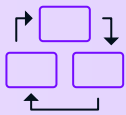


VOODOO

There's a Better Operator in You! Create Superior Red Team Operations by Outstripping Countermeasures & Cross-Platform Deep Pivoting



CROSS-PLATFORM SUPPORT

(iOS, M1, Android, IoT, macOS, Linux, Windows, etc.)

Voodoo supports targets based on Intel x64 and both traditional ARM and ARM64 processors. Being able to pivot seamlessly through all targeted endpoints means more thorough testing of targeted information systems and more accurate risk assessments.



ARMORY

(UAC Bypasses, Privilege Escalation, Active Directory Enumeration, etc.)

Toolkits should be designed to enable operators to safely and effectively get more done in less time. To this end, VooDoo provides an online "Armory" which enables operators to leverage crowdsourced and UltraViolet created "munitions" which empower operators to overcome obstacles without breaking a sweat. Each munition is rated and peer reviewed.



PIVOTING DEEP

Segmented networks are no longer an issue with the pivoting capabilities of Voodoo. Multiple agents can be chained together with dynamically created, fault tolerant routes to provide access into heavily secured networks including segments without direct internet access (Cardholder Data Environments, OT & SCADA systems, etc.).

ULTRAVIOLET VOODOO KEY BENEFITS AT A GLANCE



SCRIPTING ENGINES

Stay one step ahead of detections by leaving minimal footprints as you go. VooDoo's OPSEC centric design allows for in-memory execution of agents with the ability to load on the fly in-memory only scripting engines, enabling operators to easily load host specific tools including Python, C#, .NET, PowerShell scripts. In addition, many other types of binaries can be executed from memory only including Mach-O, Bundles, ELF, SO, PE, DLL, etc.



IOT, MOBILE & MAC

No longer are operating systems boundaries for your operations. Voodoo's cross platform design works across all major operating systems. Windows, Linux, MacOS, Android, and iOS. OS doesn't matter—traverse your target network as you please. The interface is consistent across each OS and there are no differences in command syntax. Simply select your target OS when creating a stager and then make your choice from multiple deployment methods.



MULTI-USER INTERFACE

Voodoo had teamwork in mind when it came to designing the user interface. It comes with a slick graphical web interface that supports multiple users with varying access levels. Multiple operators can interact with the same agents simultaneously. One operator can pilfer a target, while another operator is working on furthering access. Junior operators and supervisors can easily follow along with read only access in real-time.

FEATURE RICH

Custom Process Injection & AV Evasion

- Stay Hidden & Undetected on Endpoints

Memory Only Scripting & Binaries

- Python, C#, Powershell, .NET
- PE, DLL, ELF, SO, Mach-O, Bundles

Lateral Movement

- Active Directory Enumeration (BloodHound / SharpHound)
- Kerberoasting, Pass-The-Hash, WMI, etc.

Infinite Pivoting/Chaining

- Enabling access to systems otherwise inaccessible from the Internet

Cross Platform

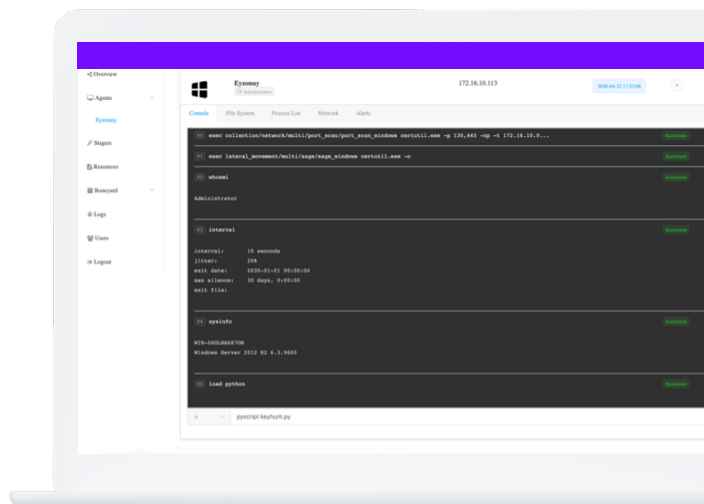
- MacOS, Linux, Windows (x86)
- Android, iOS, IoT (ARM)

Team Collaboration, Multi-Threading



BUILT BY OFFENSIVE OPERATORS FOR OFFENSIVE OPERATORS

Voodoo is a post exploitation platform for covert interactive cyber operations. Designed from the ground up to be stealthy, stable, and versatile, Voodoo enables a red team operator to chain agents together through a series of call-back (reverse) and call-in (connect) payloads, across multiple various operating systems, providing access deep into target networks in information systems which should never communicate via the Internet (SCADA networks, CDEs/ Cardholder Data Environments, internal databases, etc.)



WHY CHOOSE ULTRAVIOLET?

REAL WORLD EXPERTISE

The UltraViolet team is comprised of recognized industry experts and former NSA operators. Our team knows how to emulate the adversary because they honed their craft by being the Adversary.

TRAINING

UltraViolet provides advanced offensive trainings at Blackhat conference around the world. Included with every license purchase is access to our in-person Voodoo training course.

100% FOCUSED

UltraViolet is a solely focused cybersecurity company founded by former NSA operators and owned by security professionals. We partner with our clients and build tools and solutions to enable their mission.

ABOUT ULTRAVIOLET

UltraViolet Cyber is a leading platform enabled unified security operations company providing a comprehensive suite of security operations solutions. Founded and operated by security practitioners with decades of experience, the UltraViolet Cyber security-as-code platform combines technology innovation and human expertise to make advanced real time cybersecurity accessible for all organizations by eliminating risks of separate red and blue teams. By creating continuously optimized identification, detection and resilience from today's dynamic threat landscape, UltraViolet Cyber provides both managed and custom-tailored unified security operations solutions to the Fortune 500, Federal Government, and Commercial clients. UltraViolet Cyber is headquartered in McLean, Virginia with global offices across the U.S. and in India.

