IT SECURITY RELATED INCIDENTS

Information Assurance and Security

MAY 8, 2022

MITHILA DILSHAN WICKRAMAARACHCHI – BIT2

20s15006

Table of content

Contents

1.0 First incident

Phishing operation hits NHS email accounts to harvest Microsoft credentials

Vulnerability/Vulnerabilities

- Keep their Emil databases on premises without migrating into cloud.
- Didn’t process a continues monitor and identification method to identity any external attacks.
- Throwing unlimited money at a problem won't fix.
- The NHS also has an enormous issue due to the mixture of internal markets and over-management. For example, clinicians already working ridiculously hard have to waste significant amount of time to record their activities, to prove they aren't, er, wasting time. Something that decent local team management could accomplish with considerably more efficiency.

Threat

This is an intentional threat that is caused by any third-party property for harvesting E-mail addresses. This can be categorized into phishing attack.

Risk

There is a huge risk of harvesting e-mails. Its nhs[.]net domain serves "tens of millions" of email users, and provides infrastructure for 27,000 organizations including hospitals, health clinics, social-work organizations, suppliers and others. As a consequence of it, the email security firm detected 1,157 phishing emails originating from NHSMail accounts that belonged to 139 NHS employees in England and Scotland. According to the company's VP of Security Strategy Roger Kay, there are many undiscovered sections of this attack. Only few of they have been discovered and majority of the phishing emails were fake new document notifications with malicious links to credential harvesting site. All of the emails had the NHS email footer at the bottom. So, their customers can be easily deceived. After hijacking the victims’ e-mails, they have sent scam emails to third-parties in attempts to harvest Microsoft credentials and, in a few cases, trick recipients into sending money via advance-fee scams.

Assets

Hardware, software, email servers of the NHS, customer email address and their data.

Possible Controls

They have migrated their email database into cloud, Microsoft Exchange Online and they have processes in place to continuously monitor and identify upcoming attacks. They address them in collaboration with their partners who support and deliver the national NHSMail service. The NHS organizations running their own email systems will have similar processes and protections in place to identify and coordinate their responses, and call upon NHS Digital assistance, if they required.

2.0 Second incident

Critical vulnerabilities found in 'millions of Aruba and Avaya switches'

Vulnerability/Vulnerabilities

- They have discovered some of the vulnerabilities, collectively called TLStorm 2.0 and said they stem from insecurities in NanoSSL, a TLS library developed by Mocana that's used in the vulnerable network equipment.
- When the vulnerable network equipment uses NanoSSL to present a captive portal, criminals can exploit the TLStorm 2.0 vulnerabilities to gain remote code execution, with no need for authentication. And once they control that switch hardware, they can disable the captive portal as well as explore the network for systems to attack.
- They have a vulnerability called CVE-2022-23677, which received a 9.0 out of 10 CVSS score is due to a weakness in NanoSSL that can be exploited via a captive portal.

Threat

Gain access to networks and surf the internet by bypassing the captive portals by the digital intruders without legal authentication.

Risk

According to head of research Barak Hadad, some of the vulnerabilities can be triggered with no authentication, no user interaction or involvement. This is a very high risk and they have stated those flows could affect about 10 million devices across HPE's Aruba and Extreme Networks' Avaya switching portfolio, and have severity scores ranging from 9.0 to 9.8 out of 10. If exploited, miscreants can abuse these vulnerabilities to change the behavior of a switch, move laterally to other devices, potentially steal corporate data, and so on. Armis publicly disclosed come of the vulnerabilities of family. In addition to the usual nefarious activities, such as exfiltrating sensitive data from connected devices or deploying malware on the network, exploiting TLStorm on APC UPS machines could result in power outages. Once they exploit the TLStorm 2.0 vulnerabilities, they can control that switch hardware, they can disable the captive portal as well as explore the network for systems to attack.

Assets

Hardware (especially switches), software, networks, sensitive data, vendors.

Possible Controls

Armis security researchers worked quickly with both vendors to develop software fixes for the bugs as soon as possible for both Avaya and Aruba intermediary devices.

3.0 Third incident

Don’t expect to get your data back from the Onyx ransomware group

Vulnerability/Vulnerabilities

- Don’t have a better back up process.
- Doesn’t have an enough strong security.
- Don’t monitor what is being installed.
- Remote code execution (RCE).

Threat

This attack is done by a ransomware. Ransomware groups in recent years have ramped up the threats against victims to incentivize them to pay the ransom in return for their stolen and encrypted data. Here, the ransomware was deployed by a group called Onyx.

Risk

Even the ransom is paid new members of crew destroy files that larger than 2MB. They can’t gain them back even they are paid. The group behind the Onyx operation is overwriting the data in those files with trash data rather than encrypting it, so the data cannot be recovered via a decryption key. Given that, victims of Onyx ransomware attacks are being urged not to pay the ransom even though they are hacked. This would be a huge risk if financial or sensitive data is encrypted, overwritten, erased or even the ransom is paid their sensitive data would be published on the internet.

Assets

Hardware, software, E-mails, phone numbers, chat systems.

Possible Controls

The ADA's website suggests people contact a gmail.com address if they have any queries, indicating the extent of the cyber-assault. They hired third-party security specialists "to investigate the impact on ADA systems and restore full system functionality. After this incident they took preparatory steps in advance, including active backups, cyber hygiene, and following best practices such as [US Cybersecurity and infrastructure Security Agency] guidelines on ransomware. The most important point is, they should not try to pay to the intruders even if the data is encrypted. Just try to recover them by using anti-ransomware software or with safe booting. They can make a better back-up process day-by-day for another storage network.

END