G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

OCTOBER 2022

Highlights

Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.

November 17, 2022
10:00am

Cybersecurity is the Modern Geopolitical Battlefield

Recent Government Hacks Reveal Superpower Clashes and Regional Skirmishes

A Clash of Two Titans: China & USA

Cybersecurity operations between China and the US are as much a fight for intelligence as they are political theater. Both China and the United States have accused one another of using government agencies to hack into organizations with sensitive data. While the United States has been complaining about China's hacking network for years, China has recently begun to amplify their frustrations with purported hacking of Chinese assets.

Earlier this month, China accused NSA's TAO (Tailored Access Operations) of orchestrating thousands of attacks throughout China, including a string of attacks against China's military and aeronautical Northwestern Polytechnical University in June of 2022. China claims that TAO used the 'drinking tea' tool to exfiltrate data from the university, a tool that they claim the US has been using in its hacking operations for years. Regardless, it is clear that China wants to deflect attention away from their hacking operations by complaining about US hacking. In the same month of the attack, China attacked major US telecommunications companies.

> *Despite advances in cybersecurity, cyber espionage continues to offer threat actors a relatively low-cost, high-yield avenue of approach to a wide spectrum of intellectual property. -* Foreign Economic Espionage in Cyberspace Report, National Counterintelligence and Security Center.

Albania Severs Ties with Iran Over Cyberattack

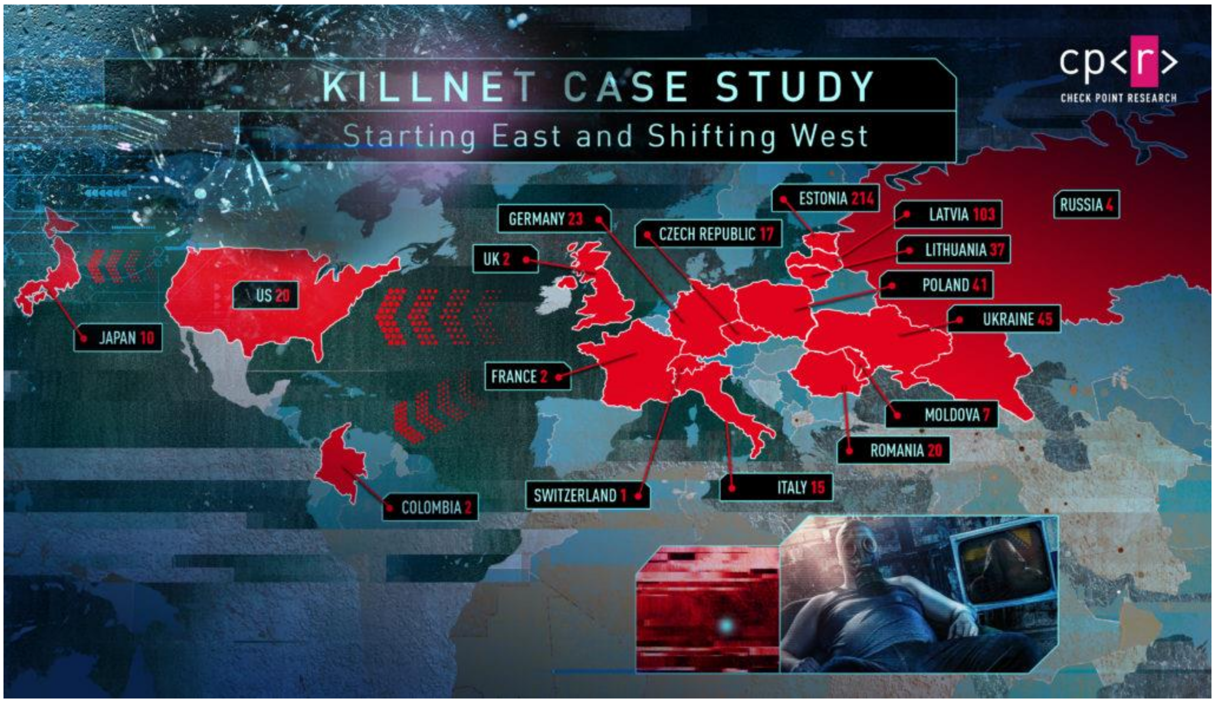
Prime Minister Edi Rama said a probe had found "incontrovertible evidence" that Iran "hired four groups to mount the attack on Albania" on 15 July. According to the PM, the hackers tried to paralyze public services, delete and steal government data. After the July attack, Albania worked with US and UK cybersecurity experts to trace the attack to Iran. While Albania is one of the smaller members of NATO, severing all diplomatic ties with Iran and ordering Iranian diplomats to leave their embassy in Albania is historical in severity as a response to a cybersecurity attack. Prior to the attack, tensions between Albania and Iran were heightened due to Albania's decision to offer asylum to thousands of Iranian dissidents. Not only that, but following Albania's decision to cut ties with Iran, Albania was subject to a second Iranian cyberattack targeting its national police.

> *“Iran’s cyber attack against Albania disregards norms of responsible peacetime State behavior in cyberspace, which includes a norm on refraining from damaging critical infrastructure that provides services to the public,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. “We will not tolerate Iran’s increasingly aggressive cyber activities targeting the United States or our allies and partners.”*

Japan and Russia Tussle

The Russian-affiliated hacking organization Killnet hacked into 20 Japanese government websites earlier in the month. The DDoS (Distributed Denial-of-Service) attack shutdown Japan’s digital agency and education ministry, Tokyo’s subway and port of Nagoya websites, as well as Japan’s social network Maci. Killnet specifically targeted Japan as both retribution for Japan’s support of Ukraine throughout the Russian-Ukrainian war, as well as disagreements over the Kuril Islands. The Soviet Union invaded the archipelago in between mainland Russia and northern Japan in the final days of WWII, after the US bombing of Nagasaki and Hiroshima. Killnet has attacked several other countries in 2022 in response to their support for Ukraine, such as Lithuania, Italy and Estonia.

Meanwhile, hacktivist group Anonymous declared cyber war against Killnet in May of 2022 at around the same time that Killnet began attacking pro-Ukranian government websites, and took Killnet’s website offline for a period of time in May. It appears that (at least for now), cyber warfare is a new proxy warfare that seeks to harm government assets and disrupt people’s daily lives, and the battles are being drawn along cold war lines and geopolitical disputes. Killnet publicly launched around the end of February 2022, at the start of the Russian–Ukrainian war. The group began their aggressive activity in March, with targets mostly in Ukraine. In April the group shifted its focus to support Russian geopolitical interests all over the world. Between late February and September, the group claimed to have executed more than 550 attacks. Only 45 of them were against Ukraine, less than 10% of the total.



Security Requirements in OCP Specifications

OCP hardware specification contributions for platform boards and systems must include a section on security. Elaine Palmer and Eric Hibbard will present a framework for simplifying security requirements using references to existing standards at this year's OCP Summit, October 20, "Due Diligence or Differentiation? Security Requirements in OCP Specifications." They will review the suggested security template, which covers:

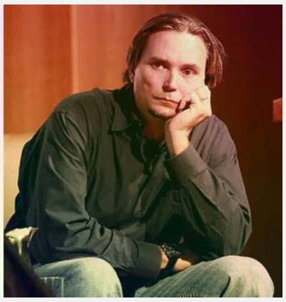
1. Cryptography, key derivation, key agreement and hashing
2. Secure Boot, Measured Boot, and Attestation
3. Product Lifecycle
4. Other Recommended Functionality

At a minimum, the security section dictates the due diligence that designers must take when designing compliant products. Some vendors will want to go further, and this section is where they can document the security features that differentiate their products from others. Secure products follow standard development processes, implement standard algorithms, and pass standard test suites.

Elaine Palmer is a Senior Technical Staff Member at the Thomas J. Watson Research Center, and a member of the IBM Academy of Technology. She led an IBM Research team that designed and developed a tamper-responding secure coprocessor for servers, and it was awarded the world's first level 4 certificate under FIPS 140-1 and a team that developed the first smart card cryptographic library to be validated at EAL5+ under the Common Criteria. She is a member of the IEEE and a Distinguished Engineer in the ACM.

Eric A. Hibbard is the Director, Product Planning – Storage Networking & Security at Samsung Semiconductor, Inc. and a cybersecurity and privacy leader with extensive experience in industry, U.S. Government, and academia. He serves in leadership positions in ISO/IEC, the InterNational Committee for Information Technology Standards (INCITS), the IEEE Computer Society, the American Bar Association (ABA), the Cloud Security Alliance (CSA), and the Storage Networking Industry Association (SNIA).

Ransomware Payout, Coverup, & Prison Potential



Joe Sullivan, a prominent security expert, spent the first eight years of his career working for the Department of Justice, first as an intern at the DOJ Miami office. He prosecuted cybercrimes for the San Francisco U.S. attorney's office, working with Robert Mueller, then as Assistant United States Attorney at the District of Nevada in Las Vegas, and worked as Assistant US Attorney at the Northern District of California. Sullivan was the top security officer at Facebook, Uber, and Cloudflare, and a Commissioner for Obama Cyber Commission. Next, he faced his previous employer U.S. attorney's office – this time as a defendant charged with obstruction of justice for concealing a 2016 breach of Uber customer and driver records from the Federal Trade Commission and for actively hiding a felony.

Sullivan authorized payments to hackers after the 2016 breach, using Bug Bounty money to make a $100k ransomware payment.

The jury rendered a unanimous verdict, finding him guilty of both charges. Sullivan faces a five-year prison sentence on the obstruction charge, three years for failing to report a felony, and fines of $500k.

This case is the first major criminal case brought against a corporate executive over a breach by outsiders. However, payoffs to extortionists, including those who steal sensitive data, have become so routine that some security firms and insurance companies specialize in handling the transactions. "Paying out the ransom I think is more common than we're led to believe. There is an attitude that's similar to a fender bender," said Michael Hamilton, founder, Critical Insight.

FBI leaders have vocally discouraged paying ransoms but have said they will not pursue the people and companies that pay ransoms as long as they don't violate sanctions prohibiting payments to named criminal groups especially close to the Russian government.

States typically require companies to disclose breaches if hackers download personal data and a certain number of users are affected. There is no federal law requiring companies or executives to reveal breaches to regulators. Federal officials have pressed for recent legislation that will require ransomware notifications from critical infrastructure victims to the Cybersecurity and Infrastructure Security Agency. The Securities and Exchange Commission is also pushing for more disclosure.

The Federal Trade Commission deposed Sullivan as part of their investigation of a 2014 breach of Uber's online systems. Ten days later, a hacker emailed Uber and described a security lapse that allowed him and a fellow hacker to download data using a digital key Uber had left exposed to get into an Amazon account and download the personal data of about 600,000 Uber drivers and additional personal information associated with 57 million riders and drivers. Uber did not publicly disclose the incident or inform the FTC until a new chief executive, Dara Khosrowshahi, joined the company in 2017.

The hackers demanded a ransom in exchange for destroying the data. Sullivan's team said they could pay under Uber's bounty program but that the top payout under it was $10k. The hackers said they would need at least $100k Sullivan paid a $100k ransom payment and had the hackers sign a nondisclosure agreement. The hackers were later arrested and pleaded guilty to hacking charges, and one testified for the prosecution in Sullivan's trial.

Federal prosecutors presented evidence that "after Uber personnel were able to identify two of the individuals responsible for the breach, Sullivan arranged for the hackers to sign fresh copies of the non-disclosure agreements in their true names. The new agreements retained the false condition that no data had been obtained. Uber's new management ultimately discovered the truth and disclosed the breach publicly, and to the FTC, in November 2017." They argued that Mr. Sullivan knew that revealing the new hack would extend the FTC investigation and hurt his reputation. "He took many steps to keep the FTC and others from finding out about it," Benjamin Kingsley, an assistant U.S. attorney, said during closing arguments. "This was a deliberate withholding and concealing of information."

"This case will certainly make executives, incident responders and anybody else connected with deciding whether to pay or disclose ransom payments think a little harder about their legal obligations. And that's not a bad thing," said Brett Callow, threat analyst at Emsisoft. "As is, too much happens in shadows, and that lack of transparency can undermine cybersecurity efforts."

Prosecutors argued in Sullivan's case that his use of a nondisclosure agreement with the hackers was evidence that he participated in a coverup. They said the break-in was a hack that was followed by extortion as the hackers threatened to publish the data they took, and so it should not have qualified for Uber's bug bounty program to reward friendly security researchers. But the reality is that as the hacking of corporations has gotten worse, the way companies have dealt with it has moved far past the letter of the law when Sullivan was accused of breaking it.

The conviction stunned corporate security and compliance members. While Sullivan directed the response to the two hackers, many others at the company were in the loop, including a lawyer on Sullivan's team, Craig Clark. Evidence showed that Sullivan told Uber's CEO, Travis Kalanick, within hours of learning about the threat himself, and that Kalanick approved Sullivan's strategy.

Most security professionals had been anticipating Sullivan's acquittal, noting that he had kept the CEO and others who were not charged informed of what was happening. "Personal liability for corporate decisions with executive stakeholder input is a new territory that's somewhat uncharted for security executives," said Dave Shackleford, Principal Consultant, Voodoo Security. "I fear it will lead to a lack of interest in our field, and increased skepticism about infosec overall."

Ransomware attacks were rare when Sullivan was charged but have increased dramatically in the last couple of years. The techniques in those attacks have also shifted. At the beginning of 2020, most ransomware merely encrypted files and demanded money for the key to unlock them. By the end of that year, most ransom attacks included the outright theft of files, setting up a second ransom demand to prevent their public release, according to a 2021 report by the Ransomware Task Force, an industry-led group that includes representatives from the U.S. Cybersecurity and Infrastructure Security Agency, the FBI, and the Secret Service. More recently, cryptocurrency exchanges have been robbed and then negotiated to give massive payments to get those funds back.

"Especially over the past six months in the crypto space, the model is 'build it until we get hacked, and we'll figure it out from there,' " said Ellis. As average payouts zoomed past Sullivan's, into the hundreds of thousands of dollars, more businesses turned to insurance companies for predictability. But often, the insurance companies reasoned it was cheaper to pay than to cover the damage from lost files. Some paid regularly, ensuring steady earnings for the gangs. Making payments illegal, as some have proposed, would not actually stop them, the FBI has said. It would instead give the extortionists yet another club to hold over their victims after payment is made. At least so far, Congress has agreed, declining to ban the transactions.

After Kalanick was forced out of the company for unrelated scandals, his replacement, Dara Khosrowshahi, came in and learned of the breach. Sullivan described it as a routine payoff but a later investigation turned up the full story, and Khosrowshahi fired Sullivan for not telling him more, sooner. Uber helped the U.S. attorney's office build their case against Sullivan.

Sullivan did not reveal the 2016 hack to Uber's general counsel but he did discuss it with Uber lawyer, Craig Clark. Like Sullivan, Clark was fired by Khosrowshahi after the new chief executive learned about the details of the breach. Clark was given immunity in exchange for testifying against Sullivan. Clark testified that Sullivan had told the Uber security team that they needed to keep the breach secret and that Sullivan had changed the nondisclosure agreement signed by the hackers to make it falsely seem that the hack was white-hat research. According to Clark, Sullivan said he would discuss the breach with Uber's "A Team" of top executives. Sullivan only told CEO, Travis Kalanick. Kalanick approved the $100k payment to the hackers. Prosecutors unsuccessfully tried to get Sullivan to implicate Kalanick.

Clark acknowledged advising the team that the attack would not have to be disclosed if the hackers were identified, agreed to delete what they had taken and could convince the company that they had not spread the data further, all of which eventually came to pass. Prosecutors were left to challenge "whether Joe Sullivan could have possibly believed that" as one of them put it in closing arguments.

Accountability for the payoff and coverup, but not for sloppy security…

There is information that an 18 year old breached Uber's network a couple of weeks ago by tricking an employee to give their login credentials by pretending to be a colleague. The hacker posted company-wide on Slack regarding the breach and the boast posts were so brazen that employees thought the entire incident was a joke. The hacker described Uber security as "awful." Screenshots included proof that the hacker had access to highly privileged security accounts, which would provide wide authority inside the company. Uber included passwords in programs used for accessing key outside resources, such as Amazon Web Services, so the hacker did not need to break into more exclusive internal accounts or even guess.

Bug Bounties Gone Bad

Bug bounty programs, like Uber's mentioned above, provide a way of paying "white hat" researchers to report security vulnerabilities, offering cash to those already inclined to stay above board.

But, Casey Ellis, founder of Bugcrowd, acknowledged that some companies use bounty programs to conceal problems that should have been disclosed under state or federal rules. "That's definitely a thing that happens," Ellis said. Bug bounties usually require nondisclosure deals, some of which last forever. "Bug bounty programs are being misused to hide vulnerability information."

Disputes between the researchers reporting the vulnerabilities and the companies are common. Disagreements include:

- Whether a bug was "in scope," meaning inside the areas where the company said it wanted help,
- How much a bug is worth, or if it is worthless because others had already found it, and
- How, or even if, the researcher can disclose the work after the bug has been fixed or the company opts not to change anything.

The bounty platforms offer arbitration to resolve disputes but since the companies pay for the arbitration, researchers see bias. And, if they complain, they get removed from the platform entirely.

"If you're hacking on a bug bounty program for the love of hacking and making security better, that's the wrong reason, because you have no control over whether a company decides to patch in a timely matter or not," said John Jackson, a researcher who cut back on his bounty work and now sells vulnerability information when he can.

Lockbit ransomware group is offering its own bug bounty program asking security researchers to submit bug reports for rewards ranging between $1,000 and $1 million. "We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million," reads the LockBit 3.0 bug bounty page (yeah, no.)

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. Registration links and more information will be available in our next newsletter, on our website, and you can always contact us directly with questions. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

Interested in Sponsoring a webinar? Contact G2M for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Cybersecurity

Bug Bounties Gone Bad? Uber Case Highlights Pressure on CISOs.	December 14
Key Cybersecurity Trends for 2023	January 12
Cybersecurity for Remote Workers & Mobile Devices	February 23
The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	March 23
Beyond the CISO Organization – Meeting the Cybersecurity Needs of the C-Suite & Boardroom	May 4
Cybersecurity- Finding, Training, & Retaining the Best Talent	May 25
xDR- The Promise versus the Reality	June 15
HIPAA, GDPR, Data Privacy, & Cybersecurity- 5 Keys to Make It All Work Together	July 13
Beyond Ratings – 5 Things You Can Do With a Third Party Risk Management (TPRM) Program	August 17
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9
Cybersecurity Predictions for 2024	December 7

Enterprise Storage & Technology

OCP 2022 Wrap Up – The Latest and Greatest in SSDs, CXL, Accelerators, and Other Big Trends for the Datacenter and the Cloud	November 15
Storage Architectures for Artificial Intelligence & Machine Learning	February 7
Memory As The New Storage – CXL, Extended Memory, & Persistent Memory. What Does the Future Hold?	March 7
The Need for Speed: NMVe & Advanced SSDs	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27
NVMe & NVMe-oF – Past, Present, & Future (at FMS)	August 2
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Upcoming Conferences

October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
October 31-Nov 1	CompTIA EMEA Member/Partner, London
October 31-Nov 2	Gartner IT Symposium/Xpo Japan, Tokyo
November 1-3	NetApp INSIGHT 2022, Virtual
November 7-9	Acronis #Cyberfit Summit 2022, Miami, FL
November 7-10	VMWare Explore Europe, Barcelona
November 9-11	IT Nation Connect, Orlando, FL
November 13-18	SC22, Dallas
November 14-16	Gartner IT Symposium/Xpo India, Kochi, India
November 14-17	Titanium Converge, Austin, TX & Virtual
November 15-17	Black Hat Middle East & Africa 2022, Saudi Arabia
November 15-17	ISC East, NYC
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
November 21-22	Gartner IT Infrastructure, Operations, & Cloud, London
November 28-Dec 2	AWS re:Invent, Las Vegas

December 1-2	Digital Transformation Expo Global, London
December 5-6	Healthcare Cybersecurity Forum, Boston, MA
December 5-8	Black Hat Europe 2022, London
December 6	Security Operations Summit, Virtual
December 6-8	Gartner IT Infrastructure, Operations & Cloud, Las Vegas
December 6-9	Cisco Live, Melbourne, Australia
December 10-14	Edge 2022: International Conf on Edge Computing, Hawaii
December 10-14	Cloud 2022: International Conf Cloud Computing, Hawaii
December 12-15	Palo Alto Networks Ignite, Las Vegas
December 13	Black Hat Cybersecurity Outlook 2023, Virtual
2023	
January 5-8	CES, Las Vegas & Virtual
January 18	SNIA Persistent Memory Summit, San Jose, CA
January 30-Feb 1	Cybertech Global TLV, Tel Aviv, Israel
February 6-10	Cisco Live, Amsterdam, Netherlands
February 13-14	Gartner Security & Risk Management, Mumbai, India
February 14-16	ESNA Expo, Long Beach, CA
February 14-17	ITExpo East, Fort Lauderdale, FL
February 27-28	Gartner Security & Risk Management Summit, Dubai
February 27-March 2	Mobile World Congress Barcelona
February 28-March 2	Rice University Energy HPCC Conference, Houston, TX
March 8-9	CloudExpo Europe, London
March 14-16	Gulf Information Security Expo, Dubai, UAE
March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas
April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas

April 17-21	HIMMS Global Health Conference, Chicago, IL
April 19-20	CyberSec Europe, Brussels, Belgium
April 24-27	RSA Conference, San Francisco
May 22-25	Dell World, Las Vegas
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 1-3	Flash Memory Summit, Santa Clara, CA
August 5-10	Black Hat USA, Las Vegas
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome

PASSWORD
G2M
RESEARCH
Effective Marketing & Communications
with Quantifiable Results