ArxNimbus

CYBERWatch

ISSUE 10 | SEPT 2024

NEW REPORT: 85% OF FIRMS FACE CYBER INCIDENTS. 11% FROM SHADOW IT.

SEE PAGE 3

LINUX VERSION OF NEW CICADA RANSOMWARE TARGETS VMWARE ESXI SERVERS

A new ransomware-as-a-service (RaaS) operation is impersonating the legitimate Cicada 3301 organization and has already listed 19 victims on its extortion portal, as it quickly attacked companies worldwide.

The new cybercrime operation is named after and uses the same logo as the mysterious 2012-2014 online/real-world game named Cicada 3301 that involved elaborate cryptographic puzzles.

WHY IS THE MIDDLE EAST LOSING SO MUCH MONEY TO CYBERCRIME?

Cybercrime costs governments and businesses trillions of dollars every year. But it costs some more than others.

In 2023, cybercrime in the Middle East cost just over $8 million (€7.2 million) per incident, according to research funded by IBM that looked into data breaches in 16 countries. That puts Saudi Arabia and the United Arab Emirates – where the IBM study focussed – second in the world when it comes to this kind of financial damage.

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

Initial Conference Takes Place for Consolidated Change Healthcare Data Breach Lawsuit

Dozens of lawsuits have been filed over the Change Healthcare cyberattack and data breach. With so many lawsuits to defend in multiple districts, Change Healthcare filed a motion for transfer and centralization of all actions related to the cyberattack and data breach with the U.S. Judicial Panel on Multidistrict Litigation (JPML).

A hospital paid 4 BTC (Bitcoin) - roughly $55,000 - to regain access to its computer systems

A hospital in Indiana paid over $50K last week in order to recover files encrypted in a ransomware attack. Hancock Regional Hospital, a facility in Greenfield, about half an hour outside of Indianapolis, paid approximately $55,000 in Bitcoin, to stop the bleeding on Friday. The Indy Star first reported on the attack on Friday, a day before the hospital decided to pay the costly ransom: 4 BTC.

Cyber attacks increase as healthcare sector faces surge

A major supplier of cloud-first security solutions, Barracuda Networks, Inc., recently released statistics indicating that more than one in five (21%) of ransomware incidents that were reported affected healthcare businesses in the previous year..

Cyber Insurers Are Intensely Scrutinizing Healthcare Clients

As threat actors continue to evolve their attacks to circumvent security measures, cyber insurers are raising the bar for prospective healthcare security clients. Underwriters are increasing their scrutiny and adding new coverage requirements, said Chris Henderson of cybersecurity company Huntress.

RUSSIAN MILITARY HACKERS LINKED TO CRITICAL INFRASTRUCTURE ATTACKS

The United States and its allies have linked a group of Russian hackers (tracked as Cadet Blizard and Ember Bear) behind global critical infrastructure attacks to Unit 29155 of Russia's Main Directorate of the General Staff of the Armed Forces (also known as GRU).

LEAKED DISNEY DATA REVEALS FINANCIAL AND STRATEGY SECRETS

Data trove sheds light on operations, exposes personal data of some staff and customers

MARSH MCLENNAN AND ZURICH URGE PUBLIC-PRIVATE ACTION TO BRIDGE CYBER PROTECTION GAP AND BOOST RESILIENCE

New York, September 5, 2024 – A new whitepaper from Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people, and Zurich Insurance Group (SWX: ZURN), a leading global multi-line insurer and provider of resilience services, highlights the critical need for greater public sector involvement to strengthen societal resilience in the event a catastrophic cyber event occurs..

NEW REPORT: 85% OF FIRMS FACE CYBER INCIDENTS, 11% FROM SHADOW IT

"Employees who use applications, devices, or cloud services [...] not approved by the IT department believe that if those IT products come from trusted providers, they should be protected and safe," said Alexey Vovk, head of information security at Kaspersky.

FORTINET CONFIRMS BREACH THAT LIKELY LEAKED 440GB OF CUSTOMER DATA

The cybersecurity company said a threat actor had unauthorized access to files on a third-party cloud-shared drive.

CHINESE BOTNET INFECTS 260,000 SOHO ROUTERS, IP CAMERAS WITH MALWARE

The FBI and cybersecurity researchers have disrupted a massive Chinese botnet called "Raptor Train" that infected over 260,000 networking devices to target critical infrastructure in the US and in other countries.

READ THEIR LIPS WITH AI

You can now upload a video of any speaker and identify inaudible speech using our model.

KASPERSKY DELETES ITSELF, INSTALLS ULTRAAV ANTIVIRUS WITHOUT WARNING

Starting Thursday, Russian cybersecurity company Kaspersky deleted its anti-malware software from customers' computers across the United States and automatically replaced it with UltraAV's antivirus solution.

#GARTNERSEC: ZERO FAILURE TOLERANCE, A CYBERSECURITY MYTH HOLDING BACK ORGANIZATIONS

Security leaders must steer away from a zero tolerance for failure approach to cybersecurity and adopt and embrace augmented cybersecurity in order to thrive.