



Global Threat Intelligence Center

Monthly Threat Report

February 2021

Contents

Feature article: Fallout continues from SolarWinds' supply chain attack	03
Spotlight article: A quick look at our Cybersecurity Advisory results from 2020	05
Spotlight article: Cyber-risk struggles to retain mindshare	06
About NTT's Global Threat Intelligence Center	07



Fallout continues from SolarWinds' supply chain attack

Lead Analyst: Jeannette Dickens-Hale, Senior All-Source Threat Intelligence Analyst, Global Threat Intelligence Center, US

On 20 February 2020, SolarWinds – a company which produces a network and applications monitoring platform – suffered a cyberattack that uploaded malware into updates of its Orion platform. The malware, dubbed Sunburst, compromised the legitimate SolarWinds software update and was distributed to more than 17,000 of SolarWinds' customers in the government and private sectors.

The intrusion still remained undetected when the threat actors removed the malware from SolarWinds' system in June 2020. According to US intelligence assessments at the time of this event, very few of the 17,000 organizations targeted were actually compromised. That assessment has since changed, and cyber analysts continue to discover more details about the SolarWinds cyberattack as the investigation continues.

Recent information regarding attribution of the SolarWinds intrusion reveals that a nation-state Advanced Persistent Threat (APT) was most likely responsible for the trojanized attack. UNC2452, also known as Dark Halo, APT29, also known as Cozy Bear, and Russian threat actor Turla have been named as likely sources of the SolarWinds attack. Cozy Bear is most often linked to the SVR, the Russian foreign intelligence service, whereas Turla is usually associated with Russian intelligence service, the FSB. Based on suspected Russian hacking tools as well as Tactics, Techniques and Procedures (TTPs), analysts identified similarities between Turla's attack methods and that of the SolarWinds attack, including the types of malware used.

Sunburst, also called Solarigate, was uploaded to the SolarWinds Orion Platform using the additional Sunspot malware, which is akin to the Kazuar backdoor used in Turla cyberattacks. Kazuar shares several features with Sunburst. Kazuar and Sunburst similarities include the algorithm used to generate victim Unique Identifiers (UIDs), extensive use of the FNV-1a hash, and the sleeping algorithm used by both

backdoors. Possible reasons for these similarities might be that Sunburst was developed by the same engineers as those who developed Kazuar, if Sunburst's developers gleaned creative ideas from Kazuar's coding, or if the malware came from the same source.

In addition to Sunspot and Sunburst, a third and fourth malware have been discovered as part of SolarWinds' attack. Threat actors deployed Teardrop, a memory-based dropper, to run Cobalt Strike Beacon on victimized networks. Cobalt Strike is a penetration testing tool favored by Red Teams to access and laterally move within networks. Raindrop malware did not appear to have been deployed directly via Sunburst, yet it appears in areas on victimized networks where at least one computer has been infected with the Sunburst Trojan.

While there are similarities between the backdoors and perhaps between the groups who created them, definitive attribution has not yet been made. SolarWinds' breach and resulting fallout continue to create on-going security challenges as new attack vectors and victims are discovered. The Russian government denies any involvement in the SolarWinds trojanized supply-chain attack. Analysts must remain vigilant in their research, identify and verify, or disprove connections between Sunburst, Kazuar and the Turla Group as more attack details are ascertained.

Analysts must remain vigilant in their research to identify, verify or disprove connections.

Recommendations

Despite similarities in TTPs and malware code developed by Russian nation-state threat actors, organizations must remain highly aware of possible supply-chain attacks as the complete threat landscape and other attack vectors relative to the SolarWinds breach are still unknown. Attack details are still unfolding, including the discovery of stolen credentials as part of the SolarWinds campaign.

The Sunburst attack was highly successful and organizations with the compromised SolarWinds software update could fall into one of the following categories:

1. Customers who have not identified the infected file `solarwinds.orion.core.businesslayer.dll`, and who must patch their systems before resuming operations.
2. Customers who have identified the infected file and have determined whether it has beacons to the command-and-control (C2) `avsvmcloud[.]com`, or not. These customers must conduct extensive monitoring of their network, searching for any anomalies, harden their devices, re-install updated software and resume operations only after no other anomalies have been found.
3. Customers who have identified the infected file, have confirmed it is communicating with `avsvmcloud[.]com` and that it is communicating with a secondary C2 must assume that their network has been compromised. CISA recommends a complete rebuild of the system if the breach compromised administrative credentials, or if Security Assertion Markup Language (SAML) abuse has been identified. If communication with `avsvmcloud[.]com` abruptly ceased prior to 14 December 2020, through no action of the cybersecurity team, assume that the network has been compromised and immediately institute the company's incident response plan.

For detailed information on best practices regarding cyber incident investigation and mitigation, please see the Joint Alert on Technical Approaches to Uncovering and Remediating Malicious Activity: <https://us-cert.cisa.gov/ncas/alerts/aa20-245a>.

Do you need help with the SolarWinds attack?

We're providing enterprises and public sector agencies that believe themselves to be at risk of compromise with a free, 30-day trial of our Specialized Sensor for SolarWinds Detection and notification for AWS and Google Cloud Platform environments. [Register here](#) for the free trial and for more information on how we can help you with urgent Digital Forensics and Incident Response or ongoing Managed Security Services for supply chain security assurance to reduce risk from similar threats in the future.

References

<https://us-cert.cisa.gov/ncas/alerts/aa20-352a>

<https://us-cert.cisa.gov/ncas/alerts/aa20-245a>

<https://www.bleepingcomputer.com/news/security/sunburst-backdoor-shares-features-with-russian-apt-malware/>



We provide a free, **30-day trial** of our **Specialized Sensor for SolarWinds Detection** and notification for AWS and Google Cloud Platform environments.



A quick look at our **Cybersecurity Advisory results from 2020**

Lead Analyst: Jason Harris, Director, Cybersecurity Transformational Consulting, Global Security Delivery, US

#Spotlight 1

Part of our ongoing business includes enabling organizations to improve their use of digital technologies – to help improve the organization’s flexibility and resiliency. In this context, we’ve seen a dramatic increase in the number of organizations across all industries which have rapidly accelerated their digital transformation in 2020 due to necessity during the COVID-19 pandemic.

This transformation has primarily been focused on dramatically increasing the number of users accessing systems and sensitive data remotely. This often includes access from devices that are not corporate-owned and controlled, in order to support end-user services. This also often includes moving applications and workloads into public cloud environments in order to support sustained operations in a more dynamic environment.

Our Cybersecurity Advisory (CA) service is a consulting-led engagement which defines a score of the maturity of an organization’s security posture. The ultimate goal of an engagement is to define the current state of security maturity, as well as the target state, and help develop a plan for an organization to reach the desired maturity, and therefore operates in a way which supports secure operations in a well-defined manner.

Unfortunately, our CA benchmarking data from engagements during 2020 show that the clients that we have assessed across all industries globally are still at a low-level Security Capability Maturity of 1.45, which is considered the initial form of a security posture and falls short of standards of good practice in every industry evaluated. Most organizations also have a limited understanding of their quantitative value at risk for their key business assets, which makes it difficult to prioritize and obtain funding for security improvement projects.

However, throughout 2020, we have seen within our client base an increased focus on understanding their Security Capability Maturity and having a comprehensive Security Improvement Roadmap developed and delivered as part of their accelerated digital transformation.

It is clear that the gap between the current state maturity and the required target state maturity required for clients in all industries to meet their business risk, governance, compliance and regulatory requirements is still significant. On top of that, funding, particularly due to the financial impact of COVID-19, continues to be a real challenge.

These issues make it more important than ever that organizations make the best use of available assets – efficiency is more critical than ever. The value organizations can obtain from conducting a Quantitative Risk Analysis on their key business assets, when combined with a comprehensive Capability Maturity Review has been significantly increased, especially when mapped to appropriate compliance standards.

The combination of these three elements of information security enables the development of a truly business-aligned and prioritized security improvement roadmap. If done correctly, it can also be justified to non-IT business stakeholders using the value at risk (VaR) of key business assets as a critical aspect.

Efficiency is more critical than ever; leveraging the appropriate analysis tools and capability reviews can significantly increase the value organizations obtain from available assets.



Cyber-risk struggles to retain mindshare

Lead Analyst: Richard Thurston, Market Insights Manager, Strategy & Alliances, NTT Ltd., UK&I

Publication of the World Economic Forum's highly regarded annual [Global Risks Report](#) in January 2021 highlighted the prevalence of global short-term thinking, and some complacency regarding cybersecurity risk.

As a not-for-profit foundation, the World Economic Forum (WEF) engages business and societal leaders to shape economic and social agendas. Its report aims to reduce the impact of global risks by improving understanding and responses. It maps 35 risks in terms of likelihood and impact based on its research of global leaders and risk professionals.

Since 2012, the top perceived risks have varied significantly with economic and technological factors falling out of the top five by likelihood and impact, as climate concerns and the pandemic rose sharply into focus.

We know that technology risk has not gone away. Just over half of organizations (50.1%) rate 'cyberattacks and data fraud due to a sustained shift in working patterns' as worrisome, according to WEF. Our [2020 Intelligent Workplace Report](#) found that more than three-quarters of organizations (76.9%) find it more difficult to spot IT security or business risk brought about by distributed working.

To prevent security issues from escalating, organizational culture must evolve and engage employees in keeping cybersecurity top of mind.

Yet complacency appears to be creeping in. WEF's data shows that the perceived likelihood of cybersecurity failures (previously categorized separately as 'cyberattacks' and 'data fraud or theft') has decreased year-on-year for the last three years. The perceived likelihood of IT infrastructure breakdown has reduced markedly this year from an average likelihood to being sixth-least likely of the 35 risks.

This may seem difficult to reconcile as we know only too well the risks to critical national infrastructure as well as organizations' private networks. What is likely happening here is that service provider networks (with the latest radio, edge and core enhancements and impressive network design and contingency planning) have remained largely robust in the face of increased load during the pandemic, and there has been little in the way of mainstream media coverage to persuade business leaders otherwise. Cyberthreats themselves create absorbing headlines in a normal year, but despite a radically evolved threat landscape in the last 12 months where threat vectors have changed to take advantage of the pandemic, these headlines have frequently tumbled down the news agenda.

WEF, which harnesses global expertise through its Centre for Cybersecurity, describes cybersecurity as a national security priority, flagging [five challenges for 2021](#) including complexity, and ecosystem threats like the SolarWinds case, which was [discussed](#) by NTT's Jeannette Dickins-Hale.

Despite the latest perceptions about threats identified in the report, cybersecurity risks have increased. To prevent issues escalating because of further loss of mindshare across the workforce, organizational culture must continue to evolve and engage employees to keep cybersecurity top of mind.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets



2020 Global Threat Intelligence Report

Our 2020 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

[Download report](#)

If you haven't already, [register to receive the Monthly Threat Reports](#) directly to your inbox each month.

