G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

JULY 2022

Highlights

[North Korean ‘Maui’ Ransomware is No Vacation for Healthcare Providers](#)

[United States Cybersecurity Labor Gap is Growing; 700,000 US Jobs are Unfilled](#)

[Rise in Cybercrime Due to Covid-19 Pandemic, Increased Device Connectivity](#)

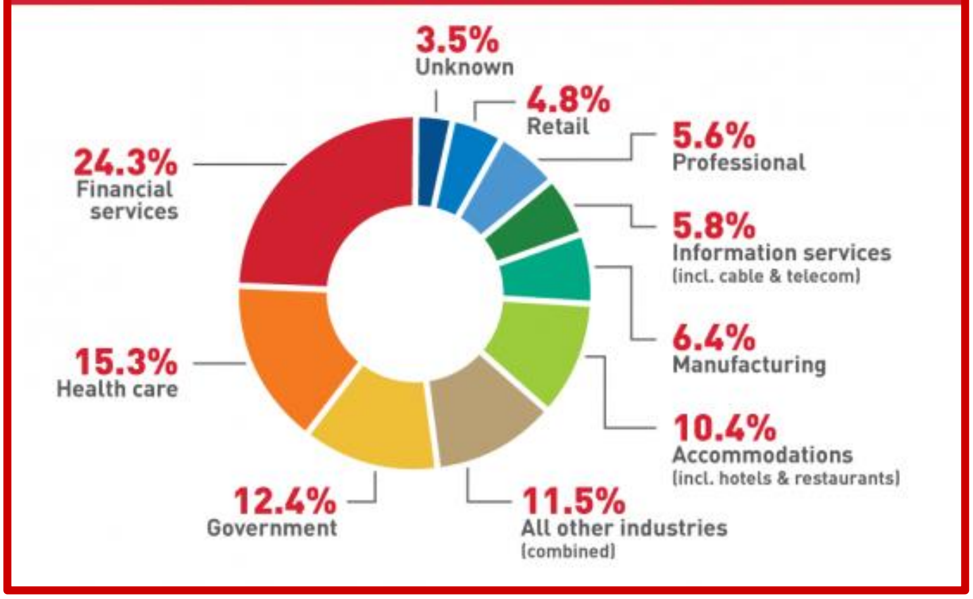
[Cybercriminals Hack into Shanghai Police Database Leaking One Billion Chinese Users’ Data](#)

[Upcoming Conferences](#)

24.3 percent of all data breaches occur at banks, credit unions and other financial institutions

[2017 Verizon Data Breach Investigations](#)

Where Breaches Happen



North Korean ‘Maui’ Ransomware is No Vacation For Healthcare Providers

Healthcare and public health sectors are increasingly vulnerable to ransomware attacks. These groups have a treasure trove of patient data, data which is much more information rich then standard consumer data. Additionally, healthcare providers and their partners are often compelled to pay, as not having access to patient data has been shown to increase patient mortality rates.

Healthcare debt collections company Professional Finance Company recently disclosed a ransomware attack that occurred in February of 2022, exposing patient data from more then 650 vendors of the company, including Arizona-based nonprofit Banner Health & Nevada physician network Renown Health. North Korean government-sponsored hackers have been targeting companies in the healthcare industry for over a year according to a recently released alert by the FBI, CISA and Treasury.

US government officials stress the importance of maintaining an offline (physically disconnected) backup of data, and to make sure that the backup data is encrypted and regularly backed up and tested. For more information on how to combat the Maui ransomware, click on this link.

Maui Ransomware Technical Details:
Maui ransomware (maui.exe) is an encryption binary. According to industry analysis of a sample of Maui (SHA256: 5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e) provided in Stairwell Threat Report: Maui Ransomware—the ransomware appears to be designed for manual execution [TA0002] by a remote actor. The remote actor uses command-line interface [T1059.008] to interact with the malware and to identify files to encrypt.

Maui uses a combination of Advanced Encryption Standard (AES), RSA, and XOR encryption to encrypt [T1486] target files:

1. Maui encrypts target files with AES 128-bit encryption. Each encrypted file has a unique AES key, and each file contains a custom header with the file’s original path, allowing Maui to identify previously encrypted files. The header also contains encrypted copies of the AES key.
2. Maui encrypts each AES key with RSA encryption.
   - Maui loads the RSA public (maui.key) and private (maui.evd) keys in the same directory as itself.

3. Maui encodes the RSA public key (maui.key) using XOR encryption. The XOR key is generated from hard drive information (\\.\PhysicalDrive0).

During encryption, Maui creates a temporary file for each file it encrypts using GetTempFileNameW(). Maui uses the temporary to stage output from encryption. After encrypting files, Maui creates maui.log, which contains output from Maui execution. Actors likely exfiltrate [TA0010] maui.log and decrypt the file using associated decryption tools. See Stairwell Threat Report: Maui Ransomware for additional information on Maui ransomware, including YARA rules and a key extractor.

The Justice Department just announced a complaint filed in the District of Kansas to forfeit cryptocurrency paid as ransom to North Korean. In May 2022, the FBI filed a sealed seizure warrant for the funds worth approximately half a million dollars. The seized funds include ransoms paid by health care providers in Kansas and Colorado.

North Korean hackers used Maui to encrypt the files and servers of a medical center in the District of Kansas. After more than a week of being unable to access encrypted servers, the Kansas hospital paid approximately $100,000 in ransomware. The FBI was able to identify the never-before-seen North Korean ransomware and trace the cryptocurrency to China-based money launderers.

> “Thanks to rapid reporting and cooperation from a victim, the FBI and Justice Department prosecutors have disrupted the activities of a North Korean state-sponsored group deploying ransomware known as ‘Maui.’ Not only did this allow us to recover their ransom payment as well as a ransom paid by previously unknown victims, but we were also able to identify a previously unidentified ransomware strain. The approach used in this case exemplifies how the Department of Justice is attacking malicious cyber activity from all angles to disrupt bad actors and prevent the next victim.”
> Deputy Attorney General Lisa O. Monaco, US Dept of Justice

Then, as a result, in April 2022, the FBI observed an approximately $120,000 Bitcoin payment into one of the seized cryptocurrency accounts identified thanks to the cooperation of the Kansas hospital. The FBI’s investigation confirmed that a medical provider in Colorado had just paid a ransom after being hacked by actors using the same Maui ransomware strain. In May 2022, the FBI seized the contents of two cryptocurrency accounts that had received funds from the Kansas and Colorado health care providers. The District of Kansas then began proceedings to forfeit the hackers’ funds and return the stolen money to the victims.

United States Cybersecurity Labor Gap Is Growing; 700,000 US Jobs are Unfilled

United States cybersecurity is in need of more warm bodies. One out of every three new cybersecurity job listings go unfilled, according to National Security Director Chris Inglis. The number of unfilled cybersecurity positions has risen from 500,000 to 700,000 over the last few months, a 40% increase. While the need for cybersecurity professionals is at an all-time high, Sandra Wheatley Smerdon, Senior Vice President of Threat Intelligence at Fortinet, notes that people who consider working in a 'helping' position don't always consider cybersecurity as a career choice:

> *When someone considers a career in a "helping" profession, their thoughts naturally turn to doctors, nurses, teachers, and first responders like police officers or emergency medical technicians. These people devote their lives to helping to keep the world safe and healthy. And although a career in cybersecurity might not be the first job to come to mind, cybersecurity professionals protect the digital world from cybercrime much the same way that police officers protect neighborhoods.*

Recently the Biden administration announced the Cybersecurity Apprenticeship Sprint, a White House initiative to reduce the employment gap in the cybersecurity space. The campaign aims to do so through public education of the availability of cybersecurity apprenticeships throughout the country, and by recruiting and enabling employers to launch apprenticeship programs in as little as 48 hours using industry-vetted standards. Secretary of Labor Marty Walsh explains the benefits of the program:

> *The 120-Day Cybersecurity Apprenticeship Sprint will increase awareness of current successful cybersecurity-related Registered Apprenticeship programs while recruiting employers and industry associations to expand and promote Registered Apprenticeships as a means to provide workers with high-quality, earn-as-you-learn training for good-paying cyber security jobs. These newly trained workers will help protect our critical infrastructure, advance our digital way of life, strengthen our economy and improve access to cybersecurity career paths for underrepresented communities, especially women, people of color, veterans and people with disabilities.*

Rise In Cybercrime Due to COVID-19 Pandemic, Increased Device Connectivity

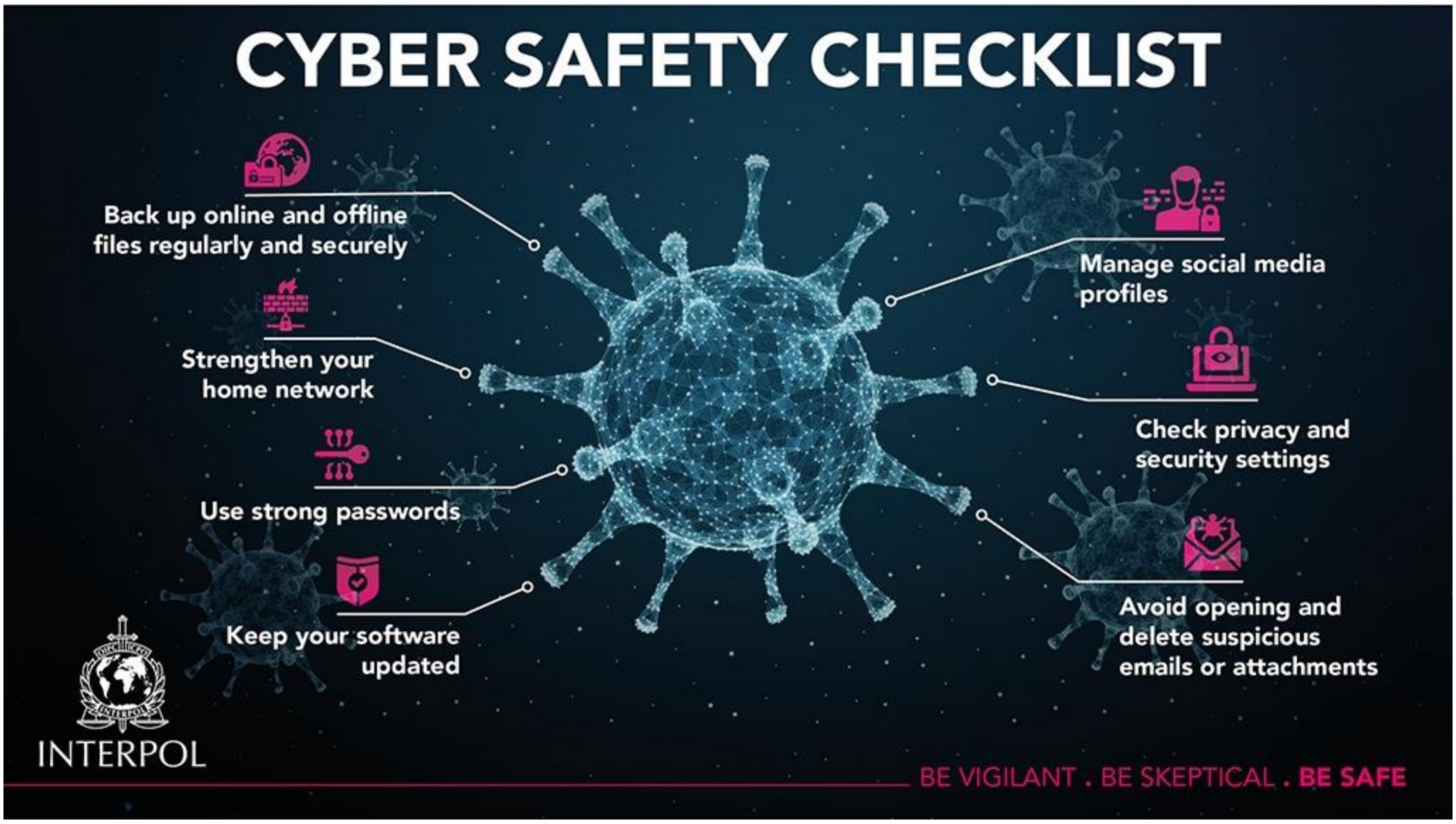
Alongside the rise in cybersecurity positions has been a rise in cybercrimes, with the largest cyber crimes ever being the LinkedIn breach causing the loss of 700M records in 2021, and the 2022 Shanghai police data breach of one billion records that we expand on more in this newsletter. What is responsible for the worldwide rise in cybercrimes? It appears that crime levels have risen due to remote work because of the COVID pandemic and increased IOT device connectivity, increasing the number of attack vectors by which hackers can gain entry into company systems.

According to ThoughtLab, the average number of cyberattacks and data breaches increased by 15.1% from the previous year. Half of US businesses still have not developed a cybersecurity plan, and cybercriminals can penetrate companies with a 93% success rate according to pentesting projects by Positive Technologies. Compromised credentials is the primary attack node (71% of attacks) that cybercriminals use to gain access to company datacenters, often due to the use of simple passwords, highlighting the importance of two-factor identification and zero trust architectures. Complex supply chains and a multitude of interaction points with vendors and third parties underscore the importance of cybersecurity solutions that include vendor and third party risk management.

Varonis provides comprehensive information regarding a variety of cybersecurity topics, offers a free security webinar, and provides the following comprehensive statistics:

- 95 percent of cybersecurity breaches are caused by human error. (World Economic Forum)
- The worldwide information security market is forecast to reach $366.1 billion in 2028. (Fortune Business Insights)
- The U.S. was the target of 46 percent of cyberattacks in 2020, more than double any other country. (Microsoft)
- 68 percent of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only five percent of companies' folders are properly protected. (Varonis)
- 54 percent of companies say their IT departments are not sophisticated enough to handle advanced cyberattacks. (Sophos)

- Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 percent of companies. (Cisco)
- 43 percent of all breaches are insider threats, either intentional or unintentional. (Check Point)
- Data breaches exposed 22 billion records in 2021. (RiskBased Security)
- Approximately 70 percent of breaches in 2021 were financially motivated, while less than five percent were motivated by espionage. (Verizon)
- In 2021, nearly 40 percent of breaches featured phishing, around 11 percent involved malware, and about 22 percent involved hacking. (Verizon)
- There were 1,862 recorded data breaches in 2021, surpassing the 2017 record of 1,506 breaches. (CNET)
- The top malicious email attachment types are .doc and .dot which make up 37 percent; the next highest is .exe at 19.5 percent. (Symantec)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)
- Around 40 percent of the world's population is offline, making them vulnerable targets for cyberattacks if and when they do connect. (Data Reportal)


CYBER SAFETY CHECKLIST
Back up online and offline files regularly and securely
Strengthen your home network
Use strong passwords
Keep your software updated
Manage social media profiles
Check privacy and security settings
Avoid opening and delete suspicious emails or attachments
INTERPOL
BE VIGILANT . BE SKEPTICAL . BE SAFE

Cybercriminals Hack Into Shanghai Police Database Leaking One Billion Chinese Users’ Data

A hacker by the pseudonym “ChinaDan” offered to sell nearly 24 terabytes (24 TB) of data, with information on 1 billion people and several billion case records for 10 Bitcoin (worth about $200,000) on an online hacking forum. The data is purported to have been obtained from the Shanghai National Police Database, and includes people’s names, birthdays, ages and mobile numbers. Luckily, the data is only static information - it doesn’t contain information about people’s activities or whereabouts - but identity theft is still a concern. A major cryptocurrency exchange said it had stepped up verification procedures to guard against fraud attempts such as using personal information from the reported hack to take over people’s accounts.

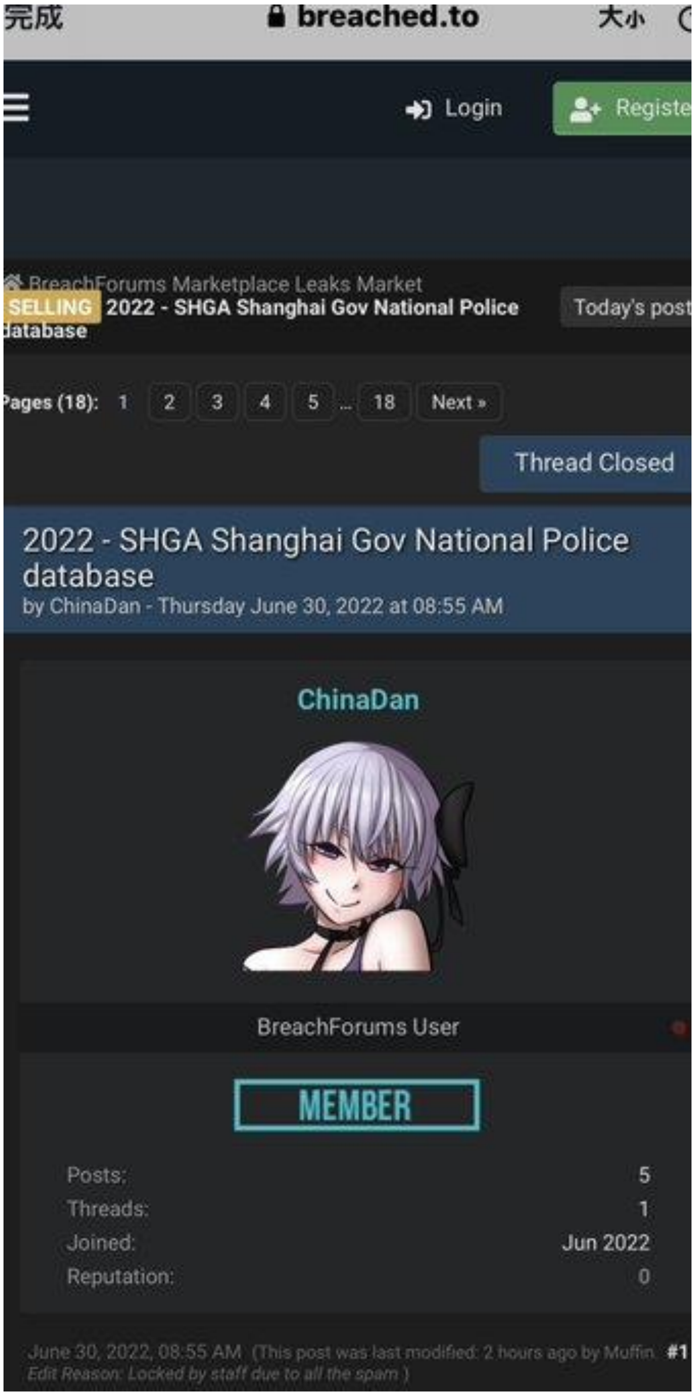
The data breach may be the largest data breach in history if verified. Last year, Facebook was hacked and 533 million users' data was published on a hacking forum. Chinese government censors have shut down keyword searches for ‘Shanghai Data Link’ after widespread discussion of the leak on Chinese social media site Weibo. While the leak is harmful from a cybersecurity perspective, ultimately it may prove to be more embarrassing to the Chinese government than harmful.

Meanwhile, all references to the data breach have been censored on Chinese social media, with blog posts about the breach quickly deleted. "Most Chinese people are asking similar questions, and the ones that are censored and deleted the most are: Has my data been leaked? How much data do they have about me? Why isn't my personal information stored securely?" Charlie Smith, co-founder of the China-based internet censorship watch website GreatFire.org, told RFA.

As one social media user commented wryly after the news broke: "Data is leaked; everyone's running around naked. It's a lovely day on the Chinese internet."

According to a Bloomberg report, the hackers accessed the police database in China’s most populous city and stole sensitive personal information on up to one billion people, including national ID numbers, mobile phone numbers, addresses, medical records, and criminal histories. Binance’s Zhao Changpeng said the attack happened because the Chinese Government developer of the police database wrote a tech blog for the Chinese Software Developer Network (CSDN) and accidentally included the credentials. Mr Changpeng published a screenshot of the credentials published on the blog.

Ren, a U.S. citizen who has lived in China for decades, found out she was a victim of the breach when she received a call from RFA confirming her personal information. "It feels so weird and creepy at the same time, as if all your personal information are just out there," she said. "I also think about my [COVID-19 test results], health code, everything related to me is tied to my passport number. Are they all public?" "What can I do now? I can't change any information, that is my identity in China, and it was leaked from the government. It's annoying, alarming, but I just can't do anything about it."



BreachForums Marketplace Leaks Market

SELLING 2022 - SHGA Shanghai Gov National Police database

2022 - SHGA Shanghai Gov National Police database
by ChinaDan - Thursday June 30, 2022 at 08:55 AM

ChinaDan

BreachForums User

MEMBER

Posts:	5
Threads:	1
Joined:	Jun 2022
Reputation:	0

June 30, 2022, 08:55 AM (This post was last modified: 2 hours ago by Muffin. #1
Edit Reason: Locked by staff due to all the spam)

Upcoming Conferences

July 25-27	Gartner Security & Risk Management Summit, Tokyo
August 2-4	Flash Memory Summit, Santa Clara
August 6-11	Black Hat USA, Vegas
August 11-14	DEF CON 30, Vegas
August 27-28	Blue Team Con, Chicago
August 29-Sept 1	VMwear Explore, San Francisco
September 8	FutureCon, Des Moines
September 12-14	Gartner Security & Risk Management Summit, London
September 13-14	CISO Forum, Virtual
September 14	Cybersecurity Expo, Phoenix
September 19-20	Industry of Things World, Berlin
September 20-22	Dreamforce, San Francisco
September 22-23	Global Cyber Conference, Zurich
September 26-28	InfoSec World, Colorado Springs
September 27-28	International Cyber Expo, London
September 28-29	IoT World, Santa Clara
September 28-30	Spiceworld, Austin, Hybrid
October 3-4	451Nexus, Las Vegas

October 5-6	Evolve, Vegas
October 10-12	ISC Security Congress, Vegas
October 11-13	Google Cloud Next, Virtual
October 17-19	Authenticate 2022, Seattle
October 17-20	Gartner IT Symposium/Xpo, Orlando
October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual

PASSWORD
G2M
RESEARCH
Effective Marketing & Communications
with Quantifiable Results