ExtraHop

SECURITY REPORT

—

Lessons Learned Investigating the SUNBURST Software Supply Chain Attack

EXECUTIVE SUMMARY

In the wake of the SolarWinds Orion SUNBURST exploit, organizations raced to understand if they had been compromised and to what extent, working around the clock to remediate the exploit before it could do further damage. But once affected SolarWinds binaries were found and patched, the real challenge began. While the exploit was first reported in December 2020, the initial intrusion is believed to have taken place months before, as early as March 2020.

To determine the full extent of the compromise, security teams needed to go back months. In the best case scenario, organizations were left to comb through what historical records they may have retained, but in many instances they were without even basic activity logs, struggling to identify the systems and timeframes on which to narrow their focus.

Unlike logs—which are often incomplete or limited in historical look back—network data can both provide real-time threat detection and capture historical data for investigation. In the case of SUNBURST, ExtraHop customers used network data from ExtraHop Reveal(x) to identify SolarWinds binaries in the environment, take rapid remediative action, and investigate the level of exposure going back to the first possible compromise.

In this report, we provide an expanded list of indicators of SUNBURST compromise as observed across affected environments protected by Reveal(x). We also share real-world examples of how organizations have used historical network data to determine whether and to what extent systems and data were compromised via SUNBURST.

TABLE OF CONTENTS

INTRODUCTION

THE SECURITY IMPLICATIONS OF A CONNECTED WORLD

——

To go forward sometimes we need to look back in time. In 2017, the NotPetya cyberattack temporarily crippled the shipping industry and many global organizations. It also revealed the depth of interdependence between global information systems. The attack started from a single stack of servers responsible for updates to a piece of common Ukrainian tax software, M.E.Doc, and used that foothold to access tens of thousands of systems around the world. Sound familiar?

Like NotPetya, the recent SolarWinds Orion SUNBURST attack exploited the software supply chain to gain access to multiple organizations with a single piece of malware. Where NotPetya was overt in its mission to wreak havoc on its targets, SUNBURST was designed to be covert, prioritizing stealth and the creation of backdoors.

What attackers intend to do with that access remains to be seen. What we do know is that the advanced defense-evasion techniques used in SUNBURST successfully bypassed most—but not all—of the security tools defenders rely on, including perimeter defenses, endpoint detection, and antivirus. Even an attack as sophisticated as SUNBURST cannot cover its tracks in network traffic.

In this report, we show how network data can be used to gain a more comprehensive understanding of the SUNBURST supply chain attack. This includes proprietary research that identified additional indications of compromise (IOCs) associated with SUNBURST. It also includes new insight into the specific attack patterns cybercriminals used to move laterally within networks, escalate privileges, and exfiltrate data. Finally, we delve into real case studies of how our customers used network detection and response (NDR) to identify affected SolarWinds binaries, forensically investigate post-compromise activity, and take swift remediative action.

Cloud Implications

Microsoft research has indicated that, after gaining a foothold, attackers then moved to gain access to cloud-based assets. Other researchers have pointed out that SolarWinds can hold cloud API keys. Large, hybrid attack surfaces pose unique challenges to understanding the extent of SUNBURST compromise.

Further complicating the investigation is the fact that the initial intrusion happened months prior. Security teams have to search backward in time, across complex (and likely hybrid) environments, to find where and when to focus deeper investigations—if evidence even still exists for that time period. This is blurring the lines between threat hunting, detection, and incident response, making it harder to answer questions like "did attackers access critical cloud infrastructure?"

Identifying SUNBURST IP Addresses With Network Data

In the immediate aftermath of the SUNBURST disclosure, ExtraHop independently researched and identified additional, previously unknown indicators of compromise (IOCs) associated with SUNBURST activity. Using a combination of OSINT tools and our own proprietary software, the ExtraHop Threat Research team compiled a list of 1700+ IP addresses associated with SUNBURST. That list was quickly shared with organizations for use in identifying IOCs shortly after SUNBURST was disclosed.

1700+ malicious IP addresses identified

REPOSITORY
The list can be accessed in the ExtraHop GitHub repository which includes a JSON file containing the suspicious IP addresses.

INSTRUCTIONS
Reveal(x) users can find instructions for searching their network history for these suspicious IP addresses in this blog.

Increase in Suspicious Activity Detected During the SUNBURST Attack

The attackers took great pains to evade all known methods of detection, but inside the network, there were indicators. The following chart shows the threat activity detected—with anonymized, aggregate data from the many environments ExtraHop secures—between January 1, 2020 and December 19, 2020. Between late March and early October, detections increase by approximately 150 percent. The privacy protections ExtraHop maintains prevents this data from including destinations—it wasn't known that the increase in traffic was largely going to the same place.

150% increase in threat activity detected and visible on the network

150% Increase in Threat Activity
ExtraHop Reveal(x) observed behavior

SolarWinds Update

FireEye Notification

J F M A M J J A S O N D
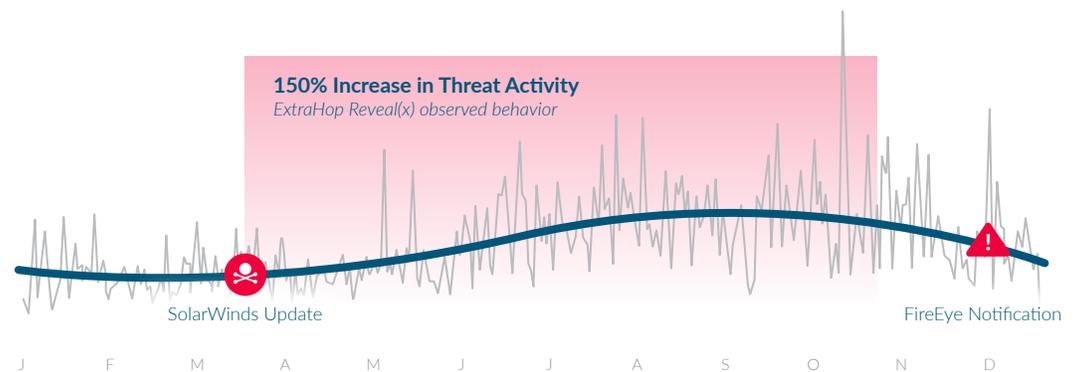
The data shows that there was a significant and suspicious change in behavior on the network. The magnitude of the increase in detections in the timeline aligns with the SUNBURST post-compromise activity at its height. It also demonstrates that the behavior of sophisticated attackers was—and is—visible on the network.

The level of stealth in this case makes attribution exceedingly difficult, but we can see the activity was there. SolarWinds is notoriously noisy, and alerts may have been ignored. Attack activity was masked, moving under the guise of a piece of trusted and legitimate software. It is difficult for anyone to know exactly what portion of the detected activity within this timeframe can be attributed to the supply chain attack. What we do know is that the behavior seen across networks was markedly different than normal.

So why were detections indicating malicious behavior like lateral movement, privilege escalation, and command and control beaconing ignored in many cases? Because the particular mechanisms of SUNBURST were designed to evade more traditional methods of security monitoring and detection, notably endpoint detection and response (EDR) and antivirus. Many organizations tried to use log and endpoint-based tools to verify the suspicious behavior they were seeing on the network. They couldn't, because SUNBURST was purpose-built to evade them. The fact that this activity was detected on the network underscores both the challenge attackers face in evading network traffic, as well as the importance of investigating significant suspicious network changes.

SUNBURST CASE STUDIES: Using Historical Network Data to Find Indicators of Compromise

From the FireEye disclosure, we know that the trojanized malware entered within a signed and legitimate software update to the SolarWinds Orion platform. Hidden within the update, it bypassed all security barriers by using the software supply chain, putting it on a fast track to objectives like the FireEye red team tools. We believe the adversaries chose SolarWinds because of the privilege it has inside the network—a position in the network that, as described in the detections discussion above, offered the attackers incredible opportunity to move laterally unnoticed.

With the initial compromise having potentially taken place months prior to the disclosure of SUNBURST, even organizations that conducted some level of investigation into earlier detections have had to comb their infrastructure to discover whether (and where) they have been compromised—sifting through logs and hiring expensive incident response firms to do investigations. Subsequent investigations solely relying on logs have proven exceptionally difficult.

The following case studies delve further into the methods the SUNBURST attackers used to evade detection and examine how network data can be used to assess the extent of the compromise and take remediative action. Identifying details about the customer organizations involved have been omitted or obscured to protect their privacy.

Initial Stages of the Attack

DNS query — 1

SolarWinds Orion

IP address of C2 server — 2

DNS

HTTP Beaconing (ongoing) — 3

C2 Server running Cobalt Strike

Domain Admin Enumeration — 4

Remote Test Creation — 5

Mailbox Export — 6

7 — **Data Exfiltration**
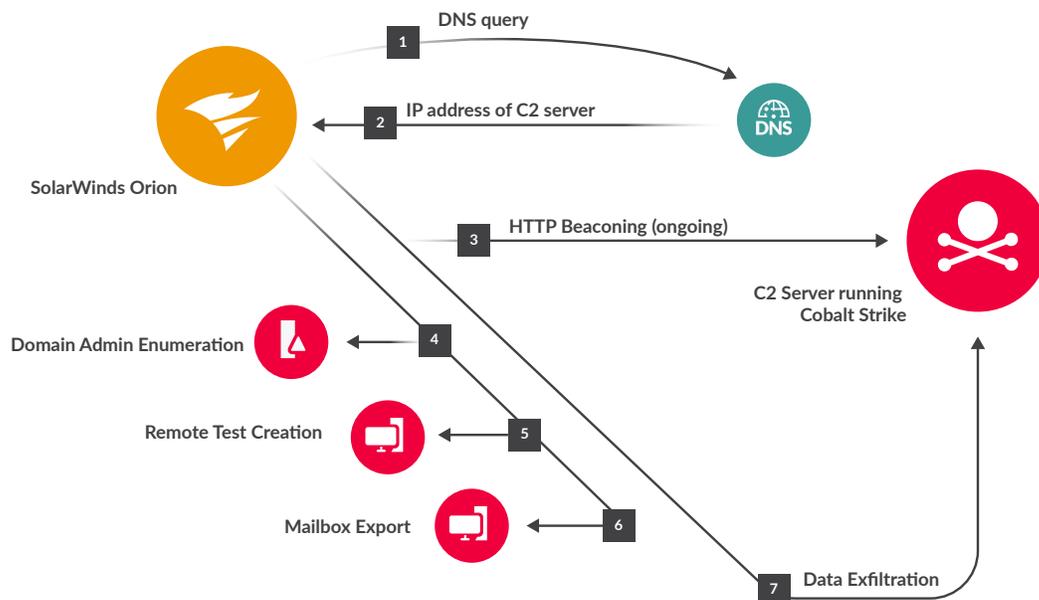
Background: Metrics-Based Investigation

For security teams, forensically investigating activity associated with impacted SolarWinds binaries was as easy as using a simple ExtraHop script to search, gather, and export data from historical metrics collected and retained by Reveal(x).

Metrics are lightweight metadata that don't contain as many details as full packets. Metrics retain pertinent information but require less storage capacity and can therefore be retained for longer periods of time. Metrics help identify what devices or systems have been accessed and can be used to build a shortlist of endpoints on which to begin investigation. In the case of SUNBURST, metrics provided—among other things—a list of connections with suspicious IP addresses, many of which were associated with the earlier detections described above.

Reveal(x) makes it possible to store more detailed network transaction records, with options for packet capture and retaining in-depth records longer using cloud records. However, in many circumstances metrics provide a good balance between the needs for efficient, cost-effective storage and data retention.

Financial Services Organization Investigates Where SolarWinds is Running

FINANCIAL SERVICES

Built over the span of years and managed in organizational silos, enterprise environments are complex, making them difficult to understand—and defend.

This large financial services organization had a complex, sprawling infrastructure which made investigating SUNBURST a huge undertaking. Log-based investigation methods would eat up the time and focus of not only the security team, but other operational teams as well. If they discovered widespread compromise in their environment, the costs in time and potential regulatory fallout would be enormous. They knew that they had two servers running SolarWinds that had received the version update, but they wanted a clearer picture of the situation so they called in ExtraHop to help.

The team quickly analyzed the network metadata they had stored going back to late 2019 and discovered numerous connections to suspicious IP addresses. In the process, they uncovered two additional servers they were not aware had been running SolarWinds. Both of the previously unknown servers had called out to suspicious domains.

They now had specific hosts and a timeframe for the potential compromise, enabling them to narrow down their search for further evidence of suspicious activity. They next discovered some CIFS and RPC activity that suggested an attacker might be attempting to gain deeper access to their systems.

The threat hunt was on, with the priority being their Active Directory services, authentication servers, and cloud. With reports of attackers seeking cloud access, financial organizations are placing even greater emphasis on securing their cloud environments.

Financial organizations have a high bar for reporting whether they've been compromised and what data may have been taken. They have experienced especially intense scrutiny around SUNBURST. Access to historical network data deep into the past helped to fast track this investigation, uncovering additional vulnerable servers and allowing them to meet reporting requirements.

Large Healthcare Organization Zeros in on Affected Hosts in a Matter of Hours

HEALTHCARE

In a field with a well-documented talent shortage, the perennial question that plagues security practitioners is where to focus their time. When stopping a breach, every second counts.

A large healthcare organization with over 30,000 servers used Reveal(x) to uncover tens of thousands of instances where the hosts on their network communicated out to suspicious IPs.

They were then able to quickly narrow it down further to a short list of internal hosts which had connected with a suspicious IP address and just a few unique IP addresses. This was accomplished by sorting the results using the host and IP address information. That effort resulted in a more efficient prioritization to continue and dive deeper into their investigations.

Even with such a large environment, the team was able to narrow the focus of their search onto thirty-seven hosts within hours. This is a task which would otherwise have taken days, if not weeks, to uncover.

Two hosts in particular stood out, both of which were mail servers handling email with their healthcare customers. They focused on those servers because they were able to exclude many of the IP addresses they uncovered: those identified as the hardcoded ones used to command the malware to start or stop beaconing, transition between active/passive mode, or to terminate itself.

When the malware initially landed in environments, it would engage in some automatic behaviors like checking in with the command and control servers. Those hardcoded behaviors were automatic—they happened in any environment that downloaded the compromised SolarWinds update. Of greater concern for security was whether attackers had actively taken any steps to gain further access.

The mail servers weren't communicating with known hardcoded IP addresses. They needed to be investigated quickly to determine whether next steps were warranted. NDR helped this organization quickly identify the activity on these servers so they could secure their environment.

ExtraHop

Finding and Preserving Evidence in a Government Agency

GOVERNMENT

Government agencies work with high-sensitivity data and are subject to strict compliance, requiring meticulous investigations in the event of a compromise. The presence of evidence is paramount to determining and reporting on exactly what happened to result in the compromise.

For one government agency, enough time had passed since the initial compromise that many of their traditional means of discovering IOCs no longer stored data from the relevant time period. However, they were able to use their network metadata to find the indicators necessary to guide deeper investigation. It told them where they needed to take a close look, saving them hours or days of potential investigation time.

That investigation validated the benefits of longer historical lookback for network metadata. They realized it was evidence in itself and needed to be preserved. They worked with ExtraHop to save those historical records and expand their storage capacity to extend the range of their lookback and keep more data for longer.
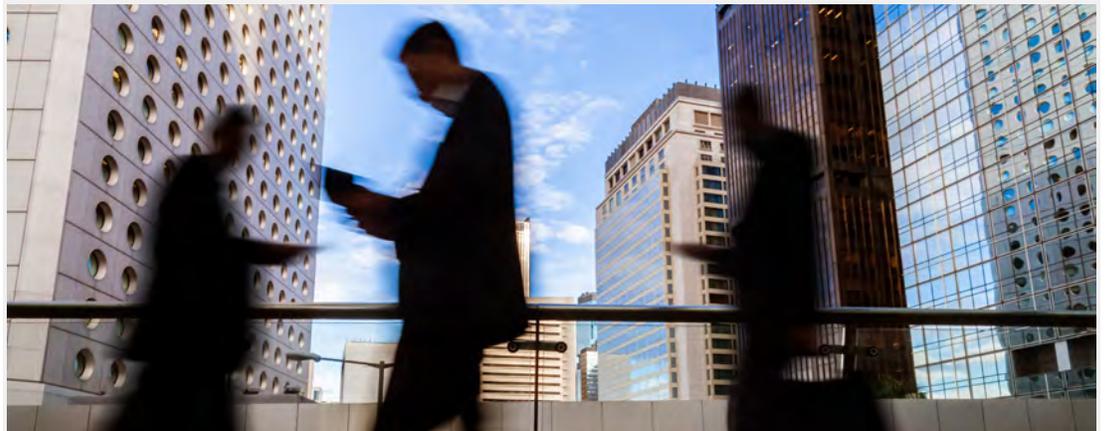
Manufacturing Company Taps Network Records as a Powerful Tool for Discovering IOCs

MANUFACTURING

In many organizations, IT Ops is responsible for monitoring the network—but for performance issues, not security. Savvy organizations know that network visibility can be used for both.

A manufacturing company had been monitoring network traffic, primarily to help them optimize performance. They were already using agent-based EDR, logs, and their next-gen firewall (NGFW) to find SUNBURST-affected systems. Based on his experience using network data to identify and investigate performance issues, the IT director decided to look to the network data to see whether it could help them identify IOCs.

By looking at five months of transaction records for more than 200,000 devices, they found several previously undiscovered IOCs. Because ExtraHop retains rich network behavior records for every device connecting to network resources, they were able to quickly track down the affected SolarWinds binaries.

SUNBURST has prompted rapid, large-scale changes at many organizations. In this case, it opened a line of communication between the network and security teams. That improved alignment is a powerful boost in visibility for both teams that will likely help strengthen their security going forward.

Gaps in Log Coverage Discovered in an Infosecurity Organization

INFOSEC

In a complex environment, some data sources, like logs, can quickly become prohibitively expensive to implement and maintain. As a result, many organizations limit where they enable logging, leaving blindspots. Since every server, device, and person interacts on the network, network visibility can expose malicious behavior.

An infosecurity organization had, in an abundance of caution, asked ExtraHop to help them check their environment for SUNBURST activity even though they had already done an extensive investigation that turned up nothing. Shifting their view to the network, they got two hits.

They had already been searching their environment for any sign of SUNBURST activity, so why had they not uncovered it sooner? Their primary source of data was activity logs, which one might expect to have turned up any IOCs.

In the initial phases of SUNBURST, before it transitioned from passive to active, it communicated with its command and control server through DNS. This technique made it difficult to detect, since DNS is a noisy protocol. Its frequent traffic also means that keeping records of DNS in logs requires a lot of storage capacity, and making that data easy to sort through for investigative purposes is a nontrivial challenge as well.

Not surprisingly, this organization, like many, hadn't enabled logging on DNS. That left a blind spot that SUNBURST took advantage of. Luckily, they had DNS visibility via the network.

An example of SUNBURST DNS activity using ExtraHop's Reveal(x) Lab
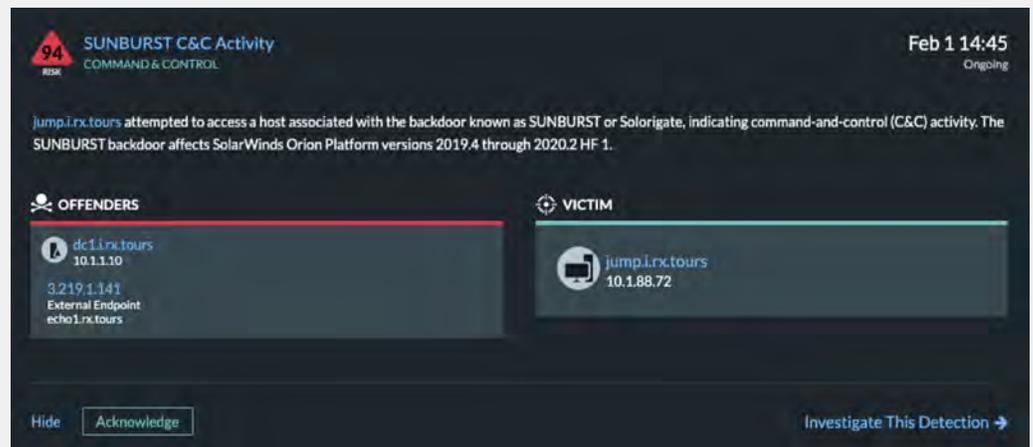
An example of SUNBURST detection on DNS activity using ExtraHop's Reveal(x) Lab

Retailer Combats Third Party Access

RETAIL

The technological supply chain is a complex web of interconnected systems. The SolarWinds backdoor attack was itself an attack on the supply chain. But the connectivity of our systems can extend even beyond the tools that we, ourselves, use. If one of the tools that your organization uses is compromised, that can also put your business at risk.

A security-minded retailer didn't have SolarWinds and used a DNS security tool. Still, they decided to turn to the network for one last check.

They only had NDR deployed in part of their network, but in those parts they were able to review data going back months. Further investigation revealed the interactions with the suspicious destination IPs were being sourced through a third-party vendor. The findings resulted in an immediate review and update of the forwarding policies, improving their overall security posture.

Conclusion

If NotPetya was viewed as a terrifying anomaly, SUNBURST must be taken as a wake-up call. Software supply chain attacks are here to stay, and they pose substantial risk to every organization. Even strong security best practices like zero trust and network segmentation aren't enough when trusted IT solutions like Solarwinds may be unmonitored or have elevated privileges. Traditional sources of security data such as logs and events leave major blind spots within modern networks. Some legacy protocols don't log at all and many devices can't be instrumented.

Advanced threats, including supply chain compromises, require heightened awareness, continuous, real-time visibility, and the ability to quickly respond to threats inside the network. Leveraging network metadata is the only way an organization can deal with the constant opacity of legacy protocols and mismatched security tools.

The SUNBURST attack worked exceptionally hard to avoid detection and spread widely. The attack was successful in disabling a long list of endpoint and other security products. If the tool could not be disabled, the malware simply stopped and moved on to other systems in that organization to expand its foothold while evading detection. But the network can't be disabled. Every single person, technology, device, and malicious actor interacts with the network—whether on premises or in the cloud. Attackers can't hide from it, nor can they determine how closely it's being watched.

When Rob Joyce, a former leader of the Tailored Access Operations unit of the NSA, gave a talk on disrupting nation-state hackers, he highlighted a source of visibility he, as a hacker, couldn't evade:

> "
> One of our worst nightmares is that out-of-band network tap that really is capturing all the data, understanding anomalous behavior that's going on, and someone's paying attention to it. You've gotta know your network. Understand your network, because we're going to.

ABOUT EXTRAHOP

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they can compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

Stop Breaches 84% Faster. **Get Started at www.extrahop.com/freetrial**

ExtraHop

info@extrahop.com
www.extrahop.com