ExtraHop Data Shows 150 Percent Increase in Suspicious Network Activity During Peak of SUNBURST Attack

Post-disclosure investigations revealed sophisticated attack patterns designed to subvert traditional security controls and detection methods

SEATTLE – February 11, 2021 – ExtraHop, the leader in cloud-native network detection and response, today released a security report offering an in-depth look at the methods cybercriminals used to evade detection during the months before the SolarWinds SUNBURST exploit was discovered. The report also reveals significant increases in suspicious network activity that went largely ignored due to the privileged and trusted status of SolarWinds within the IT environment. As part of the report, ExtraHop also released an expanded list of over 1,700 SUNBURST indicators of compromise (IOCs) as observed across affected environments protected by Reveal(x), critical information that can help organizations determine if and to what extent they've been compromised.

During its own investigation, and through its work with customers to help detect and remediate the SUNBURST exploit, ExtraHop threat researchers found that between late March 2020 and early October 2020, detections of probable malicious activity increased by approximately 150 percent. These detections which included lateral movement, privilege escalation, and command and control beaconing, evaded the more traditional detection methods like endpoint detection and response (EDR) and antivirus. Activity patterns outlined in the report indicate that the SUNBURST attackers were successful in flying under the radar of these detection methods either by disabling them, or by redirecting their approach before they could be detected.

"Unfortunately, what we found when investigating SUNBURST is that the activity was actually detected on the network," said Jeff Costlow, Deputy CISO, ExtraHop. "But because other detection methods weren't alerting on the activity, it largely went ignored. In this case, the attack was strategically designed to evade those detections, and we can expect more similar attacks to follow. It's an important reminder that the network doesn't lie."

In addition to shedding new light on how the SUNBURST attackers were able to dwell within the network unchecked for so long, the report delves into several case studies on how ExtraHop customers investigated and remediated the exploit within their own environments. The case studies include details on how customers were able to use historical metrics to determine the duration of the compromise, as well as which systems and data may have been impacted.

Download the full report here: Security Report: Lessons Learned Investigating SUNBURST Software Supply Chain Attack.

For additional information on SUNBURST, please read our blog for a deep dive on the topic and read more here for our list of 1700+ IOCs.

About ExtraHop
ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyses all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behaviour and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. Get Started at www.extrahop.com/freetrial

ENDS

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au