Malicious Trends

CYBER THREAT INTELLIGENCE REPORT | OCTOBER 2020

zvelo

MAKING THE INTERNET
SAFER AND MORE SECURE

TABLE OF CONTENTS

INTRODUCTION	1
Dataset Overview	1
Methodology	1
TRENDS BY THE NUMBERS	2-3
Common URL Observations	2-3
Trends by TLD	4-7
HTTP vs HTTPS	7
Industries Impacted	8
Linux File Extensions	8-9
IP Address URL vs Text URL	9-10
Misconfigured Web Parts	10
CONCLUSIONS	11
ABOUT zveloCTI	12

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 content categorization URL database. 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. zvelo plans to release reports similar to this one in the future to continue our mission to make the internet safer and more secure.

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

- **Phishing Intelligence: Multi-source and proprietary data to disrupt phishing attacks (MITRE T1566).**
- **Suspicious Domain Intelligence: 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 Intelligence: 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).**

DATASET OVERVIEW

The dataset used for analysis in this report consisted of 3,941,143 unique full-path URLs. These URLs were collected from June 22 - August 16, 2020 via zvelo's malicious detection system which consists of multiple trusted and proprietary sources. The dataset included a large mix of Top Level Domains (TLDs), 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 dataset. This report details many of the trends observed in the dataset. The information shared in the following sections is a mix of raw numbers and simple graphics to present the team's discoveries.

TRENDS BY THE NUMBERS

To begin with, the zvelo Cybersecurity Team reviewed the entirety of the data — 8 weeks of entries from our malicious detection system. The team then analyzed the data for obvious common trends.

TOP 15 COMMON URL OBSERVATIONS

Total 3,941,143 Count of URLs	Contains: .exe 610,763 Count of URLs	Contains: wp - 378,460 Count of URLs	Contains: mozi 376,282 Count of URLs
Contains: .arm, .x86 282,867 Count of URLs	Contains: .i 256,188 Count of URLs	Contains: .zip 247,189 Count of URLs	Contains: invoice 147,601 Count of URLs
Contains: .jpg, .png 85,925 Count of URLs	Contains: .doc, .docx 62,614 Count of URLs	Contains: .cab 21,982 Count of URLs	Contains: .js 17,097 Count of URLs
Contains: .apk 15,801 Count of URLs	Contains: .pdf 7,580 Count of URLs	Contains: .xls, .xlsx 2,158 Count of URLs	Contains: .vbs 1,959 Count of URLs

Trends by the Numbers | Common URL Observations zveloCTI™ | Malicious Trends Report

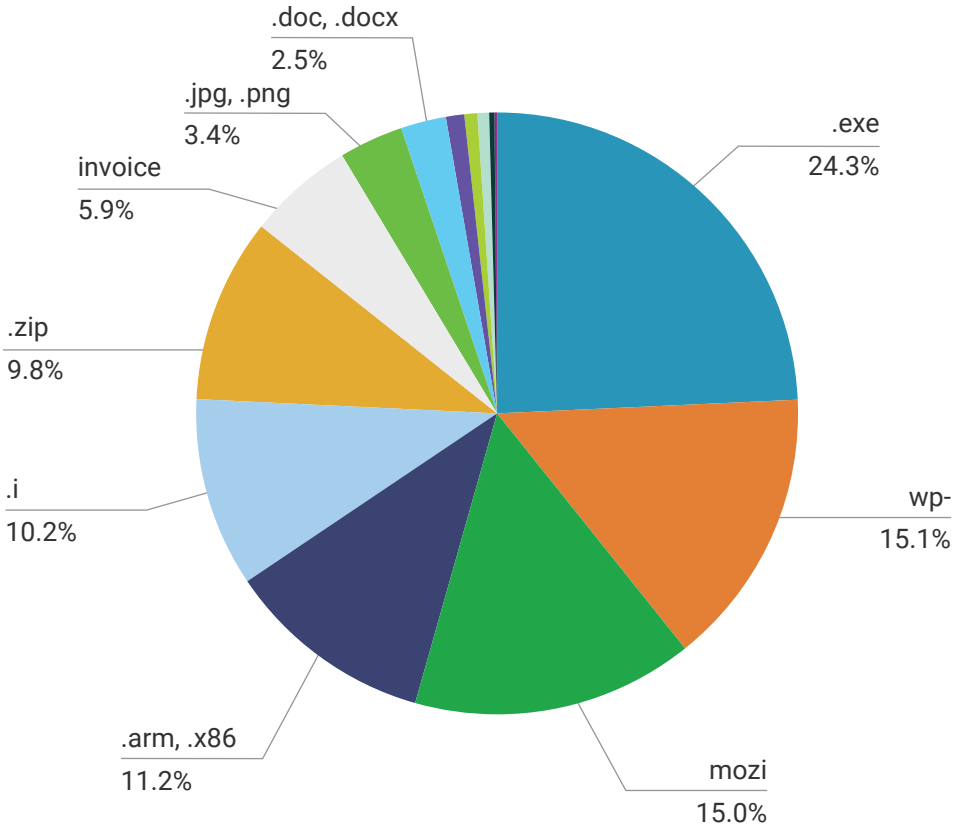
In total, common URL observations add up to 2,514,466 entries in the dataset accounting for ~64% of the malicious URLs. Further, 1,296,358 of the common URLs appear to focus on the Windows Operating System (extensions: .exe, .i, .zip, jpg/.png, .doc/.docx, .cab, .pdf, .xls/.xlsx, and .vbs). Of the 3.94M URLs reviewed, ~33% appear designed to target Windows. This is not surprising as Windows continues to dominate the desktop OS market with a share of nearly 80%[1].

RESULTING TRENDS OBSERVED

- **13 common — and related — extensions stood out:**
  - **.exe**
  - **mozi**
  - **.arm & .x86**
  - **.i**
  - **.zip**
  - **.jpg & .png**
  - **.doc & .docx**
  - **.cab**
  - **.js**
  - **.apk**
  - **.pdf**
  - **.xls & .xlsx**
  - **.vbs**
- **One unique word — invoice — appeared to be focused on stealing business or personal payment information.**
- **One compromised web-part — WordPress — used by MCAs to host malicious content without the knowledge of site owners.**

1. Statcounter: https://gs.statcounter.com/os-market-share/desktop/worldwide

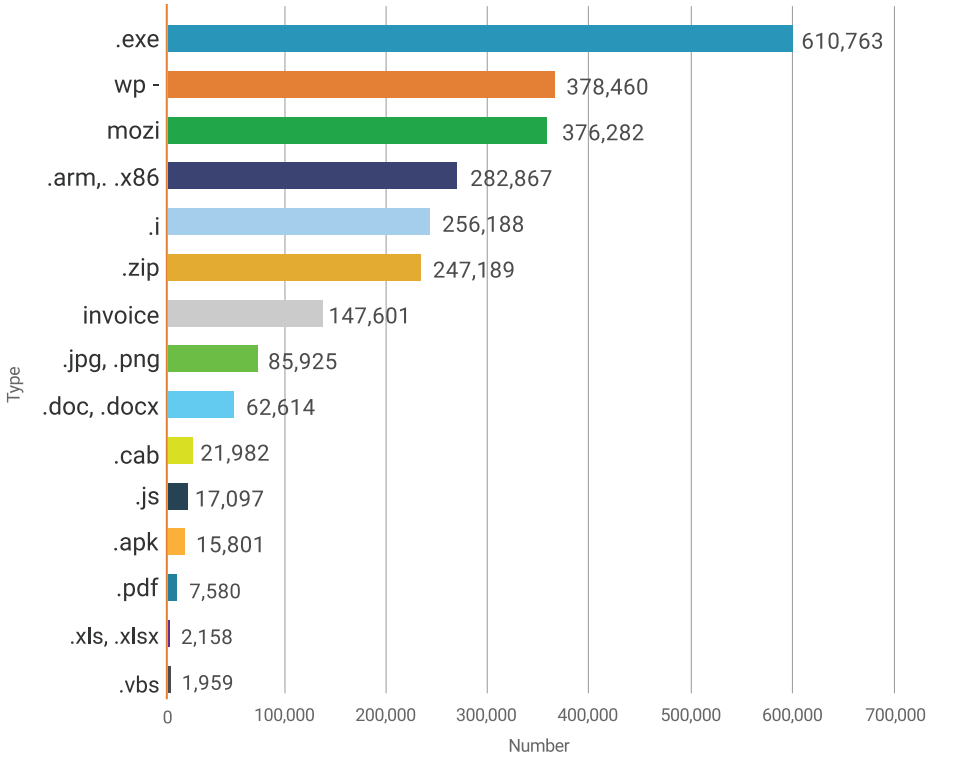
COMMON URL OBSERVATIONS | PERCENTAGES



zveloCTI™ | Malicious Trends Report | Common URL Observations

The common URL observations are broken out here to show the percentage of each compared to the 3.94M entries in the dataset.

TOP 15 COMMON URL OBSERVATIONS | URL COUNT



zveloCTI™ | Malicious Trends Report | Top 15 Common URL Observations

The common URL observations are broken out here by the URL counts, rather than percentages as represented in the chart above.

TRENDS BY TOP LEVEL DOMAIN (TLD):

Next, the zvelo Cybersecurity Team surveyed TLDs to assess common URL observations. The team specifically explored the .com, .net, .org., .top, and .xyz domains. The results for each are presented here with a brief summary of findings.

.COM | COMMON URL OBSERVATIONS by TLD

Total TLD: .com 1,423,874 Count of URLs	Contains: .exe 269,494 Count of URLs	Contains: wp - 214,153 Count of URLs	Contains: mozi 102 Count of URLs
Contains: .arm, .x86 1,044 Count of URLs	Contains: .i 20,182 Count of URLs	Contains: .zip 142,783 Count of URLs	Contains: invoice 78,204 Count of URLs
Contains: .jpg, .png 37,350 Count of URLs	Contains: .doc, .docx 34,504 Count of URLs	Contains: .cab 21,814 Count of URLs	Contains: .js 15,937 Count of URLs
Contains: .apk 3,830 Count of URLs	Contains: .pdf 5,223 Count of URLs	Contains: .xls, .xlsx 1,013 Count of URLs	Contains: .vbs 423 Count of URLs

Common URL Observations by TLD | .com

.COM FINDINGS:

- **.com URLs make up ~36% of the URLs reviewed.**
- **.exe and .zip files make up ~29% of the file extensions in the .com TLD.**
- **Compromised WordPress sites account for 15% of .com URLs — more than half of the total seen for the entire set.**

.NET | COMMON URL OBSERVATIONS by TLD

Total TLD: .net 90,102 Count of URLs	Contains: .exe 11,094 Count of URLs	Contains: wp - 17,412 Count of URLs	Contains: mozi 0 Count of URLs
Contains: .arm, .x86 857 Count of URLs	Contains: .i 2,482 Count of URLs	Contains: .zip 6,635 Count of URLs	Contains: invoice 6,110 Count of URLs
Contains: .jpg, .png 3,557 Count of URLs	Contains: .doc, .docx 5,590 Count of URLs	Contains: .cab 0 Count of URLs	Contains: .js 104 Count of URLs
Contains: .apk 323 Count of URLs	Contains: .pdf 241 Count of URLs	Contains: .xls, .xlsx 89 Count of URLs	Contains: .vbs 18 Count of URLs

Common URL Observations by TLD | .net

.NET FINDINGS:

- **.net URLs make up ~2.3% of the URLs reviewed.**
- **.exe and .zip files make up ~20% of the file extensions in the .net TLD.**
- **Compromised WordPress sites account for ~19% of .net URLs.**

TRENDS BY TOP LEVEL DOMAIN (TLD):

.ORG | COMMON URL OBSERVATIONS by TLD

Total TLD: .org 223,103 Count of URLs	Contains: .exe 142,669 Count of URLs	Contains: wp - 13,708 Count of URLs	Contains: mozi 55 Count of URLs
Contains: .arm, .x86 430 Count of URLs	Contains: .i 8,732 Count of URLs	Contains: .zip 6,962 Count of URLs	Contains: invoice 9,317 Count of URLs
Contains: .jpg, .png 2,763 Count of URLs	Contains: .doc, .docx 18,739 Count of URLs	Contains: .cab 0 Count of URLs	Contains: .js 91 Count of URLs
Contains: .apk 482 Count of URLs	Contains: .pdf 139 Count of URLs	Contains: .xls, .xlsx 30 Count of URLs	Contains: .vbs 49 Count of URLs

Common URL Observations by TLD | .org

zveloCTI™ | Malicious Trends Report

.ORG FINDINGS:

- .org URLs make up ~6% of the URLs reviewed.
- .exe files make up ~61% of the file extensions in the .org TLD.
- .doc/.docx files make up ~8% of the file extensions in the .org TLD.
- Compromised WordPress sites account for ~6% of .org URLs.

.XYZ | COMMON URL OBSERVATIONS by TLD

Total TLD: .xyz 22,510 Count of URLs	Contains: .exe 5,832 Count of URLs	Contains: wp - 3,769 Count of URLs	Contains: mozi 20 Count of URLs
Contains: .arm, .x86 892 Count of URLs	Contains: .i 124 Count of URLs	Contains: .zip 1,718 Count of URLs	Contains: invoice 706 Count of URLs
Contains: .jpg, .png 1,289 Count of URLs	Contains: .doc, .docx 312 Count of URLs	Contains: .cab 0 Count of URLs	Contains: .js 40 Count of URLs
Contains: .apk 2,367 Count of URLs	Contains: .pdf 71 Count of URLs	Contains: .xls, .xlsx 0 Count of URLs	Contains: .vbs 0 Count of URLs

Common URL Observations by TLD | .xyz

zveloCTI™ | Malicious Trends Report

.XYX FINDINGS:

- .xyz URLs make up ~0.57% of the URLs reviewed.
- .exe files make up ~26% of the file extensions in the .xyz TLD.
- .apk files make up ~10.5% of the file extensions in the .xyz TLD.
- Compromised WordPress sites account for ~17% of .xyz URLs.

TRENDS BY TOP LEVEL DOMAIN (TLD):

.TOP | COMMON URL OBSERVATIONS by TLD

Total TLD: .top 21,670 Count of URLs	Contains: .exe 7,911 Count of URLs	Contains: wp - 1,455 Count of URLs	Contains: mozi 0 Count of URLs
Contains: .arm, .x86 0 Count of URLs	Contains: .i 650 Count of URLs	Contains: .zip 264 Count of URLs	Contains: invoice 469 Count of URLs
Contains: .jpg, .png 1,194 Count of URLs	Contains: .doc, .docx 167 Count of URLs	Contains: .cab 0 Count of URLs	Contains: .js 0 Count of URLs
Contains: .apk 6,290 Count of URLs	Contains: .pdf 18 Count of URLs	Contains: .xls, .xlsx 9 Count of URLs	Contains: .vbs 0 Count of URLs

Common URL Observations by TLD | .top

zveloCTI™ | Malicious Trends Report

.TOP FINDINGS:

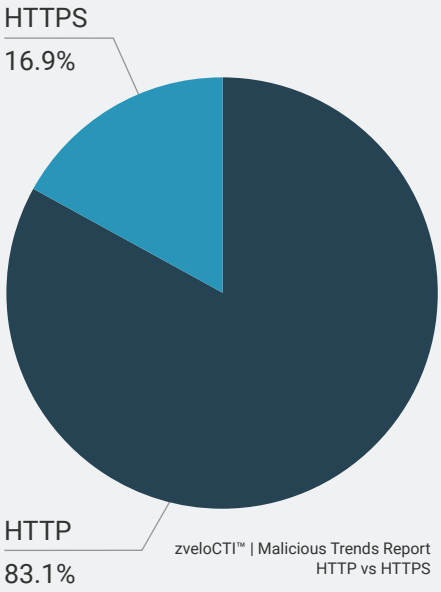
- **.top URLs make up ~0.55% of the URLs reviewed.**
- **.exe files make up ~36.5% of the file extensions in the .top TLD.**
- **.apk files make up ~29% of the file extensions in the .top TLD.**
- **Compromised WordPress sites account for ~7% of .top URLs.**

USE OF HTTP vs HTTPS:

The zvelo Cybersecurity Team continued their assessment and found that the majority of malicious URLs surveyed utilized HTTP as the primary scheme. That is not to say that every URL was using the standard HTTP port (80). In fact, MCAs were observed using numerous randomized TCP ports. Usage of HTTP was ~83.1% compared to ~16.9% for HTTPS.

Total URLS 3,941,143 Count of URLs	
HTTP 3,272,875 Count of URLs	
HTTPS 666,405 Count of URLs	

URL Observations | HTTP vs HTTPS
zveloCTI™ | Malicious Trends Report



zveloCTI™ | Malicious Trends Report
HTTP vs HTTPS

INDUSTRIES IMPACTED

In reviewing the malicious URLs in the dataset, the zvelo Cybersecurity Team observed MCAs leveraging online properties across a variety of different industries — Telecommunications, Information Technology, Payments, Banking, Travel, Cellular/Mobile, Insurance, Energy, and others.

These industries were observed to have either exploited web-parts used to host malware, or to have specific websites created to perpetrate fraud against unknowing consumers. It is likely that the myriad of specific organizations identified in the dataset are not aware their websites have been compromised for malicious purposes. Additionally, there is a high probability that many of these websites had been vulnerable to compromise for months, or even longer, judging by the sheer volume observed.

Within the Information Technology industry, the Linux operating system family had easily identifiable file extensions, as shown in the graphic below.

LINUX OS FILE EXTENSIONS | IT INDUSTRY

Contains: php 83,872 Count of URLs	Contains: .sh 75,184 Count of URLs	Contains: ftp 19,408 Count of URLs	Contains: ssh 14,586 Count of URLs
Contains: .rar 8,899 Count of URLs	Contains: ntp 8,166 Count of URLs	Contains: cron 6,178 Count of URLs	Contains: wget 5,725 Count of URLs
Contains: tftp 5,498 Count of URLs	Contains: elf 3,808 Count of URLs	Contains: .tar 2,640 Count of URLs	Contains: .gz 1,588 Count of URLs

Linux OS File Extensions | Information Technology Industry

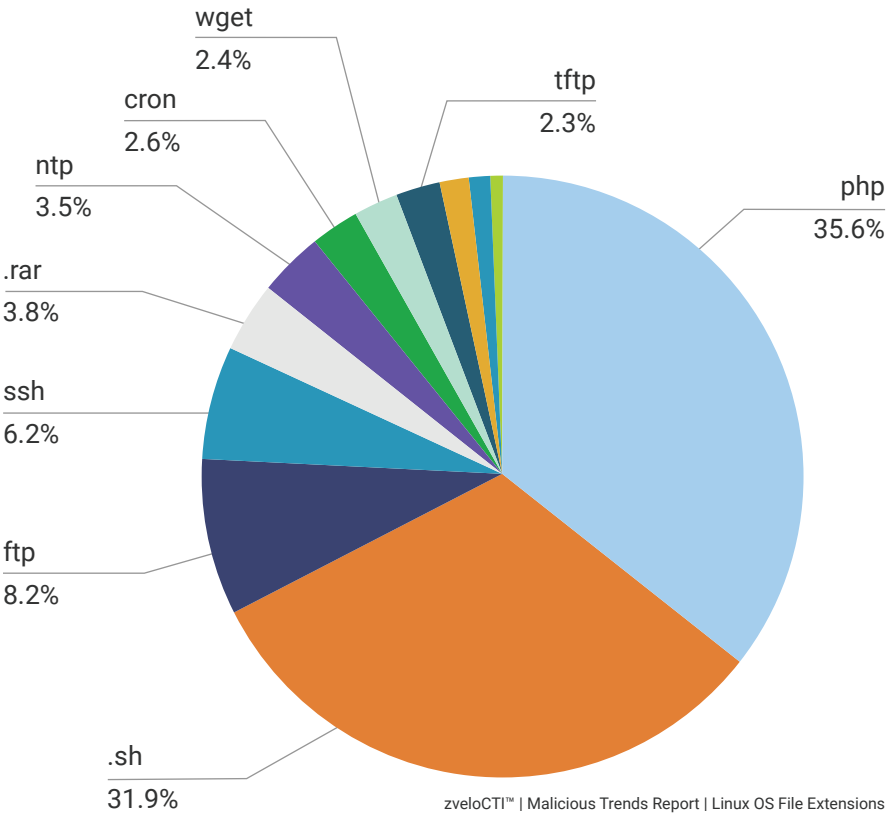
zveloCTI™ | Malicious Trends Report

THREATS BY INDUSTRY

Industries under threat or with online assets co-opted by MCAs during the 8 weeks of data reviewed include:

- **Telecommunications (Traditional)**
- **Information Technology**
- **Payments**
- **Banking**
- **Travel**
- **Cellular/Mobile**
- **Construction**
- **Insurance**
- **News/Sports**
- **Advertising**
- **Energy**

LINUX OS FILE EXTENSIONS | IT INDUSTRY



The 235,552 URLs observed represent only ~6% of the total assessed, which may indicate the MCAs' level of understanding in terms of the value Linux systems represent to their owning organizations. This is not the end of the Linux story in the dataset. The zvelo Cybersecurity Team uncovered another, more concerning issue which will be presented in the next section.

LINUX | RISK FACTOR

- **96.3% of the world's top million servers run Linux[2]**
- **90% of cloud infrastructure runs Linux[3]**
- **Organizations whose internet presence depends on Linux are facing increased risks.**

IP ADDRESS URL vs TEXT URL

A URL specifies the location of a resource on the internet. In many cases, URLs are 'text-based' (e.g. www[.]somedomain[.]com). The domains are handled by local systems utilizing the Domain Name System (DNS) to translate the human readable address into an IP address for routing across the internet.

In addition to text-based URLs, the zvelo Cybersecurity Team also observed IP address-based URLs. These types of URLs are seen when MCAs have

THREAT | DATA BREACHES

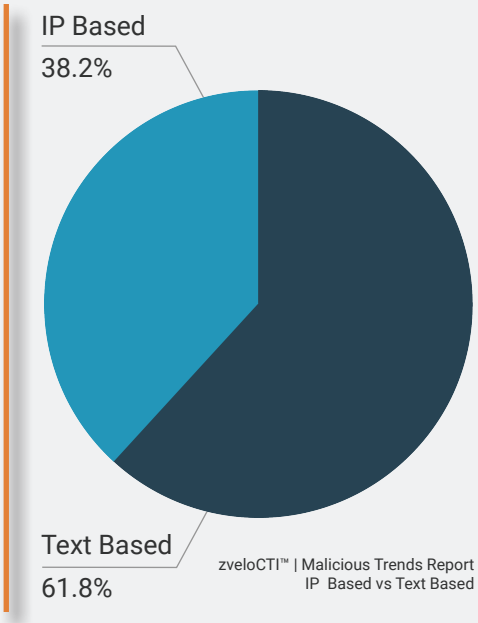
IP address-based URLs may be used to evade defenses tuned to block inbound domains. Many organizations don't filter or alert on outbound traffic. Once a victim establishes the external connection, inbound defenses allow it — exposing a security gap.

2. https://www.zdnet.com/article/can-the-internet-exist-without-linux/
3. https://hostingtribunal.com/blog/linux-statistics/

co-opted machines and route to them directly, instead of using DNS. During the investigation of the dataset used for this report, the zvelo Cybersecurity Team discovered that of the ~3.94M URLs assessed, ~1.5M were IP address-based URLs or ~38%.

Of the ~1.51M IP-based URLs, ~376.3K are associated with the Mozi malware family (an Internet of Things (IoT) botnet discovered in late 2019). Thus, Mozi accounts for Mozi malware spread peer-to-peer (P2P) via Secure Shell (SSH) bruteforce, and appears to target "cutdown" versions of Linux used in IoT devices — which in some instances, have hard-coded passwords that do not meet typical complexity requirements whatsoever. Add the ~376.3K Mozi IP-based URLs to the ~235.5K Linux URLs previously highlighted, and now the overall impact on Linux is 15% of the 3.94M URLs observed.

An additional finding in the IP-based URLs, is that ~538.6K include specific ports specified in the path (for example: hxxp://1[.]2[.]3[.]4:PORT#/evilfile). Nearly 43.3% percent of the ports used are 80 (http) and 8080 (alternate http). The rest (~57.7%) are random ports ranging from 2 to 41046. It is likely that MCAs selected the ports for each host based on what they believed would be available as viewed externally looking at the host or network firewall.



zveloCTI™ | Malicious Trends Report
IP Based vs Text Based

MISCONFIGURED WEB PARTS

From the analysis of the dataset, the zvelo Cybersecurity Team found that MCAs continue to exploit misconfigured web parts (such as Wordpress). Recently, the zvelo Cybersecurity Team defined this type of activity as 'living off the land at scale'. Much like utilizing internal network capabilities against defenders (for example, using Powershell for lateral movement), MCAs are always on the lookout for places to stash their malware. In many cases, the owner of the misconfigured web part has no idea they are hosting malware unless someone notifies them.

Of the ~3.94M URLs assessed, the zvelo Cybersecurity Team found ~610.7K or 9.6% to be (apparently) misconfigured — thus exploited — WordPress deployments.

CONCLUSIONS

The zvelo Cybersecurity Team makes the following general conclusions from the data analyzed for this report. Again, it is important to emphasize that these conclusions are intended to be high level, rather than in depth, because the implications of what has been observed will impact individual organizations very differently. When it comes to cybersecurity, it's crucial for Threat Intelligence data to be viewed based on the unique make up of an organization's Cyber Operating Environment (COE).

- Microsoft Windows and related applications continue to be a significant target for MCAs due to broad penetration of the desktop operating systems market.
- Linux, in particular IoT systems with the operating system embedded, is a much larger target for MCAs than previously thought.
- MCAs are continuing to use HTTP-based URLs more often than HTTPS.
- MCAs are extensively using IP-based URLs, apparently most often associated with Linux-based systems.
- MCAs continue to exploit misconfigured systems to gain free storage for hosting their malware.

KEY RECOMMENDATIONS

- Review any and all systems exposed to the internet.
- Inspect for misconfigurations which could be exploited by MCAs.
- Remediate any and all vulnerabilities discovered as soon as possible.
- Deny MCAs the use of these safe havens and join zvelo in making the internet safer and more secure.
- Ask for assistance if, or when, necessary! If you would like guidance on how to apply the data contained in this report to your organization's COE for actionable Threat Intelligence, please reach out to cybersecurity@zvelo.com

zveloCTI Solutions target and break the Kill Chain to disrupt attacks *before* they make it to the ActiveWeb.

zveloCTI™ SOLUTIONS

zvelo delivers a variety of Cyber Threat Intelligence (CTI) Solutions to help organizations protect against malicious activities such as those presented in this report.

- **Phishing Intelligence (Phishing Detection + Metadata)**: zvelo's AI-powered Phishing Intelligence Dataset detects phishing threats within the ActiveWeb traffic and other sensor-based data streams to deliver a richly packaged feed of highly curated and validated phishing threats that are enriched with additional data attributes like date detected, targeted brand, and more.
- **Malicious Intelligence (Malicious Detection + Metadata):** zvelo's Malicious Intelligence Dataset identifies, confirms, and enriches malicious URLs and files for direct action by defenders and analysts.
- **Suspicious New Domain Intelligence (Suspicious New Domains + Metadata):** zvelo's Suspicious Domain Intelligence combs the ProActiveWeb for signals which help identify potential threats early on to break the kill chain and block threats before they hit the ActiveWeb.

zvelo delivers meticulously curated, actionable Threat Intelligence data with industry leading accuracy and low false positive rates for maximium precision, efficacy and protection against evolving and emerging threats.

Additional Intelligence Reporting Available

- **Brand Threat Intelligence Reporting**
- **Exposed/Exploited Assets Reporting**
- **Domain Squat Reporting**

zvelo

www.zvelo.com
cybersecurity@zvelo.com