ONGOING SECURITY

TOP STORIES OF MAY 2018

"SEC RITY"
is nothing without
"U"

- May-2018 |(0Day) Microsoft Windows JScript Error Object Use-After-Free Remote Code Execution Vulnerability
- May-2018 | Announcing the May 2018 Git Security Vulnerability
- May-2018 | New Brazilian Banking Trojan MnuBot Discovered
- May-2018 | Trojan watch
- May-2018 | Multiple Vulnerabilities found in IBM QRadar
- May-2018 | Remote Authentication GeoFeasibility Tool - GeoLogonalyzer
- May-2018 | Will the Real Joker's Stash Come Forward?
- May-2018 | Taylor cryptocurrency: we've been hacked and we need your support
- May-2018 | BMO Financial Group Issues Statement
- May-2018 | Simplii Financial Advises Clients of Potential Security
- May-2018 | EOS Node Remote Code Execution Vulnerability
- May-2018 | ForgotDoor: Routers in Singapore accidentally give complete access to potential IoT attackers
- May-2018 | DDOS ATTACKS AGAIN TARGET DUTCH BANKS
- May-2018 | FBI: Kindly Reboot Your Router Now, Please
- May-2018 | 2018 Fraud World Cup
- May-2018 | Hackers Post Protest Messages On Mashad Airport Displays
- May-2018 | A bug in T-Mobile site allowed anyone see any customer's account details
- May-2018 | Coca-Cola Suffers Breach at the Hands of Former Employee
- May-2018 | SEVered: Subverting AMD's Virtual Machine Encryption
- May-2018 | Why Is Your Location Data No Longer Private?
- May-2018 | Money for nothing? Cryptocurrency "giveaways" net thousands for scammers
- May-2018 | BackSwap malware finds innovative ways to empty bank accounts
- May-2018 | This algorithm can hide secret messages in regular-looking text
- May-2018 | Z-Shave. Exploiting Z-Wave downgrade attacks
- May-2018 | 3 Charged In Fatal Kansas 'Swatting' Attack
- May-2018 | Here's How to Download All the Data Apple Collects About You
- May-2018 | Amazon confirms that Echo device secretly shared user's private audio
- May-2018 | VPNFilter EXIF to C2 mechanism analysed
- May-2018 | Android devices ship with pre-installed malware
- May-2018 | Justice Department Announces Actions to Disrupt 28 Botnet

- May-2018 | New Mac cryptominer uses XMRig
- May-2018 | New VPNFilter malware targets at least 500K networking devices worldwide
- May-2018 | TalkTalk Router - WPS Exploit (21 May 2018)
- May-2018 | Turla Mosquito: A shift towards more generic tools
- May-2018 | Hacker Makes Over $18 Million in Double-Spend Attack on Bitcoin Gold Network
- May-2018 | Backdoors in D-Link's backyard
- May-2018 | RESEARCHERS SAY MORE SPECTRE-RELATED CPU FLAWS ON HORIZON
- May-2018 | Amazon Facial Recognition Software
- May-2018 | I know where your pet is
- May-2018 | Experimental Security Assessment of BMW Cars: A Summary Report
- May-2018 | Mobile Giants: Please Don't Share the Where
- May-2018 | ZipperDown Vulnerability: 100 Million iOS Users (Not Using Zimperium) at Risk of Exploit
- May-2018 | Tracking Photo's Geo-location with GPS EXIF DATA - Forensic Analysis
- May-2018 | Parrot 4.0 is now available for download
- May-2018 | 3.2 million LA County 211 records exposed on misconfigured AWS S3 bucket
- May-2018 | Brain Food botnet gives website operators heartburn
- May-2018 | Report: Bank Attacks
- May-2018 | A Wicked Family of Bots
- May-2018 | Phishing Email Ironically Provides a List of Scammers You Should Avoid
- May-2018 | Hacked Drupal sites involved in mining campaigns, RATs distributions, scams
- May-2018 | $36k Google App Engine RCE
- May-2018 | Remote smart car hacking with just a phone
- May-2018 | Distributing Spyware via Comments Section of YouTube Videos
- May-2018 | 58% of Botnet Malware Infections Last Under a Day
- May-2018 | Roaming Mantis dabbles in mining and phishing multilingually
- May-2018 | Latin American 'Bineros' Ramping Up Fraudulent Activity
- May-2018 | CVE-2018-5737 (BIND 9.12)
- May-2018 | Judges convict crook of operating Scan4You Counter Antivirus Service
- May-2018 | System Management Mode Speculative Execution Attacks

- May-2018 | Notification of Urgent Security Updates to DrayTek routers

- May-2018 | Actor Advertises Japanese PII on Chinese Underground

- May-2018 | T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account

- May-2018 | Crypto-Hijacker Attack Victims over 500,000 Times in 3 days

- May-2018 | GPON Exploit in the Wild (II) - Satori Botnet

- May-2018 | Scanning destination port 3333

- May-2018 | CryptoMiner, WinstarNssmMiner, Has Made a Fortune By Brutally Hijacking Computers

- May-2018 | Website leaked real-time location of most US cell phones

- May-2018 | LocationSmart API Vulnerability

- May-2018 | Nethammer:Inducing Rowhammer Faults through Network Requests

- May-2018 | The new Wicked Mirai botnet leverages at least three new exploits

- May-2018 | Cisco Digital Network Architecture Center Static Credentials Vulnerability

- May-2018 | Breed of MBR Infecting Ransomware - an analysis by Quick Heal Security Labs

- May-2018 | Hardcoded Password Found in Cisco Enterprise Software, Again

- May-2018 | Revealed: Ecuador spent millions on spy operation for Julian Assange

- May-2018 | A tale of two zero-days

- May-2018 | SECURITY RESEARCH REPORT

- May-2018 | Company used by police, prisons to find any mobile device breached (again)

- May-2018 | TeleGrab - Grizzly Attacks on Secure Messaging

- May-2018 | Building cyber resilience in airports

- May-2018 | RedHat: DHCP Client Script Code Execution Vulnerability - CVE-2018-1111

- May-2018 | New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation

- May-2018 | Thieves suck millions out of Mexican banks in transfer heist

- May-2018 | Board of Control for Cricket in India (BCCI) exposed personal sensitive data

- May-2018 | Ex-CIA employee ID'd but not charged in Vault 7 leak of hacking tools

- May-2018 | Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels

- May-2018 | Signal-desktop HTML tag injection

- May-2018 | GDPR PHISHING SCAM TARGETS APPLE ACCOUNTS, FINANCIAL DATA

- May-2018 | Most Wanted Malware

- May-2018 | Danish Railway Company DSB Suffers DDoS Attack

- May-2018 | Detecting Cloned Cards at the ATM, Register

- May-2018 | Adobe Security Bulletin

- May-2018 | Misinterpretation of Intel docs is the root cause for the CVE-2018-8897 flaw in Hypervisors and OSs
- May-2018 | Microsoft Adds Support for JavaScript in Excel
- May-2018 | SIERRA WIRELESS PATCHES CRITICAL VULNS
- May-2018 | Number of DDoS Attacks Significantly Declines After Shutdown of Webstresser.org
- May-2018 | Decompiled keystore.py from ElectrumPro scam (line 223)
- May-2018 | Google released Meltdown mitigations for Android
- May-2018 | Office 365 Security Fails To Secure 100 Million Email Users
- May-2018 | Bycyklen has been hacked
- May-2018 | PoC Developed for CoinHive Mining In Excel Using Custom JavaScript Functions
- May-2018 | Backdoored Python Library Caught Stealing SSH Credentials
- May-2018 | Cryptocurrency-Mining Malware Targeting IoT, Being Offered in the Underground
- May-2018 | Thousands of Companies Are Still Downloading the Vulnerability That Wrecked Equifax
- May-2018 | Hide and Seek IoT Botnet resurfaces with new tricks, persistence
- May-2018 | MAY PATCH TUESDAY FIXES TWO BUGS UNDER ACTIVE ATTACK
- May-2018 | Budget 2018: DHA given AU$130m for 'identity management' platform
- May-2018 | FBI's 2017 Internet Crime Report
- May-2018 | SynAck targeted ransomware uses the Doppelganging technique
- May-2018 | Attack on KrebsOnSecurity Cost IoT Device Owners $323K
- May-2018 | Romanian Hackers Extradited to U.S. over $18M Vishing Scam
- May-2018 | Hackers Deface Canon Security Cameras in Japan
- May-2018 | Large cryptojacking campaign targeting vulnerable Drupal websites
- May-2018 | An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers
- May-2018 | ECB publishes European framework for testing financial sector resilience to cyber attacks

- May-2018 | Report:INDUSTRIAL COMPANIES ATTACK VECTORS

- May-2018 | Report:THE CHANGING STATE OF RANSOMWARE

- May-2018 | CSP MySQL User Manager 2.3.1 - Authentication Bypass

- May-2018 | Pr0nbots2: Revenge Of The Pr0nbots

- May-2018 | Asylo: an open-source framework for confidential computing

- May-2018 | AT&T blames "unintentional IP address conflict"

- May-2018 | ABBOTT ADDRESSES LIFE-THREATENING FLAW IN A HALF-MILLION PACEMAKERS

- May-2018 | CYBERESPIONAGE OPERATION TARGETS ANDROID USERS IN THE MIDDLE EAST.

- May-2018 | Airbnb customers being scammed by criminals

- May-2018 | GandCrab V3 Accidentally Locks Systems

- May-2018 | Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones

- May-2018 | Meltdown patch can be bypassed

- May-2018 | Rowhammer attacks

- May-2018 | Lojack Becomes a Double-Agent

- May-2018 | Microsoft released an out of RCE vulnerability in the Windows Host Compute Service Shim library (hcsshim)

- May-2018 | HACKTIVISTS, TECH GIANTS PROTEST GEORGIA'S 'HACK-BACK' BILL

- May-2018 | Critical Schneider Electric InduSoft Web Studio and InTouch Machine Edition Vulnerability

- May-2018 | When Your Employees Post Passwords Online

- May-2018 | Kaspersky Finds North American Consumers Plagued by Cyber-Stress

- May-2018 | FacexWorm Targets Cryptocurrency Trading Platforms, Abuses Facebook Messenger for Propagation

- May-2018 | DVR Login Bypass (CVE-2018-9995)

- May-2018 | SiliVaccine: Inside North Korea's Anti-Virus

- May-2018 | The Connected Car Ways to get unauthorized access and potential implications

- May-2018 | Critical RCE Vulnerability Found in Over a Million GPON Home Routers

- May-2018 | Unicef's TheHopepage May Be the First Good Use of In-Browser Mining

- May-2018 | MMap Vulnerabilities - Linux Kernel

About us

Information Security	**Políticas, Normas e Procedimentos GDPR** • Compliance • Data Protection Officer **Military-Grade Security** • Segurança Interna e de Perímetro • Hardening de Sistemas	**Hacking Critical Infrastructure** **Pentest** • Blackbox • Hacking Critical Infrastructure **Vulnerability Assessment** • SaaS, • Onsite • OnDemand	**Multidimentional Attack Surface** **Cybersecurity** **Campanha de conscientização** • ISO/IEC 27002
IDENTITY & ACCESS MANAGMENT	**Desenho do ciclo de vida de acesso** **Análise Bottom-Up** **Integração IDM/IAM com sistemas via:** • Adapters • Webservices • DB Connection	**Processos de Acesso Lógico:** • Concessão • Revogação • Alteração • Suspensão • Restauração • Revisão • Recuperação de Senhas	**Análise de Segregação de Funções** **Definição de Papéis e Funções** **Perfis de Acesso** • RBAC • MAC • DAC
SAP SECURITY	**Pentest** **Vulnerability Assessment** **Audit**	**Z-System Code Review** **SOD** **Gap Analysis**	**Report** **Compliance**
SERVICES	**Security Advisor** **Visão Holística e abordagem** • Estratégica • Táctica • Operacional	**IT Solutions** **IS Solutions**	**Alocação de Talentos** • Time & Material • BodyShop • Projetos • Banco de horas