Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

June 2020

This security bulletin is powered by Telelink's

Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

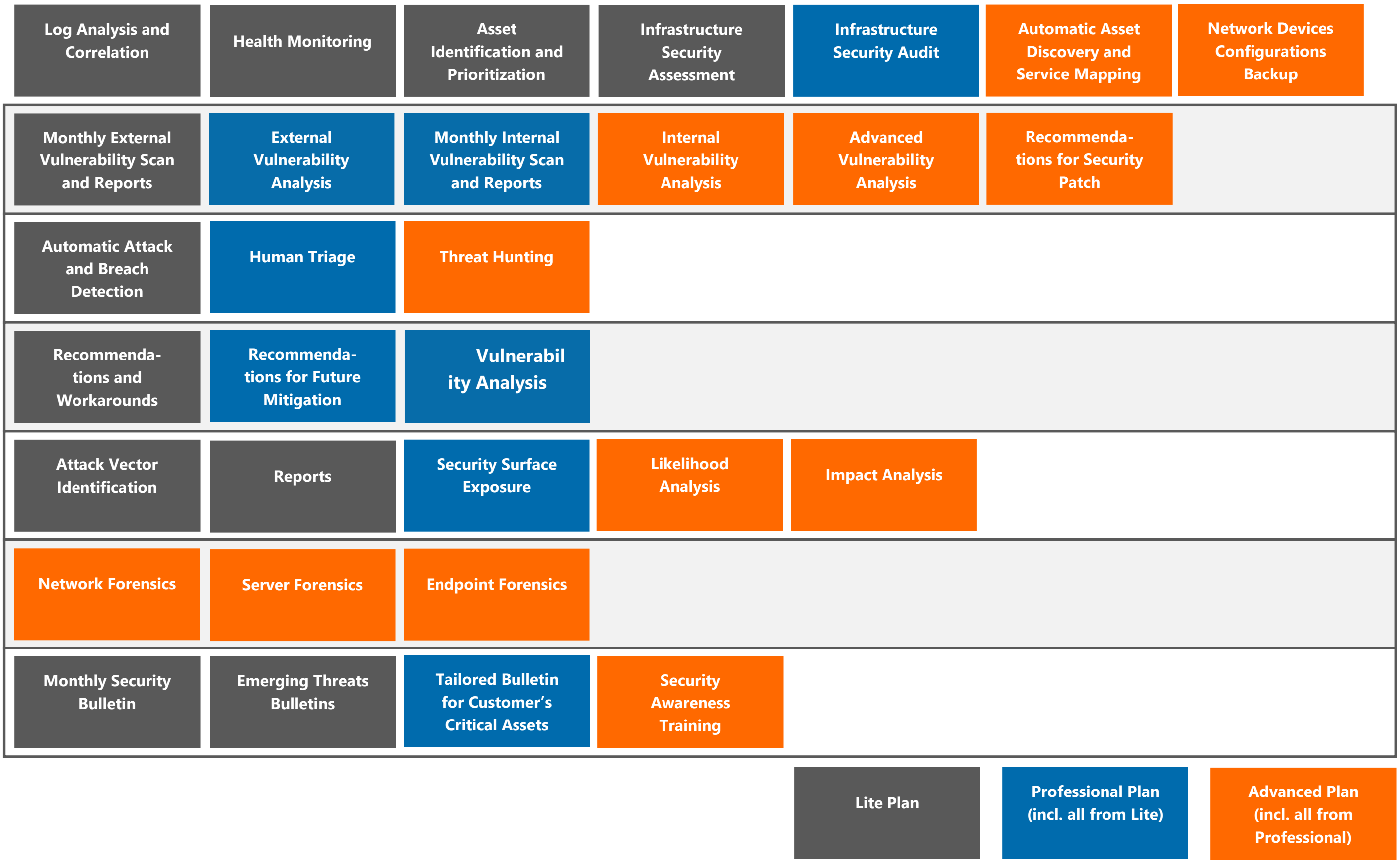
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis and cyber threat mitigation!



⬛ Log Analysis and Correlation	⬛ Health Monitoring	⬛ Asset Identification and Prioritization	⬛ Infrastructure Security Assessment	🟦 Infrastructure Security Audit	🟧 Automatic Asset Discovery and Service Mapping	🟧 Network Devices Configurations Backup
⬛ Monthly External Vulnerability Scan and Reports	🟦 External Vulnerability Analysis	🟦 Monthly Internal Vulnerability Scan and Reports	🟧 Internal Vulnerability Analysis	🟧 Advanced Vulnerability Analysis	🟧 Recommendations for Security Patch	
⬛ Automatic Attack and Breach Detection	🟦 Human Triage	🟧 Threat Hunting				
⬛ Recommendations and Workarounds	🟦 Recommendations for Future Mitigation	🟦 Vulnerability Analysis				
⬛ Attack Vector Identification	⬛ Reports	🟦 Security Surface Exposure	🟧 Likelihood Analysis	🟧 Impact Analysis		
🟧 Network Forensics	🟧 Server Forensics	🟧 Endpoint Forensics				
⬛ Monthly Security Bulletin	⬛ Emerging Threats Bulletins	🟦 Tailored Bulletin for Customer's Critical Assets	🟧 Security Awareness Training			

⬛ Lite Plan

🟦 Professional Plan (incl. all from Lite)

🟧 Advanced Plan (incl. all from Professional)

What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents:

Executive summary 4
1. Hackers say they stole millions of credit cards from Banco BCR 6
2. Microsoft Shells Out $100K for IoT Security 7
3. Cisco Webex phishing uses fake cert errors to steal credentials 8
4. Meant to Combat ID Theft, Unemployment Benefits Letter Prompts ID Theft Worries 11
5. Rail vehicle manufacturer Stadler hit by cyberattack, blackmailed 13
6. May 2020 Patch Tuesday: Microsoft fixes 111 vulnerabilities, 13 Critical 14
7. Microsoft Addresses 111 Bugs for May Patch Tuesday 15
8. What's new in Windows Subsystem for Linux 2.0, coming soon 19
9. The Connection Between Cloud Service Providers and Cyber Resilience 22
10. New iOS Jailbreak Tool Works on iPhone Models iOS 11 to iOS 13.5 24
11. 26 million LiveJournal accounts being shared on hacker forums 25
12. Thermal Imaging as Security Theater 29

Executive summary

1. Operators of the Maze Ransomware claim to have gained access to Banco BCR, the state-owned Bank of Costa Rica, and stolen 11 million credit card credentials along with other data. →

2. Microsoft has launched a bug-bounty program for its Azure Sphere offering, which is a security suite for the Internet of Things (IoT) that encompasses hardware, OS and cloud elements. The top reward will come in at $100,000 and the program is an expansion of a program unveiled at Black Hat last August - Azure Security Lab, which used to be an invite-only affair for researchers. →

3. A highly convincing series of phishing attacks are using fake certificate error warnings with graphics and formatting taken from Cisco Webex emails to steal users' account credentials are already targeting more than 5000 employees that rely on Webex. →

4. Poor execution of Unemployment Benefits program in USA lead to some unemployment applications triggering an automatic letter from U.S. Bank to the applicant. The letters are intended to prevent identity theft, but many people are mistaking these vague missives for a notification that someone has hijacked their identity. →

5. International rail vehicle construction company, Stadle with more than 11,000 employees based in 7 production locations, 5 component manufacturing sites, and 40 service locations around the world disclosed that it was the victim of a cyberattack which might have also allowed the attackers to steal company and employee data. →

6. Microsoft May Patch arrived. Check the announcement and in-depth information on the 111 bugs patched by it, including some Priviledge-Escalation. →

7. Windows Subsystem for Linux 2 (WSL2) is being released soon with the May 2020 Update (Windows 10 2004) and comes with new features and performance improvements, including real Linux kernel. Check all the other improvements and changes in the article. →

8. As organizations have increasingly turned to cloud service providers (CSPs) to support their technical infrastructure, the primarily goal is to reduce IT costs and increase the efficiency of computing resources. However, in many cases, CSPs can also offer protection from security threats and increased cyber resilience — though customers often face trade-offs when they rely on cloud providers for these protections. Explore the link between cyber resilience and CSP in this article by Josephine Wolff - assistant professor of cybersecurity policy at the Tufts University Fletcher School of Law and Diplomacy. →

9. Latest version of iPhone jailbreak tool UnC0ver uses unpatched zero-day exploit to take complete control of devices, even those running iOS 13.5 as the creator claims that this is the first 0-day jailbreak for iPhone since iOS 8. →

10. A database containing over 26 million unique LiveJournal user accounts, including plain text passwords, is being shared for free on multiple hacker forums as according to rumors LiveJournal was breached in 2014 and account credentials for 33 million users were stolen. Since approximately the 8th of May, 2020, links to a data dump have been circulating on various hacker forums, containing email addresses, usernames, profile URLs, and passwords converted to plain text after initially being stored as MD5 hashes.→

11. Is the thermal imaging, utilized by number of organizations to screen potential CoVid-19 cases a new security theatre measure? Bruce Schneier thinks so. →

1. Hackers say they stole millions of credit cards from Banco BCR

Hackers claim to have gained access to the network of Banco BCR, the state-owned Bank of Costa Rica, and stolen 11 million credit card credentials along with other data.

This attack was allegedly conducted by the operators of the Maze Ransomware, who have been behind numerous cyberattacks against high-profile victims such as IT services giant Cognizant, cyber insurer Chubb, and drug testing facility Hammersmith Medicines Research LTD.

On their data leak site, the hackers claim to have gained access to Banco BCR's network in August 2019, but did not proceed with encrypting the devices as "the possible damage was too high."

Maze claims that the bank never secured their network and once again gained access to the bank's network in February 2020.

They state that they did not encrypt the bank during the second attack because it "was at least incorrect during the world pandemic," but claim to have stolen a few years of data, including 11 million credit cards.

Of these credit cards, 4 million are stated to be unique and 140,000 allegedly belong to people from the USA.

As proof of this theft, Maze posted what they say are 240 credit card numbers, with the last four digits removed, along with expiration dates and credit card verification codes (CVC).

The ransomware operators told BleepingComputer that they have tried to contact the bank multiple times with a ransom demand and may sell the data on the dark web.

Maze states that this ransom is their "reward for pointing out problems in the security system through which half a bank could be pulled out".

If you are a credit card customer of Banco BCR, it is suggested that you contact the bank to confirm that your account is not at risk and to monitor your credit card activity for fraudulent charges.

BleepingComputer has contacted Banco BCR to confirm the attack but has not received a response as of yet.

Source: https://www.bleepingcomputer.com/news/security/hackers-say-they-stole-millions-of-credit-cards-from-banco-bcr/

2. Microsoft Shells Out $100K for IoT Security

A three-month Azure Sphere bug-bounty challenge will offer top rewards for compromising Pluton or Secure World within Microsoft's IoT security suite.

Microsoft has launched a bug-bounty program for its Azure Sphere offering, which is a security suite for the internet of things (IoT) that encompasses hardware, OS and cloud elements. The top reward will come in at $100,000.

The Azure Sphere Security Research Challenge is an expansion of a program unveiled at Black Hat last August. That program, Azure Security Lab, was an invite-only affair for researchers, who were asked to mimic criminal hackers within a special, non-customer-touching cloud environment.

This time around, the challenge will run for three months, and will be application based: Bug-hunters need to submit an application to participate by May 15. The actual challenge then starts June 1 and will run through the end of August.

A $100,000 bounty will be given "for specific scenarios": For instance, the ability to execute code on Pluton or on Secure World.

Pluton is a secure boot hardware root of trust governing firmware and hardware. Pluton is also incidentally part of Microsoft's firmware protection for the Xbox gaming system.

Secure World meanwhile is one of two operating environments found in the application processor's ARM Cortex-A subsystem, responsible for executing the operating system, applications and services (the other is called "Normal World"). Secure World executes only the Microsoft-supplied Security Monitor and other code.

Other exploitation scenarios will earn existing public Azure Bounty Program awards, with a 20 percent bonus for finding critical bugs and a 10 percent bonus for vulnerabilities rated important.

Microsoft said that eligible exploits include: The ability to either locally or remotely execute code on NetworkD; anything allowing execution of unsigned code that isn't pure return-oriented programming (ROP); ability to spoof device authentication; elevation of privilege outside of the capabilities described in the application manifest (e.g. changing user ID, adding access to a binary); ability to modify software and configuration options (except full device reset) on a device in the manufacturing state; and the ability to alter the firewall allowing communication out to other domains not in the app manifest (but not DNS poisoning).

Microsoft is offering various resources to program participants, including the Azure Sphere development kit (DevKit); product documentation; direct communication channels with the Microsoft team; and other Microsoft products and services if needed.

“Microsoft recognizes security is not a one-and-done event,” wrote Sylvie Liu, security program manager at the Microsoft Security Response Center, in announcing the challenge this week. “Risks need to be mitigated consistently over the lifetime of a constantly growing array of devices and services. Engaging the security research community to research for high-impact vulnerabilities before the bad guys do is part of the holistic approach Azure Sphere is taking to minimize the risk.”

Microsoft is also collaborating with a raft of partners on the program, including Avira, Baidu, Bitdefender, Bugcrowd, Cisco Talos, ESET, FireEye, F-Secure, HackerOne, K7 Computing, McAfee, Palo Alto Networks and Zscaler.

Microsoft continues to roll out bug-bounty programs. Last year, the computing giant released a program designed to sniff out flaws in Azure DevOps; kicked off a program with payouts as high as $100,000 for holes in identity services and implementations of the OpenID standard, Microsoft Account and Azure Active Directory; and in the wake of the Meltdown and Spectre flaws, Microsoft started a new bug bounty program targeting speculative execution side-channel vulnerabilities that offered up to $250,000 for identifying new categories of speculative execution attacks that Microsoft and other industry partners are not yet aware of.

Source: https://threatpost.com/microsoft-100k-iot-security-azure-sphere/155517/

3. Cisco Webex phishing uses fake cert errors to steal credentials

A highly convincing series of phishing attacks are using fake certificate error warnings with graphics and formatting lifted from Cisco Webex emails to steal users' account credentials.

Cisco Webex is a video and team collaboration solution that helps users set up video conferences, webinars, online meetings, and share their screens with their colleagues and friends. The platform is currently facing an influx of new users due to the unusual remote working increase caused by the COVID-19 pandemic.

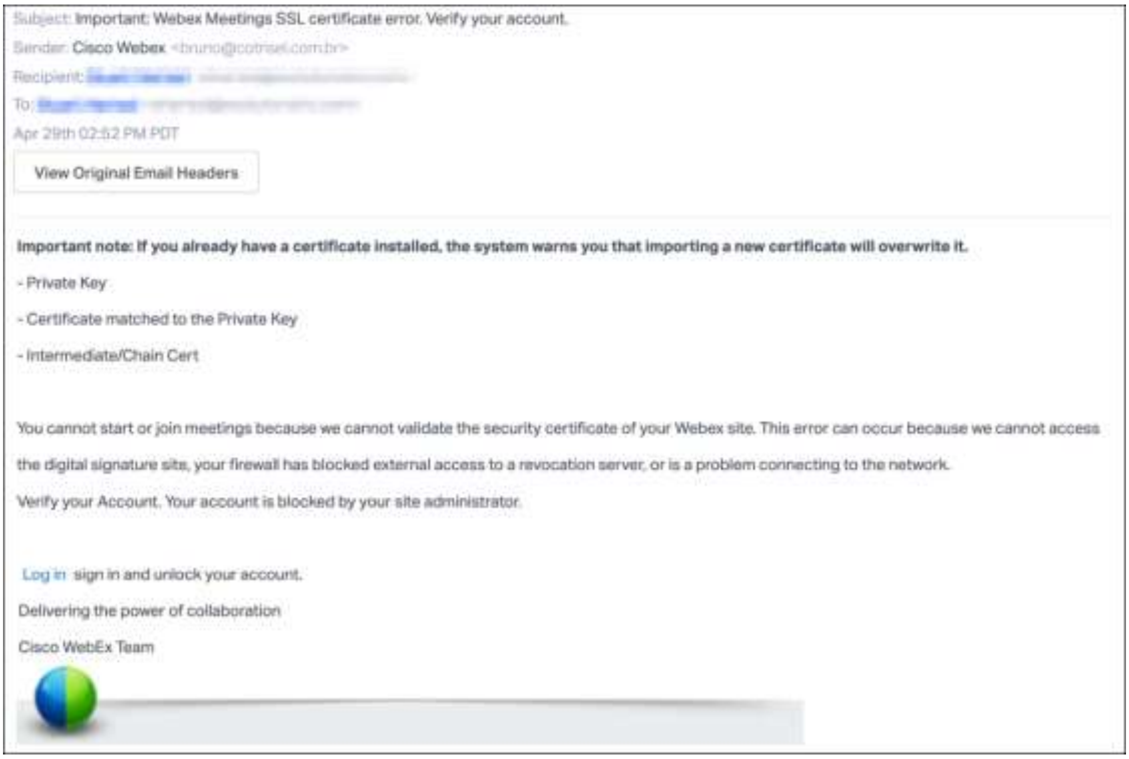
According to stats shared by email security company Abnormal Security, these phishing emails have already landed in the mailboxes of up to 5,000 targets that use Cisco Webex while working remotely.

Phishing landing pages on lookalike domains

The attackers induce a sense of urgency with their phishing messages by using cloned graphics and formatting designed to closely mimic automated SSL certificate error alerts that Cisco Webex would send to users.

The phishing emails impersonate the Cisco Webex Team and warn the targets that they have to verify their accounts as they are blocked by the administrator because of Webex Meetings SSL cert errors.

Users are then requested to click on an embedded 'Log in' hyperlink that will allow them to sign in and unlock their accounts.



Subject: Important: Webex Meetings SSL certificate error. Verify your account.

Sender: Cisco Webex <bruno@cotrisel.com.br>

Recipient: [redacted]

To: [redacted]

Apr 29th 02:52 PM PDT

Important note: If you already have a certificate installed, the system warns you that importing a new certificate will overwrite it.

- Private Key

- Certificate matched to the Private Key

- Intermediate/Chain Cert

You cannot start or join meetings because we cannot validate the security certificate of your Webex site. This error can occur because we cannot access the digital signature site, your firewall has blocked external access to a revocation server, or is a problem connecting to the network.

Verify your Account. Your account is blocked by your site administrator.

Log in sign in and unlock your account.

Delivering the power of collaboration

Cisco WebEx Team

Cisco Webex phishing email sample (Abnormal Security)

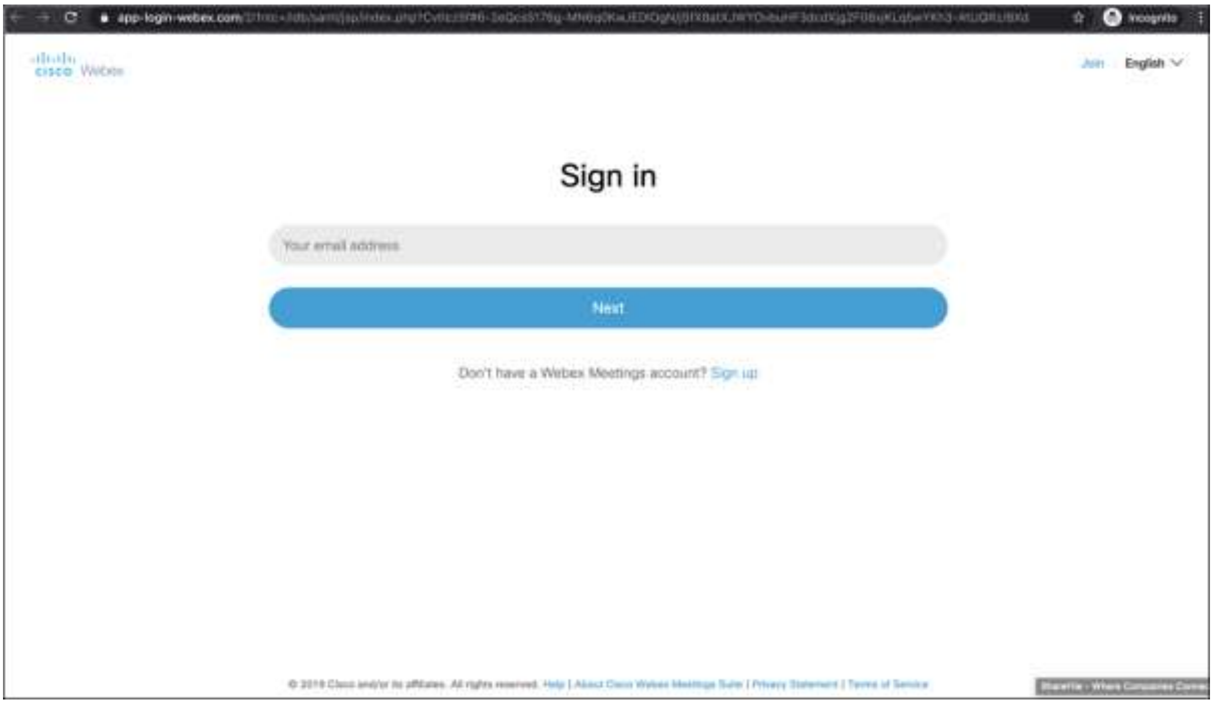
"The email includes a SendGrid link that redirects to a WebEx Cisco phishing credentials site hosted at **https://app-login-webex[.]com**," Abnormal Security's researchers found.

"The domain of this webpage has been recently registered by a registrar in the Czech Republic, and is not affiliated with Webex or Cisco more broadly."

Once they reach the phishing landing page that convincingly mimics a real Cisco Webex sign-in page, the targets who fall for the phishers' tricks and enter their credentials will have their accounts stolen and delivered to an attacker-controlled server.

"The attacker could use the compromised user account to send further attacks within the organization and to external partners," the researchers further explained.

Seeing that this phishing campaign almost perfectly clones, it should be able to bypass at least some Secure Email Gateways' (SEGs) protections and convince many of the targets to visit the attackers' phishing landing page instead of deleting or sending the phishing emails to the Spam folder.


app-login-webex.com/[illegible]

Sign in

Your email address

Next

Don't have a Webex Meetings account? Sign up

© 2019 Cisco and/or its affiliates. All rights reserved. Help | About Cisco Webex Meetings Suite | Privacy Statement | Terms of Service

Cisco Webex phishing email sample (Abnormal Security)

Other video conferencing platforms' users are also being targeted during this challenging time because of the increase in the number of remote workers.

For instance, another highly convincing phishing campaign spotted by Abnormal Security las month used cloned imagery from automated Microsoft Teams alerts to harvest Office 365 credentials from almost 50,000 users.

Phishing attacks are also targeting Zoom users with fake Zoom meeting notifications being used to threaten potential victims who work in corporate environments that their contracts will be suspended or terminated, with the end goal of harvesting their email addresses and passwords.

What makes all these phishing campaigns even more dangerous than regular ones is that their targets are currently being flooded with alerts from various online collaboration services which makes them prone to ignoring any red flags that would otherwise enable them to recognize such attacks.

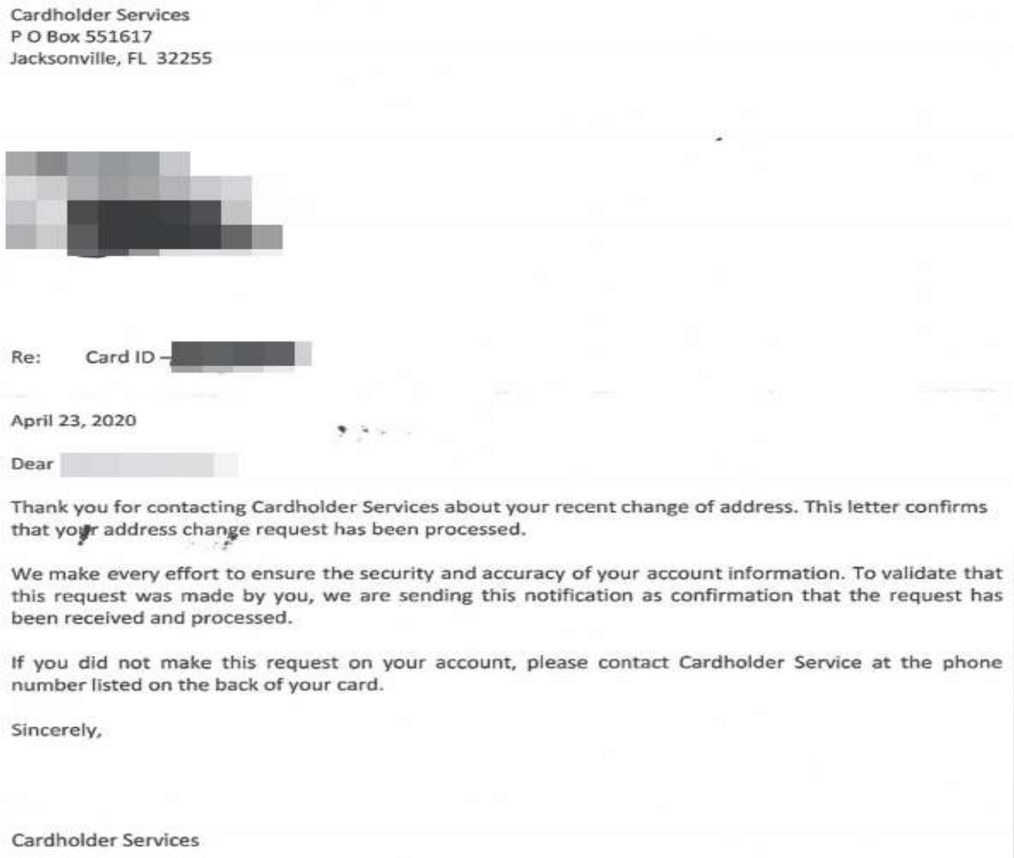
Source: https://www.bleepingcomputer.com/news/security/cisco-webex-phishing-uses-fake-cert-errors-to-steal-credentials/

4. Meant to Combat ID Theft, Unemployment Benefits Letter Prompts ID Theft Worries

Millions of Americans now filing for unemployment will receive benefits via a prepaid card issued by **U.S. Bank**, a Minnesota-based financial institution that handles unemployment payments for more than a dozen U.S. states. Some of these unemployment applications will trigger an automatic letter from U.S. Bank to the applicant. The letters are intended to prevent identity theft, but many people are mistaking these vague missives for a notification that someone has hijacked their identity.

So far this month, two KrebsOnSecurity readers have forwarded scans of form letters they received via snail mail that mentioned an address change associated with some type of payment card, but which specified neither the entity that issued the card nor any useful information about the card itself.

Searching for snippets of text from the letter online revealed pages of complaints from consumers who appear confused about the source and reason for the letter, with most dismissing it as either a scam or considering it a notice of attempted identity theft. Here's what's the letter looks like:



Cardholder Services
P O Box 551617
Jacksonville, FL 32255

[redacted]

Re: Card ID –[redacted]

April 23, 2020

Dear [redacted]

Thank you for contacting Cardholder Services about your recent change of address. This letter confirms that your address change request has been processed.

We make every effort to ensure the security and accuracy of your account information. To validate that this request was made by you, we are sending this notification as confirmation that the request has been received and processed.

If you did not make this request on your account, please contact Cardholder Service at the phone number listed on the back of your card.

Sincerely,

Cardholder Services

A scan of the form letter sent by U.S. Bank to countless people enrolling in state unemployment benefits.

My first thought when a reader shared a copy of the letter was that he recently had been the victim of identity theft. It took a fair amount of digging online to discover that the nebulously named "Cardholder Services" address in Florida referenced at the top of the letter is an address exclusively used by U.S. Bank.

That digging indicated U.S. Bank currently manages the disbursement of funds for unemployment programs in at least 17 states, including Arkansas, Colorado, Delaware, Idaho, Louisiana, Maine, Minnesota, Nebraska, North Dakota, Ohio, Oregon, Pennsylvania, South Dakota, Texas, Utah, Wisconsin, and Wyoming. The funds are distributed through a prepaid debit card called ReliaCard.

To make matters more confusing, the flood of new unemployment applications from people out of work thanks to the COVID-19 pandemic reportedly has overwhelmed U.S. Bank's system, meaning that many people receiving these letters haven't yet gotten their ReliaCard and thus lack any frame of reference for having applied for a new payment card.

Reached for comment about the unhelpful letters, U.S. Bank said it automatically mails them to current and former ReliaCard customers when changes in its system are triggered by a customer – including small tweaks to an address — such as changing "Street" to "St."

"This can include letters to people who formerly had a ReliaCard account, but whose accounts are now inactive," the company said in a statement shared with KrebsOnSecurity. "If someone files for unemployment and had a ReliaCard in years past for another claim, we can work with the state to activate that card so the cardholder can use it again."

U.S. Bank said the letters are designed to confirm with the cardholder that the address change is valid and to combat identity theft. But clearly, for many recipients they are having the opposite effect.

"We encourage any cardholders who have questions about the letters to call the number listed on the back of their cards (or 855-282-6161)," the company said.

That's nice to know, because it's not obvious from reading the letter which card is being referenced. U.S. Bank said it would take my feedback under advisement, but that the letters were intended to be generic in nature to protect cardholder privacy.

"We are always seeking to improve our programs, so thank you for bringing this to our attention," the company said. "Our teams are looking at ways to provide more specific information in our communications with cardholders."

Source: https://krebsonsecurity.com/2020/05/meant-to-combat-id-theft-unemployment-benefits-letter-prompts-id-theft-worries/

5. Rail vehicle manufacturer Stadler hit by cyberattack, blackmailed

International rail vehicle construction company, Stadler, disclosed that it was the victim of a cyberattack which might have also allowed the attackers to steal company and employee data.

Stadler manufactures a wide range of railway vehicles from high-speed trains to tramways and trams, and it is the world's leading service provider in the rack-and-pinion rail vehicle industry.

The Swiss-based company has a workforce of roughly 11,000 employees based in 7 production locations, 5 component manufacturing sites, and 40 service locations around the world.

Data leak threats

Stadler announced on Thursday evening that attackers managed to infiltrate its IT network and infect some of its machines with malware and, most probably, to collect and exfiltrate data from the compromised devices in the process.

"Stadler's internal monitoring services have established that the company's IT network was attacked with malware and that it is highly probable that an outflow of data of an as yet unknown extent has occurred," the company said.

After the attack was discovered and Stadler took measures to contain it, the threat actors behind this security incident also asked for a large ransom and are attempting to blackmail the company by threatening to leak stolen data.

The unknown perpetrators are attempting to blackmail Stadler, demanding large sums of money, and to put pressure on Stadler with the possible publication of data in order to harm the company and thus also its employees. - Stadler

The rail vehicle manufacturer said that it took the steps needed to secure its computing systems immediately after and it also hired a team of external security experts to help with the incident's investigation.

Stadler also stated that it has backups for the affected data and that it is working on restarting and, potentially, restoring the impacted systems.

While the company does not explicitly call it a ransomware attack, all the signs of one are there: attackers asking for a ransom under the threat of leaking sensitive data stolen before encrypting the systems and the mention of data backups which directly implies that its systems were encrypted (or wiped) during the attack.

The entire Stadler group impacted by the attack

Although the incident announcement doesn't disclose the number of locations and systems affected, Swiss media says that the entire Stadler group was impacted by this cyberattack, including locations from Switzerland and abroad.

Stadler also said in a statement that the company has filed a complaint with the Thurgau public prosecutor and that an investigation is ongoing.

"Despite the corona pandemic and cyber attacks, the continuation of the production of new trains and Stadler's services is guaranteed," the train manufacture emphasizes.

BleepingComputer has reached out to a Stadler spokesperson for additional details but had not heard back at the time of this publication.

Source: https://www.bleepingcomputer.com/news/security/rail-vehicle-manufacturer-stadler-hit-by-cyberattack-blackmailed/

6. May 2020 Patch Tuesday: Microsoft fixes 111 vulnerabilities, 13 Critical

With the release of the May 2020 Patch Tuesday security updates, Microsoft has released fixes for 111 vulnerabilities in Microsoft products. Of these vulnerabilities, 13 are classified as Critical, 91 as Important, 3 as Moderate, and 4 as Low.

This month there are no zero-day or unpatched vulnerabilities.

Users should install these security updates as soon as possible to protect Windows from known security risks.

For information about the non-security Windows updates, you can read about today's Windows 10 Cumulative Updates KB4556799 & KB4551853 Released.

Vulnerabilities of interest

Three Critical Microsoft Edge vulnerabilities were patched by Microsoft this month that could allow an attacker to perform remote code execution by tricking a user into visiting a maliciously crafted web site.

- CVE-2020-1056 - Microsoft Edge Elevation of Privilege Vulnerability
- CVE-2020-1059 - Microsoft Edge Spoofing Vulnerability
- CVE-2020-1096 - Microsoft Edge PDF Remote Code Execution Vulnerability

If exploited, these vulnerabilities could allow the attacker to execute commands on the computer with full user rights.

Another critical vulnerability exists in the Color Management Module (ICM32.dll) that allows attackers to perform remote code execution by tricking a user into visiting a malicious web site.

- CVE-2020-1117 | Microsoft Color Management Remote Code Execution Vulnerability

Recent security updates from other companies

Other vendors who released security updates recently include:

- **Adobe** released security updates today for Acrobat, Reader, and DNG SDK.
- **SAP** also released their monthly security updates today, with six having a CVSS score of 9 or higher.
- **vBulletin** released a security update this week for their vBulletin forum software versions 5.5.6, 5.6.0, and 5.6.1.
- **Android** released their May 2020 security updates last week.
- **Mozilla** released Firefox 76.0 last week along with security fixes.
- **Google** Chrome 81.0.4044.138 was released on May 5th, with three security fixes.
- **VMWare** released a security update for VMware vRealize Operations Manager on May 8th.

The May 2020 Patch Tuesday Security Updates

Below is the full list of resolved vulnerabilities and released advisories in the May 2020 Patch Tuesday updates. To access the full description of each vulnerability and the systems that it affects, you can view the full report here.

Source: https://www.bleepingcomputer.com/news/microsoft/may-2020-patch-tuesday-microsoft-fixes-111-vulnerabilities-13-critical/

7. Microsoft Addresses 111 Bugs for May Patch Tuesday

Important-rated EoP flaws make up the bulk of the CVEs; SharePoint continues its critical run with four worrying bugs.

Microsoft has released fixes for 111 security vulnerabilities in its May Patch Tuesday update, including 16 critical bugs and 96 that are rated important.

Unlike other recent monthly updates from the computing giant this year, none of the flaws are publicly known or under active attack at the time of release.

Along with the expected cache of operating system, browser, Office and SharePoint updates, Microsoft has also released updates for .NET Framework, .NET Core, Visual Studio, Power BI, Windows Defender, and Microsoft Dynamics.

Privilege-Escalation Bugs to the Fore

The majority of the fixes are important-rated elevation-of-privilege (EoP) bugs. There are a total of 56 of these types of fixes in Microsoft's May release, primarily impacting various Windows components. This class of vulnerabilities is used by attackers once they've managed to gain initial access to a system, in order to execute code on their target systems with elevated privileges.

Three of these bugs have received a rating of "Exploitation More Likely," pointed out Satnam Narang, staff research engineer at Tenable: A pair of flaws in Win32k (CVE-2020-1054, CVE-2020-1143) and one in the Windows Graphics Component (CVE-2020-1135).

The two flaws in Win32k both exist when the Windows kernel-mode driver fails to properly handle objects in memory, according to Microsoft's advisory. An attacker who successfully exploited either vulnerability could run arbitrary code in kernel mode; thus, an attacker could then install programs; view, change or delete data; or create new accounts with full user rights.

To exploit these, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.

The Windows Graphics Component EoP bug meanwhile is found in most Windows 10 and Windows Server builds, Jay Goodman, strategic product marketing manager at Automox, told Threatpost. "The vulnerability could allow an exploit that leverages how Windows Graphics handles objects in memory," he said. "An attacker could use this vulnerability to elevate a process' privileges, allowing the attacker to steal credentials or sensitive data, download additional malware, or execute malicious code."

It was demonstrated at this year's Pwn2Own, said Dustin Childs, researcher at Trend Micro's Zero-Day Initiative.

"While Pwn2Own may have been virtual this year, the bugs demonstrated certainly were not," he said in a Patch Tuesday analysis. "This bug from the Fluoroacetate duo of Richard Zhu and Amat Cama allows a logged-on user to take over a system by running a specially crafted program. They leveraged a use-after-free (UAF) bug in Windows to escalate from a regular user to SYSTEM."

There is also one critical EoP bug, in Microsoft Edge (CVE-2020-1056). This exists because Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain, according to

Microsoft's advisory. However, in all cases an attack requires user interaction, such as tricking users into clicking a link that takes them to the attacker's site.

"In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability," it said. "In addition, compromised websites and websites that accept or host user-provided content could contain specially crafted content that could exploit the vulnerability."

Critical Patches to Consider

Other bugs of note include two remote code execution (RCE) flaws in Microsoft Color Management (CVE-2020-1117) and Windows Media Foundation (CVE-2020-1126), which could both be exploited by tricking a user via social engineering techniques into opening a malicious email attachment or visiting a website that contains the exploit code.

"Successful exploitation would allow an attacker to perform actions on the system using the same permissions as the current user that was compromised," said Tenable's Narang. "If the user has administrative privileges, the attacker could then perform a variety of actions, such as installing programs, creating a new account with full user rights, and viewing, changing or deleting data."

The critical flaws also include updates for Chakra Core, Internet Explorer and EdgeHTML, while SharePoint has four critical bugs, continuing its dominance in that category from last month.

"Most of the critical vulnerabilities are resolved by the OS and browser updates, but there are four critical vulnerabilities in SharePoint and one in Visual Studio," Todd Schell, senior product manager, security, for Ivanti said via email.

On the SharePoint front, CVE-2020-1023 and CVE-2020-1102 are critical RCE vulnerabilities that would allow attackers to access a system and read or delete contents, make changes, or directly run code on the system.

"This gives an attacker quick and easy access to not only your organization's most critical data stored in the SQL server but also a platform to perform additional malicious attacks against other devices in your environment," Automox' Goodman told Threatpost. "Systems like SharePoint can often be difficult to take offline and patch, allowing RCE vulnerabilities to linger in your infrastructure. This gives attackers the ability to 'live off the land' and move laterally easily once access is gained via an existing exploit.

Also in SharePoint, an exploit for CVE-202-1024 would give an attacker the ability to execute arbitrary code from the SharePoint application pool and the SharePoint server farm account, potentially impacting all the users connected into and using the platform.

"If an attacker is able to access this critical component of the network, lateral movement throughout the connected filesystems would be difficult to contain," said Richard Melick, Sr., technical product manager at Automox, via email. "With Microsoft SharePoint's rise in use to support remote workers, addressing this vulnerability quickly is critical to securing a central hub of access to the full corporate network and data."

As for Visual Studio, "users of the Visual Studio Code Python Extension should take note of the two patches released this month," Childs noted, which are both RCE issues. "One is rated critical [CVE-2020-1192] while the other is rated important [CVE-2020-1171]. There's no indication as to why one is more severe than the other, and users should treat them both as critical."

Other Bugs of Note

Administrators should also pay attention to a handful of other issues in the trove of patches, such as two for VBScript (CVE-2020-1060 and CVE-2020-1058).

When exploited, both could allow an attacker to gain the same right as the current user.

"While both CVE-2020-1058 and CVE-2020-1060 are not rated critical in severity, it's very possible to see them used by attackers in the wild; both vulnerabilities impact VBScript and how the scripting engine handles objects in memory," Chris Hass, director of information security and research for Automox, told Threatpost. "Due to the versatility of VBScript in Windows, these vulnerabilities allow for several attack vectors to be explored by malicious actors."

For instance, an attacker could host a malicious webpage with a specially crafted payload to exploit any user visiting the page using Internet Explorer, inject code into a compromised webpage, or even launch a malvertising campaign to serve the payload via malicious advertisements on popular websites, he said.

He added, "An attacker could also embed an Active X control object in an application or Office document that could be used in a phishing campaign to gain code execution on the machine. It's likely only a matter of time till attackers, such as DarkHotel, incorporate these into their arsenal." DarkHotel has been known to use VBScript bugs in the past.

There's also an interesting denial-of-service vulnerability (CVE-2020-1118) in Microsoft Windows Transport Layer Security. It allows a remote, unauthenticated attacker to abnormally reboot, resulting in a denial-of-service condition.

"A NULL pointer dereference vulnerability exists in the Windows implementation of the Diffie-Hellman protocol," explained Childs. "An attacker can exploit this vulnerability by sending a malicious Client Key Exchange message during a TLS handshake. The vulnerability affects both TLS clients and TLS servers, so just about any system could be shut down by an attacker. Either way, successful exploitation will cause the lsass.exe process to terminate."

In terms of patching prioritization, "What is interesting and often overlooked is seven of the 10 CVEs at higher risk of exploit are only rated as important," Ivanti's Schell said. "It is not uncommon to look to the critical vulnerabilities as the most concerning, but many of the vulnerabilities that end up being exploited are rated as important vs. critical. If your prioritization stops at vendor severity or even CVSS scores above a certain level, you may want to reassess your metrics. Look to other risk metrics like publicly disclosed, exploited (obviously) and exploitability assessment (Microsoft specific) to expand your prioritization process."

Melick added that the critical bug in Visual Studio Code, which stems from how the Python extension loads workspace settings from a notebook file, should be a top priority, given that it's one of the most popular developer environment tools.

"Accounting for over 50 percent of the market share of developer tools, an attacker is not short of potential targets, and if successful, would have the ability to take control of the victim machine acting as the current user," he said. "Once an attacker has gained access, they could be capable of stealing critical information like source codes, inserting malicious code or backdoors into current projects, and install, modify or delete data. Due to the importance and popularity of Visual Studio Code, it is critical that organizations deploy this patch within 24 hours before this vulnerability is weaponized and deployed."

Microsoft has been on a bug-fixing roll lately; this month marks three months in a row that Microsoft has released patches for more than 110 CVEs.

"We'll see if they maintain that pace throughout the year," said Childs.

Source: https://threatpost.com/microsoft-111-bugs-may-patch-tuesday/155669/

8. What's new in Windows Subsystem for Linux 2.0, coming soon

Windows Subsystem for Linux 2 (WSL2) is being released soon with the May 2020 Update (Windows 10 2004) and comes with new features and performance improvements.

The Windows Subsystem for Linux feature allows you to install and run Linux distributions within Windows 10.

WSL version 1 (WSL1), though, used a Linux-compatible kernel that translates Linux system calls so they could communicate and work with the Windows NT kernel. This decreased the performance and made it difficult, if not impossible, to run certain Linux applications.

In Windows 10 version 2004, Microsoft has been testing new features for Windows Subsystem for Linux, which uses in-house built Linux kernel and full system call compatibility to run more Linux apps.

Under-the-hood changes

According to Microsoft, WSL 2 includes a new architecture that changes how these Linux binaries interact with Windows and hardware. The updated WSL will still provide the same user experience as WSL 1.

Real Linux kernel

Windows 10 version 2004 introduces a real Linux kernel for Windows Subsystem for Linux that will make full system call compatibility possible.

This would be the first time a Linux kernel is shipped with Windows. The kernel is based on the source available at kernel.org and it has been specially tuned for WSL 2 with optimized size and performance.

Microsoft says it will update Linux kernel through Windows Updates, which means you don't have to manually download software or tool to patch Linux kernel with security fixes.

Microsoft says that WSL 2 uses virtualization technology to run the Linux kernel within a lightweight utility virtual machine, but it won't be a traditional VM experience with limited resources and reduced integration.

WSL 2 does not have traditional virtual machine limitations such as reduced performance and limited resources.

The new virtualization technology also promises better Windows and Linux integration, fast boot times, and it won't require VM configuration or management from your end.

WSL 2 is faster than WSL 1

In WSL 2, you will notice that file intensive operations like git clone, npm install, apt update, apt upgrade, and more would be "noticeably faster".

Microsoft claimed that WSL 2 is up to 20x faster compared to WSL 1 when unpacking a zipped tarball. Likewise, it is around 2-5x faster when using git clone, npm install and cmake.

In version 2004 of Windows 10, Linux binaries use system calls execute functions such as accessing files, requesting memory, creating processes, etc.

With its own Linux kernel support, WSL 2 has access to full system call compatibility and it offers a whole new set of apps that you can run inside the container.

These improvements make WSL 2 much more powerful for you to run Linux apps.

Other improvements

WSL also comes with a long set of other improvements and bug fixes. Here's a list of all changes and fixes in the new WSL update:

- Fix issue with handling of some Unicode characters
- Fix rare cases where distros could be unregistered if launched immediately after a build-to-build upgrade.
- Fix minor issue with wsl.exe --shutdown where instance idle timers were not cancelled.
- Improve memory performance of WSL utility VM. Memory that is no longer in use will be freed back to the host.
- Fix input relay to handle cases where stdin is a pipe handle that is not closed [GH 4424]
- Make the check for \\wsl$ case-insensitive.
- Use cache=mmap as the default for 9p mounts to fix dotnet apps
- Fixes for localhost relay [GH 4340]
- Introduce a cross-distro shared tmpfs mount for sharing state between distros
- Fix restoring persistent network drive for \\wsl$
- Update Linux kernel to 4.19.81
- Change the default permission of /dev/net/tun to 0666 [GH 4629]
- Tweak default amount of memory assigned to Linux VM to be 80% of host memory
- Fix interop server to handle requests with a timeout so bad callers cannot hang the server
- Clear the signal mask before launching the processes
- Handle creation of /etc/resolv.conf symlink when the symlink is non-relative
- Use a memory cgroup to limit the amount of memory used by install and conversion operations [GH 4669]
- Make wsl.exe present when the Windows Subsystem for Linux optional component is not enabled to improve feature discoverability.
- Change wsl.exe to print help text if the WSL optional component is not installed
- Fix race condition when creating instances
- Create wslclient.dll that contains all command line functionality
- Prevent crash during LxssManagerUser service stop
- Fix wslapi.dll fast fail when distroName parameter is NULL

Source: https://www.bleepingcomputer.com/news/microsoft/whats-new-in-windows-subsystem-for-linux-20-coming-soon/

9. The Connection Between Cloud Service Providers and Cyber Resilience

Organizations in both the private and public sectors have increasingly turned to cloud service providers (CSPs) to support their technical infrastructure, primarily to reduce IT costs and increase the efficiency of computing resources. In many cases, CSPs can also offer protection from security threats and increased cyber resilience — though customers often face trade-offs when they rely on cloud providers for these protections.

In the area of cyber resilience, in particular, organizations can offload much of the responsibility for keeping computer systems up and running by relying on cloud service providers, but this also means relinquishing much of their own control over those resilience measures.

Defining Cyber Resilience

The resilience of computer systems can mean slightly different things to different organizations. For some, it refers to maintaining a system that never goes down, while for others it refers to a system's capacity to recover from incidents and outages as quickly and painlessly as possible.

The National Institute of Standards and Technology (NIST) defines the resilience of information systems as "The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs."

The Cost of Downtime

Although the types of incidents and their consequences vary from business to business, a 2014 estimate from Gartner puts the average cost of just one minute of IT downtime at $5,600, and a 2016 Ponemon Institute report raises that estimate to nearly $9,000 per minute. The ever-increasing reliance on IT services suggests that the financial consequences of unplanned outages are continually rising.

Since IT costs and efficiency are typically primary drivers of cloud service adoption, it makes sense that reducing costs due to IT outages and interruptions might also factor into the decision.

Long-Known Advantages of Cloud Services

Cloud services can help organizations with both of the components of cyber resilience: operating continuously under adverse conditions and recovering rapidly from incidents with minimal business interruptions. CSPs typically operate infrastructure with much greater capacity than individual organizations, and they may also have significantly more resources to devote to security measures and attack prevention.

Way back in 2012, a report published by ENISA, the European Union's cybersecurity agency, determined that a cloud service provider's ability to "dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (e.g., against DDoS attacks) has obvious advantages for resilience." In other words, a denial-of-service (DoS) attack that might otherwise cause company server outages can be easily absorbed by a cloud provider's larger traffic capacity and greater ability to filter traffic.

Similarly, ransomware attacks that cut organizations off from their systems and data can be overcome with the assistance of cloud providers that produce and retain back-up copies of those systems.

Alternatively, a CSP can help customers respond to natural disasters that cut off power to servers in one region by shifting their traffic and systems to servers operated in a data center somewhere else.

A 2017 white paper titled "Advancing cyber resilience with cloud computing," published by Microsoft, makes similar arguments: "Cloud computing can be a practicable and valuable tool for cyber resilience and digital continuity," the authors assert. "Thanks to its geographic replication of data, rapid scalability, security features and cost-effectiveness, cloud enables users to increase the efficiency of their operations and their agility in response to threats."

The impressive capabilities of cloud services have changed how businesses around the world operate, but ultimately, it is up to individual organizations to determine whether these long-known advantages outweigh the possible downsides.

The Trade-Offs of Cloud Services

The downside to relying on cloud services for resilience is that it can sometimes leave customers with little control over the resilience of their own computer systems and infrastructure and can also leave them vulnerable to attacks directed at their providers — as well as any mistakes the providers might make.

As more organizations rely on the same small set of cloud service providers, the consequences of each individual outage may become greater, even if the number of outages decreases. But for many small and medium-sized businesses (SMBs) that lack dedicated security staff, the risks of a cloud provider outage still won't beat out the benefit of having the enhanced security and resilience resources that large cloud providers can offer.

The post The Connection Between Cloud Service Providers and Cyber Resilience appeared first on Security Intelligence.

Source: https://securityintelligence.com/articles/the-connection-between-cloud-service-providers-and-cyber-resilience

10. New iOS Jailbreak Tool Works on iPhone Models iOS 11 to iOS 13.5

Latest version of UnC0ver uses unpatched zero-day exploit to take complete control of devices, even those running iOS 13.5.

A hacker team has released a new method to jailbreak iPhones that they claim uses a zero-day exploit that allows them to jailbreak iPhones running iOS 11 through Apple's most recent version of its mobile operating system – iOS 13.5.

Calling it a "big milestone for jailbreaking," one of its creators, a hacker called Pwn20wnd, heralded the new jailbreak release on Twitter, claiming it's the first zero-day jailbreak for the iPhone platform since iOS 8.

Hackers did not disclose the details of the unpatched iOS flaw their tool relied on. One report on Vice Motherboard said the jailbreak takes advantage of a kernel vulnerability. No matter, the hacker team expect Apple to eventually patch the flaw which is just the "nature" of the business, Pwn20wnd said in the report.

"Even when they release a patch, users can downgrade to the previous iOS version for about two weeks usually, and after that, the users should stay on their versions so that the jailbreak keeps working," according to the hacking team's report of the jailbreak posted to the Unc0ver website. The jailbreak only works on iPhones running iOS 11 through iOS 13.5 and does not work on iOS versions 12.3 to 12.3.2 and 12.4.2 to 12.4.5.

The new jailbreak enables "unrestricted storage access to jailbreak applications for sandbox backwards compatibility," while leaving security restrictions enabled for system and user applications in place, the team said. The new tools also update Phone Rebel case models and bundled packages.

Jailbreak tools are software that take advantage of vulnerabilities in iOS to allow users sometimes full control of their device. Jailbreaking bypasses DRM restrictions, allowing users to run unauthorized and custom software as well as make other tweaks to iOS.

Apple's iOS are closed-source. The company historically has cited security reasons for not permitting its users to tinker with the proprietary code for iOS. However, jailbreaks have become popular ways for iOS developers and users to hack into their own devices to make custom changes.

"Allowing you to change what you want and operate within your purview, unc0ver unlocks the true power of your iDevice," the Unc0ver team boasted on the tool's download page.

While this may be true, jailbreaking an iPhone also creates serious security concerns, as it can make jailbreak devices susceptible to rogue or unstable apps downloaded from outside of Apple's curated App Store. While potentially the new tool's feature to leave security restrictions in place could remedy this risk, it's difficult to know at this time if that will make a difference.

Just because security researchers highly discourage the practice doesn't mean iOS developers and users will listen, given the enthusiasm with which they met the release of the new Unc0ver tool. Their interest was so keen that the download site crashed not long after the release, Vice Motherboard's Joseph Cox said on Twitter.

Developers also widely applauded the tool on the social-media platform upon Pwn20wnd's announcement of its release.

"I'd like to congratulate you man you've done great for the community for the past 3 years and today will be the biggest release of them all," developer Kaleb Davison (@drdavison5) tweeted.

Another Twitter user @IOSblaraby tweeted that the release is "a big hit for Apple," citing its ability to crack even the most recent release of iOS.

Source: https://threatpost.com/new-ios-jailbreak-tool-works-on-iphone-models-ios-11-to-ios-13-5/156045/

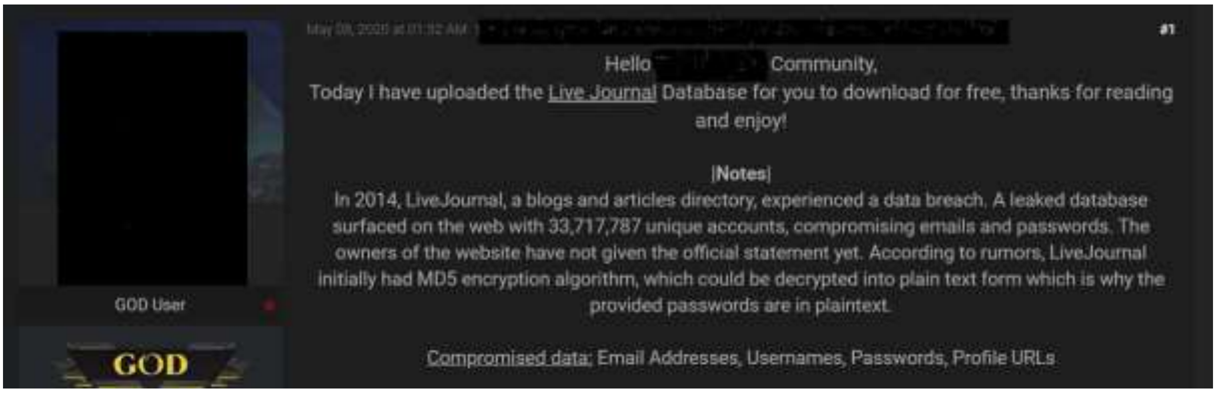
11. 26 million LiveJournal accounts being shared on hacker forums

A database containing over 26 million unique LiveJournal user accounts, including plain text passwords, is being shared for free on multiple hacker forums.

For some time, rumors have been circulating that LiveJournal was breached in 2014 and account credentials for 33 million users were stolen.

Since approximately May 8th, 2020, links to a data dump allegedly containing 33,717,787 unique accounts have been circulating on various hacker forums.

According to posts sharing the links, the database dump contains email addresses, usernames, profile URLs, and passwords. The passwords were converted to plain text after initially being stored as MD5 hashes.



[redacted]

GOD User

GOD

May 08, 2020 at 01:32 AM [redacted] #1

Hello [redacted] Community,
Today I have uploaded the Live Journal Database for you to download for free, thanks for reading and enjoy!

|Notes|
In 2014, LiveJournal, a blogs and articles directory, experienced a data breach. A leaked database surfaced on the web with 33,717,787 unique accounts, compromising emails and passwords. The owners of the website have not given the official statement yet. According to rumors, LiveJournal initially had MD5 encryption algorithm, which could be decrypted into plain text form which is why the provided passwords are in plaintext.

Compromised data: Email Addresses, Usernames, Passwords, Profile URLs

Today, numerous people have shared the alleged LiveJournal database with Troy Hunt of Have I Been Pwned, who added it to their data breach notification service.

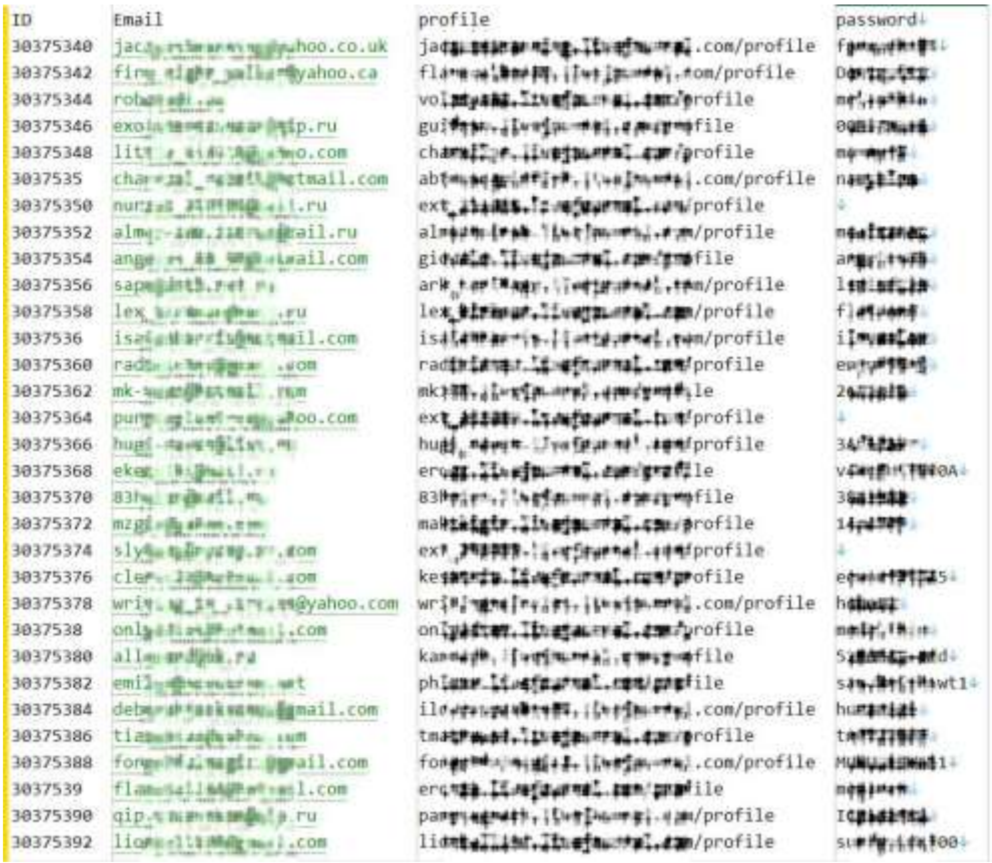
Hunt has told BleepingComputer that it appears to be the same data breach that was discussed last year.

Instead of classifying the data breach as being from 2014, though, Hunt is stating it is from 2017 based on the data dump's file name of 'LiveJournal_com_2017_33.7M.txt.'

"There's contradictory info: the Forum post says 2014 but then the file I sent you a screen cap of says 2017. There's no time stamps in the file to make it any clearer but the earliest evidence I have (based on community feedback) is 2018."

"I generally err on the side of the later date otherwise you end up with people saying "I didn't create an account until 2016 and I'm in there so you have the date wrong"," Hunt told BleepingComputer.

BleepingComputer was able to find links to the circulating database within five minutes of talking to Hunt.



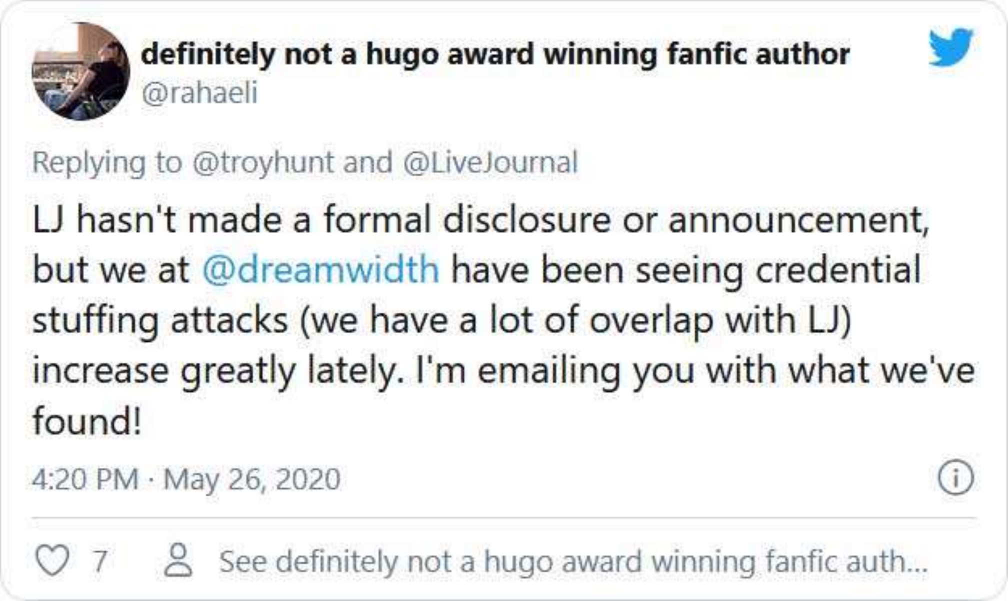
ID	Email	profile	password
30375340	jac[redacted]hoo.co.uk	ja[redacted].com/profile	f[redacted]
30375342	fir[redacted]yahoo.ca	fla[redacted]om/profile	D[redacted]
30375344	rob[redacted]	vo[redacted]profile	m[redacted]
30375346	exo[redacted]p.ru	gui[redacted]file	0[redacted]
30375348	lit[redacted]o.com	cha[redacted]profile	[redacted]
3037535	cha[redacted]tmail.com	ab[redacted].com/profile	n[redacted]
30375350	nur[redacted].ru	ext[redacted]/profile	
30375352	alm[redacted]ail.ru	al[redacted]/profile	[redacted]
30375354	ange[redacted]ail.com	gi[redacted]file	a[redacted]
30375356	sap[redacted]	ark[redacted]/profile	1[redacted]
30375358	lex[redacted].ru	lex[redacted]/profile	f[redacted]
3037536	is[redacted]ail.com	is[redacted]/profile	i[redacted]
30375360	rad[redacted]om	rad[redacted]profile	e[redacted]
30375362	mk-[redacted]	mk[redacted]le	2[redacted]
30375364	pur[redacted]hoo.com	ext[redacted]profile	
30375366	hug[redacted]	hu[redacted]profile	34[redacted]
30375368	eke[redacted]	er[redacted]le	v[redacted]0A
30375370	83h[redacted]	83[redacted]file	3[redacted]
30375372	mzg[redacted]	ma[redacted]profile	14[redacted]
30375374	sly[redacted]om	ex[redacted]profile	
30375376	cle[redacted]om	ke[redacted]ofile	e[redacted]5
30375378	wri[redacted]@yahoo.com	wr[redacted].com/profile	h[redacted]
3037538	onl[redacted].com	on[redacted]rofile	[redacted]
30375380	all[redacted]	ka[redacted]file	5[redacted]d
30375382	emi[redacted]	ph[redacted]file	s[redacted]wt1
30375384	deb[redacted]mail.com	il[redacted].com/profile	hu[redacted]
30375386	ti[redacted]	tm[redacted]profile	t[redacted]
30375388	for[redacted]ail.com	fo[redacted].com/profile	M[redacted]1
3037539	fl[redacted]l.com	er[redacted]ile	[redacted]
30375390	qip[redacted].ru	pa[redacted]/profile	I[redacted]
30375392	lio[redacted].com	li[redacted]/profile	s[redacted]00

Sample of alleged LiveJournal database

BleepingComputer has since been able to independently confirm with a few people that information for old accounts was accurately included in the database.

LiveJournal has denied being compromised

Denise Paolucci replied to Hunt's tweet today, stating that her company Dreamwidth Studios has been dealing with credential stuffing attacks that overlap with the credentials in the LiveJournal database.



definitely not a hugo award winning fanfic author
@rahaeli

Replying to @troyhunt and @LiveJournal

LJ hasn't made a formal disclosure or announcement, but we at @dreamwidth have been seeing credential stuffing attacks (we have a lot of overlap with LJ) increase greatly lately. I'm emailing you with what we've found!

4:20 PM · May 26, 2020

Paolucci shared links to Dreamwidth maintenance bulletins with BleepingComputer from 2017 and 2018 that indicate that credentials from this LiveJournal database were used in credential stuffing attacks.

In the 2017 maintenance bulletin, two customers referenced that their accounts at LiveJournal had been compromised.

"LiveJournal refugees should be especially careful not to reuse their passwords from there. A large number of people I know, including myself, got "Caught you on camera watching porn" spam, giving our old LiveJournal passwords as "evidence." In its earlier days, LJ must have been very sloppy about protecting user passwords," a customer posted.

"Let me be scrupulously careful here in how I phrase this: There are files ("dumps") on the black market that claim to be from a LiveJournal breach in 2014, and I've never seen anyone who was listed in the dumps say that their information was incorrect (and have seen many who have said it was)," Paolucci responded.

To this day, LiveJournal has never confirmed that a data breach has occurred or that the database is legitimate.

BleepingComputer has emailed LiveJournal about the circulating database but has not heard back at this time.

What should LiveJournal users do?

Hunt has added the database to the Have I Been Pwned data breach notification service, and users can use it to confirm if their email address is part of the database.

If the service shows that your email address was included, you should immediately change your passwords on LiveJournal to be safe.

This database is potentially six years old, so it hoped that users would have changed their password over the years, but to be safe, do so again.

If you use the same password at other sites, be sure to switch to a unique and complex password at these other sites.

Source: https://www.bleepingcomputer.com/news/security/26-million-livejournal-accounts-being-shared-on-hacker-forums/

12. Thermal Imaging as Security Theater

Seems like thermal imaging is the security theater technology of today.

These features are so tempting that thermal cameras are being installed at an increasing pace. They're used in airports and other public transportation centers to screen travelers, increasingly used by companies to screen employees and by businesses to screen customers, and even used in health care facilities to screen patients. Despite their prevalence, thermal cameras have many fatal limitations when used to screen for the coronavirus.

- They are not intended for distance from the people being inspected.
- They are "an imprecise method for scanning crowds" now put into a context where precision is critical.
- They will create false positives, leaving people stigmatized, harassed, unfairly quarantined, and denied rightful opportunities to work, travel, shop, or seek medical help.
- They will create false negatives, which, perhaps most significantly for public health purposes, "could miss many of the up to one-quarter or more people infected with the virus who do not exhibit symptoms," as the *New York Times recently put it*. Thus they will abjectly fail at the core task of slowing or preventing the further spread of the virus.

Source: https://www.schneier.com/blog/archives/2020/05/thermal_imaging.html

If you want to learn more about ASOC and how we can improve your security posture, contact us at: **tbs.sales@telelink.com**

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.