Highlights

Cisco Webex Predates Other Video Conferencing, as Does Its Security Protocols, Apparently

Webex, founded in 1995 and purchased by Cisco in 2007, has led the video conferencing arena long before COVID-19, when the need for socially distanced work solutions grew exponentially. Webex cashed in on that need with growth of 451%, hosting up to four million meetings in a single day and boasting over 324M users. In response to this increase in demand, IBM researchers dug into Webex processes and found three significant vulnerabilities- Hackers could join Webex meetings without being visible on the participant list; maintain audio connection to a meeting even after, seemingly, being removed; and hackers could access personal attendee information without being admitted to the meeting. Cisco has addressed these exploits but provides additional security recommendations for Webex users including continuing to test new tools for security, taking extra precautions for confidential calls, using unique meeting IDs, using meeting passwords, locking meetings, restart meetings that go back to back instead of continuing the same meeting, use notification features, and end suspicious calls.

According to a survey by Gartner, over 87% of company leaders plan to allow employees to work remotely at least part of the time, post-pandemic. 47% will allow employees to work remotely full-time. This shift means more video-conferencing, so it is time to have protocols in place to meet that increased demand.

48M Records Raided in Animal Jam Hack

An attack on a Slack server that game developer WildWorks uses for intra-company communication resulted in a raid of 48M account records for Animal Jam WildWorks game platform. Over 130M kids play Animal Jam but WildWorks has a policy of manually reviewing applications to ensure parents don’t use their children’s names as usernames. So, while hackers obtained the AWS security key from the third-party Slack server and used it to access player databases, they did obtain parent information such as name and billing address but they did not obtain the names of these children.

The game platform launched in 2010 and has over 300M individual avatars and is available in 225 countries. It is one of the most popular games for kids, especially for kids in the 9-11 age range. Animal Jam is free to play and kids can learn about nature, chat with other players, and engage in competitions for in-game prices.

While the stolen data was not highly sensitive it did include usernames and player’s date of birth. 7M parent email addresses were captured in the raid. WildWorks reset every player’s password but parents will now have to remain vigilant to protect against scams relating to the breach.

"It raises the question as to how deeply embedded technology has become in all aspects of our lives, where even children's toys and games need accounts to be setup which potentially can hold sensitive information — and make an attractive target to attackers."

He suggested that a closer partnership between manufacturing and technology could help mitigate risks to kids and their data.

"Not just in products but create [to] a culture of security that pushes good security practices to the forefront," Malik added. "While no one approach will be able to prevent all breaches, it's important that data isn't collected unless necessary, and the data that is collected, is done for legitimate purposes and secured properly."

Javvad Malik,

Security Awareness Advocate

at KnowBe4

Catching the Big Phish

SANS Institute, the most trusted resource for cybersecurity training, was victim to a phishing attack of 28k records. SANS Institute has provided security training to more than 165k professionals worldwide. Yet, cybercriminals were able to harpoon even the most ostensibly savvy professionals.

The response to address and correct the breach was swift and transparent.

"When a respected security organization, such as SANS Institute, experiences an event like this, it underscores that for many organizations attempting to prevent each and every attack is a fool's errand and an expensive one at that," comments Tim Wade, Technical Director, CTO Team at Vectra. "The real hallmark of modern security is about resilience to attacks – the capacity to perform timely detection and response before material damage is done even after preventative controls have failed. Additionally, the steps that SANS Institute is taking to both complete a thorough investigation and use the outcome of that activity to further instruct and prepare the rest of the security community should be applauded."

Leveraging Free Google Services to Phish

Armorblox threat research team illustrates 5 targeted phishing campaigns that exploit free Google services:

1) American Express Credential Phishing- Email saying the customer left out information when validating their card, hosted on a Google form with American Express branding
2) Benefactor Scam Reconnaissance- Email from a childless widow with money to bequeath
3) Security Team Impersonation- Impersonates the internal company security administrator team
4) Payslip Scam- Impersonates internal payroll team with an urgent request to verify personal information for their payslip
5) Microsoft Teams Credential Phishing- Impersonates internal IT team asking for review of a security message colleagues have shared over Microsoft Teams.

Armorblox identified other free cloud services being exploited to build phishing emails or host demains, including Microsoft OneDrive, Box, Dropbox, SendGrid, Webflow, and Amazon Simple Email Service.

Apple Security Chief - Ipads for Concealed Weapons Permit?

The adage that any news is good news doesn’t always apply. The Santa Clara County district attorney has charged Apple Security Chief, Tom Moyer, with attempted bribery for allegedly offering $70k in iPads in exchange for concealed weapons permits. Apple’s lawyer, Ed Swanson, responded, "Ultimately, this case is about a long, bitter, and very public dispute between the Santa Clara County Sheriff and the District Attorney, and Tom is collateral damage to that dispute." He said that Applie did offer to donate iPads to the department and did apply for CCW permits, but they were unrelated to each other. Two officers have been charged in an alleged scheme to deny licenses to applicants unless they received something in return. State law requires an applicant for a license demonstrate good cause for the license, complete a firearms course, and have good moral character. The sheriff has broad discretion in make the determination of who should qualify.

Anticipating Criminal Abuses of AI

A joint effort by Trend Micro, UNICRI, and Europol looks at “Malicious Uses and Abuses of Artificial Intelligence” in their 80 page report. An excerpt:

“[i]t is expected that AI will help criminals conduct social engineering at scale by automating the first steps of an attack through AI-aided content generation, improving business intelligence gathering, and speeding up the detection rate of both potential victims and business process compromise attacks.

Moreover, as defense systems increasingly employ AI-based approaches, criminals are expected to either directly attack those systems, or use AI for user behavior emulation as well.

The increasing automation of everyday life’s numerous aspects using AI-based systems also inevitably brings with it a possible loss of control over the same aspects. This would not only broaden the attack surface, but also create new types of attacks. One novel example is AI-enabled stock market manipulation that takes advantage of the use of AI-based algorithms in the area of high frequency trading.

Meanwhile, current and upcoming technologies like 5G, in combination with AI, will shape industry and further drive automation and smart technologies at scale. Presumably, criminals are likely to target or manipulate these technologies as well.

In response to the different scenarios described here, the report identified possible countermeasures, ways of mitigating risks, and several other recommendations.

It is also worth emphasizing that close cooperation with industry and academia is a must in order to develop a body of knowledge and raise awareness on the potential use and misuse of AI by criminals. Not only will such cooperation anticipate malicious and criminal activities facilitated by AI, it will also prevent, respond to, or mitigate the effects of these attacks in a proactive manner.”

Compal Security Breach but “Not Being Blackmailed by Hackers” as Cybercriminals Demand $17M

Compal is the second largest contract laptop manufactor in the world with clients including Apple, Lenovo, Dell, Toshiba, HP, and Toshiba. News agencies reported a ransomware attack on the company but Compal denied the report. The company acknowledged a security breach of 30% of its computers. Compal’s statement regarding the breach stated, “Compal is not being blackmailed by hackers as it is rumored by the outside world.” However, DoppelPaymer ransomware gang was implicated in the attacks based on a screenshot of a ransom note demanding just under $17M from the company in exchange for the decryption key.

DoppelPaymer has been linked to attacks on hospitals, universities, and both SpaceX and Tesla.

G2M Research Multi-Vendor Webinar Series

Our 2021 webinar schedule is ready! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact G2M for a prospectus.

Our October webinar “AI, GPUs, & Storage Use Cases in Healthcare” was sponsored by Kioxia (Matt Hallberg), NVIDIA (Brad Genereaux), WekaIO (Shimon Ben-David) and Datyra (Keith Klarer). View the recording and/or download a PDF of the slides.

Jan 19:	Can Your Server Handle The Size of Your SSDs?
Feb 23:	Storage Architectures to Maximize the Performance of HPC Clusters
March 23:	One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?
April 20:	The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle)
May 18:	Responsive and Efficient Storage Architectures for Social Media

June 15:	It's 2021 - Where Has NVMe-oF™ Progressed To?
July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion