THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

25 August 2021

You may need to manually copy/paste/execute hyperlinks depicted below if your computer's security settings disable embedded hyperlinks displayed within a PDF file

PERIPHERAL DEVICE'S SOFTWARE GIVING USERS ADMIN RIGHTS

Security researchers have identified Danish software vendor "Steelseries", whose software is used by a wide variety of enthusiast-level mouse and keyboard peripheral devices, can be exploited to grant Administrator privileges (from a command prompt window) when the device is plugged into a computer. Although the vendor has patched their software to remove the exploit, a hacker can theoretically leverage the older software version to exploit a computer.

https://www.bleepingcomputer.com/news/security/steelseries-bug-gives-windows-10-admin-rights-by-plugging-in-a-device/?&web_view=true

---

CRITICAL INFRASTRUCTURE ATTACKS CONTINUE TO ESCALATE

A cybersecurity analysis of cyberattacks launched against Critical Infrastructure facilities has identified a whopping 156% increase (as compared against 2020 statistics). Many of the attacks were poorly executed by inexperienced hackers – however, every cyberattack consumes scarce resources, and serves as training runs that educate hackers to later execute more successful attempts. Over 40% of all ransomware attacks in 2021 were launched against Critical Infrastructure facilities – these events (and more) are documented within a downloadable analytical report referenced from within the article.

https://cyware.com/news/cyberattack-trends-critical-infrastructure-edition-23bd1931

BEC SCAM HITS SMALL TOWN WITH A $2.3m LEARNING OPPORTUNITY

The town of Peterborough, NH (pop: 6284), fell victim to a Business Email Compromise (BEC) scam that resulted in a loss of $2.3 million. Scammers leveraged spoofed email accounts and convincingly falsified documents that were emailed to city employees that tricked them into transferring large amounts of money to criminal-owned bank accounts. The Secret Service determined the money was immediately laundered, converted to cryptocurrency and is irretrievable. $2.3 million accounts for nearly 15% of the small town's annual operating budget.

https://therecord.media/scammers-steal-2-3-million-from-small-us-town/?web_view=true

---

HACKER WHO PULLED OFF $600 MILLION HEIST OFFERED A JOB

A cryptocurrency vendor made history as incurring the largest-ever cryptocurrency theft - $600 million. Shortly after the theft, the hacker agreed to return the stolen virtual cash (which did happen) – and in an even more bizarre twist, the cryptocurrency company offered the hacker a job as its "Chief Security Advisor" and paid the hacker $500k bounty to the individual to return the money.

https://www.cnbc.com/2021/08/17/poly-network-cryptocurrency-hack-latest.html

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from unauthorized access, theft or espionage

Source
This publication incorporates open source news articles to educate readers on cyber security matters IAW USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Newsletter Team
* SA Sylvia Romero
Albuquerque FBI
* CI Agent Scott Daughtry
Purple Arrow Founder

Subscription/Questions
Click HERE to request for your employer-provided email address to be added to this product's distribution list

Purple Arrow Overview
The Purple Arrow Working Group formed in 2009 to address suspicious reporting originating from New Mexico (NM) cleared companies. Purple Arrow is a subset of the NM CI Working Group

Purple Arrow Members
Our membership includes representatives from these New Mexico-focused agencies: 902nd MI, AFOSI, DOE, DCSA, DTRA, FBI, HSI, NCIS and the US Attorney Office

Distribution
You may freely forward this product to U.S. person co-workers or other U.S. agency / U.S. company managed email accounts

Personal Email/Foreigners
The FBI will *not* send Purple Arrow products to a non-United States employer-provided email account (e.g. Hotmail, Gmail)

JFAC Partnership
The DoD's "Joint Federated Assurance Center", aka JFAC, maintains a searchable archive of this newsletter on their U.S. Navy hosted website: https://jfac.navy.mil/JFAC/partners/cybershield

UNSECURED CLOUD STORAGE "BUCKETS" BECOMING COMMONPLACE

Cloud-based storage has become a standard for many companies/organizations to store mass amounts of data – much of it being highly sensitive data – to reduce IT costs and enhance data sharing throughout their workforce. Unfortunately, these buckets are increasingly misconfigured and openly exposing that data to anyone that is looking for it. One security team's analysis of unsecured buckets identified over 4000 of them (some were highly respected businesses and law firms) – and the problem is growing.

https://www.theregister.com/2020/08/03/leaky_s3_buckets/

CONTI RANSOMWARE HITS U.S. CELLULAR NETWORK DESIGN COMPANY

Conti is believed to be a Russia-based hacking crew whose ransomware-as-a-service malware shares source code with several other malware authors – they are a serious threat to global networks, and one that the FBI has issued at least one cyber alert for. Conti recently infiltrated a U.S. cell phone design company (who is a subsidiary of the massive Finnish telecommunication company Nokia) that helps businesses/corporations build robust 4G and 5G networks. The hacking crew claimed to have stolen 250GB of sensitive data to the cloud before encrypting the business' data stored on their company network and threatening to leak the data if the ransom isn't paid. This event follows news of other telecommunication data breaches that have made headlines over the past month – likely because these companies demand massive amounts of PII from their customers (and store that data within their company network) to active a cell phone account.

https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/?&web_view=true

---

RETAIL COMPANIES INCREASINGLY TARGETED BY CYBER CRIME

The retail industry has historically faced challenges dealing with crime – typically via shoplifters and insider threat. Within the cyber realm, this business sector has been hit hard by cyber extortion schemes – cybercriminals that infiltrate their company networks typically don't encrypt their stored data, instead electing to inform the victim that they will leak the stolen company information online if the extortion monies aren't paid (to diminish consumer's faith that the company protects their PII and impact sales).

https://cybernews.com/news/retail-became-a-top-target-for-ransomware-and-data-theft/?&web_view=true

---