Questions for the Record
Senate Select Committee on Intelligence
Hearing on the Hack of U.S. Networks by a Foreign Adversary February 23, 2021

Questions for the Record for Mr. George Kurtz, President and Chief Executive Officer of CrowdStrike

[From Chairman Warner and Vice Chairman Rubio]

1. **What information, as cybersecurity firms, are you required to tell the government when looking at cyber threats? What factors influence your decisions?**

CrowdStrike protects public and private sector customers around the globe, including US Federal government agencies. These organizations receive cyber threat information via CrowdStrike's platform and threat intelligence service. The company also engages in cyber threat sharing arrangements where they do not conflict with other legal obligations, such as our customer agreements.

Some CrowdStrike customers are bound by sector-specific cyber incident or data breach reporting obligations. In these instances, CrowdStrike's offerings and service engagements provide customers with relevant information they may need to assess whether or not such notification obligations are triggered. In scenarios where there is no formal obligation to disclose incidents, customers sometimes still elect to disclose information publicly or to Government partners, and we frequently work with them to make sure such disclosures are accurate and actionable.

2. **Does the Cybersecurity Information Sharing Act of 2015 provide sufficient legal protections for the sharing of information? In what ways could it be improved?**

Advocates of cybersecurity information sharing legislation worked for years on concepts that informed the Cybersecurity Information Sharing Act of 2015. The law itself provides certain liability protections for entities that share cyber threat information. That said, many private companies still prefer not to participate in programs like the Department of Homeland Security's Automated Indicator Sharing (AIS) program, for a variety of reasons. Several issues are relevant here:

- **Availability**. There are now a variety of widely-available commercial threat intelligence solutions that provide real-time, accurate protection against cyber threats. When business groups first started advocating that Congress enact information sharing legislation in 2009-10, the state of the field was much less mature. By the time the Cybersecurity Information Sharing Act became law and the Department of Homeland Security created the Automated Indicator Sharing (AIS) program in the 2015-6 timeframe, many companies already consumed commercial threat intelligence.

- **Bi-directionality**. Some public-private sharing schemes mandate that participants provide information in order to receive information. This type of requirement seeks to address the 'free rider' problem and is a sensible requirement for schemes that involve highly sophisticated players (e.g., cybersecurity companies). However, some companies across various industries do not have the capacity to operate in reciprocal arrangements. This can be due to a lack of resources or internal sophistication in identifying and validating indicators.
- **Simplicity and actionability**. The most effective contemporary commercial cybersecurity solutions natively integrate threat intelligence, which provides two key advantages. First, it places responsibility for indicator identification/aggregation on the cybersecurity vendor(s), which often share indicators through commercial or mutual-interest-based arrangements. Second, it simplifies end-users' ability to protect their enterprises by lessening--or obviating--the need to handle raw indicators. This reduces the chances of introducing human errors that lead to distracting false positives or harmful false negatives. This approach often allows the vendor to help inform decisions around the criticality of an identified issue and, in some instances, to automate various responses. The technologies and security practices I outlined in my testimony, including XDR, threat hunting, and metrics, are built upon such innovation.
- **Scale and Context**. We believe modern cybersecurity solutions should leverage the cloud to share threat intelligence and simultaneously protect hundreds or thousands of customers across disparate industry verticals and geographies in real time. This scale would be difficult to replicate by a single government program that requires individual entities to operate as active participants. With respect to context, natively integrated intelligence solutions can allow users to immediately understand whether threat activity observed in their environment is linked to known threat actors. This empowers defenders to act with the deliberate speed needed for ever-evolving threats, a concept I outlined in my testimony.
- **IOCs vs. IOAs**. During the original push for information sharing legislation starting over 10 years ago, there were two central types of information to which organizations sought greater access. The first was contextual information. For example, an indication that there was an active campaign targeting a specific sector like water treatment facilities or the satellite communications supply chain. The second was tactics, techniques, and procedures (TTPs) or data elements like malicious file hashes or other signatures, as well as malicious domains or IP addresses, related to that malicious activity. These sorts of "indicators of compromise" (IOCs) are easily shareable between organizations.

  Today, contextual information is shared by law enforcement organizations, security vendors, and ISAC/ISAO organizations, but it's sometimes less actionable than proponents would hope. Too frequently, the lesson for defenders is that *everyone is attacking you all of the time*. This makes it difficult to adjust threat models and risk areas in response to new information.

  With respect to indicators, IOCs remain important to those defending against malicious activities, but it has become clear that they must be augmented by more subtle "Indicators of Attack" (IOAs). IOAs differ in that they characterize behaviors that, with enough specific reference cases, can be suggestive of malicious activity. For example, a

parent process spawns several child processes, one of which modifies a machine's registry, another of which writes code to disk. Depending on context, this could be part of a safe, normal, and expected business process--or a sign of a ransomware actor preparing an attack. Because of their subtle nature, IOAs are much less straightforward to share.[1]

- **Privacy**. Although various public-private information sharing arrangements include privacy commitments and/or liability protection for sharing information, it is clear that many private sector organizations maintain a cautious approach. In principle, most organizations have no concern with sharing, for example, indicators of malicious activity. In fact, they may even prefer that such information is shared with government entities. But many organizations prefer that such sharing be intermediated through a trusted third party, such as a security vendor, to reduce real or perceived issues about unauthorized disclosures, costly or disruptive follow-up engagements, and misperception about the impact of an indicator.

Information sharing is not necessarily an end goal in its own right--the point is stopping breaches and other malicious cyber activity. There is certainly a role for information sharing, but many of the technologies and strategies I detailed in my written testimony have been embraced by defenders to this end. Further, public and private sector organizations vary so widely in their roles, capacity, and security maturing that we should be skeptical of any one-size-fits-all approach to sharing.[2]

[From Senator Wyden]

3. **In your written testimony, you stated that the "threat actor took advantage of systemic weaknesses in the Windows authentication architecture," using the Golden SAML hacking technique. You also wrote that "this specific Golden SAML attack has been documented since 2017, in a sense it operates as a cloud-scale version of the Golden Ticket attack and similar identity-based attacks I originally wrote about back in 1999." Please detail your firm's efforts, prior to December 1, 2020, to:**
    a. **Urge Microsoft to fix the systemic weaknesses exploited by the Golden SAML technique;**

---

[1] Several additional complications arise with sharing IOAs. First, they may be particular to an organization's specific vantage point (e.g., endpoint solutions may provide a more textured view than, for example, perimeter solutions). Second, vendors within the same category may register IOAs, or the machine events that inform them, differently depending upon how they have instrumented the protected environment. Third, while most organizations are comfortable blocking activities based on IOCs from trusted partners (e.g., blocking traffic to and from a malicious domain), most IOA-based detections and preventions are probabilistic in nature, and organizations should use caution acting on IOAs from a different or untrusted source. Fourth, the rising abuse or misappropriation of commodity IT administration and common ecosystem tools means behaviors that are legitimate and expected in one environment may be malicious in another, and conveying that sort of detail across parties for the purpose of indicator sharing presents an operational challenge.

[2] We note a separate but related policy debate about cyber incident reporting, which this answer does not seek to address.

Since at least 2017, the Golden SAML technique has been well-known in the cybersecurity industry[3] and is the modern, cloud-scale version of authentication attacks rooted in the original Active Directory architecture. As noted in my testimony, I first wrote about Active Directory being used as an attack vector decades ago in the first edition of my book, Hacking Exposed. In subsequent editions, I addressed the threats posed by credential and token compromises, whereas an adversary's ability to obtain initial access enables them to leverage the inherent trust of Active Directory architecture to move laterally in an environment.

b. Warn your corporate and U.S. government customers about these systemic weaknesses and of the need to deploy additional defenses against the Golden SAML technique; and

Although CrowdStrike does operate a threat intelligence function that provides descriptive reports about, among other things, vulnerabilities and exploits, our primary means of delivering protection through our customers is by incorporating actionable detections into our software platform and real-time preventions according to each customer's preference. In so doing, we leverage findings from independent and industry research, threat intelligence collection, and incident response engagements.

Adversaries look to find vulnerabilities to exploit every day, and our focus is to provide technology that protects against threat actors exploiting vulnerabilities before they are known publicly. An example of this can be read in our blog which demonstrates the CrowdStrike Falcon Platform machine learning model, that was in use five months prior to the ostensible beginning of the *StellarParticle* campaign, was able to detect a malicious file leveraged by the threat actor and stop it with no prior knowledge.[4] Further, in December, CrowdStrike released a free tool to help organizations quickly and easily review excessive permissions in their Azure AD environments, help determine configuration weaknesses, and provide advice to mitigate risk.[5]

c. Protect your own IT systems from the Golden SAML technique.

While we cannot in this document disclose specifics about CrowdStrike's security architecture and controls, to include specific dates of implementation, CrowdStrike goes to great lengths to ensure the security of our internal and production environments, including our products. We reference certain aspects of our security program in a December blog post focused on software

---

3 https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

4 https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/

5 https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/

supply chain issues.[6] Further, we use our own Falcon Platform, including Falcon Identity Protection, and hunt for threats proactively across our enterprise.

###

6 https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/.