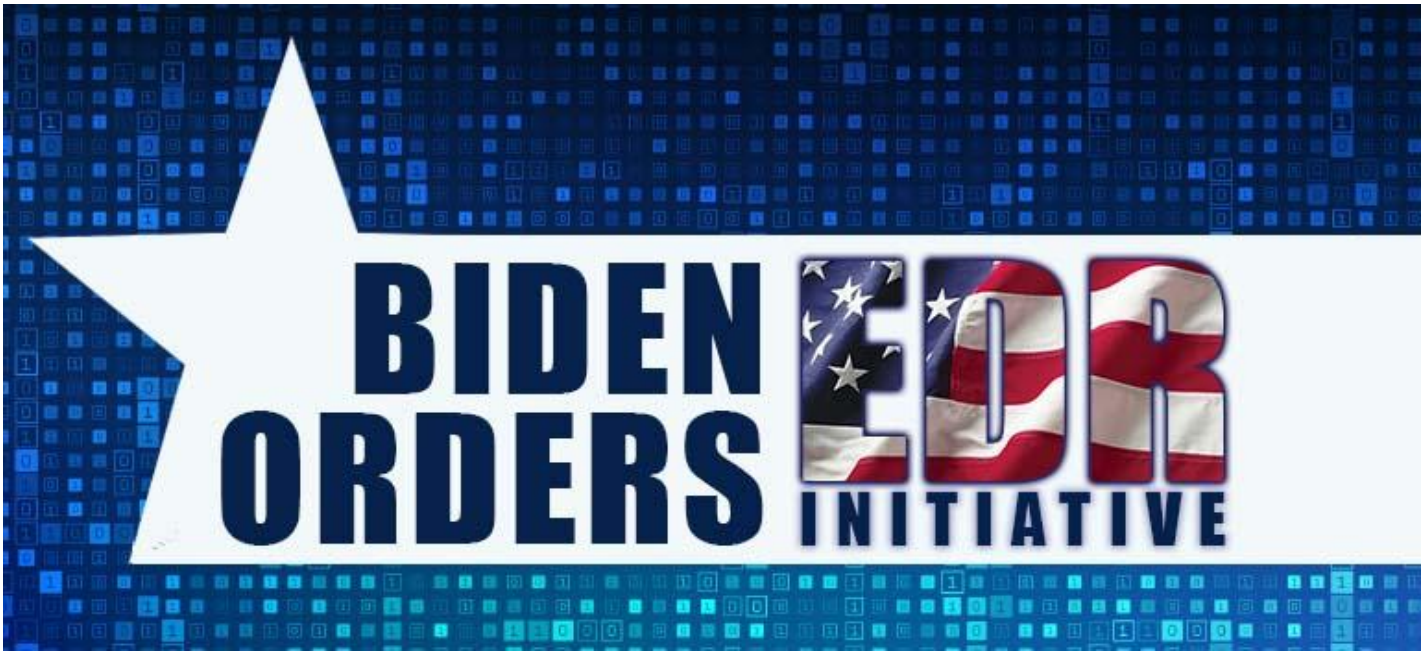
United States {CYBERSECURITY} Magazine
A Multi-Platform Publishing Portal

From the Fall 2021 Issue

Cybersecurity & Government

Biden Orders Endpoint Detection and Response (EDR) Initiative

Dr. Scott Jasper
Senior Lecturer, Captain, U.S. Navy, Retired | Naval Postgraduate School



President Biden signed an Executive Order in May 2021 to improve the Nation's cybersecurity. It claims the United States "faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector [and] the private sector." The Executive Order was released only months after the SolarWinds Supply Chain campaign was revealed by the

cybersecurity firm, FireEye, in mid-December 2020. The campaign exploited SolarWinds Orion business software updates to distribute malware that FireEye called SUNBURST. The updates were downloaded by 18,000 SolarWinds customers in the March to May 2020 timeframe. The campaign further compromised nine U.S. federal agencies, to include Treasury, State and Energy, and about a hundred select private companies mainly in the technology and telecommunications sectors. The federal agencies failed to detect the SUNBURST backdoor installation and subsequent post compromise activity.

There is no surprise that the Executive Order recognizes that the Federal Government must improve its efforts to identify, detect, and respond to ever more sophisticated cyber activity. In a concerted effort to employ all appropriate resources to maximize early detection of cybersecurity incidents, the Executive Order states Federal Agencies shall deploy an Endpoint Detection and Response (EDR) initiative within their infrastructure. What are the advantages of this deployment, and would the technology have prevented a SolarWinds attack?

SOLUTION ADVANTAGES

At a Congressional hearing in February 2021 on the SolarWinds campaign, Senator Ron Wyden remarked that America's "$6 billon cyber shield failed to stop or detect the hacks." The senator was referring to EINSTEIN, an Intrusion Detection System (IDS) used by the U.S. government. An IDS is usually deployed at strategic points throughout a network. It passively attempts to match any traffic passing by to a list of known attacks. The Cybersecurity and Infrastructure Agency (CISA) website states that EINSTEIN "identifies malicious or potentially harmful computer network activity in federal government network traffic flows based on specific known signatures." This means EINSTEIN is only as good as the latest database and cannot identify signatures or patterns not previously seen in attacks.

Attackers today are using polymorphic malware to continuously change characteristics. They are also using fileless attacks to leverage and abuse legitimate processes running on the operating system, in some instances to hide their malware. They avoid detection by disabling security software or obfuscating or encrypting data and scripts. The MITRE ATT&CK Framework tactics section on Defense Evasion describes 155 techniques used to subvert defenses. CISA openly admits that EINSTEIN is not a silver bullet and advocates for defense-in-depth to manage the risk of a cyber-attack. While EINSTEIN provides perimeter defense for federal agencies, CISA argues it must be complemented with other tools inside agency networks.

Endpoint Detection and Response is focused on advanced threats that are designed to evade defenses after penetrating the perimeter.

Endpoint Detection and Response is focused on advanced threats that are designed to evade defenses after penetrating the perimeter. The solution uses telemetry data collected from endpoint devices to detect, investigate, and remediate modern threats. It continuously analyzes files, processes, and events to find malicious behavior. The solution typically leverages cyber threat intelligence with large-scale machine learning to identify file characteristics. If still unknown, the solution can investigate further with sandbox technology to determine the attributes and nature of the file. If there is not a file to analyze, for instance in an attack manipulating legitimate processes, child processes can be checked to see if they are spawning as they should, when they should, and from where they should.

Remediation can occur by isolating the endpoint, blocking connections, or terminating processes before the attacker can move laterally in the network. An advantage of EDR is the ability to view past events, such as process creation, driver loading, network connections, and memory writing for root cause analysis. This enables visibility of the mechanisms and timeline for how a threat initially spread from its origin. Integration of this historic information with cyber threat intelligence platforms can help prevent future attacks. Many security vendors, like McAfee, have evolved the EDR solution into an Extended Detection and Response (XDR) posture, enhancing visibility and control across endpoints, networks, and cloud.

SOLARWINDS DETECTION

FireEye meticulously described in their report and additional technical details how the SolarWinds campaign utilized complex evasive techniques to successfully circumvent security controls. The Orion business software updates, called SolarWinds.Orion.Core.BusinessLayer.dll, were digitally signed and posted to the SolarWinds updates website. The plugin contained the SUNBURST backdoor, which may retrieve commands to transfer and execute files, profile and reboot systems, and disable system services. The backdoor uses obfuscated blocklists to identify processes, services and drivers associated with forensic and anti-virus tools in order to disable them. FireEye believes multiple checks for analysis tools helped SUNBURST evade detection for seven months. After remaining dormant for up to two weeks, the malware attempts to resolve a subdomain of avsvmcloud[.]com. The DNS response pointed to a Command and Control (C2) domain. The malware's network traffic masqueraded as legitimate activity by imitating the Orion Improvement Program protocol and storing data in legitimate plugin configuration files, most likely to avoid intrusion detection systems, like EINSTEIN.

The SolarWinds campaign post compromise activity also leveraged multiple techniques to disguise operations and evade detection. The attackers preferred a light malware footprint, instead using legitimate credentials and remote access. For select high visibility victims, they used the memory-only dropper named TEARDROP to deploy a second stage payload, Cobalt

Strike, which is a legitimate penetration testing tool for hands-on-keyboard activity and lateral movement. They also set hostnames on command and control infrastructure to match legitimate names on the victim environment to avoid suspicion and used primarily IP addresses originating from the same country. They gained access to networks with compromised credentials and moved across networks with multiple different credentials. Finally, they replaced legitimate files and manipulated scheduled tasks to execute utilities or tools and then restored the legitimate originals. The attackers also used steganography techniques to hide commands in multiple strings of benign code.

The Biden Executive Order calls for “bold changes and significant investments” to defend vital government institutions.

Days after the FireEye report, the CEO and Chairman of Palo Alto Networks shared their success in preventing a SolarWinds attack. A week later the cybersecurity company released further details on what their Security Operations Center (SOC) had observed earlier that year. In late September, they noticed a DNS request from their SolarWinds Orion server for the avsvmcloud[.]com domain as part of the phase to report the identity of the organization. The connection was short-lived, and no malicious content was downloaded, but the system was flagged for possible intrusion. Then, six days later in early October, a new payload, Cobalt Strike, was attempted to be downloaded, as part of the post compromise phase to gain further access. The Palo Alto Networks Cortex XDR Pro’s Behavioral Threat Protection capability instantly detected the payload and in combination with the unusual DNS requests triggered a prevention which blocked the download and raised an alert to SOC operations.

Even though the threat sought to disable security software, the Cortex XDR automated behavioral analytic capability could not be disabled through the Windows Registry, unlike at least eight other prominent endpoint security solutions. The SOC quickly isolated the server, initiated an investigation, and verified the Palo Alto Networks infrastructure was secure. Then Palo Alto Networks notified SolarWinds of the observed activity. The company also deployed a set of indicators of compromise to customers of their security products. Their investigation concluded the attempted SolarWinds attack was not successful, and that no data was compromised. The CEO and Chairman stated that at the time, they thought the attempt to download Cobalt Strike was an isolated incident.

INITIATIVE IMPLEMENTATION

The Biden Executive Order calls for “bold changes and significant investments” to defend vital government institutions. The Executive Order directs the issuance of requirements for federal agencies to adopt federal-government wide EDR approaches. It also mandates those agencies

have adequate resources to comply with these requirements. The Executive Order seems to parallel testimony to the United States Senate Select Committee on Intelligence by CEOs from leading cybersecurity firms on the SolarWinds campaign targeting critical software supply chains. For instance, the Co-Founder and CEO of CrowdStrike called for organizations to protect their development platforms and code repositories, similar to an Executive Order section that directs the issuance of guidance for standards, procedures, or criteria regarding secure software development environments.

Moreover, the CEO calls for file-based machine learning prevention to defeat novel threats, citing a CrowdStrike model that detected with high confidence the SUNSPOT malware, used to monitor when SolarWinds compiled new software and insert the malicious payload SUNBURST during the build process. Most importantly, the CEO recognizes the ability of XDR, the evolved EDR solution, to provide contextual awareness across entire environments, which he states can "generate intelligence from what otherwise may be no more than an information overload."

Also, in testimony to the Senate Committee, the CEO of FireEye, revealed how they discovered the SolarWinds impact SUNBURST. Their investigation of a breach that stole Red Team tools, by an attacker using techniques not witnessed by them or their partners in the past, led to a forensic analysis of a SolarWinds server. They decompiled and reverse engineered the platform to uncover the implant. Seemingly the only company that detected SolarWinds activity with XDR capabilities before the FireEye announcement is Palo Alto Networks. Although, their early detection of installation and compromise activity did not reveal the full extent of the campaign.

Yet when correlated with the SUNBURST disclosure in December, Palo Alto Networks initiated a comprehensive outreach engagement effort to share their unique threat intelligence insight with key U.S. government cyber operational agencies. This outreach is indicative of a proposal to the Senate by the CEO of FireEye for increased public and private sector collaboration in consistent and confidential information sharing. In fact, to enable more effective defense of federal agency systems, the Biden Executive Order mandates information sharing for ICT service providers under contract when they discover a cyber incident. The implementation of EDR across federal agencies has the potential to detect attacks of the sophisticated nature of SolarWinds, especially when enhanced with vibrant cyber threat intelligence sharing initiatives.

References

1. President Joseph Biden, "Executive Order on Improving the Nation's Cybersecurity," The White House, Presidential Actions, May 12, 2021.
2. FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," Threat Research, December 13, 2020.
3. Dustin Volz and Robert McMillian, "Massive Hacks Linked to Russia, China Exploited U.S. Internet Security Gap," *The Wall Street Journal*, March 10, 2021.
4. Cybersecurity & Infrastructure Security Agency, "EINSTEIN," Securing Federal Networks: https://www.cisa.gov/einstein
5. MITRE ATT&CK, Tactics, Defense Evasion, 19 July 2019: https://attack.mitre.org/tactics/TA0005/

6. 3nom, “What Are the Benefits of Endpoint Detection Response?” 3nom Blog.
7. McAfee, “What is Extended Detection and Response (XDR)?” McAfee Blog.
8. FireEye, “SUNBURST Additional Technical Details,” Threat Research, December 24, 2020.
9. Nikesh Arora, CEO of Palo Alto Networks, “Palo Alto Networks Rapid Response: Navigating the SolarStorm Attack,” Palo Alto Networks Blog, December 17, 2020.
10. Unit 42, “SolarStorm Supply Chain Attack Timeline,” Blog Post, December 23, 2020.
11. Sven Krasser, “Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware,” CrowdStrike Blog, January 21, 2021.
12. George Kurtz, CEO of CrowdStrike, “Testimony on Cybersecurity and Supply Chain Threats,” to the Senate Select Committee on Intelligence, February 23, 2021.
13. Kevin Mandia, CEO of FireEye, “Prepared Statement,” before the Senate Select Committee on Intelligence, February 23, 2021.
14. FireEye, “Unauthorized Access of FireEye Red Team Tools,” Threat Research, December 8, 2020.

Dr. Scott Jasper

LEAVE A COMMENT

0 Comments Sort by **Oldest**

Add a comment...

Facebook Comments Plugin

TABLE OF CONTENTS

Staying Home May Be Good for Your Health, but Is It Good For Agency Security?

The Fourth Industrial Revolution: Securing the Future

What Should Your Home Cybersecurity Set Up Look Like?

The Power of Automation

AMPLIFYING YOUR SOC EFFORTS WITH AUTOMATION

Multiparty Computation Secures Machine Identity in the New Cyber Frontier

Developing the Next Cybersecurity Generation

Turn Your Company Into an Incubator for Cyber Talent

Cybersecurity & Critical Infrastructure

What is Cyber Leadership?

Hackers Are Laying Siege to Critical Infrastructure: Here's How to Fight Back

Reducing Risk

Some Risks We Must Accept

Exploring the Differences Between Bug Hunters and Pentesters

A Software Bill of Materials Is Critical for Comprehensive Risk Management

Why We Haven't Solved the Problem of Too Many Software Bugs

Cybersecurity & RF Signatures

Digital Convenience or Big Brother? Cool Tech Might Be Our Downfall

Protecting Your Data

The Most Financially Devastating Form of Cyber-Attacks Can be Thwarted for Free

The Ardennes, Again

The Cyber-Hygiene Mantra

How to Manage Challenges of Cloud Migration and Microsoft Vulnerabilities

Trade-Offs of Convenience: Social Logins, Password Managers and Other Single Points of Failure in User Authentication

Cybersecurity & Government

Wyoming Takes a Holistic Approach in Cybersecurity Standards for Businesses, Expanding Connections, and Creating Jobs

Developing a Cybersecurity Culture

Cybersecurity Legislation

Cybersecurity & The Threat Landscape

Risk Mitigation

Preparing for Cybersecurity Threats

ISSUE INDEX