TAG Cyber
Security Annual
2022
SPECIAL REPRINT EDITION

COMPREHENSIVE CLOUD PROTECTION USING SONRAI SECURITY

AN INTEVIEW WITH ERIC KEDROSKY, CISO, SONRAI SECURITY

CHINESE ATTACKS ON U.S. TECHNOLOGY: A VIEW FROM THE TRENCHES

CASE STUDY FOR ENTERPRISE: HOW NOT TO MANAGE YOUR SECURITY VENDOR PORTFOLIO

TAG CYBER DISTINGUISHED VENDOR
sonrai SECURITY

The need to reduce cyber risk has never been greater, and Sonrai Security has demonstrated excellence in this regard. The TAG Cyber analysts have selected Sonrai Security as a 2022 Distinguished Vendor, and such an award is based on merit. Enterprise teams using Sonrai Security's platform will experience world-class risk reduction. Nothing is more important in enterprise security today.

The Editors,
TAG Cyber Security Annual
www.tag-cyber.com

COMPREHENSIVE CLOUD PROTECTION USING SONRAI SECURITY
AN INTEVIEW WITH ERIC KEDROSKY, CISO, SONRAI SECURITY
3

CHINESE ATTACKS ON U.S. TECHNOLOGY: A VIEW FROM THE TRENCHES
7

CASE STUDY FOR ENTERPRISE: HOW NOT TO MANAGE YOUR SECURITY VENDOR PORTFOLIO
15

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL

©TAG CYBER 2022

TAG CYBER sonrai

AN INTEVIEW WITH ERIC KEDROSKY, CISO, SONRAI SECURITY

COMPREHENSIVE CLOUD PROTECTION USING SONRAI SECURITY

Currently, enterprises are shifting to the public cloud, offering a great promise of agility, innovation, accessibility and lower costs. These benefits come with a significant increase in responsibility to ensure that a proper range of controls are in place to protect cloud-resident data and workloads. Sonrai Security provides a holistic approach to protecting cloud deployments using a unified commercial platform.

We wanted to gain insight from the Sonrai Security team as to how this approach addressed cloud risk for their customers, and how it employs controls focused on workloads, identities and data.

TAG Cyber: What are the primary cloud risks that your solution addresses?

SONRAI SECURITY: We believe identity and data must be at the foundation of every organization's security strategy, and our platform was created specifically with this in mind. We assess the four main pillars of cloud security: platform misconfigurations; workload vulnerabilities; data-access and exposure risk; and identity risks, such as separation of duty, toxic combinations, over-privileged identities and privilege escalation. These do not work in isolation, but all influence each other. Our unique ability to tie all these pillars together—as opposed to addressing them in silos—allows businesses to view their cloud risks in context.

TAG Cyber: How does the Sonrai Security platform work?

SONRAI SECURITY: We deliver enterprise cloud security for the public cloud that other solutions miss. Powered by our cloud identity graph, Sonrai Security Dig combines workload, platform, identity and data security in one platform. Best practices, workflow, advisors and automation support cross-team cloud-security operations. Our mission is to unearth, prioritize and remove risk across every part of a customer's public cloud, by offering complete and total visibility into all compute, identity and datastore activity. We connect the dots by finding and eliminating relationships that create toxic risk, unwanted access and lateral-movement opportunities for attackers. Our graph shows every way an identity gains privilege or access to data. Customers are able to prioritize their concerns using our platform, which eliminates meaningless alerts going to the wrong teams. The platform can automatically configure security controls tailored to unique workloads based on their business impact and risk level. Finally, we help customers operationalize and remediate issues quickly with bots, workflow and team accountability.

TAG Cyber: How does your solution integrate with the on-going journey toward greater cloud adoption by most enterprise teams?

SONRAI SECURITY: Organizations choose our platform as the foundation of their cloud security operations, whether they're fully cloud or in the midst of a digital transformation. Modern app development has eviscerated traditional security controls and created unique risks that current tools can't handle. We believe that when done correctly, the cloud delivers security far better than anything possible on prem. Sonrai Security Dig was built to tackle cloud complexity, and its ability to view identity and data risk in context is at the core of our product. Cloud

means an explosion in roles and identities. As an organization's cloud footprint grows, the complexity becomes unmanageable. The cloud begs for a new method of triaging a flood of alerts, requiring cloud, security, DevOps and audit teams to unite together. Finally, cloud means a multitude of cloud accounts, roles, service principles and data stores, all of which need to be secured.

We help reveal risks companies didn't know they had, by connecting the dots between identities, data, workloads and platform, and then remediating them at the speed and scale the cloud demands. By breaking down the silos between the pillars of cloud security, organizations obtain a level of context that allows them to prioritize concerns and operationalize remediation.

TAG Cyber: Tell us more about the workload security aspect of your solution.

SONRAI SECURITY: Knowing the age, CVSS score and exploit status of business risks is not enough to prioritize the vulnerabilities in an organization's environment. Recognizing which vulnerabilities are the most dangerous to a business means understanding threats unique to the host. Detecting workload vulnerabilities is just the first step. We examine connected platform, identity and data risks to reveal the full severity of workload vulnerability. We use analytics and proprietary risk amplifiers to highlight vulnerabilities with increased concerns, including sensitive data access, and over-privileged or exposed identities that could allow for lateral movement if that vulnerability were exploited.

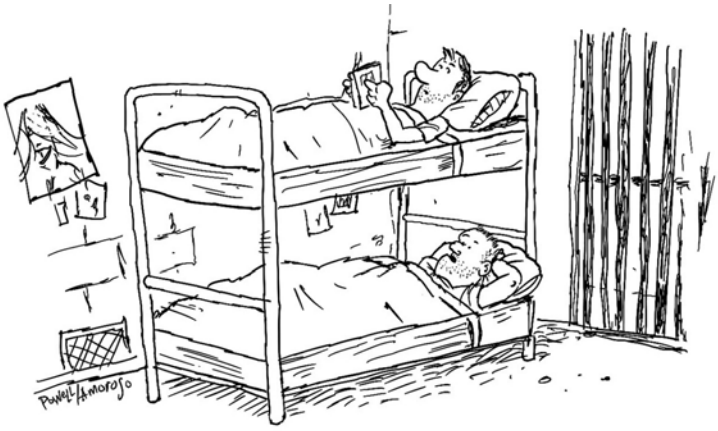
Our lightweight agentless scanner discovers a full host inventory without impacting performance or cloud spend. This helps enterprises get a clear picture of what every host is connected to, and who (or what) can access it—or already has. This allows teams to spend less time on hardening, configuration, network firewalling and micro-segmentation tasks. If a business already has a scanner in place, we offer alert prioritization with host-specific risks to further enrich the solution. Our ability to de-emphasize vulnerabilities without impacting sensitive data is one of our key capabilities, because we know the average team is drowning in security concerns.

TAG Cyber: Can you share some insights into the future of cloud security in the coming years?

SONRAI SECURITY: We strongly believe identity and data must be the foundation of every cloud-security strategy, and an organization's main goal should be protecting their data. Identity and data-access complexities are exploding in the public cloud, along with an

array of interdependencies and inheritances that first-generation security tools miss, as shown by so many data breaches in the cloud. This is going to drive CIEM to the top of a CISO's list of must-haves. Cloud adoption is going to expand rapidly. This will increase the attack surface, resulting in more malicious attacks. Increasingly sophisticated bad actors are growing alongside the cloud. Their attack methods will shift towards targeting cloud environments, expanding past simply targeting a public bucket or exploiting a VM vulnerability. This is why it is so urgent for organizations to get a hold on their security now, before things get completely out of hand.

To survive, organizations will have to adopt automation, which is the only answer for solving security concerns at the speed and scale of the cloud. Automation has been noted as a tool to leverage in the past years, but many organizations are hesitant to lean into it. Finally, the prominence and impact of data breaches has changed the role of the CISO. It will soon become fundamental to have CISOs on the executive team and in boardrooms.



"I never guessed lateral traversal would get me here."

CHINESE ATTACKS ON U.S. TECHNOLOGY: A VIEW FROM THE TRENCHES

JENNIFER BAYUK

The U.S.-China Economic and Security Review Commission (USCC), founded in 2001, wrote in its first annual report that China's goal was to quickly close the gap between the United States and its own capabilities in technology warfare.[1] A key element of China's strategy was to exploit U.S. complacency and outwit the U.S. with "Sha Shou Jian"—assassin's mace weapons. These are literally clubs, but figuratively are methods to balance asymmetric power by "using cheap things to undo expensive ones."[2] A Chinese president in the 1980s was frequently quoted as pushing an internal policy to "hide your capabilities and bide your time" and to "absolutely not take the lead in world affairs."[3] This came as no surprise to U.S. diplomats because of an ominous dictum, oft-repeated in diplomatic circles dating back to the 19th century:[4]

China is a sleeping giant, let her sleep for when she wakes, she will shake the world.

In the years since China went public with "Sha Shou Jian" and even earlier, U.S. actions to safeguard cyberspace —or more to the point, inaction — have played into China's hands. Rather than fortifying our infrastructure about China's cyberattacks, the U.S. government preferred to rely on 19th century diplomacy. Rather than admit that critical infrastructure was inherently vulnerable, U.S. companies preferred to downplay the negative impact of repeated blows from the assassin's mace. Most of us working in cybersecurity could only look on in horror. Those of us who did make a big public fuss were dismissed as "Chicken Littles."[5] Here is a historical perspective from our trenches.

2000-2005

Since 2002, the U.S. Department of Homeland Security (DHS) has coordinated efforts to share information on cybersecurity threats to U.S. critical infrastructure with the infrastructure owners via a National Infrastructure Protection Plan (NIPP). It recruited industry regulators to convene CISOs to join forces in Information Sharing and Analysis Centers (ISACs) for each critical infrastructure industry. Through the U.S. Secret Service, DHS shares classified threat information with these ISACs, and also shares publicly available government research on cyberthreats. Also in 2002, the U.S. Federal Bureau of Investigation (FBI) established a Cyber Division, which a year later was assigned program responsibility for InfraGard, an information sharing and analysis program previously established in field offices to foster public-private trust/credibility in the exchange of information concerning terrorism, intelligence, criminal and security matters.

Coincident with these initiatives was the establishment of the USCC. Created by Congress in October 2000, its mandate was to monitor, investigate and report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, for government action.

Those of us working in critical infrastructure cybersecurity became keenly aware of the extent to which our companies had become targets of nation-state information warfare. At the beginning, cyberattacks[6] seemed very targeted. For example, there was competitor espionage, revenge by disgruntled employees and credit card scams.[7] The latter made the financial industry a prime target, so the Financial Services ISAC ("FS-ISAC") was under heavy pressure from regulators to protect the American consumer. The number of records in data breaches was being reported in the tens of thousands and that seemed shocking at the time. It was enough to create awareness in business and opinion sections of newspapers, but rarely on page 1. It took destructive worms that disabled infrastructure for anyone other than techies to notice that "computer security" was a trending issue.

Nevertheless, cyberdefenders became a necessary part of critical infrastructure, and we developed fast response and recovery strategies. I personally went "to the mattress" by throwing my gym matt on the floor next to my landline speaker phone, monitoring and coaching a plethora of desktop support people around the globe as they cordoned off networks and patched PCs. The U.S. government was too busy building offensive capabilities to do anything more than warn us. We were hosted at lavish conferences and dinners by cybersecurity vendors who were getting paid to deliver zero day threats (security bugs in our vendor's code!) to nation-states (including our own).[8]

Throughout this time, the USCC published a steady stream of information on China's disregard for World Trade Organization rules on theft of intellectual property[9].

The transfer of technology by U.S. investors in China as a direct or indirect government-imposed condition of doing business with Chinese partners remains an enduring U.S. security concern as well as a violation of China's WTO agreement. A WTO complaint should be filed when instances occur.

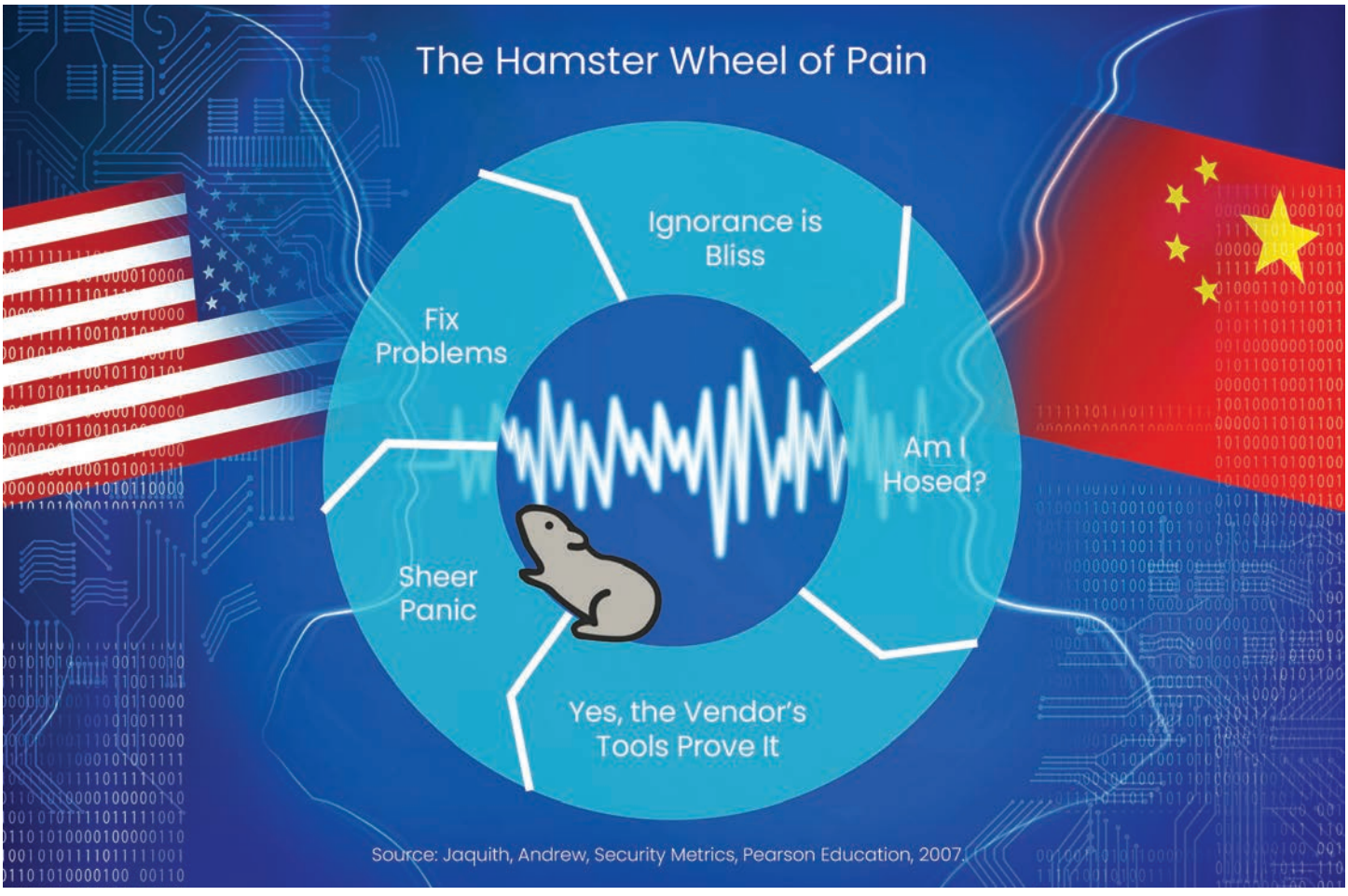
What China does with its growing technology capabilities—whether it converts them to military uses and/or to control the free flow of information to its population—is of direct national security concern to the United States.

Internally, we were identifying and responding to an endless stream of new cyberattacks, and threat actors were typically cloaked in anonymous internet traffic. Now that we know it was Chinese strategy to be entering this field, we can safely attribute some percentage of that activity at that time to China (as our adversaries, also with good basis in probability, attribute similar activities to the U.S.). Why didn't we lobby for more government involvement in defense? A significant issue was that few CISOs had permission to admit their systems had not been resilient enough to withstand the attacks. This caused considerable debate within the FS-ISAC. One CISO would ask another: "What impact did SQL Slammer have on your systems?" The other would yawn and say they were shopping for lawn furniture over the weekend, what did they miss? Yet we all knew we had our own version of mattresses.

At least in the financial industry, I understood this mindset. I saw examples in the 1990s. New York Stock Exchange computers would go down for hours, but it was never picked up by the financial industry press. No Wall Street firm wanted to risk public panic at the idea that the newfangled technology would not be able to keep track of their money, so no one in the whole industry complained in any way that might hit the papers. The mindset was that these computer security events, like unplanned outages, would also pass.

2006-2009:

One industry analyst mockingly called our predicament cybersecurity's "hamster wheel of pain."[10] A wheel of pain is a reference to ancient and medieval servility where slaves labor on turnstiles or prisoners are attached to torture mechanisms. The caged hamster (CISO), however, voluntarily embarks on the spinning wheel and continues to run as the wheel turns faster instead of trying to get off. The joke was that we were treating cyberattacks as sets of remediation projects without recognizing and remediating the root cause; that is, intent adversaries persistently hunting for vulnerable systems. Though we worked harder and faster, we never got ahead.[11]



As time went on, our participation in industry ISAC and InfraGard events provided us with ample evidence that China was unabashedly committing espionage on the U.S. government and businesses, as well as political opponents and dissidents. One of the more fascinating trails of events was China's infiltration into NASA.[12] Consequences of these attacks included a satellite diverted off course, supercomputers being physically unplugged from the network, and theft of data on rocket engine design, space shuttle operations and financial planning. Such activity was linked to network addresses in Taiwan and China. Yet there was no viable remediation activity. Rather, there is evidence that NASA officials instead retaliated against those who reported the events. Like Wall Street, NASA did not want to shake faith in its mission, so it played down both current and potential future negative impact. This response was unfortunately the norm rather than the exception. To understand the impact of this complacency among the victims requires acknowledging that it advanced China's strategy, which was specifically designed to foster such complacency. China played on our inherent aversion to bad news in order to fly under the political radar.

Mid-decade, the U.S. military adopted the term "Advanced Persistent Threat" (APT) to give a name to China's type of unrelenting targeted espionage. One of China's People's Liberation Army (PLA) Units has the dubious distinction of being the first such labeled cyber threat actor: APT1.[13] Its detectable activities have been tracked back to 2006, but it was likely formed earlier (NASA's attacks are known to date back to 1998). The ISACs continued to evolve into more structured information-sharing capabilities, providing anonymous or severely restricted distribution levels to allow cyberattack details to reach other potential victims. Though not as prominent, the USCC continued to feed us observations, and in 2007 added "key recommendations" with a strong focus on cybersecurity. In 2007 and 2008, the USCC recommended that Congress should:[14]

ensure adequate support for protecting critical American computer networks and data: The Commission recommends that Congress assess the adequacy of and, if needed, provide additional funding for military, intelligence, and homeland security programs that monitor and protect critical American computer networks and sensitive information, specifically those tasked with protecting networks from damage caused by cyber attacks.

APT had become a well-known term in cybersecurity, but the practical implications of the term "APT" had not risen to the attention of business leaders. The temptation of China's great untapped marketplace was irresistible, and despite the fact that cybersecurity APT was high on the operational risk lists, U.S. business leaders accepted those risks and dove into China's marketplace.

Early in 2008, I was part of a committee sent to Washington by my Wall Street employer to testify before the U.S. Committee on Foreign Investment in the United States (CFIUS).[15] The topic was a joint venture with a Chinese securities firm wherein we would provide back office services to support operations related to financial transactions. My role was to persuade the committee that we would be entirely in control of all the software used to process the transactions, that the Chinese members of the Joint Venture population would have no administrative or software development capability, and that our networks would ensure that all of our firm's intellectual property remained within U.S. borders. I did my best. Luckily for me, the financial crisis made the case moot. It remains for me a striking example of the differences between perceptions of threat in government and industry. Government was becoming more agitated while industry preferred to remain naively optimistic.

Though each industry ISAC member understood that risk of being a victim was increasing, the hamster wheel was in frenzied rotation and most felt they were at least one step ahead of the bad guys. Only those with cross-industry global views more fully understood the bigger picture.[16] In March 2009, TAG's own Ed Amoroso joined a group of distinguished cybersecurity experts who testified to the U.S. Senate that revenues from cybercrime exceeded those of drug crime, and were worth some $1 trillion annually. To those who understood the full extent of China's intellectual property theft, this figure was well within the range of plausible. To others in the trenches, however, it seemed like an unproven hypothetical. "What are they thinking?" sighed some CISOs, especially the less experienced ones. "They are crying Chicken Little, and we'll all be dismissed as overreacting." After all, at the time the latest USCC report had no recommendations on cybersecurity. When their companies plunged headfirst into China's marketplace, they were all-in.

By 2009 the tone of the USCC recommendations had changed. Rather than recommend that Congress spend on protection for all critical infrastructure, it recommended only that funding be provided to government to "meet the rising challenge of Chinese human intelligence and illicit technology collection," to "respond" to attacks, and to "develop effective and reliable attribution Techniques" for attacks. Where U.S. companies were mentioned, it was to recommend that Congress make sure they were not helping China (or other authoritarian countries) with censorship.[17] By the end of the decade, we knew not just from DHS and FBI, but also from increasingly credible news reports and observations of our own systems, that theft of intellectual property, denial of service attacks and malicious surveillance from China were steadily increasing. Nevertheless, none of USCC's 2007-2008 recommended protection assistance was forthcoming.

2010-2014:

The situation aligned perfectly with Sha Shou Jian. Yet the 2010 report had no substantive guidance other than that Congress request the administration to report on such hacking activit:.[18]

The Commission recommends that Congress request that the administration periodically issue a single report about the volume and seriousness of exploitations and attacks targeting the information systems of all federal agencies that handle sensitive information related to diplomatic, intelligence, military, and economic issues.

I thought it ironic that Congress had created a standing committee of experts to give them advice on this topic, and their advice was to ask someone else for a report.

One of the companies that was profoundly impacted by the pending government initiatives to deter internet censorship was Google. Yet to all appearances, its joint venture with China was successful. Like FS and NASA, the tech giant also had a tendency to hide from news of its vulnerability.[19] Circa December 2009, Google's cybersecurity staff started to detect anomalous activity on internal networks that had no explanation other than deep-rooted occupation by a data-thieving APT.[20] Within a month Google had evidence that its network was overrun with Chinese espionage agents who had infiltrated hundreds of machines with the aim of gaining access to both gmail accounts and source code. Many of us in the trenches heard rumors that, in a brash effort to eject the APT, Google trashed all of its Microsoft PCs

and made staff switch to Apple MacIntosh.[21] We applauded, though not sure whether to believe it. Soon after the public statements started to emerge, Google closed its Chinese internet search service and rerouted its search traffic to its uncensored service in Hong Kong.[22]

Further investigation soon revealed that dozens of U.S. tech companies had been similarly treated by China.[23] USCC alarm bells with respect to cybersecurity were back:[24]

The penetration of Google's computer network this year has renewed concerns about the Chinese government's tolerance or possible sponsorship of malicious computer activity.

USCC reports in 2011-2014 more regularly highlighted specific attacks, including but not limited to: RSA's networks breached by "Honker Union of China" hacker group,[25] a history of the NASA attacks, including full functional control over networks,[26] and successful large-scale espionage against DoD, DoD contractors [27] and the US Postal Service.[28] The outcry from U.S. business became too much for the U.S. government to ignore, and for the first time ever criminal charges were filed against known state actors for hacking. Five PLA members were indicted.[29] From the trenches, this was widely viewed as "security theatre," or as some referred to it, "keeping your friends out," because the only people who would bother to abide by your rules are your friends; your enemies are easily able to ignore them. The five indicted PLA members never apprehended.

As the diplomats applauded the indictments, China was given a breather from focus because other nation-states were more visibly throwing their weight around in cyberspace. North Korea decimated Sony Pictures, Iran launched denial-of service attacks against U.S. banks, Russia took down the internet and power grids in Estonia and Ukraine. These attacks seemed more alarming than China's unobtrusive though steady siphoning of U.S. secrets.

2015-NOW

Though China may had receded from the foreground in 2013-2014, a book published in 2015 brought a stark reminder that the China's intention to see Sha Shou Jian achieve objectives was a highly plausible threat.[30] Ghost Fleet portrays a scenario in which China starts a war against the United States using cyberweapons as its primary attack vehicle. The authors "spent years gathering information on everything from the next generation of Chinese drones to the ways in which certain U.S. weapons systems have already been hacked..... information is ... tucked into announcements of government contracts ... U.S. and Chinese military reports, online forums, and even leaked photos on Chinese social-media sites of ships under construction."[31]

If that did not persuade all of us hamsters of the reality of the threat, for the rest it hit home when we received official letters from the Office of Personnel Management that our own personal data has been compromised.[32] Though we did not work for the federal government, it was a condition of our participation in the DHS-run ISACs that all industry participants must have secret clearances. The online forms we filled out to apply for the secret clearances included the most detailed personal information we had ever been requested to provide: job history, past residences, travel outside the U.S., all of our family members and their birthdates. More than enough information needed to answer security questions if you were unfreezing a credit report or logging into the IRS. Our own government could not secure its own top secret clearance systems. It could not protect its cyberdefenders.

In 2016, USCC acknowledged that no actions taken by the US or anyone else in the past 15 years of its operation has deterred China to deviate from its Sha Shou Jian strategy for world domination:[33]

China continues to violate the spirit and the letter of its international obligations by pursuing import substitution policies, imposing forced technology transfers, engaging in cyber-enabled theft of intellectual property, and obstructing the free flow of information and commerce.

Nevertheless, recent history shows improvement only on the individual indictment side, not in the more ominous systemic threat. The U.S. government's ability to detect and identify accountability for APT cybercrimes improved to include apprehension and prosecution of culprits. The 2019 USCC reported Department of Justice prosecutions of individuals associated with China's cyberattacks, including but not limited to:[34] October 2018—an alleged deputy division director in the Jiangsu Department of China's Ministry of State Security, for recruiting aerospace employees from companies like GE Aviation to divulge trade secrets; Oct 2018—10 individuals, including members of Jiangsu Department of China's Ministry of State Security, for conspiring to steal sensitive data related to jetliner turbofan engines; December 2018—APT10 members, working in association with China's Ministry of State Security's Tianjin State Security Bureau, for economic espionage targeting U.S. government agencies and private companies across a broad array of industries for over a decade; April 2019—a Chinese businessman and U.S. engineer, for stealing turbine engine technology from GE Power.

Nonetheless, against the backdrop of persistent Sha Shou Jian, the prosecutions seem like more security theatre. Especially so, given that our current FBI director recently declared:[35]

China's reached a new level—more brazen, more damaging than ever before.

The U.S. belief in conventions such as the rule of law, mutually agreed goals of business joint ventures, and diplomatic resolutions to intellectual property rights violations have not made a dent in the persistent advance of China's progress toward its goal of global supremacy. The U.S. government's belief that these conventions would halt or even slow China's steady progress built on systematic theft and repurposing of U.S. data and intellectual property now seems naive and utterly ineffectual.

All indications are that China's strategy of "hide your capabilities and bide your time" has now given way to "shake the world." Ironically, NASA administrator Bill Nelson seems to be the first to emerge from slumber, recently saying:[36] "We must be very concerned that China is landing on the moon and saying: 'It's ours now and you stay out.'" Let us hope this creates a groundswell of concern leading to an appropriate defense, which in this case is most certainly not just a good offense.

Footnotes

[1] Pursuant to Public Law 106-398, October 30, 2000 as amended.

[2] Hambling, David, "China Looks to Undermine U.S. Power, With 'Assassin's Mace," Wired, July 2, 2009, https://www.wired.com/2009/07/china-looks-to-undermine-us-power-with-assassins-mace/

[3] See full explanation of the quote at: https://history.stackexchange.com/questions/54862/what-does-deng-xiaoping-mean-by-hide-your-capacities-bide-your-time

[4] See Fish, Issac Stone, "Crouching Tiger, Sleeping Giant," Foreign Policy, 1/19/16, https://foreignpolicy.com/2016/01/19/china_shakes_the_world_cliche/ Also note that "giant" is sometimes written as "lion" or "dragon," depending on the source

[5] This is a reference to a children's story where a chicken thinks the sky is falling because an acorn fell on its head.

[6] Which, if you research, you should know at the time cyberattacks were referred to as "computer security attacks" or "information security breaches" or simply "hacking" or "viruses."

[7] See for example, NYT Times Archives on searchwords like "information security, "computer virus" and "computer security," https://www.nytimes.com/search?dropmab=true&endDate=20041231&query=computer%20security&sort=best&startDate=20020101

[8] Perlroth, This Is How They Tell Me the World Ends: The Cyberweapons Arms Race, Bloomsbury, 2021.

[9] USCC 2004 Annual Report, p. 24 and 12.

[10] Source: Jaquith, Andrew, Security Metrics, Pearson Education, 2007.

[11] Even before Jaquith's analogy, we in the trenches referred to the situation less specifically as "Whac-A-Mole," an analogy with a still-popular 1970s game where the goal is to strike mechanical/virtual rodents with a mallet as they incessantly pop up in scattered patterns from numerous holes.

[12] Summarized from Epstein, Keith, and Ben Elgin, "The Taking of NASA's Secrets," Business Week, December 1, 2008, pp 73-79.

[13] Mandiant, "APT1 Exposing One of China's Cyber Espionage Units," https://www.mandiant.com/media/9941/download

[14] USCC 2007 Annual Report, p.16. The 2008 wording is very similar, USCC 2008 Annual Report, p. 18.

[15] CFIUS evolved from Defense Production Act of 1950 and a 1988 amendment, Section 721 of the legislation was revised by the Foreign Investment and National Security Act of 2007 (FINSA), establishing CFIUS authority to review foreign investments in U.S. business and real estate.

[16] Senate Commerce Committee, Hearing on Improving Cybersecurity, Statement of Edward Amoroso, https://www.commerce.senate.gov/services/files/E8D018C6-BF5F-4EA6-9ECC-A990C4B954C4, March 19, 2009. https://www.itnews.com.au/news/cyber-crime-profits-running-into-trillions-of-dollars-141172

[17] USCC 2008 Annual Report, p. 14.

[18] USCC 2011 Annual Report

[19] Perlroth, This is How They Tell Me the World Ends, 2021, ch. 5

[20] Ibid., ch 14

[21] Ibid, includes mention of an overnight raid wherein Google removed Microsoft PCs from staff offices without warning

[22] Helft and Barboza, Google Shuts China Site in Dispute Over Censorship, New York Times, March 22, 2010, https://www.nytimes.com/2010/03/23/technology/23google.html

[23] Operation Aurora

[24] USCC 2011 Annual Report

[25] USCC 2011 Annual Report

[26] USCC 2012 Annual Report

[27] USCC 2013 Annual Report

[28] USCC 2014 Annual Report

[29] US Department of Justice, Office of Public Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[30] Singer and Cole, Ghost Fleet: A Novel of the Next World War, 2015.

[31] See Ghost Fleet's authors' description of their research in: "How to Write About World War III," The Atlantic, 6/30/15, https://www.theatlantic.com/international/archive/2015/06/ghost-fleet-world-war-III/397301/

[32] Nakashima, Hacks of OPM Databases Compromised 22.1 Million People, Washington Post, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

[33] USCC 2016 Annual Report

[34] USCC 2019 Annual Report

[35] Wray, "Countering Threats Posed by the Chinese Government Inside the U.S.," Federal Bureau of Investigation, https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122

[36] Glenn, "NASA chief warns against China's moon program," The Washington Times, July 5, 2022.

CASE STUDY FOR ENTERPRISE: HOW NOT TO MANAGE YOUR SECURITY VENDOR PORTFOLIO

DR. EDWARD AMOROSO

Below is a fictitious account of an enterprise security team with a problem—namely, how to rationalize and manage the commercial investments they've made with cybersecurity vendors. Read the account and see what you would do. We've included discussion questions at the end.

ACT 1: THE VENDOR SPEND

Andrea Miller winced as she glanced over the spreadsheet of cyber security vendors. And wow, look at the amounts being spent! Three-hundred thousand here, four-hundred thousand there, and two million—TWO MILLION—being spent with a vendor that Andrea didn't even know.

She grabbed her iPhone and texted her Chief of Staff Robert: "Get the SLT on Zoom 5PM today. Need to go through this vendor list."

Andrea leaned back in her chair and sighed.

As the new CISO (just three months on the job!) for Acme Manufacturing, a product machining, assembly, fabrication and test company serving the aviation industry, she'd hoped to quickly control the budget.

"We spend a ton of money on cyber," the Acme CIO had explained to Andrea during her interview. "But we continue to have incidents. And I have this feeling that we're throwing good money at security tools that we don't need."

She glanced at the spreadsheet once again and shook her head at the total on the bottom right corner of the page: $37,587,234.

We could buy an airplane with that kind of money, she thought.

She fumbled around for a moment, and eventually pushed the right Zoom button and the spreadsheet popped up on everyone's desktop. The problem was that the list was so long, it could barely fit on everyone's screens.

ACT 2: THE TEAM EXPLAINS

Andrea held mostly face-to-face meetings at her previous company, but she was now getting comfortable with the virtual collaboration style the Acme Information Security Team had put in place.

"Thanks for getting together so fast," Andrea told her team, as she started the discussion. "I assume you all have the vendor spreadsheet, but I'll try to share my screen."

She fumbled around for a moment, and eventually pushed the right Zoom button and the spreadsheet popped up on everyone's desktop. The problem was that the list was so long, it could barely fit on everyone's screens.

"Let's just start through the list, maybe at the top," she said. "I see that we're almost spending thirty-eight million on security, and…"

"Uh, Andrea, it's more than that," John Graham-Burke interrupted.

As head of vulnerability management, John was always a voice of reason during discussions. Andrea had asked him specifically to be blunt with her—and he was happy to comply.

He continued: "You're just looking at the AIST budget, but we should also include AOIT. They have a bunch of additional vendors."

Andrea recognized AOIT as Acme Operations, Implementation and Technology, a branch of the CIO's team that did hands-on management of the security platforms, including all identity and access management.

"OK," she replied. "But let's start with what we have here."

"Fair enough," John replied. "But the other numbers are significant."

She nodded and then glanced back at the spreadsheet: "I think we can start at the top," she said. "Let's see, er—who here's one I didn't understand. I see that we're spending ten million with Notable IGA. That seems like a big number. Who, er—who is the owner of this?"

This question was met with a long quiet pause. Finally, Zoe Daschle, who ran the SOC and SIEM, chimed in: "Andrea, we really don't have owners of vendors, per se. I guess you could say that procurement owns them."

"Procurement?"

"Yes."

"Uh, huh," Andrea muttered after another pause. "Why don't we have owners for each vendor?"

"We probably should, but we manage vendors with this Excel spreadsheet and things get a little chaotic."

Andrea nodded again. This is not going well.

"What about this CloudBang EDR?" she asked. "Do we really spend nine million with them?"

Maya Sarabhai, head of security awareness and training, spoke up: "That was from our last endpoint security manager. She had worked there previously, and she signed us up. I mean, it seems like it's been good, so I don't see a problem, per se. Or at least no one has complained."

"Did this person leave the company?" Andrea asked.

Maya laughed: "Yes. She went back to work at CloudBang."

"Is that allowed?" Andrea asked.

The question was met with silence.

For the next hour, Andrea went through many names of many other vendors—and she was treated to a range of explanations: This vendor had been there as a legacy. And that vendor has a nice salesperson who gives tickets to nice events. And this other vendor was selected two years ago, and things seemed like they were sort-of OK—and on and on.

After the discussion, Andrea paused and thought to herself: Not acceptable.

ACT 3: DISCUSSING A SOLUTION

Andrea walked into Maya's private office carrying two large pumpkin spice lattes. It had been their custom these past couple of months to take turns running down to the Acme Café on the second floor for mid-afternoon refreshments and snacks.

"Oh, my gosh, what took you so long?" Maya said. "I need coffee!"

Andrea sat down. "You're going to need a real drink when you hear this," she replied. "Dan just set up a half-day review next week to go through all key vendors across IT and security."

The Dan she referred to was Dan Ford, the Number Two in finance. His nickname was Hatchet Dan because he never saw a budget he couldn't cut.

"Next week? Wow, Dan usually gives at least three weeks before he kills every program in the book," Maya replied.

"I need to bring detailed information on every one of our security vendors, and I think it comes to 87 total," Andrea said. "And they want at least two competitors listed for each vendor, along with trending information to justify the spend."

"We don't have that data."

"What about the spreadsheet? It seemed like it had many fields and I saw a bunch of detail in there."

Maya shrugged: "That data is not updated properly. It has some good hints about the vendors, but a lot of the information is just wrong. It still includes our Flunk SIEM, and we got rid of that thing a year ago."

"I didn't know that."

"Yea. They kept increasing our bill and no one noticed."

Andrea nodded and Maya was quiet. The two security executives thought for a few moments. They both understood that something needed to be done—and fast. It was not reasonable to spend this much money, without having some means for rationalization.

"Any advice on what to do?" Andrea asked.

Maya thought for a moment and then smiled: "Interns?"

QUESTIONS FOR GROUP DISCUSSION

1. Do you think the problem here stems from neglect by the security team or should the procurement team be doing a better job?
2. Do you believe it is common for enterprise security teams to have a poor understanding of their commercial portfolio?
3. Is an Excel spreadsheet the right mechanism for storing, maintaining and sharing information about cybersecurity vendors?
4. What types of services would you like to see from analysts, advisory firms or consulting teams to assist with this type of work?
5. Are you familiar with TAG Cyber's Research as a Service (RaaS) with its embedded portfolio management support? (Hint: Call us!)

sonraí SECURITY

Sonrai Security offers total cloud security in one platform that unearths, prioritizes and removes risks across every part of the cloud. Their proprietary, big data analytics engine continuously updates the paths an identity has used or could use to access data, and offers visibility rooted in full context and actionable understanding.

TAG CYBER
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG CYBER SECURITY ANNUAL
©TAG CYBER 2022