SENATE SELECT COMMITTEE ON INTELLIGENCE

George Kurtz
Co-Founder and CEO
CrowdStrike

Testimony on Cybersecurity and Supply Chain Threats

February 23, 2021

Chairman Warner, Ranking Member Rubio, and Members of the Committee, thank you for the opportunity to testify on timely cybersecurity events.

The recent campaign targeting critical software supply chains, leading to the breach of numerous organizations across industry and government, is notable due to its scope and sophistication. Nevertheless, the campaign represents an amalgamation of concepts, as well as tactics, techniques, and procedures (TTPs) we've observed adversaries using for years.

During my three decade career in cybersecurity, I have seen firsthand the evolution of adversary techniques and have been at the forefront of developing the solutions to thwart them. By the time I co-authored the original edition of Hacking Exposed in 1999, which later became the number one selling book in security, it had already been clear for some time that organizations were consistently failing to adequately defend themselves. But the problems were systemic and, despite the book's wide adoption in private sector and government security education programs and as a go-to resource in practice, they would not be solved by a book alone. Around that time I founded a cybersecurity company that focused on identification and remediation of vulnerabilities, called Foundstone. That company was later purchased by a large anti-virus vendor, for which I then became the worldwide CTO. I gained a lot of insight into how the traditional cybersecurity market was working, and I determined that, in fact, it was not working. At least, not very well.

When I co-founded CrowdStrike in 2011, it was based on a conviction that the then-dominant approaches to security were no match for adaptive and well-resourced adversaries. We set out to elevate the industry's focus from stopping malware to preventing breaches regardless of their source. To this end, from the very start we focused on unified, scalable, and multifaceted approaches to security that empower defenders against a wide range of breach vectors.

My testimony today is based on my prior and current experiences, protecting thousands of small, medium, and large organizations across the globe. While I cannot disclose certain details about any ongoing investigation, CrowdStrike's experience with sophisticated threat campaigns inform my recommendations for how we — the government and the private sector, working together — are best suited to approach this problem.

Recent Developments

I will begin by discussing our high-level findings in the supply chain compromise and what lessons we might take from it.

In mid-December, following public disclosures by multiple victims, SolarWinds engaged our professional services team to perform incident response. Although we had not worked with SolarWinds prior to this engagement, nor had they used our software in the past, our teams collaborated effectively to investigate the breach; enhance their security posture; and share actionable intelligence with the security community. With their encouragement, we continue to coordinate and share findings with customers, industry partners, and federal agencies, as appropriate.

Today, I would like to highlight a few significant capabilities this particular threat actor exhibited that were quite sophisticated, and later in my testimony I will address ways to combat these threats. Notably:

- The threat actor took advantage of systemic weaknesses in the Windows authentication architecture, allowing it to move laterally within the network, as well as between the network and the cloud, by creating false credentials, impersonating legitimate users, and bypassing multi-factor authentication.
- The threat actor modified code within the development pipeline immediately prior to the software build, the final stage before source code becomes software.
- The threat actor leveraged unique Internet Protocol (IP) addresses for command and control infrastructure for each of its victims, complicating investigations into the scope of the campaign.
- The threat actor leveraged a common encryption key to encode its malicious code and, in doing so, left fewer clues for attribution than had it used a unique method.
- The threat actor "scrubbed" the backdoor itself using a process of compiling and then decompiling the malicious code. This step, which we call *code washing*, had the effect of removing "tool marks" (clues) from which investigators could determine attribution.
- The threat actor was selective in activating the backdoors it implanted. This means that the actor actively and purposefully selected its victims from the wider universe of those who were vulnerable.

As far as scope is concerned, on Wednesday of last week, the White House noted that 18,000 organizations downloaded the malicious update, leading to known compromises of 9 federal agencies and about 100 private sector organizations.[1] Although we cannot confirm those

[1] Press Briefing, The White House, Press Secretary Jen Psaki and Deputy Nat'l Security Advisor for Cyber and Emerging Tech. Anne Neuberger (Feb. 17, 2021), https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-[...]er-and-emerging-technology-anne-neuberger-february-17-2021/.

numbers, we have no indication that would contradict this assessment, and it is consistent with what CrowdStrike has observed.

Relatedly, CrowdStrike itself may have been indirectly targeted, albeit without success, in what appears to be the same campaign. We became aware that threat actors directly targeted a third party IT reseller that managed Microsoft licenses for a number of companies, including CrowdStrike. The incident involved abnormal activity in the Microsoft Azure account the reseller uses to validate Microsoft customer licenses via API with Microsoft. However, this activity did not result in any harm to CrowdStrike, its infrastructure, or its data. Nonetheless, it is a healthy reminder that most every company and government agency employs a wide range of third party vendors, resellers, and business partners that make up its individual supply chain.

With respect to attribution, CrowdStrike refers to the *activity cluster* behind these events using the name *StellarParticle*. Members of the Committee are likely aware that we utilize a cryptonym naming convention for threat actors once we achieve a reasonably robust confidence level in our attribution.[2] For example, hacking groups associated with the People's Republic of China government are labeled as PANDAS, those associated with the Russian government as BEARS, and so on. In this case, we have yet to make such a designation based on the information available to us. We note, however, that other organizations, particularly those with access to classified intelligence, have different inputs and vantage points. In that regard, we are aware that the US Government has stated this threat actor is likely of Russian origin. While we currently are unable to corroborate that finding, we have no information to suggest it is incorrect.

Lessons for Industry & Government

Cybersecurity is an iterative process. I'd like to spend the balance of my time sharing my sense of how these events should affect cybersecurity policy and practice. Over the past few years, many within industry have begun to effectively address enterprise security. But performance is uneven, and there is much more work to be done. Areas like product security, operational technology (OT) security, and Internet of Things (IoT) security still lag behind. This campaign in particular emphasizes the need to improve two important security disciplines:

1. **Supply chain security**. An initial intrusion or data breach is not always an adversary's end goal. StellarParticle is just the latest demonstration of supply chain attacks as a threat vector. This follows a number of previous, high-impact campaigns--most notably, NotPetya in 2017 -- where the origins of attack are at the vendor-level. Fundamentally, securing the supply chain is a complex third-party partner and vendor risk management problem that spans across numerous disciplines. It demonstrates that cybersecurity is an ecosystem issue, where organizations impact one another, either for better or worse. In

[2] These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor's geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients' threat modeling process. For more detail, see: Adam Meyers, "Meet The Threat Actors: List of APTs and Adversary Groups," CrowdStrike Blog (Feb. 24, 2019), https://www.crowdstrike.com/blog/meet-the-adversaries/.

the private sector context, risk decisions should be reviewed and accepted up to the Board-level.

2. **Secure software development**. In addition to ensuring secure coding practices and adequate code review, organizations must protect their development platforms and code repositories at least as well as their enterprise environment. In practice, this means that beyond the other security concepts I am discussing today, organizations must incorporate secure implementation of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing. Fortunately, the security community has been focusing on these issues, and we commend the National Institute of Standards and Technology (NIST) for their significant and ongoing contributions to this area.

Some essential cybersecurity concepts and emerging technologies differentiate elite defenders from the pack. We encourage our customers to focus on *workload security*. Adversaries do not draw much of a distinction between targeting data on an endpoint versus a cloud environment--and defenders do so at their own peril. Legacy approaches to this problem and legacy technologies have proven ineffective time and again, with increasingly adverse impacts. Concretely, some of the keys to a strong cybersecurity posture today include:

- **Threat hunting**. We know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the kill chain. Multiple opportunities for detection help avert “silent failures” -- where a failure of security technology results in security events going completely unnoticed.

- **Speed**. We advise customers that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end. For example, during a retrospective review, a CrowdStrike machine learning model that shipped to customers in September 2019 detected with

high confidence the SUNSPOT malware, which was likely created in February 2020.[3] Leveraging these technologies is the best way to gain the initiative against adversaries.

- **Identity Protection and Authentication:** As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services multiply, enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.[4]

  Significantly, one of the most sophisticated aspects of the StellarParticle campaign was how skillfully the threat actor took advantage of architectural limitations in Microsoft's Active Directory Federation Service credentialing and authentication process. The *Golden SAML*[5] attack leveraged by StellarParticle actors allowed them to jump from customers' on-premise environments and into their cloud and cloud-applications, effectively bypassing multi-factor authentication. Although 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.

  Unfortunately, based on flaws in the authentication architecture itself, this campaign is only the latest and surely not the last of a long string of major breaches in which hackers can impersonate most anybody on a network, gain the permissions needed to perform any actions on the network, bypass multi-factor authentication entirely and, every bit as devastating as it sounds, have the ability to sign in as a compromised user no matter how many times that user resets their password. The only silver lining to the *Golden Ticket/Golden SAML* problem is that, should Microsoft address the authentication architecture limitations around Active Directory and Azure Active Directory, or shift to a different methodology entirely, a considerable threat vector would be completely eliminated from one of the world's most widely used authentication platforms. It is our every hope and, I imagine, the hope of the entire cybersecurity community either that they are able to do so or that we can move to a more community-driven approach to authentication.

---

[3] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[4] For more detail on how this concept relates to recent supply chain attacks, see Michael Sentonas, "The Imperative to Secure Identities: Key Takeaways from Recent High-Profile Breaches," CrowdStrike Blog (Dec. 15, 2020) https://www.crowdstrike.com/blog/identity-security-lesson-from-recent-high-profile-breaches/.

[5] SAML stands for Security Assertion Markup Language. For more information about how the hackers compromised SAML security tokens, see CISA Alert (AA20-352A), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations" (revised Feb. 8, 2021).

- **Zero Trust**. Due in part to many of the fundamental problems I've described about today's antiquated authentication architecture, organizations must incorporate new security protections focused on authentication. Zero Trust is a design concept that brings a holistic view of authorized identity to the enterprise. Instead of authenticating to a network or device once and having ready access to everything that's connected, users must reauthenticate or otherwise establish permission for each new device or resource they wish to access. This radically reduces or prevents lateral movement and privilege escalation during a compromise.

- **Extended Detection & Response (XDR)**. Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The XDR concept seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise. As this Committee will appreciate, XDR generates intelligence from what otherwise may be no more than an information overload.

Taken together, these concepts apply equally in commercial industry, critical infrastructure, healthcare, and government, as well as within small entities. Much more could be said about each domain, but I'll quickly address two.

First, we think the cybersecurity industry has lagged over the years in making enterprise-grade security solutions accessible to small- and medium-sized businesses. Often, adversaries specifically target smaller organizations as a means to a greater end. We are proud that a number of security companies, including CrowdStrike, are committed to offering comprehensive, easy-to-use solutions for organizations of all sizes and with varied budgets. Increasingly, even the smallest of organizations look to substitute or augment their security programs not only with state-of-the-art technologies, but also with comprehensive managed security services. Mature cybersecurity programs constantly evolve, and operate on the cutting edge of human skill and technical ability. Managed security service providers, including CrowdStrike, bring this level of capability and capacity to organizations that otherwise could not create comparable programs internally.

Second, from our perspective, there is room for improvement in Federal cybersecurity. Some of the most talented people in the field have worked or currently work in government organizations. Like us in industry, they confront adversaries daily. But in some instances, our government colleagues are hobbled by legacy technologies and programs, complex procurement processes, or compliance obligations that detract from core security work. For the Cybersecurity and Infrastructure Security Agency (CISA), new authorities to hunt across the ".gov" domain recommended by the Cyberspace Solarium Commission and granted by the FY21 National Defense Authorization Act (NDAA) could be a game-changer. Programs like the National

Cybersecurity Protection System (NCPS/"EINSTEIN") and Continuing Diagnostics and Mitigation (CDM) should be enhanced to realize this vision. And across the broader Federal government, more progress and investment can be made on IT modernization, with security as a central consideration. Finally, we support ongoing, bipartisan efforts in this Chamber to review and reform the Federal Information Security Modernization Act (FISMA).

Although I've mentioned some important, specific issues and solutions today, I'll close by encouraging the Committee to view cybersecurity holistically. Employing qualified personnel, conducting specialized training, implementing valid methodologies, strategically leveraging third-party capabilities and expertise, and having informed and involved leadership are all critical factors in a successful overarching cybersecurity risk management program. To close on a positive note, with our visibility into more than 5 trillion security events a week across thousands of customers globally, I will say that I am encouraged by the silent victories the security community experiences every second of every day. Defenders face an endless, evolving threat, but I remain optimistic that, working together, we can prevail.

I would like to thank the Committee for inviting me to testify today and for its leadership. I look forward to answering your questions.

###