MANDIANT

EBOOK

NAVIGATING THE UNC2452 INTRUSION CAMPAIGN

A brief for executives and board members

Introduction

In December 2020, FireEye was the first company to discover and report a global intrusion campaign conducted by a group of actors referred to as UNC2452. This document complements published technical threat research publications and provides a strategic perspective for CIOs, CISOs and other security professionals to consider as they respond to this intrusion campaign.

The UNC2452 Campaign in Context

The UNC2452 campaign benefits from three structural realities:

1

There are no international treaties or rules of engagement in cyber warfare. This makes it challenging for nation-states to quickly and effectively respond to campaigns within the bounds of agreed-upon norms.

2

There is limited cooperation between governments and nation-states, with no negative repercussions for attackers, who may even be government-backed.

3

Cyber crime is very lucrative, especially with the widespread adoption of unregulated financial instruments such as anonymous cryptocurrencies.

The Identity of UNC2452

The investigation is ongoing. There is no definitive answer on the identity and motivations of the actor behind this campaign. However, the group's discipline, operational security, and techniques lead us to believe it likely was a state-sponsored attack.

Such mature threat actors function like real businesses. Like any other corporation, the actor may have organizational layers, teams, stand-up meetings, project plans and even quarterly goals. They outsource work, buy tools from underground marketplaces, partner and merge with other teams and divest unprofitable assets.

These actors are generously funded and rewarded. We do not underestimate them and neither should you.

UNC2452 Campaign Overview

The scope of this supply chain attack continues to expand. Almost daily, we learn new details about the attacker toolkit, their list of victims and the motivations behind their work. The campaign appears to have begun as early as Spring 2020 and is currently ongoing. The threat actor introduced a compromise into public and private organizations' networks through the software supply chain, gaining access to victims via SolarWind's Orion IT monitoring and management software.

At this point in our investigation, we have detected this activity in multiple entities worldwide. The victims have included government, consulting, technology, healthcare, telecom, and oil and gas entities in North America, Europe, Asia, and the Middle East. There may be additional victims in other countries and verticals.

So far, observed activities point to a targeted espionage campaign, but too much remains unknown to draw definitive conclusions. We have found no indicators of extortion or financial crime by the actor. The actor used several unique malware tools like Sunburst, which does not have any connection to known ransomware.

Organizations must be resourced and prepared to continuously adapt and adjust their security programs based on emerging information. When UNC2452 leaves news headlines, organizations may become lulled into a false sense of security. Expect continued activity from this actor, as well as a new wave of copycat attacks.

You Are Likely at Risk

Given the widespread nature of the UNC2452 supply chain attack, you should assume you may be at risk. The following types of organizations are at a higher risk:

- Government organizations and institutions
- Research organizations, particularly pharmaceutical entities
- IT organizations, particularly networking and cyber security entities

Even if your organization doesn't fit into a high-risk category, you may still be or become a target.

A continuous validation of your security program, including Red Team and Purple Team assessments that emulate the tools and techniques of likely attackers, is a commonsense security practice in which you should consider engaging.

Your Action Items

First, find out whether you have been impacted.

There are two ways to do this:

- If your organization has the resources and expertise, take advantage of the many free detection, remediation and hardening tools released by the cyber security community, including the FireEye UNC2452 and Sunburst Resource Center.
- If your risk profile is high, or you have resource or expertise constraints, engage a third-party professional services organization such as Mandiant Consulting for a detailed Compromise Assessment service.

If you know you have been compromised, conduct an incident response exercise.
Many organizations turn to dedicated experts such as Mandiant Consulting for thorough, high-quality outcomes.

If you do not find signs of a compromise, stay vigilant with regular testing.
Resource your team to continuously validate your security program as more information becomes available. We anticipate new related malware types, backdoors and supply chain victims to emerge and affect your risk profile.

Red Team and Purple Team assessments are critical to continuous vigilance. You will likely find automated security validation to be indispensable.

Takeaways from the UNC2452 Campaign

Stay prepared. Attacks are constant. Breaches are inevitable.
This intrusion campaign highlighted several areas of cyber security that are likely to remain priorities in the coming months and years:

Organizations should rigorously review their supply chain security. They need to invest more resources in vendor due diligence, risk assessment and validation of secure coding and build pipeline practices. While regulations may eventually play a larger role in supply chain management, right now, individual effort matters.

Security programs need to continue to adopt modern practices such as Zero Trust Architecture, which moves defenses from static, network- based perimeters to users, assets, and resources. It is critical to protect internal networks, users and assets, as well as external ones; threats can easily move laterally and from on-premises into the cloud.

Organizations should recognize the inadequacies of legacy security practices. Cyber security spend on traditional network perimeter defenses and solutions such as virtual private networks (VPNs) will continue to experience diminishing ROI.

Visibility and observability are critical to detecting sophisticated attacks. Rich telemetry on lateral (east-west) network traffic enabled FireEye and Mandiant analysts to surface suspicious UNC2452 activity within organizational networks and assets. Monitoring data only as it entered and left the network would have been insufficient.

Security teams need to learn to lean on analytics and automation. Observing and correlating telemetry data across security controls can easily become overwhelming. To find the threats that matter, teams need usable and intuitive analytics and automation tools.

How to Prioritize Risk and Manage Your Security Budget

No organization has an unlimited security budget. Even if they did, new solutions take time to procure and deploy, and new talent, when available, takes even more time to attract and train.

To best prioritize security spend, keep in mind two timeless truths: know thyself and know thy enemy.

Identify what assets you must secure. It might be R&D data, customer information or access to finance and accounting tools. Focus budget spend around these assets and grow your defenses from there.

Learn the motivations, tactics, techniques and procedures of the threat actors most likely to target you. This will help you adapt your security program specifically to threats that you are likely to face.

If your organization needs further expertise to understand attackers and redesign your security program, threat intelligence and cyber security consulting can offer critical guidance.

Learn more at **www.Mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT