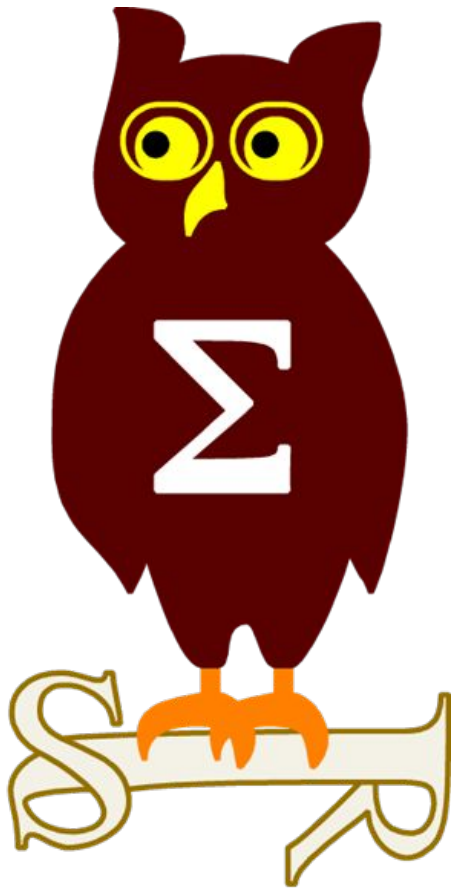


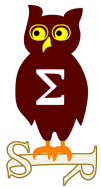
Revue d'actualité

09/10/2018



Préparée par

Étienne Baudin @etiennebaudin
Arnaud SOULLIE @arnaudsoullie
Vladi mir KOLLA @mynameisv__



Failles / Bulletins / Advisories

Pas de de bulletin de mois-ci, par manque de temps



La version non retraitée manuellement :

<https://pastebin.com/H5b2jnRY>

Faillies / Bulletins / Advisories

Microsoft - Autre

Windows 10, mise à jour d'octobre

- Plusieurs erreurs dont la suppression des données des répertoires documents, images, musique...
- Perte de l'accès internet
- Microsoft stoppe le déploiement de la mise à jour

<https://www.nextinpact.com/news/107145-windows-10-problemes-saccumulent-microsoft-bloque-october-2018-update.htm>

Azure Active Directory, suppression totale du mot de passe

- Authentification par l'application mobile et un code PIN

<https://www.clubic.com/telecharger/Microsoft/actualite-845692-applications-ligne-microsoft-utilisant-azure-mot.html>

Failles / Bulletins / Advisories

Système (principales failles)

Git

- prise de contrôle d'un système à distance (CVE-2018-17456)
- défaut de contrôle des URL commençant par le caractère '-' lors de l'utilisation de sous-modules git avec la commande récursive "git clone"

<https://seclists.org/oss-sec/2018/q4/19>

Firefox / Thunderbird

- Corrections de diverses vulnérabilités dont 3 critiques :
 - une corruption mémoire pouvant permettre l'exécution de code arbitraire ;
 - une confusion de type lors de l'allocation d'un registre en JavaScript ;
 - Fuite mémoire au sein du compilateur JIT

<https://www.mozilla.org/en-US/security/advisories/mfsa2018-25/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2018-24/>

Vulnérabilité dans Prim'X Zed!

- Création de fichier arbitraire à l'ouverture d'un conteneur chiffré

<https://primx.eu/support-1859972.aspx>

Failles / Bulletins / Advisories

Système (principales failles)

Dell Digital Delivery, Élévation locale de privilèges (CVE-2018-11072)

- L'outil tourne en SYSTEM
- Un outil user-land (fourni) peut communiquer avec permet l'injection de librairie

<http://hatriot.github.io/blog/2018/08/22/dell-digital-delivery-eop/>

Adobe, près de 50 correctifs de sécurité sur Acrobat Reader

<https://helpx.adobe.com/security/products/acrobat/apsb18-30.html>

Failles / Bulletins / Advisories

Réseau (principales failles)

Cisco

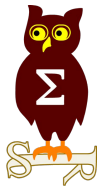
- 24 vulnérabilités corrigées en septembre, 4 critiques:
 - Cisco IOS XE Software Static Credential Vulnerability
 - Cisco Video Surveillance Manager Appliance Default Password Vulnerability
 - Cisco Identity Services Engine Unauthorized Access Vulnerability
 - Multiple Vulnerabilities in Cisco Identity Services Engine

- 36 vulnérabilités corrigées en octobre, 3 critiques :
 - Prime Infrastructure Arbitrary File Upload and Command Execution
 - 2x Digital Network Architecture Center Authentication Bypass Vulnerability

<https://tools.cisco.com/security/center/publicationListing.x>

iOS

- 1 vulnérabilité découverte à la sortie d'iOS 12
 - permet d'accéder au répertoire et photos via VoiceOver lorsque le téléphone est verrouillé
- <https://securityaffairs.co/wordpress/76700/hacking/iphone-xs-passcode-hack.html>



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des attaques par phishing utilisant les services de Cloudflare et Microsoft observées

- Utilisés afin de disposer d'un certificat valide et trusté pour rendre le site malveillant plus crédible
- Blob Azure et Cloudflare IPFS

<https://www.bleepingcomputer.com/news/security/phishing-attack-uses-azure-blob-storage-to-impersonate-microsoft/>

<https://www.bleepingcomputer.com/news/security/phishing-attacks-distributed-through-cloudflares-ipfs-gateway/>

Plus de 100 000 appareils infectés par le malware GhostDNS

- campagne en cours depuis le 21 septembre
- détourne les routeurs domestiques pour dérober des données sensibles via différents modules
- majoritairement au Brésil

<https://securityaffairs.co/wordpress/76727/malware/ghostdns-malware-campaign.html>

Piratages, Malwares, spam, fraudes et DDoS

Fuite de données

Un bug exposait les messages de millions d'utilisateurs Twitter

- dû à l'API "Account Activity"
- <1% des utilisateurs impactés soit 3 millions

<https://www.securityweek.com/millions-twitter-users-affected-information-exposure-flaw>

90 millions d'utilisateurs touchés par la vulnérabilité sur Facebook

- dû à la fonctionnalité "Aperçu en tant que"
- 5 millions d'européens
- 1,6 Md\$ d'amende max via RGPD

<https://newsroom.fb.com/news/2018/09/security-update/>

Une vulnérabilité sur les équipements MyCloud de Western Digital permet l'authentification en administrateur avec un cookie 'Cookie: username=admin'

- WD informé en avril 2017

https://www.theregister.co.uk/2018/09/18/remote_access_vulnerability_western_digital_my_cloud/



Piratages, Malwares, spam, fraudes et DDoS

Fuite de données

Les informations de cartes bancaires de clients Newegg exposées depuis un mois par le groupe Magecart

- enregistrement du domaine "neweggstats.com", le 13 août 2018 puis collection de données des cartes de crédit dérobées depuis le site de Newegg lors de l'étape de paiement

<https://www.bleepingcomputer.com/news/security/newegg-credit-card-info-stolen-for-a-month-by-injected-magecart-script/>

La société Veeam expose 200 Gb de données clients via une mauvaise configuration d'un serveur AWS

- identifié par un chercheur via Shodan
- pas de mot de passe, pas de chiffrement
- adresses email, de noms et dans certains cas d'adresses IP collectées entre 2013 et 2017

https://www.theregister-co-uk.cdn.ampproject.org/c/s/www.theregister.co.uk/AMP/2018/09/12/veeam_database_config_snafu_expose_d_millions_email_addresses/

11 millions de dossiers personnels découverts sur une base MongoDB non protégée

- 43,5 Go de données personnelles utilisées dans des campagnes marketing
- identifié par Shodan, serait originaire du site SaverSpy associé à Coupons.com
- base de données déjà compromise, contient des traces de demandes de rançon

<https://www.hackread.com/personal-unprotected-mongodb-records-leaked-online/>

Piratages, Malwares, spam, fraudes et DDoS

Fuite de données

Google, fuite potentielle de données pour 500k utilisateurs de Google+

- Google quoi !!?
- Google arrête le service
- Mais ne communique pas sur la fuite probable (et GDPR !!?)

<https://www.reuters.com/article/us-google-data/google-exposed-user-data-chose-not-to-tell-public-wsj-idUSKCN1MI1WM>

Piratages, Malwares, spam, fraudes et DDoS

Malware

LoJax, un rootkit UEFI trouvé dans la nature

- Exploite une vulnérabilité (corrigée)
- S'injecte dans l'UEFI à l'aide d'un pilote légitime
- Ajoute un implant grâce à un pilote NTFS
- Semble lié à une agence étatique russe (groupe Sednit / APT28 / Fancy Bear)

<https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/>

Le vers Viro qui se transmet par mail

- Comme dans les années 2000
- Fait des appels COM à Outlook et s'envoie aux contacts
 - Chiffre les fichiers, active un enregistreur de touches (keylogger), se connecte au C&C

<https://blog.trendmicro.com/trendlabs-security-intelligence/virobot-ransomware-with-botnet-capability-breaks-through/>

Piratages, Malwares, spam, fraudes et DDoS

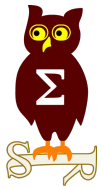
Espionnage

Les services hollandais doxxent des agent du GRU

- C'est le retour des pieds nickelés de l'espionnage (cf. CIA/Italie en 2013)
<https://twitter.com/annaholligan/status/1047792339564081153>

Une puce électronique malveillante incorporée dans des serveurs utilisés par des entreprises et des institutions américaines

- Puce de la taille d'un grain de riz découvert sur la carte mère de serveurs Super Micro
- Disposerait de sa propre mémoire et accès réseau
- Apple et Amazon auraient découverts la puce et contactés les autorités
- Sujet très rapidement démenti par :
 - Le CISO de Amazon ;
 - Apple via une lettre au Congrès
<https://www.bloomberg.com/news/videos/2018-10-04/how-china-used-a-tiny-chip-to-infiltrate-amazon-and-apple-video>
<https://arstechnica.com/tech-policy/2018/10/apple-attacks-bloomberg-spy-chip-story-in-letter-to-congress/>
- L'action Super Micro s'est effondrée de 60% à la Bourse de New York



Nouveautés, outils et techniques

Nouvelle version du WiFi

- 802.11ax => WiFi 6
- 802.11ac => WiFi 5
- 802.11n => WiFi 4

<https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-6>

Microsoft propose une alternative aux mots de passe sur les applications Office365

- possibilité de se connecter aux applications Azure AD uniquement via l'application Authenticator
- les connexions se feront en entrant un nom d'utilisateur et en approuvant une notification qui apparaît sur l'application Authenticator.
- La connexion est ensuite confirmée par le lecteur d'empreintes digitales, la reconnaissance faciale ou encore un code PIN sur le smartphone

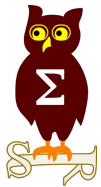
<https://nakedsecurity.sophos.com/2018/09/26/microsoft-is-killing-passwords-one-announcement-at-a-time/>

Vincent LE TOUX publie le code source de PingCastel

- Licence OSL

<https://github.com/vletoux/pingcastle>

<https://twitter.com/mysmartlogon/status/1047121216853688320>



Business et Politique

L'ANSSI publie le code de CLIP OS

- Cloisonnement Kernel et non hyperviseur
- Basé sur Gentoo !!?

<https://www.ssi.gouv.fr/en/actualite/clip-os-open-source-secured-operating-system/>

Un agent de la DGSI arrêté pour avoir vendu des informations confidentielles sur le darkweb

- Confondu grâce à son code personnel utilisé pour l'identification sur son ordinateur

<http://www.leparisien.fr/faits-divers/l-agent-de-la-dgsi-vendait-des-informations-pour-300-euros-on-pouvait-voler-une-vie-complete-01-10-2018-7908552.php>

Association ALLIANCE FRANCAISE PARIS ÎLE-DE-FRANCE condamnée par la CNIL

- Sanction de 30.000 euros
- Données personnelles aisément accessible en modifiant l'url

<https://www.cnil.fr/fr/alliance-francaise-paris-ile-de-france-sanction-de-30000eu-pour-une-atteinte-la-securite-des-donnees>

Uber va devoir déboursier 148 millions de dollars pour avoir caché une atteinte à la protection de ses données en 2016

- 600 000 conducteurs nord-américains et 57 millions de clients à travers le monde touchés
<https://thenextweb.com/security/2018/09/27/uber-148-million-fine-2016-data-breach/>

Google connecte discrètement les utilisateurs à Chrome à chaque visite d'un site appartenant à Google

- retour en arrière après la polémique
<https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome/>

Un employé d'Amazon licencié pour avoir partagé les adresses email de clients

- utilisé par des vendeurs pour proposer de revenir en arrière sur des mauvaises notes contre rémunération ou cadeaux
<https://www.zdnet.com/article/amazon-fires-employee-for-sharing-customers-email-addresses/>

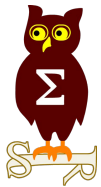
Un PDG plaide coupable dans une affaire où il est accusé d'avoir vendu des téléphones modifiés à des cartels de la drogue

- Blackberry modifiés (retrait de l'appareil photo, des microphones du GPS, etc.)
- Il risque 20 ans de prison
https://www.theregister.co.uk/2018/10/03/phone_ceo_pleads_guilty/

Jérémie Zimmermann quitte la Quadrature du Net

- Trop d'administratif, de gestion, de politique interne

<https://www.nextinpact.com/news/107107-jeremie-zimmermann-quitte-quadrature-net.htm>



Conférences

Conférences

Passées

- SSTIC - 13 au 15 juin 2018
- Pass the Salt - 2 au 4 juillet 2018

A venir

- BlackHat - 4 au 9 août 2018
- BSides LasVegas - 7 & 8 août 2018
- DEFCON - 9 au 12 août 2018



Divers / Trolls velus

Mieux qu'InfauxSec News : Sputnik News

- <<Rien n'empêche à penser que les "érodés", ces fameuses failles informatiques, utilisées par les pirates initiés, existent>>
<https://fr.sputniknews.com/france/201703081030371219-france-vote-electronique-opinion/>
<https://web.archive.org/web/20170308103413/https://fr.sputniknews.com/france/201703081030371219-france-vote-electronique-opinion/>

HTTPCS financerait des mosquées salafistes avec l'argent des saoudiens

- Mohamed Boumediene entré récemment dans le capital d'une société saoudienne
http://www.lagglorieuse.info/article_main-basse-sur-la-mosqu-e-de-la-paillade.html

Divers / Trolls velus

De participants de Botconf ciblés par un Scam

- Appel téléphonique d'un représentant de "Business Travel Management"
- Demande du numéro de CB ou de faire un paiement par virement
 - Avec un remboursement de 600€ par la conférence

DocuSign Envelope ID: 89C683EB-3469-4705-A188-9E1CED72A93E

BTM
Business Travel Management

Business Travel Management
Am Stationsgarten 45,
42327 Wuppertal,
Germany
UK: +44 0203-286-1516
GER: +49 202-2586-0977
USA: +1 786-724-0414
E-mail: support@btravelmanagement.com
Web: www.btravelmanagement.com

HOTEL BOOKING FORM

Credit Card Authorization Form for accommodation

We are delighted that you have selected Business Travel Management ("B.T.M") to provide your pre-paid room accommodation reservations. Please fill out this form completely and ("B.T.M") will process all relevant room reservations agreed upon and the relevant charges for those rooms.

HOTEL NAME:	La Quietat Hotel	PRICE PER NIGHT:	119 EUR
CARDHOLDER INFORMATION	TOTAL ROOMS: 1	TOTAL NIGHTS:	5
Authorized Contact:			
Name as it appears on Credit Card:			
Card type:	MasterCard <input type="radio"/>	Visa <input type="radio"/>	Amex <input type="radio"/>
Card Number:		Discover <input type="radio"/>	CIVV: <input type="text"/>
Billing Address:		Expiry date:	
City:		State:	
		Zip Code:	
		Country:	

Terms and Conditions: By signing, I agree to the Terms and Conditions and Cancellation Policy listed herein, as well as any Agreement of Hotel Reservation Services previously agreed upon or to be agreed upon. I certify that all information herein is complete and accurate and I hereby authorize ("B.T.M") to collect all payment for all charges relevant to room charges, service fees, and taxes as outlined in this Authorization Form, and any other agreements and communications for room accommodation reservations, which amounts have been previously agreed upon or are to be agreed upon, to the credit card listed herein. I further authorize ("B.T.M") to charge the credit card listed herein multiple times, if necessary, to satisfy the entire balance due. I certify that, I am authorized to sign for the referenced credit card. *The price per night exclusive of any taxes, hotel surcharges, and other applicable service fees.

Cardholder's Signature: Date: 9/24/2018 4: 04: 37 AM PDT

Terms and Conditions of Service and Cancellation Policy:
("B.T.M") is providing Hotel Room Reservation and Booking Service for you and your company. ("B.T.M") provides such competitive room rates and service pricing due to its ability to reserve, hold and pre-pay for rooms for its clients at the time of reservation. Business Travel Management ("B.T.M") is a privately-owned company, not affiliated with any event or other organization, and will be providing you and/or your business with hotel accommodation reservation and booking services. Final agreed upon room accommodations will be emailed to you within 7 business days of initial booking. In order to change your room accommodation reservations or your room bookings, email support@btravelmanagement.com while there is no guarantee that ("B.T.M") will be able to accommodate the requested changes. ("B.T.M") will take every effort to adjust, change and seek our customers utmost satisfaction.
*Disclaimer's Taxes and service fees will be added to your bill. ("B.T.M") understands that sometimes plans change. However, as mentioned, ("B.T.M") is able to offer such competitive pricing due to its ability to reserve, hold and pre-pay for rooms for its clients at the time of reservation. Thus, changes made after final accommodation is agreed upon, but prior to 20 days before check in will not be assessed a fee. ("B.T.M") will use its best efforts to accommodate these requests, but ("B.T.M") does not guarantee that such modifications or partial cancellations can be made, or that they can be made at the original contracted price. Refunds due to Partial cancellation will be excluded from the final invoice or refunded within 15 business days. We require 25% as a deposit at the time of the booking and the balance due will be charged 30 days prior to check in. Changes made after 14 days prior to check-in will be subject to 1 right as amendment fees per each change made, plus any fees or taxes charged by the hotel. Reservations must be cancelled in writing to support@btravelmanagement.com. In addition, should the entire reservation be cancelled you agree to pay a cancellation fee in the amount of 25% of the total cost of room accommodation. This cancellation fee reflects the ("B.T.M") services already performed on your behalf, monies already paid on your behalf and monies earned by ("B.T.M") for services deemed performed. ("B.T.M") reserves the right to waive this cancellation fee at any time, at its sole discretion on a case by case basis. ("B.T.M") accepts no charge requests after 72 hours prior to check-in. ("B.T.M") does not provide refunds for

Divers / Trolls velus

Mounir Mahjoubi vous recommande de faire une analyse de risque

- Mails il ne précise pas si c'est de l'EBIOS



Mounir Mahjoubi ✓
@mounir

Follow



Avec cette nouvelle annonce d'une faille de #sécurité chez @Google, j'invite chaque Français à regarder quelles #donneespersonnelles @facebook et @Google possèdent sur eux et à évaluer leur risque !

▶ Facebook : facebook.com/help/170173069

▶ Google : takeout.google.com/?pli=1

12:00 PM - 8 Oct 2018

<https://twitter.com/mounir/status/1049374022214008832?s=11>

Grosse panne chez Cisco WebEx

- En cause, un script qui a effacé toutes les machine virtuelles

https://www.theregister.co.uk/2018/10/03/cisco_webex_outage_script/


Divers / Trolls velus

Ca chauffe entre NSS Labs et les éditeurs d'antivirus

- NSS Labs a engagé une procédure antitrust contre CrowdStrike, Symantec, ESET et la Anti-Malware Testing Standards Organization (AMTSO)
- Ces vendeurs boycottent à plusieurs NSS Labs pour éviter les comparaisons
 - Ou imposent dans leur licence un accord pour être testé

<https://www.nsslabs.com/blog/company/advancing-transparency-and-accountability-in-the-cybersecurity-industry/>

Les best practices BGP... par la NSA

- Il faut monter des sessions BGP avec leur "route collector" 
- Leur faites-vous confiance ?
- Et le certificat est auto-signé

<https://www.iad.gov/iad/library/reports/a-guide-to-border-gateway-protocol-bgp-best-practices.cfm>





Prochains rendez-vous de l'OSSIR

Prochaine réunion

- Mardi 13 novembre 2018

After Work

- ???

Des questions ?

- C'est le moment !



Des idées d'illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous