Dark Web Made Safe and Accessible

Dangerous organizations and people operate in the shadows. If you are going to find them online, you have to go on the Dark Web.

But the Dark Web is hazardous:

- Adversaries and criminals employ sophisticated counter-surveillance tools
- They booby-trap their sites with malware
- They actively recruit legitimate analysts and researchers for illicit purposes

As a result, resource-constrained organizations (e.g., local law enforcement) too often lack Dark Web access. Large organizations (e.g., federal agencies) usually build separate “dirty” infra-structures which are expensive, labor intensive, slow, and opaque. There is a better way.

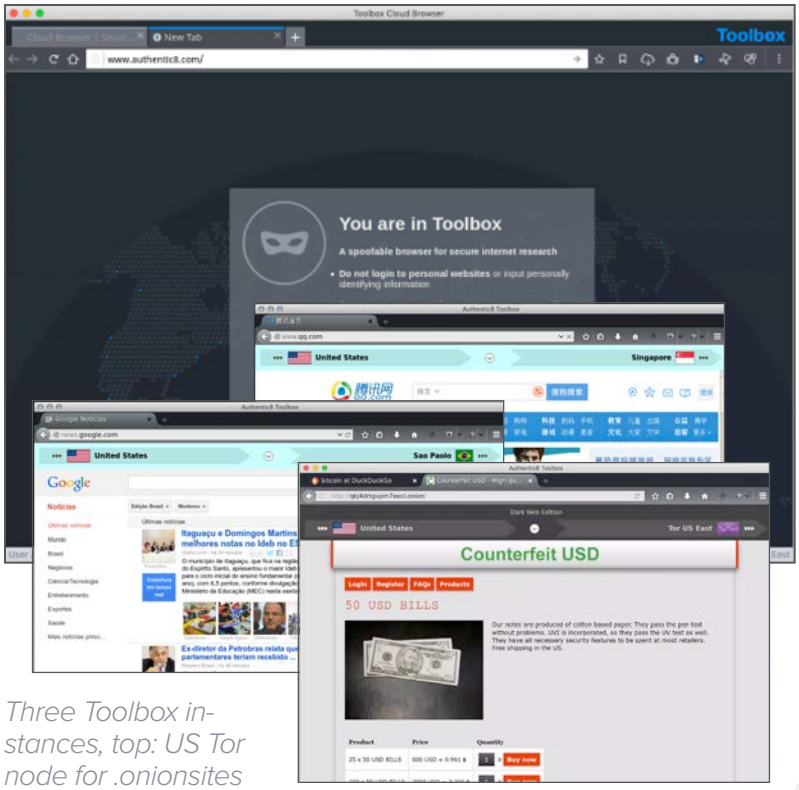
SILO RESEARCH TOOLBOX DARK WEB

Silo is the foundation of Toolbox-DW; it is a one-time-use browser built on-demand in a secure cloud-based container. All web code is rendered in the cloud and converted into a high-fidelity remote display of the session, protecting end-points from malware, ransomware, and drive-by downloads. All web activity is logged. Privileges to upload/download and to access restricted URLs are policy controlled.

Toolbox is a managed attribution and research suite layered over Silo. It allows users to spoof IPs to over 30 locales worldwide, manipulate their hardware & software fingerprints, and to collect, annotate, and store internet-based PAI. It includes tools for post-fetch language translation, web-code and traffic analysis, and linkage tracking.

PRIMARY BENEFITS

- Defeat Dark Web counter-surveillance
- Quarantine Dark Web malware
- Monitor all employee Dark Web activity
  - Manage their workflow
  - Deter illicit use of Tor access
- Access Dark Web from existing IT infrastructure
  - Reduce annual cost of Dark Web access
  - Reduce IT support workload
  - Increase speed and performance
- Enable research collaboration
- Improve research quality

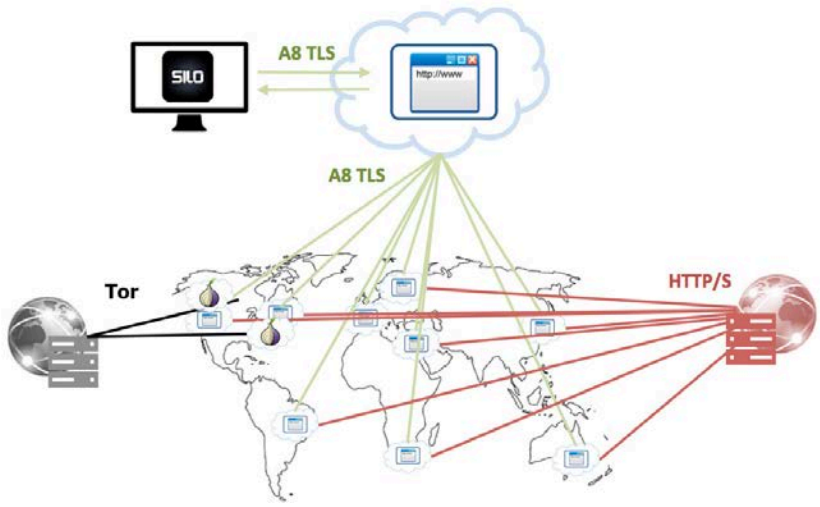


Three Toolbox instances, top: US Tor node for .onionsites

Browser Isolation, Managed Attribution, and the Tor Network

Toolbox-DW provides simple and safe “point & click” access to Dark Web (Tor) content over existing infrastructure. Toolbox-DW extends the Authentic8 global egress network to include designated .onion-capable nodes. Each node is connected via IPSec, but converts requests to SOCKS for access to the Tor network. Each Tor connection is built from scratch based on a randomly selected ingress node, relay, and egress node.

Access to the Dark Web is seamlessly integrated for Toolbox-DW users, not a separate Tor browser. Analysts have a single pane of glass to conduct research on the open, deep, and dark web. Managers have oversight of collection, research, and investigative activity. Administrators have policy control over user privileges. Executives have the protection of non-repudiable audit logs of all online activity.

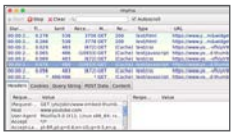


SPECIFICATIONS	
SUPPORTED PLATFORMS	Windows (XP - 10) macOS, Linux, iOS
SYSTEM REQUIREMENTS	15MB storage, ~100MB RAM
CLIENT INTERFACES	SSL Port 442 Proprietary remote display
EGRESS NODE LOCATIONS	World-wide access to Tor from the Americas, Asia, EMEA
JAVA SUPPORT	Java JRE v6-v8 isolated in sandbox
ANALYSIS TOOLS	Code Analysis, TCP capture, more
PLUGIN SUPPORT	Firefox store; any plugin not requiring restart
XTERM SUPPORT	Configurable with SSH Key bindings
LOGGING	Encrypted user and admin logs
LOG ACCESS	Within admin console (non-encrypted), or via API

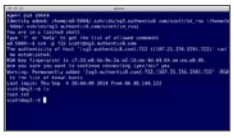
Post-fetch language translation

Encrypted cloud-based storage

Spoof mobile platforms



Capture network traffic



Run command line utilities

Analyze web code

Used by OSINT analysts, law enforcement officers, and cyber threat researchers, Silo Research Toolbox-DW is accredited on Intelligence, Defense, Justice, and other Federal networks.

To learn more, visit www.authentic8.com