Malicious Trends

CYBER THREAT INTELLIGENCE REPORT | OCTOBER 2021

TABLE OF CONTENTS

zvelo's passion is to make the internet safer and more secure by providing the industry's premium cyber threat intelligence and web classification data services.

zvelo's proprietary AI-based threat detection and categorization technologies, combines curated domains, threat and other data feeds, with a traffic stream from its partner network of 600+ million users to provide unmatched visibility, coverage, reach and accuracy for powering applications including web filtering, endpoint security, brand safety and contextual targeting, and others, as well as enriching threat intelligence and analysis.

INTRODUCTION

zvelo Malicious Trends provides insight into Malicious Cyber Actor (MCA) activities utilizing a select dataset from our Malicious Detailed Detection Feed (MDDF) and PhishBlockList (PBL) products. Focusing specifically on known malicious Uniform Resource Locators (URLs), the goal of this report is to shed light on current trends and inform defenders about potential threats they may face. The zvelo Cybersecurity Team presents their analysis of the data with some general conclusions at the end. As every organization has a different set of needs and perspectives unique to their own environment, readers must draw their own specific conclusions. This is zvelo's second annual Malicious Trends report, and we plan to continue releasing similar reports in the future — furthering our mission to make the internet safer and more secure.

DATASET OVERVIEW

The dataset used for analysis in this report consisted of the following:

- **MDDF:** 2,106,551 full-path URLs and associated metadata
- **PBL:** 946,556 full-path URLs and associated metadata
- **Total:** 3,054,107 URLs

These URLs were collected from July - September 2021 via zvelo's malicious detection system which consists of multiple trusted, proprietary, and in-house sources. The dataset includes a large mix of Top Level Domains (TLD), affording significant randomization of the entries.

METHODOLOGY

The zvelo Cybersecurity Team analyzed the full-path URLs using in-house tools to identify unique trends in the malicious (MDDF) and phishing (PBL) datasets. This report details many of the trends observed in the datasets. The information shared in the following sections is a mix of raw numbers and simple graphics to present the team's discoveries. There are both commonalities and distinctions between the malicious and phishing metadata. As such, this year's report will address malicious and phishing trends separately.

zvelo Cyber Threat Intelligence (CTI) Solutions leveraged to produce this report:

- **PhishBlockList (PBL):** Multi-source and proprietary data to disrupt phishing attacks (MITRE T1566).
- **Malicious Detailed Detection Feed (MDDF):** Multi-source and proprietary enrichment and at-scale analysis of malware-associated files to extract pertinent Indicators of Compromise (IOC) (multiple MITRE ATT&CK techniques).
- **Suspicious New Registrations Feed (SNRF):** Multi-source and proprietary methods to detect, assess, and score newly registered domains to disrupt the MCAs attempts to establish their malicious infrastructure (MITRE PRE-ATT&CK "Establish & Maintain Infrastructure").

MALICIOUS DATA

TRENDS BY THE NUMBERS

To begin with, the zvelo Cybersecurity Team reviewed the entirety of the data — 2.1+ million entries from our malicious detection system. The team then analyzed the data for obvious common trends. The resulting trends observed proved interesting.

TOP 15 COMMON URL OBSERVATIONS

Total 2,106,551	Contains: .php 182,250	Contains: /mozi 152,744	Contains: .html, .htm 77,926
Contains: .exe 77,753	Contains: wp- 38,623	Contains: .asp, .aspx 27,792	Contains: /%, /& 21,897
Contains: .apk 20,896	Contains: .pdf 18,971	Contains: .i, bin.sh 17,632	Contains: Base64 Encoding 12,458
Contains: .js, .jar 11,616	Contains: .jpg, .png 10,598	Contains: .zip, .rar 7,007	Contains: arm, x86 6,337

Malicious Trend by the Numbers | Common Observations by URL Counts

zveloCTI™ | Malicious Trends Report 2021

In total, common URL observations add up to 2,514,466 entries in the dataset, accounting for ~32% of the malicious URLs. Further, 684,500 common URLs appear to focus on active scripting/content which could impact multiple Operating Systems. This year's observations also show that .exe files, specifically targeting Windows, account for only ~3.6% (77K) of URLs reviewed compared to ~33% in 2020. The reason for this reduction is still under investigation.

This year's analysis shows a significant uptick in script files (.php, .asp and .aspx, .i and bin.sh, and .js and .jar) which accounted for 239,290 entries (11%). The observation /% and /& path variables could point to even greater usage of active content by MCAs looking to redirect victims over a series of hops, not just a single URL.

RESULTING TRENDS OBSERVED

- Top 15 common — and related — extensions that stood out:
  - .php
  - /mozi
  - .html, .htm
  - .exe
  - wp-
  - .asp, .aspx
  - /%, /&
  - .apk
  - .pdf
  - .i, bin.sh
  - Base64 Encoding
  - .js, .jar
  - .jpg, .png
  - .zip, rar
  - arm, x86

To download a complete copy of the 2021 Malicious Trends Report, please visit www.zvelo.com

zvelo

www.zvelo.com
cybersecurity@zvelo.com