

Forum:[Hack Forums](#)

Thread: [WraithKit v1.2 - Advanced Exploit Kit Framework | FUD](#)

WraithTools - September 18, 2025, 1:08 pm

? DISCLAIMER

This project is for educational and authorized security testing purposes only. Unauthorized use of this software for malicious purposes is illegal and unethical. Users are responsible for complying with all applicable laws and regulations.

? Overview

WraithKit is a comprehensive exploit framework designed for security researchers and penetration testers. It provides a web-based command and control interface, multiple exploit modules, advanced target fingerprinting, and sophisticated payload delivery mechanisms.

IMAGES

<https://ibb.co/F4nb4MM4>

<https://ibb.co/jZLm7VB6>

Key Capabilities

- Web-based C2 Interface - Professional dashboard for managing operations
- Multi-Vector Exploits - Browser, document, and application-based attacks
- Advanced Fingerprinting - Detailed target reconnaissance and profiling
- Stealth Operations - Anti-detection and evasion capabilities
- Modular Architecture - Extensible framework for custom exploits

? Features

? Web Command & Control Interface

Dashboard Management

- Real-time Operations Dashboard - Monitor active campaigns and targets
- User Authentication System - Secure multi-operator access control
- Session Management - Track and manage compromised systems
- Statistics & Analytics - Detailed reporting on campaign effectiveness

Target Management

- Victim Tracking Interface - Comprehensive target database
- Geographic Mapping - Visual representation of infected systems
- System Profiling - Detailed hardware and software inventory
- Access Control Matrix - Role-based operator permissions

? Advanced Target Reconnaissance

Browser Fingerprinting

// Automatic browser detection and profiling

- Browser type, version, and capabilities detection
- Plugin enumeration and vulnerability assessment

- Screen resolution and hardware profiling
- Network configuration analysis

System Intelligence Gathering

- Operating System Detection - Windows, macOS, Linux identification
- Hardware Profiling - CPU, memory, and graphics card detection
- Software Inventory - Installed applications and security tools
- Network Analysis - IP geolocation, ISP, and proxy detection

? Exploit Modules

Browser Exploits

// Memory corruption and browser-specific attacks

- Buffer overflow exploitation techniques
- Heap spray and ROP chain construction
- JavaScript engine vulnerabilities
- Plugin and extension targeting

Features:

- Memory Corruption Exploits - Advanced buffer overflow techniques
- Heap Spray Attacks - Reliable memory layout manipulation
- Return-Oriented Programming (ROP) - Bypass DEP/ASLR protections
- JavaScript Engine Targeting - V8, SpiderMonkey, and Chakra exploits

Document Exploits

// Malicious document generation and delivery

- RTF document weaponization
- Office macro exploitation
- PDF vulnerability targeting
- Email attachment vectors

Supported Formats:

- Rich Text Format (RTF) - Memory corruption through document parsing
- Microsoft Office Documents - Macro-based and memory corruption attacks
- PDF Documents - JavaScript and plugin-based exploitation
- Email Attachments - Social engineering delivery vectors

? Payload Delivery System

Multi-Stage Delivery

// Sophisticated payload deployment mechanisms

- Encrypted payload transmission
- Anti-analysis evasion techniques
- Persistence establishment
- Command and control communication

Delivery Methods:

- Staged Payloads - Multi-part delivery to evade detection
- Encrypted Transmission - Runtime decryption and execution
- Polymorphic Code - Self-modifying payloads for signature evasion
- Fileless Execution - Memory-only payload deployment

Payload Types

- Remote Access Tools (RATs) - Full system control and monitoring
- Information Stealers - Credential harvesting and data exfiltration
- Cryptocurrency Miners - Covert mining operations
- Botnet Agents - Integration with larger command networks

? Evasion & Anti-Analysis

Detection Evasion

- Sandbox Detection - Identify and evade automated analysis systems
- Virtual Machine Detection - Recognize virtualized environments
- Debugger Evasion - Anti-debugging and analysis techniques
- Behavioral Analysis Bypass - Time-delayed and conditional execution

Traffic Obfuscation

- Encrypted C2 Communications - Secure command and control channels
- Domain Generation Algorithms - Dynamic server resolution
- Traffic Mimicry - Disguise malicious traffic as legitimate requests
- Proxy Chain Support - Multi-hop communication routing

Key Features

- Multi-threaded Request Handling - Concurrent target management
- Payload Routing - Automatic exploit delivery based on fingerprinting
- Access Logging - Detailed interaction tracking
- Error Handling - Graceful failure management

Fingerprinting Engine

// Advanced target reconnaissance and profiling

- Browser detection and version analysis
- Plugin enumeration and capability assessment
- Hardware profiling and system specifications
- Network configuration and geolocation

Collected Information:

- Browser Details - Type, version, rendering engine
- System Information - OS, architecture, hardware specs
- Network Data - IP address, ISP, geographic location
- Security Software - Antivirus and firewall detection

Authentication System

// Secure operator authentication and session management

- Multi-user access control
- Session token management

- Role-based permissions
- Activity logging and audit trails

Access Control

// Permission management and operator roles

- Administrator privileges
- Operator-level access
- Read-only monitoring
- Custom permission matrices

PRICING

1 Month - \$900

3 Month - \$1400

Free domain changes and exploit recrypts throughout to keep it FUD

[contract=tid]Start Contract[/contract]

MeW11 - September 18, 2025, 5:46 pm

looks good, glws

Chornaya Magiya - September 19, 2025, 7:56 am

I believe u should rewrite normally what is your software since from current info is very confusing what its actually is and why and how its used

WraithTools - September 19, 2025, 1:42 pm

(Sep 19, 2025 07:56 AM)Chornaya Magiya Wrote: [\[CITE\]](#) I believe u should rewrite normally what is your software since from current info is very confusing what its actually is and why and how its used
Its a BEP. It exploits vulnerabilities in systems to execute a payload silently. Can be iframed on to websites for silent drive by downloads.

NiNJAA - September 21, 2025, 3:49 pm

make a video and upload it

m0narch - September 23, 2025, 6:32 am

image links got banned btw

Monyaks - September 25, 2025, 8:17 am

Please upload a video example.

WraithTools - September 25, 2025, 8:47 am

(Sep 25, 2025 08:17 AM)Monyaks Wrote: [\[CITE\]](#) Please upload a video example.
Yes we will do.

kannima - October 19, 2025, 9:45 pm

Please tell me your Telegram ID.

WraithTools - October 20, 2025, 9:00 am

(Oct 19, 2025 09:45 PM)kannima Wrote: [\[CITE\]](#) Please tell me your Telegram ID.
PM me

casperr - October 21, 2025, 3:24 pm

Hey looks good I would like to see a video or any pictures of the features

WraithTools - *October 21, 2025, 3:57 pm*

v2 will be released very soon and a video to accompany it.

Annason - *October 29, 2025, 3:34 pm*

Please give me you telegram account