Target. Hunt. Disrupt.

DATASHEET

SQRRL ENTERPRISE
TEST DRIVE VM
Featuring Web Proxy Data and Threat Intelligence

Using Web Proxy Data Beyond Web Traffic Control

Web proxies have long served as a way for organizations to monitor and control the influx of web traffic that permeates their network, but proxy data can be far more useful for network defenses than just web traffic control and automated monitoring.

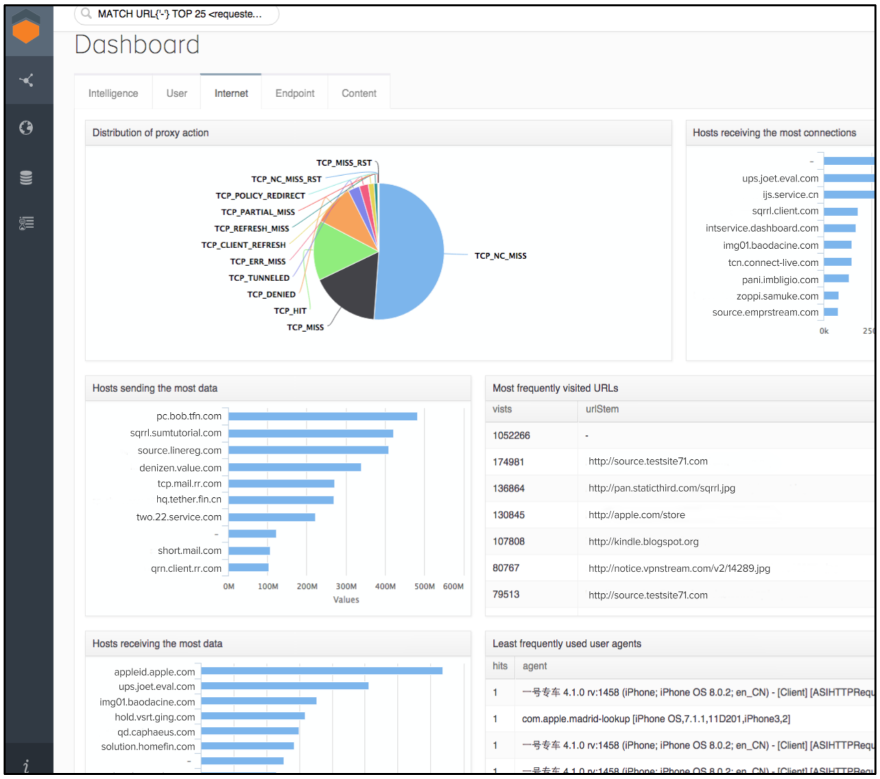
Command and Control (C2) and data exfiltration activities typically use HTTP and other common network protocols originating within an organization's network perimeter to carry out malicious actions. Web proxy data provides an incredibly rich single data source that can be effectively leveraged for proactive cyber investigations and network security.

With the Sqrrl Test Drive VM featuring Web Proxy Data and Threat Intelligence, users are able to hunt for cyber threats using web proxy data enriched with geolocation data and open source threat intelligence. By modeling this enriched log data as linked data, analysts can detect and investigate malicious actors before they can fully execute their objective. In other words, you can start conducting cyber hunt missions with the web proxy data that you already have.

The Sqrrl web proxy solution comes prepopulated with an analytical model and the rules for automatically transforming your proxy logs into linked data. All you need to do is load your data into a configured directory, and Sqrrl will take care of the rest. When the process is complete, you can use Sqrrl's out-of-the-box dashboard reports and analyst hunting guides to discover and investigate latent threats in your web traffic.

Sqrrl Web Proxy Test Drive VM features:

- Analytic model for web proxy data
- Simplified proxy data loading utility
- Automated threat intelligence matching
- Automated GeoIP enrichment
- Analyst investigative workflow guides
- Security and threat hunting oriented Dashboard reports



Most frequently visited URLs

vists	urlStem
1052266	-
174981	http://source.testsite71.com
136864	http://pan.staticthird.com/sqrrl.jpg
130845	http://apple.com/store
107808	http://kindle.blogspot.org
80767	http://notice.vpnstream.com/v2/14289.jpg
79513	http://source.testsite71.com

Least frequently used user agents

hits	agent
1	一号专车 4.1.0 rv:1458 (iPhone; iPhone OS 8.0.2; en_CN) - [Client] [ASIHTTPRequ
1	com.apple.madrid-lookup [iPhone OS,7.1.1,11D201,iPhone3,2]
1	一号专车 4.1.0 rv:1458 (iPhone; iPhone OS 8.0.2; en_CN) - [Client] [ASIHTTPRequ
1	一号专车 4.1.0 rv:1458 (iPhone; iPhone OS 8.0.2; en_CN) - [Client] [ASIHTTPRequ

Sqrrl categories and reports provide trailheads and detailed insights on activities that can streamline a hunt

Dashboards

Sqrrl's dashboards simplify and streamline the workflow for analysts who are investigating what might be happening on their network. By quickly launching an interactive linked-data investigation from a summary metric, analysts can answer questions like "*Which users are most frequently accessing the servers on the internet which are receiving the most uploads, and what websites do they visit in common? Which hosts have the most intel matches and which other hosts are they connecting to within the network?* or *Which users have the most denied requests and what websites are they trying to access?*"

Sqrrl Web Proxy Data + Threat Intelligence Exploration Categories

Category	Description	Example Hunting Trailheads
Intelligence	Activity containing matches with threat intelligence data. This includes browsing category intelligence in proxy data and open source threat intelligence that Sqrrl integrates.	What is the entity with the most common threat intelligence matches that my clients and user accounts are contacting the most on my network?
User	User behaviors and outliers that isolate and indicate suspicious activity and potentially compromised accounts.	Which users have the most proxy denied requests and which websites are they trying to access?
Internet	Host, user agent, and domain activities and protocol requests that rapidly identify suspicious traffic.	Which are the domains to which hosts on my network are sending the most data and how many intelligence matches are there with those domains?
Endpoint	The most active hosts and most suspicious endpoint behaviors, as well as port usage, used to monitor an internal network for threats.	Are there unfamiliar destinations to which the clients on my network with the most outgoing connections are directing their traffic?
Content	Detailed views on the types of websites and files that users and clients are accessing on a network in order to investigate specific	What is the extent of the connection between a phishing related URL and a potentially compromised account?

Key Benefits

- Visual Hunting on Proxy Data
  - Prebuilt models populated with your data
  - Explore and discover potential threats visually
  - Sqrrl Hunting Guides can grant any analyst hunting expertise
- Threat Intelligence Fusion
  - Multiple intel sources fused into a single pane of glass
  - Preconfigured with 3 highly rated OSINT feeds
- Powerful Linked Data Analysis Platform
  - Automatic graph extraction from your data
  - Big Data core easily stores data for years
  - Industry leading data-centric security
- Rapid Deployment
  - No configurations, no parsing, no code to write
  - Preconfigured VM requires only simply dropping files into a directory

ABOUT SQRRL

sqrrl
Target. Hunt. Disrupt.

Sqrrl was founded in 2012 by creators of Apache Accumulo™. With their roots in the U.S. Intelligence Community, Sqrrl's founders have deep experience working at the intersection of advanced cybersecurity and Big Data problems. Sqrrl is headquartered in Cambridge, MA and is a venture-backed company with investors from Matrix Partners, Atlas Venture, and Rally Ventures.