RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

October 17, 2024

A MYSTERIOUS HACKING GROUP HAS 2 NEW TOOLS TO STEAL DATA FROM AIR-GAPPED MACHINES

Dan Goodin | Wired | October 12, 2024

Researchers have unearthed two sophisticated tool sets that a nation-state hacking group—possibly from Russia—used to steal sensitive data stored on air-gapped devices, meaning those that are deliberately isolated from the internet or other networks to safeguard them from malware. One of the custom tool collections was used starting in 2019 against a South Asian embassy in Belarus. A largely different tool set created by the same threat group infected a European Union government organization three years later. Researchers from ESET, the security firm that discovered the toolkits, said some of the components in both were identical to those fellow security firm Kaspersky described in research published last year and attributed to an unknown group, tracked as GoldenJackal, working for a nation-state. Based on the overlap, ESET has concluded that the same group is behind all the attacks observed by both firms. The practice of air gapping is typically reserved for the most sensitive networks or devices connected to them, such as those used in systems for voting, industrial control, manufacturing, and power generation. A host of malware used in espionage hacking over the past 15 years (for instance, here and here) demonstrate that air gapping isn't a foolproof protection.

Read the full article here.

WHITE HOUSE FORMS EMERGENCY TEAM TO DEAL WITH CHINA ESPIONAGE HACK

Ellen Nakashima | The Washington Post | October 11, 2024

The Biden administration this week stood up a multi-agency team to confront a growing crisis involving Chinese cyberattacks of U.S. telecommunications companies believed to be for intelligence gathering. The breach now has affected "about 10 or 12" companies, two people familiar with the investigation said, speaking like others interviewed for this article on the condition of anonymity because of the matter's sensitivity. The people did not specify if the companies were all American firms or if some were subsidiaries. At least three major companies were breached: AT&T, Verizon and Lumen. All have declined to comment. The U.S. government, the companies themselves and security firms that are helping investigate the intrusions still do not know how the attacker first penetrated the companies' networks. That lack of a clear entry point is making it difficult to kick the attacker out, several people familiar with the matter said.

Read the full article here.

U.S. OFFICIALS RACE TO UNDERSTAND SEVERITY OF CHINA'S SALT TYPHOON HACKS

Dustin Volz and Drew FitzGerald | The Wall Street Journal | October 11, 2024

U.S. officials are racing to understand the full scope of a China-linked hack of major U.S. broadband providers, as concerns mount from members of Congress that the breach could amount to a devastating counterintelligence failure. Federal authorities and cybersecurity investigators are probing the breaches of Verizon Communications, AT&T and Lumen Technologies. A stealthy hacking group known as Salt Typhoon tied to Chinese intelligence is believed to be responsible. The compromises may have allowed hackers to access information from systems the federal government uses for court-authorized network wiretapping requests, The Wall Street Journal reported last week. Among the concerns are that the hackers may have essentially been able to spy on the U.S. government's efforts to surveil Chinese threats, including the FBI's investigations.

Read the full article here.

AGENCIES WARN ABOUT RUSSIAN GOVERNMENT HACKERS GOING AFTER UNPATCHED VULNERABILITIES

Tim Starks | CYBERSCOOP | October 11, 2024

Russian government hackers are targeting known, unpatched vulnerabilities to victimize specific organizations like governments and defense contractors while also scanning the internet for any susceptible systems to attack, U.S. and U.K. cyber agencies said in a joint alert. The threat actors tied to the Russian Foreign Intelligence Service (SVR) "are highly capable of and interested in exploiting software vulnerabilities" in order to both gain initial access to their target organization and then move around in its systems, the Thursday advisory states. It's an attempt by the FBI, the National Security Agency, Cyber National Mission Force and the United Kingdom's National Cyber Security Centre to warn the public about the tactics and techniques the SVR has employed in recent attacks. It's an update of a 2021 advisory. They wrote that there are two types of target entities for the SVR attackers: "targets of intent," which includes tech companies, think tanks and international organizations, and also "targets of opportunity."

Read the full article here.

LAWMAKERS PRESS AGENCIES, TELECOMS FOR MORE DETAILS ON SALT TYPHOON HACKS

Derek B. Johnson | CYBERSCOOP | October 11, 2024

Members of Congress are pressing federal agencies and telecommunications companies for more information about a reported Chinese government-backed hacking campaign that breached the networks of at least three major U.S. telecoms. Earlier this month, the Wall Street Journal reported that a hacking group tied to Beijing successfully broke into the networks of Verizon, AT&T and Lumen Technologies. The hackers reportedly went undetected for months, possibly gaining access to systems and infrastructure used to process court-authorized wiretaps. On Thursday, Republican and Democratic leaders on the House Energy and Commerce Committee wrote to the three telecommunication firms asking for more information on their response, calling the incident "extremely alarming for both economic and national security reasons."

Read the full article here.

CMMC 2.0 FINAL RULE RELEASED: NEW COMPLIANCE STANDARDS SET TO BEGIN NEXT YEAR

Carley Welch | Breaking Defense | October 11, 2024

The final rule for the long-awaited Cybersecurity Maturity Model Certification (CMMC) 2.0, which sets new standards for contractors who handle controlled unclassified information (CIU), was released today for public inspection and will hit the federal register on Oct. 15. Starting in 2025, the Department of Defense will begin to implement its requirement that all defense contractors be CMMC compliant at the time a contract is awarded. However, in order to avoid a scramble to meet the new regulations with little notice, those requirements will become mandatory after a three-year phase-in period. "The DoD's follow-on Defense Federal Acquisition Regulation Supplement (DFARS) rule change to contractually implement the CMMC Program will be published in early to mid-2025," a DoD press release said.

Read the full article here.

CHINESE RESEARCHERS BREAK RSA ENCRYPTION WITH A QUANTUM COMPUTER

Gyana Swain | CSO | October 14, 2024

In a potentially alarming development for global cybersecurity, Chinese researchers have unveiled a method using D-Wave's quantum annealing systems to crack classic encryption, potentially accelerating the timeline for when quantum computers could pose a real threat to widely used cryptographic systems. Published in the Chinese Journal of Computers under the title "Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage," the paper outlined how D-Wave's machines were used to break RSA encryption and attack symmetric encryption systems, raising serious questions about the future of cybersecurity. The research team, led by Wang Chao from Shanghai University, found that D-Wave's quantum computers can optimize problem-solving in a way that makes it possible to attack encryption methods such as RSA.

Read the full article here.

SCALE OF CHINESE SPYING OVERWHELMS WESTERN GOVERNMENTS

Max Colchester and Daniel Michaels | The Wall Street Journal | October 14, 2024

Beijing is conducting espionage activities on what Western governments say is an unprecedented scale, mobilizing security agencies, private companies and Chinese civilians in its quest to undermine rival states and bolster the country's economy. Rarely does a week go by without a warning from a Western intelligence agency about the threat that China presents. Last month alone, the Federal Bureau of Investigation said a Chinese state-linked firm hacked 260,000 internet-connected devices, including cameras and routers, in the U.S., Britain, France, Romania and elsewhere. A Congressional probe said Chinese cargo cranes used at U.S. seaports had embedded technology that could allow Beijing to secretly control them. The U.S. government alleged that a former top aide to New York Gov. Kathy Hochul was a Chinese agent. U.S. officials last week launched an effort to understand the consequences of the latest Chinese hack, which compromised systems the federal government uses for court-authorized network wiretapping requests.

Read the full article here.

RISING CYBERSECURITY THREATS TARGET U.S. HIGHER EDUCATION INSTITUTIONS

Scoop News Group | EDSCOOP | October 14, 2024

With nearly 6,000 higher education institutions housing vast amounts of sensitive data—ranging from personal information to research with national security implications—colleges and universities have become prime targets for cybercriminals and nation-state actors. Limited resources and complex IT systems, however, have left these institutions increasingly vulnerable to attacks, prompting higher education officials to look for a more strategic and layered defense approach, according to a new report. Higher education institutions face unique challenges due to the diversity and scale of their operations. Universities manage a wide range of services that depend on different technology platforms, starting with online education but also including housing, retail, financial services, sporting events and government-funded research.

Read the full article here.

MICROSOFT DIGITAL DEFENSE REPORT 2024

Microsoft | October 2024

The data, insights, and events in this report represent July 2023 through June 2024 (Microsoft fscal year 2024), unless otherwise noted. Please note that due to rounding, the percentages in some charts may not total 100%. Relevant discussion from the 2023 edition of the Microsoft Digital Defense Report is referenced in this report. You can access the 2023 report in the archive section at aka.ms/MDDR.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

5 CYBER READINESS PRACTICES TO BOOST YOUR CYBERSECURITY

Travelers

Cyber threats are an ever-present concern across businesses, nonprofits and public entities with organizations of all sizes often targeted by advanced and evolving attacks. The annual Travelers Risk Index shows cybersecurity persistently remains a top concern. The impact of cybercrimes like ransomware attacks, social engineering fraud and business email compromise make the implementation of robust cyber readiness practices essential for every organization. Implementing these Travelers cyber readiness practices can help achieve a high five for cyber readiness in protecting your sensitive data, trust and operations. Security and privacy protection challenges are ubiquitous. According to Tim Francis, Travelers Enterprise Cyber Lead, protecting privacy and sensitive data is essential for all companies. He recommends all organizations adopt a culture that will constantly strive to protect systems, privacy and sensitive data.

Read the full article here.

CYBERSECURITY MATURITY MODEL CERTIFICATION

Chief Information Officer (U.S. Department of Defense)

With this final rule, DoD establishes the Cybersecurity Maturity Model Certification (CMMC) Program in order to verify contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The mechanisms discussed in this rule will allow the Department to confirm a defense contractor or subcontractor has implemented the security requirements for a specified CMMC level and is maintaining that status (meaning level and assessment type) across the contract period of performance. This rule will be updated as needed, using the appropriate rulemaking process, to address evolving cybersecurity standards, requirements, threats, and other relevant changes.

View the full resource here.

SAFEGUARDING INTERNATIONAL SCIENCE: RESEARCH SECURITY FRAMEWORK

Gregory F. Strouse, Claire M. Saundry, Timothy Wood, Philip Bennett, and Mary Bedner | NIST
August 31, 2023

The U.S. science and research ecosystem retains its leadership by actively engaging with the global community through the conduct of mutually beneficial collaborative research and the welcoming of international scientists. Coupled with that, the national and economic security of the United States depends on effective risk management practices for organizations that engage in international collaborative research to protect against undue foreign influence and interference.

View the full resource here.

CYBER ESPIONAGE JOB AID

Defense Counterintelligence and Security Agency | August 2024

The malicious theft of data, information, or intellectual property from, and/or through computer systems. Unlike traditional espionage, which might involve physical infiltration or human intelligence sources (HUMINT), cyber espionage leverages malware, spyware, and phishing attacks to exploit vulnerabilities in computer systems and networks. Some methods include social engineering, malware distribution, advanced persistent threat (APT), watering hole attacks, and spear phishing, but this list is by no means all-inclusive.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute