Date	Attack	Actor	Details
6/26/2004	Operation Pawn Storm	Fancy Bear	Operation Pawn Storm – later named FANCY BEAR by cybersecurity firm Crowdstrike - emerges. Operation Pawn Storm is an ongoing cyber espionage campaign that's as far-reaching as it is ambitious. It has been known to primarily target military, embassy, and defense contractor personnel from the United States and its allies, including government institutions such as the North Atlantic Treaty Organization (NATO). Opposing factions, dissidents of the Russian government, international media, and high-profile political personalities in Ukraine are targeted as well.
1/1/2005	Turla aka Uroburos or Snake (2005 - 2014)	Venomous Bear	Attributed to Russia. Targets were in the United States, western Europe, and the Ukraine. This was a long running surveillance campaign that was started in 2005. initial intelligence had indicated western powers were key targets, but it was later determined embassies for Eastern Bloc nations were of more interest. Embassies in Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, and Germany were all attacked, though researchers from Kaspersky Lab and Symantec could not confirm which countries were the true targets. In one case from May 2012, the office of the prime minister of a former Soviet Union member country was infected, leading to 60 further computers being affected, Symantec researchers said. There were some other victims, including the ministry for health of a Western European country, the ministry for education of a Central American country, a state electricity provider in the Middle East and a medical organisation in the US, according to Symantec. It is believed the group was also responsible for a much - documented 2008 attack on the US Central Command. The attackers - who continue to operate - have ostensibly sought to carry out surveillance on targets and pilfer data, though their use of encryption across their networks has made it difficult to ascertain exactly what the hackers took.Kaspersky Lab, however, picked up a number of the attackers searches through their victims emails, which included terms such as Nato and EU energy dialogue Though attribution is difficult to substantiate, Russia has previously been suspected of carrying out the attacks and Symantecs Gavin O' Gorman told the Guardian a number of the hackers appeared to be using Russian names and language in their

4/1/2007	Estonian DDoS April-May 2007		Estonia, a tiny Baltic nation that was occupied by the Soviet Union until 1991, angered Moscow by planning to move a Russian World War II memorial and Russian soldiers' graves. Russia retaliating by temporarily disabling Estonia's internet, an especially harsh blow in the world's most internet dependent economy. The distributed denial of service (DDoS) attack focused on government offices and financial institutions, disrupting communications.
6/1/2008	Lithuanian Web Site Defacement		Russia punished another former possession in the Baltic. When the Lithuanian government outlawed the display of Soviet symbols, Russian hackers defaced government web pages with hammer-and-sickles and five-pointed stars.
8/1/2008	Georgian Internet Shut Down	Russian Cyber-crime or Hacker Collective	After Georgia's pro-Western government sent troops into a breakaway republic backed by Moscow, Russian land, sea and air units invaded the country – and Russian hackers attacked Georgia's internet, the first time Russia coordinated military and cyber action. Georgia's internal communications were effectively shut down.
1/1/2009	Kyrgyzstan Internet DDoS	Russian Cyber-crime or Hacker Collective	As part of an effort to persuade the president of Kyrgyzstan to evict an American military base, Russian hackers shut down two of the country's four internet service providers with a DDOS attack. It worked. Kyrgyzstan removed the military base. Subsequently, Kyrgyzstan received $2 billion in aid and loans from the Kremlin.
4/1/2009	Kazakhstan DDoS	Russian Cyber-crime or Hacker Collective	After a media outlet in Kazakhstan published a statement by Kazakhstan's president that criticized Russia, a DDOS attack attributed to Russian elements shut down the outlet.
8/1/2009	Georgian Facebook and Twitter Shut Down	Russian Cyber-crime or Hacker Collective	Russian hackers shut down Twitter and Facebook in Georgia to commemorate the first anniversary of the Russian invasion.
1/1/2012	Red October (2012)	FSB	Targets included Russian Federation member states, eastern European countries, the Middle East, Australia, east Africa, and Brazil. Primarily an espionage campaign.
7/26/2013	Authorities bust Russian credit card hackers	Russian Cyber-crime or Hacker Collective	Authorities bust a gang of mostly Russian hackers who stole more than 160 million credit card numbers over eight years, making the scheme the largest cyber heist in the U.S. to date.

3/1/2014	Cyber and Military Annexation of Crimea	GRU	For the second time, the Russian government allegedly coordinated military and cyber action. A DDOS attack 32 times larger than the largest known attack used during Russia's invasion of Georgia disrupted the internet in Ukraine while Russian-armed pro-Russian rebels were seizing control of the Crimea.
3/6/2014	US sanctions Russia over Ukraine and Crimea	USA	The United States issues the first of its sanctions on Russia for invading Ukraine and forcing the annexation of Crimea
5/1/2014	Ukrainian Presidential Election Interference	Russian Cyber-crime or Hacker Collective	Three days before Ukraine's presidential election, a Russia-based hacking group, took down the country's election commission in an overnight attack. Even a back-up system was taken down, but Ukrainian computer experts were able to restore the system before election day. Ukrainian police say they arrested hackers who were trying to rig the results. The attack was aimed at creating chaos and hurting the nationalist candidate while helping the pro-Russian candidate. Russia's preferred candidate lost.
10/13/2014	iSight Report	Sandworm	Cybersecurity firm iSight Partners publishes a report explaining how a Russian government-backed hacking group nicknamed Sandworm is exploiting a flaw in Microsoft's Windows operating system. iSight says Sandworm launched cyber espionage operations against NATO, Poland, Ukraine, the European Union, and specific European telecommunications and energy firms.
10/17/2014	State Department Email Breach	Cozy Bear	The State Department tells Reuters that hackers recently attacked the department's unclassified email system, which then had to be taken down to improve security. The timing of the State Department attack coincides with the one at the White House.
10/29/2014	White House Breach	Cozy Bear	White House officials tell The Washington Post hackers breached the unclassified network of the Executive Office of the President sometime earlier in the month. Sources suspect Russian government sponsored hackers are behind the attack.

4/8/2015	French TV5 Monde	Cozy Bear	A massive synchronized cyberattack takes over all of TV5Monde’s 11 TV channels, its social media accounts and websites, and its company email. The global French-language network, which provides 24-hour news and entertainment programming to 260 million homes worldwide, goes dark for four hours before officials regain control. A group calling itself the Islamic State’s “Cyber Caliphate” takes responsibility for the attack, but investigators soon uncover evidence pointing to Russian Intelligence-linked FANCY BEAR using ISIS’ name to cover its tracks. US federal officials call the State Department email hack the "worst ever’ cyberattack intrusion against a federal agency.” They suspect Russian hackers are responsible for it as well as the contemporary attacks on the White House and other US federal agencies. Two years later, The Washington Post reports new details about the incident, including confirmation that COZY BEAR was the culprit.
4/8/2015	Crowdstrike Report on Russian Cyber Activity	Cozy Bear	Crowdstrike co-founder Dmitri Alperovitch tells The Daily Beast his cybersecurity firm has seen a dramatic increase in Russian cyber activity since the United States imposed sanctions in 2014. Alperovitch points to COZY BEAR and explains the group’s activity is not retaliatory but rather Russia’s attempt to stay globally competitive via cyber espionage.
5/8/2015	Bundestag Surveillance	Fancy Bear	Hackers spend weeks cyber spying on the German parliament’s computer network. The attack targets digital information from offices of at least 16 people within the Bundestag, including German Chancellor Angela Merkel. Authorities discover FANCY BEAR is responsible, having gained access via spear phishing. German investigators discovered hackers had penetrated the computer network of the German Bundestag, the most significant hack in German history. The BfV, German’s domestic intelligence service, later said Russia was behind the attack and that they were seeking information not just on the workings of the Bundestag, but German leaders and NATO, among others. Security experts said hackers were trying to penetrate the computers of Chancellor Angela Merkel’s Christian Democratic party.

6/1/2015	Office of Personnel Management	Cozy Bear	United States Office of Personnel Management announced that it had been the target of a data breach targeting the records of as many as four million people. The final estimate of the number of stolen records is approximately 21.5 million. This includes records of people who had undergone background checks, but who were not necessarily current or former government employees. Other US government agencies hacked around the same time include the U.S. Postal Service, and the National Oceanic and Atmospheric Administration (NOAA). US federal officials call the State Department email hack the "worst ever’ cyberattack intrusion against a federal agency.” They suspect Russian hackers are responsible for it as well as the contemporary attacks on the White House and other US federal agencies. Two years later, The Washington Post reports new details about the incident, including confirmation that COZY BEAR was the culprit.
6/1/2015	DNC Infiltration (June 2015 to November 2016)	Cozy Bear	Attackers use COZY BEAR to infiltrate the Democratic National Committee network undetected and camps out for more than a year spying on internal chats and emails. Russian hackers penetrated Democratic party computers, and gained access to the personal emails of Democratic officials, which in turn were distributed to the global media by WikiLeaks. Both the CIA and the FBI now believe the intrusions were intended to undermine the election, hurt Hillary Clinton and help Donald Trump win.
7/25/2015	Pentagon Joint Chiefs Email Compromise	Russian Cyber-crime or Hacker Collective	Russian hackers use spear phishing to infiltrate the Pentagon Joint Chief of Staff’s unclassified email system, forcing U.S. officials to take it down for nearly two weeks. The shutdown impacts some 4,000 military and civilian personnel.
10/1/2015	Dutch Government Breach regarding Flight MH17	Attributed to Russian Government	Security experts believe that the Russian government tried to hack into the Dutch government’s computers to pull out a report about the shoot down of Flight MH17 over Ukraine. The Dutch Safety Board headed the investigation of the Malaysia Airlines downing, and concluded that the passenger plane was brought down by a Russian-made missile fired from an area held by pro-Russian rebels.

12/23/2015	Ukrainian Power Grid Attack	Russian Cyber-crime or Hacker Collective	A sophisticated, well-coordinated attack that experts attribute to Russian hackers takes down a Ukrainian power grid, leaving close to 250,000 people without electricity. Hackers believed to Russian took over the control center of a Ukrainian power station, locking controllers out of their own systems and eventually leaving 235,000 homes without power.
1/1/2016	Finnish Foreign Ministry	Russian Cyber-crime or Hacker Collective	A security firm announces that it believes Russian hackers were behind attacks on Finland's Foreign Ministry several years before.
3/19/2016	John Podesta (DNC) Email Compromise	Cozy Bear	Hillary Clinton's campaign Chairman John Podesta clicks on a malicious spear phishing email link, unknowingly giving suspected Russian Intelligence hackers access to his Gmail account.
4/1/2016	Second DNC Attack	Fancy Bear, Cozy Bear	Hackers use FANCY BEAR in a second independent attack on the DNC network. The committee's IT team notices something is wrong and alerts executives who call in Crowdstrike. Crowdstrike identifies two separate hacker groups in the system, FANCY BEAR and COZY BEAR. News organizations begin reporting on the DNC attack. The Kremlin denies Russian involvement. The DNC and Crowdstrike believe hackers stole the committee's entire database of opposition research on Donald Trump but "no financial information or sensitive employee, donor or voter information was accessed by the Russian attackers."
6/15/2016	Crowdstrike Report on DNC Attacks	Fancy Bear, Cozy Bear	Crowdstrike posts Bears in the Midst: Intrusion into the Democratic National Committee, a detailed explanation of how it believes COZY BEAR and FANCY BEAR hacked the DNC. That same day, someone calling himself Guccifer 2.0 posts on a newly created Wordpress site that he alone is responsible for the hack. He releases what appears to be the stolen Trump opposition research as well as some additional documents and spreadsheets designed to disprove the DNC's claim it hadn't lost any sensitive information. Guccifer 2.0 says Wikileaks has the rest of his yield and will be publishing it shortly. Crowdstrike stands by its assessment that Russian operatives are responsible, and other security experts agree, calling Guccifer 2.0 an intentional Russian disinformation campaign.

7/8/2016	US Election Systems	Attributed to Russian Government	Russian cybercriminals breached election-related computer systems in at least 21 states.
7/22/2016	Wikileaks Published DNC Emails	Wikileaks	Wikileaks publishes the first wave of tens of thousands of stolen emails and attachments from seven officials at the DNC.
7/28/2016	Cyber Attack Against Democratic Congressional Campaign Committee (DCCC)	Attributed to Russian Government	FBI is investigating a cyber attack against the Democratic Congressional Campaign Committee (DCCC), which likely started in March or April but wasn't discovered until June. Tens of thousands of pages of stolen documents and sensitive information turn up online by August, including "the home addresses, cellphone numbers and personal email addresses of Democratic House members." Starting in August, Guccifer 2.0 sends information to political bloggers focused on specific House races in key states like Florida, Pennsylvania, New Hampshire, Ohio, Illinois and North Carolina.
9/13/2016	Colin Powell Gmail Leak	Attributed to Russian Government	DCLeaks posts more than two years' worth of emails stolen from former Secretary of State Colin Powell's Gmail account
10/9/2016	Podesta Emails Published	Wikileaks	Wikileaks starts publishing thousands of John Podesta's stolen emails including hundreds of attachments.
10/17/2016	Email and Network Breaches Attributed to Russia By DHS	DHS	The Department Of Homeland Security and the Office of the Director of National Intelligence on Election Security issue a joint statement saying they are confident the Russian government is behind the recent email and computer network hacks, adding, "[t]hese thefts and disclosures are intended to interfere with the US election process." It continues: "Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company." However, US Intelligence is not yet prepared to attribute these activities to the Russian government.

11/9/2016	Phishing Attacks on Think Tanks and NGOs	Attributed to Russian Government	an advanced persistent threat (APT) group launched a series of coordinated and well-planned spear phishing campaigns. Volexity observed five different attack waves with a heavy focus on U.S.-based think tanks and non-governmental organizations (NGOs). These e-mails came from a mix of attacker created Google Gmail accounts and what appears to be compromised e-mail accounts at Harvard's Faculty of Arts and Sciences (FAS). These e-mails were sent in large quantities to different individuals across many organizations and individuals focusing in national security, defense, international affairs, public policy, and European and Asian studies.
12/1/2016	German Election Interference	Attributed to Russian Government	BfV head Hans-Georg Maasen warned "There is growing evidence of attempts to influence the federal election next year," referring to German parliamentary elections likely to take place in September 2017. Maasen specifically cited Russia as the source of the attacks, adding, "We expect a further increase in cyber attacks in the run-up to the elections." Experts believe the Russians are trying to damage incumbent Chancellor Merkel, who supported sanctions against Putin's personal associates after Russia annexed Crimea.
12/22/2016	Ukrainian Army Android hack	Fancy Bear	Crowdstrike publishes a report explaining how FANCY BEAR implant malware into Android devices to "track and target Ukrainian artillery units from late 2014 through 2016." However, both the International Institute for Strategic Studies (IISS) and the Ukrainian Ministry of Defense say the cybersecurity firm's assessment is wrong because its conclusions rely on misread IISS information. Crowdstrike changes key part of its report three months later but refuses to retract it entirely. The alleged error casts doubt in some circles as to the overall accuracy of Crowdstrike's previous Russian hacking assessments.
12/29/2016	Russian Diplomats Expelled	President Obama	President Obama orders sanctions against Russian intelligence services and officials, expelling 35 diplomats from the country and shuttering two Russian-owned recreational compounds, one in Maryland and one in New York. The move is in response to Russia's cyber attacks during the 2016 campaign.

12/29/2016	Report on Grizzly Steppe	US-CERT, DHS	This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.
12/31/2016	Vermont Electric Attack	Grizzly Steppe	Russian hackers got into a computer at Burlington Electric in Vermont. While the hackers did not disrupt operations and the affected laptop was not connected to the grid, the breach shows the true vulnerability of our nation's electrical systems.
2/3/2017	Cyber attacks on Norway and Netherlands governments	Cozy Bear	hackers targeted members of the Norwegian and Dutch governments in 2017
2/10/2017	Enhanced Analysis of GRIZZLY STEPPE Activity	US-CERT, DHS	The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) has collaborated with interagency partners and private-industry stakeholders to provide an Analytical Report (AR) with specific signatures and recommendations to detect and mitigate threats from GRIZZLY STEPPE actors.

3/1/2017	German an French Election Campaigns (March, April, May 2017)	Fancy Bear	According to analysts at Trend Micro as reported by Wired, FANCY BEAR sets up phishing sites aimed at “campaigns of left-leaning politicians Emmanuel Macron and Angela Merkel in upcoming French and German elections.” Less than 48 hours before France’s runoff election between Emmanuel Macron and Marine Le Pen, someone anonymously posts 9GB of stolen internal information from the Macron campaign. Capitalizing on rules forbidding candidates from public speaking two days before an election, the data dump appears designed to limit Macron’s defense. Macron wins the election handily. Security firms again recognize the hack to be the work of FANCY BEAR. National Security Advisor Mike Rogers testifies before the Senate Armed Services Committee and says he warned French authorities the US was seeing suspicious Russian cyberactivity prior to the Macron leak. Rogers says he asked how his team could help and adds he is doing the same with his counterparts in German and Britain.
5/23/2017	Qatar News Agency Breach	Attributed to Russian Government	Qatar’s News Agency is hacked. The hacker posts a fake statement attributed to Qatar Sheikh Tamim Bin Hamad al-Thani that flatters Iran and angers Saudi Arabia and other regional allies. The Saudis, the UAE, Bahrain, and Egypt immediately break relations with Qatar, ban its media, and declare a trade and diplomatic boycott, accusing Qatar of supporting terrorism. US intelligence officials believe the UAE is behind the attacks. US investigators now suspect Russia may be behind the Qatar News Agency cyber attack, planting fake information in an effort to cause trouble between the US and its allies.
7/9/2017		Dragonfly	behind cyber breaches at about 100 power companies and nuclear plant operators since the beginning of 2017. Half of those were in the United States.

9/13/2017	DHS Bans Kaspersky	DHS, FBI	The U.S. Department of Homeland Security officially bans federal use of software from Kaspersky Lab, a Moscow-based cybersecurity company that U.S. officials believe has ties to the Kremlin and Russian intelligence. The Wall Street Journal, followed by multiple other outlets, reports that Russian-linked hackers broke into a National Security Agency contractor's home computer in 2015 and stole highly classified information. The hackers gained access using antivirus software made by Kaspersky Lab.
1/22/2018	Russia Meddles in Swedish Elections	Attributed to Russian Government	Anders Thornberg, the director of Swedish Security Services (SAPO) was accusing the Russians of engaging in social media driven misinformation campaign very similar to what happened in recent elections in France and Germany, and in the US during the last Presidential Election. Evidently Putin is concerned that Sweden may join NATO, and is actively campaigning for candidates who are opposed to NATO.
2/15/2018	Petya Ransomware	US-CERT, DHS	The scope of this Alert's analysis is limited to the newest Petya malware variant that surfaced on June 27, 2017. This malware is referred to as "NotPetya" throughout this Alert. On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list. Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods.

3/15/2018	Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors	US-CERT, DHS	This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on Russian government actions targeting U.S. Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors. It also contains indicators of compromise (IOCs) and technical details on the tactics, techniques, and procedures (TTPs) used by Russian government cyber actors on compromised victim networks. DHS and FBI produced this alert to educate network defenders to enhance their ability to identify and reduce exposure to malicious activity. DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).
4/20/2018	Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices	US-CERT, DHS	Since 2015, the U.S. Government received information from multiple sources—including private and public sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of enterprise-class and SOHO/residential routers and switches worldwide. The U.S. Government assesses that cyber actors supported by the Russian government carried out this worldwide campaign. These operations enable espionage and intellectual property theft that supports the Russian Federation's national security and economic goals.
11/16/2018	US spear-phishing campaign	Cozy Bear	A Russian state-sponsored cyber-espionage group has come back to life after a one-year period of inactivity with a relative large spear-phishing campaign that has targeted both the US government and private sector.

11/20/2018	new malware against US and European targets	Fancy Bear	A Russian government-backed hacking group is distributing a new form of trojan malware as part of a cyber espionage campaign targeting the US and Europe, according to security researchers. Named Cannon after references in the malicious code, the malware gathers system information and takes screenshots of infected PCs and has been operating since at least late October.