ONGOING SECURITY

"SEC RITY"
is nothing
without
"U"

- Cryptocurrency Leaks Personal Information for Thousands of Investors

- NATO Won Cyber Defence Exercise Locked Shields 2018

- Oracle Weblogic Server POC(CVE-2018-2628)

- Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

- Facebook Tracking PoC via Faasos

- Uber's Bug Bounty Program

- Telegram DOWN - Popular messaging app not working as major outage confirmed

- Long Prison Sentence for Man Who Hacked Jail Computer System to Bust Out Friend

- Supporting Same-Site Cookies in Firefox 60

- Two security experts discovered that the control panel of a Ski lift in Austria was exposed online without any protection

- PoC for a NTFS crash Windows7 & Windows10 versions

- NTLM Credentials Theft via PDF Files

- ISLAMIC STATE PROPAGANDA MACHINE HIT BY LAW ENFORCEMENT IN COORDINATED TAKEDOWN ACTION

- PoC Code Published for Triggering an Instant BSOD on All Recent Windows Versions

- Metamorfo Campaigns Targeting Brazilian Users

- Python-Based Malware Uses NSA Exploit to Propagate Monero (XMR) Miner

- "Rubella Macro Builder" Crimeware Kit Emerges on Underground

- Update to enable mitigation against Spectre, Variant 2

- Necurs Evolves to Evade Spam Detection via Internet Shortcut File

- WORLD'S BIGGEST MARKETPLACE SELLING INTERNET PARALYSING DDOS ATTACKS TAKEN DOWN

- Cyber Security Breaches Survey 2018

- Researchers Find Way to Create Master Keys to Hotels

- DDoS attacks in Q1 2018

- RESEARCHERS HACKED AMAZON'S ALEXA TO SPY ON USERS, AGAIN

- Ski lift shut down on the same day

- Hacker Hijacks DNS Server of MyEtherWallet to Steal $160,000

- Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach

- VPN Leaks Found on 3 Major VPNs

- Vulnerability Disclosure: Tegra SoCs

- Portugal Joins NATO Cyber-Defence Centre

- macOS App Can Detect Evil Maid Attacks

- Thai Airways Website Hacked

- Here are the 30 Red Bull websites that are hacked

- Transcription Service Leaked Medical Records

- Windows: WLDP CLSID policy .NET COM Instantiation UMCI Bypass

- ZLAB Malware Analysis Report - The Bandios malware suite

- New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia

- BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets

- Internet Explorer Zero-Day Exploited in the Wild by APT Group

- SunTrust to Offer Free Identity Protection

- The Week in Ransomware - April 20th 2018 - Reveton Charges, GandCrab, and More

- Is Facebook's Anti-Abuse System Broken?

- Kaspersky Lab Rails Against Twitter Ad Ban

- Cisco SAML Authentication Vulnerability

- Website leaves database of medics wide open

- LinkedIn AutoFill Exposed Visitor Name, Email to Third-Party Websites

- A Google update just created a big problem for anti-censorship tools

- Cisco WebEx Clients Remote Code Execution Vulnerability

- Over 20,000,000 of Chrome Users are Victims of Fake Ad Blockers

- CLOUD CREDENTIALS: NEW ATTACK SURFACE FOR OLD PROBLEM

- 2018 Data Breach Investigations Report

- Comodo Cybersecurity's First Quarter 2018 Threat Report

- RSAC: The Five Most Dangerous New Attacks According to SANS

- Rockwell Automation Stratix and ArmorStratix Switches

- Users don't want iOS to merge with MacOS, Apple chief says

- Block Buster: How A Private Intelligence Platform Leaked 48 Million Personal Data Records

- iOS Trustjacking Attack Exposes iPhones to Remote Hacking

- FDA Wants Medical Devices to Have Mandatory Built-In Update Mechanisms

- A Sobering Look at Fake Online Reviews

- No boundaries for Facebook data: third-party trackers abuse Facebook Login

- What Data Does Facebook Collect When I'm Not Using Facebook, and Why?
- Tens of thousands per Gram
- Critical Vulnerability Found in Majority of LG NAS Devices
- Leaking ads
- Avast's investigations of the CCleaner APT
- Ransomware XIAOBA Repurposed as File Infector and Cryptocurrency Miner
- 34 Tech Firms Sign Accord Not to Assist Government Hacking Operations
- Teen charged in Nova Scotia government breach says he had 'no malicious intent'
- A Review of Recent Drupal Attacks (CVE-2018-7600)
- GRIZZLY STEPPE - Russian Malicious Cyber Activity
- Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
- Deleted Facebook Cybercrime Groups Had 300,000 Members
- GOOGLE PLAY BOOTS THREE MALICIOUS APPS FROM MARKETPLACE TIED TO APTS
- WhatsApp photo drug dealer caught by 'groundbreaking' work
- Chinese Mobile Device Maker ZTE Banned From Buying U.S. Goods
- Ransomware attack cost city $2.7 million, records show
- JavaScript SecureRandom() isn't securely random - many old web wallets affected
- Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
- Android Apps for Kids
- TaskRabbit Takes Down App and Website After Getting Hacked
- Take Down 52.000 infected servers
- From Bangkok to Phuket, they cry out: Oh, Bucket! Thai mobile operator spills 46k people's data
- Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank
- WINDOWS IIS 6.0 CVE-2017-7269 IS TARGETED AGAIN TO MINE ELECTRONEUM
- Unsafe Opcodes exposed in Intel SPI based products
- Roaming Mantis uses DNS hijacking to infect Android smartphones
- Uncovering Drupalgeddon 2
- Cybercriminals Earn Millions, And Spend It Wildly
- Microsoft engineer charged with money laundering linked to Reveton ransomware
- Full version of the speech by Director GCHQ at CYBERUK

- PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines

- New 'Early Bird' Code Injection Technique Discovered

- When Identity Thieves Hack Your Accountant

- Wallet hack: Exchange firm loses bitcoins worth Rs 20 crore in Delhi

- Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims

- Nation-State Attacks Take 500% Longer to Find

- Malware Distribution Campaign Has Been Raging for More Than Four Months

- Glitch in malspam campaign temporarily reduces spread of GandCrab

- UPnProxy: Blackhat Proxies via NAT Injections

- Security flaws in Siemens devices

- SAP Cyber Threat Intelligence report

- Internet healt Report

- APT Trends report Q1 2018

- Operation Parliament, who is doing what?

- Klepto Currency: Are Hackers Cryptojacking Your Processing Power?

- Brazilian Criminals Use HTTP Injectors to Gain Free Mobile Internet Access

- Warning: Your Windows PC Can Get Hacked by Just Visiting a Site!!!

- Vevo YouTube Channels Suffer Music Video Hack

- Home Secretary Announces Police Crackdown on Dark Web

- Facebook Offering $40,000 Bounty

- Stealing Credit Cards from FUZE over Bluetooth - CVE-2018-9119

- Adobe, Microsoft Push Critical Security Fixes

- Public services at the Caribbean island Sint Maarten shut down by a cyber Attack

- SirenJack: how activate sirens and trigger false alarms2018 Data Breach Investigations Report

- Cinema voucher-pusher tells customers: Cancel your credit cards, we've been 'attacked'

- CVE-2018-4878 Exploit Builder

- WORD ATTACHMENT DELIVERS FORMBOOK MALWARE, NO MACROS REQUIRED

- Critical Code Execution Flaw Found in CyberArk Enterprise Password Vault

- Debian Bug report logs - #894667 beep: CVE-2018-0492

- Iran hit by global cyber attack that left U.S. flag on screens

- New Matrix Ransomware Variants Installed Via Hacked Remote Desktop Services

- Netskope Discovers ATMJackpot Siphoning Cash

- Don't Give Away Historic Details About Yourself

- Analysis of New Agent Tesla Spyware Variant

- Managing and Mitigating Security Vulnerabilities at Auth0

- Finland's 3rd Largest Data Breach Exposes 130,000 Users' Plaintext Passwords

- A totality - a full 100% - of web applications are vulnerable to hackers

- How to keep your ISP's nose out of your browser history with encrypted DNS

- FBI raids Backpage founders' homes in Arizona

- Fake Software Update Abuses NetSupport Remote Access Tool

- Computer system transcribes words users 'speak silently'

- New MacOS Backdoor Linked to OceanLotus Found

- Best Buy: Updates on [24]7.ai Cyber Incident

- Defend yourself from cybercrime with new Office 365 capabilities

- Statement on Data Security Incident

- APNewsBreak: US suspects cellphone spying devices in DC

- Secret Service Warns of Chip Card Scheme

- Multiple CVE reports published for the Spring Framework

- Meet VirusTotal Droidy, our new Android sandbox

- North Korea-Linked Lazarus APT suspected for online Casino assault

- Announcing Windows 10 Insider Preview Build 17639 for Skip Ahead

- Pocket cryptofarms

- Dot-cm Typosquatting Sites Visited 12M Times So Far in 2018

- Cisco Smart Install Remote Code Execution

- Latitude Technologies Current System Status

- Data on up to 87 million Facebook users shared with UK firm

- Microsoft: microcode revision guidance

- Hacking your brain(scan): security bugs in EEG software open hospitals to attack

- Korean cryptocurrency exchange boss arrested for fraud

- Compromised Magento Sites Delivering Malware
- Most Businesses Overlook One Common Mainframe Security Vulnerability
- Four Gas Pipeline Data Systems Shut Down as Cyberattack Hits
- Attacker Behavior Industry Report
- Pixel/Nexus Security Bulletin - April 2018
- Android Security Updates
- Fake AV Investigation Unearths KevDroid, New Android Malware
- FIN7 hackers stole credit and debit card information from millions of consumers who have purchased goods at Saks Fifth Avenue and Lord & Taylor stores
- Protecting users from extension cryptojacking
- Panerabread.com Leaks Millions of Customer Records
- US Govt Wants Nearly All Visa Applicants to Hand Over Personal Info
- How Cambridge Analytica's Facebook targeting model really worked
- HERE'S WHAT YOU SHOULD KNOW REGARDING OUR HIV STATUS DATA AND PRIVACY POLICY
- U.S. Department of Defense Kicks Off Fifth Bug Bounty Challenge With HackerOne
- Apple Plans to Use Its Own Chips in Macs From 2020, Replacing Intel
- OpenBSD 6.3
- A Trojan with Hidden Malicious Code Steals User's Messenger App Information

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