SolarWinds/SUNBURST: Behavioral analytics and Collective Defense in action

ironnet.com/blog/solarwinds/sunburst-behavioral-analytics-and-collective-defense-in-action

Dec 31, 2020

Editor's note: View this post as a downloadable PDF, and read related articles Why the SolarWinds supply chain attack matters and SolarWinds/SUNBURST: DGA or DNS tunneling?

The recent widespread SolarWinds/SUNBURST hack and IronNet's initial detection of associated behaviors on May 31, 2020, highlights the need for companies, industries, and governments to work together to identify potential large-scale cyber threat activity and to take coordinated action.

Today, most companies and government agencies focus on defending themselves against potential threats, consuming huge amounts of internal resources and only sharing information sporadically with others through traditional means, including email lists and message boards.

This approach is likely to fail every time.

Why? Because individual organizations continue to battle highly capable — and highly coordinated — cyber threat actors , including nation-state and advanced criminal groups. The most effective way for private industry and individual government agencies to stand a chance against such threats, is to work together.

Organizations first need behavioral analytics that constantly look deep into individual networks and hunt for threats as they enter the network, as well as during successive stages of the attack. With those insights we can create a Collective Defense network, where individual companies share anonymized threat information in real-time and collaborate to triage and stop potential threats. This Collective Defense approach allows defenders to function on par with the attacker: hunting and fighting as a team, through knowledge sharing, crowdsourcing, and collaborative action.

Background

Cyber attacks are growing in frequency and intensity. On December 13th, news broke of a widespread network intrusions based on a software supply chain compromise of IT service provider SolarWinds. Quickly underscoring the severity of this breach, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Department of Homeland Security (DHS) released alerts, and researchers at FireEye published technical details indicating that the software supply chain compromise occurred earlier and resulted in a trojanized version of SolarWinds' Orion remote management software. This version, which FireEye dubbed SUNBURST, was distributed to SolarWinds customers between March and June.

Media reporting has attributed these compromises to threat actors associated with Russian intelligence services. This follows previous reporting attributing the FireEye breach to APT29 (aka Cozy Bear), a threat actor linked to Russia's SVR intelligence service. Media reporting indicates these threat actors were able to penetrate deep into networks for many months and were able to obtain administrative rights as well as establish legitimate-appearing credentials and points of entry. Given the scale and scope of these adversary activities, it is critical that we take action now to limit further incidents.

> The adversary will continue to modify their techniques...Their goal is to hide in the noise of normal network activities, which is why being able to detect behaviors and collaborate broadly in real time is so critical.

SUNBURST tactics, techniques, and procedures

The threat actor used several sophisticated techniques to hide command and control traffic, such as mimicking SolarWinds' Orion traffic and leveraging infrastructure providers to masquerade as trusted geolocated environments.

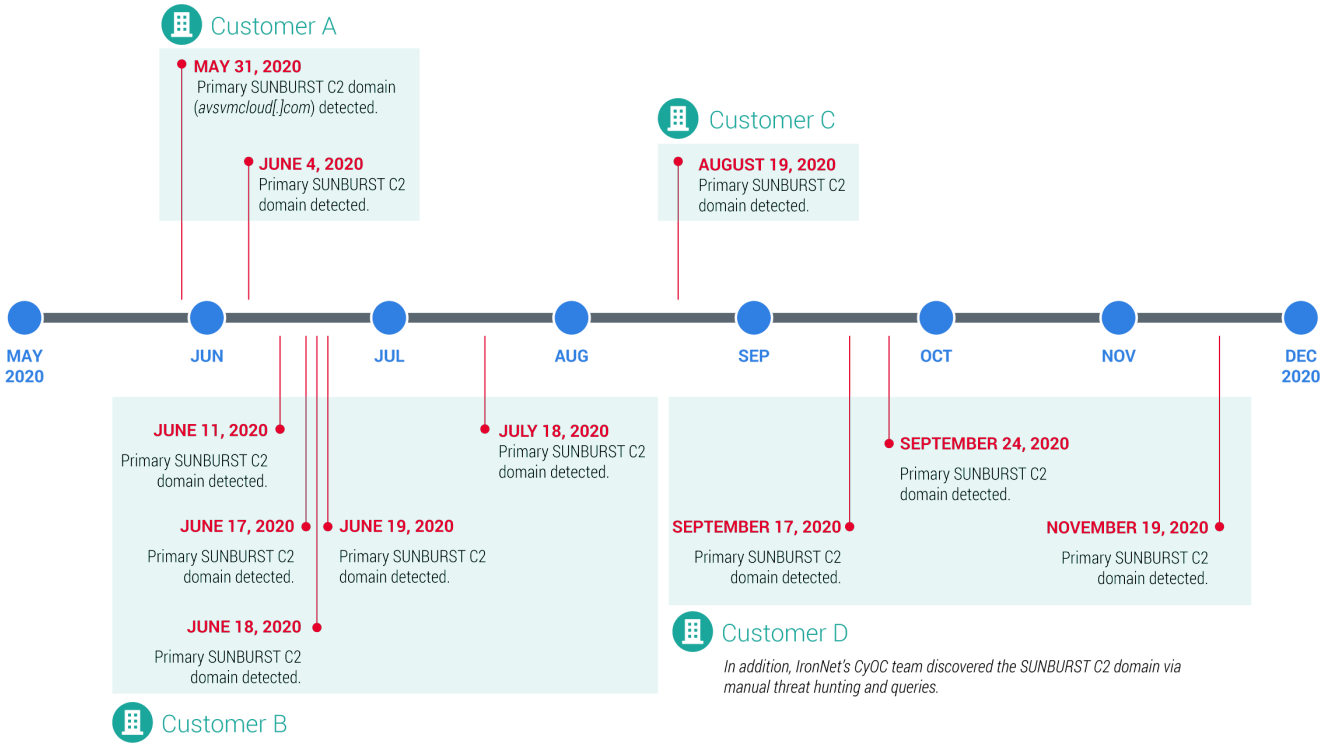
While one of the distinctive network behaviors associated with SUNBURST that has been discussed by the cybersecurity community is command and control (C2) using Domain Generation Algorithm (DGA), it is our perspective at IronNet that this behavior more closely aligns with DNS tunneling. In fact, our initial detections of the SUNBURST C2 domain in early Summer 2020 were based upon our DNS tunneling analytic.

More than 18,000 SolarWinds customers downloaded the update that had the SUNBURST backdoor and were exposed. The actor then chose a much smaller set of companies and government agencies they wanted to exploit and downloaded a second set of tools and compromised those networks.

How IronNet detected — and correlated — SUNBURST

On May 31, 2020, using the DNS tunneling analytic within IronDefense, IronNet's network detection and response solution, we first detected the initial SUNBURST behavior in near-real-time on a customer's network.

Upon detection, an alert was automatically shared into the customer's IronDefense instance and into IronDome, our Collective Defense platform, where the same behavior was subsequently detected and correlated across four customer environments spread over six months. While the significance of these alerts did not rise to an actionable level, providing our customers the ability to identify this unusual behavior propagating across multiple organizations enables them to collaborate in real time and significantly increase their ability to identify and stop the threat before it spreads. Moreover, based on our analysis and continued assessment, none of our customer networks were compromised by the second stage deployments of SolarWinds. It is our assessment that if such an attempt had been made, it likely would have been detected and actionable.



We know that in the future, the adversary will continue to modify their advanced techniques in an attempt to hide their access operations, elevate privileges, move laterally, steal data, and potentially take more aggressive action to modify or delete information. As in this case, their goal is to hide in the noise of normal network activities, which is why being able to detect behaviors and collaborate broadly in real time is so critical.

This is why IronNet was founded: We use advanced behavioral analytics and machine learning techniques to find suspicious behaviors and leverage our game-changing collective defense capability to crowdsource knowledge from our customers to help them identify new and novel threats. This allows our clients to see things others might miss, as well as to find threat actors who've already gotten in and are trying to hide.

Had a large percentage of those exposed to SolarWinds detected the behavior and been sharing information about this potential threat and collaborating on it in realtime, it is significantly more likely that the campaign would have been recognized early on.

The Call to Action

More than 18,000 companies were exposed to the SolarWinds hack. Each of those companies worked individually to protect their networks. Imagine if the security analysts for those 18,000 companies had been working together at network speed and sharing crowdsourced knowledge, leveraging their collective expertise to defend themselves, their industries, and the nation.

Now is the time to make this paradigm shift from defending in isolation to Collective Defense. In order to truly create a real-time defensive capability, we must leverage:

- Behavioral analytics to detect anomalies that are invisible to signature-based systems.
- An expert system to help us deal with false positives and work at speed.
- A flexible hunt platform for analysts to find nation state actors early on.
- A machine learning engine that correlates events across organizations and industries. For example:
    - Companies from specific industries or sectors;
    - Cross-industry collaborations, such as critical infrastructure providers;
    - Federal government organizations from different departments and agencies; and
    - Collaboration across the public and private sectors to address broad campaigns like this one.
- Sharing anonymized threat information, as appropriate, with the government to empower our national defense.

This will enable us to build the real-time radar picture of cyberspace that will allow the government and industry to work together to defend their own companies, their sectors, and the nation. This is the IronNet vision.

What IronNet customers are saying

At IronNet, we remain highly engaged with our customers as the SolarWinds/SUNBURST hack continues to unfold. This engagement goes beyond the real-time sharing and collaboration enabled by our IronDefense solution and the IronDome platform. From our executive leadership and security operations center, to our customer success team, IronNet is working closely, on a daily basis, with our customers to get them the latest on discussions taking place at the local, state, national, and international level, and gathering their feedback and input. This tight partnership with our customers is what sets IronNet apart from other security vendors and is a dynamic that we are committed to from the top down to every single employee.

Here are a few comments customers have made throughout this event:

“IronNet has the best visibility, tools, and people to support our investigation.” - Large energy utility company

“We cannot thank IronNet enough for all their support throughout this Incident.” - Large investment company

“Thanks for hunting so hard and supporting us through this investigation.” - Large banking company

“As a customer of IronNet I am proud to be able to say that we have the best network and collective defense platform to help build our internal cyber resilience.” - International financial firm

”Thank you [IronNet] for your vigilance and consultation throughout.” - Mid-sized banking company

“IronNet is a partner, not a vendor. You are the first call I make when I need support and a second set of eyes to help determine ‘what’s next’.” - Large energy utility company

“I’m really happy with the level of support [IronNet] has provided during this situation.” - Large energy utility company

For more information on how Collective Defense can provide you with greater visibility and cyber defense, view our on-demand demo or request a live demo today.

About Ironnet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Back to IronNet Blog