JANUARY 29, 2021

THE SOLARWINDS CYBERATTACK

share tweet email print

KEY TAKEAWAYS

- The SolarWinds computer hack is one of the most sophisticated and large-scale cyber operations ever identified. The U.S. government has stated the operation is an intelligence gathering effort and has attributed it to an actor that is likely Russian in origin.
- The operation has affected federal agencies, courts, numerous private sector companies, and state and local governments across the country.
- It is an example of a digital supply chain attack, in which hackers insert malicious code into trusted third-party software, thus infecting potentially all of the hacked company's customers.

The SolarWinds computer hack is a serious security issue for the United States. The operation has affected federal agencies, the federal courts, numerous private-sector companies, and state and local governments across the country. It is one of the most sophisticated cyberattacks ever conducted. Only a handful of countries could mount the effort and resources necessary to conduct an operation of this scale, technical sophistication, and apparent objective.

The operation is an example of a digital supply chain attack, in which hackers insert malicious code into trusted third-party software, thus infecting potentially all of the hacked software company's customers. Increasing the cybersecurity of digital supply chains is a top cybersecurity issue facing the 117th Congress, the Biden administration, and American technology companies.

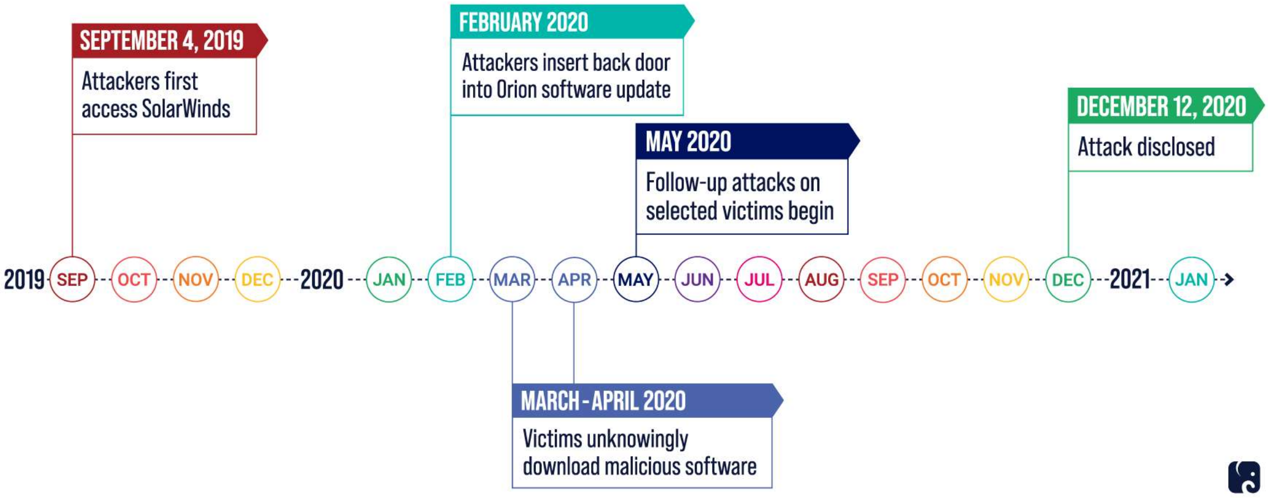
A DIGITAL TROJAN HORSE

SolarWinds is a company based in Austin, Texas, that provides large-scale information technology infrastructure management software and services to businesses and government agencies. It has more than 320,000 customers in 190 countries, including 499 of the Fortune 500.

In December 2020, FireEye, a cybersecurity consulting firm, uncovered and disclosed what is now called the SolarWinds operation. Hackers inserted malicious code into an update for SolarWinds' popular network management platform, known as Orion. Customers who routinely updated their Orion software unknowingly downloaded the embedded virus into their systems. Once inside, the attackers could choose which areas to access and were able to move through systems and conduct their operations undetected.

The attackers were meticulous in covering their tracks and took extreme steps to remain undiscovered. While investigations are ongoing, SolarWinds' current understanding is that the operation began in September 2019, when attackers first breached the system. How the attackers gained access is still unknown. The malware was deployed in February 2020, and customers downloaded the Orion update through March and April. By last May, attackers had started to move within the targeted systems, reading emails and other documents. They remained undetected for the next eight months. According to DHS, given the persistence of these attackers, the campaign may be ongoing and other attacks and victims may be identified as the investigation continues.

SOLARWINDS OPERATION TIMELINE


SEPTEMBER 4, 2019
Attackers first access SolarWinds
FEBRUARY 2020
Attackers insert back door into Orion software update
MAY 2020
Follow-up attacks on selected victims begin
DECEMBER 12, 2020
Attack disclosed
2019
SEP
OCT
NOV
DEC
2020
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
2021
JAN
MARCH - APRIL 2020
Victims unknowingly download malicious software

On January 5, the FBI, Cybersecurity and Infrastructure Security Agency, Office of the Director of National Intelligence, and National Security Agency released a joint statement saying that their investigation so far indicated "an Advanced Persistent Threat actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort."

The agencies noted that while there were approximately 18,000 private and public sector victims that downloaded the infected Orion software, "a much smaller number have been compromised by follow-on activity on their systems." Government agencies confirmed to be affected by the attack include at least the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Labor, State, and Treasury, as well as the National Institutes of Health. More agencies are likely to be added to the list as investigators learn more about the attack.

The Department of Justice says it believes the attackers accessed "around 3%" of DOJ email inboxes but not any classified systems. The hackers reportedly breached the email system used by the most senior Treasury Department officials. They also targeted state and local governments and the federal court system. The federal judiciary's electronic case management and filing system was likely compromised as part of the operation. This puts at risk sensitive case records and information that would be of great value to Russian intelligence, including trade secrets, investigative techniques, and information on targets of surveillance operations. Federal courts are currently accepting highly sensitive case documents only in paper form or on secure devices like thumb drives as they respond to the breach.

Data from Microsoft shows that global IT companies, think tanks, non-governmental organizations, and government contractors working for defense and national security organizations appear to have been targeted in the operation. Targeted private-sector companies reportedly include Belkin, Cisco, Deloitte, Intel, Nvidia, and VMware. The head of FireEye has stated that around 50 organizations were "genuinely impacted" by the operation.

The economic damage from the operation is likely to be immense. Some experts estimate it may cost as much as $100 billion over many months to root out malicious code and ensure systems are not compromised. From an espionage perspective, the damage is impossible to calculate but is likely to be substantial. Federal agencies and global companies may spend years determining whether they were breached, what information was accessed, and what communications were read. Officials are still trying to understand the exact purpose of the operation and whether there may be more sinister objectives in addition to espionage, such as inserting backdoor access into key government agencies, major IT and cybersecurity companies, critical infrastructure like the electric grid, and nuclear storage facilities. This access may allow the hacker to affect the integrity and availability of these systems, including disrupting essential services.

THE FEDERAL RESPONSE TO THE OPERATION

The federal government spends billions of dollars each year on cybersecurity. Yet for months, none of the government's defenses, spread across dozens of federal agencies, detected the intrusion. Responding to the attack and strengthening supply chain security is one of the top cybersecurity issues facing the 117th Congress, the Biden administration, and American technology companies.

President Biden's nominees who will lead the response to the operation and formulate U.S. cybersecurity policy have highlighted the urgent threat the attack presents. Alejandro Mayorkas, nominated to head DHS, stated at his confirmation hearing, "the cybersecurity of our nation will be one of my highest priorities because I concur with you that the threat is real, and the threat is every day, and we have to do a better job than we are doing now." Director of National Intelligence Avril Haines cited the asymmetry of the cyber threat as among the greatest that we face in the United States. Secretary of Defense Lloyd Austin committed to a top-down review of DOD's cyber operations during his confirmation hearing and said of the attack, "Russia should be held accountable."

President Biden has proposed a significant investment in modernizing and securing federal IT as part of the administration's $1.9 trillion coronavirus relief proposal. It calls for $9 billion for the Technology Modernization Fund, an existing fund authorized by the Modernizing Government Technology Act of 2017. The fund received $100 million in fiscal year 2018 and $25 million in fiscal years 2019 and 2020.

The Cybersecurity and Infrastructure Security Agency and the national cyber director – a new position Congress created in the fiscal year 2021 National Defense Authorization Act – will play key roles in responding to the attack and developing policies to improve the nation's cybersecurity. U.S. Comptroller General Gene Dodaro highlighted the role of the national cyber director in a recent RPC interview, saying: "it will be especially critical to fill this position and to ensure that the director has the authorities and capabilities necessary to (1) ensure that federal entities are effectively executing their assigned activities intended to support the nation's cybersecurity strategy and (2) coordinate the government's efforts to overcome the nation's cyber-related threats and challenges."

Senator Rubio, the top Republican on the Intelligence Committee, has called the operation "a grave risk to federal, to state, to local governments, to critical infrastructure, to the private sector" and said, "America must retaliate." Senator Warner, the committee's top Democrat, has said Congress will reexamine whether there should be a national data breach notification requirement. Senators Wicker, Thune, and Moran released a joint statement after receiving a briefing from the Commerce Department on the operation: “Cyberattacks by nation states like Russia and China threaten our economy and national security. Our response should be swift and clear.” Senators Portman and Peters announced that the Homeland Security and Governmental Affairs Committee would hold hearings on the attack and work on “bipartisan comprehensive cybersecurity legislation.”

The Government Accountability Office has conducted oversight of cybersecurity and provided federal agencies numerous recommendations to better manage supply chain risk. Other policy options for Congress include: reviewing CISA’s authorities and resources; increasing sharing and analysis of threat intelligence between the public and private sectors; strengthening and establishing international rules and norms in cyberspace; oversight of DHS, the FBI, NSA, U.S. Cyber Command, the Commerce Department, and other agencies; and taking steps to hold other countries accountable for cyberattacks, whether through sanctions or other means.

ISSUE TAG: TECHNOLOGY