ANTONIO COSTA

Cyber security specialist | Cyber security engineer

@ coolerlair@gmail.com Brazil, Sao paulo https://github.com/CoolerVoid

EXPERIENCE

Principal cyber security engineer | cyber security specialist

MERCADO BITCOIN

October 2019 – On going full time Brazil - Sao paulo

- Automation every task with robots(GraphQL, codeQL, REST, bypass captcha etc).
- Codereview(following OWASP, NIST, MITRE, CERT) and pentest.
- SAST/DAST tools configuration.
- Threat intelligence services.
- I Helped all developers to make hardening and code patches in security issues.
- Research for security solutions.
- I have been written formal reports to explain vulnerabilities and how to write the fix following each context of language.
- I developed solutions for geo-localization with authentication
- Reverse engineering, IOC creation etc...

Developer, reverse engineer and researcher

Itau unibanco

Juny 2018 – September 2019 Brazil - Sao paulo

- Automation every task with robots on IMAP and SMTP protocols.
- Patch to fix bugs in local projects.
- I wrote some reports about local security.
- Threat intelligence services
- Hookings in C++ to protect sandbox etc.
- Pentest, codereview(following OWASP, NIST, MITRE, CERT) etc.
- Reverse engineering, IOC creation etc...

Pentester, Developer and researcher

CONVISO

Jan 2011 – may 2018 Curitiba - Brazil

- Penetration Test on Network, System, Web and WiFi. Vulnerability Assessment with automated and manual approach Basis of Bug Hunting through reverse engineering, tests or code review. Mitigating and preventing any threat spread, patch for any source code.
- Selenium robots to automate evidences
- Articles, tools etc.

Developer, Programmer

Freelancer

jan 2006 – Jan 2011 Sao paulo - Brazil

- Software Developer in ASM, C, C++, Perl, PHP and javascript for systems like e-commerce, CMS, PoS, web robots, IDS... Programming embedded systems with AVR, ARM and PIC...

MOST PROUD OF

Honors & Awards
First position on Top C GitHub developers in Sao paulo city git-awards.com/users/search?login=CoolerVoid

STRENGTHS

Hard-working | Hacking | Motivator

LANGUAGES

English	●●●○○
Spanish	●●○○○
Portuguese	●●●●●

PROGRAMMING SKILLS

Ansi C	●●●●●
C++	●●●●●
Rust	●●●●●
Assembly	●●●●○
Common Lisp	●●●●○
Racket Lisp	●●●○○
Python	●●●●●
Perl	●●●●●
Go	●●●●○
C#	●●●○○
Ruby	●●●○○
PHP	●●●●●
javascript	●●●●○
Java	●●●○○
Cobol	●●○○○

OS SKILLS

OpenBSD	●●●●○
Linux	●●●●●
Windows	●●●●○
MacOS	●●●●○

EDUCATION

Systems Analyst

UNASP

Sept 2010 – June 2013 - locked

PRESENTATIONS

Articles

- “https://linuxsecurity.com/features/features/octopuswaf” (2020). In: *Octopus WAF*.
- “https://www.darknet.org.uk/2019/07/mosca-manual-static-analysis-tool-to-find-bugs/” (2019). In: *Mosca – Manual Static Analysis Tool*.
- “https://medium.com/code-fighters/bank-malware-mitigations-42ee244100bf” (2018). In: *Bank malware mitigations*.
- “https://medium.com/code-fighters/firefox-tunnel-to-bypass-any-firewall-bc6f8b432980” (2018). In: *Firefox tunnel to bypass any firewall*.
- “https://hackaday.com/2017/08/13/complete-ir-control/” (2017). In: *Hack any TV remote control*.
- “blog.conviso.com.br/criando-seu-proprio-sistema-anti-spam/” (2016). In: *Improving spam detection with automatons*.
- “https://www.darknet.org.uk/2016/10/raptor-waf-c-based-web-application-firewall/” (2016). In: *Raptor WAF*.

Presentations in conferences

- https://pt.slideshare.net/antoniocooler/burlando-waf-20 (2015). “TDC Sao paulo - Bypass WAF”. in: *TDC SP*.
- https://pt.slideshare.net/antoniocooler/0d1n (2014). “Bsides Sao paulo - od1n web hacking tool”. In: *Bsides SP*.
- http://www.softwarelivre.gov.br/eventos/seminarios-tecnologicos-seguranca-da-informacao (2014). “TDC Sao paulo - the developers conference - Development Pitfalls”. In: *TDC SP*.
- – (2013). “Seminário Tecnológico de Segurança da Informação - Automação para o web hacking”. In: *SERPRO GOV*.
- https://pt.slideshare.net/antoniocooler/vivendo-de-hacking (2012). “Semana da computação - Vivendo do hacking”. In: *UNASP*.
- https://pt.slideshare.net/conviso/web-spiders-automao-para-web-hacking (2012). “Automação para o web hacking”. In: *OWASP Floripanopolis*.
- https://pt.slideshare.net/antoniocooler/detector-de-ladro-com-laser (2011). “Detector de ladrão usando laser”. In: *YSTS*.

TECHNICAL SKILLS

- Skill full in Penetration Testing and Secure Code Review.
- Great experience in Operating System, Network Administration and programming.
- Great experience to problem solving, full skill how to automate just about anything.
- Great experience to low level programming, like develop drivers and kernel solutions.

DBMS SKILLS

SQLite
Postgre
Redis
MySQL
MongoDB
CouchDB
SQL server

UI SKILLS

GTK
QT
WxWidgets
X11
WinAPI

RED TEAM SKILLS

- UAC bypass
- DACL evasion
- Bypass firewalls
- Bypass AV
- Simulate DoS threat
- API Hookings
- RootKit creation
- form grabbing
- Persistence
- Screenlogger testing
- Keylogger os
- Phishing ops
- Pharming ops
- Drop spread
- Packing obfuscation etc
- Fuzzing

CURRENT STUDY

- Python (Django + SQLalchemy)
- Rust Programming (Rocket+Diesel)
- Linux kernel resources to create drivers
- Follow OpenBSD sources commits etc
- RaspBerry PI other ARMs
- AWS Solutions/ GPC and attack vectors
- follow hackaday articles
- MQL metatrader query language to automate trading
- NLP to classify texts

OPEN SOURCE PROJECTS

- HiddenWall is a Linux kernel module generator for custom rules with netfilter. (block ports, Hidden mode, rootkit functions etc). The motivation: on bad situation, attacker can put your iptables/ufw to fall... but if you have HiddenWall, the attacker will not find the hidden kernel module that block external access, because have a hook to netfilter on kernel land(think like a second layer for firewall) https://github.com/CoolerVoid/HiddenWall.
- OctopusWAF is a open source Web application firewall, is made in C language uses libevent to make multiple connections. Event-driven architecture is optimized for a large number of parallel connections (keep-alive) which is important for high performance AJAX applications. This tool is very light, you can deploy in any please, this resource turn perfect to protect specific endpoint that need a custom protection. https://github.com/CoolerVoid/OctopusWAF
- 0d1n is a Open Source web application bruteforcer and Fuzzer. If your objective is automate exhaustive tests and search for anomalies (read vulnerabilities) 0d1n can increase your productivity following web parameters, files, directories, forms and other things. https://github.com/CoolerVoid/0d1n
- Raptor is a Web application firewall made in C language, uses Horspool, karprabin or DFA to match and block SQL injection, Cross site scripting and path traversal attacks. https://github.com/CoolerVoid/raptor_waf
- strcmp() function implementation with intel's SSE 4.2 instruction faster than original C strcmp() becauses uses SIMD with 128bit registers. https://github.com/CoolerVoid/cooler_sse42_strcmp
- libFastKNN is a C++ library of k-nearest neighbors algorithm (k-NN), faster because uses Armadillo lib, in k-NN classification, the output is a class membership. An object is classified by a majority vote of its neighbors, with the object being assigned to the class most common among its k nearest neighbors (k is a positive integer, typically small). If k = 1, then the object is simply assigned to the class of that single nearest neighbor. https://github.com/CoolerVoid/libfast_knn
- OptionsCat is a web server in C language using mongoose with web sockets(wss), have functions like european options tool, compound calc, finance manager for traders... uses the Black-Scholes model for calculating the premium of an option. https://github.com/CoolerVoid/optionscat
- Heap detective, tool to tokenize C++ code and use taint analysis to search memory pitfalls like UAF and memory leaks. https://github.com/CoolerVoid/heap_detective
- Nozes is a Pentest cmd manager. You can automate and save your pentest attacks in one click. Uses PHP with SQLite at background... look that following https://github.com/CoolerVoid/nozes
- libTextBayes a c++ library to help detect spam in text content using machine learning.
- Thread pool library for C language. https://github.com/CoolerVoid/tombpool
- Port Knocking technique for shell with AES256-GCM https://github.com/CoolerVoid/ninja$_shell$
- AritEval Arithmetic expression evaluator for C language with anti-integer-overflow resources https://github.com/CoolerVoid/arit$_eval$
- The way to use firefox to make a tunnel to remote communication, bypass any firewall... https://github.com/CoolerVoid/firefox$_tunnel$

A DAY OF MY LIFE