

Wanderley Caloni

São Bernardo do Campo - SP

Contato: (11) 8438-5306 - wanderley@caloni.com.br

Última atualização: Jul/2009

Objetivo

Desenvolvedor especializado em sistemas operacionais

Resumo das qualificações

Desenvolvedor de software de sistema em plataforma Windows com dez anos de experiência no mercado.

Empregos anteriores

2008 -- Atual SCUA Information Security

Desenvolvedor de Sistemas e Coordenador de Projetos

2005 -- 2008 Open Communications Security

Desenvolvedor de Sistemas e Analista de Ameaças

2000 -- 2005 SCUA Segurança da Informação

Desenvolvedor de Interface com Usuário e de Sistemas

Graduação

Superior Completo - Arquitetura de Redes - IBTA - 2005/2008

Inglês: Intermediário

Russo: Iniciante

Habilidades

Programação em C/C++ (Ótimo) - 10 anos

Desenvolvimento de sistemas Windows (Ótimo) - 8 anos

Coordenação de projetos (Bom) - 6 meses

Comunicação e participação em equipes (Ótimo)

Capacitação

Experiência de 10 anos em sistemas Windows com atuação em empresas de segurança da informação, ótimo relacionamento em equipe, visão sistêmica de solução de problemas, mantenedor de bases de conhecimento, coordenação de pessoas e cronogramas.

Histórico técnico

Inventário de hardware (WMI/SMBIOS) e software (registro)
Proteção da área de transferência e PrintScreen através de hook de janelas e manipulação de mensagens globais
Escrita de alertas no log de eventos do sistema através de drivers
Comunicação user/kernel mode através de DeviceIoControl
Acesso remoto de desktop através de ferramenta similar ao VNC
Ferramenta de execução remota similar ao PsExec
Controle de impressão de documentos através de regex (Boost) usando hook do Shell
Gerenciamento de diretivas de acesso do sistema durante logon e logoff de usuários (registro e hooks)
Migração de base de dados CTree para SQL (classes OLE)
Autenticação Windows com serviço DCOM e GINA customizada ou Credential Provider (Vista)
Sincronismo remoto de base de dados CTree usando serviço DCOM
CD Linux bootável com scripts bash e ferramentas de criptografia de discos em linguagem C
Driver de criptografia de discos rígidos e armazenamento USB (PenDrives)
Análise de telas azuis ou dumps de memória usando WinDbg
Serviço COM de execução de aplicativos na conta de sistema
Customização da MBR (Master Boot Record) de acordo com características da BIOS
Biblioteca de criptografia Blowfish e SHA-1 em C++ e Assembly 16 bits
Driver de auditoria de acesso com memória compartilhada e eventos entre user e kernel
Hook de API em kernel mode para plataformas NT e 9X
Carregador de boot em Assembly 16 bits; depuração usando Debug.com
Proteção de executáveis através de autenticação em domínio configurado no resource dos arquivos
DLL de proteção à navegação em Internet Explorer 6/7 e Firefox 1/2 com injeção de código
Assembly 32 bits
Biblioteca de proteção de código, strings e execução monitorada; uso de interrupções Win32
Biblioteca de geração de log centralizado através de memória mapeada e eventos globais
BHO (Browser Helper Object) e ActiveX para Internet Explorer 6/7 e plugin XPI para Mozilla/Firefox
Gerenciamento de projetos com Source Safe, Bazaar e scripts Batch
Depuração de kernel mode em plataforma NT usando SoftIce e WinDbg, em 9X usando SoftIce e WDeb98
Engenharia reversa de trojans feitos em C++, Visual Basic e Delphi usando WinDbg e IDA
Ferramenta de diagnóstico que lista arquivos, serviços, drivers, registro, partições, processos, etc da máquina
Monitoramento de jobs em Windows 2000+ para controle de instalação e atualização de produtos
Monitoramento da frequência de uso de aplicações usando hook de janelas invasiva e não-invasiva
Engenharia reversa do dicionário Houaiss e importação para o formato Babylon
Controle de build com Cruise Control .NET, servidor de símbolos com Debugging Tools for Windows
Documentação de projetos através de Doxygen e Wiki (Trac)
Interfaces de gerenciamento em C++ Builder 5/6 e bibliotecas Visual C++
Analisador de e-mails usando expressões regulares (ATL)
Interfaces de análise em Visual C++ (MFC /ATL/WTL)
Análise de logs e edição global de projetos utilizando regular expressions
Desenvolvimento de artigos através de blogue técnico e comunidade Code Project

Artigos relevantes

Antidebug: interpretação baseada em exceção
Debug da BIOS com o SoftIce 16 bits
Carregando DLLs arbitrárias pelo WinDbg
Analisando dumps com WinDbg e IDA
RmThread - Code execution in Another Process Context
Function Overload by Return
Windows Jobs com Completion Port

Palestras

Threads no CPP ISO
Dicas e Truques de Portabilidade