

Wanderley Caloni

São Bernardo do Campo - SP - Brasil

Contact: +55 (11) 8438-5306 - wanderley@caloni.com.br

Last update: 2009-07

Purpose

Operating System Developer Specialist

Qualifications summary

Ten years experience in system software developer for Windows platform.

Previous jobs

2008 -- Current SCUA Information Security
System Developer and Project Coordinator

2005 -- 2008 Open Communications Security
System Developer and Threats Analyst

2000 -- 2005 SCUA Segurança da Informação
User Interface Developer and System Developer

Graduation

Graduate - Network Architecture - IBTA - 2005/2008

English: Intermediate

Russian: Beginner

Skills

C++ Programming (Great) - 10 years

Windows system development (Great) - 8 years

Projects coordination (Good) - 6 months

Team participating and communication skills (Great)

Capacitation

Ten years experience in Windows operating systems developing in information security companies; great team relationship; problem solving using systemic vision, knowledge bases maintenance, chronograms and people coordination.

Technical historic

Software and hardware inventory
Clipboard and PrintScreen protection using windows hooks and global messages manipulation
Driver writing system event log
DeviceIoControl user/kernel communication
Desktop remote control using VNC technique
Remote execution tool PsExec (SysInternals) like
Print control using regex (Boost) and shell hook
Access policies management during user logon/logoff (register and hooks)
Datgabase migration CTree -> SQL (OLE classes)
Windows authentication using custom GINA and DCOM; Credential Provider (Vista)
CTree database synchronism using custom DCOM service
Bootable Linux CD with bash scripts and disk cryptography tools using C language
Hard disk encryption and PenDrive (USB) storage control
Blue Screen analysis using memory dumps and WinDbg live (Gflags)
System account execution using custom COM service
MBR (Master Boot Record) customization library
Blowfish/SHA-1 encryption library using C++ and 16 bits Assembly
Log access driver using shared memory between user and kernel mode
Kernel mode API hook for 9X and NT platforms
16 bits Assembly loader; debugging using debug.com tool
Executable protection using embedded domain authentication recorded inside files resources
Internet Explorer 6/7 and Firefox 1/2 browsing protection using Assembly 32 bits code injection
Code, strings and execution protection library (using Win32 interruptions)
Centralized log generation library using shared memory and global events
Internet Explorer 6/7 BHO (Broser Helper Object) and ActiveX; Mozilla/Firefox XPI plugin
Projects management using Source Safe, Bazaar and Batch (Win) scripts
Kernel mode debugging using SoftIce and WinDbg for NT platform, SoftIce and WDeb98 for 9X platform
Trojans reverse engineering (C++, Visual Basic, Delphi) using WinDbg and IDA
Diagnostic tool listing files, services, drivers, register, disk partitions, processes, etc
Jobs monitoring in Win2000+ to installation and update control
Application use monitoring using noninvasive and invasive windows hooks
Houaiss reverse engineering and Babylon importation (dictionaries)
Build control with Cruise Control .NET, symbol server with Debugging Tools
Projects documentation using Doxygen and Wiki (Trac)
Management interfaces using C++ Builder 5/6 and Visual C++ custom libraries
E-mails analyzer using regular expressions (ATL classes)
Configuration interfaces using Visual C++ (MFC /ATL/WTL)
Project and tracing analysis using regular expressions (Vim and Grep)
Articles development using technical blog and Code Project community.

Articles

Antidebug: interpretation exception based
BIOS debugging using SoftIce 16 bits
Loading arbitrary DLLs using WinDbg
Analysing dumps with WinDbg and IDA

RmThread - Code execution in Another Process Context
Function Overload by Return
Windows Jobs with Completion Port

Lectures

CPP ISO Threads
Portability Nuts and Bolts