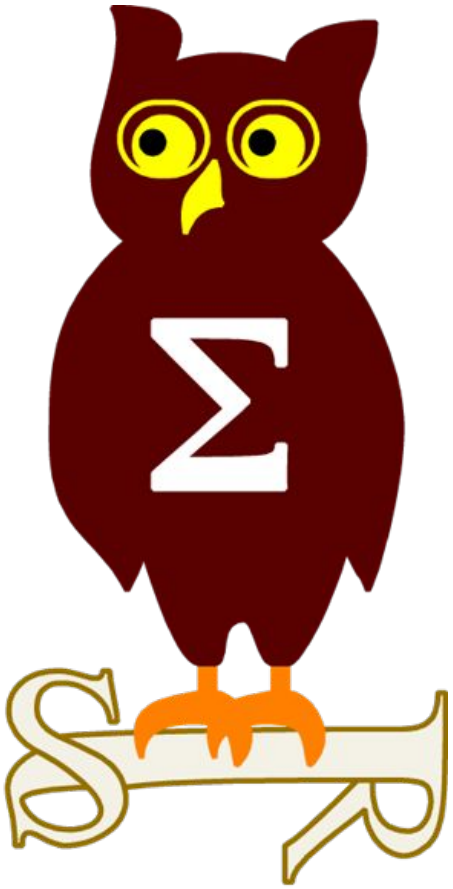
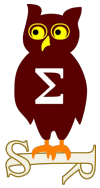


Revue d'actualité

14/05/2019

Préparée par

*Étienne **B**audin @etiennebaudin*
*Arnaud **S**OULLIE @arnaudsoullie*



Failles / Bulletins / Advisories

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-037 Vulnérabilités dans Internet Explorer (5 CVE)

- Exploit:
  - 1 x Manipulation de données
  - 3 x Exécution de code à distance
  - 1 x Vol d'informations
- Crédits:
  - Rio Sherri of MDSec (CVE-2019-0764)
  - HexKitchen of Trend Micro's Zero Day Initiative (CVE-2019-0752)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0753, CVE-2019-0835, CVE-2019-0862)

MS19-038 Vulnérabilités dans Edge (9 CVE)

- Exploit:
  - 1 x Vol d'informations
  - 7 x Exécution de code à distance
  - 1 x Manipulation de données
- Crédits:
  - Karel Kahula and Spencer Guest (CVE-2019-0833)
  - MoonLiang of Tencent Security Xuanwu Lab (CVE-2019-0739)
  - Rio Sherri of MDSec (CVE-2019-0764)
  - Bruno Keith (CVE-2019-0812)
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0829)
  - Qixun Zhao of Qihoo 360 Vulcan Team (CVE-2019-0806, CVE-2019-0810, CVE-2019-0861)
  - Suyoung Lee of Web Security & Privacy Lab in KAIST
  - HyungSeok Han of SoftSec Lab in KAIST
  - Sang Kil Cha of SoftSec Lab in KAIST
  - Sooel Son of Web Security & Privacy Lab in KAIST (CVE-2019-0860)

Dont 1 commune avec IE:

- CVE-2019-0764

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-039 Vulnérabilités dans Microsoft XML (5 CVE)

- Affectés : Toutes versions
- Exploit:
  - 5 x Exécution de code à distance
- Crédits:
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795)

MS19-040 Vulnérabilités dans Microsoft Windows (18 CVE)

- Affectés : Toutes versions
- Exploit:
  - 3 x Exécution de code à distance
  - 7 x Élévation de privilèges
  - 7 x Vol d'informations
  - 1 x Contournement de restrictions de sécurité
- Crédits:
  - Yuki Chen of Qihoo 360 Vulcan Team (CVE-2019-0794, CVE-2019-0842)
  - James Forshaw of Google Project Zero (CVE-2019-0805, CVE-2019-0730, CVE-2019-0731, CVE-2019-0732, CVE-2019-0796, CVE-2019-0836)
  - Tristan Bennett of Seamless Intelligence (CVE-2019-0838)
  - ? (CVE-2019-0839)
  - JunGu and ZiMi of Alibaba Orion Security Lab (CVE-2019-0840)
  - Wenxu Wu (@ma7h1as) of Tencent Security Xuanwu Lab (CVE-2019-0841)
  - Yaniv Frank of SophosLabs (CVE-2019-0845)
  - Michael James Loftus (CVE-2019-0848)
  - Jaewon Min (@binerdd) (CVE-2019-0685)
  - Amit Klein and Benny Pinkas of Bar Ilan University (CVE-2019-0688)
  - zhong_sf of Qihoo 360 Vulcan Team (CVE-2019-0814)
  - RanchoIce of Tencent ZhanluLab (CVE-2019-0837)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-041 Vulnérabilités dans Microsoft Graphics (4 CVE)

- Affectés : Toutes versions
- Exploit:
  - 2 x Vol d'informations
  - 1 x Élévation de privilèges
  - 1 x Exécution de code à distance
- Crédits:
  - riusksk of VulWar Corp (CVE-2019-0802, CVE-2019-0849)
  - Donghai Zhu of Alibaba Cloud Intelligence Security Team (CVE-2019-0803)
  - Hossein Lotfi working Trend Micro's Zero Day Initiative (CVE-2019-0853)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-043 Vulnérabilités dans .NET Core (1 CVE)

- Exploit:
  - 1 x Déni de service
- Crédits:
  - Giorgi Dalakishvili of the Bank of Georgia (CVE-2019-0815)

MS19-044 Vulnérabilités dans Microsoft Office (8 CVE)

- Exploit:
  - 7 x Exécution de code à distance
  - 1 x Élévation de privilèges
- Crédits:
  - Jaanus Kääp of Clarified Security (CVE-2019-0822, CVE-2019-0828)
  - Gal De Leon and Bar Lahav of Palo Alto Networks (CVE-2019-0823, CVE-2019-0824)
  - Honggang Ren of Fortinet's FortiGuard Labs (CVE-2019-0825)
  - rgod of 9sg Security Team - rgod@9sgsec.com working Trend Micro's Zero Day Initiative (CVE-2019-0826, CVE-2019-0827)
  - rgod working Trend Micro's Zero Day Initiative (CVE-2019-0801)

MS19-045 Vulnérabilités dans Office SharePoint (2 CVE)

- Exploit:
  - 2 x Vol de session
- Crédits:
  - Huynh Phuoc Hung, @hph0var (CVE-2019-0830, CVE-2019-0831)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-046 Vulnérabilités dans Windows Kernel (3 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Vol d'informations
  - 1 x Exécution de code à distance
  - 1 x Élévation de privilèges
- Crédits:
  - Huynh Phuoc Hung, @hph0var (CVE-2019-0830, CVE-2019-0831)
  - JunGu and ZiMi of Alibaba Orion Security Lab (CVE-2019-0844)
  - Australian Cyber Security Centre - Australian Signals Directorate (CVE-2019-0856)
  - (Vasily Berdnikov) of Kaspersky Lab
  - (Boris Larin) of Kaspersky Lab (CVE-2019-0859)

MS19-047 Vulnérabilités dans Microsoft JET Database Engine (5 CVE)

- Affectés : Toutes versions
- Exploit:
  - 5 x Exécution de code à distance
- Crédits:
  - Gal De Leon and Bar Lahav of Palo Alto Networks (CVE-2019-0846, CVE-2019-0847)
  - Honggang Ren of Fortinet's FortiGuard Labs (CVE-2019-0851, CVE-2019-0877)
  - Hardik Shah of McAfee (CVE-2019-0879)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-048 Vulnérabilités dans Microsoft Exchange Server (2 CVE)

- Exploit:
  - 2 x Vol de session
- Crédits:
  - Cameron Vincent (CVE-2019-0858)
  - Ashar Javed of Hyundai AutoEver Europe GmbH (CVE-2019-0817)

MS19-049 Vulnérabilités dans CSRSS (1 CVE)

- Affectés : Toutes versions
- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - James Forshaw of Google Project Zero (CVE-2019-0735)

MS19-050 Vulnérabilités dans Windows Hyper-V (1 CVE)

- Affectés : Windows 10, Windows Server 2019, Windows Server, version 1709 / 1803
- Exploit:
  - 1 x Exécution de code à distance
- Crédits:
  - ? (CVE-2019-0786)

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Avis

MS19-051 Vulnérabilités dans Windows Admin Center (1 CVE)

- Exploit:
  - 1 x Élévation de privilèges
- Crédits:
  - ? (CVE-2019-0813)

MS19-052 Vulnérabilités dans Open Source Software (1 CVE)

- Affectés : Open Enclave SDK
- Exploit:
  - 1 x Vol d'informations
- Crédits:
  - Eduard Marin (The University of Birmingham, UK) (CVE-2019-0876)

Failles / Bulletins / Advisories

Microsoft - Advisories

Mise à jour pour Windows XP Embedded POSReady

- Windows XP Embedded Service Pack 3 (SP3) fin de support en **janvier 2016**
- Windows Embedded POSReady 2009 fin de support en **avril 2019**

Failles / Bulletins / Advisories

Microsoft - Autre

1 exploit pour Microsoft Powershell ISE

- Prise de contrôle du système via l'exécution d'un fichier malveillant

  http://hyp3rlinx.altervista.org/advisories/WINDOWS-POWERSHELL-ISE-FILENAME-PARSING-FLAW-RCE-0DAY.txt

2 exploits pour Microsoft Windows

- Élévation de privilèges via l'exécution d'un .exe malveillant
- Prise de contrôle d'un système via l'ouverture d'un fichier de contact malveillant

  https://github.com/rogue-kdc/CVE-2019-0841/

1 exploit pour IE 11

- vol et manipulation de données via l'exécution d'un fichier malveillant

http://hyp3rlinx.altervista.org/advisories/MICROSOFT-INTERNET-EXPLORER-v11-XML-EXTERNAL-ENTITY-INJECTION-0DAY.txt

Failles / Bulletins / Advisories

Système (principales failles)

Élévation de privilèges locale via une vulnérabilité dans Apache HTTP Server

- code d'exploitation disponible

  https://www.exploit-db.com/exploits/46676

Prise de contrôle du système via une vulnérabilité au sein de Tomcat

- Erreur dans la manière dont JRE transmettait les arguments de ligne de commande à Windows
- code d'exploitation disponible

  http://tomcat.apache.org/security-9.html
  http://tomcat.apache.org/security-7.html
  http://tomcat.apache.org/security-8.html

Prise de contrôle du système via une vulnérabilité au sein de SQLite3

- via une requête SQL causant un accès mémoire après libération

  https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0777

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle du système et contournement de restrictions de sécurité via 5 vulnérabilités au sein de Symfony

- manque de filtrage sur la méthode HTTP X-Http-Method-Override
- absence de contrôle sur l'entrée utilisateur utilisé pour générer le Service ID
- manque de contrôle sur les objets pouvant être sérialisé
- erreur au sein du cookie de session
- manque de contrôles sur les messages de validation du thème formulaire du moteur de template PHP

https://symfony.com/blog/cve-2019-10913-reject-invalid-http-method-overrides
https://symfony.com/blog/cve-2019-10910-check-service-ids-are-valid
https://symfony.com/blog/cve-2019-10912-prevent-destructors-with-side-effects-from-being-unserialized
https://symfony.com/blog/cve-2019-10911-add-a-separator-in-the-remember-me-cookie-hash
https://symfony.com/blog/cve-2019-10909-escape-validation-messages-in-the-php-templating-engine

Prise de contrôle du système et contournement de sécurité via 41 vulnérabilités au sein de Google Chrome

- via l'ouverture d'une page web ou d'un fichier PDF

https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_23.html

Élévation de privilèges via une vulnérabilité au sein de macOS

- code d'exploitation disponible (via l'exécution d'un fichier spécifique)

https://github.com/ChiChou/sploits/tree/master/CVE-2019-8513

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle d'un système via une vulnérabilité au sein de PostgreSQL

- code d’exploitation Metasploit disponible
- pas de correctif disponible
- exploitation permet à des superutilisateurs ou utilisateurs du groupe pg_read_server_files d’exécuter du code arbitraire dans le contexte de l’utilisateur système de la base de données

https://www.postgresql.org/about/news/1935/

Failles / Bulletins / Advisories

Système (principales failles)

Patch Oracle

- 297 vulnérabilités dans 53 produits :
  - 5 vulnérabilités dans Java ;
  - 43 dans MySQL ;
  - 6 dans Database ;
  - 15 dans Oracle VM ;
  - 44 dans Oracle Fusion Middleware (1 exploit publié le 19/04)

https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

Prise de contrôle du système à distance via une vulnérabilité au sein d'Oracle WebLogic

- 0day publiée le 21/04 pour une erreur de sérialisation
- Code d'exploitation disponible le 30/04
- Patch le 29/04 par Oracle

https://www.exploit-db.com/exploits/46780
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
https://medium.com/@knownseczoomeye/knownsec-404-team-oracle-weblogic-deserialization-rce-vulnerability-0day-alert-90dd9a79ae93

Failles / Bulletins / Advisories

Système (principales failles)

Prise de contrôle du système via 2 vulnérabilités au sein du CMS Sitecore

- mauvaise vérification des objets reçus par le serveur sous la forme de données binaires (unsafe object deserialization)
- Erreur au sein du traitement des jetons Anti-CSRF (Cross-Site Request Forgery)
- Exploit disponible, sans authentification préalable sur les versions 8.x

https://www.synacktiv.com/ressources/advisories/Sitecore_CSRF_deserialize_RCE.pdf

Prise de contrôle d'un système via une vulnérabilité dans Atlassian Confluence

- code d'exploitation publiée (vulnérabilité corrigée en mars)
- manque de vérification des données saisies par l'utilisateur et envoyées au connecteur Widget. Injection de code possible via une Server-Side Template Injection
- exploitations observée pour déployer le ransomware Grandcrab

https://github.com/rapid7/metasploit-framework/pull/11717/files
https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html
https://blog.alertlogic.com/active-exploitation-of-confluence-vulnerability-cve-2019-3396-dropping-gandcrab-ransomware/

Élévation de privilèges via une vulnérabilité dans l'image docker officiel Alpine Linux

- le mot de passe de l'utilisateur root est NULL par défaut

https://talosintelligence.com/vulnerability_reports/TALOS-2019-0782

Failles / Bulletins / Advisories

Réseau (principales failles)

Patchs Cisco

- 70 vulnérabilités pour 26 produits
- 3 vulnérabilités critiques pour :
  - Cisco Nexus 9000
    - Existence de paire de clés SSH par défaut
    - RCE avec privilèges root
  - Cisco Elastic
    - manque de validation sur l'API
    - RCE avec privilèges admin via une requête API
  - Cisco IOS XR
    - mauvaise isolation d'une interface d'admin
    - DOS à RCE

- Produits vulnérables
  - Cisco Aironet Series Access Points
  - Cisco Application Policy Infrastructure Controller
  - Cisco ASR 9000 Series
  - Cisco Directory Connector
  - Cisco DNA Center
  - Cisco Elastic Services
  - Cisco Email Security Appliance
  - Cisco Expressway Series and Cisco TelePresence
  - Cisco Expressway Series
  - Cisco Firepower
  - Cisco HyperFlex HX-Series
  - Cisco Identity Services Engine
  - Cisco IOS XR
  - Cisco IP Phone 7800 Series and 8800 Series
  - Cisco Nexus 9000 Series Fabric Switches
  - Cisco Prime Collaboration
  - Cisco Prime Network Registrar
  - Cisco Registered Envelope
  - Cisco Small Business RV320 and RV325 Routers
  - Cisco Small Business Switches
  - Cisco UCS B-Series Blade Servers
  - Cisco Umbrella
  - Cisco Unified Communications Manager
  - Cisco Web Security Appliance
  - Cisco Wireless LAN Controller

https://tools.cisco.com/security/center/Search.x?publicationTypeIDs=1&firstPublishedStartDate=2019%2F04%2F09&firstPublishedEndDate=2019%2F05%2F13&limit=100

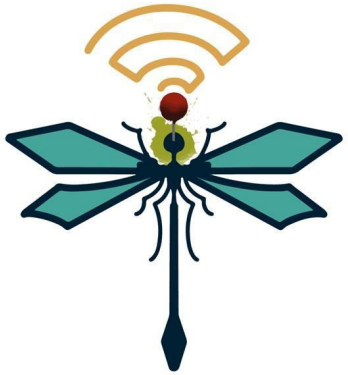
Failles / Bulletins / Advisories

Réseau (principales failles)

Publication des vulnérabilités Dragonblood affectant le standard WPA3

- 5 vulnérabilités
  - déni de service du point d’accès ;
  - contournement de sécurité via l'utilisation forcée d'un protocole vulnérable ;
  - vol d'informations via une attaque par canaux auxiliaires.
- WPA3 revue par le groupe Wifi Alliance pour les corriger

https://wpa3.mathyvanhoef.com/



Failles / Bulletins / Advisories

Hardware / IoT

Failles / Bulletins / Advisories

Android / iOS

30 vulnérabilités au sein d'Android

- provenaient de diverses erreurs mémoires (dépassement de tampon, dépassement de capacité...)
- la plus critique : RCE via l'ouverture d'un fichier malveillant dans le contexte d'un process privilégié

https://source.android.com/security/bulletin/2019-05-01.html#2019-05-01-details

Google annonce une évolution du système de mise à jour de sécurité dans Android Q

- nommé Project Mainline
- Envoi des mises à jour de sécurité automatiquement via OTA sans passer par le constructeur sur 14 modules dont le module gérant les codecs médias
- Note importante :
  - les constructeurs peuvent opt-out certains modules mais pas tous
  - fonctionne uniquement à partir d'Android Q

https://techcrunch.com/2019/05/07/android-q-security-updates/

https://www.theverge.com/2019/5/7/18531350/google-android-q-project-mainline-security-updates-play-store-io-2019

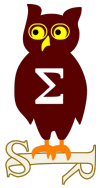
Failles / Bulletins / Advisories

Android / iOS

Une vulnérabilité affectant WhatsApp pourrait avoir été exploitée pour injecter un logiciel espion

- Erreur de gestion des appels VOIP. En envoyant des paquets SRTCP spécialement construits, un attaquant était en mesure d'exécuter du code arbitraire sur l'appareil via un simple appel (sans répondre)
- Attaque ciblés sur un avocat ayant travaillé sur le dossier NSO Group

https://www.theverge.com/2019/5/14/18622744/whatsapp-spyware-nso-pegasus-vulnerability



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Une porte dérobée a été découverte dans le package Ruby officiel bootstrap-sass

- exécution de code arbitraire sur le serveur Rails
- 2 comptes de mainteneurs supposés compromis

https://snyk.io/blog/malicious-remote-code-execution-backdoor-discovered-in-the-popular-bootstrap-sass-ruby-gem/

Le service de webmail de Microsoft affecté par une fuite de données

- Le pirate a récupéré les données de connexion d'un technicien de Microsoft
- Il a consulté les données liées à certains comptes (adresse email, adresses email des personnes avec qui les victimes ont correspondu, objets des emails).
- Selon une source de Motherboard, la compromission aurait permis d'accéder à n'importe quel compte n'appartenant pas à une entreprise

https://interestingengineering.com/microsoft-suffers-security-breach-of-webmail-services
https://motherboard.vice.com/en_us/article/ywyz3x/hackers-could-read-your-hotmail-msn-outlook-microsoft-customer-support

Sea Turtle, une campagne de phishing à grande échelle

- 40 organisations ciblés dans 13 pays
- DNS hijacking via une injection de code sur des routeurs Cisco
- Découvert par Talos

https://interestingengineering.com/microsoft-suffers-security-breach-of-webmail-services
https://motherboard.vice.com/en_us/article/ywyz3x/hackers-could-read-your-hotmail-msn-outlook-microsoft-customer-support

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Une base de données Docker Hub expose les données sensibles de 190 000 utilisateurs

- accès non autorisé à cette base de données
- noms d'utilisateurs, empreintes des mots de passe et jetons Github / Bitbucket
- utilisateurs contactés, secrets réinitialisés

https://success.docker.com/article/docker-hub-user-notification

Une campagne publicitaire exploitant une vulnérabilité dans Chrome touche un demi-milliard d'utilisateurs d'iOS

- par un groupe nommé eGlobber
- États-Unis et Europe majoritairement touchés
- découpée en 8 campagnes de 24 à 48 heures ayant pour but de piéger des utilisateurs via une offre lucrative qui parvenait à contourner le mécanisme intégré à Google Chrome de bloqueur de fenêtre

https://threatpost.com/easter-attack-apple-ios/143901/

Fuite de 60 millions de données LinkedIn depuis des serveurs non sécurisés

- 230 GB de données des profils des utilisateurs dont des données cachés (emails personnels, etc.)
- Pas de mot de passe dérobés

https://threatpost.com/easter-attack-apple-ios/143901/

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

EternalBlue est toujours utilisé pour infecter des systèmes non maintenus

- identifié par la société Keysight
- le nombre de scans de vulnérabilités par des attaquants multiplié par 3 entre janvier et décembre 2018
- Apache Struts et Cisco Smart Install ont également le vent en poupe

https://about.keysight.com/en/newsroom/pr/2019/15apr-nr19059-ixia-security-report-2019.pdf

900 000 systèmes SAP seraient vulnérables à un code d'exploitation

- codes d'exploitation publiées pour NetWeaver et S/4HANA
- prise de contrôle d'un système sans authentification
- provient de configuration par défaut notamment des ACL
- SAP publie des notes pour informer des meilleures pratiques

https://www.bleepingcomputer.com/news/security/public-10kblaze-exploits-may-impact-90-percent-of-sap-production-systems/
https://www.onapsis.com/10kblaze

Un pirate vide des dépots Git et demande des rançons

- 0,1 Bitcoin
- attaque le 3 mars sur les différents services (Github, Bitbucket, Gitlab)
- a priori via du credentials stuffing ou via des identifiants publiés dans de fichiers de configurations
- les dépôts n'étaient en réalité par supprimés, seuls les git commit header sont altérés

https://security.stackexchange.com/questions/209448/gitlab-account-hacked-and-repo-wiped

Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Armagadd-on 2.0 : toutes les extensions de Mozilla Firefox inopérantes suite à l'expiration d'un certificat intermédiaire

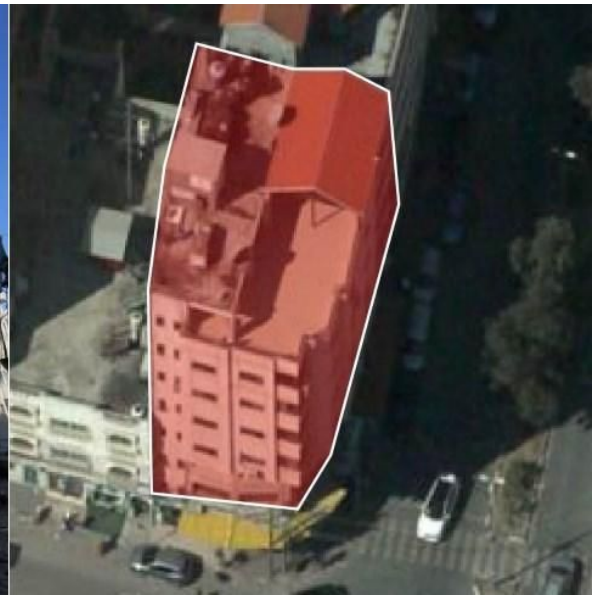
- lié à la fonctionnalité intégrée dans la version 43 de signature des extensions par Mozilla
- correctif le 5 mai

https://blog.mozilla.org/addons/2019/05/04/update-regarding-add-ons-in-firefox/

Israel répond à des attaquants du Hamas par un bombardement

- aucun détail sur la cyberattaque orchestrée par le Hamas
- la vidéo depuis le drone partagée sur les réseaux sociaux
- pas la première fois, les USA l'avait déjà fait en 2015

https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/



Piratages, Malwares, spam, fraudes et DDoS

Hack 2.0

Des données personnelles de millions de citoyens indiens exposées sur Internet

- base détecté via Shodan le 23 avril 2019
- base MongoDB non protégée accessible jusqu'au 8 mai (effacé par un groupe de pirate)
- 275 millions d'enregistrements de citoyens :
  - nom ;
  - sexe ;
  - date de naissance ;
  - adresse email ;
  - numéro de téléphone ;
  - détails sur le cursus scolaire ;
  - informations professionnelles (historique des employeurs, compétences, domaine d'activité) ;
  - salaire actuel.
- Le proprietaire est inconnu

https://www.bleepingcomputer.com/news/security/over-275-million-records-exposed-by-unsecured-mongodb-database/

Piratages, Malwares, spam, fraudes et DDoS
Espionnage

Le groupe de cyber espionnage Buckeye employait des outils dévoilés par les Shadow Brokers

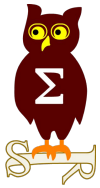
- aussi nommé APT3, Gothic Panda ou Pirpi
- Groupe connu depuis 2009 ciblant des organisations aux USA puis à Hong Kong.
- En 2017, 3 membres avaient été inculpés par le Département de la Justice aux USA. Ils travaillaient pour le Boyusec, entrepreneur pour le Ministère Chinois de la Sécurité de l'Etat.
- Symantec a identifié que ce groupe utilisait ces outils au moins un an avant leur fuite
- On ne connait pas le mode d'obtention de ces outils

https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

Des accès et le code source de 3 antivirus américains mis en vente sur le Dark Web

- pour $300,000 pour 30 To volés
- les noms ne sont pas dévoilés
- le groupe Fxmsp à l'origine de la vente (parle russe et anglais)

https://blog.mozilla.org/addons/2019/05/04/update-regarding-add-ons-in-firefox/



Nouveautés, outils et techniques

Crypto et Divers

Divers

Mozilla met en place une base de données commune des autorités de certification

- appelée CCADB, vocation à proposer une base de données collaboratives des CA dignes de confiance
- Initiative supportée par Google, Cisco, Apple et Microsoft

https://blog.mozilla.org/security/2019/04/15/common-ca-database-ccadb/

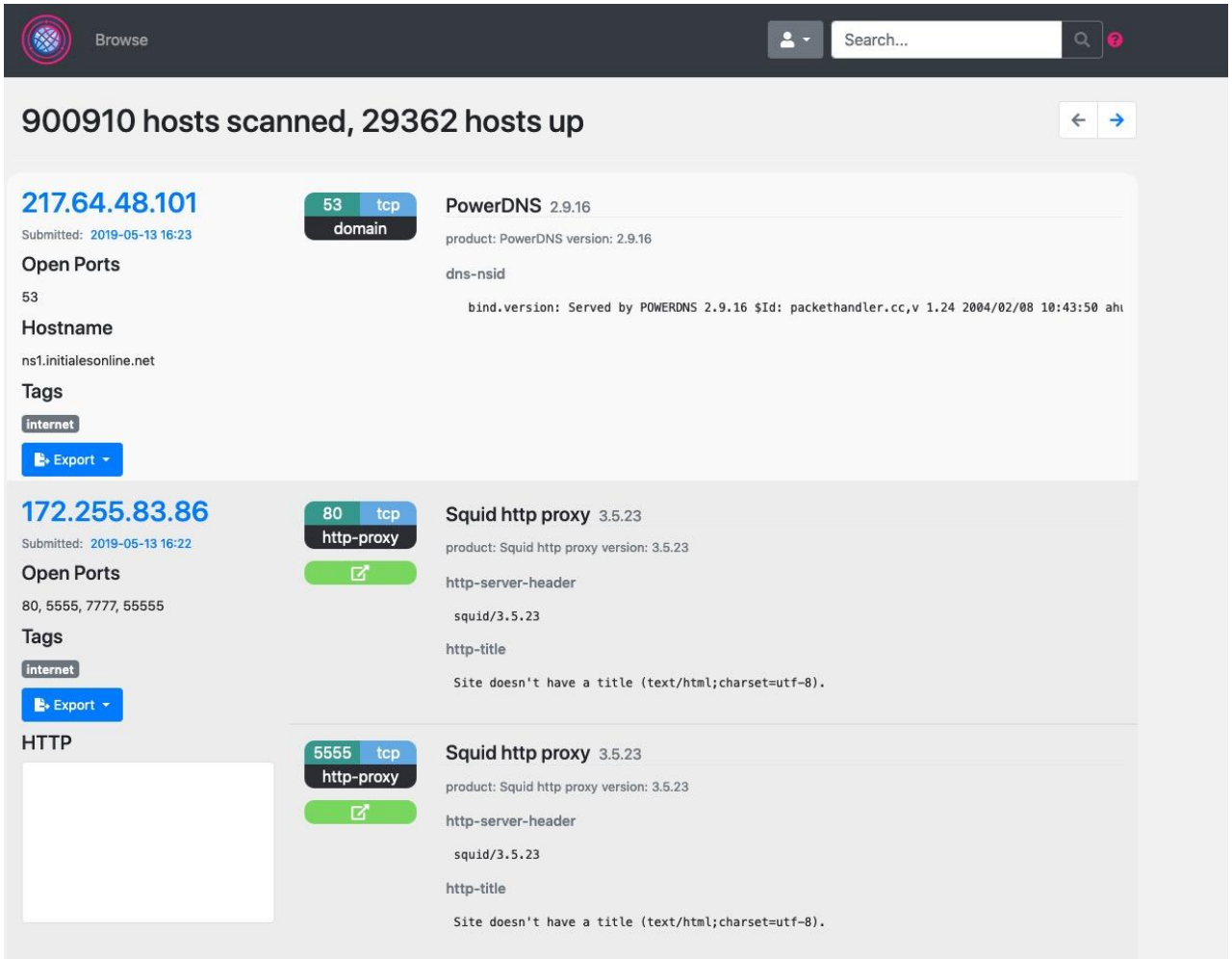
Pentest

Techniques & outils

Natlas

- Shodan-like on premise

  https://natlas.io/search



Pentest
Pirater les pirates

Le code source du trojan bancaire Carbanak a été publié

- découvert sur VirusTotal par des chercheurs de FireEye
- utilisé par le groupe FIN7 contre des institutions bancaires pour dérober des millions de dollars
- FE a commencé à publier une série d'article en détaillant le code

https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-one-a-rare-occurrence.html
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-two-continuing-source-code-analysis.html
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-three-behind-the-backdoor.html
https://www.fireeye.com/blog/threat-research/2019/04/carbanak-week-part-four-desktop-video-player.html

Plusieurs serveurs de commande de botnet compromis à cause de faibles identifiants

https://www.ankitanubhav.info/post/c2bruting

Une vulnérabilité permet de provoquer le déni de service d'un serveur de contrôle d'un botnet basé sur Mirai

- En entrant un nom d'utilisateur composé de plus de 1 024 caractères dans le formulaire d'authentification, il est possible de provoquer le déni de service du serveur de contrôle (crash).

https://www.ankitanubhav.info/post/crash

Business et Politique

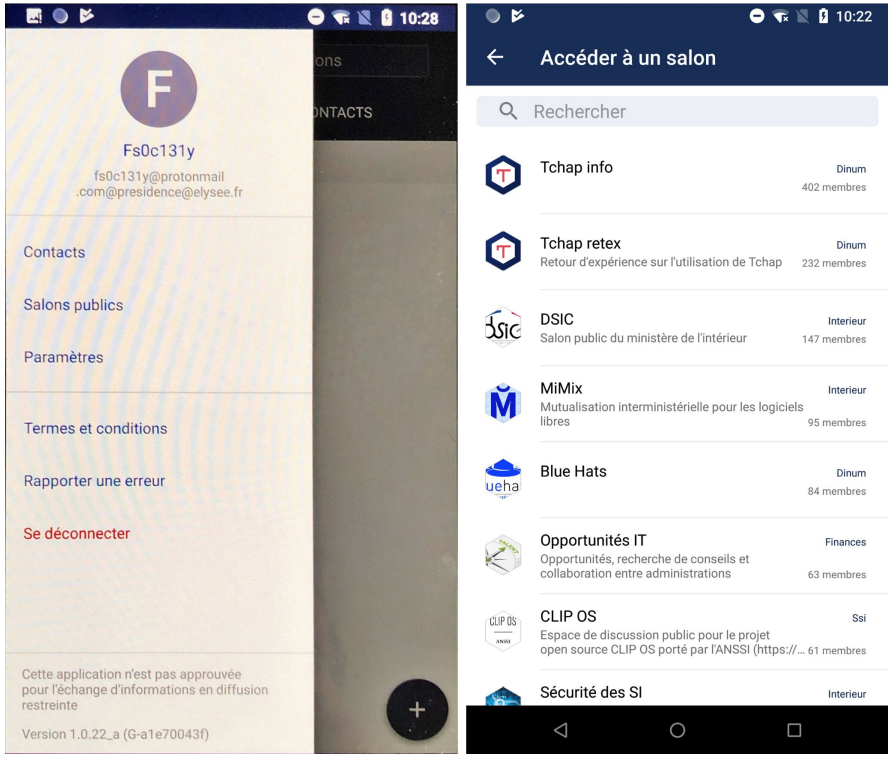
Business

France

L'application française de messagerie Tchap est lancée

- vulnérabilité découverte à sa sortie par un chercheur
- erreur dans la gestion des adresses email normalement restreinte à @elysee.fr
  - @protonmail.com@presidence@elysee.fr fonctionnait
- vulnérabilité corrigée immédiatement 👍

https://techcrunch.com/2019/04/19/security-flaw-in-french-government-messaging-app-exposed-confidential-conversations/
https://www.numerique.gouv.fr/espace-presse/lancement-de-tchap-la-messagerie-instantanee-des-agents-de-letat/



Business

France

Alsid lève 13 millions d'euros

https://capitalfinance.lesechos.fr/deals/capital-risque/cybersecurite-alsid-souvre-a-idinvest-et-leve-13-m-1012206

Orange rachète SecureLink

https://www.linformaticien.com/actualites/id/51957/cybersecurite-orange-rachete-le-neerlandais-securelink.aspx

Business

International

Droit / Politique

France

La CNIL enregistre un nombre record de plaintes en 2018

- en augmentation de 32%
- 85% des plaintes sont fondées
- 400 contrôles réalisés menant à 49 mises en demeures et 11 sanctions (9 rendues publiques)
- les sujets les plus fréquents
  - réputation en ligne (près d'un tiers des plaintes) ;
  - prospection commerciale abusive (21% des plaintes) ;
  - gestion des ressources humaines (16,5% des plaintes) : surveillance de l'activité des salariés en ligne, vidéosurveillance ;
  - secteur bancaire (9% des plaintes) : inscriptions abusives aux fichiers de la Banque de France, non-respect de la portabilité des données.

https://www.lemondeinformatique.fr/actualites/lire-la-cnil-a-enregistre-un-record-de-11077-plaintes-en-2018-75003.html

Droit / Politique
International

La société Ticketmaster poursuivie en justice suite à un vol de données bancaires en ligne

- 5 millions de livres demandés
- Fait suite à la découverte en juin 2018 d'un vol de données de 40 000 utilisateurs
- Magecart responsable de l'inclusion d'un formulaire malveillant

https://www.riskiq.com/blog/labs/magecart-ticketmaster-breach/

Europol parvient à fermer deux marketplaces du Dark Web

- Wall Street Market : 5 400 vendeurs et 1,1 millions de clients
- Silkkitie (nommé aussi Valhalla Market) : plus petite mais plus vieilles (2013)
- 550 000€ saisie et 1 million d'euros en Bitcoin et Monero
- Collaboration internationale :
  - WSM
    - Police criminelle fédérale allemande
    - Police nationale néerlandaise
    - Europol
    - Eurojust
    - Polices américaines (IRS, DEA, FBI, IRS, HSI, USPIS, USDJ)
  - Silkkitie
    - Douanes finlandaises
    - Police nationale française (Cocorico)
    - Europol assisté par Bitdefender

https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Droit / Politique

International

Le FBI fait tomber le site Deep dot web

- Arrestations en Israël, France, Allemagne, Pays-Bas, Brésil
- Plusieurs millions de dollars générés via des commissions pour du référencement de liens

https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Conférences

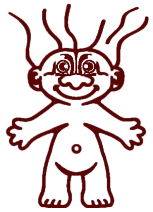
Conférences

Passées

- Hack in the Box – 6 au 10 mai 2019 à Amsterdam

A venir

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



Divers / Trolls velus

Divers / Trolls velus

Enfin...

- Windows met à jour le Terminal et le rend open source
- emojis, accélération GPU, liens cliquables, redimensionnement vertical, personnalisable...
- et même une vidéo promotionnelle

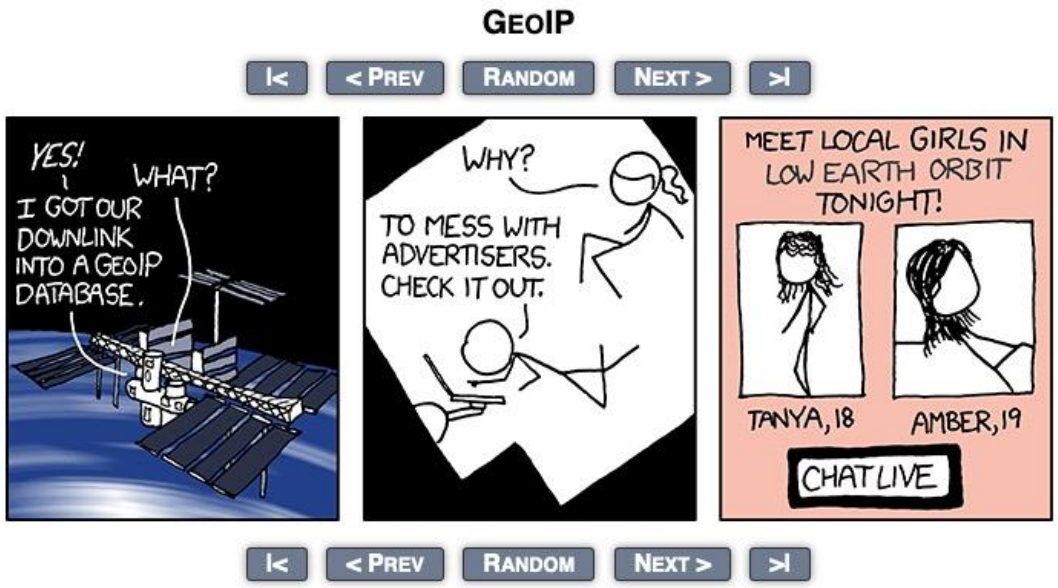
This is the year of the Linux desktop

Divers / Trolls velus

Nokia propose un lecteur biométrique de nouvelle génération

- on est pas encore convaincu...

Divers / Trolls velus



Divers / Trolls velus

Facebook...

- “The future is private” selon Mark Zuckerberg
- Son co-fondateur promeut le démantèlement de l’organisation
- L’entreprise s’attend à une amende de 3 à 6 milliards de dollars par la FTC
- Vote proposé par des actionnaires pour faire sortir Mark de son poste de CEO

https://www.theverge.com/2019/4/30/18524188/facebook-f8-keynote-mark-zuckerberg-privacy-future-2019
https://9to5mac.com/2019/05/09/breakup-facebook-cofounder/
https://9to5mac.com/2019/04/24/facebook-earnings-q1-2019/

“We don’t exactly have the strongest reputation on privacy right now.”

- Mark Zuckerberg

Divers / Trolls velus

Le site matrix.org compromis

- L'attaquant partage ses recommandations de sécurité sur le Github

78 Open ✓ 143 Closed Author Labels

- [SECURITY] 2FA is gud
  #365 opened an hour ago by matrixnotorg
- [SECURITY] Signing keys in production?!?
  #364 opened an hour ago by matrixnotorg
- [SECURITY] Monitor log files to avoid relying on external whitehats
  #363 opened an hour ago by matrixnotorg
- [SECURITY] Git is not a secret store
  #362 opened an hour ago by matrixnotorg
- [SECURITY] Ansible management of sshd_config
  #361 opened an hour ago by matrixnotorg
- [SECURITY] Controlled Production Access
  #360 opened 2 hours ago by matrixnotorg
- [SECURITY] Jenkins Slave listening to SSH on the internet
  #359 opened 2 hours ago by matrixnotorg
- [SECURITY] Principle of Least Privilege
  #358 opened 2 hours ago by matrixnotorg
- [SECURITY] SSH Agent Forwarding
  #357 opened 2 hours ago by matrixnotorg

```
Time for actual transparency.

Linux ares.matrix.org 3.16.0-4-amd64 #1 SMP Debian 3.16.39-1+deb8u2 (2017-03-07) x86_64 GNU/Linux
Linux hera.matrix.org 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64 GNU/Linux
Linux themis.matrix.org 3.16.0-5-amd64 #1 SMP Debian 3.16.51-3+deb8u1 (2018-01-08) x86_64 GNU/Linux
Linux hebe 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u4 (2018-08-21) x86_64 GNU/Linux
Linux nyx.matrix.org 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u2 (2018-02-21) x86_64 GNU/Linux
Linux hermes.matrix.org 3.16.0-4-amd64 #1 SMP Debian 3.16.51-2 (2017-12-03) x86_64 GNU/Linux
Linux aphrodite.matrix.org 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64 GNU/Linux
Linux pheme.matrix.org 3.16.0-4-amd64 #1 SMP Debian 3.16.43-2+deb8u2 (2017-06-26) x86_64 GNU/Linux
Linux homonoia.matrix.org 3.16.0-4-amd64 #1 SMP Debian 3.16.39-1+deb8u2 (2017-03-07) x86_64 GNU/Linux
Linux hephaestus.matrix.org 3.16.0-4-amd64 #1 SMP Debian 3.16.43-2+deb8u3 (2017-08-15) x86_64 GNU/Linux
Linux clio.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6 (2018-10-08) x86_64 GNU/Linux
Linux juventas.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u5 (2018-09-30) x86_64 GNU/Linux
Linux iris.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6 (2018-10-08) x86_64 GNU/Linux
Linux hypnos.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u6 (2018-10-08) x86_64 GNU/Linux
Linux demeter.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u3 (2018-08-19) x86_64 GNU/Linux
Linux phobos.matrix.org 4.9.0-8-amd64 #1 SMP Debian 4.9.110-3+deb9u3 (2018-08-19) x86_64 GNU/Linux
Linux eris.matrix.org 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64 GNU/Linux

root@hebe:/var/lib/postgresql# df -h
df -h
Filesystem                              Size  Used Avail Use% Mounted on
udev                                     63G     0   63G   0% /dev
tmpfs                                    13G   67M   13G   1% /run
/dev/vda1                               505G  7.6G  492G   2% /
tmpfs                                    63G   28K   63G   1% /dev/shm
tmpfs                                   5.0M     0  5.0M   0% /run/lock
tmpfs                                    63G     0   63G   0% /sys/fs/cgroup
/dev/mapper/data--group-data--volume  9.5T  6.7T  2.4T  74% /mnt/data
tmpfs                                    13G     0   13G   0% /run/user/0
tmpfs                                    13G     0   13G   0% /run/user/1002

$ cat users.txt | grep arathorn | head -n1
@arathorn:matrix.org|$2a$12$u1ual.yp7rnSjXRgwZ5ZIOxa0D9txCT64i3Y/jmbtgQ6ByxVr59zu
$ wc -l users.txt
5493973

See you soon.
```

Prochains rendez-vous de l’OSSIR

Prochaines réunions

Prochaine réunion

- Mardi 11 juin 2019

After Work

-

Questions ?

Des questions ?

- C’est le moment !

Des idées d’illustrations ?

Des infos essentielles oubliées ?

- Contactez-nous