Hard lessons learned: Threat intel takeaways from the community response to Solarigate

accenture.com/us-en/blogs/cyber-defense/threat-intel-takeaways-solarigate

Share

Since the December 8 FireEye announcement of an internal breach, the cybersecurity world has been beset by breaking information providing new parts to the evolving story that has affected many companies and government organizations. Today, it appears that the supply chain breach of SolarWinds is perhaps one of the largest and most sophisticated cyber intrusions ever. As 2021 begins, we find ourselves already wanting to know how we, as cyber intelligence providers, can learn from this breach and better communicate about cyber threats to our customers?

Background

As has been widely reported, it appears that SolarWinds was the initial point of compromise for FireEye and other organizations worldwide, including local and federal government agencies, information and communications technology companies, health-related and pharmaceutical organizations, and educational entities worldwide. However, as new information continues to come to light, researchers have identified likely additional infection vectors used by the same actor.

This breach is remarkable for its complexity, its targeting of U.S. national security interests, and the breadth of potential targets. The malware used is highly advanced and well-disguised with defense evasion features. Although many suspect it to be of Russian origin, to date no cyber security vendor has definitively linked the malware to a known group or previously identified malware family. Using a supply chain vendor to infect tertiary victims at scale is an increasingly popular tactic amongst advanced threat actors, with some of the most high-profile supply chain attacks including the ASUS compromise, CCleaner supply chain attack, NotPetya attack, amongst others.

What does this breach mean for cyber threat intelligence (CTI)?

The technological sophistication and the potentially enormous reach of the supply-chain tactic make the SolarWinds breach truly an industry-changing hack. Breaches this large can serve as a catalyst for change, and signs of change can already be seen in the way CTI practitioners communicate to stakeholders and customers. Specifically, this compromise has brought more teamwork across the cyber threat intel field, more sharing of behavior analytics, and a level of comfort with reporting even in the absence of definitive attribution.

<<< Start >>>

> Perhaps the most overdue change is for CTI to move away from sharing solely indicators of compromise (IOCs) to sharing behavior analytics.

<<< End >>>

These changes, some overdue, will help CTI analysts become more agile and effective at communicating intelligence with our customers in five ways:

1. **Ensure proactive threat hunting and integration with endpoint detection and response (EDR) services** to inform the analytic process and include threat hunting behavior analytics in the final product.
2. **Fuse intelligence into incident response procedures** to advise and identify the most damaging threats, vulnerabilities, and active compromises in victim networks and, conversely, **feed incident response data into threat intelligence platforms** to inform wider compromise implications.
3. **Increase timeliness in reporting** so customers can stay ahead of the game. Reducing the requirement to attribute threat activity, while also working more closely with intelligence partners will shorten the analytic production timeline.
4. **Understand the full attacker lifecycle** by ensuring that threat investigators place equal effort in pinpointing the initial attack vector as they place in malware identification and remediation.

5. **Expand the CTI customer base** by demonstrating that threat intelligence can benefit governance, risk, and compliance offices and acquisition units within organizations in addition to their IT departments. Companies can deter and quickly mitigate cyber threats, particularly supply chain attacks, with a whole-of-business awareness of the threats and required responses.

Behavior analytic sharing

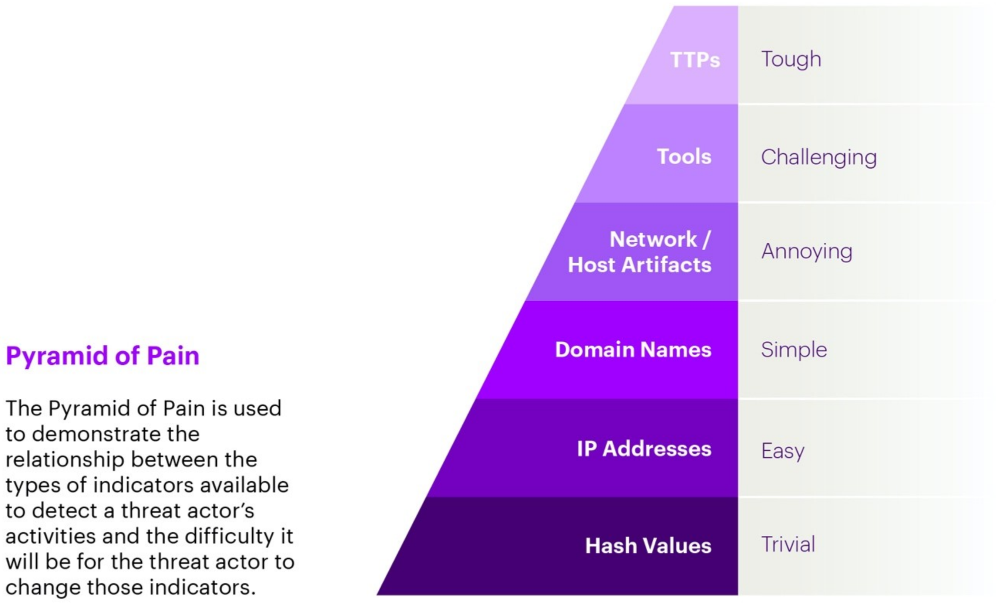
Perhaps the most overdue change is for CTI to move away from sharing solely indicators of compromise (IOCs) to sharing behavior analytics. As observed in some of the leading analysis by FireEye, Microsoft, and others, intelligence vendors are sharing behavior detections. Monitoring for threat activity solely based on IOCs fails to detect novel campaigns such as the SolarWinds supply chain breaches.

Behavioral analytics speaks to the threat actor’s tactics, techniques, and procedures (TTPs) and is the most difficult for a threat actor to change from one victim to the next. Thus, they appear at the highest level of the Pyramid of Pain hierarchy conceptualized by David J. Bianco. In contrast, threat actors can easily change the hash values of their malware and can vary their C2 infrastructure making it difficult for defenders to stay ahead of their antics if only monitoring for IOCs. For example, within the SolarWinds investigation, Accenture CTI has observed several different hash values of the TEARDROP malware where the malware code was identical except some samples had null bytes added into the code, demonstrating how easily threat actors can change these indicators.

At a level of abstraction above IOCs, threat actors can change their toolset, which is more difficult to do but will stave off defenders looking for tool reuse. Despite this, there are often similar artifacts between tools that allow researchers to attribute it.

Pushing the CTI industry towards sharing actionable detection opportunities based on attacker TTPs is a more resilient approach to detecting advanced attackers.

<<< Start >>>



Pyramid of Pain

The Pyramid of Pain is used to demonstrate the relationship between the types of indicators available to detect a threat actor's activities and the difficulty it will be for the threat actor to change those indicators.

Based on Pyramid of Pain by David J. Bianco. Graphic by Accenture.

<<< End >>>

T.E.A.M. (together everyone achieves more)

The SolarWinds breach exemplifies the benefit of intelligence sharing and building industry partnerships. Beginning with the initial announcement by FireEye and followed quickly by blogs by Microsoft and others, public and private entities were teaming together to identify and disrupt the breach.

These partnerships go beyond what has been publicly disclosed, with intelligence sharing conversations amongst stakeholders throughout the industry happening daily. Formal partnerships and informal partnerships have ensured customers are getting the latest intelligence and indicators of compromise. These partnerships are evident in the constant flow of security vendor blogs – each adding a piece to the puzzle. Intelligence partnering and transparent information sharing is demonstrating that the cyber defense industry is greater than the sum of its parts.

Within organizations, teamwork across multiple teams – from CTI, to Incident Response, to endpoint detection and response (EDR) services – is enabling cyber threat analysts to provide customers with timely and actionable intelligence. Building upon the behavior analytics sharing, practitioners can recommend immediate actions that customers can take to mitigate and begin to remediate the risk. Within Accenture, we take a team approach to providing mitigations – giving organizations short-, medium-, and long-term suggestions aimed at benefitting our customers' governance, risk, and compliance (GRC), IT, and acquisition departments.

A change to attribution

A final insight of the SolarWinds response is a move away from definitively attributing the compromise to a known threat group prior to reporting on it. Eliminating the requirement to attribute threat activity allows intelligence analysts to get the vital information into stakeholders' hands as quickly as possible. Analysts can focus on getting technical details with concrete detection or mitigation recommendations out quickly while spending dedicated time after the initial publication on determining attribution.

In the past, CTI has largely focused on grouping threat activity and attributing it to a specific known nation-state or defined espionage or criminal threat group. However, attribution to an identifiable group is increasingly difficult.

With the commodification of tools, more and more groups are using the same tools - whether open-source tools or utilities inherent to the operating system. Threat actors, particularly advanced actors, are also more deftly removing signs of their custom malware and presence in a network. This makes it difficult to track a threat group by, for example, using the same custom tool across campaigns. On the other hand, individual developers likely take their tools with them as they change teams or may work as contractors to multiple teams, so CTI researchers can find the same tool or code overlap across multiple groups, making it difficult to distinguish the unique group attribution.

The cyber security vendor reporting related to the SolarWinds breach is proving that CTI teams can share quality threat intelligence without having direct attribution to a known, attributed threat group. Perhaps this breach will disrupt the way that CTI has adhered to attribution, instead moving intelligence past group attribution to a discussion of novel tactics and behaviors with attribution limited to the state level, rather than to specific groups.

Conclusion

As CTI teams change how they communicate intelligence to customers, the teams should also change how they collect and monitor intelligence. Instead of building intelligence requirements based on threat groups, we will define our requirements based on known malicious behaviors -- looking for evidence of a compromise through defined malicious TTPs. Identifying attacker behavior patterns allow threat hunters to track cyber attackers regardless of whether they change their tooling or infrastructure.

CTI teams monitor passive external sources as well as current triggering geopolitical events to preempt threat actor activities, fusing and contextualizing data to pass to customers to help protect their networks. Keeping a constant awareness of the most pressing issues and iteratively adjusting our collection and priorities keeps CTI at the forefront of new threat actor developments.

The Accenture Cyber Threat Intelligence (ACTI) team provides actionable and relevant threat intelligence to support decision makers. The intelligence analysis and assessments in this report are grounded in verified facts; more information on this activity is available to subscription customers on ACTI IntelGraph. IntelGraph is a proprietary next generation security intelligence platform that allows users to search, visualize, and contextualize the relationships between malicious actors, their tools and the vulnerabilities they exploit.

Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture help organizations protect their valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademark.

Alexandrea Berninger

Security Delivery Associate Manager

Alexandrea is an intelligence analyst for Accenture's Cyber Threat Intelligence team.

Follow me:

Subscribe to Accenture's Cyber Defense Blog Subscribe to Accenture's Cyber Defense Blog

Subscribe