ELISITY

Sunburst Backdoor Malware

How software-defined perimeter and nano-segmentation can prevent software supply chain attacks from triggering and spreading.

CASE STUDY

DECEMBER 2020

Sunburst Global Malware Campaign

In December 2020, a global malware campaign, code named UNC24522, was discovered by cyber- security giant Fireye. This widespread effort targeted several US government agencies, critical infrastructure entities, and over 400 private sector organizations. Believed to be a state- sponsored hack, the software supply chain attack initially compromised SolarWinds Orion products of 2019.4 HF5, version 2019.4.5200.9083 or higher. However, subsequent research confirmed that the initial infection vectors were not limited to Orion products.

According to CISA public sources, "this threat posed a grave risk to the Federal Government and state, local, tribal, and territorial governments, as well as critical infrastructure entities and other private sector organizations."

This case study analyzes the malware's characteristics and investigates a direct link between its success and ineffective segmentation.

What is Sunburst?

UNC24522, commonly named "Sunburst" is a new blended threat that:

1. Is installed as a trojanized, yet securely signed, update to SolarWinds's Orion IT monitoring and management software
2. Masquerades network traffic as OIP protocol to store reconnaissance results
3. Enables the infected host to connect to a Command and Control (C&C) server via obfuscated communication to receive further commands and exfiltrate information
4. Checks for internal malware sandboxes to understand anti- forensic activities
5. Performs privilege escalations to highly privileged AD accounts - including creating valid tokens to access highly sensitive resources
6. Compromises hosts, transfer files, execute files, disable services, and impersonates users to extract sensitive identity, data, and resources.

"In the first [technique], the actors compromised on- premises components of a federated SSO infrastructure and steal the credential or private key that is used to sign SAML tokens. Using the private keys, the actors then forge trusted authentication tokens to access cloud resources."

NSA Advisory

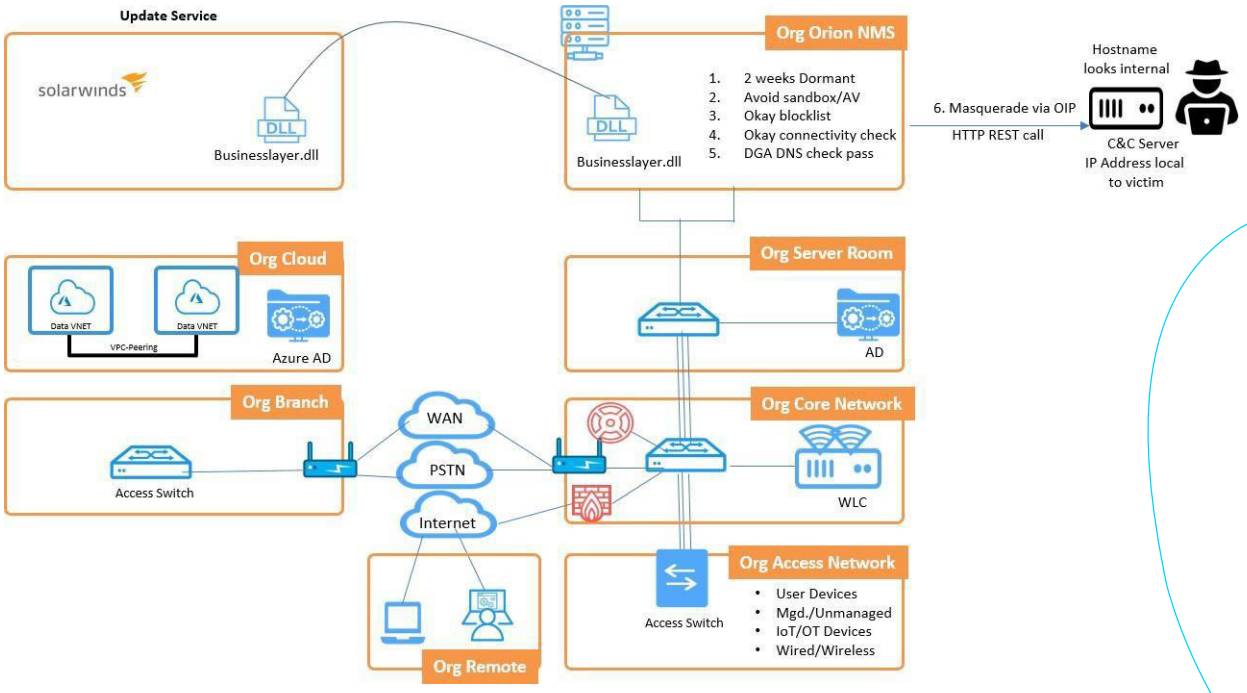

Figure 1: Sunburst multi-tiered attack framework

Multiple Deception Techniques

Sunburst uses multiple approaches to conceal itself and to complicate eradication efforts. These include using virtual private servers, often with IP addresses in the home country of the victim and using spoofed or compromised tokens for lateral movement. In addition, the malware remained hidden for several months (since at least March 2020) and spread via both known and previously unknown vulnerabilities.

While a list of comprehensive initial infection vectors is presently still being investigated, the two known vectors include:

- Compromising the software supply chain for Orion through an internal SolarWinds workstation
- Using a previously stolen secret key to generate a cookie to bypass the multi-factor authentication protecting access to SolarWinds Outlook Web Application

In the Orion case, the malware was waiting in the downloads site as an update to a plugin, which, when downloaded, remained latent for at least two weeks,and then "wakes up" to establish back-door communication to local Command and Control (C2) servers, where the hostname was set to local, and the IP address appeared to originate from the same country. Recovery efforts are expected to be measured in months of intensive effort due to lack of knowledge of the extent of each individual compromise.

Over the past 2 weeks, the scale and complexity of these Advanced Persistent Threat attacks has set a new bar for threat impact. Especially considering that on December 17, The U.S. Cybersecurity & Infrastructure Security Agency (CISA) issued an alert stating that the previously identified access vector (the compromise of Orion) was not the only attack of its kind. Regardless of the source of the attack, one thing is clear: you need to pay urgent attention to your cyber-security strategy, and should already be evaluating your potential exposures, as well as planning a response to a similar attack.

Technologies that Could Have Disrupted This Attack

Even for organizations that are not directly affected by this Sunburst attack, it's time to take stock of your current cybersecurity protections. This massive attack should serve as a warning sign, and should also demonstrate the lack of preparedness at even some of the most sophisticated organizations in the world.

So how do you best defend against these new, highly complex attacks? Let's look at a few boundary protections that could have disrupted this attack.

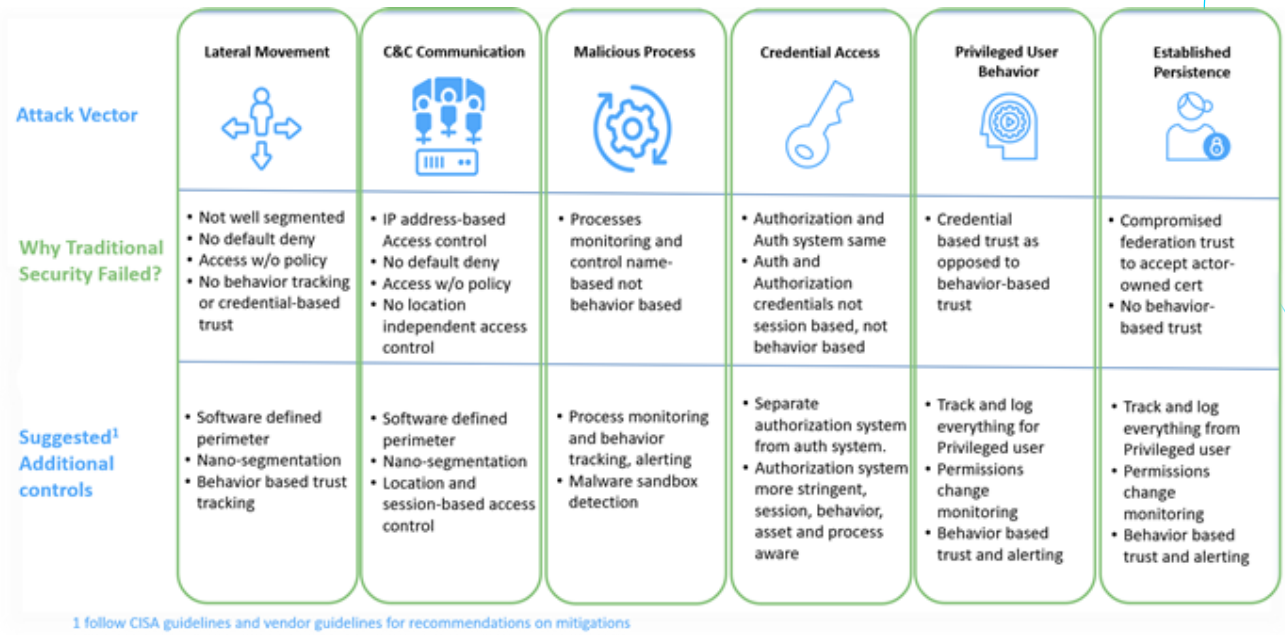

Figure 2: Traditional Security Approaches to stopping a Sunburst-like Attack

Access Control

The malware should have been blocked when it masqueraded via OIP and made a HTTP REST call to a hostname with local IP address. However, traditional IP Access control is not enough to stop these types of attacks. An identity based Zero Trust (ZT) access mechanism is required, where an explicit policy is in place for accessing any resource—both internal and external to the organization. If the malware was triggered, but unable to reach out to C2 servers, there would be an opportunity to significantly limit damage and data extraction efforts.

A Software Defined Perimeter (SDP) solution could have helped by preventing anyone outside the organization from viewing the entire network landscape. SDP cloaks the network and allows access to internal resources only when there is an explicit policy configured. This solution policy, when combined with location based and session-based tracking is extremely powerful and successful in preventing unauthorized access to any systems.

In a combined nano-segmented, SDP solution, the trust is tracked based on the user behavior, as opposed to role and credentials and started to move laterally, this system would have alerted the SOC about suspicious activities, with context for immediate follow up and action.

Threat Prevention

The attacked system's process and user behavior monitoring could have detected the infected hosts and prevented the malware from spreading to other segments via known vulnerabilities. Once the behavior was detected to be deviating from the standard, and the analysis of the process is detected and analyzed in a sandbox, a just-in time dynamic identity-based policy could have been distributed and applied to further contain the malware by preventing exploitation in other areas of the network, both locally, and in connected and cloud environments.

In the Sunburst attack, the attacker compromised credential access to enumerate users and admins through the on-premise server. They gained access as a global admin or used a SAML token signing certificate to further their objective. Separating authentication systems from authorization systems - with separate token for access to session, location - is the recommended best practice. An authentication system is typically not network traffic aware, and as such is not able to observe and respond to malicious activities. What's needed is a system with more stringent, policy based access. A system that's network traffic aware, location and session aware, privileged user aware, and performs behavior tracking, can serve as an additional deterrent for attackers.

It's now clearer than ever - Authentication-based trust is no longer enough to prevent these types of attacks. Behavior based trust, or more broadly, Cognitive Trust is required to track user behavior— especially privileged user behavior. These types of systems track all privileged user activity, including escalation, policy changes, process changes, user, and asset behavior, among others, and then alert the SOC teams for appropriate actions.

The fact that the Sunburst malware successfully infected such a large number of high-level targets shows that there were insufficient security control mechanisms in place. Organizations often struggle to establish cohesiveness due to varying security characteristics, including traditional systems alongside new systems attempting to drive digital transformation in enterprises.

Fortunately, as the cyber-threats get more advanced, newer technologies such as Cognitive Trust, present opportunities to successfully deter these types of attacks and limit fallout.

ZERO TRUST. ZERO FRICTION.

Start your zero trust journey with Elisity Cognitive Trust.

Request a proof-of-concept with frictionless, non-disruptive deployment of the Cognitive Trust platform at www.elisity.com/request-poc

> "Over the last 10 years, we have seen an increase in operational technology connecting to the corporate network, expanding the attack surface. No other vendor can provide the network visibility, telemetry, intelligence, and micro-segmentation required to effectively accelerate the time to reduce risk in both greenfield and brownfield environments."
>
> Mike Elmore
> CISO
> GSK Consumer Healthcare

> "Elisity offers a new and modern approach to protecting business-critical applications and data in the cloud and on-premises."
>
> Shamus McGillicuddy
> Vice President
> Enterprise Management Associates (EMA)

About Elisity

Elisity offers an identity-driven control plane for corporate networking and remote access without tying customers to a particular network or network security technology. Its Cognitive Trust platform, delivered as a cloud-based service, is deployed as an overlay or underlay on whatever WAN and/or SD-WAN infrastructure an enterprise prefers to protect data, users, devices, and applications. Based in San Jose, Elisity is backed by Two Bear Capital, AllegisCyber Capital, and Atlantic Bridge.

Follow on Twitter and LinkedIn or go to www.elisity.com.

www.elisity.com
info@elisity.com
sales@elisity.com

100 Century Center Ct
Suite 710
San Jose, CA 95112