2020 United States federal government data breach

In 2020, a major cyberattack by a group backed by a foreign government penetrated thousands of organizations globally including multiple parts of the United States federal government, leading to a series of data breaches.[1][28][29] The hacking group Cozy Bear (APT29), backed by the Russian intelligence agency SVR, was identified as the likely culprit.[27][26] The cyberattack and data breach were reported to be among the worst cyber-espionage incidents ever suffered by the U.S., due to the sensitivity and high profile of the targets and the long duration (eight to nine months) in which the hackers had access.[35] Within days of its discovery, at least 200 organizations around the world had been reported to be affected by the attack, and some of these may also have suffered data breaches.[1][36][37] Affected organizations worldwide included NATO, the U.K. government, the European Parliament, Microsoft and others.[36]

The attack, which had gone undetected for months, was first publicly reported on December 13, 2020,[25][26] and was initially only known to have affected the U.S. Treasury Department and the National Telecommunications and Information Administration (NTIA), part of the U.S. Department of Commerce.[42] In the following days, more departments and private organizations reported breaches.[1][5][36]

The cyberattack that led to the breaches began no later than March 2020.[9][10] The attackers exploited software or credentials from at least three U.S. firms: Microsoft, SolarWinds, and VMware.[43][21] A supply chain attack on Microsoft cloud services provided one way for the attackers to breach their victims, depending upon whether the victims had bought those services through a reseller.[16][17][18] A supply chain attack on SolarWinds's Orion software, widely used in government and industry, provided another avenue, if the victim used that software.[12][44] Flaws in Microsoft and VMware products allowed the attackers to access emails and other documents,[23][24][14][15] and to perform federated authentication across victim resources via single sign-on infrastructure.[21][45][46]

In addition to the theft of data, the attack caused costly inconvenience to tens of thousands of SolarWinds customers, who had to check whether they had been breached, and had to take systems offline and begin months-long decontamination procedures as a precaution.[47][48] U.S. Senator Richard J. Durbin described the cyberattack as tantamount to a declaration of war.[49][4] President Donald Trump was silent for days after the attack, before spuriously suggesting that China, not Russia, might have been responsible for it, and that "everything is well under control".[50][51]

Contents

Background

2020 United States federal government data breach



U.S. federal institutions reportedly breached. From top, clockwise: Defense,[1] Labor,[2] Energy,[3] State,[4] National Institutes of Health,[5] Commerce,[4] Homeland Security,[4] Treasury,[4] Agriculture,[6] Justice[7]

Date

Methodology
- Microsoft exploits
- SolarWinds exploit
- VMware exploits

Discovery
- Microsoft exploits
- SolarWinds exploit
- VMware exploits

Responsibility
- Conclusions by investigators
- Statements by U.S. government officials
- Denial of involvement

Impact
- List of confirmed connected data breaches
  - U.S. federal government
  - U.S. state and local governments
  - Private sector

Investigations and responses
- Technology companies and business
- U.S. government
  - Security agencies
  - Congress
  - The judiciary
  - President Trump
  - President Biden
- Rest of the world
- Cyber espionage or cyberattack?
- Debate on possible U.S. responses

See also

References

	▪ Before October 2019 (start of supply chain compromise)[8] ▪ March 2020 (possible federal breach start date)[9][10] ▪ December 13, 2020 (breach acknowledged)[9][10]
Duration	At least 8 months[11] or 9 months[12]
Location	United States, United Kingdom, Spain, Israel, United Arab Emirates, Canada, Mexico, others[13]
Type	Cyberattack, data breach
Theme	Malware, backdoor, advanced persistent threat, espionage
Cause	▪ Microsoft Outlook Web App software bug[14][15] ▪ Microsoft supply chain attack (reseller compromise)[16][17][18] ▪ SolarWinds supply chain attack (SUNBURST trojan)[19][20] ▪ VMware software bug[21][22] ▪ Zerologon software bug[23][24]
Target	U.S. federal government, state and local governments, and private sector
First reporter	▪ FireEye (responsible disclosure)[1] ▪ NSA (responsible disclosure)[21] ▪ Reuters (public disclosure)[25][26]
Suspects	

Background

The global data breach occurred over the course of at least 8 or 9 months during the final year of the presidency of Donald Trump.[11][12] Throughout this time, the White House lacked a cybersecurity coordinator, Trump having eliminated the post itself in 2018.[52][53] When the breach was discovered, the U.S. also lacked a Senate-confirmed Director of CISA, the nation's top cybersecurity official, responsible for coordinating incident response.[54][40][41] The incumbent, Chris Krebs, had been fired by Trump on November 18, 2020.[55][56][57] Also at that time, the DHS, which manages CISA, lacked a Senate-confirmed Secretary, Deputy Secretary, General Counsel, Undersecretary for Intelligence and Analysis, and Undersecretary for Management; and Trump had recently forced out the Deputy Director of CISA.[58][59][60] Numerous federal cybersecurity recommendations made by the Government Accountability Office and others had not been implemented.[61]

- Berserk Bear (Russia)[23]
- Cozy Bear (Russia)[27][26]
- FSB (Russia)[23]
- SVR (Russia)[27][26]

SolarWinds, a Texas-based provider of network monitoring software to the U.S. federal government, had shown several security shortcomings prior to the attack.[62][63] SolarWinds did not employ a chief information security officer or senior director of cybersecurity.[4][64] Cybercriminals had been selling access to SolarWinds's infrastructure since at least as early as 2017.[63][62] SolarWinds had been advising customers to disable antivirus tools before installing SolarWinds software.[62] In November 2019, a security researcher had warned SolarWinds that their FTP server was not secure, warning that "any hacker could upload malicious [files]" that would then be distributed to SolarWinds customers.[65][62][66][63] And SolarWinds's Microsoft Office 365 account had been compromised, with the attackers able to access emails and possibly other documents.[67][68]

On December 7, 2020, a few days before trojaned SolarWinds software was publicly confirmed to have been used to attack other organizations, longstanding SolarWinds CEO Kevin Thompson retired.[69][70] That same day, two private equity firms with ties to SolarWinds's board sold substantial amounts of stock in SolarWinds.[69] The firms denied insider trading.[69][71]

Methodology

Multiple attack vectors were used in the course of breaching the various victims of the incident.[72][73]

Microsoft exploits

> If you think about data that is only available to the CEO, or data that is only available to IT services, [the attacker would get] all of this data.
>
> — Sami Ruohonen, F-Secure[23]

The attackers exploited flaws in Microsoft products, services, and software distribution infrastructure.[23][15][9][18]

At least one reseller of Microsoft cloud services was compromised by the attackers, constituting a supply chain attack that allowed the attackers to access Microsoft cloud services used by the reseller's customers.[16][17][18]

Alongside this, "Zerologon", a vulnerability in the Microsoft authentication protocol NetLogon, allowed attackers to access all valid usernames and passwords in each Microsoft network that they breached.[23][24] This allowed them to access additional credentials necessary to assume the privileges of any legitimate user of the network, which in turn allowed them to compromise Microsoft Office 365 email accounts.[23][24]

Additionally, a flaw in Microsoft's Outlook Web App may have allowed attackers to bypass multi-factor authentication.[14][15][74]

Attackers were found to have broken into Microsoft Office 365 in a way that allowed them to monitor NTIA and Treasury staff emails for several months.[9][39][55] This attack apparently used counterfeit identity tokens of some kind, allowing the attackers to trick Microsoft's authentication systems.[39][75][76] The presence of single sign-on infrastructure increased the viability of the attack.[46]

SolarWinds exploit

> This is classic espionage. It's done in a highly sophisticated way ... But this is a stealthy operation.
>
> — Thomas Rid, *The Washington Post*[12]

Here, too, the attackers used a supply chain attack.[77] The attackers accessed the build system belonging to the software company SolarWinds, possibly via SolarWinds's Microsoft Office 365 account, which had also been compromised at some point.[78][62][67][68]

The attackers established a foothold in SolarWinds's software publishing infrastructure no later than September 2019.[79][80] In the build system, the attackers surreptitiously modified software updates provided by SolarWinds to users of its network monitoring software Orion.[81][82] The first known modification, in October 2019, was merely a proof of concept.[8] Once the proof had been established, the attackers spent December 2019 to February 2020 setting up a command-and-control infrastructure.[8]

In March 2020, the attackers began to plant remote access tool malware into Orion updates, thereby trojaning them.[12][44][83][84][85] These users included U.S. government customers in the executive branch, the military, and the intelligence services (see Impact section, below).[9][86] If a user installed the update, this would execute the malware payload, which would stay dormant for 12–14 days before attempting to communicate with one or more of several command-and-control servers.[87][88][89][90] The communications were designed to mimic legitimate SolarWinds traffic.[78][91] If able to contact one of those servers, this would alert the attackers of a successful malware deployment and offer the attackers a back door that the attackers could choose to utilise if they wished to exploit the system further.[90][92] The malware started to contact command-and-control servers in April 2020, initially from North America and Europe and subsequently from other continents too.[93][90]

The attackers appear to have utilized only a small fraction of the successful malware deployments: ones located within computer networks belonging to high-value targets.[87][12] Once inside the target networks, the attackers pivoted, installing exploitation tools such as Cobalt strike components,[94][91] and seeking additional access.[78][1] Because Orion was connected to customers' Office 365 accounts as a trusted 3rd-party application, the attackers were able to access emails and other confidential documents.[95] This access apparently helped them to hunt for certificates that would let them sign SAML tokens, allowing them to masquerade as legitimate users to additional on-premises services and to cloud services like Microsoft Azure Active Directory.[95][78][96] Once these additional footholds had been obtained, disabling the compromised Orion software would no longer be sufficient to sever the attackers' access to the target network.[5][97][98] Having accessed data of interest, they encrypted and exfiltrated it.[77][1]

The attackers hosted their command-and-control servers on commercial cloud services from Amazon, Microsoft, GoDaddy and others.[99] By using command-and-control IP addresses based in the U.S., and because much of the malware involved was new, the attackers were able to evade detection by Einstein, a national cybersecurity system operated by the Department of Homeland Security (DHS).[89][4][100]

FBI investigators recently found that a separate flaw in software made by SolarWinds Corp was used by hackers tied to another foreign government to help break into U.S. government computers.[101]

VMware exploits

Vulnerabilities in VMware Access and VMware Identity Manager, allowing existing network intruders to pivot and gain persistence, were utilized in 2020 by Russian state-sponsored attackers.[21][22] As of December 18, 2020, while it was definitively known that the SUNBURST trojan would have provided suitable access to exploit the VMware bugs, it was not yet definitively known whether attackers had in fact chained those two exploits in the wild.[21][22]

Discovery

Microsoft exploits

During 2019 and 2020, cybersecurity firm Volexity discovered an attacker making suspicious usage of Microsoft products within the network of a think tank whose identity has not publicly been revealed.[102][103][14] The attacker exploited a vulnerability in the organization's Microsoft Exchange Control Panel, and used a novel method to bypass multi-factor authentication.[14] Later, in June and July 2020, Volexity observed the attacker utilising the SolarWinds Orion trojan; i.e. the attacker used Microsoft vulnerabilities (initially) *and* SolarWinds supply chain attacks (later on) to achieve their goals.[14] Volexity said it was not able to identify the attacker.[14]

Also in 2020, Microsoft detected attackers using Microsoft Azure infrastructure in an attempt to access emails belonging to CrowdStrike.[104] That attack failed because - for security reasons - CrowdStrike does not use Office 365 for email.[104]

Separately, in or shortly before October 2020, Microsoft Threat Intelligence Center reported that an apparently state-sponsored attacker had been observed exploiting zerologon, a vulnerability in Microsoft's NetLogon protocol.[23][24] This was reported to CISA, who issued an alert on October 22, 2020, specifically warning state, local, territorial and tribal governments to search for indicators of compromise, and instructing them to rebuild their networks from scratch if compromised.[23][105] Using VirusTotal, *The Intercept* discovered continued indicators of compromise in December 2020, suggesting that the attacker might still be active in the network of the city government of Austin, Texas.[23]

SolarWinds exploit

On December 8, 2020, the cybersecurity firm FireEye announced that red team tools had been stolen from it by what it believed to be a state-sponsored attacker.[106][107][108] FireEye was believed to be a target of the SVR, Russia's Foreign Intelligence Service.[27][109] FireEye says that it discovered the SolarWinds supply chain attack in the course of investigating FireEye's own breach and tool theft.[110][111]

After discovering that attack, FireEye reported it to the U.S. National Security Agency (NSA), a federal agency responsible for helping to defend the U.S. from cyberattacks.[1] The NSA is not known to have been aware of the attack before being notified by FireEye.[1] The NSA uses SolarWinds software itself.[1]

Some days later, on December 13, when breaches at the Treasury and Department of Commerce breaches were publicly confirmed to exist, sources said that the FireEye breach was related.[9][27] On December 15, FireEye confirmed that the vector used to attack the Treasury and other government departments was the same one that had been used to attack FireEye: a trojaned software update for SolarWinds Orion.[65][112]

The security community shifted its attention to Orion. The infected versions were found to be *2019.4* through *2020.2.1 HF1*, released between March 2020 and June 2020.[83][94] FireEye named the malware SUNBURST.[19][20] Microsoft called it Solorigate.[62][20] The tool that the attackers used to insert SUNBURST into Orion updates was later isolated by cybersecurity firm CrowdStrike, who called it SUNSPOT.[79][113][82]

Subsequent analysis of the SolarWinds compromise using DNS data and reverse engineering of Orion binaries, by DomainTools and ReversingLabs respectively, revealed additional details about the attacker's timeline.[8]

VMware exploits

Some time before December 3, 2020, the NSA discovered and notified VMware of vulnerabilities in VMware Access and VMware Identity Manager.[21] VMware released patches on December 3, 2020.[21] On December 7, 2020, the NSA published an advisory warning customers to apply the patches because the vulnerabilities were being actively exploited by Russian state-sponsored attackers.[21][114]

Responsibility

Conclusions by investigators

SolarWinds said it believed the malware insertion into Orion was performed by a foreign nation.[9][10] Russian-sponsored hackers were suspected to be responsible.[115][9][25] U.S. officials stated that the specific groups responsible were probably the SVR or Cozy Bear (also known as APT29).[27][26] FireEye gave the suspects the placeholder name "UNC2452";[78][14] incident response firm Volexity called them "Dark Halo".[14][103] On December 23, 2020, the CEO of FireEye said Russia was the most likely culprit and the attacks were "very consistent" with the SVR.[116] One security researcher offers the likely operational date, February 27, 2020 with a significant change of aspect on October 30, 2020.[117]

In January 2021, cybersecurity firm Kaspersky said SUNBURST resembles the malware Kazuar, which is believed to have been created by Turla,[118][113][119][120] a group known from 2008 that Estonian intelligence previously linked to the Russian federal security service, FSB.[121]

FBI investigators found that suspected Chinese hackers exploited a flaw in software made by SolarWinds Corp to help break into U.S. government computers such as the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture, potentially compromising the data on thousands of government employees. The hack is separate as the suspected Chinese hackers exploited a separate bug in Orion's code to help spread across networks that they had already comprised. Former U.S. chief information security officer Gregory Touhill compared the fact that Russia and China targeting the same software product to Drafting in motorsport.[122][101]

Statements by U.S. government officials

On October 22, 2020, CISA and the FBI identified the Microsoft zerologon attacker as Berserk Bear, a state-sponsored group believed to be part of Russia's FSB.[23]

On December 18, U.S. Secretary of State Mike Pompeo said Russia was "pretty clearly" responsible for the cyber attack.[123][124][125]

On December 19, U.S. president Donald Trump publicly addressed the attacks for the first time, suggesting without evidence that China, rather than Russia, might be responsible.[50][126][125][51] The same day, Republican senator Marco Rubio, acting chair of the Senate Intelligence Committee, said it was "increasingly clear that Russian intelligence conducted the gravest cyber intrusion in our history."[37][127]

On December 20, Democratic senator Mark Warner, briefed on the incident by intelligence officials, said "all indications point to Russia."[128]

On December 21, 2020, Attorney General William Barr said that he agreed with Pompeo's assessment of the origin of the cyberhack and that it "certainly appears to be the Russians," contradicting Trump. [129][130][131]

On January 5, 2021, CISA, the FBI, the NSA, and the Office of the Director of National Intelligence, all confirmed that they believe Russia was the most likely culprit.[132][133][134]

Denial of involvement

Russia denied involvement.[135]

The Chinese foreign ministry said attributing cyberattacks was a "complex technical issue" and any allegations should be supported with evidence. "China resolutely opposes and combats any form of cyberattacks and cyber theft," it said in a statement.[101]

Impact

> This is a much bigger story than one single agency. This is a huge cyber espionage campaign targeting the U.S. government and its interests.
>
> — U.S. government source[9]

Discovery of the breaches at the Treasury and the Department of Commerce immediately raised concerns that the attackers would attempt to breach other departments, or had already done so.[75][25] Further investigation proved these concerns to be well-founded.[1] Within days, additional federal departments were found to have been breached.[1][136][6]

SolarWinds said that of its 300,000 customers, 33,000 use Orion.[1] Of these, around 18,000 government and private users downloaded compromised versions.[1][5][137]

Compromised versions were known to have been downloaded by the Centers for Disease Control and Prevention, the Justice Department, and some utility companies.[1] Other prominent U.S. organisations known to use SolarWinds products, though not necessarily Orion, were the Los Alamos National Laboratory, Boeing, and most Fortune 500 companies.[1][138] Outside the U.S., reported SolarWinds clients included parts of the British government, including the Home Office, National Health Service, and signals intelligence agencies; the North Atlantic Treaty Organization (NATO); the European Parliament; and likely AstraZeneca.[5][36] FireEye said that additional government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East may also have been affected.[5]

Simply downloading a compromised version of Orion was not necessarily sufficient to result in a data breach; further investigation was required in each case to establish whether a breach resulted.[1][139] These investigations were complicated by: the fact that the attackers had in some cases removed evidence;[72] the need to maintain separate secure networks as organizations' main networks were assumed to be compromised;[72] and the fact that Orion was itself a network monitoring tool, without which users had less visibility of their networks.[77] As of mid-December 2020, those investigations were ongoing.[1][5]

As of mid-December 2020, U.S. officials were still investigating what was stolen in the cases where breaches had occurred, and trying to determine how it could be used.[9][140] Commentators said that the information stolen in the attack would increase the perpetrator's influence for years to come.[67][141][90] Possible future uses could include attacks on hard targets like the CIA and NSA,[4] or using blackmail to recruit spies.[142] Cyberconflict professor Thomas Rid said the stolen data would have myriad uses.[140] He added that the amount of data taken was likely to be many times greater than during Moonlight Maze, and if printed would form a stack far taller than the Washington Monument.[140]

Even where data was not exfiltrated, the impact was significant.[48] The Cybersecurity and Infrastructure Security Agency (CISA) advised that affected devices be rebuilt from trusted sources, and that all credentials exposed to SolarWinds software should be considered compromised and should therefore be reset.[143] Anti-malware companies additionally advised searching log files for specific indicators of compromise.[144][145][146]

However, it appeared that the attackers had deleted or altered records, and may have modified network or system settings in ways that could require manual review.[72][147] Former Homeland Security Advisor Thomas P. Bossert warned that it could take years to evict the attackers from US networks, leaving them able to continue to monitor, destroy or tamper with data in the meantime.[47] Harvard's Bruce Schneier, and NYU's Pano Yannakogeorgos, founding dean of the Air Force Cyber College, said that affected networks may need to be replaced completely.[148][149]

Through a manipulation of software keys, Russian hackers were able to access the email systems used by the Treasury Department's highest-ranking officials. This system, although unclassified, is highly sensitive because of the Treasury Department's role in making decisions that move the market, as well as decisions on economic sanctions and interactions with the Federal Reserve.[131]

Anonymous FBI sources revealed that internal investigations had discovered suspected Chinese attackers using computer infrastructure and hacking tools previously deployed by state-backed Chinese cyberspies. They had hacked into the National Finance Center, a federal payroll agency inside the U.S. Department of Agriculture, potentially compromising the data of thousands of government employees, possibly to better collect intelligence. The NFC is responsible for handling the payroll of multiple government agencies, including several involved in national security, such as the FBI, State Department, Homeland Security Department and Treasury Department. Records held by the NFC include federal employee social security numbers, phone numbers and personal email addresses as well as banking information. On its website, the NFC says it "services more than 160 diverse agencies, providing payroll services to more than 600,000 Federal employees."[101]

List of confirmed connected data breaches

U.S. federal government

Branch	Institution	Affected part(s) include	Assets accessed	Sources
Executive	Department of Agriculture	National Finance Center		[6][150][96][151][152][101]
	Department of Commerce	National Telecommunications and Information Administration		[153][1][154][155][88][90][156][151][157][158][152][159][160]
	Department of Defense	Parts of The Pentagon		[1][161][159][160]
	Department of Energy	National Nuclear Security Administration		[3][162][163][164][165][157][158][152][159][166][160]
	Department of Health and Human Services	National Institutes of Health		[161][156][158][152]
	Department of Homeland Security	Cybersecurity and Infrastructure Security Agency		[155][154][88][90][156][1][151][158][152][167]
	Department of Justice		~3000 Microsoft Office 365-hosted email accounts	[168][7][169][170][171][172]
	Department of Labor	Bureau of Labor Statistics		[2]
	Department of State			[1][161][156][158][152][160]
	Department of the Treasury			[1][154][161][153][88][90][156][151][157][158][152][46][160]
Judicial	Administrative Office of the United States Courts	Case Management/Electronic Case Files	Court documents, including sealed case files	[173][174][175][176][177][178][179][180][181]

U.S. state and local governments

Department	Affected part(s) include	Sources
Arizona	Pima County	[182][183]
California	California Department of State Hospitals	[184]
Ohio	Kent State University	[184]
Texas	Austin City	[23]

Private sector

Organization	Assets accessed	Sources
Belkin		[184]
Cisco Systems		[185][186][187][158][183]
Cox Communications		[182][8][188][183]
Equifax		[187]
Fidelis		[189]
FireEye	▪ Red team tools	[155][161][88][156]
Malwarebytes		[190][191][192]
Microsoft	▪ Product source code ▪ Reseller accounts	[43][164][193][194][195][196][197][3][198][199][187][158][159][160][167][200][201][202][203][204][205][206]
Mimecast	▪ Cryptographic certificate ▪ Microsoft Office 365-hosted email	[207][208][209][210][211][212]
Nvidia		[184]
Palo Alto Networks		[189]
Qualys		[189]
SolarWinds	▪ Microsoft Office 365-hosted email ▪ Build system	[155][161][88][199][198]
A think tank (unnamed as of December 15, 2020)		[14][139][103][15][74][134]
VMware		[184]

Investigations and responses

Technology companies and business

On December 8, 2020, before other organizations were known to have been breached, FireEye published countermeasures against the red team tools that had been stolen from FireEye.[109][213]

On December 15, 2020, Microsoft announced that SUNBURST, which only affects Windows platforms, had been added to Microsoft's malware database and would, from December 16 onwards, be detected and quarantined by Microsoft Defender.[214][156]

GoDaddy handed ownership to Microsoft of a command-and-control domain used in the attack, allowing Microsoft to activate a killswitch in the SUNBURST malware, and to discover which SolarWinds customers were infected.[65]

On December 14, 2020, the CEOs of several American utility companies convened to discuss the risks posed to the power grid by the attacks.[1] On December 22, 2020, the North American Electric Reliability Corporation asked electricity companies to report their level of exposure to Solarwinds software.[215]

SolarWinds unpublished its featured customer list after the hack,[216] although as of December 15, cybersecurity firm GreyNoise Intelligence said SolarWinds had not removed the infected software updates from its distribution server.[65][67][217]

Around January 5, 2021, SolarWinds investors filed a class action lawsuit against the company in relation to its security failures and subsequent fall in share price.[218][219] Soon after, SolarWinds hired a new cybersecurity firm co-founded by Krebs.[220]

The Linux Foundation pointed out that if Orion had been open source, users would have been able to audit it, including via reproducible builds, making it much more likely that the malware payload would have been spotted.[221]

U.S. government

On December 18, 2020, U.S. Secretary of State Mike Pompeo said that some details of the event would likely be classified so as not to become public.[81]

Security agencies

On December 12, 2020, a National Security Council (NSC) meeting was held at the White House to discuss the breach of federal organizations.[9] On December 13, 2020, CISA issued an emergency directive asking federal agencies to disable the SolarWinds software, to reduce the risk of additional intrusions, even though doing so would reduce those agencies' ability to monitor their computer networks.[1][143] Russia denied involvement in the attacks.[222]

On December 14, 2020, the Department of Commerce confirmed that it had asked the CISA and the FBI to investigate.[9][27][223] The NSC activated Presidential Policy Directive 41, an Obama-era emergency plan, and convened its Cyber Response Group.[224][52] The U.S. Cyber Command threatened swift retaliation against the attackers, pending the outcome of investigations.[225]

The Federal Energy Regulatory Commission (FERC) helped to compensate for a staffing shortfall at CISA.[162][77][163] The FBI, CISA, and the Office of the Director of National Intelligence (ODNI) formed a Cyber Unified Coordination Group (UCG) to coordinate their efforts.[226]

On December 24, 2020, CISA said state and local government networks, in addition to federal ones, and other organizations, had been impacted by the attack, but did not provide further details.[227]

On February 2, 2021, *Reuters* reported that anonymous FBI sources revealed that internal investigations had discovered suspected Chinese attackers using computer infrastructure and hacking tools previously deployed by state-backed Chinese cyberspies.[101]

Congress

The Senate Armed Services Committee's cybersecurity subcommittee was briefed by Defense Department officials.[98] The House Committee on Homeland Security and House Committee on Oversight and Reform announced an investigation.[43] Marco Rubio, acting chair of the Senate Intelligence Committee, said the U.S. must retaliate, but only once the perpetrator is certain.[228] The committee's vice-chairman, Mark Warner, criticized President Trump for failing to acknowledge or react to the hack.[229]

Senator Ron Wyden called for mandatory security reviews of software used by federal agencies.[155][151]

On December 22, 2020, after U.S. Treasury Secretary Steven Mnuchin told reporters that he was "completely on top of this", the Senate Finance Committee was briefed by Microsoft that dozens of Treasury email accounts had been breached, and the attackers had accessed systems of the Treasury's Departmental Offices division, home to top Treasury officials.[46][131] Senatory Wyden said that the briefing showed that the Treasury "still does not know all of the actions taken by hackers, or precisely what information was stolen".[46][131]

On December 23, 2020, Senator Bob Menendez asked the State Department to end its silence about the extent of its breach, and Senator Richard Blumenthal asked the same of the Veterans Administration.[230][231]

The judiciary

The Administrative Office of the United States Courts initiated an audit, with DHS, of the U.S. Judiciary's Case Management/Electronic Case Files (CM/ECF) system.[173][180] It stopped accepting highly sensitive court documents to the CM/ECF, requiring those instead to be accepted only in paper form or on airgapped devices.[175][176][177]

President Trump

President Donald Trump made no comment on the hack for days after it was reported, leading Senator Mitt Romney to decry his "silence and inaction".[232] On December 19, Trump publicly addressed the attacks for the first time; he downplayed the hack, contended that the media had overblown the severity of the incident, said that "everything is well under control"; and proposed, without evidence, that China, rather than Russia, might be responsible for the attack. Trump then pivoted to insisting that he had won the 2020 presidential election.[126][125][123][233][234] He speculated, without evidence, that the attack might also have involved a "hit" on voting machines, part of a long-running campaign by Trump to falsely assert that he won the 2020 election. Trump's claim was rebutted by former CISA director Chris Krebs, who pointed out that Trump's claim was not possible.[1][234][235] Adam Schiff, chair of the House Intelligence Committee, described Trump's statements as dishonest,[236] calling the comment a "scandalous betrayal of our national security" that "sounds like it could have been written in the Kremlin."[234]

Former Homeland Security Advisor Thomas P. Bossert said, "President Trump is on the verge of leaving behind a federal government, and perhaps a large number of major industries, compromised by the Russian government," and noted that congressional action, including via the National Defense Authorization Act would be required to mitigate the damage caused by the attacks.[30][237][47] Russell Brandom, policy editor for *The Verge*, called the U.S. ill-prepared for the hack, and criticized Trump for having consistently "treated the federal cybersecurity effort as one more partisan battleground, with attacks and vulnerabilities embraced or rejected largely on the basis of their value as a political cudgel"; Brandom wrote that "this is no way to run the world's most powerful intelligence apparatus."[54] Fred Kaplan, writing in *Slate*, criticized Trump for promoting fake claims of election fraud while "ignoring a real cybersecurity crisis," writing: "For all of Trump's wailing about fictitious hacks that stole the election, he has been otherwise notably uncurious about the nation's cybersecurity."[52] *Esquire* commentator Charles P. Pierce criticized the Trump administration for being "asleep at the switch" and termed Trump a "crooked, incompetent agent of chaos."[238]

President Biden

Then president-elect Joe Biden said that, "A good defense isn't enough; we need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place. I will not stand idly by in the face of cyberassaults on our nation."[239] Biden said he has instructed his transition team to study the breach, will make cybersecurity a priority at every level of government, and will identify and penalize the attackers.[73][3] Biden's incoming chief of staff, Ron Klain, said the Biden administration's response to the hack would extend beyond sanctions.[240]

On December 22, 2020, Biden said that, "I see no evidence that it's under control," and reported that his transition team was still being denied access to some briefings about the attack by Trump administration officials.[241][242]

In January 2021, Biden named appointees for two relevant White House positions: Elizabeth Sherwood-Randall as homeland security adviser, and Anne Neuberger as deputy national security adviser for cyber and emerging technology.[243]

Rest of the world

NATO said that it was "currently assessing the situation, with a view to identifying and mitigating any potential risks to our networks."[36] On December 18, the United Kingdom National Cyber Security Centre said that it was still establishing the attacks' impact on the UK.[244] The UK and Irish cybersecurity agencies published alerts targeting SolarWinds customers.[135]

On December 23, 2020, the UK Information Commissioner's Office - a national privacy authority - told UK organizations to check immediately whether they were impacted.[116][245]

On December 24, 2020, the Canadian Centre for Cyber Security asked SolarWinds Orion users in Canada to check for system compromises.[246][247]

Cyber espionage or cyberattack?

The attack prompted a debate on whether the hack should be treated as cyber espionage, or as a cyberattack constituting an act of war.[248] Most current and former U.S. officials considered the 2020 Russian hack to be a "stunning and distressing feat of espionage" but not a cyberattack because the Russians did not appear to destroy or manipulate data or cause physical damage (for example, to the electrical grid).[249] Erica Borghard of the Atlantic Council and Columbia's Saltzman Institute and Jacquelyn Schneider of the Hoover Institution and Naval War College argued that the breach was an act of espionage that could be responded to with "arrests, diplomacy, or counterintelligence" and had not yet been shown to be a cyberattack, a classification that would legally allow the U.S. to respond with force.[250] Law professor Jack Goldsmith wrote that the hack was a damaging act of cyber-espionage but "does not violate international law or norms" and wrote that "because of its own practices, the U.S. government has traditionally accepted the legitimacy of foreign governmental electronic spying in U.S. government networks."[251] Law professor Michael Schmitt concurred, citing the *Tallinn Manual*.[252]

By contrast, Microsoft president Brad Smith termed the hack a cyberattack,[249] stating that it was "not 'espionage as usual,' even in the digital age" because it was "not just an attack on specific targets, but on the trust and reliability of the world's critical infrastructure."[253][254] U.S. Senator Richard J. Durbin (D-IL) described the attack as tantamount to a declaration of war.[49][4]

Debate on possible U.S. responses

Writing for *Wired*, Borghard and Schneider opined that the U.S. "should continue to build and rely on strategic deterrence to convince states not to weaponize the cyber intelligence they collect". They also stated that because deterrence may not effectively discourage cyber-espionage attempts by threat actors, the U.S. should also focus on making cyber-espionage less successful through methods such as enhanced cyber-defenses, better information-sharing, and "defending forward" (reducing Russian and Chinese offensive cyber-capabilities).[250]

Writing for *The Dispatch*, Goldsmith wrote that the failure of defense and deterrence strategies against cyber-intrusion should prompt consideration of a "mutual restraint" strategy, "whereby the United States agrees to curb certain activities in foreign networks in exchange for forbearance by our adversaries in our networks."[251]

Cybersecurity author Bruce Schneier advocated against retaliation or increases in offensive capabilities, proposing instead the adoption of a defense-dominant strategy and ratification of the Paris Call for Trust and Security in Cyberspace or the Global Commission on the Stability of Cyberspace.[255]

In the *New York Times*, Paul Kolbe, former CIA agent and director of the Intelligence Project at Harvard's Belfer Center for Science and International Affairs, echoed Schneier's call for improvements in the U.S.'s cyberdefenses and international agreements. He also noted that the US is engaged in similar operations against other countries in what he described as an ambient cyber-conflict.[256]

In *Slate*, Fred Kaplan argued that the structural problems that enable computer network intrusions like this had been public knowledge since 1967 and that successive U.S. governments had failed to implement the structural defenses repeatedly requested by subject experts.[257] He pointed out that an escalatory response to espionage would be counterproductive for U.S. interests, whereas finally strengthening the defenses and drawing clear red lines in the gray areas of cyber-conflict policy would be more fruitful strategies.[258]

See also

- Cyberwarfare in the United States
- Cyberwarfare by Russia
- EternalBlue
- Global surveillance disclosures (2013–present)
- List of data breaches
- Moonlight Maze
- Office of Personnel Management data breach
- Security dilemma
- The Shadow Brokers
- 2008 cyberattack on United States

References

1. Sanger, David E.; Perlroth, Nicole; Schmitt, Eric (December 15, 2020). "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit" (https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html). *The New York Times*. Archived (https://web.archive.org/web/20201218062201/https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html) from the original on December 18, 2020. Retrieved December 15, 2020.
2. Morath, Eric; Cambon, Sarah Chaney (January 14, 2021). "SolarWinds Hack Leaves Market-Sensitive Labor Data Intact, Scalia Says" (https://www.wsj.com/articles/solarwinds-hack-leaves-market-sensitive-labor-data-intact-scalia-says-11610627053). *The Wall Street Journal*.
3. "Hackers Tied to Russia Hit Nuclear Agency; Microsoft Is Exposed" (https://www.bloomberg.com/news/articles/2020-12-17/u-s-states-were-also-hacked-in-suspected-russian-attack). Bloomberg L.P. December 17, 2020. Archived (https://web.archive.org/web/20201218062228/https://www.bloomberg.com/news/articles/2020-12-17/u-s-states-were-also-hacked-in-suspected-russian-attack) from the original on December 18, 2020. Retrieved December 17, 2020.
4. Sanger, David E.; Perlroth, Nicole; Barnes, Julian E. (December 16, 2020). "Billions Spent on U.S. Defenses Failed to Detect Giant Russian Hack" (https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html). *The New York Times*. Archived (https://web.archive.org/web/20201216200710/https://www.nytimes.com/2020/12/16/us/politics/russia-hack-putin-trump-biden.html) from the original on December 16, 2020. Retrieved December 16, 2020.

5. Stubbs, Jack; Satter, Raphael; Menn, Joseph (December 15, 2020). "U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack" (https://www.reuters.com/article/global-cyber-idUSKBN28O1Z3). *Reuters*. Archived (https://web.archive.org/web/20201215113854/https://www.reuters.com/article/global-cyber-idUSKBN28O1Z3) from the original on December 15, 2020. Retrieved December 15, 2020.
6. Fung, Brian. "Why the US government hack is literally keeping security experts awake at night" (https://www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html). CNN. Archived (https://web.archive.org/web/20201217062640/https://www.cnn.com/2020/12/16/tech/solarwinds-orion-hack-explained/index.html) from the original on December 17, 2020. Retrieved December 18, 2020.
7. Goodin, Dan (January 7, 2021). "DoJ says SolarWinds hackers breached its Office 365 system and read email" (https://arstechnica.com/information-technology/2021/01/doj-says-solarwinds-hackers-breached-its-office-365-system-and-read-email/). *Ars Technica*.
8. "SolarWinds Likely Hacked at Least One Year Before Breach Discovery" (https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery). *SecurityWeek.com*.
9. Bing, Christopher (December 14, 2020). "Suspected Russian hackers spied on U.S. Treasury emails – sources" (https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN28N0PG). *Reuters*. Archived (https://web.archive.org/web/20201214025738/https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive-idUSKBN28N0PG) from the original on December 14, 2020. Retrieved December 14, 2020.
10. O'Brien, Matt; Bajak, Frank (December 15, 2020). "EXPLAINER: How bad is the hack that targeted US agencies?" (https://www.chron.com/news/article/Explainer-How-bad-is-the-hack-that-targeted-US-15800740.php). *Houston Chronicle*. Archived (https://web.archive.org/web/20201214232009/https://www.chron.com/news/article/Explainer-How-bad-is-the-hack-that-targeted-US-15800740.php) from the original on December 14, 2020. Retrieved December 15, 2020.
11. "SolarWinds Orion: More US government agencies hacked" (https://www.bbc.com/news/technology-55318815). BBC. December 15, 2020. Archived (https://web.archive.org/web/20201216130015/https://www.bbc.com/news/technology-55318815) from the original on December 16, 2020. Retrieved December 16, 2020.
12. "Russian hack was 'classic espionage' with stealthy, targeted tactics" (https://web.archive.org/web/20201214201505/https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government/). *The Washington Post*. December 14, 2020. Archived from the original (https://www.washingtonpost.com/technology/2020/12/14/russia-hack-us-government/) on December 14, 2020. Retrieved December 18, 2020.
13. Cook, James (December 18, 2020). "Microsoft warns UK companies were targeted by SolarWinds hackers" (https://www.telegraph.co.uk/technology/2020/12/18/microsoft-warns-uk-companies-targeted-solarwinds-hackers/) – via www.telegraph.co.uk.
14. "Group Behind SolarWinds Hack Bypassed MFA to Access Emails at US Think Tank" (https://www.securityweek.com/group-behind-solarwinds-hack-bypassed-mfa-access-emails-us-think-tank). *SecurityWeek.com*. Archived (https://web.archive.org/web/20201216144033/https://www.securityweek.com/group-behind-solarwinds-hack-bypassed-mfa-access-emails-us-think-tank) from the original on December 16, 2020. Retrieved December 17, 2020.
15. Goodin, Dan (December 15, 2020). "SolarWinds hackers have a clever way to bypass multi-factor authentication" (https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/). *Ars Technica*. Archived (https://web.archive.org/web/20201216212004/https://arstechnica.com/information-technology/2020/12/solarwinds-hackers-have-a-clever-way-to-bypass-multi-factor-authentication/) from the original on December 16, 2020. Retrieved December 17, 2020.
16. "Russian hackers compromised Microsoft cloud customers through third party, putting emails and other data at risk" (https://www.msn.com/en-us/news/us/russian-hackers-compromised-microsoft-cloud-customers-through-third-party-putting-emails-and-other-data-at-risk/ar-BB1cdqp0). *www.msn.com*.
17. Satter, Joseph Menn, Raphael (December 24, 2020). "Suspected Russian hackers used Microsoft vendors to breach customers" (https://www.reuters.com/article/us-global-cyber-usa-idUSKBN28Y1BF) – via www.reuters.com.
18. Perlroth, Nicole (December 25, 2020). "Russians Are Believed to Have Used Microsoft Resellers in Cyberattacks" (https://www.nytimes.com/2020/12/24/us/russia-microsoft-resellers-cyberattacks.html) – via NYTimes.com.
19. "Microsoft, FireEye confirm SolarWinds supply chain attack" (https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/). ZDNet. December 14, 2020. Archived (https://web.archive.org/web/20201216173348/https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/) from the original on December 16, 2020. Retrieved December 16, 2020.

20. "Sunburst Trojan – What You Need to Know" (https://www.deepinstinct.com/2020/12/16/sunburst-trojan-what-you-need-to-know/). *Deep Instinct*. December 16, 2020. Archived (https://web.archive.org/web/20201218062210/https://www.deepinstinct.com/2020/12/16/sunburst-trojan-what-you-need-to-know/) from the original on December 18, 2020. Retrieved December 17, 2020.
21. "VMware Flaw a Vector in SolarWinds Breach?" (https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/). Krebs on Security. December 7, 2020. Retrieved December 18, 2020.
22. "VMware Falls on Report Its Software Led to SolarWinds Breach" (https://www.bloomberg.com/news/articles/2020-12-18/vmware-falls-on-report-its-software-led-to-solarwinds-breach). Bloomberg. December 18, 2020. Retrieved December 18, 2020.
23. Hvistendahl, Mara; Lee, Micah; Smith, Jordan (December 17, 2020). "Russian Hackers Have Been Inside Austin City Network for Months" (https://theintercept.com/2020/12/17/russia-hack-austin-texas/). *The Intercept*. Archived (https://web.archive.org/web/20201217234405/https://theintercept.com/2020/12/17/russia-hack-austin-texas/) from the original on December 17, 2020. Retrieved December 18, 2020.
24. "CISA orders agencies to quickly patch critical Netlogon bug" (https://www.cyberscoop.com/cisa-netlogon-microsoft-vulnerability-emergency/). *CyberScoop*. September 21, 2020. Archived (https://web.archive.org/web/20201030201359/https://www.cyberscoop.com/cisa-netlogon-microsoft-vulnerability-emergency/) from the original on October 30, 2020. Retrieved December 18, 2020.
25. Bing, Christopher (December 13, 2020). "REFILE-EXCLUSIVE-U.S. Treasury breached by hackers backed by foreign government – sources" (https://www.reuters.com/article/usa-cyber-treasury-idUSL1N2IT0I8). *Reuters*. Archived (https://web.archive.org/web/20201214024713/https://www.reuters.com/article/usa-cyber-treasury-idUSL1N2IT0I8) from the original on December 14, 2020. Retrieved December 14, 2020.
26. Nakashima, Ellen (December 13, 2020). "Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm" (https://web.archive.org/web/20201213220635/https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html). *The Washington Post*. Archived from the original (https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html) on December 13, 2020. Retrieved December 14, 2020.
27. "Federal government breached by Russian hackers who targeted FireEye" (https://www.nbcnews.com/news/us-news/russian-hackers-breach-u-s-government-effort-aimed-agencies-private-n1251057). NBC News. Archived (https://web.archive.org/web/20201214024737/https://www.nbcnews.com/news/us-news/russian-hackers-breach-u-s-government-effort-aimed-agencies-private-n1251057) from the original on December 14, 2020. Retrieved December 14, 2020.
28. "US cyber-attack: Russia 'clearly' behind SolarWinds operation, says Pompeo" (https://www.bbc.co.uk/news/world-us-canada-55374945). BBC. December 19, 2020. Retrieved December 19, 2020.
29. Washington, Georgi Kantchev in Moscow and Warren P. Strobel in (January 2, 2021). "How Russia's 'Info Warrior' Hackers Let Kremlin Play Geopolitics on the Cheap" (https://www.wsj.com/articles/how-russias-info-warrior-hackers-let-kremlin-play-geopolitics-on-the-cheap-11609592401). *Wall Street Journal*. ISSN 0099-9660 (https://www.worldcat.org/issn/0099-9660). Retrieved January 5, 2021.
30. Bossert, Thomas P. (December 17, 2020). "Opinion | I Was the Homeland Security Adviser to Trump. We're Being Hacked" (https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html). *The New York Times*. Archived (https://web.archive.org/web/20201217112609/https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html) from the original on December 17, 2020. Retrieved December 17, 2020.
31. "U.S. Agencies Exposed in Attack by Suspected Russian Hackers" (https://www.bloomberg.com/news/articles/2020-12-14/u-s-government-agencies-attacked-by-hackers-in-software-update). Bloomberg L.P. December 14, 2020. Archived (https://web.archive.org/web/20201216002322/https://www.bloomberg.com/news/articles/2020-12-14/u-s-government-agencies-attacked-by-hackers-in-software-update) from the original on December 16, 2020. Retrieved December 17, 2020.
32. "Cyber attack may be 'worst hacking case in the history of America' " (https://www.reviewjournal.com/news/politics-and-government/cyber-attack-may-be-worst-hacking-case-in-the-history-of-america-2223270/). *Las Vegas Review-Journal*. December 17, 2020. Archived (https://web.archive.org/web/20201218062142/https://www.reviewjournal.com/news/politics-and-government/cyber-attack-may-be-worst-hacking-case-in-the-history-of-america-2223270/) from the original on December 18, 2020. Retrieved December 18, 2020.

33. "US under major active cyberattack from Russia, Trump's former security adviser warns" (https://www.independent.co.uk/news/world/americas/russia-cyber-attack-us-trump-b1775632.html). *The Independent*. December 17, 2020. Archived (https://web.archive.org/web/20201218062142/https://www.independent.co.uk/news/world/americas/russia-cyber-attack-us-trump-b1775632.html) from the original on December 18, 2020. Retrieved December 17, 2020.
34. "What we know – and still don't – about the worst-ever US government cyber-attack" (https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government). *The Guardian*. December 18, 2020.
35. [30][31][32][33][34]
36. "U.K. Government, NATO Join U.S. in Monitoring Risk From Hack" (https://www.bloomberg.com/news/articles/2020-12-14/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack). Bloomberg L.P. December 14, 2020. Archived (https://web.archive.org/web/20201215021953/https://www.bloomberg.com/news/articles/2020-12-14/u-k-government-nato-join-u-s-in-monitoring-risk-from-hack) from the original on December 15, 2020. Retrieved December 16, 2020.
37. "At Least 200 Victims Identified in Suspected Russian Hacking" (https://www.bloomberg.com/news/articles/2020-12-19/at-least-200-victims-identified-in-suspected-russian-hacking). December 19, 2020 – via www.bloomberg.com.
38. Macias, Amanda (December 13, 2020). "White House acknowledges reports of cyberattack on U.S. Treasury by foreign government" (https://www.cnbc.com/2020/12/13/cyber-hack-on-us-treasury-by-foreign-government-.html). CNBC. Archived (https://web.archive.org/web/20201214015022/https://www.cnbc.com/2020/12/13/cyber-hack-on-us-treasury-by-foreign-government-.html) from the original on December 14, 2020. Retrieved December 14, 2020.
39. Sanger, David E. (December 13, 2020). "Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect" (https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html). *The New York Times*. Archived (https://web.archive.org/web/20201214013043/https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html) from the original on December 14, 2020. Retrieved December 14, 2020.
40. Rosenberg, Adam. "Russian government-backed hackers breached the U.S. Treasury, Commerce departments" (https://mashable.com/article/us-treasury-hacked-office-365/). *Mashable*. Archived (https://web.archive.org/web/20201214032732/https://mashable.com/article/us-treasury-hacked-office-365/) from the original on December 14, 2020. Retrieved December 14, 2020.
41. Wade, Peter (December 13, 2020). "Treasury, Commerce, Other Agencies Hacked by Russian Government Spies, Report Says" (https://www.rollingstone.com/politics/politics-news/treasury-commerce-russian-government-spies-1103205/). *Rolling Stone*. Archived (https://web.archive.org/web/20201214024218/https://www.rollingstone.com/politics/politics-news/treasury-commerce-russian-government-spies-1103205/) from the original on December 14, 2020. Retrieved December 14, 2020.
42. [26][38][39][40][41]
43. Menn, Joseph (December 18, 2020). "Microsoft says it found malicious software in its systems" (https://www.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7). *Reuters*. Archived (https://web.archive.org/web/20201218062143/https://www.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7) from the original on December 18, 2020. Retrieved December 17, 2020.
44. Wolff, Josephine (December 16, 2020). "What We Do and Don't Know About the Massive Federal Government Hack" (https://slate.com/technology/2020/12/solarwinds-hack-commerce-treasury-breach.html). *Slate*. Archived (https://web.archive.org/web/20201216210929/https://slate.com/technology/2020/12/solarwinds-hack-commerce-treasury-breach.html) from the original on December 16, 2020. Retrieved December 17, 2020.
45. Cimpanu, Catalin (December 18, 2020). "NSA warns of federated login abuse for local-to-cloud attacks" (https://www.zdnet.com/article/nsa-warns-of-federated-login-abuse-for-local-to-cloud-attacks/). *Zero Day*. Ziff-Davis. Retrieved December 19, 2020.
46. Satter, Raphael (December 22, 2020). " 'Dozens of email accounts' were hacked at U.S. Treasury -Senator Wyden" (https://uk.reuters.com/article/uk-global-cyber-idUKKBN28V2XQ) – via uk.reuters.com.
47. "It could take years to evict Russia from the US networks it hacked, leaving it free to destroy or tamper with data, ex-White House official warns" (https://www.msn.com/en-us/news/politics/it-could-take-years-to-evict-russia-from-the-us-networks-it-hacked-leaving-it-free-to-destroy-or-tamper-with-data-ex-white-house-official-warns/ar-BB1c0ouw). MSN.

48. "Here are the critical responses required of all businesses after SolarWinds supply-chain hack" (https://www.scmagazine.com/home/security-news/here-are-the-critical-responses-required-of-all-businesses-after-solarwinds-supply-chain-hack/). *SC Media*. December 15, 2020. Archived (https://web.archive.org/web/20201216143142/https://www.scmagazine.com/home/security-news/here-are-the-critical-responses-required-of-all-businesses-after-solarwinds-supply-chain-hack/) from the original on December 16, 2020. Retrieved December 16, 2020.
49. Gould, Joe (December 17, 2020). "No. 2 Senate Democrat decries alleged Russian hack as 'virtual invasion' " (https://www.c4isrnet.com/congress/2020/12/17/no-2-senate-democrat-russia-hack-a-virtual-invasion/). *Defense News*.
50. Colvin, Jill; Lee, Matthew (December 19, 2020). "Trump downplays Russia in first comments on hacking campaign" (https://apnews.com/article/donald-trump-politics-mark-levin-coronavirus-pandemic-hacking-6080f156125a4a46edef2a6dcf826611). Associated Press. Retrieved December 20, 2020.
51. Stracqualursi, Veronica; Liptak, Kevin; Hansler, Jennifer (December 19, 2020). "Trump downplays massive cyber hack on government after Pompeo links attack to Russia" (https://www.cnn.com/2020/12/19/politics/pompeo-us-government-hack-russia/index.html). *CNN*. Retrieved December 19, 2020.
52. Kaplan, Fred (December 15, 2020). "Trump Has Been Whining About Fake Fraud—and Ignoring a Real Cybersecurity Crisis" (https://slate.com/news-and-politics/2020/12/solarwinds-trump-hack-fireeye.html). *Slate*. Archived (https://web.archive.org/web/20201216060553/https://slate.com/news-and-politics/2020/12/solarwinds-trump-hack-fireeye.html) from the original on December 16, 2020. Retrieved December 16, 2020.
53. Perlroth, Nicole; Sanger, David E. (May 16, 2018). "White House Eliminates Cybersecurity Coordinator Role (Published 2018)" (https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html). *The New York Times*. Archived (https://web.archive.org/web/20201213234429/https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html) from the original on December 13, 2020. Retrieved December 16, 2020.
54. Brandom, Russell (December 14, 2020). "Trump's chaos made America a sitting duck for cyberattacks" (https://www.theverge.com/2020/12/14/22174429/solarwinds-hack-russia-cisa-christopher-krebs-cybersecurity-infrastructure). *The Verge*. Archived (https://web.archive.org/web/20201215170320/https://www.theverge.com/2020/12/14/22174429/solarwinds-hack-russia-cisa-christopher-krebs-cybersecurity-infrastructure) from the original on December 15, 2020. Retrieved December 17, 2020.
55. "Russian government hackers behind breach at US treasury and commerce departments" (https://www.independent.co.uk/news/world/americas/us-politics/us-treasury-hackers-breach-trump-russia-b1772639.html). *The Independent*. December 13, 2020. Archived (https://web.archive.org/web/20201213233930/https://www.independent.co.uk/news/world/americas/us-politics/us-treasury-hackers-breach-trump-russia-b1772639.html) from the original on December 13, 2020. Retrieved December 14, 2020.
56. Nakashima, Ellen; Miroff, Nick (November 17, 2020). "Trump fires top DHS official who refuted his claims that the election was rigged" (https://www.washingtonpost.com/national-security/trump-fires-dhs-election-official/2020/11/17/97d3fa5c-251c-11eb-952e-0c475972cfc0_story.html). *The Washington Post*. Archived (https://web.archive.org/web/20201118041406/https://www.washingtonpost.com/national-security/trump-fires-dhs-election-official/2020/11/17/97d3fa5c-251c-11eb-952e-0c475972cfc0_story.html) from the original on November 18, 2020. Retrieved November 18, 2020.
57. Bowden, John (December 13, 2020). "Hackers backed by foreign government breach Treasury, Commerce departments: reports" (https://thehill.com/policy/cybersecurity/530035-hackers-backed-by-foreign-government-breach-treasury-report). *The Hill*. Archived (https://web.archive.org/web/20201215005023/https://thehill.com/policy/cybersecurity/530035-hackers-backed-by-foreign-government-breach-treasury-report) from the original on December 15, 2020. Retrieved December 15, 2020.
58. Cobb, Adrienne (December 15, 2020). "Forensic News Roundup: Russia hacks U.S. government, Trump silent" (https://forensicnews.net/forensic-news-roundup-russia-hacks-u-s-government-trump-silent/). *Forensic News*. Archived (https://web.archive.org/web/20201218062144/https://forensicnews.net/forensic-news-roundup-russia-hacks-u-s-government-trump-silent/) from the original on December 18, 2020. Retrieved December 17, 2020.
59. "Leadership" (https://www.dhs.gov/leadership). *Department of Homeland Security*. September 7, 2006. Archived (https://web.archive.org/web/20201216103017/https://www.dhs.gov/leadership) from the original on December 16, 2020. Retrieved December 17, 2020.
60. Miller, Maggie (November 12, 2020). "Senior DHS cybersecurity official to step down at end of week" (https://thehill.com/policy/cybersecurity/525721-senior-dhs-cybersecurity-official-to-step-down-at-end-of-week). *The Hill*. Archived (https://web.archive.org/web/20201128225021/https://thehill.com/policy/cybersecurity/525721-senior-dhs-cybersecurity-official-to-step-down-at-end-of-week) from the original on November 28, 2020. Retrieved December 17, 2020.

61. Sebenius, Alyza (January 13, 2021). "SolarWinds Hack Followed Years of Warnings of Weak Cybersecurity" (https://www.bloomberg.com/news/articles/2021-01-13/solarwinds-hack-followed-years-of-warnings-of-weak-cybersecurity). *Bloomberg.com*. Retrieved January 13, 2021.
62. "The SolarWinds Perfect Storm: Default Password, Access Sales and More" (https://threatpost.com/solarwinds-default-password-access-sales/162327/). *threatpost.com*. Archived (https://web.archive.org/web/20201217143937/https://threatpost.com/solarwinds-default-password-access-sales/162327/) from the original on December 17, 2020. Retrieved December 17, 2020.
63. "Hackers used SolarWinds' dominance against it in sprawling spy campaign" (https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8). *Reuters*. December 16, 2020. Archived (https://web.archive.org/web/20201217222405/https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8) from the original on December 17, 2020. Retrieved December 16, 2020.
64. "SolarWinds Adviser Warned of Lax Security Years Before Hack" (https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack). December 21, 2020. Retrieved December 22, 2020 – via www.bloomberg.com.
65. "SolarWinds Hack Could Affect 18K Customers" (https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/). Krebs on Security. Archived (https://web.archive.org/web/20201216063419/https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/) from the original on December 16, 2020. Retrieved December 16, 2020.
66. Varghese, Sam. "SolarWinds FTP credentials were leaking on GitHub in November 2019" (https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html). *itwire.com*. Archived (https://web.archive.org/web/20201215011307/https://itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html) from the original on December 15, 2020. Retrieved December 17, 2020.
67. McCarthy, Kieren. "SolarWinds: Hey, only as many as 18,000 customers installed backdoored software linked to US govt hacks" (https://www.theregister.com/2020/12/15/solar_winds_update/). *The Register*. Archived (https://web.archive.org/web/20201216222506/https://www.theregister.com/2020/12/15/solar_winds_update/) from the original on December 16, 2020. Retrieved December 16, 2020.
68. Claburn, Thomas. "We're not saying this is how SolarWinds was backdoored, but its FTP password 'leaked on GitHub in plaintext' " (https://www.theregister.com/2020/12/16/solarwinds_github_password/). *The Register*. Archived (https://web.archive.org/web/20201218002615/https://www.theregister.com/2020/12/16/solarwinds_github_password/) from the original on December 18, 2020. Retrieved December 17, 2020.
69. Novet, Jordan (December 16, 2020). "SolarWinds hack has shaved 23% from software company's stock this week" (https://www.cnbc.com/2020/12/16/solarwinds-hack-triggers-23percent-stock-haircut-this-week-so-far.html). CNBC. Archived (https://web.archive.org/web/20201216223540/https://www.cnbc.com/2020/12/16/solarwinds-hack-triggers-23percent-stock-haircut-this-week-so-far.html) from the original on December 16, 2020. Retrieved December 17, 2020.
70. McCarthy, Kieren. "SolarWinds' shares drop 22 per cent. But what's this? $286m in stock sales just before hack announced?" (https://www.theregister.com/2020/12/16/solarwinds_stock_sale/). *The Register*. Archived (https://web.archive.org/web/20201217150244/https://www.theregister.com/2020/12/16/solarwinds_stock_sale/) from the original on December 17, 2020. Retrieved December 17, 2020.
71. "SolarWinds falls under scrutiny after hack, stock sales" (https://www.marketwatch.com/story/solarwinds-falls-under-scrutiny-after-hack-stock-sales-01608166019). *MarketWatch*. Associated Press. Archived (https://web.archive.org/web/20201217023156/https://www.marketwatch.com/story/solarwinds-falls-under-scrutiny-after-hack-stock-sales-01608166019) from the original on December 17, 2020. Retrieved December 17, 2020.
72. Menn, Joseph (December 18, 2020). "Microsoft says it found malicious software in its systems" (https://uk.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7). *Reuters*. Archived (https://web.archive.org/web/20201218062157/https://uk.reuters.com/article/uk-usa-cyber-breach-idUKKBN28R3B7) from the original on December 18, 2020. Retrieved December 18, 2020.
73. Sanger, David E.; Perlroth, Nicole (December 17, 2020). "More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government" (https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html). *The New York Times*. Archived (https://web.archive.org/web/20201217202216/https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html) from the original on December 17, 2020. Retrieved December 17, 2020.

74. "How the SolarWinds Hackers Bypassed Duo's Multi-Factor Authentication – Schneier on Security" (https://www.schneier.com/blog/archives/2020/12/how-the-solarwinds-hackers-bypassed-duo-multi-factor-authentication.html). *schneier.com*. Archived (https://web.archive.org/web/20201217224933/https://www.schneier.com/blog/archives/2020/12/how-the-solarwinds-hackers-bypassed-duo-multi-factor-authentication.html) from the original on December 17, 2020. Retrieved December 17, 2020.
75. "US treasury hacked by foreign government group – report" (https://www.theguardian.com/technology/2020/dec/13/us-treasury-hacked-group-backed-by-foreign-government-report). *The Guardian*. December 13, 2020. Archived (https://web.archive.org/web/20201214030019/https://www.theguardian.com/technology/2020/dec/13/us-treasury-hacked-group-backed-by-foreign-government-report) from the original on December 14, 2020. Retrieved December 14, 2020.
76. "Foreign government hacked into US Treasury Department's emails – reports" (https://news.sky.com/story/foreign-government-hacked-into-us-treasury-departments-emails-reports-12160763). Sky News. Archived (https://web.archive.org/web/20201214032244/https://news.sky.com/story/foreign-government-hacked-into-us-treasury-departments-emails-reports-12160763) from the original on December 14, 2020. Retrieved December 14, 2020.
77. "No One Knows How Deep Russia's Hacking Rampage Goes" (https://www.wired.com/story/russia-solarwinds-supply-chain-hack-commerce-treasury). *Wired*. Archived (https://web.archive.org/web/20201217013054/https://www.wired.com/story/russia-solarwinds-supply-chain-hack-commerce-treasury/) from the original on December 17, 2020. Retrieved December 16, 2020.
78. Goodin, Dan (December 14, 2020). "~18,000 organizations downloaded backdoor planted by Cozy Bear hackers" (https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/). *Ars Technica*. Archived (https://web.archive.org/web/20201216194610/https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/) from the original on December 16, 2020. Retrieved December 17, 2020.
79. Cimpanu, Catalin (January 12, 2021). "Third malware strain discovered in SolarWinds supply chain attack" (https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/). *ZDNet*. Retrieved January 13, 2021.
80. Sebastian, Dave (January 12, 2021). "SolarWinds Discloses Earlier Evidence of Hack" (https://www.wsj.com/articles/solarwinds-discloses-earlier-evidence-of-hack-11610473937). *WSJ*. Retrieved January 13, 2021.
81. Sharwood, Simon. "Trump administration says Russia behind SolarWinds hack. Trump himself begs to differ" (https://www.theregister.com/2020/12/20/solarwinds_update_trump_contradicts_pompeo_russia_attribution/). *The Register*.
82. Corfield, Gareth (January 12, 2021). "SolarWinds malware was sneaked out of the firm's Orion build environment 6 months before anyone realised it was there – report" (https://www.theregister.com/2021/01/12/solarwinds_tech_analysis_crowdstrike/). *The Register*. Retrieved January 13, 2021.
83. Cimpanu, Catalin. "Microsoft to quarantine SolarWinds apps linked to recent hack" (https://www.zdnet.com/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/). ZDNet. Archived (https://web.archive.org/web/20201217002642/https://www.zdnet.com/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/) from the original on December 17, 2020. Retrieved December 16, 2020.
84. Lyons, Kim (December 13, 2020). "Hackers backed by Russian government reportedly breached US government agencies" (https://www.theverge.com/2020/12/13/22173035/hackers-russia-breached-us-government-agencies-email-cozy-bear). *The Verge*. Archived (https://web.archive.org/web/20201214190936/https://www.theverge.com/2020/12/13/22173035/hackers-russia-breached-us-government-agencies-email-cozy-bear) from the original on December 14, 2020. Retrieved December 15, 2020.
85. "CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products" (https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network). CISA. Archived (https://web.archive.org/web/20201215035936/https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network) from the original on December 15, 2020. Retrieved December 15, 2020.
86. "U.S. Government Agencies Hit by Hackers During Software Update" (https://www.msn.com/en-us/news/politics/u-s-government-agencies-hit-by-hackers-during-software-update/ar-BB1bTMl4?fbclid=IwAR2jsg56Z2yz2pshs-3DmTZio5STK_0MHCWDIiB8yr-VVAew-vvBpCgLqUE). MSN. Archived (https://web.archive.org/web/20201218062145/https://www.msn.com/en-us/news/politics/u-s-government-agencies-hit-by-hackers-during-software-update/ar-BB1bTMl4) from the original on December 18, 2020. Retrieved December 14, 2020.

87. Cimpanu, Catalin. "Microsoft and industry partners seize key domain used in SolarWinds hack" (https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/). ZDNet. Archived (https://web.archive.org/web/20201217003334/https://www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/) from the original on December 17, 2020. Retrieved December 17, 2020.
88. "DHS Among Those Hit in Sophisticated Cyberattack by Foreign Adversaries – Report" (https://threatpost.com/dhs-sophisticated-cyberattack-foreign-adversaries/162242/). *threatpost.com*. Archived (https://web.archive.org/web/20201216200536/https://threatpost.com/dhs-sophisticated-cyberattack-foreign-adversaries/162242/) from the original on December 16, 2020. Retrieved December 17, 2020.
89. Timberg, Craig; Nakashima, Ellen (December 16, 2020). "Russians outsmart US government hacker detection system — but Moscow denies involvement" (https://www.independent.co.uk/news/world/americas/us-russia-hacking-cyber-security-b1774793.html). *The Independent*. Archived (https://web.archive.org/web/20201218062145/https://www.independent.co.uk/news/world/americas/us-russia-hacking-cyber-security-b1774793.html) from the original on December 18, 2020. Retrieved December 16, 2016.
90. "SolarWinds: Why the Sunburst hack is so serious" (https://www.bbc.com/news/technology-55321643). BBC. December 16, 2020. Archived (https://web.archive.org/web/20201216221808/https://www.bbc.com/news/technology-55321643) from the original on December 16, 2020. Retrieved December 18, 2020.
91. "SolarWinds Orion and UNC2452 – Summary and Recommendations" (https://www.trustedsec.com/blog/solarwinds-orion-and-unc2452-summary-and-recommendations/). *TrustedSec*. December 14, 2020. Archived (https://web.archive.org/web/20201215232939/https://www.trustedsec.com/blog/solarwinds-orion-and-unc2452-summary-and-recommendations/) from the original on December 15, 2020. Retrieved December 17, 2020.
92. "FireEye, Microsoft create kill switch for SolarWinds backdoor" (https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/). *BleepingComputer*. Archived (https://web.archive.org/web/20201217033942/https://www.bleepingcomputer.com/news/security/fireeye-microsoft-create-kill-switch-for-solarwinds-backdoor/) from the original on December 17, 2020. Retrieved December 18, 2020.
93. "Trend data on the SolarWinds Orion compromise" (https://blog.cloudflare.com/solarwinds-orion-compromise-trend-data/). *The Cloudflare Blog*. December 16, 2020. Archived (https://web.archive.org/web/20201216170227/https://blog.cloudflare.com/solarwinds-orion-compromise-trend-data/) from the original on December 16, 2020. Retrieved December 16, 2020.
94. "After high profile hacks hit federal agencies, CISA demands drastic SolarWinds mitigation" (https://www.scmagazine.com/home/security-news/apts-cyberespionage/disconnect-or-power-down-after-high-profile-hacks-cisa-demands-drastic-solarwinds-mitigation/). *SC Media*. December 14, 2020. Archived (https://web.archive.org/web/20201215070401/https://www.scmagazine.com/home/security-news/apts-cyberespionage/disconnect-or-power-down-after-high-profile-hacks-cisa-demands-drastic-solarwinds-mitigation/) from the original on December 15, 2020. Retrieved December 17, 2020.
95. "Mitigating Cloud Supply-chain Risk: Office 365 and Azure Exploited in Massive U.S Government Hack" (https://www.ciphercloud.com/mitigating-cloud-supply-chain-risk-office-365-and-azure-exploited-in-massive-u-s-government-hack/). CipherCloud. December 18, 2020. Archived (https://web.archive.org/web/20201218062211/https://www.ciphercloud.com/mitigating-cloud-supply-chain-risk-office-365-and-azure-exploited-in-massive-u-s-government-hack/) from the original on December 18, 2020. Retrieved December 18, 2020.
96. "Massive hack of US government launches search for answers as Russia named top suspect" (https://abc57.com/news/massive-hack-of-us-government-launches-search-for-answers-as-russia-named-top-suspect). *ABC57*. Archived (https://web.archive.org/web/20201218062229/https://abc57.com/news/massive-hack-of-us-government-launches-search-for-answers-as-russia-named-top-suspect) from the original on December 18, 2020. Retrieved December 17, 2020.
97. Dorfman, Zach. "What we know about Russia's sprawling hack into federal agencies" (https://www.axios.com/russias-sprawling-hack-of-federal-agencies-alarms-43a9f6f7-5d85-49a6-828b-8371129c276e.html). *Axios*. Archived (https://web.archive.org/web/20201215111038/https://www.axios.com/russias-sprawling-hack-of-federal-agencies-alarms-43a9f6f7-5d85-49a6-828b-8371129c276e.html) from the original on December 15, 2020. Retrieved December 16, 2020.
98. "Schiff calls for 'urgent' work to defend nation in the wake of massive cyberattack" (https://www.msn.com/en-us/news/politics/schiff-calls-for-urgent-work-to-defend-nation-in-the-wake-of-massive-cyberattack/ar-BB1bZtaQ). MSN. Archived (https://web.archive.org/web/20201217013952/http://www.msn.com/en-us/news/politics/schiff-calls-for-urgent-work-to-defend-nation-in-the-wake-of-massive-cyberattack/ar-BB1bZtaQ) from the original on December 17, 2020. Retrieved December 17, 2020.

99. "Unraveling Network Infrastructure Linked to the SolarWinds Hack" (https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack). *DomainTools*. Archived (https://web.archive.org/web/20201217173553/https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack) from the original on December 17, 2020. Retrieved December 17, 2020.
100. "The U.S. government spent billions on a system for detecting hacks. The Russians outsmarted it" (https://www.seattletimes.com/nation-world/the-u-s-government-spent-billions-on-a-system-for-detecting-hacks-the-russians-outsmarted-it/). *The Seattle Times*. Archived (https://web.archive.org/web/20201218062159/https://www.seattletimes.com/nation-world/the-u-s-government-spent-billions-on-a-system-for-detecting-hacks-the-russians-outsmarted-it/) from the original on December 18, 2020. Retrieved December 16, 2020.
101. Menn, Christopher Bing, Jack Stubbs, Raphael Satter, Joseph (February 3, 2021). "Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources" (https://www.reuters.com/article/us-cyber-solarwinds-china-exclusive-idUSKBN2A22K8). *Reuters*. Retrieved February 8, 2021.
102. "Dark Halo Leverages SolarWinds Compromise to Breach Organizations" (https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/). Volexity.
103. Tarabay, Jamie (December 15, 2020). "Hacking Spree by Suspected Russians Included U.S. Think Tank" (https://www.bloomberg.com/news/articles/2020-12-15/hacking-spree-by-suspected-russians-included-u-s-think-tank). Bloomberg L.P. Archived (https://web.archive.org/web/20201218062232/https://www.bloomberg.com/news/articles/2020-12-15/hacking-spree-by-suspected-russians-included-u-s-think-tank) from the original on December 18, 2020. Retrieved December 17, 2020.
104. "Microsoft alerts CrowdStrike of hackers' attempted break-in" (https://www.cyberscoop.com/crowdstrike-solarwinds-targeted-microsoft/). *CyberScoop*. December 24, 2020.
105. "Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets" (https://us-cert.cisa.gov/ncas/alerts/aa20-296a). CISA.
106. "Hackers backed by foreign government reportedly steal info from US Treasury" (https://www.timesofisrael.com/hackers-backed-by-foreign-government-reportedly-steal-info-from-us-treasury/). *The Times of Israel*. Archived (https://web.archive.org/web/20201214031245/https://www.timesofisrael.com/hackers-backed-by-foreign-government-reportedly-steal-info-from-us-treasury/) from the original on December 14, 2020. Retrieved December 14, 2020.
107. Sanger, David E.; Perlroth, Nicole (December 8, 2020). "FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State" (https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html). *The New York Times*. Archived (https://web.archive.org/web/20201215184304/https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html) from the original on December 15, 2020. Retrieved December 15, 2020.
108. "US cybersecurity firm FireEye says it was hacked by foreign government" (https://www.theguardian.com/technology/2020/dec/08/fireeye-hack-cybersecurity-theft). *The Guardian*. December 9, 2020. Archived (https://web.archive.org/web/20201216014233/https://www.theguardian.com/technology/2020/dec/08/fireeye-hack-cybersecurity-theft) from the original on December 16, 2020. Retrieved December 15, 2020.
109. "Russia's FireEye Hack Is a Statement—but Not a Catastrophe" (https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/). *Wired*. Archived (https://web.archive.org/web/20201216000225/https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/) from the original on December 16, 2020. Retrieved December 17, 2020.
110. "Suspected Russia SolarWinds hack exposed after FireEye cybersecurity firm found "backdoor" " (https://www.newsweek.com/solarwinds-russia-hack-cyberattack-fireeye-software-malware-backdoor-cybersecurity-1554730). *Newsweek*. December 15, 2020. Archived (https://web.archive.org/web/20201216043909/https://www.newsweek.com/solarwinds-russia-hack-cyberattack-fireeye-software-malware-backdoor-cybersecurity-1554730) from the original on December 16, 2020. Retrieved December 16, 2020.
111. "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor" (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html). *FireEye*. December 13, 2020. Archived (https://web.archive.org/web/20201215110129/https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html) from the original on December 15, 2020. Retrieved December 15, 2020.

12. Paul, Kari (December 15, 2020). "What you need to know about the biggest hack of the US government in years" (https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department). *The Guardian*. Archived (https://web.archive.org/web/20201216090102/https://www.theguardian.com/technology/2020/dec/15/orion-hack-solar-winds-explained-us-treasury-commerce-department) from the original on December 16, 2020. Retrieved December 16, 2020.
13. Gatlan, Sergiu (January 12, 2021). "New Sunspot malware found while investigating SolarWinds hack" (https://www.bleepingcomputer.com/news/security/new-sunspot-malware-found-while-investigating-solarwinds-hack/). *BleepingComputer*. Retrieved January 13, 2021.
14. Goodin, Dan (December 7, 2020). "NSA says Russian state hackers are using a VMware flaw to ransack networks" (https://arstechnica.com/information-technology/2020/12/nsa-says-russian-state-hackers-are-using-a-vmware-flaw-to-ransack-networks/). *Ars Technica*. Retrieved December 19, 2020.
15. Bing, Christopher (December 14, 2020). "Russian-sponsored hackers behind broad security breach of U.S. agencies: sources" (https://www.japantimes.co.jp/news/2020/12/14/world/us-treasury-hack/). *The Japan Times*. Archived (https://web.archive.org/web/20201214010144/https://www.japantimes.co.jp/news/2020/12/14/world/us-treasury-hack/) from the original on December 14, 2020. Retrieved December 14, 2020.
16. Katz, Justin (December 23, 2020). "50 orgs 'genuinely impacted' by SolarWinds hack, FireEye chief says" (https://defensesystems.com/articles/2020/12/23/solarwinds-hack-impact.aspx). *Defense Systems*.
17. Slowik, Joe. (14 December 2020). "Unraveling Network Infrastructure Linked to the SolarWinds Hack". DomainTools website (https://www.domaintools.com/resources/blog/unraveling-network-infrastructure-linked-to-the-solarwinds-hack#) Retrieved 27 December 2020.
18. "SolarWinds malware has "curious" ties to Russian-speaking hackers" (https://arstechnica.com/information-technology/2021/01/solarwinds-malware-has-curious-ties-to-russian-speaking-hackers/). *Ars Technica*. January 11, 2021. Retrieved January 13, 2021.
19. Corfield, Gareth (January 12, 2021). "Kaspersky Lab autopsies evidence on SolarWinds hack" (https://www.theregister.com/2021/01/12/solarwinds_russia_kaspersky/). *The Register*. Retrieved January 13, 2021.
20. Greenberg, Andy (January 11, 2021). "SolarWinds Hackers Shared Tricks With Known Russian Cyberspies" (https://www.wired.com/story/solarwinds-russia-hackers-turla-malware/). *Wired*. Retrieved January 13, 2021.
21. Roth, Andrew (January 11, 2021). "Global cyber-espionage campaign linked to Russian spying tools" (https://www.theguardian.com/world/2021/jan/11/solarwinds-hack-russian-spying-tools-hackers-malware-fsb). *the Guardian*. Retrieved January 13, 2021.
22. Castronuovo, Celine (February 2, 2021). "US payroll agency targeted by Chinese hackers: report" (https://thehill.com/policy/cybersecurity/537067-us-payroll-agency-targeted-by-chinese-hackers-report). *TheHill*. Retrieved February 10, 2021.
23. "Trump downplays government hack after Pompeo blames it on Russia" (https://www.theguardian.com/us-news/2020/dec/19/mike-pompeo-we-can-say-pretty-clearly-russia-behind-hack-us-agencies). *the Guardian*. December 19, 2020.
24. Byrnes, Jesse (December 19, 2020). "Pompeo: Russia 'pretty clearly' behind massive cyberattack" (https://thehill.com/homenews/administration/530962-pompeo-russia-pretty-clearly-behind-massive-cyberattack). *The Hill*.
25. "Trump downplays massive US cyberattack, points to China" (https://www.dw.com/en/trump-downplays-massive-us-cyberattack-points-to-china/a-55996519). *Deutsche Welle*. December 19, 2020.
26. Axelrod, Tal (December 19, 2020). "Trump downplays impact of hack, questions whether Russia involved" (https://thehill.com/homenews/administration/530982-trump-downplays-impact-of-government-hack-in-first-public-remarks). *The Hill*.
27. "US cyber-attack: Around 50 firms 'genuinely impacted' by massive breach" (https://www.bbc.com/news/world-us-canada-55386947). December 20, 2020. Retrieved December 21, 2020 – via www.bbc.com.
28. "Trump finds himself isolated in refusal to blame Russia for big cyberattack" (https://www.latimes.com/world-nation/story/2020-12-20/lawmakers-experts-baffled-trump-brushes-off-suspected-russian-hack). *Los Angeles Times*. December 20, 2020. Retrieved December 21, 2020.
29. Janfaza, Rachel (December 21, 2020). "Barr contradicts Trump by saying it 'certainly appears' Russia behind cyberattack" (https://edition.cnn.com/2020/12/21/politics/william-barr-russia-cyberattack/index.html). *cnn.com*. CNN. Retrieved December 26, 2020.
30. Wilkie, Christina (December 21, 2020). "Attorney General Barr breaks with Trump, says SolarWinds hack 'certainly appears to be the Russians' " (https://www.cnbc.com/2020/12/21/barr-says-solarwinds-hack-certainly-appears-to-be-the-russians-.html). *CNBC*. NBCUniversal News Group. Retrieved December 22, 2020.

31. Sanger, David E.; Rappeport, Alan (December 22, 2020). "Treasury Department's Senior Leaders Were Targeted by Hacking" (https://www.nytimes.com/2020/12/21/us/politics/russia-hack-treasury.html). *New York Times*.
32. "US: Hack of Federal Agencies 'Likely Russian in Origin' " (https://www.securityweek.com/us-hack-federal-agencies-likely-russian-origin). *SecurityWeek*. Associated Press. January 5, 2021. Retrieved January 13, 2021.
33. Goodin, Dan (January 6, 2021). "Bucking Trump, NSA and FBI say Russia was "likely" behind SolarWinds hack" (https://arstechnica.com/tech-policy/2021/01/feds-say-that-russia-was-likely-behind-months-long-hack-of-us-agencies/). *Ars Technica*.
34. "Russians are 'likely' perpetrators of US government hack, official report says" (https://www.theguardian.com/technology/2021/jan/05/russians-likely-perpetrators-us-government-hack). *the Guardian*. January 5, 2021. Retrieved January 13, 2021.
35. "U.S. Agencies and Companies Secure Networks After Huge Hack" (https://time.com/5921684/us-computer-networks-hack-russia/). *Time*. December 15, 2020. Archived (https://web.archive.org/web/20201216052021/https://time.com/5921684/us-computer-networks-hack-russia/) from the original on December 16, 2020. Retrieved December 16, 2020.
36. Richards, Zoë (December 15, 2020). "Report: Massive Russian Hack Effort Breached DHS, State Department And NIH" (https://talkingpointsmemo.com/news/report-massive-russian-hack-effort-breached-dhs-state-department-and-nih). *Talking Points Memo*. Archived (https://web.archive.org/web/20201215155700/https://talkingpointsmemo.com/news/report-massive-russian-hack-effort-breached-dhs-state-department-and-nih) from the original on December 15, 2020. Retrieved December 17, 2020.
37. Cimpanu, Catalin. "SEC filings: SolarWinds says 18,000 customers were impacted by recent hack" (https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/). ZDNet. Archived (https://web.archive.org/web/20201215101510/https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/) from the original on December 15, 2020. Retrieved December 15, 2020.
38. Jankowicz, Mia; Davis, Charles. "These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia" (https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12). *Business Insider*. Archived (https://web.archive.org/web/20201216135705/https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12) from the original on December 16, 2020. Retrieved December 16, 2020.
39. "SolarWinds: The Hunt to Figure Out Who Was Breached" (https://www.bankinfosecurity.com/solarwinds-hunt-to-figure-out-who-was-breached-a-15608). *bankinfosecurity.com*. Archived (https://web.archive.org/web/20201216172413/https://www.bankinfosecurity.com/solarwinds-hunt-to-figure-out-who-was-breached-a-15608) from the original on December 16, 2020. Retrieved December 17, 2020.
40. "Hack may have exposed deep US secrets; damage yet unknown" (https://www.independent.co.uk/news/hack-may-have-exposed-deep-us-secrets-damage-yet-unknown-hackers-hackers-donald-trump-government-us-b1774648.html). *The Independent*. December 15, 2020. Archived (https://web.archive.org/web/20201218062211/https://www.independent.co.uk/news/hack-may-have-exposed-deep-us-secrets-damage-yet-unknown-hackers-hackers-donald-trump-government-us-b1774648.html) from the original on December 18, 2020. Retrieved December 16, 2020.
41. "US agencies, companies secure networks after huge hack" (https://apnews.com/article/us-agencies-hacked-global-cyberspying-328b4936f2535418b27cb90afa858489). *AP NEWS*. December 14, 2020. Archived (https://web.archive.org/web/20201218062233/https://apnews.com/article/us-agencies-hacked-global-cyberspying-328b4936f2535418b27cb90afa858489) from the original on December 18, 2020. Retrieved December 16, 2020.
42. "Deep US institutional secrets may have been exposed in hack blamed on Russia" (https://www.theguardian.com/technology/2020/dec/16/us-institutional-secrets-exposed-hack-russia). *The Guardian*. December 16, 2020. Archived (https://web.archive.org/web/20201217173005/https://www.theguardian.com/technology/2020/dec/16/us-institutional-secrets-exposed-hack-russia) from the original on December 17, 2020. Retrieved December 17, 2020.
43. "Emergency Directive 21-01" (https://cyber.dhs.gov/ed/21-01/). *cyber.dhs.gov*. Archived (https://web.archive.org/web/20201215153142/https://cyber.dhs.gov/ed/21-01/) from the original on December 15, 2020. Retrieved December 15, 2020.

44. "How Russian hackers infiltrated the US government for months without being spotted" (https://www.technologyreview.com/2020/12/15/1014462/how-russian-hackers-infiltrated-the-us-government-for-months-without-being-spotted/). *MIT Technology Review*. Archived (https://web.archive.org/web/20201218062222/https://www.technologyreview.com/2020/12/15/1014462/how-russian-hackers-infiltrated-the-us-government-for-months-without-being-spotted/) from the original on December 18, 2020. Retrieved December 17, 2020.
45. "SolarWinds advanced cyberattack: What happened and what to do now" (https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/). *Malwarebytes Labs*. December 14, 2020. Archived (https://web.archive.org/web/20201216164030/https://blog.malwarebytes.com/threat-analysis/2020/12/advanced-cyber-attack-hits-private-and-public-sector-via-supply-chain-software-update/) from the original on December 16, 2020. Retrieved December 16, 2020.
46. "Overview of Recent Sunburst Targeted Attacks" (https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html). *Trend Micro*. Archived (https://web.archive.org/web/20201215170319/https://www.trendmicro.com/en_us/research/20/l/overview-of-recent-sunburst-targeted-attacks.html) from the original on December 15, 2020. Retrieved December 18, 2020.
47. "Hackers' Monthslong Head Start Hamstrings Probe of U.S. Breach" (https://www.bloomberg.com/news/articles/2020-12-18/hackers-lurking-in-networks-for-months-snarl-solarwinds-probes). Bloomberg. December 18, 2020. Retrieved December 18, 2020.
48. "Hacked networks will need to be burned 'down to the ground' " (https://www.independent.co.uk/news/hacked-networks-will-need-to-be-burned-down-to-the-ground-hackers-fireeye-us-networks-networks-b1776430.html). *The Independent*. December 18, 2020.
49. Satter, Raphael (December 24, 2020). "Experts who wrestled with SolarWinds hackers say cleanup could take months - or longer" (https://uk.reuters.com/article/us-global-cyber-usa-solarwinds-idUSKBN28Y1K3) – via uk.reuters.com.
50. "Biden taps trusted figures to lead US climate fight; FDA says Moderna vaccine is highly protective; SolarWinds hack fallout spreads" (https://www.pri.org/stories/2020-12-16/biden-taps-trusted-figures-lead-us-climate-fight-fda-says-moderna-vaccine-highly). *The World from PRX*. Archived (https://web.archive.org/web/20201216171836/https://www.pri.org/stories/2020-12-16/biden-taps-trusted-figures-lead-us-climate-fight-fda-says-moderna-vaccine-highly) from the original on December 16, 2020. Retrieved December 17, 2020.
51. "What Matters: The suspected Russian hack of the US government, explained" (https://www.msn.com/en-us/news/politics/what-matters-the-suspected-russian-hack-of-the-us-government-explained/ar-BB1bXqYK). MSN. Archived (https://web.archive.org/web/20201216015012/http://www.msn.com/en-us/news/politics/what-matters-the-suspected-russian-hack-of-the-us-government-explained/ar-BB1bXqYK) from the original on December 16, 2020. Retrieved December 17, 2020.
52. Geller, Eric; Rayasam, Renuka; Ward, Myah (December 17, 2020). "The Big Hack: What we know, what we don't" (https://www.politico.com/newsletters/politico-nightly/2020/12/17/the-big-hack-what-we-know-what-we-dont-491184). *Politico*. Retrieved December 19, 2020.
53. Bing, Christopher (December 13, 2020). "EXCLUSIVE-U.S. Treasury breached by hackers backed by foreign government – sources" (https://www.reuters.com/article/usa-cyber-amazoncom-idUSL1N2IT0HS). *Reuters*. Archived (https://web.archive.org/web/20201215134315/https://www.reuters.com/article/usa-cyber-amazoncom-idUSL1N2IT0HS) from the original on December 15, 2020. Retrieved December 18, 2020.
54. Nakashima, Ellen; Timberg, Craig. "DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign" (https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html). *The Washington Post*. Archived (https://web.archive.org/web/20201216082355/https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html) from the original on December 16, 2020. Retrieved December 17, 2020.
55. Cohen, Zachary; Salama, Vivian; Fung, Brian. "US officials scramble to deal with suspected Russian hack of government agencies" (https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html). CNN. Archived (https://web.archive.org/web/20201216041022/https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html) from the original on December 16, 2020. Retrieved December 18, 2020.

56. Cimpanu, Catalin. "Microsoft to quarantine SolarWinds apps linked to recent hack" (https://www.zdnet.com/index.php/category/2381/index.php/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/). ZDNet. Archived (https://web.archive.org/web/20201218062252/https://www.zdnet.com/index.php/category/2381/index.php/article/microsoft-to-quarantine-solarwinds-apps-linked-to-recent-hack-starting-tomorrow/) from the original on December 18, 2020. Retrieved December 17, 2020.
57. "US nuclear agency a target in 'massive' cyber attack on federal government by suspected Russian hackers" (https://news.sky.com/story/biden-to-make-cybersecurity-a-top-priority-after-massive-hack-attack-on-the-us-government-12165958). Sky News.
58. "The SolarWinds cyberattack: The hack, the victims, and what we know" (https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/). *BleepingComputer*.
59. Dozier, Kimberly (December 18, 2020). "U.S. Cyber Experts Scramble to Assess the Scope of the 'Hack of a Decade' " (https://time.com/5923056/cyber-attack-us-government/). *Time*. Retrieved December 19, 2020.
60. "As Understanding of Russian Hacking Grows, So Does Alarm" (https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html). *The New York Times*. January 2, 2021. Retrieved January 13, 2021.
61. Stubbs, Jack; Satter, Raphael; Menn, Joseph (December 15, 2020). "U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack" (https://www.reuters.com/article/uk-global-cyber-idUKKBN28O1KN). *Reuters*. Archived (https://web.archive.org/web/20201215132412/https://www.reuters.com/article/uk-global-cyber-idUKKBN28O1KN) from the original on December 15, 2020. Retrieved December 18, 2020.
62. "Nuclear weapons agency breached amid massive cyber onslaught" (https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855). *Politico*. Archived (https://web.archive.org/web/20201217222530/https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855) from the original on December 17, 2020. Retrieved December 17, 2020.
63. "Nuclear Weapons Agency Hacked in Widening Cyberattack – Report" (https://threatpost.com/nuclear-weapons-agency-hacked-cyberattack/162387/). *threatpost.com*. Archived (https://web.archive.org/web/20201218051458/https://threatpost.com/nuclear-weapons-agency-hacked-cyberattack/162387/) from the original on December 18, 2020. Retrieved December 17, 2020.
64. Goodin, Dan (December 17, 2020). "Microsoft is reportedly added to the growing list of victims in SolarWinds hack" (https://arstechnica.com/information-technology/2020/12/microsoft-is-reportedly-added-to-the-growing-list-of-victims-in-solarwinds-hack/). *Ars Technica*. Archived (https://web.archive.org/web/20201218062247/https://arstechnica.com/information-technology/2020/12/microsoft-is-reportedly-added-to-the-growing-list-of-victims-in-solarwinds-hack/) from the original on December 18, 2020. Retrieved December 18, 2020.
65. "Department of Energy says it was hacked in suspected Russian campaign" (https://www.nbcnews.com/news/us-news/department-energy-says-it-was-hacked-suspected-russian-campaign-n1251630). NBC News. Archived (https://web.archive.org/web/20201218062228/https://www.nbcnews.com/news/us-news/department-energy-says-it-was-hacked-suspected-russian-campaign-n1251630) from the original on December 18, 2020. Retrieved December 18, 2020.
66. "Security experts warn of long-term risk tied to Energy Department breach" (https://www.scmagazine.com/home/government/security-experts-warn-of-long-term-risk-tied-to-energy-department-breach/). *SC Media*. December 21, 2020.
67. "Microsoft Says Russian Hackers Viewed Some of Its Source Code" (https://www.nytimes.com/2020/12/31/technology/microsoft-russia-hack.html). *The New York Times*. December 31, 2020. Retrieved January 13, 2021.
68. Paul, Kari (January 6, 2021). "DoJ confirms email accounts breached by SolarWinds hackers" (https://www.theguardian.com/technology/2021/jan/06/doj-email-systems-solarwinds-hackers). *the Guardian*. Retrieved January 13, 2021.
69. "Justice Department Says It's Been Affected by Russian Hack" (https://www.securityweek.com/justice-department-says-its-been-affected-russian-hack). *SecurityWeek*. Associated Press. January 6, 2021. Retrieved January 11, 2021.
70. Claburn, Thomas (January 7, 2021). "JetBrains' build automation software eyed as possible enabler of SolarWinds hack" (https://www.theregister.com/2021/01/07/jetbrains_solarwinds_accusation/). *The Register*. Retrieved January 12, 2021.
71. "Widely Used Software Company May Be Entry Point for Huge U.S. Hacking" (https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html). *The New York Times*. January 6, 2021. Retrieved January 12, 2021.

72. Gatlan, Sergiu (January 6, 2021). "SolarWinds hackers had access to over 3,000 US DOJ email accounts" (https://www.bleepingcomputer.com/news/security/solarwinds-hackers-had-access-to-over-3-000-us-doj-email-accounts/). *BleepingComputer*. Retrieved January 13, 2021.
73. Volz, Dustin; McMillan, Robert (January 7, 2021). "Federal Judiciary's Systems Likely Breached in SolarWinds Hack" (https://www.wsj.com/articles/federal-judiciarys-systems-likely-breached-in-solarwinds-hack-11610040175). *WSJ*. Retrieved January 12, 2021.
74. "SolarWinds Hack Compromises U.S. Courts Electronic Filings (1)" (https://news.bloomberglaw.com/us-law-week/cyberbreach-compromises-u-s-courts-electronic-filings). *news.bloomberglaw.com*.
75. Miller, Maggie (January 7, 2021). "Federal judiciary likely compromised as part of SolarWinds hack" (https://thehill.com/policy/cybersecurity/533177-federal-judiciary-likely-compromised-as-part-of-solarwinds-hack). *TheHill*. Retrieved January 12, 2021.
76. Krebs, Brian (January 7, 2021). "Sealed U.S. Court Records Exposed in SolarWinds Breach" (https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/). *Krebs on Security*. Retrieved January 12, 2021.
77. Starks, Tim (January 7, 2021). "Federal courts are latest apparent victim of SolarWinds hack" (https://www.cyberscoop.com/solarwinds-hack-us-courts/). *CyberScoop*. Retrieved January 12, 2021.
78. Clark, Mitchell (January 7, 2021). "Federal courts go low-tech for sensitive documents following SolarWinds hack" (https://www.theverge.com/2021/1/7/22219275/federal-judiciary-system-further-securing-sealed-documents-solarwinds-hack). *The Verge*. Retrieved January 12, 2021.
79. Kovacs, Eduard (January 8, 2021). "Probe Launched Into Impact of SolarWinds Breach on Federal Courts" (https://www.securityweek.com/probe-launched-impact-solarwinds-breach-federal-courts). *SecurityWeek*. Retrieved January 12, 2021.
80. Gatlan, Sergiu (January 7, 2021). "US Judiciary adds safeguards after potential breach in SolarWinds hack" (https://www.bleepingcomputer.com/news/security/us-judiciary-adds-safeguards-after-potential-breach-in-solarwinds-hack/). *BleepingComputer*. Retrieved January 13, 2021.
81. Corfield, Gareth (January 8, 2021). "US courts system fears SolarWinds snafu could have let state hackers poke about in sealed case documents" (https://www.theregister.com/2021/01/08/solarwinds_court_docs/). *The Register*. Retrieved January 13, 2021.
82. Stubbs, Jack; McNeill, Ryan (December 18, 2020). "SolarWinds hackers broke into U.S. cable firm and Arizona county, web records show" (https://uk.reuters.com/article/us-usa-cyber-idUKKBN28S2B9). *Reuters*.
83. Stubbs, Jack (December 19, 2020). "Hackers' broad attack sets cyber experts worldwide scrambling to defend networks" (https://www.reuters.com/article/us-global-cyber/hackers-broad-attack-sets-cyber-experts-worldwide-scrambling-to-defend-networks-idUSKBN28S2V3). Reuters.
84. Volz, Kevin Poulsen, Robert McMillan and Dustin (December 21, 2020). "WSJ News Exclusive | SolarWinds Hack Victims: From Tech Companies to a Hospital and University" (https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402) – via www.wsj.com.
85. "Cisco Latest Victim of Russian Cyber-Attack Using SolarWinds" (https://www.bloomberg.com/news/articles/2020-12-18/cisco-latest-victim-of-russian-cyber-attack-using-solarwinds). Bloomberg. December 18, 2020. Retrieved December 19, 2020.
86. "SolarWinds Supply Chain Hit: Victims Include Cisco, Intel" (https://www.bankinfosecurity.com/solarwinds-orion-campaign-victims-include-cisco-intel-a-15619). Bankinfosecurity.com. December 17, 2020. Retrieved December 19, 2020.
87. Brewster, Thomas. "SolarWinds Hack: Cisco And Equifax Amongst Corporate Giants Finding Malware... But No Sign Of Russian Spies" (https://www.forbes.com/sites/thomasbrewster/2020/12/19/solarwinds-hack-cisco-and-equifax-amongst-corporate-giants-finding-malware-but-no-sign-of-russian-spies/). *Forbes*.
88. Schmaltz, Trey (December 18, 2020). "La. retirement system warned it may have been target of Russian hack; Cox also investigating" (https://www.wbrz.com/news/la-retirement-system-warned-it-may-have-been-target-of-russian-hack-cox-also-investigating). WBRZ.
89. "Four security vendors disclose SolarWinds-related incidents" (https://www.zdnet.com/article/four-security-vendors-disclose-solarwinds-related-incidents/). *U.S.* January 26, 2021. Retrieved February 1, 2021. "This week, four new cyber-security vendors -- Mimecast, Qualys, Palo Alto Networks, and Fidelis -- have added their names to the list of companies that have installed trojanized versions of the SolarWinds Orion app."
90. https://www.businessinsider.com/cybersecurity-firm-malwarebytes-was-breached-by-solarwinds-hackers-2021-1

91. https://www.bloomberg.com/news/articles/2021-01-19/suspected-russian-hackers-targeted-security-firm-malwarebytes
92. https://www.reuters.com/article/us-global-cyber-malwarebytes/malwarebytes-says-some-of-its-emails-were-breached-by-solarwinds-hackers-idUSKBN29O2CB
93. Menn, Joseph (December 18, 2020). "Exclusive: Microsoft breached in suspected Russian hack using SolarWinds – sources" (https://www.reuters.com/article/global-cyber-microsoft-exclusive-int-idUSKBN28R3BW). *Reuters*. Archived (https://web.archive.org/web/20201218062230/https://www.reuters.com/article/global-cyber-microsoft-exclusive-int-idUSKBN28R3BW) from the original on December 18, 2020. Retrieved December 18, 2020.
94. Cimpanu, Catalin. "Microsoft confirms it was also breached in recent SolarWinds supply chain hack" (https://www.zdnet.com/article/microsoft-was-also-breached-in-recent-solarwinds-supply-chain-hack-report/). ZDNet. Archived (https://web.archive.org/web/20201218042137/https://www.zdnet.com/article/microsoft-was-also-breached-in-recent-solarwinds-supply-chain-hack-report/) from the original on December 18, 2020. Retrieved December 18, 2020.
95. Bass, Dina. "Microsoft Says Its Systems Were Exposed to SolarWinds Hack" (https://www.bloomberg.com/news/articles/2020-12-18/microsoft-says-its-systems-were-exposed-in-solarwinds-hack). Bloomberg L.P. Archived (https://web.archive.org/web/20201218062223/https://www.bloomberg.com/news/articles/2020-12-18/microsoft-says-its-systems-were-exposed-in-solarwinds-hack) from the original on December 18, 2020. Retrieved December 18, 2020.
96. Novet, Jordan (December 17, 2020). "Microsoft was reportedly swept up in SolarWinds hack" (https://www.cnbc.com/2020/12/17/microsoft-shares-fall-after-report-it-was-swept-up-in-solarwinds-hack.html). CNBC. Archived (https://web.archive.org/web/20201218062249/https://www.cnbc.com/2020/12/17/microsoft-shares-fall-after-report-it-was-swept-up-in-solarwinds-hack.html) from the original on December 18, 2020. Retrieved December 18, 2020.
97. Thomson, Iain. "US nuke agency hacked by suspected Russian SolarWinds spies, Microsoft also installed backdoor" (https://www.theregister.com/2020/12/18/solarwinds_nnsa_microsoft_cisa/). *The Register*.
98. "Microsoft acknowledges it was hacked via SolarWinds exploit" (https://www.slashgear.com/microsoft-acknowledges-it-was-hacked-via-solarwinds-exploit-18651720/). *SlashGear*. December 18, 2020.
99. Robles, C. J. (December 17, 2020). "Microsoft, SolarWinds Hacking Can Be a National Security Issue?" (https://www.techtimes.com/articles/255184/20201217/microsoft-solarwinds-corp-attackers-remove-evidences-biggest-hack-decade.htm). *Tech Times*.
00. "SolarWinds hackers accessed Microsoft source code, the company says" (https://web.archive.org/web/20210101155157/https://www.cnbc.com/2021/01/01/solarwinds-hackers-accessed-microsoft-source-code-the-company-says.html). *CNBC*. January 1, 2021. Archived from the original (https://www.cnbc.com/2021/01/01/solarwinds-hackers-accessed-microsoft-source-code-the-company-says.html) on January 1, 2021. Retrieved January 13, 2021. "Modifying source code — which Microsoft said the hackers did not do — could have potentially disastrous consequences given the ubiquity of Microsoft products, which include the Office productivity suite and the Windows operating system. But experts said that even just being able to review the code could offer hackers insight that might help them subvert Microsoft products or services."
01. "Here's why it's so dangerous that SolarWinds hackers accessed Microsoft's source code" (https://bgr.com/2021/01/01/solarwinds-hack-microsoft-source-code-breach/). *BGR*. January 1, 2021. Retrieved January 13, 2021. "More than two weeks after the hacks, Microsoft disclosed that the attackers were able to access a critical piece of software, the source code from one or more undisclosed products. Microsoft explained in a blog post that the hackers were not able to modify the source code. But even just a glance at a source code from a company like Microsoft might be enough for hackers to develop new attacks that compromise other Microsoft products. ... Microsoft's blog post is meant to reassure governments and customers, but the fact remains that hackers might be in possession of the kind of secrets they shouldn't have access to. Time will tell if gaining access to Microsoft's source code will allow the same team of attackers to create even more sophisticated hacks."
02. "Software Giant Admits That SolarWinds Hackers Viewed Microsoft Source Code" (https://www.cpomagazine.com/cyber-security/software-giant-admits-that-solarwinds-hackers-viewed-microsoft-source-code/). *CPO Magazine*. January 7, 2021. Retrieved January 13, 2021. "Microsoft disclosed [that] the hacking group behind the SolarWinds attack also viewed Microsoft source code for unnamed products. ... Microsoft, however, downplayed the breach, saying that the security of its products does not depend on the secrecy of its source code. Contrarily, Microsoft source code for most high-profile products remains to be among the most jealously guarded corporate secrets, shared only with a few trusted customers and governments."

03. Stanley, Alyse (December 31, 2020). "Microsoft Says SolarWinds Hackers Also Broke Into Company's Source Code" (https://gizmodo.com/microsoft-says-solarwinds-hackers-also-broke-into-its-s-1845974783). *Gizmodo*. Retrieved January 13, 2021. "While hackers may not have been able to change Microsoft's source code, even just sneaking a peek at the company's secret sauce could have disastrous consequences. Bad actors could use that kind of insight into the inner workings of Microsoft's services to help them circumvent its security measures in future attacks. The hackers essentially scored blueprints on how to potentially hack Microsoft products."
04. Bradley, Susan (January 4, 2021). "SolarWinds, Solorigate, and what it means for Windows updates" (https://www.computerworld.com/article/3602549/solarwinds-solorigate-and-what-it-means-for-windows-updates.html). *Computerworld*. Retrieved January 13, 2021. "Microsoft investigated further and found that while the attackers were not able to inject themselves into Microsoft's ADFS/SAML infrastructure, 'one account had been used to view source code in a number of source code repositories. The account did not have permissions to modify any code or engineering systems and our investigation further confirmed no changes were made.' This is not the first time Microsoft's source code has been attacked or leaked to the web. In 2004, 30,000 files from Windows NT to Windows 2000 leaked onto the web via a third party. Windows XP reportedly leaked online last year."
05. Satter, Raphael (December 31, 2020). "Microsoft says SolarWinds hackers were able to view its source code but didn't have the ability to modify it" (https://www.businessinsider.com/solarwinds-hackers-were-able-to-access-microsoft-source-code-microsoft-blog-post-2020-12). *Business Insider*. Retrieved January 13, 2021. "Ronen Slavin, [chief technology officer at source code protection company Cycode], said a key unanswered question was which source code repositories were accessed. ... Slavin said he was also worried by the possibility that the SolarWinds hackers were poring over Microsoft's source code as prelude for something more ambitious. 'To me the biggest question is, "Was this recon for the next big operation?"' he said."
06. Spring, Tom (January 12, 2021). "Critical Microsoft Defender Bug Actively Exploited; Patch Tuesday Offers 83 Fixes" (https://threatpost.com/critical-microsoft-defender-bug-exploited/162992/). *Threatpost*. Retrieved January 13, 2021. "Last month, Microsoft said state-sponsored hackers had compromised its internal network and leveraged additional Microsoft products to conduct further attacks."
07. "Email security firm Mimecast says hackers hijacked its products to spy on customers" (https://web.archive.org/web/20210112194050/https://www.reuters.com/article/us-global-cyber-mimecast-idUSKBN29H22K). *U.S.* January 12, 2021. Archived from the original (https://www.reuters.com/article/us-global-cyber-mimecast-idUSKBN29H22K) on January 12, 2021. Retrieved January 13, 2021. "Three cybersecurity investigators, who spoke on condition of anonymity to discuss details of an ongoing probe, told Reuters they suspected the hackers who compromised Mimecast were the same group that broke into U.S. software maker SolarWinds and a host of sensitive U.S. government agencies."
08. "Mimecast Discloses Certificate Incident Possibly Related to SolarWinds Hack" (https://www.securityweek.com/mimecast-discloses-certificate-incident-possibly-related-solarwinds-hack). *SecurityWeek.Com*. January 13, 2021. Retrieved January 13, 2021. "According to Mimecast, it learned from Microsoft that hackers had compromised a certificate used to authenticate Mimecast Continuity Monitor, Internal Email Protect (IEP), and Sync and Recover products with Microsoft 365 Exchange Web Services. ... The company has not shared any details about the attacks abusing the compromised certificate, but some experts have speculated that the certificate may have allowed the hackers to intercept Mimecast customers' communications. ... According to Reuters, people with knowledge of the situation believe this incident may be related to the recently disclosed supply chain attack involving Texas-based IT management solutions provider SolarWinds."
09. Seals, Tara (January 12, 2021). "Mimecast Certificate Hacked in Microsoft Email Supply-Chain Attack" (https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/). *Threatpost*. Retrieved January 13, 2021. "Mimecast provides email security services that customers can apply to their Microsoft 365 accounts by establishing a connection to Mimecast's servers... A compromise means that cyberattackers could take over the connection, though which inbound and outbound mail flows, researchers said. It would be possible to intercept that traffic, or possibly to infiltrate customers' Microsoft 365 Exchange Web Services and steal information. 'The attack against Mimecast and their secure connection to Microsoft's Office 365 infrastructure appears to be the work of the same sophisticated attackers that breached SolarWinds and multiple government agencies,' Saryu Nayyar, CEO at Gurucul, said via email."
10. "SolarWinds attackers suspected in Microsoft authentication compromise" (https://www.scmagazine.com/home/email-security/solarwinds-attackers-suspected-in-microsoft-authentication-compromise/). *SC Media*. January 12, 2021. Retrieved January 13, 2021.

11. Spadafora, Anthony (January 12, 2021). "Mimecast may also have been a victim of the SolarWinds hack campaign" (https://www.techradar.com/news/mimecast-may-also-have-been-a-victim-of-the-solarwinds-hack-campaign). *TechRadar*. Retrieved January 13, 2021. "The reason that Mimecast may have been attacked by the same threat actor behind the SolarWinds hack is due to the fact that these hackers often add authentication tokens and credentials to Microsoft Active Directory domain accounts in order to maintain persistence on a network and to achieve privilege escalation."
12. McMillan, Robert (January 13, 2021). "SolarWinds Hackers' Attack on Email Security Company Raises New Red Flags" (https://www.wsj.com/articles/solarwinds-hackers-attack-on-email-security-company-raises-new-red-flags-11610510375). *WSJ*. Retrieved January 13, 2021. "The Mimecast hackers used tools and techniques that link them to the hackers who broke into Austin, Texas-based SolarWinds Corp., according to people familiar with the investigation. The link to the SolarWinds hackers was reported earlier by Reuters."
13. "fireeye/red_team_tool_countermeasures" (https://github.com/fireeye/red_team_tool_countermeasures). *GitHub*. Archived (https://web.archive.org/web/20201216112625/https://github.com/fireeye/red_team_tool_countermeasures) from the original on December 16, 2020. Retrieved December 17, 2020.
14. "Microsoft to quarantine compromised SolarWinds binaries tomorrow" (https://www.bleepingcomputer.com/news/security/microsoft-to-quarantine-compromised-solarwinds-binaries-tomorrow/). *BleepingComputer*. Archived (https://web.archive.org/web/20201216154827/https://www.bleepingcomputer.com/news/security/microsoft-to-quarantine-compromised-solarwinds-binaries-tomorrow/) from the original on December 16, 2020. Retrieved December 17, 2020.
15. "Grid regulator warns utilities of risk of SolarWinds backdoor, asks how exposed they are" (https://www.cyberscoop.com/nerc-alert-solarwinds-grid-russia/). *CyberScoop*. December 23, 2020.
16. Brandom, Russell (December 15, 2020). "SolarWinds hides list of high-profile customers after devastating hack" (https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised). *The Verge*. Archived (https://web.archive.org/web/20201216093459/https://www.theverge.com/2020/12/15/22176053/solarwinds-hack-client-list-russia-orion-it-compromised) from the original on December 16, 2020. Retrieved December 16, 2020.
17. Varghese, Sam. "iTWire - Backdoored Orion binary still available on SolarWinds website" (https://www.itwire.com/security/backdoored-orion-binary-still-available-on-solarwinds-website.html). *www.itwire.com*.
18. "Class Action Lawsuit Filed Against SolarWinds Over Hack" (https://www.securityweek.com/class-action-lawsuit-filed-against-solarwinds-over-hack). *SecurityWeek.Com*. January 6, 2021. Retrieved January 13, 2021.
19. McCarthy, Kieren (January 5, 2021). "Ah, right on time: Hacker-slammed SolarWinds sued by angry shareholders" (https://www.theregister.com/2021/01/05/solarwinds_sued/). *The Register*. Retrieved January 13, 2021.
20. "SolarWinds Taps Firm Started by Ex-CISA Chief Chris Krebs, Former Facebook CSO Alex Stamos" (https://www.securityweek.com/solarwinds-taps-firm-launched-cisa-chief-chris-krebs-former-facebook-cso-alex-stamos). *SecurityWeek.Com*. January 8, 2021. Retrieved January 13, 2021.
21. Vaughan-Nichols, Steven J. (January 14, 2021). "SolarWinds defense: How to stop similar attacks" (https://www.zdnet.com/article/solarwinds-defense-how-to-stop-similar-attacks/). *ZDNet*. Retrieved January 15, 2021.
22. "Potentially major hack of government agencies disclosed" (https://www.cbsnews.com/news/solarwinds-orion-hack-government-agencies-treasury-fireeye/). CBS News. Archived (https://web.archive.org/web/20201215232830/https://www.cbsnews.com/news/solarwinds-orion-hack-government-agencies-treasury-fireeye/) from the original on December 15, 2020. Retrieved December 16, 2020.
23. "US government agencies, including Treasury, hacked; Russia possible culprit" (https://abc11.com/treasury-hack-cyber-attack-on-russia-today/8753611/). WTVD. December 14, 2020. Archived (https://web.archive.org/web/20201214025001/https://abc11.com/treasury-hack-cyber-attack-on-russia-today/8753611/) from the original on December 14, 2020. Retrieved December 15, 2020.
24. Geller, Eric. " 'Massively disruptive' cyber crisis engulfs multiple agencies" (https://www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376). *Politico*. Archived (https://web.archive.org/web/20201216092339/https://www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376) from the original on December 16, 2020. Retrieved December 16, 2020.
25. "US vows 'swift action' if defense networks hit by alleged Russia hack" (https://www.newsweek.com/us-swift-action-defense-networks-alleged-russia-hack-1554693). *Newsweek*. December 14, 2020. Archived (https://web.archive.org/web/20201216053800/https://www.newsweek.com/us-swift-action-defense-networks-alleged-russia-hack-1554693) from the original on December 16, 2020. Retrieved December 16, 2020.

26. "FBI, CISA, ODNI Describe Response to SolarWinds Attack" (https://www.securityweek.com/fbi-cisa-odni-describe-response-solarwinds-attack). *SecurityWeek.com*. Archived (https://web.archive.org/web/20201218062236/https://www.securityweek.com/fbi-cisa-odni-describe-response-solarwinds-attack) from the original on December 18, 2020. Retrieved December 18, 2020.
27. Satter, Raphael (December 24, 2020). "U.S. cyber agency says SolarWinds hackers are 'impacting' state, local governments" (https://uk.reuters.com/article/us-global-cyber-usa-idUKKBN28Y09L) – via uk.reuters.com.
28. Daugherty, Alex (December 18, 2020). "Intel chairman Rubio says 'America must retaliate' after massive cyber hack" (https://www.miamiherald.com/news/politics-government/article247946080.html). *Miami Herald*.
29. Dwyer, Colin (December 19, 2020). "Pompeo Says Russia 'Pretty Clearly' Behind Cyberattack, Prompting Pushback From Trump" (https://www.npr.org/2020/12/19/948318197/pompeo-russia-pretty-clearly-behind-massive-solarwinds-cyberattack). *NPR*. Retrieved December 20, 2020.
30. "Lawmakers want more transparency on SolarWinds breach from State, VA" (https://www.cyberscoop.com/menendez-blumenthal-state-va-solarwinds/). *CyberScoop*. December 23, 2020.
31. "Veterans Affairs Officials Inexplicably Blow Off Briefing on SolarWinds Hack" (https://gizmodo.com/veterans-affairs-officials-inexplicably-blow-off-briefi-1845946394). *Gizmodo*.
32. "Hacking campaign targeted US energy, treasury and commerce agencies" (https://www.theguardian.com/technology/2020/dec/17/us-government-cyber-attack-hack-russia). *The Guardian*. December 17, 2020. Archived (https://web.archive.org/web/20201217192805/https://www.theguardian.com/technology/2020/dec/17/us-government-cyber-attack-hack-russia) from the original on December 17, 2020. Retrieved December 18, 2020.
33. Jill Colvin & Matthew Lee, Trump downplays Russia in first comments on hacking campaign (https://apnews.com/article/donald-trump-politics-mark-levin-coronavirus-pandemic-hacking-6080f156125a4a46edef2a6dcf826611), Associated Press (December 19, 2020).
34. Justin Sink, Trump Downplays Huge Hack Tied to Russia, Suggests China (https://www.bloomberg.com/news/articles/2020-12-19/trump-downplays-massive-hack-floats-china-as-possible-culprit), Bloomberg News (December 19, 2020).
35. Canales, Katie (December 19, 2020). "Former US cybersecurity chief Chris Krebs warned not to 'conflate' voting system security with SolarWinds hack despite Trump's claim" (https://www.businessinsider.com/krebs-do-not-conflate-voting-security-solarwinds-hack-2020-12). *Business Insider*. Retrieved December 20, 2020.
36. Bing, Christopher; Landay, Jonathan (December 19, 2020). "Trump downplays impact of massive hacking, questions Russia involvement" (https://uk.reuters.com/article/uk-u-s-cyber-breach/trump-downplays-impact-of-massive-hacking-questions-russia-involvement-idUKKBN28T0QI). Reuters.
37. "Russia Could Fake Government Emails After SolarWinds Hack: Ex-Trump Adviser Thomas Bossert" (https://www.msn.com/en-us/news/politics/russia-could-fake-government-emails-after-solarwinds-hack-ex-trump-adviser-thomas-bossert/ar-BB1c0qKx). MSN. Archived (https://web.archive.org/web/20201218062228/https://www.msn.com/en-us/news/politics/russia-could-fake-government-emails-after-solarwinds-hack-ex-trump-adviser-thomas-bossert/ar-BB1c0qKx) from the original on December 18, 2020. Retrieved December 17, 2020.
38. Pierce, Charles P. (December 15, 2020). "Somebody Was Asleep at the Switch Here" (https://www.esquire.com/news-politics/politics/a34978841/russia-hack-us-government-systems-trump-administration/). *Esquire*. Archived (https://web.archive.org/web/20201217130024/https://www.esquire.com/news-politics/politics/a34978841/russia-hack-us-government-systems-trump-administration/) from the original on December 17, 2020. Retrieved December 17, 2020.
39. 'They potentially have the capacity to cripple us': Romney raises alarm about cyberattack tied to Russia (https://www.usatoday.com/story/news/politics/2020/12/20/mitt-romney-says-trumps-comments-cyber-attack-disappointing/3981759001/), *USA Today* (December 20, 2020).
40. Satter, Raphael (December 20, 2020). "Biden chief of staff says hack response will go beyond 'just sanctions' " (https://www.reuters.com/article/usa-cyber-breach-idUSKBN28U0IK). *Reuters*. Retrieved December 20, 2020.
41. "Biden Says Hack of U.S. Shows Trump Failed at Cybersecurity" (https://www.bloomberg.com/news/articles/2020-12-22/biden-says-hack-of-u-s-shows-trump-failed-at-cyber-security). December 22, 2020 – via www.bloomberg.com.
42. Lewis, Simon (December 23, 2020). "Trump must blame Russia for cyber attack on U.S., Biden says" (https://www.reuters.com/article/us-usa-biden-idUKKBN28W1ZF). *Reuters*.

43. "Biden to Restore Homeland Security and Cybersecurity Aides to Senior White House Posts" (https://www.nytimes.com/2021/01/13/us/politics/biden-homeland-security-cybersecurity.html). *The New York Times*. January 13, 2021. Retrieved January 13, 2021. "President-elect Joseph R. Biden Jr., facing the rise of domestic terrorism and a crippling cyberattack from Russia, is elevating two White House posts that all but disappeared in the Trump administration: a homeland security adviser to manage matters as varied as extremism, pandemics and natural disasters, and the first deputy national security adviser for cyber and emerging technology. ... Mr. Trump dismantled the National Security Council's pandemic preparedness office, and while he had an active cyberteam at the beginning of his term, it languished. 'It's disturbing to be in a transition moment when there really aren't counterparts for that transition to be handed off,' Ms. Sherwood-Randall said. ... The SolarWinds hacking, named after the maker of network management software that Russian intelligence agents are suspected of having breached to gain access to the email systems of government agencies and private companies, was a huge intelligence failure."
44. Corera, Gordon (December 18, 2020). "SolarWinds: UK assessing impact of hacking campaign" (https://www.bbc.com/news/technology-55368213). *BBC News*. Retrieved December 18, 2020.
45. "UK organisations using SolarWinds Orion platform should check whether personal data has been affected" (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/12/uk-organisations-using-solarwinds-orion-platform-should-check-whether-personal-data-has-been-affected/). *ico.org.uk*. December 23, 2020.
46. "CSE warns companies to check IT systems following SolarWinds hack - CBC News" (https://www.cbc.ca/news/politics/cse-solarwinds-warning-1.5854614). *CBC*. December 19, 2020. Retrieved December 25, 2020.
47. Security, Canadian Centre for Cyber (August 15, 2018). "Canadian Centre for Cyber Security" (https://cyber.gc.ca/en/). *Canadian Centre for Cyber Security*.
48. Wolfe, Jan; Pierson, Brendan (December 19, 2020). "Explainer-U.S. government hack: espionage or act of war?" (https://uk.reuters.com/article/global-cyber-legal/explainer-us-government-hack-espionage-or-act-of-war-idUKL1N2IY3EH). *Reuters*. Retrieved December 19, 2020.
49. Dilanian, Ken (December 18, 2020). "Suspected Russian hack: Was it an epic cyber attack or spy operation?" (https://www.nbcnews.com/news/us-news/suspected-russian-hack-was-it-epic-cyber-attack-or-spy-n1251766). *NBC News*. Retrieved December 19, 2020.
50. Erica Borghard; Jacquelyn Schneider. "Russia's Hack Wasn't Cyberwar. That Complicates US Strategy" (https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy/). *Wired*. Archived (https://web.archive.org/web/20201218062246/https://www.wired.com/story/russia-solarwinds-hack-wasnt-cyberwar-us-strategy/) from the original on December 18, 2020. Retrieved December 17, 2020.
51. Goldsmith, Jack. "Self-Delusion on the Russia Hack" (https://thedispatch.com/p/self-delusion-on-the-russia-hack). *thedispatch.com*.
52. "Russia's SolarWinds Operation and International Law" (https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/). *Just Security*. December 21, 2020.
53. "Microsoft president calls SolarWinds hack an 'act of recklessness' " (https://arstechnica.com/information-technology/2020/12/only-an-elite-few-solarwinds-hack-victims-received-follow-on-attacks/). *Ars Technica*. December 18, 2020. Retrieved December 18, 2020.
54. "US cyber-attack: US energy department confirms it was hit by Sunburst hack" (https://www.bbc.com/news/world-us-canada-55358332). *BBC News*. December 18, 2020. Retrieved December 18, 2020.
55. Schneier, Bruce (December 23, 2020). "The US has suffered a massive cyberbreach. It's hard to overstate how bad it is | Bruce Schneier" (https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols) – via www.theguardian.com.
56. Kolbe, Paul R. (December 24, 2020). "Opinion | With Hacking, the United States Needs to Stop Playing the Victim" (https://www.nytimes.com/2020/12/23/opinion/russia-united-states-hack.html) – via NYTimes.com.
57. Kaplan, Fred (December 18, 2020). "The Government Has Known About the Vulnerabilities That Allowed Russia's Latest Hack for Decades—and Chose Not to Fix Them" (https://slate.com/news-and-politics/2020/12/solarwinds-russian-hack-cybersecurity.html). *Slate Magazine*.
58. Kaplan, Fred (December 23, 2020). "Should the U.S. Retaliate for Russia's Big Hack?" (https://slate.com/news-and-politics/2020/12/solarwinds-hack-retaliation-options-cyberwar-russia.html). *Slate Magazine*.

Retrieved from "https://en.wikipedia.org/w/index.php?title=2020_United_States_federal_government_data_breach&oldid=1006025964"

This page was last edited on 10 February 2021, at 17:09 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.