GAO@100
A Century of Non-Partisan Fact-Based Work

Cybersecurity:
Federal Response to SolarWinds and Microsoft Exchange Incidents

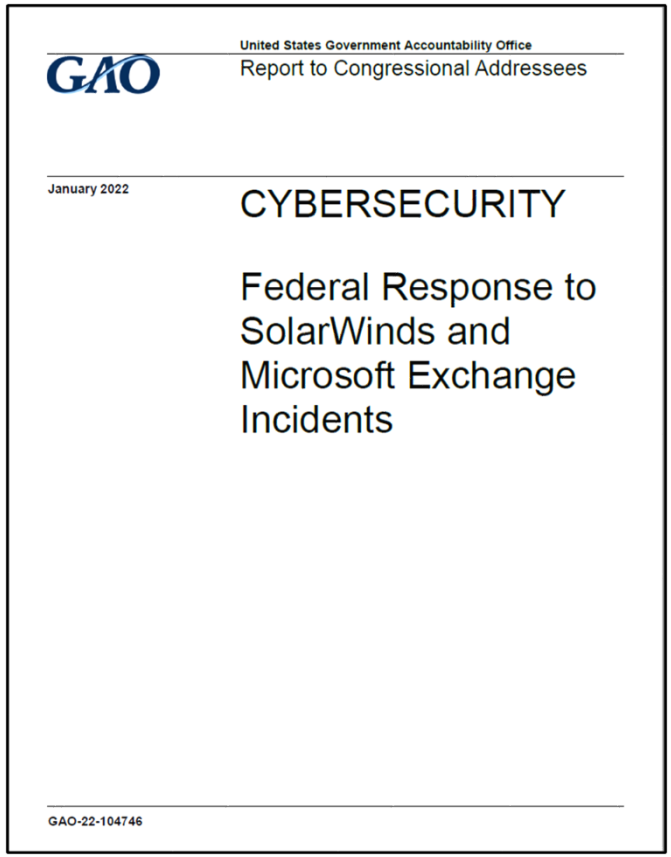
Jennifer R. Franks

Director, Information Technology and Cybersecurity

March 9, 2022

Agenda

- GAO's High-Risk List
- The Report
  - Background
  - SolarWinds Breach
  - Microsoft Exchange Vulnerability
  - Federal Steps Taken
  - Challenges Faced
  - Lessons Learned
- Q/A


United States Government Accountability Office
GAO
Report to Congressional Addressees
January 2022
CYBERSECURITY
Federal Response to SolarWinds and Microsoft Exchange Incidents
GAO-22-104746

GAO-22-104746

GAO High-Risk List

- In 1990, GAO began a program to report on government operations that we identified as “high risk.” Since then, generally coinciding with the start of each new Congress, we have reported on the status of progress to address high risk areas and update the High Risk List.

GAO High-Risk List

Source: GAO analysis. | GAO-21-119SP

GAO High-Risk List:
Ensuring the Cybersecurity of the Nation

- Information Security was added to the High Risk List in 1997 and has been updated with advancements in technology
  - 2003 - critical infrastructure concerns
  - 2015 - personally identifiable information
  - 2018 - comprehensive national strategy & oversight

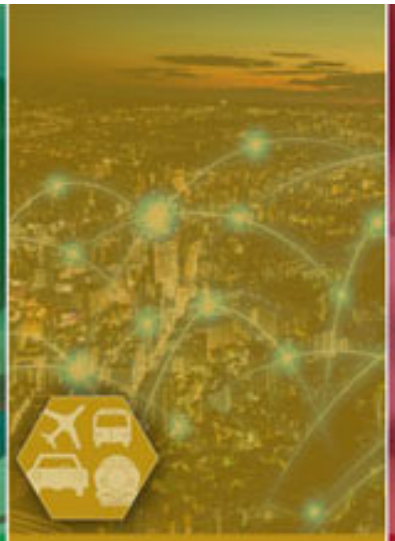
Cybersecurity High Risk Areas

Establishing a comprehensive cybersecurity strategy and performing effective oversight

1. Develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace.
2. Mitigate global supply chain risks (e.g., installation of malicious software or hardware).
3. Address cybersecurity workforce management challenges.
4. Ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things).

Securing federal systems and information

5. Improve implementation of government-wide cybersecurity initiatives.
6. Address weaknesses in federal agency information security programs.
7. Enhance the federal response to cyber incidents.



Protecting cyber critical infrastructure

8. Strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks).

Protecting privacy and sensitive data

9. Improve federal efforts to protect privacy and sensitive data.
10. Appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

Background: Why Did We Do This Work?

- Risks to information technology systems are increasing
- Escalating and emerging threats from around the globe
- Emergence of new and more destructive attacks
- Insider threats from witting or unwitting employees
- Recent incidents highlight significant cyber threats and the range of consequences that these attacks pose

Background: Why Did We Do This Work?

- A recent such incident, involving SolarWinds, resulted in one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector.

- Another incident included zero-day Microsoft Exchange Server vulnerabilities that had the potential to affect email servers across the federal government and provide malicious threat actors with unauthorized remote access.

Key Objectives

1. Provide a summary of the SolarWinds and Microsoft Exchange cybersecurity incidents;

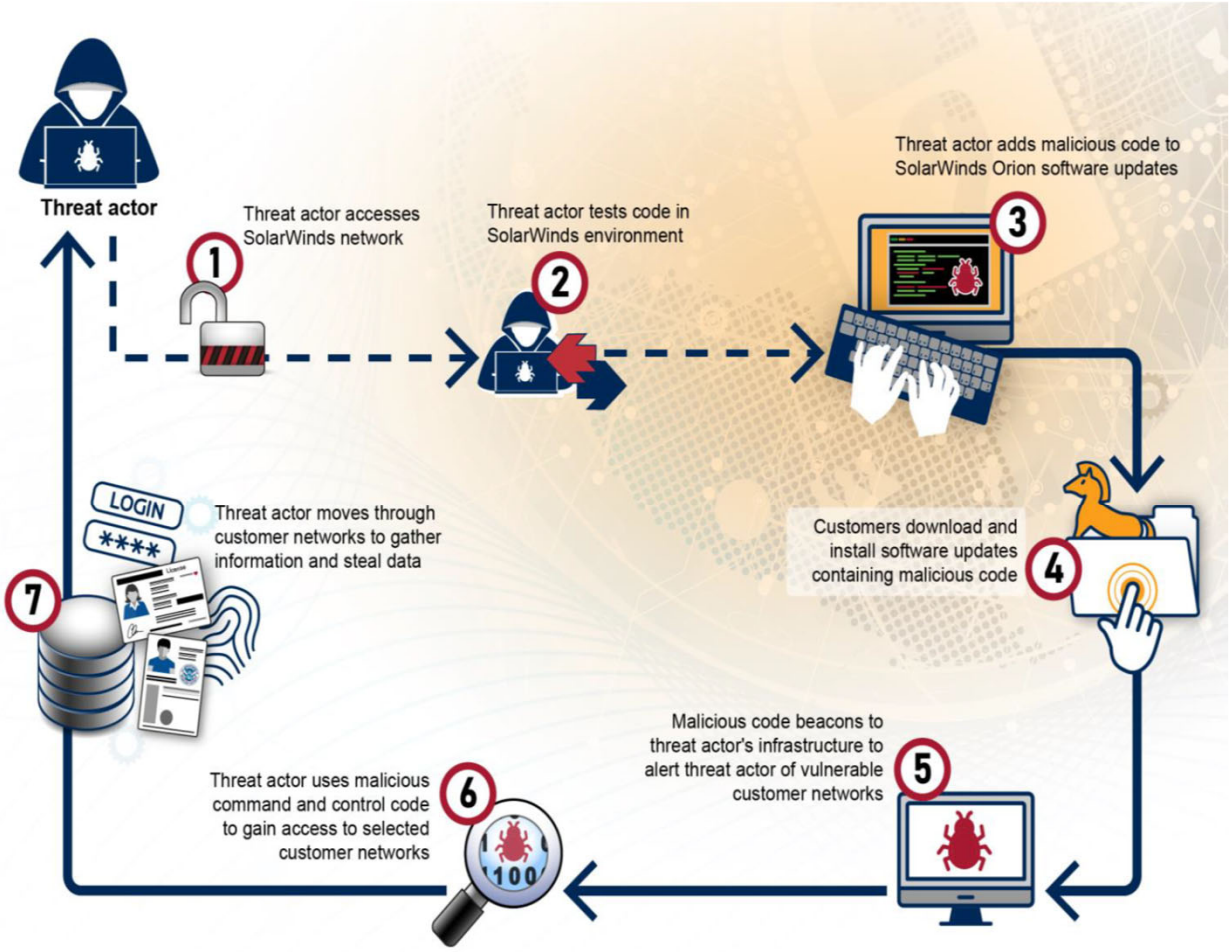
2. Determine the steps federal agencies have taken to coordinate and respond to the incidents; and

3. Identify lessons federal agencies have learned from the incidents.

SolarWinds: What happened?

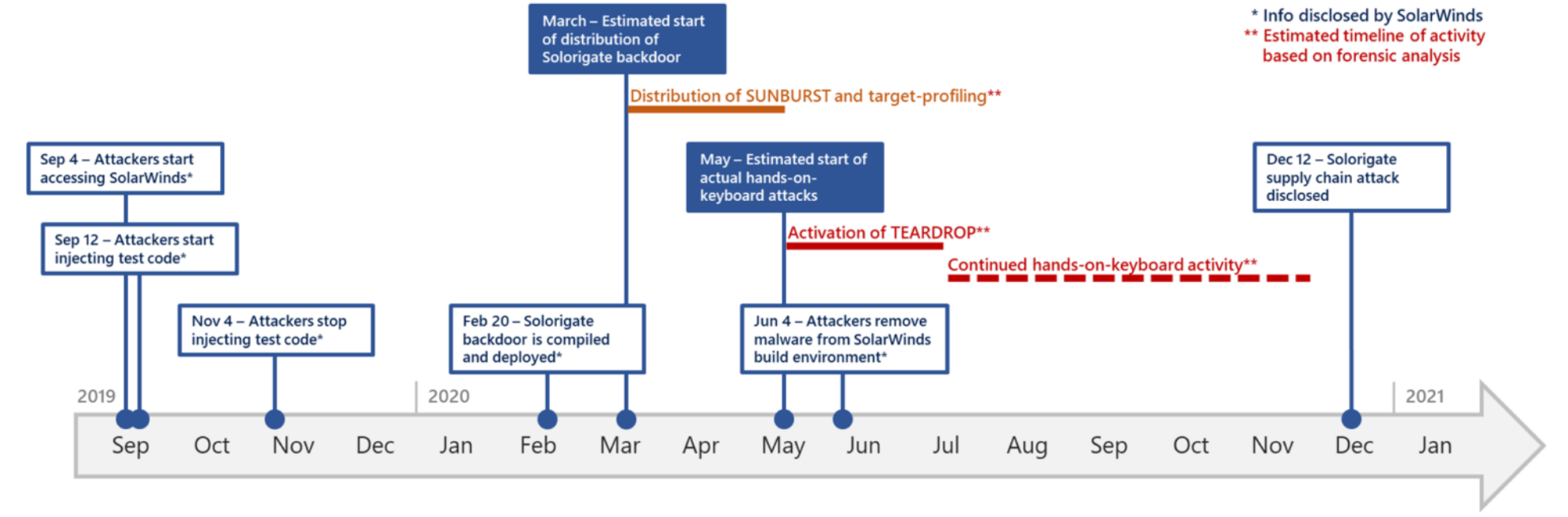
- Who is SolarWinds?
- What is the Orion Platform software that was compromised?

SolarWinds: What happened? (The Attack)



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

SolarWinds: What happened? (The Timeline)



Source: Microsoft

SolarWinds: What happened?

- Attack requires manual intervention by threat actor; more likely the attacker prioritized efforts on high-value targets such as government agencies and private companies that maintain sensitive and/or financially valuable information.
- Patches were digitally signed as trusted.
- Because the code was signed, organizations generally had no reason to believe software was compromised, but the attacker had complete control.
- Once software installed, attacker used advanced methods to remain undetected.
- Established “phone home” connection to command and control servers–used to perform manual interventions.
- While connected through Orion, the threat actor had the ability to:
  - Move laterally to breach other systems and applications on the network.
  - Plant subsequent malware/backdoors to maintain persistence access and execute future attacks.

SolarWinds: The Discovery

- FireEye experienced a compromise of its internal systems and cybersecurity tools and made public statement on December 9, 2020.
- FireEye issued blog post on December 13, 2020 that alerted affected organizations about the malware to help in detection efforts.
- Microsoft flagged digital certificates of the malware and “sinkholed” the domains used by the attacker on December 15, 2020

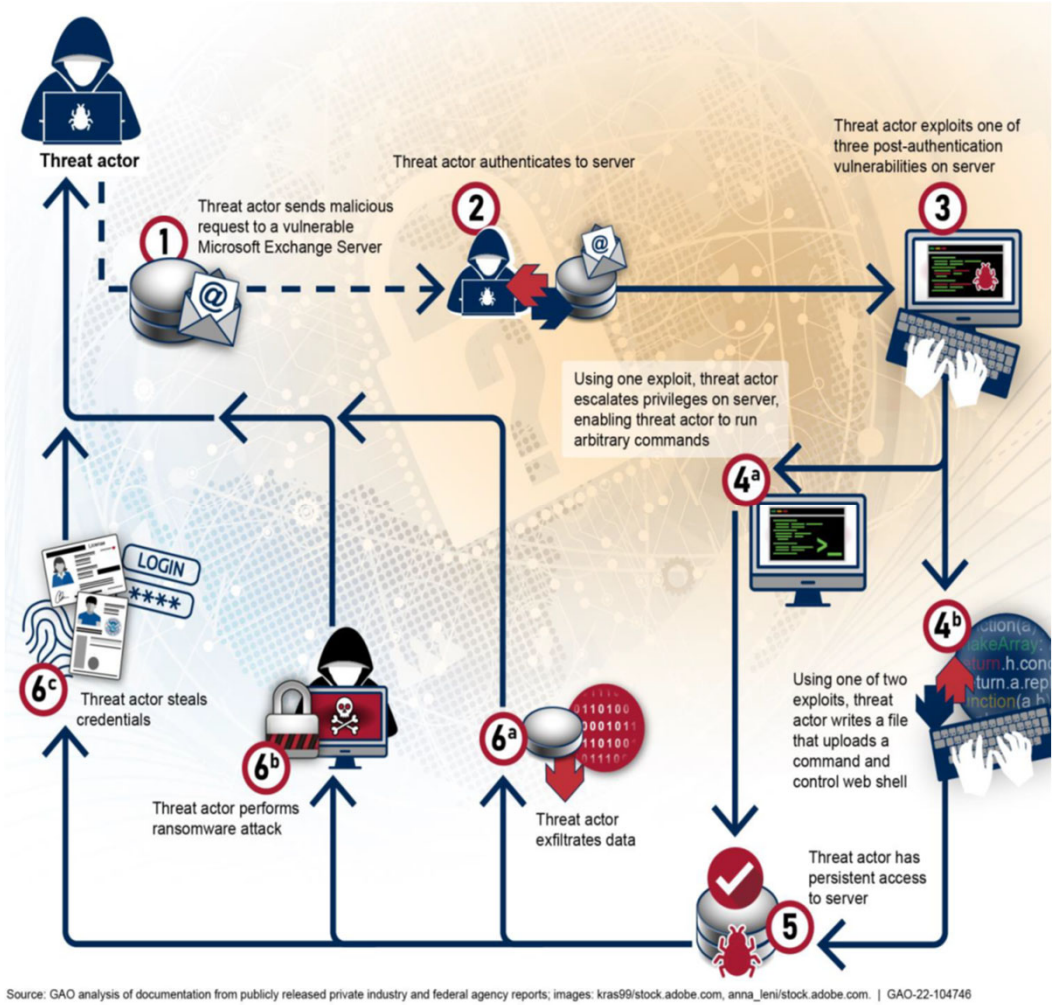
SolarWinds: Potential Impact

- Scale of this attack is massive and global.
- Trust in supply chain / third-party vendors' security — was due diligence of vendor cybersecurity sufficient?
- Potential exposure and national economy, safety, and security implications.
- Likely months, if not years, before know full extent of damage.
- New Guidance—Congress, White House Executive Orders, OMB Memos, NIST, DHS Binding Operational Directives, etc.

Microsoft Exchange: What happened?

- What is the vulnerability?
- Affect on the federal government?

Microsoft Exchange:
What happened? (The Vulnerability)



Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

Microsoft Exchange: What happened?

- On March 2, 2021, Microsoft reported the exploitation of zero-day vulnerabilities used to gain unauthorized access to on-premise Microsoft Exchange Server versions 2013, 2016, and 2019.
- The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources.
- Once a connection was successfully made, the threat actor could leverage other vulnerabilities to escalate account privileges and install web shells on the affected server.
- The web shells allowed the threat actor to remotely access a Microsoft Exchange Server, allowing for persistent malicious operations even after the vulnerabilities were patched.

Microsoft Exchange: Potential Impact

- After the initial exploitation, the threat actors could gain persistent and privileged escalation of accounts to access files and mailboxes on the Microsoft Exchange Server as well as potentially pivot to access other systems and networks within that agency.

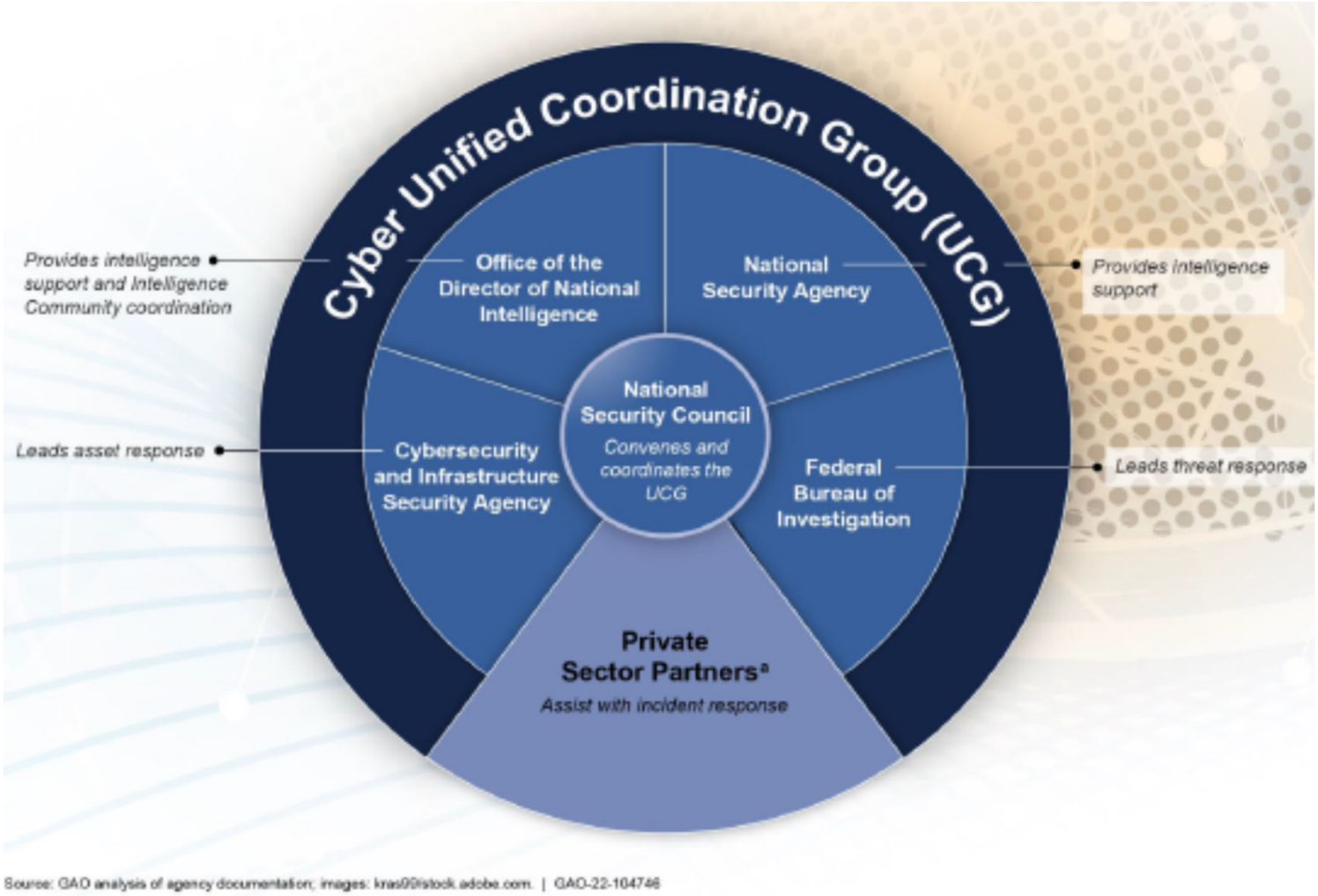
- Further, the persistent access could enable the threat actor to steal credentials and information including PII, encrypt data for ransom, and carry out other types of attacks.

Federal Steps Taken

- Two Cyber Unified Coordination Groups (UCG) established—one for the SolarWinds incident and one for the Microsoft Exchange incident, both consisting of members from:
  - Cybersecurity and Infrastructure Security Agency (CISA)
  - Federal Bureau of Investigation (FBI)
  - Office of the Director of National Intelligence (ODNI)
  - National Security Agency (NSA)

- According to UCG agencies, the Microsoft Exchange UCG also integrated several private sector partners in a more robust manner than their involvement in past UCGs.

The Cyber Unified Coordination Group



Source: GAO analysis of agency documentation; images: kras99/stock.adobe.com. | GAO-22-104746

Federal Steps Taken: CISA

- Serves as a central point of contact and federal lead for asset response activities for government, private sector, and international partners.
- Provides technical assistance upon request.
- Facilitates information sharing and operational coordination through its release of numerous alerts, advisories, and tools, including details on indicators of compromise.
- Engages with public and private stakeholders across relevant critical infrastructure communities to promote dissemination of information and ensure steps were being taken to identify and mitigate compromises.

Federal Steps Taken: FBI

- Acts as the federal lead in threat response activities.
- Investigates and gathers intelligence in order to attribute, pursue, and disrupt the responsible threat actor.
- Identifies victims, collect evidence, and analyze evidence to determine attribution.
- Investigates results to provide indicators of compromise to network defenders and intelligence to government and private sector partners to enable further actions.
- Provides direct incident response assistance.

Federal Steps Taken: ODNI

- Serves as the federal lead for intelligence support and related activities.
- Responsible for managing threat and asset response for intelligence community networks and systems, with support from other agencies as needed.
- Provides situational awareness for stakeholders and coordinate intelligence.

Federal Steps Taken: NSA

- Provides intelligence, cybersecurity expertise, and actionable guidance to UCG partners, as well as national security systems, DOD, and Defense Industrial Base system owners.

- Engages with UCG and industry partners to assess the scope and scale of incidents, and provide technical mitigation guidance.

Federal Challenges Faced

No Easy Fix! Just removing and updating Orion software may not remove attacker. Specifically—

- Attacker likely moved laterally & planned since day one for eventual discovery.
- Required some agencies to reset/rebuild aspects of their network (user authentications, trusted identities, login credentials).
- To mitigate potential second-stage attacks (additional malware that was planted and is waiting silently) agencies may need to perform robust threat hunting activities and engage with private partners.

Federal Challenges Faced

- These incidents highlight the lack of Federal guidance and oversight regarding supply chain review and vulnerability assessment.
- Agencies historically haven't kept sufficient logs/records for forensics to reconstruct what happened or that would aid in detecting suspicious activity that may persist on their networks (GAO-19-545).
- Existing gaps in capacity (skill gap and/or headcount gap) exacerbated the challenge of incident response and threat hunting.
- Existing resources in public and private sector overwhelmed and overburdened in addressing these and other incidents.

Lessons Learned: Coordination with Private Sector

- Federal agencies' coordination with the Private Sector reportedly led to desirable outcomes:
  - Allowed the quick identification of the scale of the SolarWinds incident leading to a faster response.
  - Provided increased visibility on the status of patching and exploitation in the case of the Microsoft Exchange vulnerabilities.
  - Provided the opportunity for the federal government to build trust with the private sector, which may lead to increased coordination for future significant cyber incidents.

Lessons Learned: Coordination Across Government

- Federal agencies' coordination with each other reportedly led to desirable outcomes:
  - UCG as a centralized forum for interagency communication enhanced the participating agencies' coordination efforts.
  - The regular cadence of meetings allowed the UCG members to coordinate and streamline information sharing.
  - UCG communication allowed the FBI to quickly collaborate with other agencies enabling the FBI to provide victims in the public and private sectors with security advisories, including technical advisories developed with other federal agencies that assisted in remediating relevant vulnerabilities.

Lessons Learned: Information Sharing Restrictions

- Federal agencies' information sharing restrictions and limited evidence collection reportedly led to undesirable outcomes:
  - Information sharing of law enforcement information difficult due to the classification levels for information.
  - A shared channel (outside of email) to share information would have been beneficial.
  - Information dissemination should have been an automated process rather than the manual process.
  - Varying levels of data log preservation among agencies and a lack of data collection tools limited evidence collection for the incidents.

Lessons Learned: UCGs

- The National Security Council conducted a review of the SolarWinds incident after the UCG's dissolved, observations include:
  - Aligning technology investments with operational priorities.
  - Improving public-private engagement.
  - Improving threat intelligence acquisition, sharing, and use among federal agencies.

Check out our related blogs…

April 2021: *https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic*

February 2022: *https://www.gao.gov/blog/hacks-bring-new-urgency-moves-congress-and-agencies-reduce-future-cybersecurity-risks*

Questions?

Jennifer Franks | U.S. GAO
Franksj@gao.gov