Malicious Detection

Real-Time Threat Detections & Intelligence for OEMs

zvelo employs a crowd-sourced approach for obtaining a constant stream of URLs for analysis. This continuous stream of ActiveWeb (URLs actively visited by end users) comes from the zvelo global network of customers across a number of high traffic markets: Network Security, Subscriber Analytics, and Ad Tech. This includes over 650 million end users and growing—and is the primary in-house source for threat corpora used to train human-supervised machine learning systems. This combined and integrative approach empowers us to continuously enhance, optimize, and fine-tune our malicious detection capabilities in an ever-changing threat landscape.

650M+ End User Network
Our global network generates hundreds of millions of URLs, and billions of interactions on a daily basis. This ActiveWeb traffic is leveraged to perform industry-leading content categorization and malicious detection. This includes:

- Supporting over 650 million end users
- Covering numerous industries including:
  - Network Security
  - Subscriber Analytics
  - Ad Tech
  - ActiveWeb Input and queries on
    - Web Content
    - Web Traffic from browsers
    - Web-connected Device activity

Multi-Vector Threat Detection
zvelo leverages an integrative, multi-vector approach and in-house analysis to detect, monitor, and accurately categorize website content at the domain and full-page level—as well as new threats. Our approach combines the following methods:

- URLs/Website Detection
  - Link Analysis
  - Content Analysis
  - Static, Heuristic, & Behavioral Anomaly Analysis
  - In-house and 3rd Party Tools
- Browser/Traffic Detection
  - Bot/Non-Human Analysis
  - Data Center/Crawler Analysis
- Data Mining
  - Deep Pattern Cross-Matching Analysis
  - Predictive Analysis
We categorize the Web®

MALICIOUS DETECTION

10 Unique Malicious Categories

zvelo threat detection systems identify and categorize target URLs into ten (10) unique malicious categories:

**Ad Fraud**
Sites that are being used to commit fraudulent online display advertising transactions using ad impression boosting techniques including (but not limited to) ad stacking, iframe stuffing, and hidden ads. Sites that have high non-human web traffic and with rapid, large and unexplained changes in traffic.

**Spyware & Questionable Software**
Software that reports information back to a central server such as spyware or keystroke loggers. Also includes software that may have legitimate purposes, but some users may object to having on their system.

**Botnet**
Bots are compromised machines running software that is used by hackers to send spam, phishing attacks, and denial of service attacks.

**Malware Distribution Point**
Web pages that host viruses, exploits, and other malware are considered Malware Distribution Points.

**Phishing/Fraud**
Web pages that impersonate other web pages usually with the intent of stealing passwords, credit card numbers, etc. Also includes web pages that are part of scams such as a “419” scam—where a person is convinced to hand over money with the expectation of a big payback that never comes.

**Command & Control Centers**
Internet servers used to send commands to infected machines called bots.

**Malware Call-Home**
When viruses and spyware report information back to a particular URL or check a URL for updates, this is considered a malware call-home address.

**Compromised & Links to Malware**
Compromised web pages are pages that appear to be legitimate, but house malicious code or link to malicious websites hosting malware. These sites have been compromised by someone other than the site owner.

**Spam URLs**
URLs that frequently occur in spam messages.

**Cryptocurrency Mining**
Websites that use cryptocurrency mining technology without user permission.

Human-Supervised Machine Learning
The zveloLABS team continuously samples malicious detections to profile, test, and validate threats. The results of the continuous sampling are then used to feed/train the supervised machine learning systems—as well as adjust and tune the efficiency, accuracy, and overall effectiveness of the malicious detection systems.

URL, Domain, and Path Coverage
One of the critical features that zvelo provides is an ability for deep analysis due to full path detection. In a nutshell, page and path-level reporting provides analytical credibility to what is being marked as malicious. The majority of malicious URLs are detailed down to the path level. For non-IP based URLs, 88.35% are marked as malicious down to the path level. For IP-based URLs, the number is significantly higher with 99.70% being identified as having a path. This is unique because DNS-based systems typically only work at the domain only.

Malicious URL Revisit Process
Due to the variable lifecycle of malicious URLs, it is imperative be able to inspect and detect URLs quickly to ensure they are still malicious. zvelo Malicious Detection includes an automated revisit process where malicious URLs are revisited on a set schedule. Each day, up to 300,000 malicious URLs are re-analyzed to determine if they are still infected or are now clean. Since zvelo is able to obtain the full path, it is able to revisit the exact URL and obtain crucial results on a granular and highly accurate level.

For more information about our industry-leading OEM solutions for Content Categorization, Malicious and Phishing Detection, Subscriber Analytics, Brand Safety, and more—visit us at zvelo.com. MKT-MDO-003 | April 2019