Fancy Bear

"STRONTIUM" redirects here. For other uses, see Strontium (disambiguation).
Fancy Bear

Formation	c. (circa) 2004–2007[2]
Type	Advanced persistent threat
Purpose	Cyberespionage, cyberwarfare
Region	Russia
Methods	Zero-days, spearphishing, malware
Official language	Russian
Parent organization	GRU[1][2][3]
Affiliations	Cozy Bear
Formerly called	• APT28 • Pawn Storm • Sofacy Group • Sednit • STRONTIUM • Tsar Team • Threat Group-4127 • Grizzly Steppe (when combined with Cozy Bear)

Fancy Bear (also known as **APT28** (by Mandiant), **Pawn Storm**, **Sofacy Group** (by Kaspersky), **Sednit**, **Tsar Team** (by FireEye) and **STRONTIUM** (by Microsoft))[2][4] is a Russian cyber espionage group. Cybersecurity firm CrowdStrike has said with a medium level of confidence that it is associated with the Russian military intelligence agency GRU.[5] [6] The UK's Foreign and Commonwealth Office[7] as well as security firms SecureWorks,[8] ThreatConnect,[9] and Mandiant,[10] have also said the group is sponsored by the Russian government. In 2018, an indictment by the United States Special Counsel identified Fancy Bear as GRU **Unit 26165**.[3][2]

The name "Fancy Bear" comes from a coding system security researcher Dmitri Alperovitch uses to identify hackers.[11]

Likely operating since the mid-2000s, Fancy Bear's methods are consistent with the capabilities of state actors. The group targets government, military, and security organizations, especially Transcaucasian and NATO-aligned states. Fancy Bear is thought to be responsible for cyber attacks on the German parliament, the Norwegian parliament, the French television station TV5Monde, the White House, NATO, the Democratic National Committee, the Organization for Security and Co-operation in Europe and the campaign of French presidential candidate Emmanuel Macron.[12]

The group promotes the political interests of the Russian government, and is known for hacking Democratic National Committee emails to attempt to influence the outcome of the United States 2016 presidential elections.

Fancy Bear is classified by FireEye as an advanced persistent threat.[10] Among other things, it uses zero-day exploits, spear phishing and malware to compromise targets.

Discovery and security reports

Trend Micro designated the actors behind the Sofacy malware as **Operation Pawn Storm** on October 22, 2014.[13] The name was due to the group's use of "two or more connected tools/tactics to attack a specific target similar to the chess strategy,"[14] known as pawn storm.

Network security firm FireEye released a detailed report on Fancy Bear in October 2014. The report designated the group as "Advanced Persistent Threat 28" (APT28) and described how the hacking group used zero-day exploits of the Microsoft Windows operating system and Adobe Flash.[15] The report found operational details indicating that the source is a "government sponsor based in Moscow". Evidence collected by FireEye suggested that Fancy Bear's malware was compiled primarily in a Russian-language build environment and occurred mainly during work hours paralleling Moscow's time zone.[16] FireEye director of threat intelligence Laura Galante referred to the group's activities as "state espionage"[17] and said that targets also include "media or influencers."[18][19]

The name "Fancy Bear" derives from the coding system that Dmitri Alperovitch's company CrowdStrike uses for hacker groups. "Bear" indicates that the hackers are from Russia. "Fancy" refers to "Sofacy", a word in the malware that reminded the analyst who found it, of Iggy Azalea's song "Fancy".[1]

Attacks

Fancy Bear's targets have included Eastern European governments and militaries, the country of Georgia and the Caucasus, Ukraine,[20] security-related organizations such as NATO, as well as US defense contractors Academi (formerly known as Blackwater and Xe Services), Science Applications International Corporation (SAIC),[21] Boeing, Lockheed Martin, and Raytheon.[20] Fancy Bear has also attacked citizens of the Russian Federation

that are political enemies of the Kremlin, including former oil tycoon Mikhail Khodorkovsky, and Maria Alekhina of the band Pussy Riot.[20] SecureWorks, a cybersecurity firm headquartered in the United States, concluded that from March 2015 to May 2016, the "Fancy Bear" target list included not merely the United States Democratic National Committee, but tens of thousands of foes of Putin and the Kremlin in the United States, Ukraine, Russia, Georgia, and Syria. Only a handful of Republicans were targeted, however.[22] An AP analysis of 4,700 email accounts that had been attacked by Fancy Bear concluded that no country other than Russia would be interested in hacking so many very different targets that seemed to have nothing else in common other than their being of interest to the Russian government.[20]

Fancy Bear also seems to try to influence political events in order for friends or allies of the Russian government to gain power.

In 2011–2012, Fancy Bear's first-stage malware was the "Sofacy" or SOURFACE implant. During 2013, Fancy Bear added more tools and backdoors, including CHOPSTICK, CORESHELL, JHUHUGIT, and ADVSTORESHELL.[23]

Attacks on prominent journalists in Russia, the United States, Ukraine, Moldova, the Baltics, and elsewhere

From mid-2014 until the fall of 2017, Fancy Bear targeted numerous journalists in the United States, Ukraine, Russia, Moldova, the Baltics, and other countries who had written articles about Vladimir Putin and the Kremlin. According to the Associated Press and SecureWorks, this group of journalists is the third largest group targeted by Fancy Bear after diplomatic personnel and U.S. Democrats. Fancy Bear's targeted list includes Adrian Chen, the Armenian journalist Maria Titizian, Eliot Higgins at Bellingcat, Ellen Barry and at least 50 other *New York Times* reporters, at least 50 foreign correspondents based in Moscow who worked for independent news outlets, Josh Rogin, a *Washington Post* columnist, Shane Harris, a *Daily Beast* writer who in 2015 covered intelligence issues, Michael Weiss, a CNN security analyst, Jamie Kirchick with the Brookings Institution, 30 media targets in Ukraine, many at the Kyiv Post, reporters who covered the Russian-backed war in eastern Ukraine, as well as in Russia where the majority of journalists targeted by the hackers worked for independent news (e.g. *Novaya Gazeta* or *Vedomosti*) such as Ekaterina Vinokurova at Znak.com and mainstream Russian journalists Tina Kandelaki, Ksenia Sobchak, and the Russian television anchor Pavel Lobkov, all of which worked for Dozhd.[24]

German attacks (from 2014)

Fancy Bear is thought to have been responsible for a six-month-long cyber-attack on the German parliament that began in December 2014.[25] On 5 May 2020, German federal prosecutors issued an arrest warrant for Dimitri Badin in relation with the attacks.[26] The

attack completely paralyzed the Bundestag's IT infrastructure in May 2015. To resolve the situation, the entire parliament had to be taken offline for days. IT experts estimate that a total of 16 gigabytes of data were downloaded from Parliament as part of the attack.[27]

The group is also suspected to be behind a spear phishing attack in August 2016 on members of the Bundestag and multiple political parties such as Linken-faction leader Sahra Wagenknecht, Junge Union and the CDU of Saarland.[28][29][30][31] Authorities feared that sensitive information could be gathered by hackers to later manipulate the public ahead of elections such as Germany's next federal election which was due in September 2017.[28]

U.S. military wives' death threats (February 10, 2015)

Five wives of U.S. military personnel received death threats from a hacker group calling itself "CyberCaliphate", claiming to be an Islamic State affiliate, on February 10, 2015.[32][33][34][35] This was later discovered to have been a false flag attack by Fancy Bear, when the victims' email addresses were found to have been in the Fancy Bear phishing target list.[33] Russian social media trolls have also been known to hype and rumor monger the threat of potential Islamic State terror attacks on U.S. soil in order to sow fear and political tension.[33]

French television hack (April 2015)

On April 8, 2015, French television network TV5Monde was the victim of a cyber-attack by a hacker group calling itself "CyberCaliphate" and claiming to have ties to the terrorist organization Islamic State of Iraq and the Levant (ISIL). French investigators later discounted the theory that militant Islamists were behind the cyber-attack, instead suspecting the involvement of Fancy Bear.[36]

Hackers breached the network's internal systems, possibly aided by passwords openly broadcast by TV5,[37] overriding the broadcast programming of the company's 12 channels for over three hours.[38] Service was only partially restored in the early hours of the following morning and normal broadcasting services were disrupted late into April 9.[38] Various computerised internal administrative and support systems including e-mail were also still shut down or otherwise inaccessible due to the attack.[39][38] The hackers also hijacked TV5Monde's Facebook and Twitter pages to post the personal information of relatives of French soldiers participating in actions against ISIS, along with messages critical of President François Hollande, arguing that the January 2015 terrorist attacks were "gifts" for his "unforgivable mistake" of partaking in conflicts that "[serve] no purpose".[40][38]

The director-general of TV5Monde, Yves Bigot, later said that the attack nearly destroyed the company; if it had taken longer to restore broadcasting, satellite distribution channels would have been likely to cancel their contracts. The attack was designed to be destructive, both of equipment and of the company itself, rather than for propaganda or espionage, as had been the case for most other cyber-attacks. The attack was carefully planned; the first known penetration of the network was on January 23, 2015.[41] The attackers then carried out

reconnaissance of TV5Monde to understand the way in which it broadcast its signals, and constructed bespoke malicious software to corrupt and destroy the Internet-connected hardware that controlled the TV station's operations, such as the encoder systems. They used seven different points of entry, not all part of TV5Monde or even in France—one was a company based in the Netherlands that supplied the remote controlled cameras used in TV5's studios.[41] Between February 16 and March 25 the attackers collected data on TV5 internal platforms, including its IT Internal Wiki, and verified that login credentials were still valid.[41] During the attack, the hackers ran a series of commands extracted from TACACS logs to erase the firmware from switches and routers.[41]

Although the attack purported to be from IS, France's cyber-agency told Bigot to say only that the messages *claimed to be* from IS. He was later told that evidence had been found that the attackers were the APT 28 group of Russian hackers. No reason was found for the targeting of TV5Monde, and the source of the order to attack, and funding for it, is not known. It has been speculated that it was probably an attempt to test forms of cyber-weaponry. The cost was estimated at €5m ($5.6m; £4.5m) in the first year, followed by recurring annual cost of over €3m ($3.4m; £2.7m) for new protection. The company's way of working had to change, with authentication of email, checking of flash drives before insertion, and so on, at significant detriment to efficiency for a news media company that must move information.[42]

root9B report (May 2015)

Security firm root9B released a report on Fancy Bear in May 2015 announcing its discovery of a targeted spear phishing attack aimed at financial institutions. The report listed international banking institutions that were targeted, including the United Bank for Africa, Bank of America, TD Bank, and UAE Bank. According to the root9B, preparations for the attacks started in June 2014 and the malware used "bore specific signatures that have historically been unique to only one organization, Sofacy."[43] Security journalist Brian Krebs questioned the accuracy of root9B's claims, postulating that the attacks had actually originated from Nigerian phishers.[44] In June 2015 well respected security researcher Claudio Guarnieri published a report based on his own investigation of a concurrent SOFACY attributed exploit against the German Bundestag[45] and credited root9B with having reported, "the same IP address used as Command & Control server in the attack against Bundestag (176.31.112.10)", and went on to say that based on his examination of the Bundestag attack, "at least some" indicators contained within root9B's report appeared accurate, including a comparison of the hash of the malware sample from both incidents. root9B later published a technical report comparing Claudio's analysis of SOFACY attributed malware to their own sample, adding to the veracity of their original report.[46]

EFF spoof, White House and NATO attack (August 2015)

In August 2015, Fancy Bear used a zero-day exploit of Java, spoofing the Electronic Frontier Foundation and launching attacks on the White House and NATO. The hackers used a spear phishing attack, directing emails to the false URL electronicfrontierfoundation.org.[47][48]

World Anti-Doping Agency (August 2016)

In August 2016, the World Anti-Doping Agency reported the receipt of phishing emails sent to users of its database claiming to be official WADA communications requesting their login details. After reviewing the two domains provided by WADA, it was found that the websites' registration and hosting information were consistent with the Russian hacking group Fancy Bear.[49][50] According to WADA, some of the data the hackers released had been forged.[51]

Due to evidence of widespread doping by Russian athletes, WADA recommended that Russian athletes be barred from participating in the 2016 Rio Olympics and Paralympics. Analysts said they believed the hack was in part an act of retaliation against whistleblowing Russian athlete Yuliya Stepanova, whose personal information was released in the breach.[52] In August 2016, WADA revealed that their systems had been breached, explaining that hackers from Fancy Bear had used an International Olympic Committee (IOC)-created account to gain access to their Anti-doping Administration and Management System (ADAMS) database.[53] The hackers then used the website fancybear.net to leak what they said were the Olympic drug testing files of several athletes who had received therapeutic use exemptions, including gymnast Simone Biles, tennis players Venus and Serena Williams and basketball player Elena Delle Donne.[54] The hackers honed in on athletes who had been granted exemptions by WADA for various reasons. Subsequent leaks included athletes from many other countries.[53]

Dutch Safety Board and Bellingcat

Eliot Higgins and other journalists associated with Bellingcat, a group researching the shooting down of Malaysia Airlines Flight 17 over Ukraine, were targeted by numerous spearphishing emails. The messages were fake Gmail security notices with Bit.ly and TinyCC shortened URLs. According to ThreatConnect, some of the phishing emails had originated from servers that Fancy Bear had used in previous attacks elsewhere. Bellingcat is known for having demonstrated that Russia is culpable for the shooting down of MH17, and is frequently derided by the Russian media.[55][56]

The group targeted the Dutch Safety Board, the body conducting the official investigation into the crash, before and after the release of the board's final report. They set up fake SFTP and VPN servers to mimic the board's own servers, likely for the purpose of spearphishing usernames and passwords.[57] A spokesman for the DSB said the attacks were not successful.[58]

Democratic National Committee (2016)

Fancy Bear carried out spear phishing attacks on email addresses associated with the Democratic National Committee in the first quarter of 2016.[59][60] On March 10, phishing emails that were mainly directed at old email addresses of 2008 Democratic campaign staffers began to arrive. One of these accounts may have yielded up to date contact lists. The next day, phishing attacks expanded to the non-public email addresses of high level Democratic Party officials. Hillaryclinton.com addresses were attacked, but required two factor authentication for access. The attack redirected towards Gmail accounts on March 19. Podesta's Gmail account was breached the same day, with 50,000 emails stolen. The phishing attacks intensified in April,[60] although the hackers seemed to become suddenly inactive for the day on April 15, which in Russia was a holiday in honor of the military's electronic warfare services.[61] The malware used in the attack sent stolen data to the same servers that were used for the group's 2015 attack on the German parliament.[1]

On June 14, CrowdStrike released a report publicizing the DNC hack and identifying Fancy Bear as the culprits. An online persona, Guccifer 2.0, then appeared, claiming sole credit for the breach.[62]

Another sophisticated hacking group attributed to the Russian Federation, nicknamed Cozy Bear, was also present in the DNC's servers at the same time. However the two groups each appeared to be unaware of the other, as each independently stole the same passwords and otherwise duplicated their efforts. Cozy Bear appears to be a different agency, one more interested in traditional long-term espionage.[61] A CrowdStrike forensic team determined that while Cozy Bear had been on the DNC's network for over a year, Fancy Bear had only been there a few weeks.[1]

Ukrainian artillery

An infected version of an app to control the D-30 Howitzer was allegedly distributed to the Ukrainian artillery

See also: Russian military intervention in Ukraine (2014–present)

According to CrowdStrike from 2014 to 2016, the group used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android app whose original purpose was to control targeting data for the D-30 Howitzer artillery. The app, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums. CrowdStrike initially claimed that more than 80% of Ukrainian D-30 Howitzers were destroyed in the war, the highest percentage loss of any

artillery pieces in the army (a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces[63]).[64] According to the Ukrainian army CrowdStrike's numbers were incorrect and that losses in artillery weapons "were way below those reported" and that these losses "have nothing to do with the stated cause".[65] CrowdStrike has since revised this report after the International Institute for Strategic Studies (IISS) disavowed its original report, claiming that the malware hacks resulted in losses of 15–20% rather than their original figure of 80%.[66]

Windows zero-day (October 2016)

On October 31, 2016, Google's Threat Analysis Group revealed a zero-day vulnerability in most Microsoft Windows versions that is the subject of active malware attacks. On November 1, 2016, Microsoft Executive Vice President of the Windows and Devices Group Terry Myerson posted to Microsoft's Threat Research & Response Blog, acknowledging the vulnerability and explaining that a "low-volume spear-phishing campaign" targeting specific users had utilized "two zero-day vulnerabilities in Adobe Flash and the down-level Windows kernel." Microsoft pointed to Fancy Bear as the threat actor, referring to the group by their in-house code name *STRONTIUM*.[67]

Dutch ministries (February 2017)

In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands revealed that Fancy Bear and Cozy Bear had made several attempts to hack into Dutch ministries, including the Ministry of General Affairs, over the previous six months. Rob Bertholee, head of the AIVD, said on *EenVandaag* that the hackers were Russian and had tried to gain access to secret government documents.[68]

In a briefing to parliament, Dutch Minister of the Interior and Kingdom Relations Ronald Plasterk announced that votes for the Dutch general election in March 2017 would be counted by hand.[69]

IAAF hack (February 2017)

The officials of International Association of Athletics Federations (IAAF) stated in April 2017 that its servers had been hacked by the "Fancy Bear" group. The attack was detected by cybersecurity firm Context Information Security which identified that an unauthorised remote access to IAAF's servers had taken place on February 21. IAAF stated that the hackers had accessed the *Therapeutic Use Exemption* applications, needed to use medications prohibited by WADA.[70][71]

German and French elections (2016–2017)

See also: French presidential election, 2017; German federal election, 2017; and 2017 Macron e-mail leaks

Researchers from Trend Micro in 2017 released a report outlining attempts by Fancy Bear to target groups related to the election campaigns of Emmanuel Macron and Angela Merkel. According to the report, they targeted the Macron campaign with phishing and attempting to install malware on their site. French government cybersecurity agency ANSSI confirmed these attacks took place, but could not confirm APT28's responsibility.[72] Marine Le Pen's campaign does not appear to have been targeted by APT28, possibly indicating Russian preference for her campaign. Putin had previously touted the benefits to Russia if Marine Le Pen were elected.[73]

The report says they then targeted the German Konrad Adenauer Foundation and Friedrich Ebert Foundation, groups that are associated with Angela Merkel's Christian Democratic Union and opposition Social Democratic Party, respectively. Fancy Bear set up fake email servers in late 2016 to send phishing emails with links to malware.[74]

International Olympic Committee (2018)

On January 10, 2018, the "Fancy Bears Hack Team" online persona leaked what appeared to be stolen International Olympic Committee (IOC) and U.S. Olympic Committee emails, dated from late 2016 to early 2017, were leaked in apparent retaliation for the IOC's banning of Russian athletes from the 2018 Winter Olympics as a sanction for Russia's systematic doping program. The attack resembles the earlier World Anti-Doping Agency (WADA) leaks. It is not known whether the emails are fully authentic, because of Fancy Bear's history of salting stolen emails with disinformation. The mode of attack was also not known, but was probably phishing.[75][76]

Cyber Security experts have also claimed that attacks also appear to have been targeting the professional sports drug test bottling company known as the Berlinger Group.[77]

Swedish Sports Confederation

The Swedish Sports Confederation reported Fancy Bear was responsible for an attack on its computers, targeting records of athletes' doping tests.[78]

United States conservative groups (2018)

The software company Microsoft reported in August 2018 that the group had attempted to steal data from political organizations such as the International Republican Institute and the Hudson Institute think tanks. The attacks were thwarted when Microsoft security staff won control of six net domains.[79] In its announcement Microsoft advised that "we currently have no evidence these domains were used in any successful attacks before the DCU transferred control of them, nor do we have evidence to indicate the identity of the ultimate targets of any planned attack involving these domains".[80]

The Ecumenical Patriarchate and other clergy (August 2018)

According to the August 2018 report by the Associated Press, Fancy Bear had been for years targeting the email correspondence of the officials of the Ecumenical Patriarchate of Constantinople headed by the Ecumenical Patriarch Bartholomew I.[81] The publication appeared at a time of heightened tensions between the Ecumenical Patriarchate, the seniormost of all the Eastern Orthodox Churches, and the Russian Orthodox Church (the Moscow Patriarchate) over the issue of the full ecclesiastical independence (autocephaly) for the Orthodox Church in Ukraine, sought after by the Ukrainian government. The publication cited experts as saying that the grant of autocephaly to the Church in Ukraine would erode the power and prestige of the Moscow Patriarchate and would undermine its claims of transnational jurisdiction.[81] Cyber attacks also targeted Orthodox Christians in other countries as well as Muslims, Jews and Catholics in the United States, Ummah, an umbrella group for Ukrainian Muslims, the papal nuncio in Kiev and Yosyp Zisels, who directs Ukraine's Association of Jewish Organizations and Communities.[81]

Indictments in 2018

FBI wanted poster of officers indicted in connection to Fancy Bear

In October 2018, an indictment by a U.S. federal grand jury of seven Russian men, all GRU officers, in relation to the attacks was unsealed. The indictment states that from December 2014 until a least May 2018, the GRU officers conspired to conduct "persistent and sophisticated computer intrusions affecting U.S. persons, corporate entities, international organizations, and their respective employees located around the world, based on their strategic interest to the Russian government."[82][83] The U.S. Department of Justice stated that the conspiracy, among other goals, aimed "to publicize stolen information as part of an influence and disinformation campaign designed to undermine, retaliate against, and otherwise delegitimize" the efforts of the World Anti-Doping Agency, an international anti-doping organization that had published the McLaren Report, a report that exposed extensive doping of Russian athletes sponsored by the Russian government.[82] The defendants were charged with computer hacking, wire fraud, aggravated identity theft, and money laundering.[82]

2019 think tank attacks

In February 2019, Microsoft announced that it had detected spear-phishing attacks from APT28, aimed at employees of the German Marshall Fund, Aspen Institute Germany, and the German Council on Foreign Relations.[84][85] Hackers from the group purportedly sent phishing e-mails to 104 email addresses across Europe in an attempt to gain access to employer credentials and infect sites with malware.[86][87]

2019 strategic Czech institution

In 2020, the Czech National Cyber and Information Security Agency reported a cyber-espionage incident in an unnamed strategic institution, possibly the Ministry of Foreign Affairs,[88] most likely carried out by Fancy Bear.[89]

2020 Norwegian Parliament attack

In August 2020 the Norwegian Storting reported a "significant cyber attack" on their e-mail system. In September 2020, Norway's foreign minister, Ine Marie Eriksen Søreide, accused Russia of the attack. Norwegian Police Security Service concluded in December 2020 that "The analyses show that it is likely that the operation was carried out by the cyber actor referred to in open sources as APT28 and Fancy Bear," and that "sensitive content has been extracted from some of the affected email accounts.".[90]

Characteristics and techniques

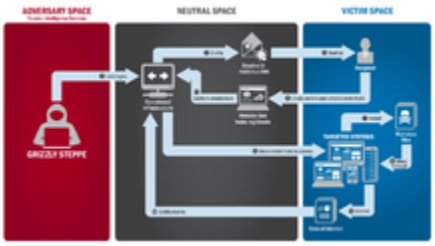

Diagram showing Grizzly Steppe's (Fancy Bear and Cozy Bear) process of employing spear phishing

Fancy Bear employs advanced methods consistent with the capabilities of state actors.[91] They use spear phishing emails, malware drop websites disguised as news sources, and zero-day vulnerabilities. One cybersecurity research group noted their use of six different zero-day exploits in 2015, a technical feat that would require large numbers of programmers seeking out previously unknown vulnerabilities in top-of-the-line commercial software. This is regarded as a sign that Fancy Bear is a state-run program and not a gang or a lone hacker.[92][93]

One of Fancy Bear's preferred targets is web-based email services. A typical compromise will consist of web-based email users receiving an email urgently requesting that they change their passwords to avoid being hacked. The email will contain a link to a spoof website that is designed to mimic a real webmail interface, users will attempt to login and

their credentials will be stolen. The URL is often obscured as a shortened bit.ly link[94] in order to get past spam filters. Fancy Bear sends these phishing emails primarily on Mondays and Fridays. They also send emails purportedly containing links to news items, but instead linking to malware drop sites that install toolkits onto the target's computer.[92] Fancy Bear also registers domains that resemble legitimate websites, then create a spoof of the site to steal credentials from their victims.[62] Fancy Bear has been known to relay its command traffic through proxy networks of victims that it has previously compromised.[95]

Software that Fancy Bear has used includes ADVSTORESHELL, CHOPSTICK, JHUHUGIT, and XTunnel. Fancy Bear utilises a number of implants, including Foozer, WinIDS, X-Agent, X-Tunnel, Sofacy, and DownRange droppers.[62] Based on compile times, FireEye concluded that Fancy Bear has consistently updated their malware since 2007.[95] To avert detection, Fancy Bear returns to the environment to switch their implants, changes its command and control channels, and modifies its persistent methods.[91] The threat group implements counter-analysis techniques to obfuscate their code. They add junk data to encoded strings, making decoding difficult without the junk removal algorithm.[95] Fancy Bear takes measures to prevent forensic analysis of its hacks, resetting the timestamps on files and periodically clearing the event logs.[62]

According to an indictment by the United States Special Counsel, X-Agent was "developed, customized, and monitored" by GRU Lieutenant Captain Nikolay Yuryevich Kozachek.[2]

Fancy Bear has been known to tailor implants for target environments, for instance reconfiguring them to use local email servers.[95] In August 2015, Kaspersky Lab detected and blocked a version of the ADVSTORESHELL implant that had been used to target defense contractors. An hour and a half following the block, Fancy Bear actors had compiled and delivered a new backdoor for the implant.[23]

Education

Unit 26165 was involved in the design of the curriculum at several Moscow public schools, including School 1101.[96]

Related personas

Fancy Bear sometimes creates online personas to sow disinformation, deflect blame, and create plausible deniability for their activities.[97]

Guccifer 2.0

Main article: Guccifer 2.0
An online persona that first appeared and claimed responsibility for the DNC hacks the same day the story broke that Fancy Bear was responsible.[98] Guccifer 2.0 claims to be a Romanian hacker, but when interviewed by *Motherboard* magazine, they were asked

questions in Romanian and appeared to be unable to speak the language.[99] Some documents they have released appear to be forgeries cobbled together from material from previous hacks and publicly available information, then salted with disinformation.[99]

Fancy Bears' Hack Team

A website created to leak documents taken in the WADA and IAAF attacks was fronted with a brief manifesto dated September 13, 2016, proclaiming that the site is owned by "Fancy Bears' hack team", which it said is an "international hack team" who "stand for fair play and clean sport".[100] The site took responsibility for hacking WADA and promised that it would provide "sensational proof of famous athletes taking doping substances", beginning with the US Olympic team, which it said "disgraced its name by tainted victories".[100] WADA said some of the documents leaked under this name were forgeries, and that data had been changed.[101][100]

Anonymous Poland

A Twitter account named "Anonymous Poland" (@anpoland) claimed responsibility for the attack on the World Anti-Doping Agency[102] and released data stolen from the Court of Arbitration for Sport, a secondary target.[103][104] ThreatConnect supports the view that Anonymous Poland is a sockpuppet of Fancy Bear, noting the change from a historical focus on internal politics. A screen capture video uploaded by Anonymous Poland shows an account with Polish language settings, but their browser history showed that they had made searches in Google.ru (Russia) and Google.com (US), but not in Google.pl (Poland).[103]

See also

Notes

2.^ Aleksei Sergeyevich Morenets (Моренец Алексей Сергеевич), Evgenii Mikhaylovich Serebriakov, Ivan Sergeyevich Yermakov (Ермаков Иван Сергеевич), Artem Andreyevich Malyshev (Малышев Артём Андреевич), Dmitriy Sergeyevich Badin (Бадин Дмитрий Сергеевич, Oleg Mikhaylovich Sotnikov (Олег Михайлович Сотников), Alexey Valerevich Minin (Алексей Валерьевич Минин).[83]

References

1. ^ *a b c d Ward, Vicky (October 24, 2016). "The Man Leading America's Fight Against Russian Hackers Is Putin's Worst Nightmare". Esquire.com.*
2. ^ *a b c d Poulson, Kevin (21 July 2018). "Mueller Finally Solves Mysteries About Russia's 'Fancy Bear' Hackers". The Daily Beast. Retrieved 21 July 2018.*
3. ^ *a b "Indicting 12 Russian Hackers Could Be Mueller's Biggest Move Yet". Wired. Retrieved 4 October 2018.*

4. ^ DimitrisGritzalis , Marianthi Theocharidou , George Stergiopoulos (2019-01-10). Critical Infrastructure Security and Resilience: Theories, Methods, Tools ... Springer, 2019. ISBN 9783030000240.
5. ^ "INTERNATIONAL SECURITY AND ESTONIA" (PDF). Valisluureamet.ee. 2018. Archived from the original (PDF) on 26 October 2020. Retrieved 4 October 2018.
6. ^
7. ^ Wintour, Patrick (3 October 2018). "UK accuses Kremlin of ordering series of 'reckless' cyber-attacks". the Guardian. Retrieved 4 October 2018.
8. ^ Threat Group-4127 Targets Hillary Clinton Presidential Campaign. Secureworks.com (Report). 16 June 2016. Archived from the original on 20 July 2016. Retrieved 22 December 2016. and is gathering intelligence on behalf of the Russian government.
9. ^ "Russian Cyber Operations on Steroids". Threatconnect.com. 19 August 2016. Russian FANCY BEAR tactics
10. ^ a b "APT28: A Window into Russia's Cyber Espionage Operations?". Fireeye.com. 27 October 2016. We assess that APT28 is most likely sponsored by the Russian government
11. ^ "The Man Leading America's Fight Against Russian Hackers Is Putin's Worst Nightmare". Esquire.com. 2016-10-24. Retrieved 2017-05-07.
12. ^ Hern, Alex (8 May 2017). "Macron hackers linked to Russian-affiliated group behind US attack". the Guardian. Retrieved 16 March 2018.
13. ^ Gogolinski, Jim (22 October 2014). "Operation Pawn Storm: The Red in SEDNIT". Trend Micro.
14. ^ "Operation Pawn Storm: Using Decoys to Evade Detection" (PDF). Trend Micro. 2014.
15. ^ Menn, Joseph (April 18, 2015). "Russian cyber attackers used two unknown flaws: security company". Reuters.
16. ^ Kumar, Mohit (October 30, 2014). "APT28 — State Sponsored Russian Hacker Group". The Hacker News.
17. ^ Mamiit, Aaron (October 30, 2014). "Meet APT28, Russian-backed malware for gathering intelligence from governments, militaries: Report". Tech Times.
18. ^ "APT28: A Window into Russia's Cyber Espionage Operations?". FireEye.com. October 27, 2014.
19. ^ Weissman, Cale Guthrie (June 11, 2015). "France: Russian hackers posed as ISIS to hack a French TV broadcaster". Business Insider.
20. ^ a b c d Satter, Raphael; Donn, Jeff; Myers, Justin (2 November 2017). "Digital hitlist shows Russian hacking went well beyond U.S. elections". Chicago Tribune. AP. Retrieved 10 November 2017.
21. ^ Yadron, Danny (October 28, 2014). "Hacking Trail Leads to Russia, Experts Say". Wall Street Journal.
22. ^ SATTER, RAPHAEL; DONN, JEFF (November 1, 2017). "Russian hackers pursued Putin foes, not just U.S. Democrats". US News & World Report. Associated Press. Retrieved November 2, 2017.

23. ^ a b *Kaspersky Lab's Global Research & Analysis Team (December 4, 2015). "Sofacy APT hits high profile targets with updated toolset - Securelist". Securelist.*
24. ^ *"Russian hackers hunted journalists in years-long campaign". Star-Advertiser. Honolulu. Associated Press. December 22, 2017. Retrieved December 23, 2017.*
25. ^ *"Russian Hackers Suspected In Cyberattack On German Parliament". London South East. Alliance News. June 19, 2015.*
26. ^ *Reuters (5 May 2020). "Germany Issues Arrest Warrant for Russian Suspect in Parliament Hack: Newspaper". The New York Times.*
27. ^ *Bennhold, Katrin (13 May 2020). "Merkel Is 'Outraged' by Russian Hack but Struggling to Respond". The New York Times. Retrieved 14 May 2020.*
28. ^ a b *"Hackers lurking, parliamentarians told". Deutsche Welle. Retrieved 21 September 2016.*
29. ^ *"Hackerangriff auf deutsche Parteien". Süddeutsche Zeitung. Retrieved 21 September 2016.*
30. ^ *Holland, Martin. "Angeblich versuchter Hackerangriff auf Bundestag und Parteien". Heise. Retrieved 21 September 2016.*
31. ^ *"Wir haben Fingerabdrücke". Frankfurter Allgemeine. Retrieved 21 September 2016.*
32. ^ *"Russian Hackers Who Posed As ISIS Militants Threatened Military Wives". Talkingpointsmemo.com. 8 May 2018. Retrieved 4 October 2018.*
33. ^ a b c *"Russian hackers posed as IS to threaten military wives". Chicago Tribune. Archived from the original on 12 June 2018. Retrieved 7 June 2018.*
34. ^ *Brown, Jennings. "Report: Russian Hackers Posed as ISIS to Attack U.S. Military Wives". gizmodo.com. Retrieved 4 October 2018.*
35. ^ *"Russian hackers posed as IS to threaten military wives". Apnews.com. Retrieved 4 October 2018.*
36. ^ a b c d *Suiche, Matt (June 10, 2017). "Lessons from TV5Monde 2015 Hack". Comae Technologies. Archived from the original on June 13, 2017.*
37. ^ *Gordon Corera (10 October 2016). "How France's TV5 was almost destroyed by 'Russian hackers'". BBC News.*
38. ^ *Walker, Danielle (May 13, 2015). "APT28 orchestrated attacks against global banking sector, firm finds". SC Magazine. Archived from the original on March 2, 2018. Retrieved September 1, 2015.*
39. ^ *Doctorow, Cory (August 28, 2015). "Spear phishers with suspected ties to Russian government spoof fake EFF domain, attack White House". Boing Boing.*
40. ^ *Quintin, Cooper (August 27, 2015). "New Spear Phishing Campaign Pretends to be EFF". Eff.org.*
41. ^ *Hyacinth Mascarenhas (August 23, 2016). "Russian hackers 'Fancy Bear' likely breached Olympic drug-testing agency and DNC, experts say". International Business Times. Retrieved September 13, 2016.*
42. ^ *Gallagher, Sean (6 October 2016). "Researchers find fake data in Olympic anti-doping, Guccifer 2.0 Clinton dumps". Ars Technica. Retrieved 26 October 2016.*

43. ^ *Thielman, Sam (August 22, 2016). "Same Russian hackers likely breached Olympic drug-testing agency and DNC". The Guardian. Retrieved December 11, 2016.*
44. ^ a b *Meyer, Josh (September 14, 2016). "Russian hackers post alleged medical files of Simone Biles, Serena Williams". NBC News.*
45. ^ *"American Athletes Caught Doping". Fancybear.net. September 13, 2016. Archived from the original on December 24, 2017. Retrieved November 2, 2016.*
46. ^ *Nakashima, Ellen (28 September 2016). "Russian hackers harassed journalists who were investigating Malaysia Airlines plane crash". Washington Post. Retrieved 26 October 2016.*
47. ^ *ThreatConnect (28 September 2016). "ThreatConnect reviews activity targeting Bellingcat, a key contributor in the MH17 investigation". ThreatConnect. Retrieved 26 October 2016.*
48. ^ *Feike Hacquebord (22 October 2015). "Pawn Storm Targets MH17 Investigation Team". Trend Micro.*
49. ^ *"Russia 'tried to hack MH17 inquiry system'". AFP. 23 October 2015. Archived from the original on 21 August 2018. Retrieved 4 November 2016.*
50. ^ *Sanger, David E.; Corasaniti, Nick (14 June 2016). "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump". The New York Times. Retrieved 26 October 2016.*
51. ^ a b *Satter, Raphael; Donn, Jeff; Day, Chad (4 November 2017). "Inside story: How Russians hacked the Democrats' emails". AP. Retrieved 10 November 2017.*
52. ^ a b *"Bear on bear". The Economist. 22 September 2016. Retrieved 14 December 2016.*
53. ^ a b c d *Alperovitch, Dmitri (June 15, 2016). "Bears in the Midst: Intrusion into the Democratic National Committee »". Crowdstrike.com.*
54. ^ *Meyers, Adam (22 December 2016). "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units". Crowdstrike.com.*
55. ^ *Kuzmenko, Oleksiy; Cobus, Pete. "Cyber Firm Rewrites Part of Disputed Russian Hacking Report". Voanews.com. Retrieved 26 March 2017.*
56. ^ *Gallagher, Sean (1 November 2016). "Windows zero-day exploited by same group behind DNC hack". Ars Technica. Retrieved 2 November 2016.*
57. ^ *Modderkolk, Huib (February 4, 2017). "Russen faalden bij hackpogingen ambtenaren op Nederlandse ministeries". De Volkskrant (in Dutch).*
58. ^ *Cluskey, Peter (February 3, 2017). "Dutch opt for manual count after reports of Russian hacking". The Irish Times.*
59. ^ *Rogers, James (April 3, 2017). "International athletics body IAAF hacked, warns that athletes' data may be compromised". Fox News.*
60. ^ *Eric Auchard (24 April 2017). "Macron campaign was target of cyber attacks by spy-linked group". Reuters.com. Retrieved 27 April 2017.*
61. ^ *Seddon, Max; Stothard, Michael (May 4, 2017). "Putin awaits return on Le Pen investment". Financial Times. Archived from the original on May 5, 2017.*

62. ^ *Matsakis, Louise (January 10, 2018). "Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban". Wired.*
63. ^ Rebecca R. Ruiz, Rebecca Russian Hackers Release Stolen Emails in New Effort to Undermine Doping Investigators, *New York Times* (January 10, 2018).
64. ^ Nick Griffin, Performanta,[1] Archived 2018-02-06 at the Wayback Machine (January 26, 2018).
65. ^ *Johnson, Simon; Swahnberg, Olof (May 15, 2018). Pollard, Niklas; Lawson, Hugh (eds.). "Swedish sports body says anti-doping unit hit by hacking attack". Reuters.*
66. ^ *Smith, Brad (21 August 2018). "We are taking new steps against broadening threats to democracy". Microsoft. Retrieved 22 August 2018.*
67. ^ a b c *Raphael Satter (27 August 2018). "Russian Cyberspies Spent Years Targeting Orthodox Clergy". Bloomberg. Associated Press.*
68. ^ a b *Brady, Scott W. "Indictment 7 GRU Officers_Oct2018" (PDF). United States District Court for the Western District of Pennsylvania. Retrieved July 8, 2018.*
69. ^ *Dwoskin, Elizabeth; Timberg, Craig (February 19, 2019). "Microsoft says it has found another Russian operation targeting prominent think tanks". The Washington Post. The "spear-phishing" attacks — in which hackers send out phony emails intended to trick people into visiting websites that look authentic but in fact enable them to infiltrate their victims' corporate computer systems — were tied to the APT28 hacking group, a unit of Russian military intelligence that interfered in the 2016 U.S. election. The group targeted more than 100 European employees of the German Marshall Fund, the Aspen Institute Germany, and the German Council on Foreign Relations, influential groups that focus on transatlantic policy issues.*
70. ^ *Burt, Tom (February 20, 2019). "New steps to protect Europe from continued cyber threats". Microsoft. The attacks against these organizations, which we're disclosing with their permission, targeted 104 accounts belonging to organization employees located in Belgium, France, Germany, Poland, Romania, and Serbia. MSTIC continues to investigate the sources of these attacks, but we are confident that many of them originated from a group we call Strontium. The attacks occurred between September and December 2018. We quickly notified each of these organizations when we discovered they were targeted so they could take steps to secure their systems, and we took a variety of technical measures to protect customers from these attacks.*
71. ^ *Tucker, Patrick (2019-02-20). "Russian Attacks Hit US-European Think Tank Emails, Says Microsoft". Defense One. Retrieved 2019-04-07.*
72. ^ a b *Robinson, Teri (14 June 2016). "Russian hackers access Trump files in DNC hack". SC Magazine US. Archived from the original on 20 December 2016. Retrieved 13 December 2016.*
73. ^ a b c *Thielman, Sam; Ackerman, Spencer (29 July 2016). "Cozy Bear and Fancy Bear: did Russians hack Democratic party and if so, why?". The Guardian. ISSN 0261-3077. Retrieved 2016-12-12.*
74. ^ *Cluley, Graham (20 October 2016). "New ESET research paper puts Sednit under the microscope". WeLiveSecurity. Retrieved 26 October 2016.*

75. ^ *Frenkel, Sheera (October 15, 2016). "Meet Fancy Bear, The Russian Group Hacking The US Election". BuzzFeed.*
76. ^ *Troianovski, Anton; Nakashima, Ellen; Harris, Shane (December 28, 2018). "How Russia's military intelligence agency became the covert muscle in Putin's duels with the West". The Washington Post. Archived from the original on December 29, 2018.*
77. ^ *Koebler, Jason (15 June 2016). "'Guccifer 2.0' Claims Responsibility for DNC Hack, Releases Docs to Prove it". Motherboard. Retrieved 3 November 2016.*
78. ^ a b *Franceschi-Bicchierai, Lorenzo. "'Guccifer 2.0' Is Bullshitting Us About His Alleged Clinton Foundation Hack". Motherboard. Retrieved 3 November 2016.*
79. ^ a b c *Bartlett, Evan (26 March 2018). "Fancy Bears: Who are the shady hacking group exposing doping, cover-ups and corruption in sport?". The Independent. Retrieved 24 May 2018.*
80. ^ *BBC (5 October 2016). "Fancy Bears doping data 'may have been changed' says Wada". BBC. Retrieved 3 November 2016.*
81. ^ *Nance, Malcolm (2016). The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election. Skyhorse Publishing. ISBN 978-1-5107-2333-7.*
82. ^ a b *Cimpanu, Catalin (23 August 2016). "Russia Behind World Anti-Doping Agency & International Sports Court Hacks". Softpedia.*
83. ^ *Feike Hacquebord (2017). Two Years of Pawn Storm — Examining an Increasingly Relevant Threat (PDF) (Report). Trend Micro.*

External links

"Microsoft Security Intelligence Report: Strontium". Microsoft Malware Protection Center. November 15, 2015.

Hacking in the 2010s

Timeline

Major incidents

- Operation Aurora
- Australian cyberattacks
- Operation ShadowNet
- Operation Payback

2010

2011	• DigiNotar • DNSChanger • HBGary Federal • Operation AntiSec • Operation Tunisia • PlayStation • RSA SecurID compromise
2012	• LinkedIn hack • Stratfor email leak • Operation High Roller
2013	• South Korea cyberattack • Snapchat hack • Cyberterrorism Attack of June 25 • 2013 Yahoo! data breach • Singapore cyberattacks
2014	• Anthem medical data breach • Operation Tovar • 2014 celebrity nude photo leak • 2014 JPMorgan Chase data breach • Sony Pictures hack • Russian hacker password theft • 2014 Yahoo! data breach
2015	• Office of Personnel Management data breach • Hacking Team • Ashley Madison data breach • VTech data breach • Ukrainian Power Grid Cyberattack • SWIFT banking hack
2016	• Bangladesh Bank robbery • Hollywood Presbyterian Medical Center ransomware incident • Commission on Elections data breach • Democratic National Committee cyber attacks • Vietnam Airport Hacks • DCCC cyber attacks • Indian Bank data breaches • Surkov leaks • Dyn cyberattack • Russian interference in the 2016 U.S. elections • 2016 Bitfinex hack

2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
2018	• Trustico • Atlanta cyberattack • SingHealth data breach
2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking
Hacktivism	• Anonymous associated events • CyberBerkut • GNAA • Goatse Security • Lizard Squad • LulzRaft • LulzSec • New World Hackers • NullCrew • OurMine • PayPal 14 • RedHack • TeaMp0isoN • TDO • UGNazi • Ukrainian Cyber Alliance

Advanced persistent threats	• Bureau 121 • Charming Kitten • Cozy Bear • Dark Basin • Elfin Team • Equation Group • Fancy Bear • Guccifer 2.0 • Hacking Team • Helix Kitten • Iranian Cyber Army • Lazarus Group (BlueNorOff) (AndAriel) • NSO Group • PLA Unit 61398 • PLA Unit 61486 • PLATINUM • Pranknet • Red Apollo • Rocket Kitten • Syrian Electronic Army • Tailored Access Operations • The Shadow Brokers • Yemen Cyber Army
Individuals	• George Hotz • Guccifer • Jeremy Hammond • Junaid Hussain • Kristoffer von Hassel • Mustafa Al-Bassam • MLT • Ryan Ackroyd • Sabu • Topiary • Track2 • The Jester

Major vulnerabilities publicly disclosed	• Evercookie (2010) • iSeeYou (2013) • Heartbleed (2014) • Shellshock (2014) • POODLE (2014) • Rootpipe (2014) • Row hammer (2014) • JASBUG (2015) • Stagefright (2015) • DROWN (2016) • Badlock (2016) • Dirty COW (2016) • Cloudbleed (2017) • Broadcom Wi-Fi (2017) • EternalBlue (2017) • DoublePulsar (2017) • Silent Bob is Silent (2017) • KRACK (2017) • ROCA vulnerability (2017) • BlueBorne (2017) • Meltdown (2018) • Spectre (2018) • EFAIL (2018) • Exactis (2018) • Speculative Store Bypass (2018) • Lazy FP State Restore (2018) • TLBleed (2018) • SigSpoof (2018) • Foreshadow (2018) • Microarchitectural Data Sampling (2019) • BlueKeep (2019) • Kr00k (2019)
Malware	
2010	• Bad Rabbit • SpyEye • Stuxnet
2011	• Alureon • Duqu • Kelihos • Metulji botnet • Stars

2012	• Carna • Dexter • FBI • Flame • Mahdi • Red October • Shamoon
2013	• CryptoLocker • DarkSeoul
2014	• Brambul • Carbanak • Careto • DarkHotel • Duqu 2.0 • FinFisher • Gameover ZeuS • Regin
2015	• Dridex • Hidden Tear • Rombertik • TeslaCrypt
2016	• Hitler • Jigsaw • KeRanger • MEMZ • Mirai • Pegasus • Petya (NotPetya) • X-Agent
2017	• BrickerBot • Kirk • LogicLocker • *Rensenware* ransomware • Triton • WannaCry • XafeCopy

- Grum
- Joanap
- NetTraveler
- R2D2
- Tinba
- Titanium
- Vault 7
- ZeroAccess botnet

2019