THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

18 November 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

SURVEY OF CRITICAL INFRASTRUCTURE PROS YIELDS BAD NEWS

A California-based security firm conducted a survey of CIOs and CISOs working in the energy and critical infrastructure sectors throughout Germany, USA, Australia and the U.K. An overwhelming percentage of responses (83%) stated their network had at least one cybersecurity breach in the past three years. A majority (78%) of those polled stated a major challenge they face is the use of multi-vendor technologies within their network, which ratchets up the complexity of IT challenges.

https://www.itpro.co.uk/security/cyber-security/361518/83-of-critical-infrastructure-companies-have-experienced-breaches-in

---

FBI IDENTIFIES VULNERABLE VPN NETWORK DEVICES

The FBI's forensic examination of an Advanced Persistent Threat (APT) that was targeting a specific U.S. based company's VPN products concluded this week. Their findings determined the malicious actors were targeting a zero-day vulnerability inherit within several of the company's offerings, starting in May 2021. The vulnerability permitted hackers to exploit the device's firmware to install software onto the device that provided them with root-level access. The company issued a firmware update on 16 Nov 2021.

https://therecord.media/fbi-an-apt-abused-a-zero-day-in-fatpipe-vpns-for-six-months/

JOINT CYBER ADVISORY WARNS OF IRAN TARGETING OF PRODUCTS

A recently issued joint advisory via the FBI, CISA and cyber agencies representing Australia and the U.K. warns of Iran's cyber hacking teams targeting efforts against two popular products. The state-sponsored hackers are leveraging identified vulnerabilities to deploy ransomware onto compromised systems. The article provides port numbers and a TCP/IP address of concern.

https://www.bleepingcomputer.com/news/security/us-uk-warn-of-iranian-hackers-exploiting-microsoft-exchange-fortinet/

BEWARE OF TINY FONTS WITHIN HTML-FORMATTED EMAILS

A new phishing method, coined "one Font", has been discovered by cybersecurity researchers which leverages 1 point sized font within the HTML-formatted email (8 point –vs- .) to bypass email server filters which use natural language rules to detect/quarantine mass marketing emails. This new phishing method emulates the 2018-era "ZeroFont" campaign, which embedded zero-sized text within email to trick email server scanning algorithms into permitting the malicious email to make it into recipient's inboxes.

https://heimdalsecurity.com/blog/email-filters-duped-by-tiny-font-size-in-bec-phishing-attacks/?web_view=true
https://www.cybertalk.org/2021/11/11/this-tiny-font-phishing-campaign-could-fool-your-o365-email-filters/

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 Joshua Rock
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

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the Purple Arrow Working Group or NM CI Working Group

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

RUSSIAN AND CHINESE HACKERS TEAMING UP VIA DARKWEB FORUMS

Cybersecurity and law enforcement professionals closely monitor underground/DarkWeb/hacker forums to monitor discussions, identify new exploits and potentially intercept hacking operations before they are deployed. One particular Russian-language hacking forum has featured an unusual uptick in Russian hackers extending an olive branch to their Chinese counterparts to collaborate on future hacking operations – and based upon the volume of newly created forum accounts being linked to China, their efforts appear to be paying off.

https://www.bleepingcomputer.com/news/security/russian-ransomware-gangs-start-collaborating-with-chinese-hackers/?&web_view=true

---

BATCH OF 7 MILLION STOLEN EMAIL ADDRESSES POSTED FOR SALE

The recent data breach of a large U.S. based financial services/cryptocurrency/stock market oriented company resulted in the loss of approximately seven million email accounts that were stored on their systems. Hackers infiltrated the network via a compromised employee computer system and proceeded to conduct reconnaissance across its customer support systems to locate/exfiltrate valued data. The hacker, who identified themselves as “pompompurin” (a name associated with a happy golden retriever dog character by a Japanese company in 1996) on the underground forum, is seeking over $10k from buyers for the stolen information.

https://www.bleepingcomputer.com/news/security/7-million-robinhood-user-email-addresses-for-sale-on-hacker-forum/?&web_view=true

---

NORTH KOREAN HACKING GROUP ‘LAZARUS’ RESURFACES

The Lazarus Group was especially prevalent between 2010 and 2020 and is best known for breaching a large U.S. entertainment company in 2014 to steal unreleased movies and employee data. The North Korean government-sponsored hacking group has recently resurfaced to begin targeting IT supply chains and security researchers via an updated version of their ‘DeathNote’ ransomware, which first surfaced back in 2018. Lazarus was identified by one cybersecurity vendor as the most active hacking group of 2020, and have targeted the defense industry via their ‘ThreatNeedle’ malware.

https://cyware.com/news/lazarus-is-back-at-it-again-6faf10e1
https://www.2-spyware.com/remove-deathnote-hackers-ransomware-virus.html
https://securelist.com/lazarus-threatneedle/100803/
