# Vault 7: CIA Hacking Tools Revealed

Releases ▼ Documents ▼

Navigation:

## Directory

Departments / Branches / Groups

### Embedded Development Branch (EDB)

- USB Emulation Evaluation
- 2014-01-09 Retrospective for SparrowHawk 2.0 orig
- Hive *empty*
- Pterodactyl Tips
- SQRL
- 2013-04-16 - Meeting Notes
- EDB Home *incomplete*
    - Virtualized Development / Test Environment
    - How-To Articles
        - EFI/UEFI Information
            - EFI Program Testing Considerations
            - Setting Up a Linux Build Environment for EFI
            - ExitBootServices Hooking
            - Active EFI/UEFI Projects
            - EFI Basics: NVRAM Variables
            - EDK2 Compiler Information and CI Concerns
        - Cross-compile for Linux/TILE-GX
        - Use the EDB Domain Server on DEVLAN
        - Building PolarSSL for Solaris x86 and SPARC
        - Create a Solaris Boot Server for a Subnetwork
        - Use the Solaris Automated Install Server
        - Enable debug output on PolarSSL
        - Triage SOHO device
    - Projects
        - DerStarke
            - Updating DerStarke v1.4 to Yosemite
            - Creating new Unlock files future firmwares

            - Hive
            - Sparrowhawk
            - MaddeningWhispers
            - BaldEagle
            - Bee Sting - Proxy with iFrame injection
        - Development Devices and Hosts
            - Working with MikroTik RouterOS 6.X
            - IBM AIX Power7 740 PowerPC PPC 64-bit
        - Mission and Vision Statement
        - Meeting Notes
            - 2014-10-23 Branch Direction Meeting notes
        - Future Project Ideas
        - Embedded Devices Order Status
        - Retrospectives
            - 2014-01-09 Retrospective for Sparrowhawk
        - Product Requirements
            - Pterodactyl Requirements
        - Personnel
        - Small Routers

**Remote Development Branch (RDB)**

- Personnel
- RDB Home
    - Personnel
    - Including 3rd party python libraries for DART remote testing
    - Mission and Vision Statement
    - Umbrage *empty*
        - PIQUE Assessments *empty*
        - Hacking Team Source Dump Map
        - Component Library
            - Data Collection
                - Webcam Capture
                - Windows API Keyloggers
                - DirectInput Keylogger
                - SetWindowsHookEx WH_KEYBOARD and WH_KEYBOARD_LL Key Logger
                - Internet Explorer Password Collection
            - Privilege Escalation

- Elevated COM Object UAC Bypass (WIN 7)
- Data Destruction
  - Wiped Locked Files
- Persistence
  - Image File Execution Options
  - Windows FAX DLL Injection
  - Shell Extension Persistence
  - OCI.DLL Service Persistence
  - VBR Persistence
- Kernel Land
  - Kernel to User land: APC injection
- PSP/Debugger/RE Avoidance
  - Run Out The Clock (PSP Avoidance)
  - Anti-Sandboxing: Wait for Mouse Click
  - Process Hollowing
  - Debug Print Debugger Detection
  - API Memcpy
  - MBR File Handle
- Stealth
  - DLL Injection using SetWindowsHookEx
  - CreateRemoteThread DLL Injection
  - Kaspersky "heapgrd" DLL Inject

- ShoulderSurfer
- Reforge
  - Reforge bytecode specification
  - Archive Grammer notes
- Projects

**Operational Support Branch (OSB)**

- Duqu 2.0 Kaspersky Write-Up
- Time Stomper *empty*
- Munge Payload *empty*
- Fight Club *empty*
- Rain Maker Temp User Guide
- Rain Maker Version Archive *empty*
- System Monitoring and Manipulation *SECRET*
- Dancefloor - Linux *empty*
- Jukebox - Mac *empty*

- Jukebox - Mac
- Bartender - Windows *empty*
- Margarita v1.6 User Guide
- OSBTest
- OSB Home
  - Retrospectives
  - Personnel
    - Mission and Vision Statement *empty*
  - New Developer Exercises *SECRET*
    - 3. Visual Studio *SECRET*
    - 10. Verbiage and Acronyms *SECRET*
    - 11. Issues and Documentation *SECRET*
    - 12. Bonus: Capture The Flag *SECRET*
    - 2. Source Control *SECRET*
      - OSB Workflow In Git
    - 9. Tradecraft
    - 8. Bamboo And Dart *SECRET*
    - 4. Introduction to Win32 Programming. *SECRET*
    - 5. Win32 Programming Gotchas *SECRET*
    - 6. Basic Forensics *SECRET*
    - 7. The Art of Unit Tests *SECRET*
    - 1. Setting Up Your Development Environment. *SECRET*
  - OSB's ESXi Server
    - Shellterm 2.10 Test Server *SECRET*
    - Shellterm v3.0.1 Test Server *SECRET*
  - 2015 Top bits
  - Payload Deployment Unit Tests Issue Tracker *SECRET*
  - Projects
    - HyenasHurdle BSOD
    - Flash Bang *SECRET*
      - Flash Bang Supporting Documents *empty*
      - Flash Bang v1.1 (Current Version) *SECRET*
      - Flash Bang Archived Versions *empty*
        - Flash Bang v1.0 *SECRET*
    - Magical Mutt *SECRET*
      - Magical Mutt v1.0 *SECRET*
        - Magical Mutt v1.0 Sprint 2 Retrospective 2016-02-24

        - Magical Mutt v1.0 Sprint 1 Retrospective 2016-02-16
- Melomy DriveIn *SECRET*
    - Melomy DriveIn v1.0 *SECRET*
- RickyBobby *SECRET*
    - RickyBobby Automated Testing
- Fight Club *SECRET*
    - Fight Club Archived Versions *empty*
        - Fight Club v1.0 *SECRET*
    - Fight Club Supporting Documents *empty*
    - Fight Club v1.1 (Current Version) *SECRET*
- Taxman
- Rain Maker *SECRET*
    - Rain Maker Supporting Documents
        - Rain Maker v1.0 Developer Notes *SECRET*
        - Rain Maker v1.0 User Guide
        - Rain Maker v1.0 Unclassified User Guide
    - Rain Maker v1.0 (Current Version) *SECRET*
    - Rain Maker Archived Versions
- Improvise
    - User Guide *empty*
    - Developer Guide *empty*
- Basic Bit *SECRET*
    - Basic Bit v1.1 *SECRET*
    - Basic Bit Archived Versions
        - Basic Bit v1.0 *SECRET*
- ConnectifyMe Research *SECRET*
- Fine Dining
    - Fine Dining (Case Officer Toolset) Concepts
    - Infector Config XML Schema
    - Fine Dining Tool Module Lists
        - Thunderbird Portable DLL Hijack
        - Chrome Portable DLL Hijack
        - LBreakout2 Game Portable DLL Hijack
        - 2048 Game DLL Hijack
        - FoxitReader Portable DLL Hijack
        - Sophos Virus Removal Tool DLL Hijack

                    - Kaspersky TDSS Killer Portable DLL Hijack
                    - ClamWin Portable DLL Hijack
                    - Iperius Backup DLL Hijack
                    - OperaMail DLL Hijack
                    - Sandisk Secure Access v2 DLL Hijack
                    - LibreOffice Portable DLL Hijack
                    - BabelPad Portable Hijack
                    - Notepad++ DLL Hijack
                    - McAfee Stinger Portable DLL Hijack
                    - Skype Portable DLL Hijack
                    - Opera Portable DLL Hijack
                - Fine Dining Process, Training, and Approval *empty*
            - HammerDrill v2.0 *SECRET*
                - HammerDrill v2.0 Developer Notes *SECRET*
        - How-to articles
            - Doxygen Documentation
        - OSB Passwords *SECRET*
        - Helpful Tools
            - Time Stomper *SECRET*
            - Munge Payload *SECRET*
            - Error Munger *SECRET*

**Mobile Development Branch (MDB)**

- MDB Home
    - Projects *empty*
        - Tomahawk
    - Personnel
    - Mission and Vision Statement

**Automated Implant Branch (AIB)**

- Frog Prince Releases
- User Guide *empty*
- Grasshopper Requirements
- Tools *empty*
- AIB Home
    - Personnel
    - Mission and Vision Statement *empty*
    - Projects
        - CandyMountain *empty*

- CandyMountain
    - CandyMountain Releases
- Grasshopper *empty*
    - Grasshopper Design
    - Grasshopper OS/PSP Characterization
    - Grasshopper Developer Guide
    - Grasshopper Releases
    - Grasshopper Persistence Techniques
- MagicVikings *empty*
    - MagicVikings Releases
- AntHill
    - AntHill 2.0
- Galleon
    - The Seven Seas Transport
- Assassin *empty*
    - Assassin Design *empty*
    - Assassin Releases
- HercBeetle
- Frog Prince
    - Frog Prince Execute Command Test
    - Frog Prince Set Command
    - Frog Prince Put Command Test
    - Frog Prince Install Test
    - Frog Prince Memory Load Command
    - Frog Prince Get Command Test
    - Frog Prince De-Install Tests
    - Frog Prince Memory Unload Command
- Hornet *empty*
    - Hornet Releases
- The Gibson
    - Queue
    - Queue Tar File Format
    - Queue Proxy
        - Proxy JSON Outputs
- Cascade
    - MacAfee Virus Scan blocking injection into svchost
    - ESET firewall blocking for udp, tcp, and icmp

- Caterpillar
    - Post Processor Redesign
    - Caterpillar Releases
    - Test PCAPs
- Project Requirements *empty*
    - Medusa v2.0 *empty*
        - Port Existing Collide-Compatible Tasker to Generic Python Application
- File lists
- Product Requirements

**Network Devices Branch (NDB)**

- asdf *empty*
- DNS Checkin - BIND
- Perseus Testing Status
- JIRA reports
- vSphere Web Client Slow to Open Consoles
- VMware - Workaround for OVF Deployment Failed
- Configure Wireshark on Ubuntu
- test *empty*
- User #71462's Task List
- What is User #71490's nickname going to be?
- Decision log
- NetApp FAS2552 Layout
- File lists
- Network Devices Branch
    - Meeting notes
    - Archive *empty*
    - Test Range Notes
        - PackGen Issue with 32-bit Libraries [Xetron]
        - Create new NDB custom JIRA project
        - Cloning a VM Checklist - Linux
            - Install Fluxwire v2.3
        - COG ICON VM Modifications
        - New Test Preparation Checklist
        - Listening Post (LP) Creation
        - NS1 - DNS (BIND) Server
        - NS2 - DNS (BIND) Server

  - Setup Ubuntu Web Server for HTTPS
  - RSPAN with VMware
  - How to Create a New swindle.crt file for Blot [Xetron]
  - CentOS 6.6 VM (Blot)
  - Ubuntu Base VM Configuration
  - CT - ICON1
- Tool Quick Start Guides *empty*
  - Windex 5.3
  - Chimay Red, TinyShell, and BusyBox Quick Start Guide
- NDB Test Range Task Report
- Lab Infrastructure
  - Obselete VMs - Pruned from Inventory
  - VMware Servers
  - Console Servers
  - NDB Lab SAN Switch Port Mapping
- Lab Demonstrations
- Push-up Tracker
- Operations/Testing
  - Cannoli v2.0
    - JQJPRIZE - ASUS AC68U
    - cppcheck analysis
    - JQJCALIBAR - ZXHN-F660
  - JQJSLASHER
    - JQJSlasher - Ops Testing
  - JQJDRAGONSEED - Earl Grey
    - Earl Grey v1.0.2 cppcheck analysis
    - Earl Grey Testing
  - JQJTHRESHER
    - Aquaman-5h HG 3.3.1 - Full Test [Xetron]
    - JQJTHRESHER Command Notes
    - Aquaman-5h Test Notes ***TOP SECRET*** [Xetron]
    - Aquaman-5h-Without-Snooping Test Notes [Xetron]
  - New Operation Requirements
  - JQJSTEPCHILD *empty*
    - JQJSTEPCHILD - Op2
    - JQJSTEPCHILD - Op1
  - Perseus *empty*

- Perseus
    - Perseus 1.1.0b1 (Beta 1)
        - Perseus 1.1.0b1 Mikrotik RB450G - Test 2 Notes
        - Perseus 1.1.0b1 Mikrotik RB493G - Test 1 Notes
    - Perseus 1.1.0
        - DUT5 - x86 VM - Notes
        - DUT2 - RB450G - General Info
            - Baseline Resource Measurements
            - Test Notes
        - DUT4 - RB1100AH - v1.1.0 Notes
        - DUT1 - RB493G - Notes
        - DUT3 - RB450G - Long Term Test
    - Perseus 1.3.0 *empty*
        - DUT6 - RB800 - v1.3.0 Notes
    - Perseus 1.2.0
        - DUT6 - RB800 - v1.2.0 Notes
        - DUT4 - RB1100AH - v1.2.0 Notes
- MikroTik
    - MikroTik Hotspot / Paywall Analysis
- JQJSECONDCUT
    - Cinnamon 5.0.1 cppcheck analysis
    - Cinnamon Cisco881 Testing [Xetron]
- Bumble
    - Bumble - Device Configuration
    - Bumble 3.1 Test Notes
    - Config Explanation
    - HP CLI Cheatsheet
    - Bumble 3.2.1 Test Notes
    - Bumble Test Timeline
    - Bumble 3.0.0/3.1Beta Test Notes
    - HP MSR Performance Baseline *empty*
- JQJFIRESHOT *empty*
    - BuzFuz Testing
        - Testing Notes
- JQJHAIRPIECE
    - JQJHAIRPIECE - HG Testing [Xetron]
    - JQJHAIRPIECE - ROCEM TESTING [Xetron]

  - JQJDISRUPT - WAG200G
  - JQJADVERSE
    - Powerman-1r Testing [Xetron]
    - HG v3.1.3-Adverse-01 Testing [Xetron]
    - ROCEM v1.2-Adverse-1r Testing [Xetron]
  - Felix *empty*
    - Felix v1.0 Test Notes
    - Felix Automation Test Coverage
    - Build Felix LP
    - Felix 1.1 Test Notes - MikroTik MIPS-BE
  - Cytolysis [Xetron]
    - Cytolysis CONOP Notes [Xetron]
    - Cytolysis-1h HG v3.1.6 Delivery
    - Cytolysis-1h Testing [Xetron]
    - Cytolysis-1h HG v3.1.6 Test Plan [Xetron]
  - Felix v1.0
- Test Range Infrastructure
  - Network *empty*
    - VTP Configuration
  - Training *empty*
    - HunGrrr Training
  - Storage *empty*
    - NetApp FAS2552 Layout
    - NetApp Build Document
    - Test Range NetApp Licenses
  - Servers *empty*
    - Active Directory / DHCP / DNS
    - Authenticate vCenter with AD
    - RANCID - Test Range
    - vRealize Orchestrator
    - Solarwinds
    - AAA Server
    - vRealize Operations Manager
  - IXIA
- Lab Notes
  - Asterisk Service Run Level

            - BIND (DNS) Server
            - PowerShell Notes
            - Configure SNMP for ESXi
            - Ubuntu Server VM Template Creation Checklist
            - RANCID - NDB Lab
        - How-to articles
            - TC Qdisk network delay
            - Setup Fluxwire v3.3
            - SOHO Triage
            - Add vCenter Tester Account With Limited Permissions
            - Install ia32-libs on Debian 8.1

**Technical Advisory Council (TAC)**

- Technical Advisory Council (TAC)
    - Discussion Corner
        - What did Equation do wrong, and how can we avoid doing the same?
        - Maslow's Hierarchy of Code Review
    - Meeting Minutes *empty*
    - Charter *empty*
    - Topics *empty*

**CCI Europe Engineering**

- CCI Europe Engineering
    - EDG Familiarization TDY

## Projects

**JQJHENDRICK**

- JQJHENDRICK
- JQJHENDRICK Home

**Improvise**

- IMPROVISE
    - 2. User Guide *empty*
    - 1. Project Status *empty*
    - 3. Developer Guide *empty*
- IMPROVISE Home

**GreenPacket**

- HTTP
- HTTP Tunnel
- GreenPacket Home

**Philosoraptor**

**Marble Framework**

**Kraken**

- Retrospectives
  - 2015-12-29 Retrospective
  - 2016-02-16 Retrospective
  - 2015-11-09 Retrospective

**Tremor**

- TREMOR_Docs
  - Tremor Weekly Report
    - 2015-12-11 Meeting notes
  - Getting started
    - Making a template
  - Meeting notes
  - File lists
  - TREMOR Archive

## Operating Systems / Platforms

**iOS**

- HACKME
- iOS
  - Analyzing a New Shared Cache With PensiveTrace 1.5.1
  - NGINX proxy/redirector
  - ARM64 Addressing Modes
  - NightSkies/Mcnugget iOS version support matrix
  - Device Out of Space?
  - iOS Builds
  - Hamr Testing With WildTurkey
  - Reflash Device Procedure *TOP SECRET*
    - Reflash Log *CONFIDENTIAL*
    - Reflash iOS Device
  - iOS Exploits [NSA] [FBI] [GCHQ] [MI5]
  - Ghidra
  - DTO Logging
  - Captive Portal
  - SOT RAM Size Per Model
  - Pairing Records
  - SMG
  - Rebooter Testing Herd
  - How-to articles

  - iOS Debugging
  - Create New Repository (Project)
- Workshops
  - TRICLOPS FALL 2014
  - Workshop Stuff
  - (TS//SI//REL US, UK, CAN) TRICLOPS Summer 2015 - Ottawa
- Design Notes
  - Bootstrapper (FURTIVESYRINGE) Design
- Devices On Loan
- iPad Air 2 and iPhone 4 Devices
- File Lists
  - Releases
- Binary Verifier
- IOS cc_fips_test cleanup
- iOS relay and web inspector
- MDF Issues
- iOS Developer Setup Guide - New Developers Click Here
  - iOS Development Process
  - Building Nightskies (crunchylimeskies)
  - Tips & Tricks
    - Random bits of knowledge
  - Generating and Installing Provisioning Profiles for Xcode
  - DRBOOM
  - End to End Nightskies 3.x Install with Poseidon
  - iOS Team Acronyms and Terms SECRET
  - Development Resources
    - PyPi
    - Homebrew
- iOS Servers
- Tools / Software Transfer Procedure
- iOS Triage Process
  - Notes from iOS 8.4.1 Triage
  - iOS Firmware Updating to latest procedure / Adding Exploit Support For New Devices
- Software Licenses
  - Sublime License
  - Omnigraffle License Keys
- SoT v 1.1 Tests

            - SOL v 1.1 Test Results
        - MCNUGGET
            - Mcnugget 3 QuickRef
            - Mcnugget Test Checklist
            - EVE_EARTH String Obfuscation
            - pycrypto
            - Testing Different Network Connectivity States Using Network Link Conditioner
        - Research *empty*
            - iOS 9 Research
            - IOKit
            - Unactivated Device Exploit Research
            - iOS 8 Research
            - Reverse Engineering
            - User Agent samples
        - Interesting Files on Devices

**MacOS X**

- Ghidra 6.0.10 on OSX/El Capitan
- Nope
    - Mach-O Symbol and Entitlement Tools
    - OS X Security Product Paths
    - Enabling OS X Updates on Devlan
    - Making Make Suck Less
    - Mac OS Kernel Debugging
    - Why POSIX Daemonization is Complicated
    - OS X Kext Development Tips
    - OS X NetInstall Images

**Mac**

- Mac Development
    - How-To Articles
    - Write to protected directories by using filenames in rootless_whitelist
    - Troubleshooting articles
    - SDK-Based Development
    - VMWare Fusion Keys
    - OSX 10.11 El Capitan Changes
- Mac Development Home

**Android**

- Android
  - General Android Info, Tips and Tricks *empty*
    - adb shell commands
    - Android USB reverse tethering
    - selinux
    - Installing APK
  - Hamrtoe Test Harness
  - MDB Coding Convesions *empty*
    - Python Coding Conventions
    - C Coding Conventions
  - Lab Configuration
    - Simulating Packet Delay / Dropped Packets
    - NGinx Redirector Configuration
  - Getting started
    - Making a template
  - RoidRage
    - RoidRage Bootstrap Methods
      - RoidRage Debuggerd Startup (kitkat)
      - Sysmon Startup Method
      - RoidRage Debuggerd Startup (ICS/JB)
    - Anger Management / RoidRage ICD
  - Droid Bamboo Agent
  - Mobile Tiger MDB
  - Remote Debugging Chrome On Android
  - AngerManagement
    - AngerManagement_Legacy
    - AMSupported
  - Compiling Busybox for android
  - Operations Support
    - JQJGUNSHY: Samsung Galaxy Tab 2 GT-P3100
    - HeliosYolo
    - JQJGUNSHY: how to build tools
    - Current Ops Requests
  - Android Exploits and Techniques [NSA] [FBI] [GCHQ] [MI5]
    - Cobalt
    - Remote Code Execution (RCE) Exploits - Helios

      - Flameskimmer (FS2) Porting
      - BaronSamedi
      - Chronos
    - Spottsroide Development Setup
    - New Developers Guide for MDB
    - How-to articles
      - Configuring the Font for the sidebar in Sublime
    - Android Developer Setup
      - MDB DNS Entries
      - Using Poseidon and the NSX LP (used for NightSkies and RoidRage)
  - Android Home

**Linux**

- Linux Home
  - How-to articles
  - SSH PortForwarding
  - Key-Based SSH Login
  - Install WANem to hard drive
  - CactiEZ Syslog Fix
  - Install Ubuntu on Mac Hardware
  - Wireshark on Ubuntu
  - Create Squid Proxy Server

**VMware**

- VMware
  - Modify Web Client Timeout
  - Workaround for OVF Deployment Failed
  - Enable Copy/Paste for VMs
  - How-to articles
  - vSphere Web Client Slow to Open VM Consoles

## Development / Tools

**Git Distributed Version Control**

- Git Distributed Version Control Home
  - How-to articles
    - Remove Binary Files from a Git Repository
    - Use Git Submodules to Manage Libraries
    - Creating an empty commit in a new project
    - Merge Git Repositories?

            - Convert a Mercurial Repository to Git on Windows
            - Change Author Details of All Commits in a Git Repository
        - Git Workflows
        - Git Tutorials
            - Git For Visual Studio Users
        - Git Tools
            - Repo
        - Git Reference
        - Git Tips & Tricks

**Playground**

- Funny Code 2013a
- User #71474's Wiki Page
- Diagram
- Git Tutorials
- Playground Home
    - Testing how to make a decision
    - Decision log
    - 2015-11-09 Retrospective
    - Retrospectives

**Collaboration and Partnership**

- Collaboration and Partnership Efforts
    - NERDS (Networking, Engineering, Research, and Development Symposium)
        - Past Presentations

**AED Development Tradecraft**

- Port windows-based Medusa builder to Linux/python
- Product Requirements
- AED Development Tradecraft Home
    - Development Tradecraft DOs and DON'Ts *SECRET*
    - AED Development Workflow
        - Code Review
        - Delivery & Deployment
        - Integration & Acceptance Testing
        - Project Planning
        - Documentation
        - Developer Testing
        - Source Control

    - Persistent storage option
    - Specific Tradecraft Techniques
        - Detecting and Bypassing Personal Security Products (PSPs)
            - AVG Fake Installer Trick
            - AVG Catches a Payload Dropped to Disk and Launched via Link File Well After Execution SECRET
            - Bitdefender Resource Defeat
            - PSPs vs. DLL Injection SECRET
            - Rising Thinks You're Signed
            - F-Secure Entropy Defeat
            - Comodo 6.X Gaping Hole of DOOM
            - Avira Entropy Defeat
            - Comodo Recycle Bin Defeat
            - Anti-Sandboxing: Wait for Mouse Click
        - Process Enumeration
            - WMI Process Watcher

**DNS Resolvers**

- DNS Resolvers Home

**EDG Tools of the Trade**

- EDG Tools of the Trade Home
    - SourceTree
    - Sublime Text
        - anaconda_sublime
        - DashDoc
    - Make
    - VMWare Fusion Professional
    - 010 Editor
        - Compound File Binary File Format Template (Microsoft Office Word)
        - SweetScape Binary Template Archive
        - Link File Template
    - VMware Workstation
    - KMS Keys
    - Docker
    - Cuckoo Sandbox
    - Google Mock
    - Vim
        - Vimrc Tips
        - Vim Editing Tips

        - Vim Editing Tips
    - Winhex
    - Ghidra
    - Dia
    - Visual Assist
    - Google Test Library
    - Incandescent Mind

**EDG Tricks of the Trade**

- EDG Tricks of the Trade Home
    - Creating a Winshell Test Environment
    - How-To Articles
        - Updating the Windows Symbol share via the Internet
        - Debugging a VMWare Guest
        - Grab Windows Symbols From The Share
        - How-To: Configure a non-domain-joined Windows workstation to use DevLAN's WSUS (Windows Server Update Services) host
    - Shell Scripting Tricks
    - Strings-GUI: A quick and easy way for Windows developers to examine strings, in binaries for delivery (without even launching CMD!)
    - How-To: Install old versions of the .NET Framework on Windows 8.1

**DEVLAN Resources**

- Internet Relay Chat
- DEVLAN Resources
    - Partial OpenBSD Mirror
    - Chrome Plugins
    - DEVLAN Domain Controller Certificate Authority
    - Internet Relay Chat (IRC)
    - Solaris Automated Install Server
    - Linux Package Repository Mirrors setup
    - Old Wiki

**DART**

- Watch For PSP Popups
- Dart Home
    - How-to articles
        - Throw GoogleTest Executables Against Dart via Bamboo (Alternatively, How to Stop Testing on User #1179751's Build Agents)
        - Remote Commit to a New Tyrant Server

            - Run GoogleTest Executables in DART (The Easy Way)
            - Manually Add a Computer to Tyrant
            - How to click controls
            - Get database information about VM's (or fun with db_admin)
            - Check for PSP Detection
            - How to click controls and send text, alternate method
            - Making life less painful with PyCharm
        - DART Resource Naming Standards
        - Common Issues
        - Client functions of DART listing
        - Getting Started with DART
            - How to DART your executable
            - What is What in DART
            - My First DART Test
        - Running undermine tests in PyCharm
        - Setting up new DART tester VM (Fedora 20)
        - LoggedLeaf
        - DART may be sporadically up and down this afternoon after 2p

**NSA Tools**

- NSA Tools Home

**Knowledge Base**

- Bypassing Windows User Account Control (UAC) and ways of mitigation (GreyHatHacker.net - reddit.com/r/netsec)
- Modify ACL Code Snippet (System Volume Information - OSB Module)
- Removable Media Link File Execution (EVRemovableMediaLink_EZC - EZCheese) SECRET
- Test Files
- File lists
- Code Sample
- test troubleshooting article
- Testing A How-To Article
- Tech Topics and Techniques Knowledge Base
    - EDG Code Libraries
        - Concepts and Conventions
            - Concepts: EDG Project Wizard
            - Concepts: Git/Stash/Submodules
            - Concepts: High Level
        - Survey Library SECRET
        - Re-signature Guidelines and Signature Documentation SECRET

  - NOD In-memory Code Execution Specifications
  - NOD Kernel Execution Specification
  - CODEX Data Standard
- AED Liaison Libraries
- Multiple Platforms
  - Shellcode
    - Shellcode Database
- Windows
  - Windows Concepts SECRET
    - Opportunistic Locks SECRET
  - Interesting Microsoft Files
    - Windows Theme Files (.theme)
    - MUM Files (.mum) empty
    - Local files (.local) empty
    - PIF Files (.pif) empty
    - Autorun.inf empty
    - Control Panel Files (.cpl)
    - Desktop.ini empty
    - Windows Library Files (.library-ms)
    - Manifest files (.manifest) empty
    - NTFS Alternate Data Streams (ADS)
  - Windows symbol server
  - Component Object Model
    - CLSIDs and Junction Folders (Persistence and then some) SECRET
  - Windows Code Snippets
    - Machine Information (Windows)
      - WMI in C++ via WbemScripting
      - File Information
        - Get File Major/Minor Version Numbers (MISCFileVersion_WIN32) SECRET
      - User Information
        - Verify User is in the Administrator Group via Net User API (MISCIsUserInAdminGroup_NET) SECRET
        - Get Current User And Domain (MISCUserAndDomain_TOK) SECRET
      - Registry Information
        - Create, Delete, and Write Registry Values (MISCCreateRegistryEntries_WIN32) SECRET
      - Windows Network Adapter Information
        - Windows MAC Address Whitelisting Snippet

        - Create Process With WMI
        - Use COM to Create a 32-bit Process on 64-bit Windows (MISC32Surrogate_COM) SECRET
- Payload Deployment Modules (KB)
    - Payload Deployment Modules: On Disk Executables
        - Create Process And Choose A User To Run As Via The Task Scheduler (TaskSchedulerRun_SPKL - Speckled) SECRET
        - Create Process As Current User +Admin (CreateProcessAsUser_LEP - Leopard) SECRET
        - Create Process Using Temp Directory (LoadFromDisk_GHR - Gharial) SECRET
        - Create Process Using WMI (CreateProcessWMI_TIG - Tiger) SECRET
        - Create Process (CreateProcess_SPF - Spadefoot) SECRET
        - Create A Process Via COM Class Creation (COMLocalServerRun_SHTA - Shasta) SECRET
        - Create Process And Pipe The Results (CreateProcessPipe_GHRN - Greenhorn) SECRET
        - Create Process Via ShellExecute (ShellExecute_CRS - Chorus) SECRET
    - Payload Deployment Modules: In-Memory Dll Execution
        - Load Library From Memory (LoadLibraryFromMemory_INTD - Intradermal) SECRET
        - Load ICE Dll In-Memory (LoadICEFromMemory_INTD - Intradermal) SECRET
        - Inject Dll From Memory Into A Remote Process (InjectLibraryFromMemory_NCPT - Inception) LIAISON Releasable SECRET
        - Inject Fire and Forget Dll From Memory Into Remote Process (InjectFireAndForgetFromMemory_HYPD - Hypodermic) SECRET
        - Load Fire and Forget Dll In-Memory (LoadFireAndForgetFromMemory_INTD - Intradermal) SECRET
        - Inject Dll From Memory Into A Remote Process (InjectLibraryFromMemory_HYPD - Hypodermic) SECRET
    - Payload Deployment Modules: In-Memory Executables
    - Payload Deployment Modules: On Disk Dll Loading
        - Load Library From Disk Using Temp Directory (LoadLibraryFromDisk_CMN - Caiman) SECRET
- Windows Shortcut Files (Link Files)
    - Giraffe Link Files (MISCLinkWriter_GRF) SECRET
- Data Transfer Modules (KB)
    - Data Transfer Via Data File (DTFile_GLPH - GLYPH) SECRET
    - Transferring Data Using NTFS Alternate Data Streams (DTNtfsAds_BK - Brutal Kangaroo) SECRET
    - Transfer Data By Appending To An Existing File (DTFile_PICT - PICTOGRAM) SECRET
- Windows List Snippets
    - Windows Linked List Snippet
    - Windows Array List Snippet SECRET
- Windows Registry Snippets
- Searching

            - Memory Searching - Naive Sequence Search (MISCMemorySearch_NSS) *SECRET*
        - Windows Access Control Snippets
            - Lock and Unlock System Volume Information (MISCFolderAccessControl_SVI) *SECRET*
        - Windows Function Hooking
            - Hook Functions by Replacing References (MISCHookFunctions_RPRF_NTRN) *SECRET*
            - Hook Functions via Export Address Table (MISCHookFunctions_EAT_NTRN) *SECRET*
            - Hook Functions via Import Address Table (MISCHookFunctions_IAT_NTRN) *SECRET*
            - Hook Functions via Microsoft Detours (MISCHookFunctions_DTRS) *SECRET*
        - Privilege Escalation Modules (KB)
            - Calvary UAC Bypass (PEUCalvary_x86x64) *SECRET*
            - LinkedIn User Mode LPE (PEULinkedIn_x86x64) *SECRET*
            - Artillery UAC Bypass (PEUArtillery_x86x64) *SECRET*
            - SandWorm INF File Install (PEUSandWorm_x86x64) *SECRET*
            - LinkedOut User Mode LPE (PEULinkedOut_x86x64) *SECRET*
            - Vanguard LPE *SECRET*
    - Junction Folders *empty*
    - Windows Configuration and Logging Storage
        - Interesting Log/Data Locations *SECRET*
    - Exploitation Articles
        - UAC Bypass Articles
            - Bypassing Windows User Account Control (UAC) and ways of mitigation (GreyHatHacker.net - reddit.com/r/netsec)
    - Windows Debugging
        - WinDbg
            - WinDbg Cheat Sheet
    - Windows Registriy Information
        - CLSIDs (Class IDs)
            - CLSIDs Windows 8 Enterprise x86 Office 2013
            - CLSIDs Windows 7 Professional x86 With Office 2010
            - CLSIDs Windows 7 Ultimate SP1 x64 Office 2010
            - CLSIDs Windows 8.1 Enterprise x64 with Office 2013
        - Interesting and Useful Registry Keys
- Personal Security Products (PSPs)
    - ClamAV *SECRET*
    - Articles On Bypassing PSPs
    - Norton *SECRET*
    - Kaspersky *SECRET*

            - Kaspersky *SECRET*
            - Avira *SECRET*
            - Zone Alarm *SECRET*
            - Rising *SECRET*
            - Articles on Exploiting PSPs
            - PSP Process Names from DART
            - F-Secure *SECRET*
            - Zemana Antilogger *empty*
            - EMET (Enhanced Mitigation Experience Toolkit) *SECRET*
            - Malwarebytes Anti-Malware *SECRET*
            - Bitdefender *SECRET*
            - Panda Security *SECRET*
            - Trend Micro *SECRET*
            - ESET *SECRET*
            - Avast
            - AVG *SECRET*
            - Symantec *SECRET*
            - McAfee *SECRET*
            - Comodo *SECRET*
            - Microsoft Security Essentials *SECRET*
            - GDATA *SECRET*
    - User #71471's Knowledge Base Home

**EDG Mobile**

- EDG Mobile
    - Mobile Ops Status/Priority
    - Android Exploit/Tool Coverage
    - Shared links
        - Android
        - Aquarius Stash Project
        - MDB
            - MDB static leases
        - IOS Projects (MDB)
        - Poseidon Web Application
        - Android Projects (MDB)
    - MDB AngerManagement Op Delivery
- EDG Mobile Home

**Joint Development Workshop**

- JDW
  - JDW 18 (2015)
    - JDW 18 Lessons Learned
    - JDW 18 Results
  - JDW 19 (2016)
    - JDW 19 Planning Notes *empty*

## Users

**User #524297**

- Home
  - Engineering Log
  - Single Bus Theory
  - Idea Box

**User #71384**

- User #71384's Home
  - SSL / TLS Certificates
  - Eclipse User Notes
  - Remote Debugging with Eclipse
  - Linux ARP Options
  - Git Notes
  - MIPS Cross-compile of ngrep (open source)
  - Building Cross Compilers with Crosstool-NG

**User #1179751**

- User #1179751's Home
  - Test Page
  - New Confluence Plugins

**User #71489**

- testing
- User #71489's Home

**User #71473**

- Retrospectives
- Wait, didn't I just securely delete that file? *SECRET*
- User #71473's Home
  - File lists
  - TODO: Something *SECRET*
  - User #71472's awesome tool names page
  - HammerDrill *SECRET*

    - HammerDrill
    - User #71473 Home
      - Test Files
      - AV Defeats
        - Comodo Recycle Bin Defeat
        - F-Secure Entropy Defeat
        - Bitdefender Resource Defeat
        - Avira Entropy Defeat
        - AVG Fake Installer Trick
        - Comodo 6.X Gaping Hole of DOOM
        - List of ideas for fun and interesting ways to kill/crash a process (WreckingCrew)
- **User #71488**
  - User #71488's Home
    - SOLDER
- **User #71466**
  - User #71463's Wiki Page
    - Funny Code 2010
    - Funny Code 2014
    - Funny Code 2013
    - Funny Code 2011
    - Funny Code 2015
    - Funny Code 2009
    - Funny Code 2012
- **User #?**
  - User #?'s Home
- **User #71487**
  - User #71487's Home
- **User #?**
  - User #?'s Home
    - Strategic Projects
- **User #?**
  - User #?'s Home
    - Reading list
    - regsvr32
- **User #71484**
  - User #71484's Home
    - User #71464's Tool Name Ideas

**User #71480**

- User #71480's Home
  - Practices of an Agile Developer

**User #71475**

- User #71475's Home
  - Faces of the Internet
    - Sideways Faces
    - Multiline Faces
    - Weird right to left faces
    - One Line Faces
    - Japanese style Faces
  - Scratch pad
  - Using pyenv on devlan
  - Devlan simple pip index
  - How-to articles

**User #71476**

- User #71476.'s Home
  - Images
  - File lists

**User #71483**

- Misc
- User #71483's Personal Space
  - Product requirements
    - DriftingShadows 1.10 Requirements *SECRET*
    - StrawHat 1.0 Requirements *SECRET*
    - DriftingShadows 1.9 Requirements *SECRET*
    - TheIronBank 1.0 Requirements *SECRET*
  - File lists
    - DriftingShadows 1.10
    - Test
    - DriftingShadows 1.9
    - JQJSNICKER
    - Update

**User #71478.. User #71468**

- User #71478.. User #71468's Home

**User #71482**

- User #71482's Home

**User #71467**

- User #71467's Home
  - User #71467's Task List

**User #71465**

- User #71470's Home

**User #71495**

- User #71495's Home

**User #1179751 F.**

- User #71481's Home

**User #20251227**

- Notes on Browser-Based Credential Stealing
- User #20251227's Home
  - Page of Holding
  - Welcome
  - Scratch Pad

**User #71469**

- User #71469 Home

**User #71485**

- User #71485's Home
  - How-to articles
  - Router Exploitation
    - SOHO ROM Exploitation
  - Installing VS2013 Update 5 on Windows 10

**User #71486**

- User #71486.'s Home
  - User #?'s Test

**User #71493**

- User #71493's Home

**User #71479**

- User #71479's Home
  - Ubuntu-Foo

**User #71491**

- User #71491's Home

**User #71477**

- User #71477's Home

DTO Transfer Log

XYLOPHAGE Research

**User #71494**

User #71494's Home

Caterpillar ICE Command-Line Documentation

**User #71492**

User #71492's Home