT network had been compromised by Cozy Bear.[57] It stated that user data and its TeamViewer remote desktop software product was unaffected.[58]

- 2016 United States election interference by Russia
- *The Plot to Hack America*
- Vulkan files leak

1. ^ Jump up to: *a b c d* *"MiniDuke relation 'CozyDuke' Targets White House"*. *Threat Intelligence Times. 27 April 2015. Archived from the original on 11 June 2018. Retrieved 15 December 2016.*
2. ^ Jump up to: *a b c* *Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee". CrowdStrike Blog. Archived from the original on 24 May 2019. Retrieved 27 September 2016.*
3. ^ *"INTERNATIONAL SECURITY AND ESTONIA" (PDF). www.valisluureamet.ee. 2018. Archived from the original (PDF) on 2023-02-02. Retrieved 2020-12-15.*
4. ^ Jump up to: *a b c d* *Andrew S. Bowen (January 4, 2021). Russian Cyber Units (Report). Congressional Research Service. p. 1. Archived from the original on August 5, 2021. Retrieved July 25, 2021.*
5. ^ *Zettl-Schabath, Kerstin; Bund, Jakob; Gschwend, Timothy; Borrett, Camille (23 February 2023). "Advanced Threat Profile - APT29" (PDF). European Repository of Cyber Incidents. Archived (PDF) from the original on 19 April 2023. Retrieved 3 October 2024.*
6. ^ Jump up to: *a b* *Satter, Raphael; Corder, Mike (January 26, 2018). "Report: Dutch spies caught Russian hackers on tape". AP News. Archived from the original on 2 October 2024. Retrieved 3 October 2024.*
7. ^ *"International Security and Estonia" (PDF). Estonian Foreign Intelligence Service. 2018. Archived from the original (PDF) on 2 February 2023. Retrieved 3 October 2024.*
8. ^ *"Who Is COZY BEAR?". CrowdStrike. 19 September 2016. Archived from the original on 15 December 2020. Retrieved 15 December 2016.*
9. ^ *"F-Secure Study Links CozyDuke to High-Profile Espionage" (Press Release). 30 April 2015. Archived from the original on 7 January 2017. Retrieved 6 January 2017.*
10. ^ *"Cyberattacks Linked to Russian Intelligence Gathering" (Press Release). F-Secure. 17 September 2015. Archived from the original on 7 January 2017. Retrieved 6 January 2017.*
11. ^ *"Dukes Archives". Volexity. Retrieved 2024-10-03.*
12. ^ *Weise, Karen (January 19, 2024). "Microsoft Executives' Emails Hacked by Group Tied to Russian Intelligence". The New York Times. Archived from the original on January 20, 2024. Retrieved January 20, 2024.*
13. ^ *"Midnight Blizzard". www.microsoft.com. Retrieved 2024-10-03.*
14. ^ *"The CozyDuke APT". securelist.com. 2015-04-21. Retrieved 2024-10-03.*
15. ^ *"UNC2452 Merged into APT29 | Russia-Based Espionage Group". Google Cloud Blog. Retrieved 2024-10-03.*
16. ^ *Team, Microsoft Defender Security Research (2018-12-03). "Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers". Microsoft Security Blog. Retrieved 2024-10-03.*
17. ^ Jump up to: *a b c d* *""Forkmeiamfamous": Seaduke, latest weapon in the Duke armory". Symantec Security Response. 13 July 2015. Archived from the original on 14 December 2016. Retrieved 15 December 2016.*

18. ^ *Harding, Luke; Ganguly, Manisha; Sabbagh, Dan (2023-03-30). "'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics". The Guardian. ISSN 0261-3077. Retrieved 2024-10-03.*
19. ^ Jump up to: **a b c d** *Kaspersky Lab's Global Research & Analysis Team (3 July 2014). "Miniduke is back: Nemesis Gemina and the Botgen Studio". Securelist. Archived from the original on 12 May 2020. Retrieved 19 May 2020.*
20. ^ Jump up to: **a b** *Baumgartner, Kurt; Raiu, Costin (21 April 2015). "The CozyDuke APT". Securelist. Archived from the original on 30 January 2018. Retrieved 19 May 2020.*
21. ^ *"CosmicDuke is a newer version of the MiniDuke backdoor". APT Kaspersky Securelist. Retrieved 2024-10-03.*
22. ^ *"The Case of The Modified Binaries". Leviathan Security Group - Penetration Testing, Security Assessment, Risk Advisory. Retrieved 2024-10-03.*
23. ^ *"OnionDuke: APT Attacks Via the Tor Network". F-Secure Labs. 14 November 2014. Retrieved 2024-10-03.*
24. ^ *"HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group". FireEye. 9 July 2015. Archived from the original on 23 March 2019. Retrieved 7 August 2015.*
25. ^ *"Threat Profile: APT29" (PDF). Blackpoint Cyber. June 2024. Retrieved 3 October 2024.*
26. ^ *Noack, Rick (January 26, 2018). "The Dutch were a secret U.S. ally in war against Russian hackers, local media reveal". The Washington Post. Archived from the original on January 26, 2018. Retrieved February 15, 2023.*
27. ^ *Kube, Courtney (7 August 2015). "Russia hacks Pentagon computers: NBC, citing sources". Archived from the original on 8 August 2019. Retrieved 7 August 2015.*
28. ^ *Starr, Barbara (7 August 2015). "Official: Russia suspected in Joint Chiefs email server intrusion". Archived from the original on 8 August 2019. Retrieved 7 August 2015.*
29. ^ *"Bear on bear". The Economist. 22 September 2016. Archived from the original on 20 May 2017. Retrieved 14 December 2016.*
30. ^ *Ward, Vicky (October 24, 2016). "The Man Leading America's Fight Against Russian Hackers Is Putin's Worst Nightmare". Esquire. Archived from the original on January 26, 2018. Retrieved December 15, 2016.*
31. ^ *"PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs". Volexity. November 9, 2016. Archived from the original on December 20, 2016. Retrieved December 14, 2016.*
32. ^ *"Norge utsatt for et omfattende hackerangrep". NRK. February 3, 2017. Archived from the original on February 5, 2017. Retrieved February 4, 2017.*
33. ^ *Stanglin, Doug (February 3, 2017). "Norway: Russian hackers hit spy agency, defense, Labour party". USA Today. Archived from the original on April 5, 2017. Retrieved August 26, 2017.*
34. ^ *Modderkolk, Huib (February 4, 2017). "Russen faalden bij hackpogingen ambtenaren op Nederlandse ministeries". De Volkskrant (in Dutch). Archived from the original on February 4, 2017. Retrieved February 4, 2017.*
35. ^ *Cluskey, Peter (February 3, 2017). "Dutch opt for manual count after reports of Russian hacking". The Irish Times. Archived from the original on February 3, 2017. Retrieved February 4, 2017.*
36. ^ *"Operation Ghost: The Dukes aren't back – they never left". ESET Research. October 17, 2019. Archived from the original on March 11, 2020. Retrieved February 8, 2020.*

37. ^ *"NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID"*. National Security Agency Central Security Service. Archived from the original on 11 December 2020. Retrieved 25 July 2020.
38. ^ *"CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development – Thursday, July 16, 2020"*. cse-cst.gc.ca. Communications Security Establishment. 14 July 2020. Archived from the original on 16 July 2020. Retrieved 16 July 2020.
39. ^ James, William (16 July 2020). *"Russia trying to hack and steal COVID-19 vaccine data, says Britain"*. Reuters UK. Archived from the original on 17 July 2020. Retrieved 16 July 2020.
40. ^ *"UK and allies expose Russian attacks on coronavirus vaccine development"*. National Cyber Security Centre. 16 July 2020. Archived from the original on 16 July 2020. Retrieved 16 July 2020.
41. ^ Sanger, David E.; Perlroth, Nicole (December 8, 2020). *"FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State"*. The New York Times. Archived from the original on December 15, 2020. Retrieved December 15, 2020.
42. ^ agencies, Guardian staff and (December 9, 2020). *"US cybersecurity firm FireEye says it was hacked by foreign government"*. the Guardian. Archived from the original on December 16, 2020. Retrieved December 15, 2020.
43. ^ *"Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor"*. FireEye. Archived from the original on 2020-12-15. Retrieved 2020-12-15.
44. ^ *"Security Advisory | SolarWinds"*. www.solarwinds.com. Archived from the original on 2020-12-15. Retrieved 2020-12-15.
45. ^ *"cyber.dhs.gov - Emergency Directive 21-01"*. cyber.dhs.gov. 13 December 2020. Archived from the original on 15 December 2020. Retrieved 15 December 2020.
46. ^ Cimpanu, Catalin. *"SEC filings: SolarWinds says 18,000 customers were impacted by recent hack"*. ZDNet. Archived from the original on 2020-12-15. Retrieved 2020-12-15.
47. ^ SEC-T (2021-10-16). *SEC-T 0x0D: Erik Hjelmvik - Hiding in Plain Sight - How the SolarWinds Hack Went Undetected*. Retrieved 2025-05-22 – via YouTube.
48. ^ Nakashima, Ellen; Timberg, Craig. *"Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce"*. Washington Post. ISSN 0190-8286. Archived from the original on 2020-12-13. Retrieved 2020-12-14.
49. ^ *"Important steps for customers to protect themselves from recent nation-state cyberattacks"*. 14 December 2020. Archived from the original on 20 December 2020. Retrieved 16 December 2020.
50. ^ Goodin, Dan; Timberg. *"~18,000 organizations downloaded backdoor planted by Cozy Bear hackers"*. Ars Technica. Archived from the original on 2020-12-16. Retrieved 2020-12-15.
51. ^ Sanger, David E. (2020-12-13). *"Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect"*. The New York Times. ISSN 0362-4331. Archived from the original on 2020-12-13. Retrieved 2021-10-03.
52. ^ Jump up to: **a** **b** Turton, William; Jacobs, Jennifer (6 July 2021). *"Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit"*. Bloomberg News. Archived from the original on 6 July 2021. Retrieved 7 July 2021.
53. ^ Campbell, Ian Carlos (6 July 2021). *"Russian hackers reportedly attacked GOP computer systems in the U.S"*. The Verge. Archived from the original on 7 July 2021. Retrieved 7 July 2021.
54. ^ Nafisi, Ramin (2021-09-27). *"FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor"*. Microsoft Security Blog. Retrieved 2024-10-03.

55. ^ *"MagicWeb: NOBELIUM's post-compromise trick to authenticate as anyone". Microsoft Security Blog. Microsoft. 24 August 2022. Archived from the original on 26 August 2022. Retrieved 26 August 2022.*
56. ^ *Franceschi-Bicchierai, Lorenzo (19 January 2024). "Hackers breached Microsoft to find out what Microsoft knows about them". Techcrunch. Retrieved 22 January 2024.* {{cite news}} : CS1 maint: deprecated archival service (link)
57. ^ *"Teamviewer accuses Russia-linked hackers of cyberattack". Reuters. 28 June 2024. Retrieved 30 June 2024.*
58. ^ *Kunz, Christopher (2024-06-28). "TeamViewer-Angriff: Die Spur führt nach Russland". Heise online (in German). Retrieved 2024-10-02.*

- Russian government employees charged in hacking campaigns
