The SolarWinds/SUNBURST attack:

IronNet behavioral analytics and Collective Defense in action

IronNet detected the initial behavior associated with the SolarWinds/SUNBURST attack, which is still creating waves of repercussions across the public and private sectors

INCLUDED IN THIS DOCUMENT ARE:

Background and executive summary

On December 13th, news broke of a widespread series of 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 in 2020 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 well-known threat actor linked to Russia's SVR intelligence service.

SUNBURST tactics, techniques, and procedures

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

While one of the distinctive network behaviors 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. Our detections of the SUNBURST C2 domain were based upon our DNS tunneling analytic, and for that reason, we will refer to this approach throughout this analysis.

This adversary applied advanced techniques often attributed to nation-state threat actors:

- The compromise of the SolarWinds Orion update mechanism that was used to place implants greatly expanded the attacker's target landscape. A seemingly legitimate software update allowed the adversary to leverage the supply chain to distribute a backdoor software update component called a dynamic link library, or DLL.
- Once inside, the threat actor leveraged multiple techniques to move laterally through computing networks undetected by using sophisticated evasion capabilities, credential reuse, multi-factor authentication bypass, and other advanced "living off the land" techniques. CISA reports it is likely the adversary has additional initial access vectors and tactics, techniques, and procedures (TTPs) that have not yet been discovered.

How IronNet detected — and correlated — SUNBURST

On May 31, using the DNS tunneling analytic within IronDefense, IronNet's network detection and response solution, we first detected the 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, by providing our clients the ability to identify such unusual behavior propagating across multiple organizations and to collaborate in real-time, we significantly increase the ability of individual clients to identify, collaborate on, 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.

This timeline is outlined below. The attackers sought to hide their activity through the following actions:

- Using DNS tunneling as a command channel, not a data channel, which reduced overall noise and volume of the identified C2.
- Registering the domain more than a year in advance of its use and with a highly reputable domain registrar using standard paid privacy protection services.
- In addition, for the instances that IronNet observed, there was a lack of CNAME responses to DNS queries, which, based on reporting, indicates a lack of direct actions on objectives taken by the attacker.

Most importantly, this is not just another Intrusion Detection System (IDS) alert. If the attacker would have pivoted to high-interaction actions on objective and created noise in one customer environment, the rest would likely have been notified. As we saw above, advanced actors will continually seek to hide their activities, but this is where Collective Defense is the path forward for better defense. The investigation and sharing of information related to alerts in one customer aid the investigation in the rest.

This is why IronNet was founded: We use advanced behavioral analytics and machine learning techniques to find suspicious behavior and leverage our game-changing collective defense capability to crowdsource knowledge from our industry-leading clients 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 in network noise. *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 real-time, it is significantly more likely that the campaign would have been recognized early on.*

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 team and CyOC, 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 CUSTOMER

"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 CUSTOMER

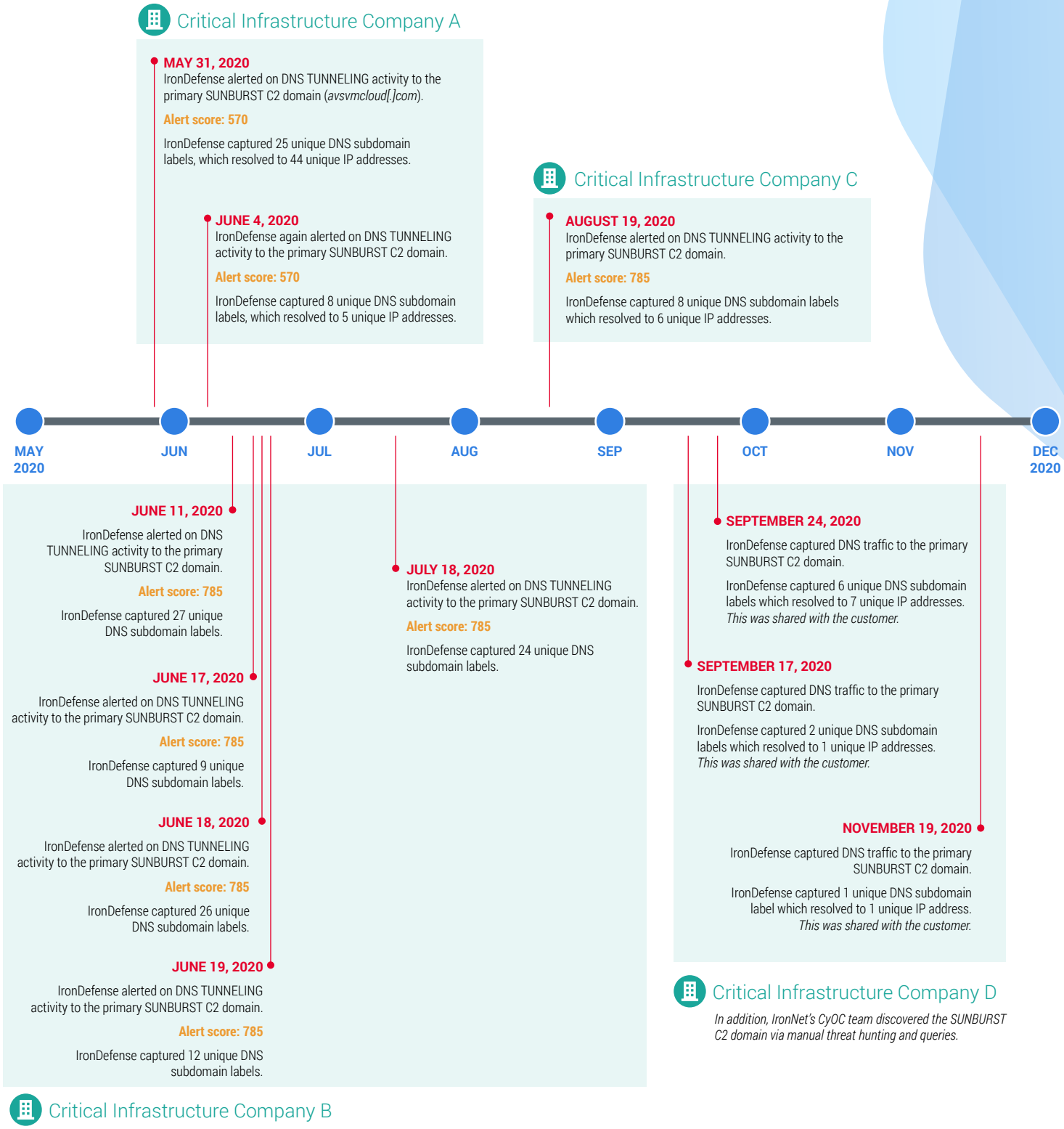
"IronNet is a partner, not a vendor. You are the first call I make when I need support and a second set of eyes to help determine 'what's next'." - LARGE ENERGY UTILITY COMPANY

"I'm really happy with the level of support [IronNet] has provided during this situation."
- LARGE ENERGY UTILITY COMPANY

Timeline of IronNet detections and correlations

Between May 31st and August 19th, IronDefense generated multiple DNS tunneling alerts across three different critical infrastructure customers. As all three customers were IronDome participants, the activity was correlated by IronDome based upon the primary SUNBURST C2 domain (avsvmcloud[.]com). IronNet hunters were also able to identify additional activity in a fourth customer based on manual threat hunting.

All of the following correlations were made within a single sector Dome. The dates and severity associated with these alerts are as follows:



IronDome Correlations

All of these alerts were correlated in IronDome. Read on for more information about what this means.

Why Collective Defense correlation matters

IronDome is where the collaboration at the heart of Collective Defense happens. When alerts from one customer's environment are shared among other members of their community (i.e., within their "dome,") all members can apply threat intelligence rules to proactively search their networks for the same behavior — threats they might not have otherwise known were present in their networks.

The combination of IronNet's Expert System rating, along with the proactive intelligence provided by the IronDome Collective Defense model, helps security operations analysts prioritize and better manage the overwhelming volume of daily alerts they face.

How we are supporting our customers

While information on this incident remains incomplete, IronNet has taken proactive steps to ensure the security of our networks and our customers. The findings described above were immediately provided to the affected customers upon discovery.

Additionally, based upon the technical details contained in multiple reports from FireEye, Volexity, and CISA, the IronNet team has taken the following actions:

- Executed five Threat Defined Queries (TDQ) in each of our monitored customer environments and our own networks to ensure no known SUNBURST or APT29-linked IOCs have been recently observed.
- Deployed multiple Threat Intelligence Rules (TIR) for the SUNBURST IOCs and historical APT29-linked IOCs as applicable and appropriate.
- Deployed multiple Suricata Rules to IronSensor for SUNBURST countermeasures released by FireEye. (FireEye-SUNBURST, FireEye-Beacon)
- Deployed Yara Signatures for SUNBURST in our ReversingLabs malware store for identification of any permutations of the two SUNBURST components, i.e., the malicious update file and the packaged DLL.
- Executed and analyzed the malicious MSP update package (SolarWinds-Core-v2019.4.5220Hotfix5.msp) and extracted DLL.
    - » Analysis and reverse engineering are ongoing.

Looking ahead

IronNet's behavioral analytics identified, alerted, and correlated on various instances of this malicious behavior from May to August 2020 with our DNS tunneling analytic.

This is important proof that IronNet's behavioral network detections and Collective Defense correlations work. Attacks like SolarWinds/SUNBURST highlight the need for more emphasis on correlated events in IronDome. For that reason, IronNet is committing dedicated resources to investigating IronDome-correlated threats to provide the most thorough and timely investigation possible.

IronNet is analyzing these behaviors and testing improvements to optimize prioritization for the future. In addition, we are looking at how we can combine multiple analytical detection techniques to increase accuracy, including assessing beaconing, anomalous file share access, or remote desktop access activity that may be related.

IronNet continues to integrate machine-based learning and behavioral analytics into our products and leverage in-house expertise and technology partners to be the best at detecting advanced threats. Real-time knowledge sharing of unknown threats can happen only with Collective Defense. As the IronDome platform collects and shares threat intelligence in real time and with situational context, members of the IronDome ecosystem can work together quickly to defend against a threat.

We are fully dedicated to advancing our Collective Defense mission to strengthen cybersecurity. We hope you will consider partnering with us to defend your network, while also contributing to the Collective Defense of sectors and the nation.

For more information on how Collective Defense can provide you with greater visibility and cyber defense please visit ironnet.com request a demo.

SUGGESTED RESOURCES:

Collective Defense: See how it works in 3 minutes

See IronNet's Collective Defense Correlation Dashboard in action

View the December 2020 IronNet threat intelligence brief