White-Hat Hacker Team, Led By 20 Year Old, Finds 55 Apple Website Vulnerabilities, 11 Critical

For three months, Sam Curry and his team of white-hat hackers tackled Apple's Security Bounty program which pays friendly hackers to find vulnerabilities in their website and products. Like other similar programs, Apple pays cash for vulnerabilities based on their severity of the exploit. Curry and 4 fellow hackers found 55 vulnerabilities, 11 critical, 29 high severity, 13 medium severity, and 2 low severity reports. Critical bugs allowed access to core Apple infrastructure and included Remote Code Execution via Authorization and Authentication Bypass, Authentication Bypass via Misconfigured Permissions allows Global Administrator Access, Command Injection via Unsanitized Filename Argument, Remote Code Execution via Leaked Secret and Exposed Administrator Tool, Memory Leak leads to Employee and User Account Compromise allowing access to various internal applications, Vertica SQL Injection via Unsantized Input Parameter, Wormable Stored XSS allows Attackers to Fully Compromise Victim iCloud Account (2), Full Response SSRF allows Attacker to Read Internal Source Code and Access Protected Resources, Blind XSS allows Attacker to Access Internal Support Portal for Customer and Employee Issue Tracking, and Server-Side PhantaomJS Execution allows attacker to Access Internal Resources and Retrieve AWS IAM Keys.

Curry explains the stored XSS vulnerability was wormable, meaning it could spread from user to user just by opening a malicious email. He and his team will earn around $500k for their efforts.

Volunteers Fight Back Against Hospital Ransomware Attacks

Randomware attacks on hospitals has been an important security issue, particularly during this period of strain on the healthcare system. Attacks have been persistent and world-wide as hackers exploit the current global healthcare crisis. We highlighted this issue in our May and September cybersecurity newsletters.

Of course, these cyberattacks did not start with this pandemic. WannaCry, a ransomware attack, decimated UK hospitals in 2017. Over 200k computers were impacted worldwide. And, in UK hospitals, with older Windows operating systems, the worm jumped from computer to computer, encrypting files, and crippling hospitals to the point that 19k appointments and surgeries had to be canceled, costing the National Health Service over $100M.

Volunteers – the Cyber Threat Intelligence League – are tackling these healthcare attacks by looking for vulnerabilities in medical provider systems. The team of cybersecurity researchers partnered with health care and other ISACs for help in getting identified threats directly to the appropriate personnel. They build an infrastructure of over a thousand volunteers, each vetted for their identities and skillset. The group's mission was initially only directed at protecting hospitals but they have experts in everything from advanced persistent threats to malware analysis to dark web tracking so they have tackled various challenges as the need and their expertise warrants. Led by employees from Microsoft, Clearsky, and Okta, CTI League has members from 80 countries and partners with the Department of Homeland Security and FBI.

The 4 goals of the CTI League are to 1) reduce the level of threat to the MS-LSO by preventing cyber-attacks, 2) Neutralize cyber threats looking to harm MS-LSO and to exploit the current COVID-19 pandemic, 3) Support law enforcement organizations in their fight against threats that are a danger for public safety, and 4) Create a disinformation resilience of the MS-LSO.

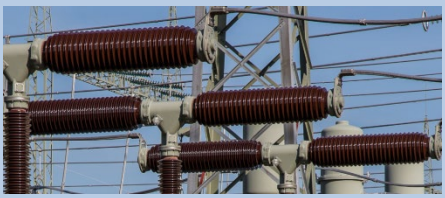
Twitter Account Hack?

Dutch security researcher, Victor Gevers, reported that he was able to access President Donald Trump's Twitter account by guessing his password – maga2020! According to Gevers, he tried to alert Trump's campaign and Twitter but received no response. Later, he found that Twitter account had added two-factor authentication. The White House says – Fake News!

Gevers is a security researcher at the GDI Foundation and Chair of the Dutch Institute for Vulnerability Disclosure, a group that finds and reports security vulnerabilities. He has worked in this area for 19 years and has provided over 5000 responsible disclosures worldwide. Gevers said he was able to access the account on the fifth attempt.

Person, woman, man, camera… Bottom line, use two-factor authentication to protect your accounts.

The Aurora Generator Test and Taking Down A Power Grid



Six Russian GRU military intelligence agency hackers, called Sandworm, are charged with substantial cyberattacks including sabotaging the 2018 Winter Olympics and attacking Ukraine's power grid. The power grid attack was not just designed to cause a blackout. It was designed to damage electrical equipment and is modeled after the Aurora Generator Test, a project designed by the US government to imagine and test catastrophic threats to critical infrastructure. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers describes the Aurora Generator Test and how just 30 lines of code blew up a 27 ton generator, critical infrastructure equipment beyond repair.

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 September webinar "Edge Computing/Storage – Get (and Keep) Your Data Off Of My Cloud" was sponsored by Lightbits Labs, ScaleFlux, and NGD Systems. View the recording and/or download a PDF of the slides.

Our October webinar "AI, GPUs, and Storage Use Cases in Healthcare" was sponsored by NVIDIA, Kioxia, WekaIO, and Datyra. View the recording and/or download a PDF of the slides.

G2M RESEARCH

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

Upcoming 2020 AI & Cybersecurity Events - All Virtual

Cybersecurity & Cloud Expo, November 4-5

AI & Big Data Expo, November 5-6

Cybersecurity & Fraud Summit, November 17

AI Summit, December 9-10

Survey results from our Webinar, "AI, GPUs, and Storage Use Cases in Healthcare" sponsored by NVIDIA, Kioxia, WekaIO, and Datyra

What are your greatest concerns when building large AI/ML training data sets?

The amount of time it will take to run the training data through the model: **39%**

The cost of the hardware required to run the training model: 33%

Managing the various training and verification datasets: 6%

Managing and archiving the results of training runs: 11%

Other issues: 0%

No opinion: 11%