Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Summary | Broken Trust: Lessons from Sunburst

More than an IT problem or a mythical adversary, the Sunburst crisis was a failure of strategy. Existing policy tools were poorly utilized and or too slow to keep pace with the risk they hoped to manage. Industry could have done more to enable users to defend themselves against the latest threats and reduce the consequences of low probability, high impact failures. In this report, the Cyber Statecraft Initiative's Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo build on the Breaking Trust dataset to present the first significant, public, analysis of the policy dimensions of the Sunburst campaign, and capture a new understanding of what happened. An important conventional wisdom about Sunburst is wrong – this was not just about software supply chains security but also very much about the security of cloud computing. For the 'shared responsibility' model of cloud computing to work, cloud providers have to build services which users can effectively defend.

Efforts to improve the baseline defensibility of the technology ecosystem and reform federal cybersecurity policies must be informed by the strategic logic of the intelligence contest in which the United States and its allies are engaged. Sunburst was not an isolated or unprecedented incident. The United States must drive policy that enables both offensive and defensive operations which are faster, better balanced, and work effectively together under conditions of persistent engagement. Getting the strategy right is essential to maintaining the strength and security of the United States in this evolving contest for information, and with it the chance for leverage in the cyber domain.

Sunburst

In December 2020, cybersecurity firm FireEye disclosed the first publicly known elements of what would prove to be one of the most expansive cyber-espionage campaigns of a young century. An adversary had infiltrated the software development infrastructure of Texas-based vendor SolarWinds and compromised the Orion software. After more than a year of planning, preparation, and practice runs, the adversary inserted the Sunburst malware [1] into regular Orion updates for approximately 18,000 SolarWinds customers.

The SolarWinds supply-chain compromise, while significant, was only one of the vectors used to penetrate more than one hundred actively exploited targets' on-premises and cloud infrastructure. By the Cybersecurity and Infrastructure Security Agency's (CISA) estimate, as many as 30 percent of these compromises occurred independent of the Orion program. The adversary's ultimate objective in every publicly discussed SolarWinds case was organizational email accounts, calendars, and related data. To facilitate this access, the intruders persistently and effectively abused several of Microsoft's identity and access management (IAM) products, granting themselves 'permissions' to pilfer systems largely undetected. In many instances, the central focus of these intruders appears also to have been Microsoft's software as a service (SaaS) suite—Office 365—with SolarWinds and others serving as vectors to that end.

The scale and severity of this compromise, which affected multinational firms like Intel and Microsoft, and dozens of critical infrastructure sectors and agencies like the National Nuclear Security Administration,

[1] This report uses the label "Sunburst" for this ongoing campaign. While public reporting initially focused on SolarWinds, and the compromise of this vendor's Orion software was significant, it was just one of multiple vectors used to gain access to targeted organizations and compromise both on-premises and cloud services. As a supply-chain compromise, Sunburst is not unique; it shares common traits with, and reflects lessons unlearned from, at least seven other major software supply-chain attacks from the last decade.

illuminate the weaknesses of current US cyber strategy. The failure to detect an intrusion of this scale is evidence of how far myriad cybersecurity certification and authorization regimes lag behind real-world application. For example, SolarWinds Orion was certified by DoDIN's APL and had a plethora of other approvals. In theory, updates to software systems on the APL are carefully reviewed, but because government audits and certifications are periodic and not real-time, security cannot keep pace with evolving threats. Increased frequency and depth of software audits would have improved Sunburst's incident response, though many agencies struggle to understand and prioritize their own software portfolio.

Historical Roots of Sunburst

The staggering scope of Sunburst may overshadow the fact that there have been more than half a dozen software supply-chain attacks over the past decade similar in their methodology and intent. The main report highlights seven of these attacks. In each, the adversary stealthily infiltrated sensitive networks and accessed systems for months, if not years. The tactics used in these operations prioritized stealth not as a secondary concern but as intrinsic to their goal. Many of these operations targeted administrative and security tools because of their significant permissions and significant access to protected networks. This efficiency makes software supply chain attacks particularly compelling, and helps explain why there have been at least one hundred and thirty-eight attacks and vulnerability disclosures since 2010.

Contributing Factors to Sunburst

Though mature organizations should assume compromises to be inevitable, especially in the face of better resourced and skilled adversaries, more could have been done to faster discover and mitigate Sunburst. The issue is not that the intruders got through, rather, that they were allowed to roam freely for so long. Three main factors contributed to the wide scale and longevity of the Sunburst campaign: deficiencies in risk management, increasing reliance on hard-to-defend linchpins, and constricted policy adaptability.
Federal enterprise risk management is too heavily weighted on pure management rather than risk prioritization. Government will play a key role in software supply chain security, but its programs for preventing, detecting, and mitigating supply chain attacks are in dire need of rejuvenation.

This risk management problem is not new. In 2016, the Office of Management and Budget (OMB) issued a memorandum defining a program to identify certain federal information systems and data as High Value Assets (HVAs), for which unauthorized access could cause a significant impact to US national security. CISA's Continuous Diagnostic and Management (CDM) program was supposed to track each agency's security management configurations and supply-chain risk management programs, but there have been numerous setbacks. CDM could have been a valuable asset in preventing and responding to Sunburst. ICT supply-chain risk management practices are also woefully underdeveloped throughout the federal civilian government. Only five out of twenty-three examined agencies had full risk assessment processes. Additionally, the private sector is restrained in sharing threat information due to liability concerns. The overemphasis on prevention, rather than mitigation and response, forces government to fight an unwinnable battle without the full and necessary support of industry.

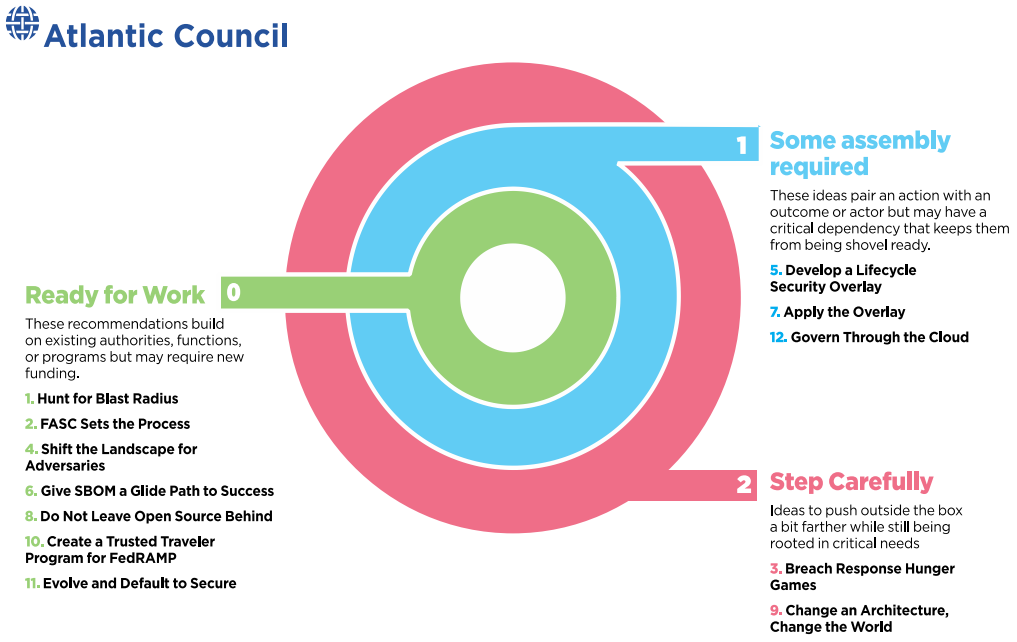
Sunburst is critically differentiated from other software supply-chain attacks by its abuse of on-premises and cloud identity and access management (IAM) services, enabling the adversary to move from local networks into users' software as a service (SaaS) environments. As cloud computing matures the security and defensibility of linchpin systems, like IAM services, become increasingly important both for users and policymakers. This implicates all cloud service providers, especially the three 'hyperscale' firms in the United States, Amazon, Microsoft, and Google. Policymakers and CSPs must do more to provide guidance and build defensible technologies. The National Security Agency's alerts on cloud configuration security and least permission practices only became public in January 2020 and February 2021, respectively,

indicating a reactive stance rather than proactive management. These issues will only multiply as more organizations transition their mission-critical workloads to the cloud.

Toward a More Competitive Cybersecurity Strategy

Government and industry can learn from this incident, but these systemic risks can only be addressed by pursuing speed, balance, and concentrated action in a revised cybersecurity strategy. The United States should work to adopt strategy of persistent "flow." Government must maintain balance whilst anticipating its adversaries' moves and seeking points of strategic leverage. Defensive and offensive activities need to be better tied together and policy must seek to enable defenders to move faster and with greater concentration to the point of action against an evolving risk landscape. In this constant flow of activity, security relies on seeking and maintaining initiative in a dynamic conflict environment, even as conditions and adversary positions change rapidly.

The existing federal policy architecture is crowded and confusing; rather than being thorough, it may induce avoidable mistakes and conceal urgent issues under the burden of checkbox compliance regimes. Security regimes do not sufficiently ensure product security over a product's entire lifecycle. More importantly, existing frameworks focus too much on classifying the risks from the compromise of information, rather than on the potential blast radius of compromise. Most concerningly, evaluations across the board take too long and are too periodically reassessed. Industry must be a partner in driving these changes with both public and private stakeholders focusing on a model of operational collaboration vs. simply sharing information. The report offers three clusters of recommendations to 1) Ruthlessly Prioritize Risk, 2) Improve the Defensibility of Linchpin Software, and 3) Enhance the Adaptability of Federal Cyber Risk Management. For more on these recommendations, including anonymized comments from industry and government stakeholders, find the full report here.



The Sunburst crisis can be a catalyst for change and, while near-term reforms are practicable, change must extend beyond the security of code or shifting how the government buys technology. In an intelligence contest, tactical and operational information about an adversary—such as insight on forthcoming sanctions or the shape of a vulnerable network—is strategic leverage. The United States and its allies must acknowledge that this is a fight for that leverage and address where US strategy falls short to ensure cyberspace remains a safe, secure, and useful domain.