"SolarWinds breach: Priority near-term, mid-term and long-term responses"

The Accenture Cybersecurity Forum (ACF) convened a special virtual roundtable titled: "SolarWinds breach: Priority near-term, mid-term and long-term responses," on December 21, 2020.

On December 8, 2020, US-based security firm FireEye announced it had suffered a cybersecurity breach. The initial point of compromise is now known to be the breach of SolarWinds, a supply-chain contact for FireEye and other organizations worldwide, including government agencies, universities, and software and telecommunications companies.

During this roundtable we examined the impact and implications of the SolarWinds breach. What are members' perspectives on this current breach? How are CISOs working to identify the full extent of enterprise risk exposure across the ecosystem? Given the complexity of this event, what are CISOs' near- term, mid-term and long-term priorities? Our speakers included Accenture Security subject-matter experts, peer CISOs and board members. The session was hosted by Kris Burkhardt, Accenture CISO and ACF chair.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Threat actor behavior

Cyber experts see this attack as "particularly troublesome," because it is broad-based and affects many industries. Threat actor behavior, culminating in the SolarWinds breach, was first identified in October 2019. A patch went live after what appears to be an eight-month dwell time; this indicates that the perpetrator is patient and persistent. A cybersecurity expert described the behavior: "They're nesting like a tick and preparing to attack opportunistically."

The tactics, techniques and procedures associated with this breach are consistent with the capabilities of a nation-state group. While media outlets have largely linked the activity to APT29 (AKA Cozy Bear, JACKMACKEREL), a threat group associated with the Russian government, Accenture CTI analysts have not verified the attribution.

The objectives of this threat actor behavior are to:

1) determine the risk level of their operations by the capabilities of the organizations in which they land

2) quickly achieve a secondary means of command and control of, and access to, the targeted environment.

A cybersecurity expert added: "We can't predict their intentions or their reactions, so it takes a comprehensive approach to block access."

Communications and leadership

CISOs recognize their responsibility to deliver reliable, consistent communications to the board and senior leadership, particularly during such a highly publicized cyber threat. One CISO said: "I'm spending time monitoring the news coverage that's coming in because it helps me filter and manage what senior leadership is getting from the outside and balance that with the information we're putting out."

Filtering is important given the flood of information about the breach. For example, a cybersecurity expert said: "Any information coming out of SolarWinds should be suspect, given the threat actor's carte blanche access to their environment." A CISO said: "Every vendor is trying to give me information. It's coming so fast that it's a challenge to weed through all the noise." Other CISOs have found worthwhile information from FireEye, Microsoft and the National Security Agency.

Board members and CISOs both said that the board wants to know in simple, non-technical terms:

1) What happened;

2) How is it affecting our company and the status of our environment; and

3) How will this impact our customers?

A CISO added: "It's important to talk to the board regardless of whether you have a problem or not." Checking with the CEO and/or General Counsel can ensure that communications are conducted within defined parameters.

Optimal methods for resolution

The risk posed by third parties was a commonly expressed concern. "This situation is creating a complete breakdown of trust," said a cybersecurity expert. "We'll need to see how vendors will give CISOs the appropriate level of confidence that they are not putting your enterprise at risk."

The expert encouraged CISOs to look to the National Institute of Standards and Technology (NIST) for sound third-party compliance practices and also drastically increase the immediacy of the program. "A quarterly scan is not good enough," he said. A comprehensive security plan should identify third-party risks and how to address them. "It's a lot about knowing yourself, and where

your partners have access, and how you can start to logically gerrymander those lines around your risk and your business," he said.

CISOs advocate a tiered approach to evaluating the risks posed by third parties but several said it was also important to examine second tier vendors. Threat actors will pivot laterally across the supply chain in the search for vulnerabilities. A CISO noted that most vendors will have the integrity to say whether or not they have been impacted and, hopefully, that they will continue to monitor the situation.

Suggested leading practices:

- Expect that this breach requires an enduring response posture to defend against a patient, persistent and highly skilled threat actor. "You will need long-dwell analytics to surface this kind of activity," said a cybersecurity expert.
- Confirm that systems are clean, patched when necessary, and forensically evaluated. As part of their incident response, a CISO said that old servers were quarantined to retain forensic information while new servers were built.
- Extend your efforts to endpoint detection and response.
- Strict review of the enterprise authentication fabric. Infuse cyber threat intelligence throughout the organization.
- Deploy analytics to your own software developed by the enterprise and historical data. One CISO said they conduct historical analysis of DNS logs and other data after "any new threat intel."
- As stated above, identifying trusted sources of information about the breach was another concern. A CISO said: "Every vendor is trying to give me information. It's coming so fast that it's a challenge to weed through all the noise." Other CISOs have found worthwhile information from FireEye, Microsoft and the National Security Agency.
- Compartmentalize your intelligence into the things you can take action on, and the things you'll need to discuss with the board and senior leadership.
- Prioritize the immediate patching of SolarWinds' Orion—the adversary's initial access is through Orion and then the deployment of second-stage tools. Additionally, maximize telemetry collection on any Orion-related behavior including network and file logs.
- Reduce the attack surface—"The complexity of your environment is an enemy that has to be addressed," said a CISO. One CISO said his enterprise is re-examining its entire architecture as part of a threat landscape reduction strategy.
- Be proactive in communicating with the board and senior leadership—"The board won't be happy if you come back in three months and say, 'Oh, we forgot to tell you,'" said an ACF board member. Communicate in clear, non-technical terms and focus on the issues that matter most to the board.

- Don’t waste a crisis —Addressing this threat may present opportunities to reduce the application portfolio and number of vendors and make the case for additional cybersecurity investments. This threat may also present an opportunity to drive organizational and processes changes that were resisted in the past. “Take this as an opportunity to make fundamental changes. Simple is always slightly better,” said a cybersecurity expert.
- Re-examine trust—Ask third parties what specific measures they are taking to earn your trust relative to securing key assets such as personalized identifiable information, mission-critical systems and networks.
- Look at your logs—Analyze past events in software and operating systems to detect threats. Patient threat actors may know how long records are kept so consider extending the time frames to maintain logs.

Conclusion

With the SolarWinds breach, it is clear that cybersecurity defense requires what an expert called: “An enduring response to a highly skilled threat actor that has brought its A-game.” The threat actor’s intentions can’t be predicted but the SolarWinds breach clearly presents a particularly broad and troublesome challenge across a variety of industries. A CISO added: “This experience reinforces the larger issue about how we build-in security throughout the organization. It’s broader than security risk, or technology risk, resiliency or our ability to understand. This is the future of where our profession is headed.”

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 514,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.