confluera

CYBERATTACK CASE STUDY

Identifying & Intercepting UNC2452 (SolarWinds Attack)

Unprecedented Attack Unnerves Global Governments and Businesses

In December 2020, Reuters reported that monitoring products recently released by the IT company SolarWinds may have been compromised by a nation-state's sophisticated and coordinated attack[1]. While SolarWinds, along with the world's most prominent security organizations, are scrambling to identify the techniques used in the attack and respond accordingly, this security crisis has unnerved business and government leaders worldwide. How was it possible for a group of hackers to break into these systems and fly under the radar for weeks, months, or even years, despite all the possible security controls in place? With global security spend topping $120 billion[2], how are these adversaries able to carry out attack campaigns at such a massive scale?

New Scale, Common Approach

While the scope of the SolarWinds Attack is unprecedented, the approach taken is not new. Most breaches reported over the last decade show that attackers follow the same pattern — lay low and move slow. This "no-rush" approach allows them to take advantage of the most significant vulnerability in security controls: the fact that such tools only show a point-in-time view of an attacker's actions. Most security controls have been designed to win the battles against attackers, but none of them, even collectively, know how to win the war. Often when organizations lose a security battle, they initiate investigations, and, after digging deeper, discover that a war has been raging undetected. But by that time, it's too late to intercept the attacks that inflict the most damage.

Initial reports from Microsoft and FireEye suggest that UNC2452 began as early as March 2020 and went unnoticed for months. It started with an "Initial Access" attack through a malicious code injection (SUNBURST and TEARDROP malware) in SolarWinds' Orion product. The malware stayed dormant in victims' networks for two weeks and then activated, opening ingress backdoors, a "Command and Control" technique. This backdoor move enabled hackers to navigate across the network through "Discovery" and "Lateral Movement" techniques, gain elevated credentials through "Credential Access" tactics, and execute the "Exfiltrate" attack on victims' files.

The threat actors used multiple suspicious techniques and stayed dormant between making these attacks, compromising numerous hosts across the infrastructure. Since most of their actions were seen in isolation (if seen at all), the indicators of compromise visible to security teams at different points in time may not have been compelling enough to take action. This inability to see the forest through the trees is precisely where the prevailing security infrastructure is failing.

Current Solutions Are Inadequate

There have been numerous well-intentioned efforts to intercept and block cyberattacks. A case in point is the MITRE ATT&CK initiative, launched seven years ago to systematically categorize adversary behavior for attack simulation. However, simulations are simply not enough for hardening IT environments, especially since it's only possible to simulate a minuscule number of the many combinations of attack tactics used. Security leaders require predictive and holistic solutions so they can intercept their adversaries' actions before damage.

Most security controls have been designed to win the battles against attackers, but none of them, even collectively, know how to win the war.

While many security tools have evolved to become adept at identifying intrusions and point-in-time malicious activities on hosts and networks, they have little to no capability to track the progress of actors like UNC2452. Most detection and response solutions operate in a siloed fashion — endpoint platforms show host alerts while network solutions show suspicious network activity. Such reporting either gets lost in the noise of signals generated in an infrastructure of scale or requires manual investigations post-facto.

Most security controls are designed to win the battles against attackers, but none of them, even collectively, know how to win the war.

Connecting the Attack Chain

To win the war against attackers like UNC2452, leaders need a security framework that automatically connects the chain of attackers' activities across hosts and networks, irrespective of the time gap between attackers' actions. Such a security platform tracks the trail of all activities within an infrastructure across time so that detection becomes simply a matter of following the trail of compromise. This framework of execution trails, built off of system-level events across the infrastructure, enables organizations to track threat actors like UNC2452. Irrespective of how many hosts a threat actor hops over or the amount of time he or she remains dormant, such a platform can track an attack's progress and, most importantly, intercept it before it becomes a major incident.

> "Confluera helped to confirm that no indicators of compromise related to this breach had been found and enabled us to generate a report detailing our security controls and response to the SolarWinds breach."
>
> *– Director, Information Security Operations at a higher education provider*

On the Hunt, Follow the Trails

Traditional incident response involves hunting for indicators of compromise. A stealthy attacker would likely perform a clean sweep of such indicators and potentially interweave suspicious activity with legitimate actions and delays, making incident investigation an increasingly difficult task.

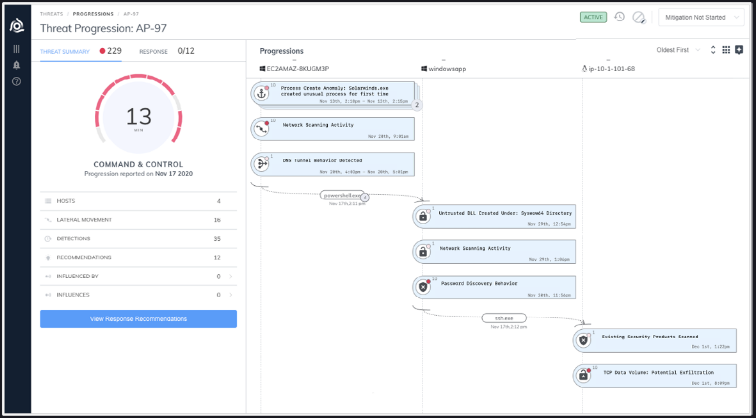
For example, creating or modifying a file or loading a dynamic link library (DLL) are high-frequency operations performed through millions of legitimate processes. Sifting through such voluminous security event data that lacks context — i.e., related events and indicators — is not only time consuming but also likely to lead security analysts astray.

Organizations need to leverage trail identifiers to eliminate this complexity and gain a big picture view of an entire attack campaign. A threat investigation may start with a typical indicator search, but when results also include trail identifiers, analysts can immediately find all related artifacts and activities, gaining a complete view of the campaign activities and timeline. Perhaps most importantly, following the attack trail in real-time allows analysts to intercept the campaign before attackers have made substantial progress.

Using Trails to Assess Attack Impact

When the news of SolarWinds attack broke, one of our customers wanted to leverage the power of trails to check if they were impacted.

We began by searching for the affected DLL and process across all systems where Confluera is deployed. The results, which were available almost instantaneously, showed the trail identifiers, which allowed us to closely look into all activities and events that were part of or related to Orion's usage. Confluera's Threat Hunting feature also allowed us to search for the presence of other indicators such as files and network connections.



Threat Progression: AP-97

THREAT SUMMARY ● 229 RESPONSE 0/12

13 MIN

COMMAND & CONTROL
Progression reported on Nov 17 2020

HOSTS	4
LATERAL MOVEMENT	16
DETECTIONS	35
RECOMMENDATIONS	12
INFLUENCED BY	0
INFLUENCES	0

EC2AMAZ-8KUGM3P
- Process Create Anomaly: Solarwinds.exe created unusual process for first time — Nov 13th, 2:10pm – Nov 13th, 2:15pm
- Network Scanning Activity — Nov 20th, 9:01am
- DNS Tunnel Behavior Detected — Nov 20th, 4:03pm – Nov 20th, 5:01pm

powershell.exe — Nov 17th,2:11 pm

windowsapp
- Untrusted DLL Created Under: Syswow64 Directory — Nov 29th, 12:54pm
- Network Scanning Activity — Nov 29th, 1:06pm
- Password Discovery Behavior — Nov 30th, 11:56pm

ssh.exe — Nov 17th,2:12 pm

ip-10-1-101-68
- Existing Security Products Scanned — Dec 1st, 1:22pm
- TCP Data Volume: Potential Exfiltration — Dec 1st, 8:09pm

Based on the investigation's results, we quickly ascertained no evidence of suspicious activity by UNC2452 was found.

About Confluera Confluera is the leading provider of Extended Detection and Response (XDR) and is the only vendor that offers real-time sequencing of various attack steps found in modern cyberattacks. Confluera's patented machine learning technology automates the tedious and error-prone task of correlating events, removes the complexity of manual analysis of multiple systems, and provides a high degree of detection accuracy not previously possible. To learn more about Confluera's award-winning solution, visit www.confluera.com.

[1] Source: Satter, Raphael. "IT Company SolarWinds Says It May Have Been Hit in 'Highly Sophisticated' Hack." Reuters, 13 Dec. 2020, Accessed 27 Jan 2021. https://www.reuters.com/article/us-usa-solarwinds-cyber/it-company-solarwinds-says-it-may-have-been-hit-in-highly-sophisticated-hack-idUSKBN28N0Y7.

[2] Source: "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020." Gartner. 17 June 2020. Accessed 27 20 2021. https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem