GAO Highlights

Highlights of GAO-22-104746, a report to congressional addressees

January 2022

CYBERSECURITY

Federal Response to SolarWinds and Microsoft Exchange Incidents

Why GAO Did This Study

The risks to information technology systems supporting the federal government and the nation's critical infrastructure are increasing, including escalating and emerging threats from around the globe, the emergence of new and more destructive attacks, and insider threats from witting or unwitting employees. Information security has been on GAO's High Risk List since 1997.

Recent incidents highlight the significant cyber threats facing the nation and the range of consequences that these attacks pose. 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. According to CISA, the potential exploitation from both incidents posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited and the prevalence of affected software.

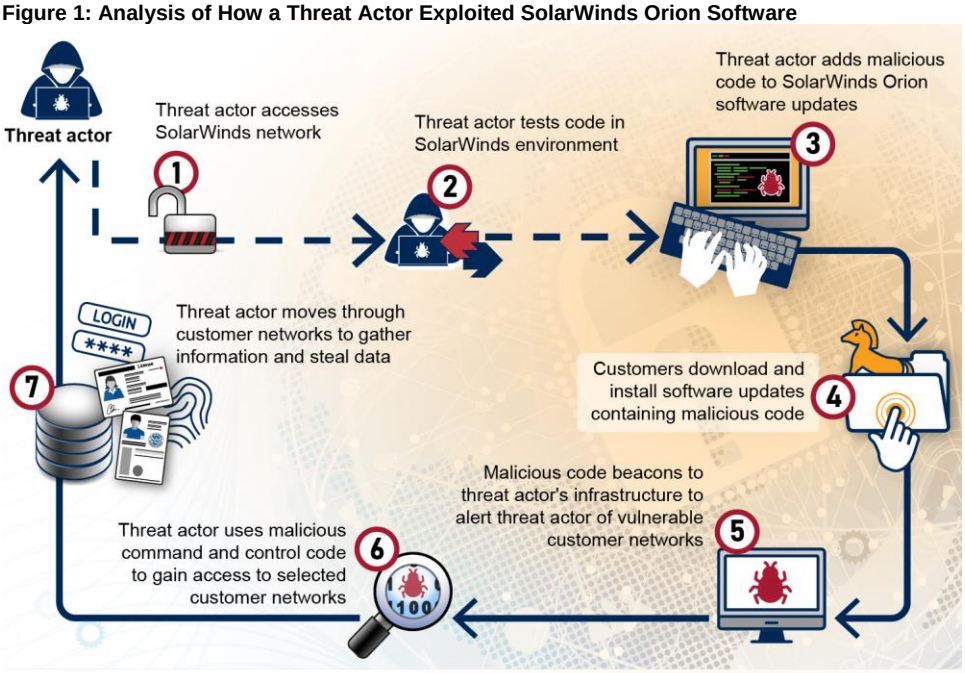
GAO performed its work under the authority of the Comptroller General to conduct an examination of these cybersecurity incidents in light of widespread congressional interest in this area. Specifically, GAO's objectives were to (1) summarize the SolarWinds and Microsoft Exchange cybersecurity incidents, (2) determine the steps federal agencies have taken to coordinate and respond to the

View GAO-22-104746. For more information, contact Nick Marinos (202) 512-9342 or marinosn@gao.gov or Jennifer Franks (404) 679-1831 or franksj@gao.gov.

What GAO Found

Beginning as early as January 2019, a threat actor breached the computing networks at SolarWinds—a Texas-based network management software company, according to the company's Chief Executive Officer. The federal government later confirmed the threat actor to be the Russian Foreign Intelligence Service. Since the company's software, SolarWinds Orion, was widely used in the federal government to monitor network activity and manage network devices on federal systems, this incident allowed the threat actor to breach several federal agencies' networks that used the software (see figure 1).

Figure 1: Analysis of How a Threat Actor Exploited SolarWinds Orion Software



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

While the response and investigation into the SolarWinds breach were still ongoing, Microsoft reported in March 2021 the exploitation or misuse of vulnerabilities used to gain access to several versions of Microsoft Exchange Server. This included versions that federal agencies hosted and used on their premises. According to a White House statement, based on a high degree of confidence, malicious cyber actors affiliated with the People's Republic of China's Ministry of State Security conducted operations utilizing these Microsoft Exchange vulnerabilities. The vulnerabilities initially allowed threat actors to make authenticated connections to Microsoft Exchange Servers from unauthorized external sources. Once the threat actor made a connection, the actor then could leverage other vulnerabilities to escalate account privileges and install web shells that enabled the actor to remotely access a Microsoft Exchange Server. This in turn allowed for persistent malicious operations even after the vulnerabilities were patched (see figure 2).

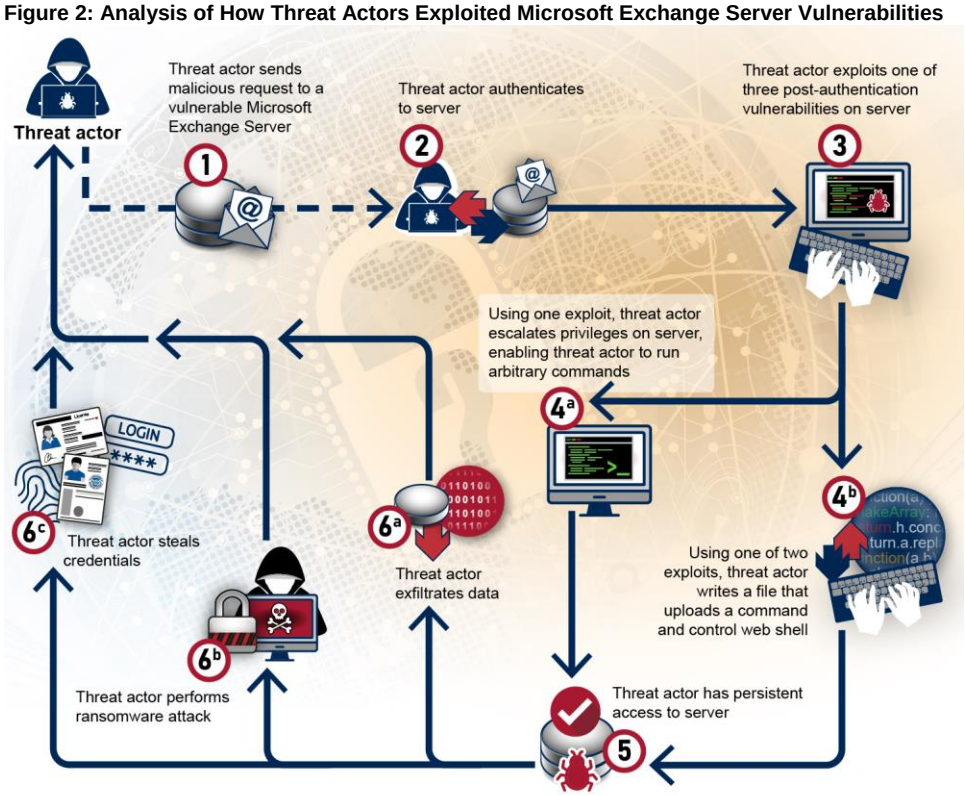
incidents, and (3) identify lessons federal agencies have learned from the incidents.

To do so, GAO reviewed documentation such as descriptions of the incidents, federal agency press releases, response plans, joint statements, and guidance issued by the agencies responsible for responding to the incidents: DHS (CISA), the Department of Justice (FBI), and ODNI with support from NSA. In addition, GAO analyzed incident reporting documentation from affected agencies and after-action reports to identify lessons learned. For all objectives, GAO interviewed agency officials to obtain additional information about the incidents, coordination and response activities, and lessons learned.

What GAO Recommends

Since 2010, GAO has made about 3,700 recommendations to agencies aimed at remedying cybersecurity shortcomings. As of November 2021, about 900 of those recommendations had not yet been fully implemented. GAO will continue to monitor federal agencies' progress in fully implementing these recommendations, including those related to software supply chain management and cyber incident management and response. Five of six agencies provided technical comments, which we incorporated as appropriate.

Figure 2: Analysis of How Threat Actors Exploited Microsoft Exchange Server Vulnerabilities



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

Federal agencies took several steps to coordinate and respond to the SolarWinds and Microsoft Exchange incidents including forming two Cyber Unified Coordination Groups (UCG), one for the SolarWinds incident and one for the Microsoft Exchange incident. Both UCGs consisted of the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI), with support from the 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.

CISA issued emergency directives to inform federal agencies of the vulnerabilities and describe what actions to take in response to the incidents. To aid agencies in conducting their own investigations and securing their networks, UCG agencies also provided guidance through advisories, alerts, and tools. For example, the Department of Homeland Security (DHS), including CISA, the FBI, and NSA released advisories for each incident providing information on the threat actor's cyber tools, targets, techniques, and capabilities. CISA and certain agencies affected by the incidents have taken steps and continue to work together to respond to the SolarWinds incident. Agencies have completed steps to respond to the Microsoft Exchange incident.

Agencies also identified multiple lessons from these incidents. For instance,

- coordinating with the private sector led to greater efficiencies in agency incident response efforts;
- providing a centralized forum for interagency and private sector discussions led to improved coordination among agencies and with the private sector;
- sharing of information among agencies was often slow, difficult, and time consuming and;
- collecting evidence was limited due to varying levels of data preservation at agencies.

Effective implementation of a recent executive order could assist with efforts aimed at improving information sharing and evidence collection, among others.