ELSEVIER

network SECURITY

ISSN 1353-4858 January 2021

www.networksecuritynewsletter.com

Featured in this issue:

How can mobile networks protect critical infrastructure?

Critical infrastructure is being targeted by hostile states, terrorists and criminals for the purposes of disruption, espionage and financial gain.

Increasingly, these national infrastructure sites rely on technology to monitor, measure and manage activities. And one piece of technology that could play a significant role is the IMSI-catcher. By being able to detect mobile devices used by persons of interest, critical infrastructure organisations can throw up a defensive shield fine-tuned to provide geographical coverage of a specific location, explains Andy Gent of Revector.

Full story on page 6…

Relying on firewalls? Here's why you'll be hacked

Firewalls remain the first line of defence for many organisations. But confidence in their ability to stop attacks is waning.

To better protect our enterprises, we must accept that firewalls have become almost redundant and look for more-effective approaches. And one proven choice is software-based segmentation, which is more adaptable to business considerations and today's workloads, says Dave Klein of Guardicore.

Full story on page 9…

The event data management problem: getting the most from network detection and response

Detecting cyberthreats has become a big data management challenge. Threat actors employ advanced strategies to hide in hard-to-find places on your network.

In order to detect these threats, you must consolidate data from your entire IT environment and analyse it. Many organisations already collect data from multiple sources but still have blind spots in their environment where they don't have visibility. It's time to fill those gaps, argues Sudhir Udipi of Securonix.

Full story on page 12…

SolarWinds supply chain breach threatens government agencies and enterprises worldwide

A breach of SolarWinds' Orion system and network monitoring platform has led to backdoors being implanted in the networks of thousands of the company's customers. Orion is used heavily by governments and most of the Fortune 500 companies.

SolarWinds has enormous market penetration, being used by 300,000 organisations of which about 33,000 use the Orion platform. The company believes that up to 18,000 of its customers may have installed malicious updates.

Continued on page 2...

Contents

Editorial Office: Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Sarah Jenkins
Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Columnists: Andrew Cooke, Airbus Security; Karen Renaud; Dave Spence, Context Information Security; Colin Tankard, Digital Pathways

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

...Continued from front page

The attackers had somehow gained access to the software build system used by SolarWinds. They were able to insert functions into the source code of a particular dynamic library (.dll) file used by the Orion system – SolarWinds.Orion.Core.BusinessLayer.dll. The .dll was subsequently built, signed and distributed by SolarWinds as part of its normal updating processes – a form of what is known as a supply chain attack.

The SolarWinds breach was revealed on 13 December 2020, with coordinated statements from the US Government, Microsoft and security firm FireEye. However, five days earlier, FireEye announced that it had been hacked by a nation-state APT group and that some of its software tools had been stolen. This turned out to be the first publicly acknowledged incident related to the SolarWinds issue. The installation of trojanised updates may have begun in March 2020, with further changes to the source code being made up until June.

The rogue code – dubbed SunBurst by FireEye and Solarigate by Microsoft – opens a backdoor in the affected systems. While the subsequent behaviour of the attackers is not known in more than a few instances, the backdoor could be used to gather data, perform lateral movement within networks, install additional malware and elevate privileges. Microsoft said it believed the ultimate aim was to gain access to victims' cloud accounts. Microsoft has a technical analysis of the backdoor here: http://bit.ly/3bvs8Ya.

A statement from the FBI, NSA, the Office of the Director of National Intelligence (ODNI) and the Cyber security and Infrastructure Security Agency (CISA) said that "fewer than 10" US Government agencies had been impacted, but it's known that these included the Department of Justice (DoJ), Department of the Treasury, the National Telecommunications and Information Administration (NTIA), the Department of State, the National Institutes of Health (NIH, part of the Department of Health), the Department of Homeland Security (DHS), the Department of Energy (DOE), the National Nuclear Security Administration (NNSA, which deals with nuclear weapons) and the governments of some, undisclosed states. The statement also said that the US Government believes the campaign was focused on data and intelligence gathering. The statement is here: http://bit.ly/3oCm7fW.

The DoJ said that around 3% of the department's Office 365 email inboxes – that's around 3,450 accounts – were accessed by the malware. The malicious activity was detected on 24 December 2020. The department was able to block further access. US Treasury email accounts were also compromised.

It's also possible that the threat actors were able to gain access to an unknown number of sealed court documents held on the systems of the Administrative Office (AO) of the US Courts. This could put ongoing cases in jeopardy.

"The AO is working with the Department of Homeland Security on a security audit relating to vulnerabilities in the Judiciary's Case Management/Electronic Case Files system (CM/ECF) that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings," the agency said in a statement, available here: http://bit.ly/3qa8Uvq. It's believed by some sources that the Sunburst attack downloaded a second piece of malware, dubbed Teardrop, onto the AO's systems.

SolarWinds is also widely used in the UK public sector and military services, including the Royal Navy, Royal Air Force, the signals intelligence agency GCHQ, the Cabinet Office and the Ministry of Justice.

In addition to FireEye, tech companies affected by the campaign included Microsoft, VMware and Cisco. Microsoft said that around 40 of its customers were also impacted, 80% of them in the US and 44% of them in the IT sector. The attack against its own systems led to some source code being viewed.

"We detected unusual activity with a small number of internal accounts and upon review, we discovered one account had been used to view source code in a number of source code repositories," said the firm. "The account did not have permissions to modify any code or engineering systems and our investigation further confirmed no changes were

Threatwatch

Microsoft flaw not fixed

A zero-day flaw in Windows, first exploited in May 2020 and patched by Microsoft in June, is still exploitable using a slightly different approach. The original vulnerability (CVE-2020-0986) was first detailed by Kaspersky after it had been used by threat actors for privilege escalation. However, Maddie Stone, a researcher at Google Project Zero, pointed out that, "The original issue was an arbitrary pointer dereference which allowed the attacker to control the src and dest pointers to a memcpy." Microsoft's patch changed the pointers to offsets, but these can still be used to control the parameters, and Stone provided a proof of concept. The new issue is now tracked as CVE-2020-17008 and there's more information here: http://bit.ly/35z482E.

FBI Egregor warning

The FBI has issued a Private Industry Notification (PIN) warning businesses of a major ransomware campaign that is currently targeting enterprises. The Egregor operation has compromised at least 150 organisations since it started operating in September 2020. And the group behind the campaign appears to be large, well-resourced and ramping up operations. Because of the large number of actors involved in deploying Egregor, the tactics, techniques, and procedures (TTPs) used in its deployment can vary widely, creating significant challenges for defence and mitigation," the FBI says in its advisory, which is available here: http://bit.ly/3nAuJTe.

New e-commerce skimmer

A new payment card data skimmer has been discovered that targets e-commerce sites running on Shopify, BigCommerce, Zencart and Woocommerce. It injects a malicious checkout page with a keylogger in order to capture payment card details entered by customers. According to researchers at Dutch cyber security company Sansec, who found the skimmer, when customers click the 'Proceed' button, the skimmer displays an error and then redirects them to the legitimate checkout page. This means transactions ultimately proceed as normal, which helps avoid suspicion that there's something wrong. There's more information here: http://bit.ly/2XvsbuS.

Gitpaste is back

The Gitpaste-12 worm and bot malware, which spreads via GitHub and uses Pastebin to host its malicious payloads, has appeared again, this time with more than 30 new exploits. Researchers at Juniper Threat Labs first spotted it on 10 November 2020 and say that the additional exploits are designed to target Linux systems, IoT devices and open-source code libraries. "The wave of attacks used payloads from yet another GitHub repository, which contained a Linux crypto-miner ('ls'), a list of passwords for brute-force attempts ('pass') and a statically linked Python 3.9 interpreter of unknown provenance," said Asher Langton, a researcher at Juniper. There's more information here: http://juni.pr/3oHfoRW.

Bouncy Castle bug

The Bouncy Castle cryptography library for Java and C#/.NET has a severe authentication bypass vulnerability (CVE-2020-28052). The open source library is extremely popular (the .NET version alone has been downloaded over 16 million times). But according to Synopsys Cyber security Research Centre, a flaw in the OpenBSDBcrypt class, which implements the Bcrypt password hashing algorithm, could make solutions using the library vulnerable to the brute-forcing of credentials. Bouncy Castle versions 1.65 and 1.66 are vulnerable but the problem has been fixed in 1.67 and developers are encouraged to recompile their code with the newer version. There's more information here: http://bit.ly/39j12Re.

made. These accounts were investigated and remediated."

While many official sources, particularly within the US Government, were reluctant to attribute blame at first, those in the security field were confident early on that this was the work of Russian hackers. FireEye is tracking the threat actor as UNC2452 while US security firm Volexity has linked this campaign to a threat actor it calls Dark Halo. Volexity said it has seen Dark Halo attack the same US thinktank three times between late 2019 and July 2020, with the third attack using the SolarWinds exploit.

In an interview in December, US Secretary of State Mike Pompeo said: "We can say pretty clearly that it was the Russians that engaged in this activity". But it wasn't until 6 January 2021 that the FBI, NSA and the CISA issued a joint statement pinning the attack on Russia.

Many people in the security industry believe the threat actors belong to the group known as APT29 or Cozy Bear, widely believed to be part of Russia's SVR foreign intelligence agency, although there's some suggestion the FSB internal security agency may have been involved too.

One indication that this was the work of a nation-state APT group was the patience and care with which the attack was mounted. There is evidence that the first modification of source code was made as far back as October 2019. There was no backdoor in that case – the changes were minor and had no effect. But the attackers were able to analyse whether the changes would be spotted.

Also, once the backdoor was rolled out, it seems that the attackers delayed exploiting many of the compromised organisations, sometimes for months – probably in an effort to keep a low profile. The malware itself remained inactive on new hosts for up to two weeks, again probably as an anti-detection method.

Russia has form with supply chain attacks. In 2017, the NotPetya ransomware campaign infected code within the MEDoc accounting software produced by the Linkos Group company in Ukraine. The infected code was subsequently distributed as part of the normal update process.

Just how the attackers were able to gain access to SolarWinds' development systems is still under investigation. Infections may have been aided by SolarWinds' advice to customers to add its products to the allow list in anti-malware software.

Security researcher Vinoth Kumar claimed to have warned SolarWinds back in November that he had found a plaintext FTP password – 'solarwinds123' – in a public GitHub repository. The password, he said, gave access to the firm's update server. It had been exposed for at least several months by the time he found it.

Anti-malware firms have begun detecting the malicious binaries and Microsoft, FireEye and GoDaddy have collaborated on a kill switch using wildcard DNS resolution to prevent the malware connecting to command and control servers. However, these measures will not work against any other malware that was downloaded by the backdoor following the initial infection.

SolarWinds has an advisory here: www.solarwinds.com/securityadvisory.