ArxNimbus

CYBERWatch

ISSUE 6 | FEBRUARY 2024

THE CHINESE MAFIA IS RUNNING A SCAM FACTORY

PAGE 3

CISA, FBI WARN OF CHINA-LINKED HACKERS PRE-POSITIONING FOR 'DESTRUCTIVE CYBERATTACKS AGAINST US CRITICAL INFRASTRUCTURE'

Hackers connected to China's government are conducting attacks with the long-term goal of causing physical destruction, according to a new advisory from several of the world's leading cyber agencies.

IRAN-ISRAEL CYBER WAR GOES GLOBAL

What started off as posturing from the Islamic Republic has turned into more serious cyberattacks against the US.

A MESSAGE FROM OUR CEO

Welcome to our latest newsletter, and thank you for joining us on the critical mission to eradicate cybersecurity risk. In this effort, we face many challenges. We are seeing an emerging pattern of nation-state "grade" attack vectors, and increased sophistication in the efforts of cybersecurity insurers, and a significantly more aggressive stance on the part of regulators. All of these are pointing to a new level in our collective cybersecurity efforts, that we must all make efforts to understand adapt to in our strategies and efforts.

This month we share several vital developments in all these categories and more. Today, our actuarial cyber risk analysis is in use across cyber insurance policies in force for at least fifty of the S&P 500 companies. Local governments, SMBs, health care are benefitting from regulator-approved, data driven risk management. Let us know how far and how fast you're ready to go in managing and reducing these rapidly expanding cyber risks.

R David Moon
CEO/Founder, Arx Nimbus LLC

HEALTHCARE IN FOCUS

HIPPA Journal Review of Security Breaches in 2023

An unwanted record was set in 2023 with 725 large security breaches in healthcare reported HHS, beating the record of 720 healthcare security breaches set the previous year.

CISA's Healthcare Risk and Vulnerability Assessment Reveals Sector-Wide Improvement Areas

CISA urged the healthcare sector to use phishing resistant MFA, implement network segmentation, and verify the implementation of appropriate hardening measures to mitigate cyber risk.

LockBit shows no remorse for ransomware attack on children's hospital

Ransomware gang LockBit is claiming responsibility for an attack on a Chicago children's hospital in an apparent deviation from its previous policy of not targeting nonprofits. Set $800k ransom demand.

Health Care Privacy and Security In 2024: Six Critical Topics to Watch

Reflection on the flurry of ac- tivity in the health care data privacy and security space in 2023 and look ahead to what lay ahead in 2024.

Why HHS' Cybersecurity Concept Paper Falls Short for Healthcare

The recent Cybersecurity concept paper from HHS, while a gesture towards progress, falls critically short of what's imperative in today's climate.

RUSSIAN AND NORTH KOREAN HACKERS USED OPENAI TOOLS TO HONE CYBERATTACKS

Microsoft and OpenAI say that state backed-hackers were using generative AI tools to improve their cyberattacks. The groups used OpenAI tools to draft phishing emails, debug code and research targets.

WEF: AI IS TRANSFORMING CYBERSECURITY: HOW CAN SECURITY EXPERTS RESPOND?

AI has made it easier for cybercriminals to create exploit programs, posing a significant threat to cybersecurity.

DEEPFAKE SCAMMER WALKS OFF WITH $25 MILLION IN FIRST-OF-ITS-KIND AI HEIST

Hong Kong firm reportedly tricked by simulation of multiple people in video chat.

CYBERATTACKS ON CLOROX, JOHNSON CONTROLS COST COMPANIES $76M COMBINED

Cybersecurity incidents in 2023 cost Clorox and Johnson Controls nearly $76 million combined, according to reports filed with the SEC. The inci- dents underscore the painful reality that such attacks cost real money.
SEC Filings: Clorox ; Johnson Controls

HOW CHINESE MAFIA RUNS A SCAM FACTORY IN MYANMAR

In KK Park, on the Myanmar-Thai border, those who refuse to scam face torture, starvation and even murder. DW investigates one of Asia's most brutal scam compounds.

LEGAL/REGULATORY

WHY THE US NEEDS COMPREHENSIVE CYBERSECURITY LEGISLATION

Taking a hands-off approach to cybersecurity is no longer good enough for any organization. One thing is clear, though: cybersecurity has reached a critical tippin point.

REDEFINING THE CYBERSECURITY PARADIGM: CISOS AND BOARDS IN THE WAKE OF REGULATORY SHAKEUPS

In an age where cyber threats loom large over the financial sector's horizon, recent regulatory actions signal a paradigm shift in the regulatory framework governing cybersecurity.

THE FTC'S EXPANDED CYBERSECURITY REQUIREMENTS AFFECTING NON-BANKING SMALL BUSINESSES

The expansion of the FTC's Safeguards Rule will require businesses to notify customers/FTC of cyber breaches that had previously been excluded from reporting regulations.

ONCD IS STUDYING 'LIABILITY REGIMES' FOR SOFTWARE FLAWS

Progress report on Biden Admin Executive Order on Artificial Intelligence.

SEC FINAL RULE: CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE AND INCIDENT DISCLOSURE

Overview and recommendations on how to comply with new SEC Rules & Reporting requirements from Blackberry Intelligence Unit.