PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Threat and vulnerabilities

ATMs in Thailand hacked; 12 million baht stolen; 10,000 ATMs prone to hackers

Ransomware

Wildfire ransomware code cracked: Victims can now unlock encrypted files for free

Opera hack

Opera browser sync service hacked; users' data and saved passwords compromised

Top stories

India seeks report from DCNS on Scorpene submarine data leak

Russian hackers targeted Arizona election system

pwc

ATMs in Thailand hacked; 12 million baht stolen; 10,000 ATMs prone to hackers

An Eastern European gang of criminals has stolen over 12 Million Baht (approximately US$350,000) from a total of 21 ATMs in Bangkok and other five provinces by hacking a Thai bank's ATM network; police said Wednesday

The Central Bank of Thailand (BoT) has issued a warning to all commercial banks about security flaws in roughly 10,000 ATMs that were exploited to steal cash from the machines.

The warning came shortly after the state-owned Government Savings Bank (GSB) shut down approximately 3,000 of their ATMs following an ongoing police investigation into the recent hack in which hackers were able to infect many its cash machines with malware.

GSB found that millions of Thailand Baht were stolen between August 1 and 8 from 21 ATMs across the provinces of Bangkok, Phuket, Chumphon, Prachuap Khiri Khan, Phetchaburi, and Surat Thani, the Bangkok Post reports.

The hackers made over 12.29 Million Thailand Baht (US$346,000) by inserting cards installed with malware into multiple ATMs to spew out cash, up to 40,000 Baht each transaction.

GSB President Chartchai Payuhanaveechai told the local media that the bank has reviewed security camera footage and identified potential suspects as foreign nationals who infected their cash machines with malware that forced them to dispense cash.

Payuhanaweechai also ensured its customers that they are not affected by the theft as the gang's malware only tricked the bank ATMs to release cash without authorization, not from customers' accounts.

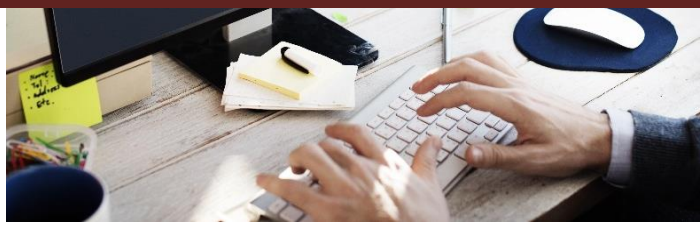
Thai police suspect a ring of at least 25 Eastern European nationals committed the crime and link them to a similar hacking theft occurred last month when the top eight banks in Taiwan were forced to shut down hundreds of its ATMS after thieves used malware to steal NT$70 Million ($2.17 Million) in cash.

Source:
http://thehackernews.com/2016/08/thailand-atm-hack.html

Our perspective

We recommend a security review of ATMs to understand if the existing machines are vulnerable to the Ripper ATM malware. Identified open vulnerabilities need to be remediated via patching or appropriate technology controls (e.g. direct ATM physical access for software updates). Regular monitoring of ATMs for unusual physical device access as well as transactions needs to be enhanced.

Wildfire ransomware code cracked: Victims can now unlock encrypted files for free



Victims of a ransomware campaign aimed at Dutch speakers don't have to pay hackers after the No More Ransom project cracked its cipher.

Victims of the Wildfire ransomware can get their encrypted files back without paying hackers for the privilege, after the No More Ransom initiative released a free decryption tool.

No More Ransom runs a web portal that provides keys for unlocking files encrypted by various strains of ransomware, including Shade, Coinvault, Rannoh, Rakhn and, most recently, Wildfire.

Aimed at helping ransomware victims retrieve their data, No More Ransom is a collaborative project between Europol, the Dutch National Police, Intel Security, and Kaspersky Lab.

Wildfire victims are served with a ransom note demanding payment of 1.5 Bitcoins -- the cryptocurrency favored by cybercriminals -- in exchange for unlocking the encrypted files. However, cybersecurity researchers from McAfee Labs, part of Intel Security, point out that the hackers behind Wildfire are open to negotiation, often accepting 0.5 Bitcoins as a payment.

Most victims of the ransomware are located in the Netherlands and Belgium, with the malicious software spread through phishing emails aimed at Dutch speakers. The email claims to be from a transport company and suggests that the target has missed a parcel delivery -- encouraging them to fill in a form to rearrange delivery for another date. It's this form which drops Wildfire ransomware onto the victim's system and locks it down.

Researchers note that those behind Wildfire have "clearly put a lot of effort into making their spam mails look credible and very specific" - even adding the addresses of real businesses in The Netherlands - arousing suspicion that there are Dutch speaking actors involved in the ransomware campaign.

Working in partnership with law enforcement agencies, cybersecurity researchers were able to examine Wildfire's control server panel, which showed that in a one month period the ransomware infected 5,309 systems and generated a revenue of 136 Bitcoins (€70,332).

Researchers suggest that the malicious code -- which contains instructions not to infect Russian-speaking countries -- means Wildfire operates as part of a ransomware-as-service franchise, with software likely to be leased out by developers in Eastern Europe.

Whoever is behind Wildfire, victims no longer need to pay a ransom in order to get their files back, with the decryptor tool now available to download for free from the No More Ransom site. The tool contains 1,600 keys for Wildfire, and No More Ransom says more will be added in the near future.

Source:
http://www.zdnet.com/article/wildfire-ransomware-code-cracked-victims-can-now-unlock-encrypted-files-for-free/

Our perspective

Ransomware is affecting multiple users globally. We recommend that our clients ensure an up-to-date antivirus solution, regular patching of their OS and applications, and monitoring of perimeter security device alerts. In addition, regular backup of important files is strongly advised to ensure that business disruption is minimal in case of a targeted attack.

Opera browser sync service hacked; users' data and saved passwords compromised

Opera has reset passwords of all users for one of its services after hackers were able to gain access to one of its Cloud servers this week.

Opera Software reported a security breach last night, which affects all users of the sync feature of its web browser.

So, if you've been using Opera's Cloud Sync service, which allows users to synchronize their browser data and settings across multiple platforms, you may have hacked your passwords, login names, and other sensitive data.

Opera confirmed its server breach on Friday, saying the "attack was quickly blocked" but that it "believe some data, including some of [their] sync users' passwords and account information, such as login names, may have been compromised."

Since the company has already reset passwords of all of its registered Opera Sync users and emailed them with details, you need not worry about your account.

"Although we only store encrypted (for synchronized passwords) or hashed and salted (for authentication) passwords in this system, we have reset all the Opera sync account passwords as a precaution," Opera Software explained in a blog post.

Additionally, the company has also informed all Opera Sync users about the security breach and recommended them to change passwords for their Opera Sync accounts as soon as possible. You can obtain a new password for Opera sync using the password resetting page.

The complete details about the intrusion and extent of the breach are yet unknown.

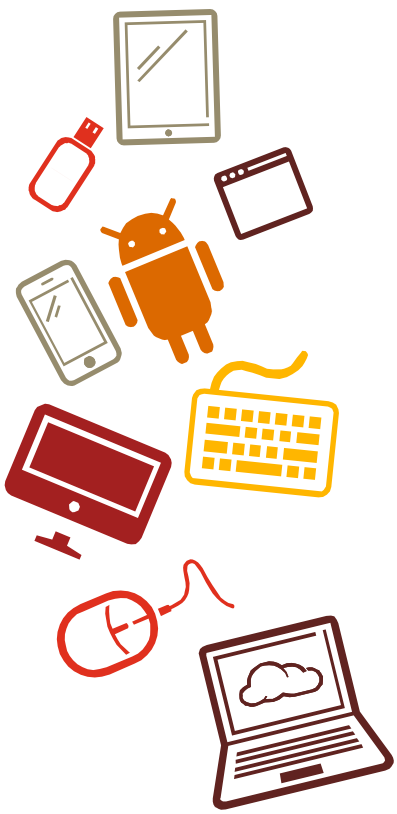
"Opera Software encouraged users to reset passwords for any third party websites they may have synced with its service.

However, if you are the one using the same password for multiple sites, you are also advised to change your passwords for those sites manually.

Since we've repeatedly seen folks reusing passwords across multiple services with recent high-profile account hacking, you are advised to use a good password manager always to keep a strong, unique password for your online accounts.

Source:

http://thehackernews.com/2016/08/opera-browser-hacked.html



India seeks report from DCNS on Scorpene submarine data leak

India will ask French defence contractor DCNS for a report on the leak of documents of Indian Navy's Scorpene submarine project, a government official said on Wednesday, hours after a newspaper report said India's critical next-generation submarine programme had been hit by a massive data leak.

The Indian Navy was assessing the damage done to its submarine project after a report in The Australian said some 22,400 pages of data related to the six Scorpene submarines that the French government-owned DCNS was building for the Indian Navy have been leaked.

"The stunning leak... details the entire secret combat capability of the six Scorpene submarines..." The Australian report said, adding that the leaked documents were marked "Restricted Scorpene India" and gave the combat capabilities of India's new submarine fleet.

The Scorpene was a "conventional boat", i.e., not carrying nuclear weapons, but the leak was still a serious issue if it is related to the India-specific Scorpene, analysts said. Pakistan and China are seen as India's main rivals in the region with the former having acquired French-made Agosta submarines in 1999.

In New Delhi, the Indian Navy in a statement said it was "examining" available information at the ministry of defence and "an analysis is being carried out by the concerned specialists".

"It appears that the source of leak is from overseas and not in India," the statement said.

The leaked documents contain a trove of information including the frequencies at which submarines gather intelligence and the levels of noise the subs make at various speeds, the report said.

It also contains information on the submarine's diving depths, range and endurance, besides its magnetic, electromagnetic and infrared data.

Defence minister Manohar Parrikar has ordered a probe into the newspaper report, saying the documents could have been obtained through hacking.

"I have asked the navy chief to investigate the matter and find what has been leaked and how much of it is about us," Parrikar told reporters.

India is currently building six Scorpene submarines in partnership with DCNS under a $3.5 billion deal signed in 2005. The first of the six submarines, INS Kalvari, is likely to be inducted into the Indian Navy by the end of 2016 to augment its dwindling fleet. The remaining are likely to be delivered by 2020.

All six submarines are being built at the Mazagon Docks Ltd in Mumbai.

India has a fleet of 13 ageing submarines, only half of which are operational at any time, opening up a major gap with China which is expanding its maritime presence in the Indian Ocean.

Variants of the DCNS submarines built in India are being used by Malaysia and Chile. Brazil is also due to deploy the vessels from 2018. And Australia too awarded DCNS a $38 billion contract to design and build its next generation of submarines.

DCNS told the French news agency AFP that it was aware of the articles published in the Australian press and "national security authorities" had launched an inquiry into the matter.

"This inquiry will determine the precise nature of the documents which have been leaked, the potential damage to our customers as well as those responsible," DCNS said.

"It is not clear whether the leak refers to the Indian submarine (with Indian specifications) or of the Scorpene in general. If it does, then it's a compromise of the credibility of the platform," said retired commodore C.U. Bhaskar, currently director with the New Delhi based Society for Policy Studies think tank.

India seeks report from DCNS on Scorpene submarine data leak

"But till that is established, we need to be cautious," he said, adding India would have to look at including a clause on data protection in all future defence pacts of this kind included under the Make in India programme of the government.

Make in India was launched in 2014 by the Narendra Modi government to establish India's image as a manufacturing hub and boost the making of defence hardware in India. India is one of the world's largest importers of arms.

According to The Australian news report, the data is thought to have been removed from France in 2011 by a former French naval officer who at the time was a subcontractor for DCNS.

The data is believed to have passed through firms in South-East Asia before eventually being mailed to a company in Australia, the newspaper said.

Retired brigadier Rumel Dahiya, deputy director general of New Delhi-based Institute of Defence Studies and Analyses, a think-tank, said the damage to India's submarine programme depended on who had access to the leaked documents.

It could be our adversaries or commercial competitors," he said, adding that if it was the former, the situation would be serious.

In cases of defence and national security, when something like this happens, "one works on the assumption that the worst has happened", Dahiya added.

Former Indian naval chief admiral Arun Prakash was of the view that "India does not have an option but to take the six submarines" contracted under this agreement though India could impose penalties on DCNS for the leak.

Former Indian naval chief admiral Arun Prakash was of the view that "India does not have an option but to take the six submarines" contracted under this agreement though India could impose penalties on DCNS for the leak.

Source:

http://www.livemint.com/Politics/ivESz72UtXJD1chwHjQPVN/Manohar-Parrikar-says-Scorpene-document-leak-a-case-of-hack.html

Russian hackers targeted Arizona election system

Hackers targeted voter registration systems in Illinois and Arizona, and the FBI alerted Arizona officials in June that Russians were behind the assault on the election system in that state.

The bureau described the threat as "credible" and significant, "an eight on a scale of one to 10," Matt Roberts, a spokesman for Arizona Secretary of State Michele Reagan (R), said Monday. As a result, Reagan shut down the state's voter registration system for nearly a week.

It turned out that the hackers had not compromised the state system or even any county system. They had, however, stolen the username and password of a single election official in Gila County.

Roberts said FBI investigators did not specify whether the hackers were criminals or employed by the Russian government. Bureau officials on Monday declined to comment, except to say that they routinely advise private industry of cyberthreats detected in investigations.

The Arizona incident is the latest indication of Russian interest in U.S. elections and party operations, and it follows the discovery of a high-profile penetration into Democratic National Committee computers. That hack produced embarrassing emails that led to the resignation of DNC Chairwoman Debbie Wasserman Schultz and sowed dissension on the eve of Hillary Clinton's nomination as the party's presidential candidate.

The Russian campaign is also sparking intense anxiety about the security of this year's elections. Earlier this month, the FBI warned state officials to be on the lookout for intrusions into their election systems. The "flash" alert, which was first reported by Yahoo News, said investigators had detected attempts to penetrate election systems in several states and listed Internet protocol addresses and other technical fingerprints associated with the hacks.

In addition to Arizona, Illinois officials discovered an intrusion into their election system in July. Although the hackers did not alter any data, the intrusion marks the first successful compromise of a state voter registration database, federal officials said.

"This was a highly sophisticated attack most likely from a foreign (international) entity," said Kyle Thomas, director of voting and registration systems for the Illinois State Board of Elections, in a message that was sent to all election authorities in the state.

The Illinois hackers were able to retrieve voter records, but the number accessed was "a fairly small percentage of the total," said Ken Menzel, general counsel for the Illinois election board.

State officials alerted the FBI, he said, and the Department of Homeland Security also was involved. The intrusion in Illinois led to a week-long shutdown of the voter registration system.

The FBI has told Illinois officials that it is looking at foreign government agencies and criminal hackers as potential culprits, Menzel said.

At least two other states are looking into possible breaches, officials said. Meanwhile, states across the nation are scrambling to ensure that their systems are secure.

Until now, countries such as Russia and China have shown little interest in voting systems in the United States. But experts said that if a foreign government gained the ability to tamper with voter data — for instance by deleting registration records — such a hack could cast doubt on the legitimacy of U.S. elections.

"I'm less concerned about the attackers getting access to and downloading the information. I'm more concerned about the information being altered, modified or deleted.

Russian hackers targeted Arizona election system

That's where the real potential is for any sort of meddling in the election," said Brian Kalkin, vice president of operations for the Center for Internet Security, which operates the MS-ISAC, a multistate information-sharing center that helps government agencies combat cyberthreats and works closely with federal law enforcement.

James R. Clapper Jr., the director of national intelligence, has told Congress that manipulation or deletion of data is the next big cyberthreat — "the next push on the envelope."

Tom Hicks, chairman of the federal Election Assistance Commission, an agency set up by Congress after the 2000 Florida recount to maintain election integrity, said he is confident that states have sufficient safeguards in place to ward off attempts to manipulate data.

For example, if a voter's name were deleted and did not show up on the precinct list, the individual could still cast a provisional ballot, Hicks said. Once the voter's status was confirmed, the ballot would be counted.

Hicks also said the actual systems used to cast votes "are not hooked up to the Internet" and so "there's not going to be any manipulation of data." However, more than 30 states have some provisions for online voting, primarily for voters living overseas or serving in the military.

This spring, a DHS official cautioned that online voting is not yet secure.

"We believe that online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results," said Neil Jenkins, an official in the department's Office of Cybersecurity and Communications.

Private-sector researchers are also concerned about potential meddling by Russians in the U.S. election system. Rich Barger, chief information officer at ThreatConnect, said that several of the IP addresses listed in the FBI alert trace back to a website-hosting service called King Servers that offers Russia-based technical support. Barger also said that one of the methods used was similar to a tactic employed in other intrusions suspected of being carried out by the Russian government, including one this month on the World Anti-Doping Agency.

"The very fact that [someone] has rattled the doorknobs, the very fact that the state election commissions are in the crosshairs, gives grounds to the average American voter to wonder: Can they really trust the results?" Barger said.

Earlier this month, DHS Secretary Jeh Johnson held a conference call with state elections officials, offering his assistance in protecting against cyberattacks.

Johnson said that DHS was "not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems," according to a readout of the call.

It was not clear whether he was aware at the time of the FBI's investigations in Arizona and Illinois.

Source:

https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

©2016 PwC. All rights reserved

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

All images in this presentation are protected by copyright, trademark, patent, trade secret and other intellectual property laws and treaties. Any unauthorised use of these images may violate such laws and shall be punishable under appropriate laws. Our sharing of this presentation along with such protected images with you does not authorise you to copy, republish, frame, link to, download, transmit, modify, adapt, create derivative works based on, rent, lease, loan, sell, assign, distribute, display, perform, license, sub-license or reverse engineer the images. In addition, you should desist from employing any data mining, robots or similar data and/or image gathering and extraction methods in connection with the presentation.

© 2016 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

VS/August2016-7281