OCTOBER 2018

Cyber Security Awareness Month

INFOSEC NEWSBYTES OF THE WEEK | ISSUE 2

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

Bloomberg reported that China had inserted tiny chips into computer equipment manufactured for about 30 US companies, including Apple and Amazon, to steal its technology secrets, citing government and corporate sources. The report further said that the chips were used in equipment made for various US companies and government agencies.

According to Bloomberg, Amazon in its three-year secret investigation uncovered the malicious chips while examining servers manufactured by a start-up called Elemental technologies, which Amazon eventually acquired.

Bloomberg also reported that a unit of the Chinese People's Liberation Army infiltrated the supply chain of computer hardware maker Super Micro Computer Inc to plant malicious chips that could be used to steal corporate and government secrets.

The investigation found that Elemental servers, which were assembled by Super Micro, were tainted with tiny microchips that were not part of their design, Bloomberg said. Amazon reported the matter to US authorities, who determined that the chips allowed attackers to create "a stealth doorway" into networks using those servers, the report said.

Apple and Amazon both denied the report on Thursday, according to Reuters. In a detailed statement on its website Apple wrote, The October 8, 2018 issue of Bloomberg Businessweek incorrectly reports that Apple found "malicious chips" in servers on its network in 2015. As Apple has repeatedly explained to Bloomberg reporters and editors over the past 12 months, there is no truth to these claims.

PoC Attack Escalates MikroTik Router Bug To 'As Bad As It Gets'

Security researchers from Tenable Research uncovered a new technique to exploit MikroTik routers utilising a vulnerability, registered as "CVE-2018-14847," that had been previously patched. This vulnerability is an existing traversal bug in a system's "Winbox," which is a management component and Windows GUI application that MikroTik's RouterOS software is on.

This new attack technique exploits this vulnerability to allow unauthorised remote code execution. A threat actor can use the vulnerability to read and write files on a router after gaining unauthorised access to administrator credentials and can be utilised to get a root shell on the router. While a patch was released for this vulnerability in August 2018, approximately only 30% of routers were patched.

BDO TRA Recommendation:
As a patch has been released for this vulnerability, it is critical to apply it if you have a MikroTik RouterOS versions 6.40.9, 6.42.7 and 6.43. This should stop this vulnerability from being exploited in the future. MikroTik routers also have had several other vulnerabilities uncovered.

For more information on those, visit https://www.tenable.com/blog/tenable-research-advisory-multiple-vulnerabilities-discovered-in-mikrotiks-routeros

At BDO, we have the expertise and experience in a range of cybersecurity services and solutions. Please feel free to contact us and let us know how we can assist you.

FOR MORE INFORMATION

Jonas Jonga| IT Partner
+263242703876-8
jjonga@bdo.co.zw

Frances Sithole| Head of TRA
+263 773 686 729 or +263242703876-8
fsithole@bdo.co.zw

Phishing Attack Uses Azure Blob Storage To Impersonate Microsoft

A new Office 365 phishing campaign has been observed using the Microsoft Azure Blob storage. Threat actors are sending phishing emails containing a PDF attachment that pretends to be from a law firm in Denver, Colorado. The malicious document contains a button to download the PDF file that is supposed to be an unknown scanned document. If users click the "download" button, they are redirected to an HTML page

(https://onedriveunbound80343.blob.core.windows.net)

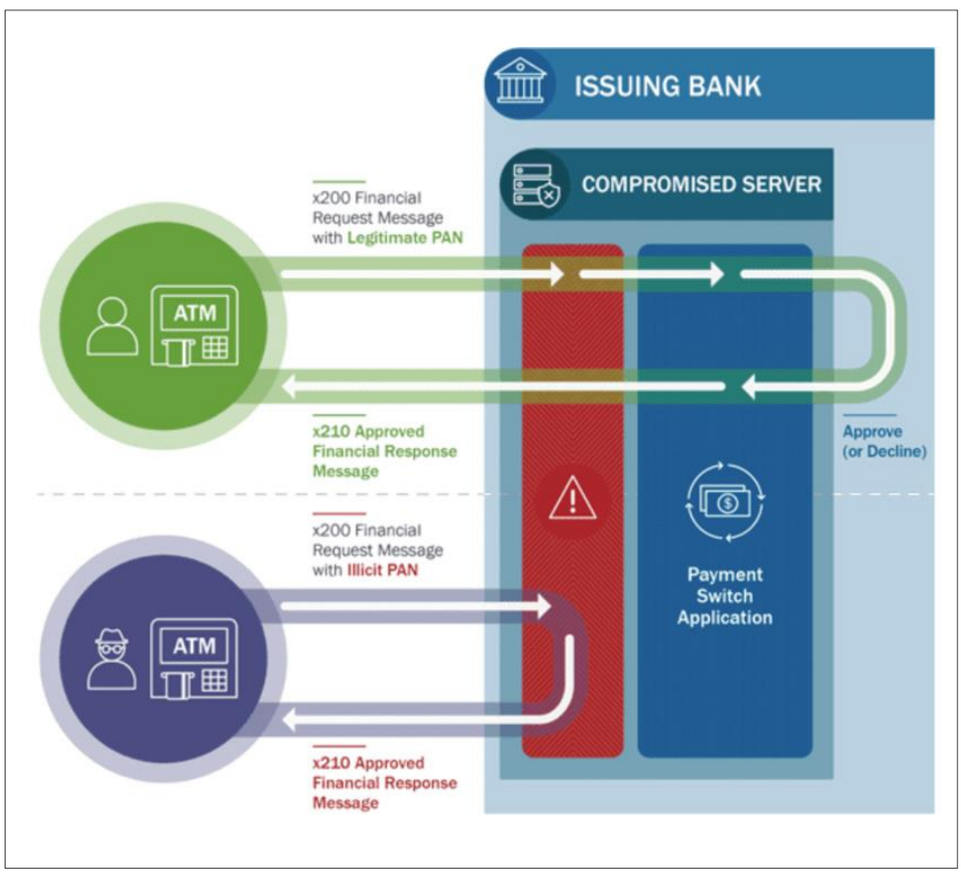
that appears to be an Office 365 login form stored on the Azure Blob storage. The HTML page even contains a signed SSL certificate that is issued by "Microsoft IT TLS CA 5" to feign legitimacy under suspicion. If a user enters in their Microsoft Office 365 credentials, that information is sent to the threat actors' server.

BDO TRA Recommendation:
Organisations should educate employees on how to recognise suspicious emails and non-standard web page addresses. Phishing emails represent a significant security risk because the sending email will often appear legitimate to the target; sometimes a target company email is compromised and used for such emails. Education is the best defence, inform your employees on what to expect for information requests from their managers and colleagues. Employees should also be aware of whom to contact when they suspect they are the target of a possible phishing attack.

Bank Servers Hacked To Trick ATMs Into Spitting Out Millions In Cash

North Korean Advanced Persistent Threat (APT) group "Hidden Cobra," also known as Lazarus Group, have been observed launching a new attack on ATMs to get them to distribute cash by compromising a bank server. This campaign, dubbed, "FASTCash" compromises bank networks, though the initial attack vector is currently unknown, and infects them with Windows-based malware. The malware then affects the payment switch application server which allows the APT group to intercept transaction requests that are linked to the ATM cards and responds with a legitimate-looking validation response.

The fake validation response bypasses actual authentication of the account balance and allows the ATM to give the actor the money. This campaign has been seen targeting banks in Africa and Asia, though it is also suspected that some US banks have also been targeted.



Source: https://thehackernews.com/2018/10/bank-atm-hacking.html

Answering A Video Call Could Compromise Your WhatsApp Account

What if just receiving a video call on WhatsApp could hack your smartphone?

This sounds filmy, but Google Project Zero security researcher Natalie Silvanovich found a critical vulnerability in WhatsApp messenger that could have allowed hackers to remotely take full control of your WhatsApp just by video calling you over the messaging app.

The vulnerability is a memory heap overflow issue which is triggered when a user receives a specially crafted malformed RTP packet via a video call request, which results in the corruption error and crashing the WhatsApp mobile app.

Since the vulnerability affect RTP (Real-time Transport Protocol) implementation of Whatsapp, the flaw affects Android and iOS apps, but not WhatsApp Web that relies on WebRTC for video calls.

In other words, hackers only need your phone number to completely hijack your WhatsApp account and spy on your secret conversations.

Silvanovich discovered and reported the vulnerability to the WhatsApp team in August this year. WhatsApp acknowledged and patched the issue on September 28 in its Android client and on October 3 in its iPhone client.

So if you have not yet updated your WhatsApp for Android or WhatsApp for iOS, You should consider upgrading now.

THREE WAYS A DATA BREACH CAN OCCUR

Knowing what you should be looking for can help you prevent attacks as well as quickly identify and respond to suspicious activity. This article looks at some real-world examples of some of the most common causes of data breaches and explains how they occurred.

MALWARE

Contrary to what many people think, you don't need to be a sophisticated criminal hacker to commit cybercrime. Malware is a perfect example of just how simple attacks can be.

Here is how it works: cyber attackers purchase a piece of malware that is designed to exploit a specific vulnerability. They find a system that contains that vulnerability. First, they plant the malware after which they scoop up the rewards.

However, there are many types of malware you need to be aware of, including adware, spyware, bots, ransomware, Trojan horses, viruses and worms. It is often hard to know when you have been infected, as some malware sits on computers drawing as little attention to itself as possible. Other malware, such as ransomware, makes its presence clear, locking users' computers and demanding payment for the decryption key.

EMPLOYEE NEGLIGENCE

There are more ways your employees can mess up than you can think of. For example, they could lose a laptop or USB containing sensitive information, misconfigure databases, accidentally disclose information or let a crook into your building and access your files.

Accidental breaches are impossible to eradicate, because people inevitably make mistakes. Sometimes it is just negligence: the employee forgot to follow the rules. Other times, breaches are the result of miscommunication: an employee wasn't told what to do.

Most human error-related breaches involve a little of both.

Organisations can address both these failings by emphasising information security staff awareness training. It will help employees understand their security responsibilities, as well as helping the organisation understand its weaknesses and what it needs to improve.

PHISHING

Attackers send tens of millions of phishing emails every year, impersonating legitimate organisations and attempting to get recipients to click malicious links or attachments. If you fall for their scams, you hand over your personal information or allow malware to infect your systems.

Phishing attacks are often generic messages sent in bulk in the hope of catching people off guard. You might receive a message claiming to be an invoice that you need to pay, or someone pretending to be a colleague might ask you to send over a document.

Attacks often take advantage of current events. All you had to do was follow the link and provide your personal details.

Except that there is no prize. The perpetrators get away with people's names and financial details, and off they go on a fraud splurge.