SENTARIS MONTHLY BRIEFING

JUNE 2020

INSIDE THIS ISSUE

FOREWORD BY OUR MANAGING DIRECTOR

JUSTIN WAITE

This month has seen a rise in reports of cyber attacks against some very large brands, including an announcement by the Australian government about sustained attacks. Unfortunately with the increased reports and media attention, comes with it vendors offering to sell silver-bullet products to solve all your security problems. I am not suggesting that some of these controls are not an important addition to your security arsonel, but there is a lot of merit in ensuring you have the basics right first. This is often the greatest return on investment when it comes to preparing your organisation for cyber threats. See https://www.business.gov.au/Risk-management/Cyber-security/How-to-protect-your-business-from-cyber-threats as a starting point.

Sentaris

DRINKS GIANT LION HIT BY CYBER ATTACK AS HACKERS TARGET CORPORATE AUSTRALIA

Original article by Paul Harris and can be found at *https://www.theage.com.au/technology/drinks-giant-lion-hit-by-cyber-attack-as-hackers-target-corporate-australia-20200609-p550pu.html*

The Australian beverages giant behind milk brands Dairy Farmers and Pura and XXXX Gold beer has been hit by a major cyber attack that has disrupted manufacturing and knocked out its internal IT systems.

Staff at Lion, which was previously known as Lion Nathan, lost remote access on Tuesday morning as a result of the attack, which has also impacted the processing of customer orders.

“We are working with expert advisors to address the issue. We have alerted the authorities and are working hard to minimise disruption to customers and suppliers,”

The Foreign Investment Review Board is assessing the bid after the Australian Competition and Consumer Commission gave the offer the green light in February. Federal Treasurer Josh Frydenberg will have the final say over whether the sale goes ahead.

Contacted by*The Sydney Morning Herald* and *The Age* on Tuesday, Lion confirmed it had been hit by a cyber attack that had forced it to shut down its IT systems. "Lion has experienced a cyber incident and has taken the precaution of shutting down our IT systems, causing some disruption to our suppliers and customers," the company said via a public relations firm.

"We are working with expert advisors to address the issue. We have alerted the authorities and are working hard to minimise disruption to customers and suppliers. We will provide further updates when we can, and we thank our customers and suppliers for their patience."

The company said its beer business had ceased manufacturing as a result of the attack, but said it had enough stocks already brewed in the wake of the COVID-19 pandemic to keep supplying pubs and restaurants as they re-open. Its dairy and juice business has also been impacted, and is now producing perishables at a limited capacity.

Continue reading at *https://www.theage.com.au/technology/drinks-giant-lion-hit-by-cyber-attack-as-hackers-target-corporate-australia-20200609-p550pu.html*

Sentaris

FISHER & PAYKEL APPLIANCES STRUCK BY NEFILIM RANSOMWARE

Original article by Juha Saarinen and can be found at https://www.itnews.com.au/news/fisher-paykel-appliances-struck-by-nefilim-ransomware-549102

Fisher & Paykel Appliances is the latest big brand name to be struck down by ransomware, shutting down its operations while it recovered following the attack.

The whitegoods manufacturer's spokesperson Andrew Luxmoore confirmed the attack to iTnews, saying it took place early last week.

"The attempt was identified quickly and, as a result, we locked down our IT ecosystem immediately," he said.

"We are currently working with third party experts to restore our systems and our ability to take and fulfil orders, as well as introducing additional security measures."

Luxmoore said the attack impacted manufacturing and distribution at F&P Appliances, with its facilities shut down while dealing with the ransomware attack.

The ransomware used in the Fisher & Paykel attack was Nefilim.

Nefilim was also used in devastating attack on Toll Group earlier this year, in which over 200 gigabytes of data was exfiltrated.

Following the example of other ransomware criminal gangs such as Maze, Sodinokibi, and DoppelPaymer, the extortionists behind Nefilim threaten to release victims' data in order to force them to pay a ransom.

The attack on Fisher & Paykel Appliances comes as attacks against large corporates in the region mount up, including also one on beverages giant Lion and Japanese car manufacturer Honda, both of which impacted production lines.

Luxmoore said Fisher & Paykel Appliances is working with other businesses to understand how it can better protect itself from this type of criminal activity.

Continue reading at https://www.theage.com.au/technology/drinks-giant-lion-hit-by-cyber-attack-as-hackers-target-corporate-australia-20200609-p550pu.html

"We are currently working with third party experts to restore our systems and our ability to take and fulfil orders, as well as introducing additional security measures."

Sentaris

SODINOKIBI RANSOMWARE NOW SCANS NETWORKS FOR POS SYSTEMS

Original article by Lindsey O'Donnell and can be found at https://threatpost.com/sodinokibi-ransomware-now-scans-networks-for-pos-systems/156855/

Attackers are compromising large companies with the Cobalt Strike malware, and then deploying the Sodinokibi ransomware.

Cybercriminals behind recent Sodinokibi ransomware attacks are now upping their ante and scanning their victims' networks for credit card or point of sale (PoS) software. Researchers believe this is a new tactic designed to allow attackers to get the biggest bang for their buck – ransom payments and credit card data.

The compromise of PoS software – which is commonly installed on credit card terminals at retailer stores or restaurants – is a cybercriminal favorite for siphoning credit card information from unknowing customers. In this campaign, researchers found the Sodinokibi ransomware sniffing out PoS systems on the compromised networks of three "large" unnamed companies in the services, food, and healthcare sectors.

However, it's not yet clear whether the attackers are targeting this PoS software to encrypt it as part of the ransomware attack, or because they want to scrape the credit card information on the systems as a way to make even more money in addition to the ransomware attack.

"While many of the elements of this attack are 'typical' tactics seen in previous attacks using Sodinokibi, the scanning of victim systems for PoS software is interesting, as this is not typically something you see happening alongside targeted ransomware attacks," said Symantec researchers in a Tuesday analysis. "It will be interesting to see if this was just opportunistic activity in this campaign, or if it is set to be a new tactic adopted by targeted ransomware gangs."

Steve Doherty, Symantec threat intelligence analyst, told Threatpost that the PoS scanning payload was observed being downloaded from Pastebin. It scans for processes related to PoS software, he said.

"It will be interesting to see if this was just opportunistic activity in this campaign, or if it is set to be a new tactic adopted by targeted ransomware gangs."

Sentaris

HONDA PAUSES PRODUCTION DUE TO CYBERATTACK

Original article by Shiho Takezawa, Tsuyoshi Inajima, and Siddharth Vikram Philip, and can be found at https://www.bloomberg.com/news/articles/2020-06-09/honda-suspends-vehicle-shipments-after-suspected-cyberattack

Honda Motor Co. said a cyberattack has disrupted its internal network and brought some factories around the world to a standstill.

Production has been halted at car factories in Ohio and Turkey, as well as at motorcycle plants in India and South America, and the company is working to fix systems, spokesman Hidenori Takeyasu said. Japanese operations weren't affected and Honda's other plants in the U.S. have resumed manufacturing.

Honda said there's no indication of an information breach and the impact on business will be minimal.

The disruption comes as manufacturers have shut some offices and plants and let staff work from home due to the coronavirus pandemic. Carmakers have slowly started to ramp up production around the world after countries gradually began lifting lockdown measures put in place to halt the spread of the pandemic. Honda resumed operations in the U.S. May 11, and had planned to reopen its U.K. plant this week.

Production at the factory in Swindon, England, will restart Wednesday, two days later than planned, a person familiar with the situation said.

Honda said there's no indication of an information breach and the impact on business will be minimal. A spokesman for the company's North American business said it isn't aware of any loss of personal information and that output had resumed at most plants in the U.S. The automaker is "currently working toward the return to production of our auto and engine plants in Ohio," spokesman Chris Abbruzzese said in an email.

Honda's two car assembly plants in Ohio have a combined annual capacity of 680,000 vehicles, more than half of its total automotive production in the U.S. Those factories make models such as the Accord sedan and CR-V crossover.

Keep reading at https://www.bloomberg.com/news/articles/2020-06-09/honda-suspends-vehicle-shipments-after-suspected-cyberattack

Sentaris

CYBER-ATTACK AUSTRALIA: SOPHISTICATED ATTACKS FROM 'STATE-BASED ACTOR'

Original article by Daniel Hurst, and can be found at https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

A wide range of political and private-sector organisations in Australia have come under cyber-attack carried out by a "sophisticated state-based cyber-actor", the Australian government has revealed.

Scott Morrison, the prime minister, disclosed the far-reaching attacks at a media conference in Canberra on Friday, while the defence minister, Linda Reynolds, declared that malicious cyber-activity was "increasing in frequency, scale, in sophistication and in its impact".

The government did not say which country it believed was responsible, except to say it was "a state-based actor, with very significant capabilities".

The prime minister declined to respond to a specific question about whether it was China, after months of tensions in its relationship with Australia, but security experts later said they believed it, Russia and North Korea were the only countries that fell within Morrison's description.

"I'm here today to advise you that, based on advice provided to me by our cyber-experts, Australian organisations are currently being targeted by a sophisticated state-based cyber-actor," Morrison told reporters.

"This activity is targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure.

"We know it is a sophisticated state-based cyber-actor because of the scale and nature of the targeting and the tradecraft used. The Australian government is aware of and alert to the threat of cyber-attacks."

Keep reading at https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

"We know it is a sophisticated state-based cyber-actor because of the scale and nature of the targeting and the tradecraft used.

Sentaris

CORONAVIRUS WORRIES ALLOW NEW SCAMS TO TAKE HOLD

Original article by Wayne Rush, and can be found at https://www.forbes.com/sites/waynerash/2020/04/21/coronavirus-worries-allow-new-scams-to-take-hold

Cyber criminals are taking advantage of the worldwide level of concern surrounding the COVID-19 coronavirus to launch an insidious new round of attacks that are much more effective than previous cyber-attacks. “We’re seeing a massive increase in COVID-19 related phishing scams,” said Stu Sjouwerman, CEO of KnowBe4. “Everyone and their brother who were sending out normal spam and phishing went into social engineering and is sending out coronavirus scams now.”

The rise in scams related to COVID-19 is getting bad enough that the FBI started sending out alerts in March, and has since issued detailed alerts regarding scams related to health care fraud, cryptocurrency and medical supplies. With shortages in personal protective equipment (PPE), the scams are now targeting business executives who are trying to procure PPE from non-traditional sources.

Microsoft, meanwhile, is warning against coronavirus themed phishing attacks aimed at medical facilities and nursing homes. Because of this the company has implemented additional security features to its email services specifically to detect and block such attacks.

But there’s an important difference between the scams of yore and those now – according to some sources the click rate on those phishing emails has risen from less than 5 percent to over 40 percent with coronavirus scams.

Keep reading at https://www.forbes.com/sites/waynerash/2020/04/21/coronavirus-worries-allow-new-scams-to-take-hold

Sentaris is helping organisations increase awareness with a free phishing simulation.

Browse to www.sentaris.com.au/free-phishing-simulation for more information.

Sentaris

SHADOW IT: IT'S A BIGGER THREAT THAN YOU THINK

FILE SHARING, REMOTE WORK, AND VULNERABLE EMPLOYEES ARE LEAVING COMPANY NETWORKS OPEN TO POTENTIAL CYBERATTACK

Original article by Karen Roby and can be found at https://www.techrepublic.com/article/shadow-it-its-a-bigger-threat-than-you-think

TechRepublic's Karen Roby talked with Rahul Kashyap, CEO of Awake Security, about the alarming increase in shadow IT during the COVID-19 pandemic. The following is an edited transcript of their conversation.

Rahul Kashyap: Shadow IT has been a lingering problem for IT administrators for a long time. It's basically unauthorized use of tools. In most cases, it is legit use. The way I like to describe the shadow IT problem is actually simply this way: If you come in the way of an end user doing the job, they will find a way to get the job done, and they will find tools, means, or whatever. And shadow IT is a manifestation of that in many cases.

Particularly in the coronavirus time where people are locked down, and they're not well prepared for that scenario, we are seeing a huge surge in shadow IT tools of late. We are seeing an increase in file sharing applications leaking data. We are seeing an increase in the usage of remote access tools, like TeamViewer, RDP protocols, and so on. So this is an increasing trend which has definitely grown ever since we initiated the lockdown and people are working from home.

Karen Roby: File sharing is becoming a big issue Rahul, expand on that.

Rahul Kashyap: So we found that generally, it's one or two file sharing applications which IT people authorize end users to use in a large corporate environment. But we are seeing an average of five and above per user where people have a lot of file sharing applications. And many of these file sharing applications by default, try to upload a lot of files as backup. You can maybe have a file sharing application just to store and save your photographs that you just took recently over the weekend. But you may have sensitive documents from your office which are also in the same laptop and they're also getting and moving to your personal file sharing service right now.

We are seeing a lot of that loss coming in. And a lot of IT initiatives are really wanted because this is creating new data, a new case problem from corporate, particularly as people are sharing sensitive documents unknowingly into their personal accounts. But this is a very common problem we come across recently and it has really grown significantly in the last few months as well.

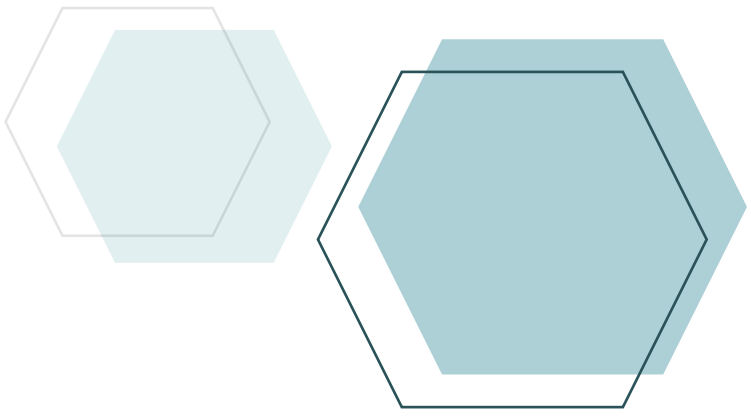
Karen Roby: Sadly, criminals really prey on people when they are most vulnerable, as we all are right now.

Rahul Kashyap: To give you an example, we have seen almost a 75% increase from January to March in people using remote access tools like LogMeIn, GoToMyPC, TeamViewer, RDP products and home-based services and so on. I completely understand. People are struggling. People are kind of just getting the job done, but attackers are using default and weak settings in some of these services to launch attacks. There have been cases where people are scanning for RDP protocol ports on the internet and then they even launch a ransomware attack if they find after boot porting, they can compromise an account. So yes, attackers are definitely taking advantage of the situation. There is confusion, there is a bit of chaos, and there's a bit of lack of control, if I may, in the entire IT environment right now and attackers, they will take advantage, and they are.

Karen Roby: What are a couple quick tips you would pass along to those looking to keep their network safe?

Rahul Kashyap: I would say it's very difficult to please people and give them tools which everybody likes, right? You may not have a success there where you give a tool and which everybody's going to like. Try to at least have tools which are user friendly. This can be easily used by people as much as you can. That's an easy one. From a security perspective, visibility and controls are more and more important, more so than ever. So if you see that there are people unknowingly using tools that are likely which can cause harm to the organization, deploy products on your network which can give you visibility and identify those kinds of activity so that you can resolve this proactively before any damage gets done. Understanding those and understanding your network has never been so important.
I think you should definitely start with visibility so that you can have efficient controls once you understand and know what's going on in the environment. I think that's the best and first thing to do. And depending upon how sensitive you are in terms of data leakage, you can add a lot more controls once you understand what's really going on in your environment. Definitely, I would highly recommend network monitoring solutions to be put behind the VPN, if required, so that you can identify fingerprint device users, who's coming to your network, and how do you manage that?

Secondly, it's very important to have cloud controls as well because not all of these services are going to the cloud. Make sure that you have a good cloud hygiene policy so that you really understand what's going out of your corporate network. The corporate network is no longer a corporate network. Now it's everybody's home. People are working so suddenly the whole thing is fragmented and blown up. It's definitely going to be challenging times for a lot of people.



www.sentaris.com.au