Ardent Insights

SolarWinds: Espionage and Exfiltration

Ardent Insights is a monthly blog series, showcasing 'actionable intelligence' on technology- and data-related risks and opportunities facing governments and the constituents they serve, especially in the realms of public safety, disaster management, national security, law enforcement, public health, and smart/resilient infrastructure and systems.

Last year was a difficult one—the Covid-19 global pandemic, economic recession, social strife, and the ever-present threats of war and climate change-accelerated natural disaster. Yet 2020 was also a milestone year for cybersecurity attacks globally. **The FBI reported a dramatic 400% increase**[1] in cyber-attacks after the onset of the pandemic, as expected with the massive online shift of work, school, and commerce. One of the largest cybersecurity breaches in history occurred during this period: **SolarWinds.** The US cybersecurity community learns more every day about the depth of this attack.

Impacting 18,000 of SolarWinds's 300,000 customers, the breach is a sprawling international cyber espionage operation that will serve as a case study for security and intelligence specialists for years to come. Enabled by the malware, now known as Sunburst, the hack epitomizes the kind of Exfiltration and Espionage (E2) attacks that will only become more common and more sophisticated as cyber becomes the preferred modus operandi of 21st Century geopolitical proxy wars.

For the uninitiated, SolarWinds (SWI) is a publicly traded, Austin-based IT infrastructure management firm that is deeply embedded in the IT management supply chain of many Fortune 500 companies and several critical government agencies. SolarWinds is known for its Orion Platform, a suite of network management, IT operations, and security products. Several of these products effectively became carriers that propagated malicious code throughout the company's network of clients, including DHS-CISA, DoD Cyber Command, DISA, NNSA, and the US Treasury Department. This attack itself has come to be known as Sunburst, Solarigate, and UNC2452.

[1] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

--

Figure 1: Known affected agencies

HOW DID THIS HAPPEN?

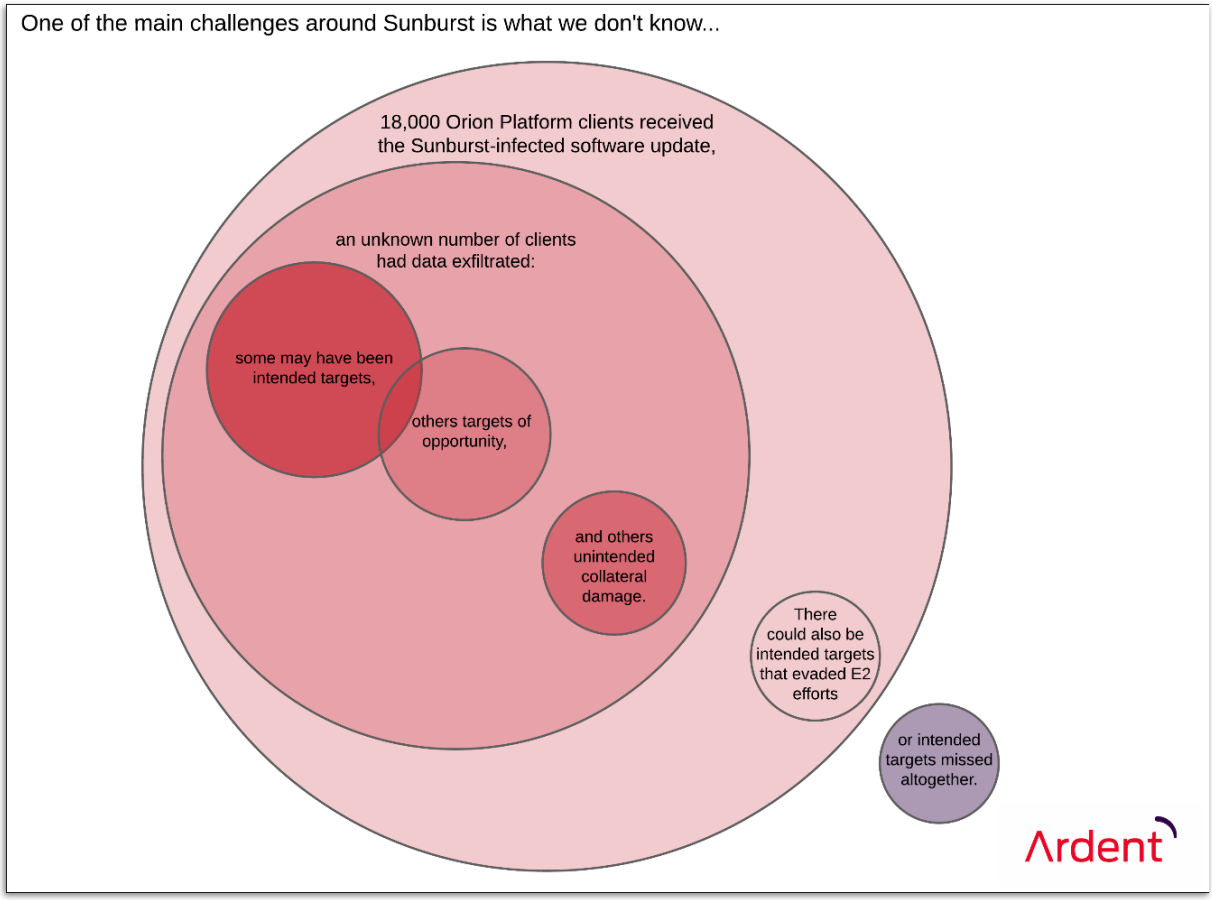
Sometime before March 2020, with evidence pointing to October 2019, hackers (likely state-sponsored Russian agents) gained access to SolarWinds's update server. In perhaps the most dramatic PSA for robust password management (or perhaps a shift towards password-less security altogether), independent security researcher Vinoth Kumar found easy access to SolarWinds's update server through the password "solarwinds123" (which was reported to the company in 2019).[2] Cyber analysts are still unsure whether this specific vulnerability led to Russian access to the server. Regardless, this demonstrates that security was lacking as hackers found their way into a key system.

After gaining access to the update server, the hackers made small tweaks to the draft code used for periodic software updates. These tweaks to the draft code were written into DLL files (dynamic-link libraries) that were then compiled into final updates before being digitally signed by SolarWinds itself. These digital signatures masked the changes, making the files appear authentic to every system that reached out for an update. These tainted updates were eventually pushed out to over 18,000 SolarWinds's clients.

The clandestine code effectively used the Orion Platform as the carrier to distribute itself, embedding access to core functions, and creating a backdoor into IT systems, including those at critical government agencies. The technique of using a less secure element of a system to gain access to a more secure element is a common tactic, an example of a Supply Chain Attack (SCA). Once delivered, the Sunburst malware acted as a Remote Access Trojan (RAT), enabling access to execute and transfer files, profile the system, reboot the machine, and disable system services.

[2] https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idUSKBN28Q07P

Figure 2: Sunburst unknown unknowns



WHY DIDN'T THEY CATCH IT?

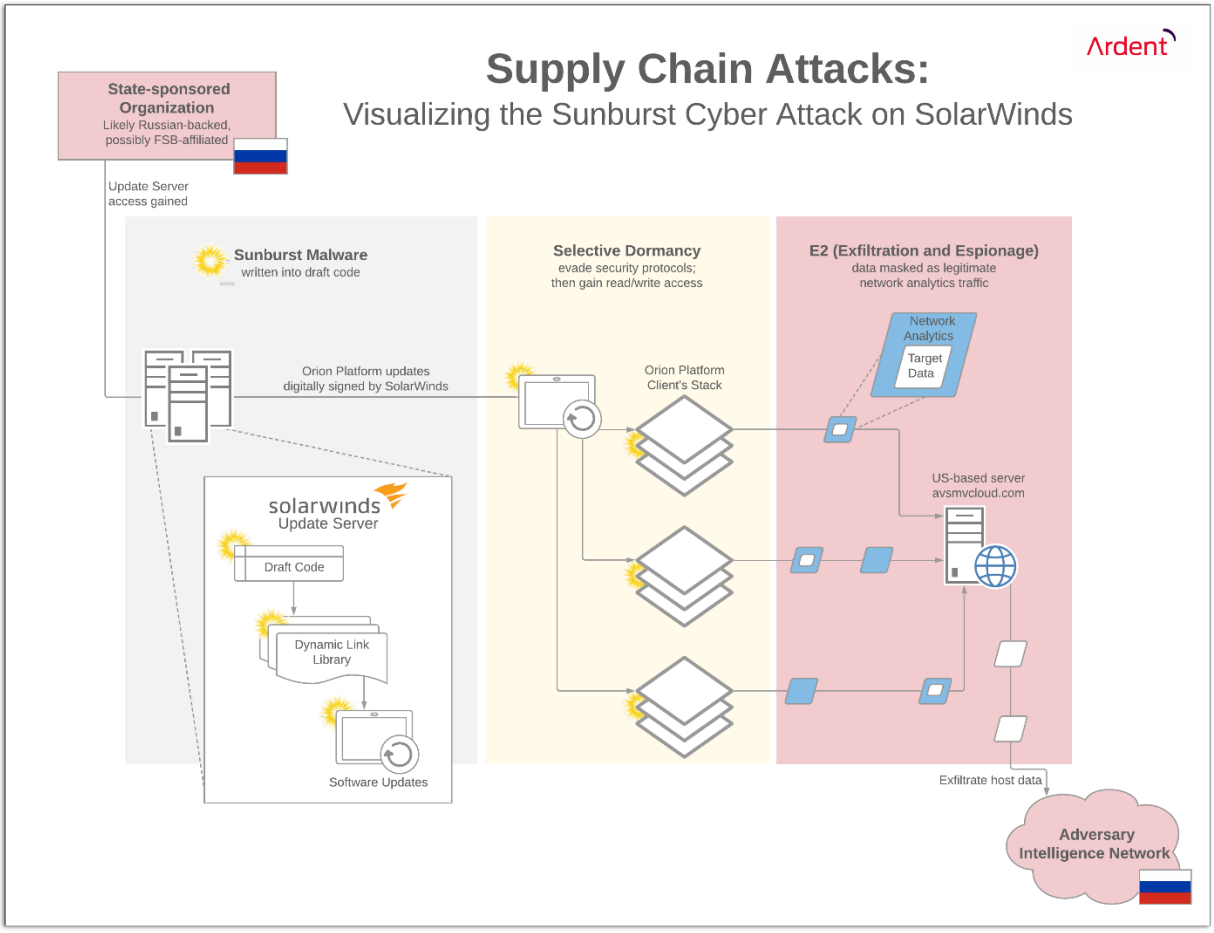
The real ingenuity behind Sunburst was that the malicious code maintained a very low profile on the system. Sophisticated in design, Sunburst intentionally minimised its footprint while testing and evading known security measures. After being embedded a client's network, Sunburst would lay dormant for two weeks to avoid arousing suspicion or triggering an active security review.

"If Sunburst sensed any security threat to itself, it would go dormant again."

After two weeks, Sunburst would activate and proceed through a detailed validation protocol using domain generation algorithms (DGAs) to test the DNS environment. It would check the domain name of the host system for key criteria, defensively evading anti-virus sandboxing, and security tools like Wireshark. Sunburst could choose to engage or not based on a variety of factors, including whether known security programs were active that could detect it. *If Sunburst sensed any security threat to itself, it would go dormant again.*

Only when it proceeded through its entire validation checklist would Sunburst begin its work and report back through data that mimicked legitimate network analytics traffic. To further obfuscate its activity, the hack's data communications were being routed first to a US-based command and control (C&C) sever using the domain avsmvcloud.com. This server was later used by FireEye (FEYE), Microsoft (MSFT), and GoDaddy (GDDY) as a kill switch to shut down the attack.

Figure 3: Sunburst distribution pathway



Sunbursts' true danger to systems comes from the access that these techniques enabled over time. The breach was clandestine, likely sponsored by Russian state actors, and remained undetected for months. These factors created what the cybersecurity community calls an "Advanced Persistence Threat" (APT). A malicious user that is able reconnoiter a network thoroughly can carry out more sophisticated and targeted espionage operations. APTs are focused on digital reconnaissance, gaining visibility of a network's internal operating environment while remaining ready to exploit any vulnerabilities. Exploiting a network could mean orchestrating second-stage attacks or direct exfiltration of data.

As more information is released, the emerging consensus amongst both US intelligence agencies and private security professionals is that Sunburst was a Russian-engineered cyber

espionage attack. Moscow-based security firm Kaspersky Lab (whose itself is banned from use by US government agencies) noted that the malware behind Sunburst looked similar to a tool called *Kazuar* used by *Turla*, a hacking group that Estonian authorities believe operates on behalf of Russia's Federal Security Service (FSB). Kaspersky detailed that similarities between the two include methods for obscuring functions, identification of victims, and the formula used to calculate the length of dormancy for the malware to avoid detection.

WHAT DOES IT MEAN?

Offensive cyber weapons, including APTs and E2s like Sunburst, are harbingers for the current age of cyber warfare. Cyber warfare itself is fast becoming the preferred domain for projecting state power in the 21st Century. As David Sanger[3] states, cyber-attack tools offer the "most inexpensive, highly destructive, highly deniable weapons" in a modern arsenal. Like insurgent tactics and terrorism, the asymmetric nature of cyber warfare favors the least networked society attacking the most networked society. Thus, open societies such as the United States, will always have more attack surfaces to defend. Or as Dr. Michael Sulmeyer[4] states, "We live in the glassiest of the glass houses."

The United States government is in the early stages of updating policies and operations that enable more fluid collaboration between the federal government, the commercial technology sector, and traditional national security and industrial base.

Sunburst and the growing list of ransomware attacks pose a fundamentally different problem vs. traditional cyberattacks. Instead of attacking US Government Agencies directly, hackers attacked a company that provides software to US government agencies. State actors have the luxury of being patient with long-term exploitation operations like Sunburst. And where one vulnerability is found to exist, organizations must assume others exist—aggressive defenses are paramount. Locating and disinfecting long-term state-sponsored APTs should become a specialized investigative skillset among America's elite cybersecurity professionals.

Beyond defensive tools to counter cyber-attacks, CISA (in concert with DHS Intelligence & Analysis, the Department of Defense US Cyber Command, and the commercial and academic cybersecurity research communities) should invest in a strategic forecasting capability to proactively identify malicious actors, emerging technical capabilities, and future attack surfaces. We understand that as with intelligence collection and analysis in any other domain, cyber domain intelligence is drowning in data…."the problem is not getting more data, but in understanding and making sense of the data" for cybersecurity operations staff, CIOs, CTOs, CDOs, and policymakers. Data science and analytics tools ranging from data visualization and business intelligence tools to more sophisticated process automation or AI/ML-based decision support models can help to greatly multiply the efficacy and

[3] National Security Correspondent and Sr. Writer, The New York Times
[4] Director for Plans and Operations for Cyber Policy in the Office of the Secretary of Defense and the former Cyber Project Director for the Belfer Center at Harvard's Kennedy School.

reach of cybersecurity research and intelligence analysts to understand and anticipate threats before they happen.

It was FireEye (FEYE) that discovered the hack in December 2020, not SolarWinds and not the government agencies that had been compromised. This is clear evidence that neither government nor the private sector can defend our networks alone. **We can only do that together—trust is essential.**

Lessons Learned

1. *The Sunburst malware is a sign of how cyberwarfare will be fought—Advanced Persistent Threats (APTs), Exfiltration and Espionage (E2)*
2. *The cyber domain will be states' preferred channel to project state power.*
3. *Modern cyber attacks are targeting SaaS vendors serving US government agencies, rather than directly targeting the agencies' networks.*
4. *If one cyber security vulnerability is found, assume others exist…hyper-vigilance is key.*
5. *Public-private cooperation, and trust, is critical.*
6. *Machines can help analysts sift through threat data more efficiently.*

Ardents Insights is a collective effort of the Ardent Data Science and Analytics Practice at ArdentMC, LLC. The team is led by Tino Dinh, ArdentMC Principal. This article was written by Andrew Terrell, Sr. Policy Consultant, and Erin Pineda, Business Consultant.