INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on Internet

SOUTH KOREA'S NUCLEAR RESEARCH AGENCY HACKED

On 18th June 2021, the 'Korea Atomic Energy Research Institute' in South Korea disclosed that the North Korean threat actors used a VPN vulnerability to penetrate their internal networks last month. The Korea Atomic Energy Research Institute, or KAERI, is a government-sponsored institute to research nuclear power and nuclear fuel technology in South Korea. The access logs show that thirteen different IPs abused the vulnerability and gained access to the internal network. Out of these thirteen different IP addresses, one of the IP address is linked to the North-Korean APT group "Kimsuky." Kimsuky APT group is active since 2012 and targets mainly the South Korean government's entities through spear-phishing e-mails. The Kimsuky group is believed to be working for the North Korean Reconnaissance General Bureau intelligence agency.

STORIES INSIDE THIS ISSUE:

KAERI faced criticism for initially denying the intrusion, and later in a press conference, a KAERI spokesperson confirmed the intrusion that took place on 14th May. The name of the VPN server is redacted in the documents presented in the press conference.

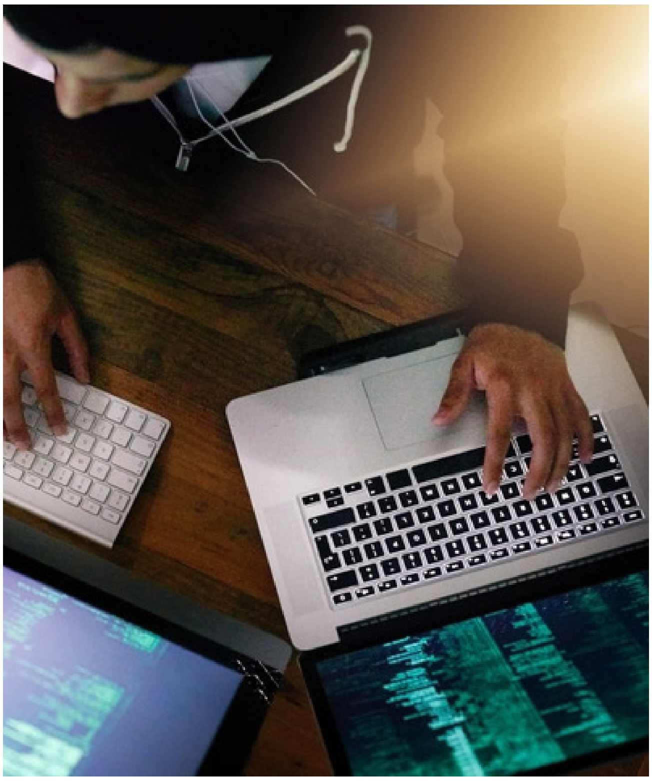
Recently Malwarebytes shared in its blog post about the cyber espionage operations by the Kimsuky APT group. The Korean Internet and Security Agency provided a detailed analysis about the phishing infrastructures and Tools, Techniques, and Procedures (TTPs) used by the Kimsuky APT group to target government entities mainly in South Korea using the 'AppleSeed' backdoor. One of the malware names that translate to "Ministry of Foreign Affairs Edition 2021-05-07" indicates that the malware is designed to target the "Ministry of Foreign Affairs of South Korea."

Source: https://www.bleepingcomputer.com/news/security/south-koreas-nuclear-research-agency-hacked-using-vpn-flaw/

DIRTYMOE MALWARE INFECTS 100,000+ WINDOWS SYSTEM ACCROSS THE WORLD

The DirtyMoe Windows botnet is active since late 2017 and is mainly used to secretly mine cryptocurrency using the victim's computer. The botnet is believed to be operated from China and exploded this year with more than 100,000 infected systems. Other aliases of the malware are PurpleFox, Perkier, and NuggetPhantom. Although the primary feature of the malware is to infect the Windows system to mine cryptocurrency behind the user's back, it is involved in a DDoS attack in 2018.

The DirtyMoe toolkit is delivered through malspam campaigns and lures users to malicious sites hosting the PurpleFox exploit kit. PurpleFox is one of the most used exploits kits of the DirtyMoe malware. DirtyMoe uses EternalBlue and three other exploits to run as a Windows service under system-level privileges. This gives the malware authors the power to reconfigure thousands of instances within a few hours.



The fascinating evolution of DirtyMoe malware from unstable versions to self-defense and hiding techniques are at par with other malware on the internet. The malware authors added a worm module that could propagate to other Windows PCs via the internet. The module performs password brute-force attacks against Windows systems that have SMB ports open to the internet.

Most of the Command and Control (C&C) servers are located in China. The C&C communication uses a unique mechanism to translate the DNS requests. Blocking the C&C servers is not an easy task as the IP addresses are different each time. The malware authors seem to be part of a large and organized group, so the DirtyMoe should be closely monitored.

30 MILLION DELL DEVICES AT RISK WITH REMOTE CODE EXECUTION VULNERABILITY

Researchers found four high-severity vulnerabilities in the BIOSConnect feature of Dell Support Assist. The vulnerabilities allow attackers to gain arbitrary code execution in the pre-boot environment on unpatched devices. The bug affects 129 models of laptops, tablets, and desktops protected by the Secure Boot and Dell Secured-core PCs feature. The affected products include models that are meant for enterprises as well. Secure Boot feature makes sure the system only uses the trusted software to boot the system in order to prevent rogue takeovers of the device. The bugs allow remote attackers to impersonate Dell.com, bypass the Secure Boot protections, and control the victim's machine. The vulnerabilities affect roughly 30 million Dell devices worldwide.

The chain of vulnerabilities carries a cumulative Common Vulnerability Scoring System (CVSS) score of 8.3 out of 10. The vulnerability affects the BIOSConnect feature in Dell SupportAssist that provides remote firmware update and OS recovery features. According to researchers, the specific vulnerability allows an attacker to remotely exploit the UEFI firmware of the host with system privileges. The CVE CVE-2021-21571 leads to an insecure TLS connection from the BIOS of the device to the Dell website. CVE-2021-21572, CVE-2021-21573, and CVE-2021-21574 are three overflow vulnerabilities that affect the OS recovery process and firmware update process. Each of these three overflow vulnerabilities can lead to arbitrary remote code execution. Dell pushed out patches for BIOS on all the models of the affected systems. Dell in its advisory mentioned that CVE-2021-21573 and CVE-2021-21574 are remediated on the server-side. The CVE-2021-21571 and CVE-2021-21572 vulnerabilities require Dell Client BIOS Updates to remediate the vulnerabilities. Dell also provided interim solutions for users who can not immediately update their BIOS. The advisory recommends that users disable BIOSConnect from the BIOS setup page and disable the HTTPS Boot feature.

Source: https://www.dell.com/support/kbdoc/en-in/000188682/dsa-2021-106-dell-client-platform-security-update-for-multiple-vulnerabilities-in-the-supportassist-biosconnect-feature-and-https-boot-feature

INDIA JUMPS 37 PLACES TO RANK 10TH IN GLOBAL CYBERSECURITY INDEX

The Global Cybersecurity Index (GCI) is a trusted reference that measures a country's commitment to cybersecurity. The GCI report is published by the International Telecommunication Union (ITU). The GCI is based on a multi-stakeholder approach that assesses a country's level of development and engagement against five key pillars:

1. Legal Measures
2. Technical Measures
3. Organizational Measures
4. Capacity Development
5. Cooperation

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

In the previous edition of the GCI released in 2018, India ranked 47th. In the 4th edition of the Global Cyber Security Index 2020 (GCI), India made a significant jump of 37 places to rank 10th in the 4th edition of GCI with a global score of 97.5. Countries filled question-based online surveys with 20 indicators that allowed experts to analyze the responses to arrive at an overall GCI score. US bagged first place with an overall GCI score of 100. The UK and Saudi Arabia shared the second rank with a 99.54 GCI score. Estonia ranked third and bagged a score of 99.48. Korea, Singapore, and Spain shared fourth place with a score of 98.52. Russia, the United Arab Emirates, and Malaysia shared the fifth rank with a score of 98.06 each. Lithuania ranked sixth, Japan at seventh, Canada at eighth, France at ninth, with India at tenth rank. In a tweet, India at UN said, "In a big leap, India jumps 37 places to be ranked 10th in Global Cybersecurity Index (GCI) 2020 launched by Int'l Telecommunication Union 4th in Asia-Pacific."

Source: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

NEW NOBELIUM ACTIVITY, MICROSOFT DISCLOSES HACK

The hackers behind one of the most significant data breaches ever to hit the US government started a new worldwide cyber attack. The attack is carried out on more than 150 government agencies, think tanks, and other organizations. Microsoft said in a terse statement that the SolarWinds supply chain attack coordinated by nation-state hackers gained access to a Microsoft employee's computer and used it to execute targeted attacks against the company's customers.

The attackers compromised three entities by password-spraying and brute-forcing techniques to gain unauthorized access to accounts. The three entities are not disclosed by Microsoft. The attackers bombarded the login servers with a large number of credentials. Microsoft, in its blog post, said the attack is "mostly unsuccessful." The customers whose accounts got compromised are contacted through the nation-state notification process.

The discoveries came with the ongoing investigation into Nobelium. Nobelium is the name Microsoft used to track the SolarWinds advanced persistent threat groups. The federal government in a statement said that the Nobelium is part of the Russian government's Federal Security Service.

Microsoft said the type of attack is not new and advised its customers to take security precautions such as enabling multi-factor authentication to protect their environments from this and similar attacks. This attack campaign targeted IT companies, government agencies, non-government organizations, think tanks, and financial institutions. The attack targeted 36 countries in total. Microsoft also said that it detected information-stealing malware on one of their customer support agents. The customer support agents have access to the basic account information of the customers, like billing contact information and the services used by the customers. As part of the ongoing investigation,

Microsoft analyzed that the information stolen from them is used to launch highly targeted attacks as part of their broader campaign. After detection, Microsoft quickly remediated and secured the device. Researchers cited that the company not yet disclosed how long the attackers compromised agents' machines.

Source: https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

MICROSOFT FIXES MAJOR SECURITY FLAW IN EDGE BROWSER

Microsoft recently addressed two critical security holes in the Microsoft Edge browser, one of which can be exploited by an attacker to circumvent security, remotely inject and execute arbitrary code on any website just by sending a message. A universal cross-site scripting (uXSS) vulnerability in Microsoft Edge's translation function left users open to attack. Researchers got a bounty of $20000 USD for finding the vulnerability. Researchers found the bug in Microsoft's Translator that comes pre-installed in the Edge Browsers on Microsoft's operating systems.

The security vulnerability is fixed, and the CVE ID is CVE-2021-34506. The vulnerability is fixed in the latest update of Microsoft Edge Stable Channel (Version 91.0.864.59).

The impact of the vulnerabilities is severe as anyone who visits a website by the Microsoft Edge browser and uses the language translator feature is open to attack. The language translator reads the content in the user's preferred language. Once the user uses the feature, malicious attackers can inject arbitrary code to perform whatever they wanted to and gain full privileges on the system. If the Microsoft Translator is set to auto-translate or activated by the user can call the malicious function set by the attacker.

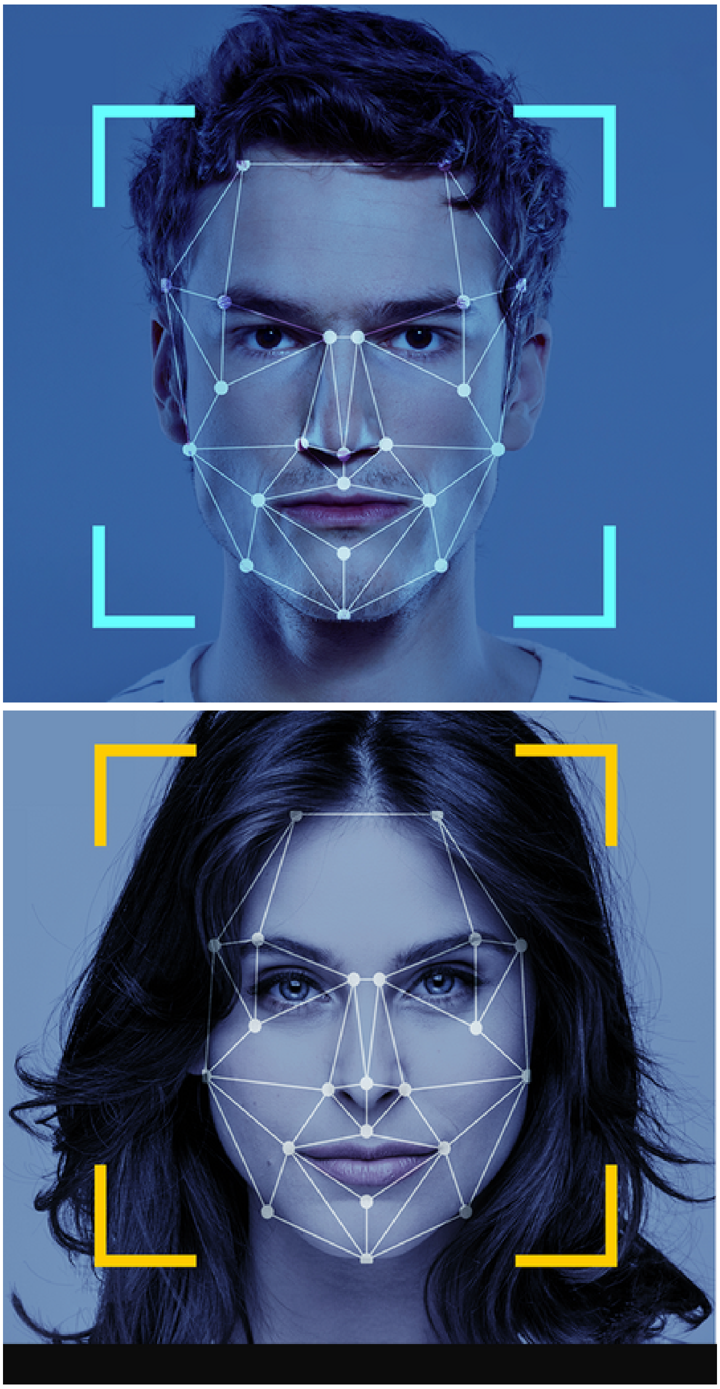
The researchers validated the proof of concept with an experiment. The researchers said that when they created a profile on Facebook with a name in a different language and sent a request to a victim who uses Microsoft Edge browser and the translator tool, it leads to the compromise of the victim's computer.

Researchers even claimed that they could bypass the YouTube application and the Windows Store Application in a victim's computer. The researchers said that when such vulnerabilities are found and exploited, the browser's behavior is affected, and its security features may be bypassed or disabled.

Source: https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

EU BODIES CALL FOR FACIAL RECOGNITION BAN IN PUBLIC PLACES

Two European Union (EU) regulatory bodies teamed up to call a ban on the use of facial recognition and other "biometric and behavioral signals" in public spaces including shops and stadiums. The two privacy bodies, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) cited the use of facial recognition is against draft European Union Rules.



In the European Commission, the union's executive body proposed a regulation that places strict safeguards on the use of artificial intelligence and have implications on the global A.I rules. The proposed regulation includes restrictions on facial recognition in public.

The European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), however want the Eurpean Commission to go a step further, warning “the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces.” They said this should cover recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals in any contexts. The draft proposal although allows high-risk AI applications to be used in areas such as migration and law enforcement. They said AI systems using biometrics to categorize individuals into clusters based on ethnicity, gender, political or sexual orientation should also be banned. The two bodies cited that using the technology to infer a person's emotions should be outlawed except for very specific cases, such as health purposes and "the proposed regulation should also prohibit any type of use of AI for social scoring, as it is against the EU fundamental values and can lead to discrimination,"

Source: https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

SAFEGUARD FROM DIGITAL THEFT

As we advance into the digital world, we see new technological inventions. Cyberspace impacts in a remarkable way the lives of individuals and society. At the same time, crime expanded into cyberspace as well. One of the cybercrimes is identity theft. The notion of identity theft is nothing new and is around for a long time in one form or the other. Large-scale data breaches are constantly affecting business. Millions of users' personal data is available for sale on the dark web. Businesses must recognise the potential devastation of a breach. The reputation damage can devastate the business. In extreme cases, the victim can take legal action like in the case of British Airways.

Identity theft or identity fraud is the "appropriation of an individual's personal information to impersonate that person in a legal sense." A cybercriminal can use the stolen data to commit online fraud, such as issuing credit cards or loans in the victim's name. One can end up paying for services and products they never use. One's personal information is spread across the internet. The digital footprint we leave can have personal information as well. This is the reason why awareness and education are required on personal information safety.

To detect identity theft, regularly review your credit cards, debit cards, and other financial accounts. Make sure to set up alerts with your bank to receive notifications of any transactions. Examine situations where your card declines. Check for missed payments on credit cards, medical bills, or loans that you know are not yours in letters or phone calls from debt collectors.

If you think you are a victim of identity fraud, contact the organization involved in the fraud. For example, if you see an unsolicited transaction with your credit or debit card. Call the bank or the organization that issued the card and notify them about the transaction. You can file a report with law enforcement for identity theft. Check with your insurance company if they have identity theft protection.
Below are some steps you can take to safeguard yourself from identity theft:
Limit the amount of personal information you give with internet services and websites.
Use a strong and unique password for all of your online accounts, and activate two-factor authentication as an added layer of security. Consider an insurance policy that provides identity theft protection.

Source: SANS

ISRAEL'S DIGITAL SHEKEL CRYPTOCURRENCY

Technological changes in the financial system with the rise of bitcoin and other digital currency upended traditional practices. Every day consumers around the world conduct digital transactions where no real money is used. The use of digital currency can increase the speed of cross-border transactions. The Bank of Israel adopted this technological change and used the blockchain technology of Ethereum. The project is at the pilot stage. The use of digital shekel is within a closed network of the bank and not connected to the general Ethereum currency network.

BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY · BITCOIN · DECENTRALIZED DIGITAL CURRENCY ·

A central bank digital currency (CBDC) needs a distributed ledger technologies such as blockchain. The Bank of Israel Deputy Governor Andrew Abir said, “The option for a CBDC is still being examined, and when we made our statement last month, it was not to say what we are doing, but rather to share what we do not know and receive feedback from the public.

INDIA FUTURE FOUNDATION

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com