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

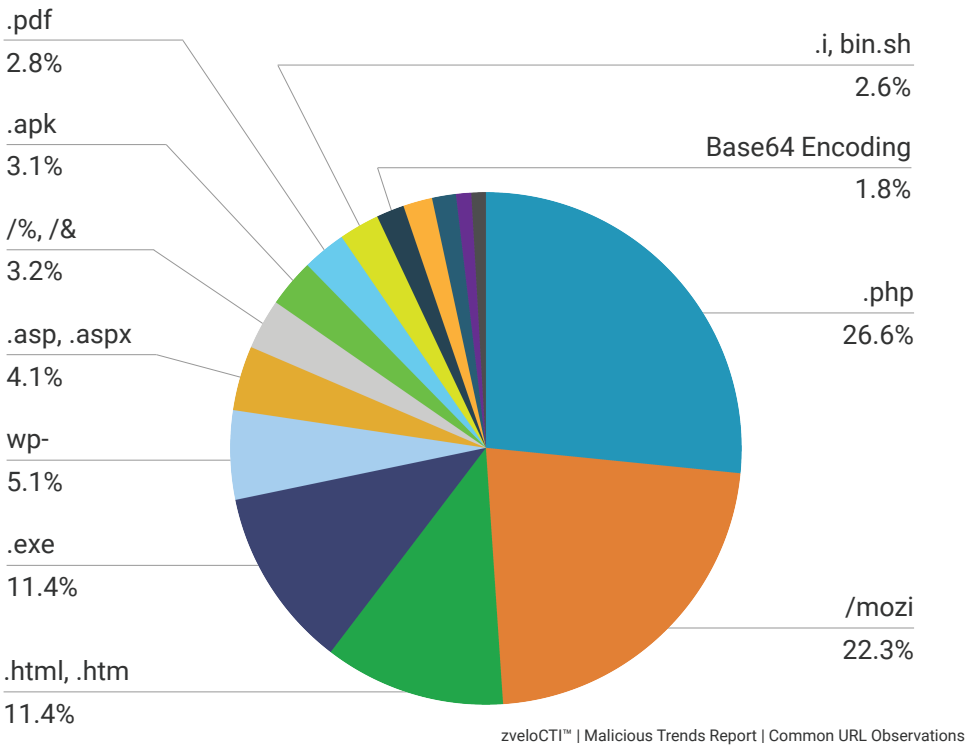
In total, common URL observations add up to 2,514,466 entries in the dataset, accounting for ~32% of the malicious URLs. Further, 684,500 common URLs appear to focus on active scripting/content which could impact multiple Operating Systems. This year's observations also show that .exe files, specifically 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
- This year's analysis shows a significant uptick in script files which accounted 11% of the URLs analyzed.
- MCAs may be looking to redirect victims over a series of hops, not just a single URL as evidenced by the observation of /% and /& path variables.

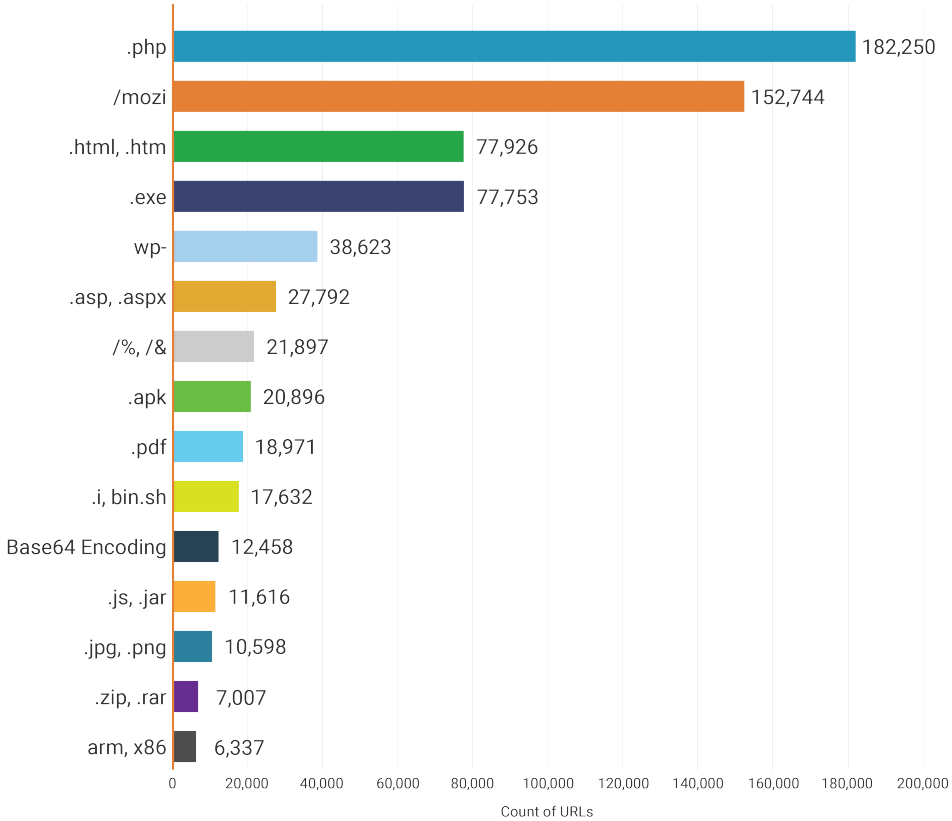
TOP 15 COMMON URL OBSERVATIONS | PERCENTAGES



zveloCTI™ | Malicious Trends Report | Common URL Observations

The top 15 common URL observations are broken out here to show the percentage of each compared to the 2.1M entries in the malicious dataset.

TOP 15 COMMON URL OBSERVATIONS | URL COUNT



Top 15 Common URL Observations | zveloCTI™ Malicious Trends Report 2021

The top 15 common URL observations are broken out here by the URL counts, rather than percentages as represented in the chart above.

MALICIOUS JAVASCRIPT

Even in 2021 Malicious Javascript remains a relevant threat. Using MDDF, the zvelo Cybersecurity Team has identified and categorized these malicious javascript files discovered on legitimate websites that have been co opted for evil, leaving the average internet user susceptible to attack. There has been a recent uptick in cases where MCAs leverage javascripts attempting to phish top companies by tricking victims into submitting their credentials for banks, social media, email providers, and more. This is higher than observed in 2020, although the normal redirects, trojans, and spyware injected into malicious javascript continue to be actively utilized and are still an attractive attack vector.

MCAs are also using heavily obfuscated malicious code in their trojanized javascripts and backdoors which often go undetected by many security vendors. White it is fairly easy to catch files dropped by clean websites that have been co-opted with malicious javascript, it is not easy to identify the dropped files as malicious when they come from seemingly legitimate URLs. Overall, it seems this attack vector is alive and well — commonly utilized by threat actors to target end users as well as to gain initial access to networks.

EXAMPLE | MALICIOUS JAVASCRIPT IN THE WILD

This is an example of malicious javascript observed in the wild (a “fake” cursor from a larger piece of code):

```
function makeNewPosition() {
var h = $(window).height() - 50, w = $(window).width() - 50, nh = Math.floor(Math.random() * h), nw = Math.floor(Math.random() * w)
return [nh, nw]
function animateDiv() {
var newq = makeNewPosition(), oldq = $(".fakeCursor").offset(), speed = calcSpeed([oldq.top, oldq.left], newq)
$(".fakeCursor").animate({ top: newq[0], left: newq[1] }, speed, function () { animateDiv()
function calcSpeed(prev, next) {
var x = Math.abs(prev[1] - next[1]), y = Math.abs(prev[0] - next[0]), greatest = x > y
x : y, speedModifier = 0.3, speed = Math.ceil(greatest / speedModifier)
return speed
```

Malware Analysis serves to help discover hidden attackers actively working to exploit your network, identify latent infections, and analyze the captured payload to help organizations protect their networks from malicious threats.

- **Static Malware Analysis** is an in-depth review of the malware binary without executing it.
- **Dynamic Malware Analysis** involves the controlled detonation of malware on a comparable victim system.
- **Advanced Dynamic Malware Analysis** includes setting up simulation infrastructure to “fool” the sample into thinking it is actually on the internet and give up its secrets.

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, .top, .cn, .ru, .xyz, .org, and .info domains. This accounts for ~69% of the malicious data set. The results (reviewing the top 15 common trends) for each are presented here with a brief summary of findings.

.COM | COMMON URL OBSERVATIONS by TLD

Total: 699,904	Contains: .php 98,634	Contains: /mozi 5	Contains: .html, .htm 34,159
Contains: .exe 47,169	Contains: wp- 22,220	Contains: .asp, .aspx 19,570	Contains: /%, /& 20,492
Contains: .apk 16,076	Contains: .pdf 15,978	Contains: .i, bin.sh 3,395	Contains: Base64 Encoding 6,069
Contains: .js, .jar 8,380	Contains: .jpg, .png 4,919	Contains: .zip, .rar 3,148	Contains: arm, x86 661

Common URL Observations by TLD | .com

zveloCTI™ 2021 Malicious Trends Report

.COM FINDINGS:

- .com URLs make up ~33% of the URLs reviewed.
- The .com TLD accounts for the majority of top 15 common trends observed.
- MCAs often rely on the .com TLD because it is usually not restricted or blocked by organizations.

.NET | COMMON URL OBSERVATIONS by TLD

Total: 217,450	Contains: .php 29,939	Contains: /mozi 1	Contains: .html, .htm 3,164
Contains: .exe 1,190	Contains: wp- 1,144	Contains: .asp, .aspx 172	Contains: /%, /& 44
Contains: .apk 2,001	Contains: .pdf 2,510	Contains: .i, bin.sh 132	Contains: Base64 Encoding 617
Contains: .js, .jar 411	Contains: .jpg, .png 982	Contains: .zip, .rar 343	Contains: arm, x86 97

Common URL Observations by TLD | .net

zveloCTI™ 2021 Malicious Trends Report

.NET FINDINGS:

- .net URLs make up ~10% of the URLs reviewed.
- .net TLD has the second most .php, .apk, and .pdf files, accounting for ~16% of the TLD.
- Similar to .com, MCAs rely on the .net TLD because it is usually not restricted or blocked by organizations.

TRENDS BY TOP LEVEL DOMAIN (TLD):

.TOP | COMMON URL OBSERVATIONS by TLD

Total: 143,560	Contains: .php 1,091	Contains: /mozi (blank)	Contains: .html, .htm 294
Contains: .exe 194	Contains: wp- 77	Contains: .asp, .aspx 124	Contains: /%, /& 5
Contains: .apk 13	Contains: .pdf 1	Contains: .i, bin.sh 66	Contains: Base64 Encoding 20
Contains: .js, .jar 66	Contains: .jpg, .png 119	Contains: .zip, .rar 29	Contains: arm, x86 11
Full-Path URLs 11,233		Base Domains, Subdomains 132,327	

Common URL Observations by TLD | .top

zveloCTI™ 2021 Malicious Trends Report

.TOP FINDINGS:

- .top URLs make up ~7% of the URLs reviewed.
- 92% of .top URLs are base domains and subdomains.
- Of note: .top base domains make up a significant portion of C2 for the ongoing IcedID campaign.

.CN | COMMON URL OBSERVATIONS by TLD

Total: 130,625	Contains: .php 2,743	Contains: /mozi (blank)	Contains: .html, .htm 1,177
Contains: .exe 3,277	Contains: wp- 280	Contains: .asp, .aspx 333	Contains: /%, /& 183
Contains: .apk 1821	Contains: .pdf 2	Contains: .i, bin.sh 50	Contains: Base64 Encoding 221
Contains: .js, .jar 310	Contains: .jpg, .png 236	Contains: .zip, .rar 108	Contains: arm, x86 35
Full-Path URLs 103,691		Base Domains, Subdomains 29,934	

Common URL Observations by TLD | .cn

zveloCTI™ 2021 Malicious Trends Report

.CN FINDINGS:

- .cn make up ~6% of the URLs reviewed.
- .cn URLs make up the third most .apk & .php files observed.
- ~79% of .cn URLs are full-path and fall outside the common trends top 15.

TRENDS BY TOP LEVEL DOMAIN (TLD):

.RU | COMMON URL OBSERVATIONS by TLD

Total: 99,446	Contains: .php 5,144	Contains: /mozi (blank)	Contains: .html, .htm 5,176
Contains: .exe 802	Contains: wp- 894	Contains: .asp, .aspx 602	Contains: /%, /& 57
Contains: .apk 87	Contains: .pdf 19	Contains: .i, bin.sh 159	Contains: Base64 Encoding 773
Contains: .js, .jar 123	Contains: .jpg, .png 999	Contains: .zip, .rar 187	Contains: arm, x86 39

Common URL Observations by TLD | .ru

zveloCTI™ 2021 Malicious Trends Report

.RU FINDINGS:

- .ru URLs make up ~5% of the URLs reviewed.
- .ru TLD has the second most Base64 encoding observed.

.XYZ | COMMON URL OBSERVATIONS by TLD

Total: 88,951	Contains: .php 2,143	Contains: /mozi (blank)	Contains: .html, .htm 915
Contains: .exe 10,991	Contains: wp- 452	Contains: .asp, .aspx 467	Contains: /%, /& 20
Contains: .apk 180	Contains: .pdf 1	Contains: .i, bin.sh 47	Contains: Base64 Encoding 221
Contains: .js, .jar 29	Contains: .jpg, .png 150	Contains: .zip, .rar 108	Contains: arm, x86 62

Common URL Observations by TLD | .xyz

zveloCTI™ 2021 Malicious Trends Report

.XYZ FINDINGS:

- .xyz URLs make up ~4% of the URLs reviewed.
- .xyz TLD has the second most .exe files observed. In short, if you receive a .exe file from the .xyz TLD, it is potentially malicious.

TRENDS BY TOP LEVEL DOMAIN (TLD):

.ORG | COMMON URL OBSERVATIONS by TLD

Total: 52,742	Contains: .php 4,612	Contains: /mozi (blank)	Contains: .html, .htm 1,469
Contains: .exe 293	Contains: wp- 1,645	Contains: .asp, .aspx 88	Contains: /%, /& 27
Contains: .apk 97	Contains: .pdf 55	Contains: .i, bin.sh 188	Contains: Base64 Encoding 627
Contains: .js, .jar 196	Contains: .jpg, .png 511	Contains: .zip, .rar 176	Contains: arm, x86 80

Common URL Observations by TLD | .org

zveloCTI™ 2021 Malicious Trends Report

.ORG FINDINGS:

- .org URLs make up ~2.5% of the URLs reviewed.
- .org TLD has the second most wp- (broken WordPress) observed; most .org TLD owners are non-profit organizations and may have limited security capabilities.

.INFO | COMMON URL OBSERVATIONS by TLD

Total: 23,741	Contains: .php 2,755	Contains: /mozi (blank)	Contains: .html, .htm 1,052
Contains: .exe 7,694	Contains: wp- 686	Contains: .asp, .aspx 213	Contains: /%, /& 7
Contains: .apk 18	Contains: .pdf 8	Contains: .i, bin.sh 47	Contains: Base64 Encoding 93
Contains: .js, .jar 19	Contains: .jpg, .png 22	Contains: .zip, .rar 620	Contains: arm, x86 10

Common URL Observations by TLD | .info

zveloCTI™ 2021 Malicious Trends Report

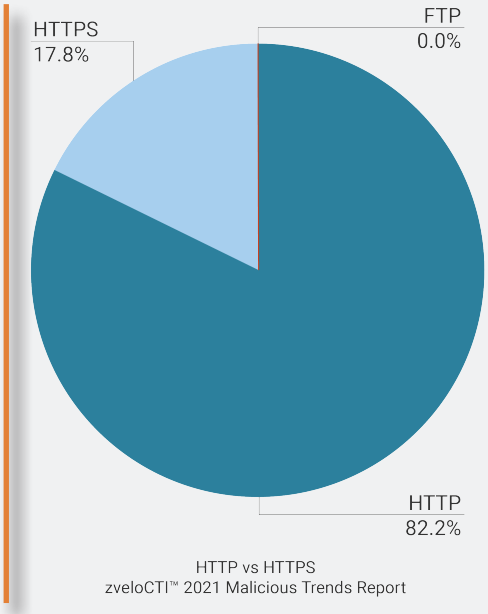
.INFO FINDINGS:

- .info URLs make up ~1.1% of the URLs reviewed.
- .info TLD has the third most .exe files observed. In short, if you receive a .exe file from the .info TLD it is potentially malicious.

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 ports (next section). Usage of HTTP was ~82.1% compared to ~17.8% for HTTPS and a small number of FTP (16 entries). Anecdotally, it is the 21st century.

AS A PROTOCOL, FTP SHOULD NEVER BE USED IN PRODUCTION SYSTEMS, AS EVIDENCED BY A RECENT FAR-REACHING CYBER ATTACK.



HTTP vs HTTPS
zveloCTI™ 2021 Malicious Trends Report

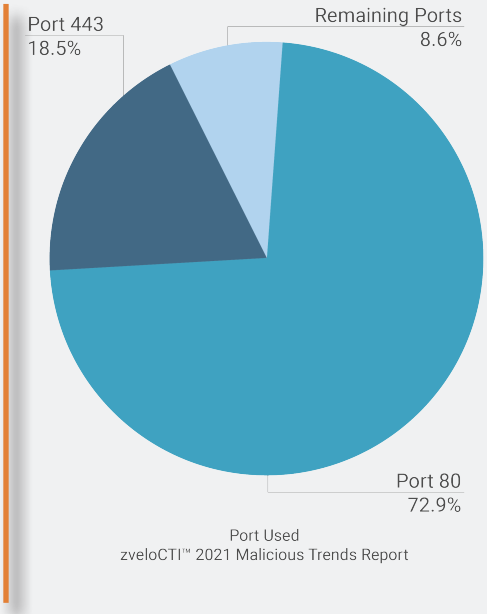
PORTS USED:

In reviewing malicious URLs, the Team found that ~73% of the ports used were Port 80, ~18.5% were Port 443, with the rest of the ports making up the remaining ~8.5%.

PORTS USED

Port 80	Port 443	Remaining Ports
1,536,303	389,911	180,337

Port Used zveloCTI™ 2021 Malicious Trends Report



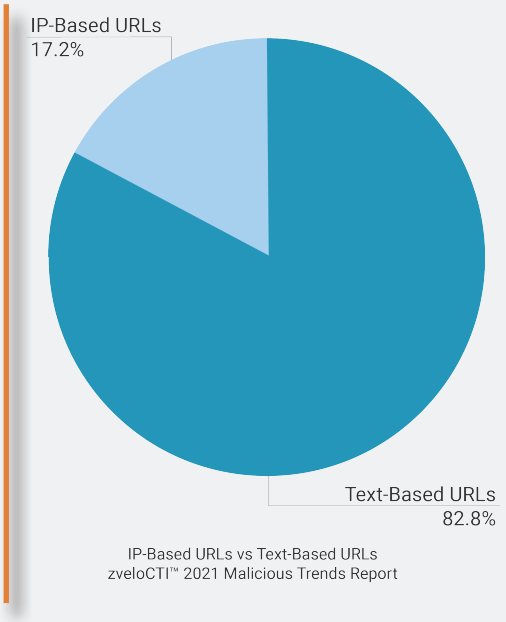
Port Used
zveloCTI™ 2021 Malicious Trends Report

Of the remaining 180,337, the bulk (~99%) appeared randomized from port 1000 to 65535 with some notable exceptions — e.g. Port 8080 and 8443, alternates for HTTP and HTTPS respectively. The apparent randomization is most likely not truly random as MCAs will tailor URLs for ports identified as being allowed through target firewalls or similar.

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 in cases where MCAs have co-opted machines and route to them directly, outside of DNS. During the investigation of the dataset used for this report, the zvelo Cybersecurity Team discovered that of the ~2.1M URLs assessed, ~438K were IP address-based URLs or ~17%.



IP-Based URLs vs Text-Based URLs
zveloCTI™ 2021 Malicious Trends Report

Of the ~438K IP-based URLs, ~150.5K 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. The impact of Mozi URLs in the threat space is ~7% of the ~2.1M URLs surveyed.

An additional finding in the IP-based URLs, are 10,641 entries that include bin.sh, which is likely linked to the BASHLITE malware known for exploiting a variety of Linux IOT variants to deliver a Distributed Denial of Service (DDoS) Attack. One unique discovery in IP-based URLs reveals 720 entries that show MCAs using Mozi to attack Netgear routers used by Satellite Internet Routers. It is interesting to note that all of the IPs in those URLs geolocate to the Far East.

END OF THE LONG TAIL

This year, the zvelo Cybersecurity Team spent time at the end of the "Long Tail". In this type of analysis, it is important to look at both the big numbers and small numbers of entries to determine if there are patterns or points of interest. Although small in number, the Team discovered potential incursions against Programmable Logic Controllers (PLC), Databases, Remote Access, and even IoT specific malware.

LONG TAIL ATTACKS

Web Alts, Port 8080, 8081, 8443 2,471	Databases, Ports 1433, 2365, 3306, 5432, 9200 937
SBIDIOT Malware 582	Remote Access, Ports 20, 21, 22, 23, 3389, 5901 397
Email, Ports 25, 110, 143, 465, 995 205	DNS, Ports 53, 5353 65
Rockwell PLCs, Ports 2222, 2223, 44818 23	GE PLCs, Port 18245, 57176 11

End of the Long Tail

zveloCTI™ 2021 Malicious Trends Report

LONG TAIL ATTACKS

Depending on the organization being targeted in these attacks, the impact of ***just one*** unknown exposed port on the internet could be devastating.

2020 RANSOMWARE LOOK BACK

2020 was the year of ransomware. It dominated the threat landscape with infections involving a variety of malware families including Ryuk, Maze, LockBit, and Netwalker, among others. MCAs targeted a broad range of verticals, including manufacturing, education, construction, facility services, food and beverage, energy and utilities, financial services, healthcare, industrial distribution, real estate, technology, and telecommunications. The top targeted vertical was manufacturing, a change from previous targets of healthcare and technology.

With all of the attacks that occurred that year, surprisingly, the second half of the year showed a sharp decline in attacks with COVID-19 related themes which have been popular since the pandemic took hold around the world. Phishing emails with malicious attachments were the top infection vector. There was a continued shift away from commodity malware such as Emotet and Trickbot. Sixty six percent of ransomware attacks have instead involved the red-teaming framework Cobalt Strike. Suggesting that ransomware actors are increasingly relying on tools in conjunction with commodity trojans.

For example, an engineering company was infected with LockBit ransomware. The adversaries used Cobalt Strike for command and control (C2) purposes, with Cobalt Strike C2 traffic being observed every six minutes. The adversaries also used an open source, post-compromise tool called "CrackMapExecWin," which is designed to automate assessments of large Active Directory networks. This tool was executed on different network ranges in the victim environment to have all the systems on those networks perform a forced Group Policy update. The Group Policy included an XML file which set up a service that executed the ransomware from a client's compromised server. The adversaries then created user accounts on compromised hosts and established remote desktop connections to targeted servers using their accounts. They evaded detection by clearing event logs. The adversaries also deployed TeamViewer, frequently used by actors to exfiltrate information.

The MCAs posted data from this attack to a site Maze uses to publish their stolen data, reflecting the fact that LockBit, along with other ransomware operations engaging in these ransomware/data theft hybrid attacks, have joined together to share resources, data, and even form a new cartel.

As Ransomware attacks continue to make headlines, organizations must evolve towards fighting Ransomware with a Defense in Depth strategy which leverages a range of security tools. The most commonly missing element of a Defense in Depth strategy is having both comprehensive Cyber Threat Intelligence and a dedicated team of security professionals who understand how to derive actionable Threat Intelligence from what would otherwise just be potentially useful data about threats.

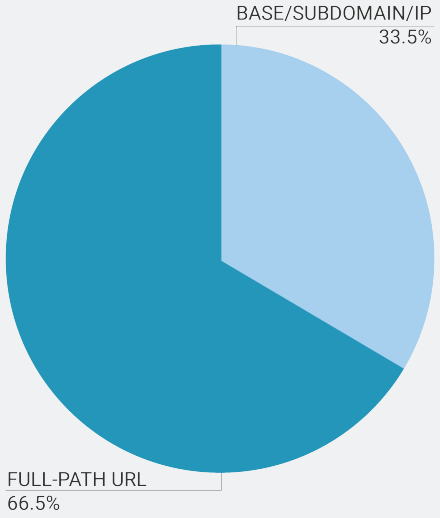
MALICIOUS CONCLUSIONS

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).

- MCAs use the .com TLD extensively because organizations rarely inspect traffic from it.
- MCAs continue to use HTTP-based URLs more often than HTTPS. Additionally, MCAs utilize ports other than 80 and 443 which they have identified as ports that are allowed through specific target firewalls.
- MCAs are extensively using IP-based URLs, apparently most often associated with Linux-based systems.
- Some TLDs (.xyz and .info) are more likely to host malicious .exe files than others.
- Although MCAs continue exploiting misconfigured systems (e.g. Wordpress) to gain free storage for their malware, those numbers have decreased from what we observed in 2020.

THE ZVELO CYBERSECURITY TEAM RECOMMENDS YOU REVIEW ANY SYSTEMS EXPOSED TO THE INTERNET TO INSPECT FOR MISCONFIGURATIONS WHICH COULD BE EXPLOITED BY MCAS, AND REMEDIATE ANY VULNERABILITIES.

- **~67% of malicious threats were detected in full-path URLs vs base domain, subdomain, and IP.**



Malicious URLs Detected at Full-Path vs Base/Subdomain/IP
zveloCTI™ 2021 Malicious Trends Report

PHISHING DATA

TRENDS BY THE NUMBERS

To start, the zvelo Cybersecurity Team reviewed the entirety of the data — 946+ thousand entries from our phishing detection system. The Team then analyzed the data for obvious common trends. The resulting trends observed proved interesting.

- The top 15 common words (and related words) that stood out included: login and signin, bank and banks, account, card and cards, mail and webmail, payment and pay, help and support, file and files, health, delivery and tracking, password, authentication and verification, office, billing and invoice, and customer.
- In the phishing space, it is apparent that MCAs are looking to harvest user credentials (~16.5% of the time) with URLs including 'login', 'signin', 'password', 'authentication' and 'verification'.
- URLs including the words 'bank', 'banks', 'account', 'payment', 'pay', 'billing', and 'invoice', account for 244,758 entries or ~26%. This indicates phishing MCAs have a distinct focus on perpetrating financial crimes.

TOP 15 COMMON WORDS OBSERVED

Total	login, signin	bank, banks	account
946,556	142,381	92,254	58,970
card, cards	**mail, webmail**	**payment, pay**	**file, files**
51,780	50,195	36,998	29,752
help, support	**health**	**delivery, tracking**	**password**
28,277	18,215	8,193	7,221
authentication, verification	**office**	**billing, invoice**	**customer**
7,147	5,212	4,756	4,381

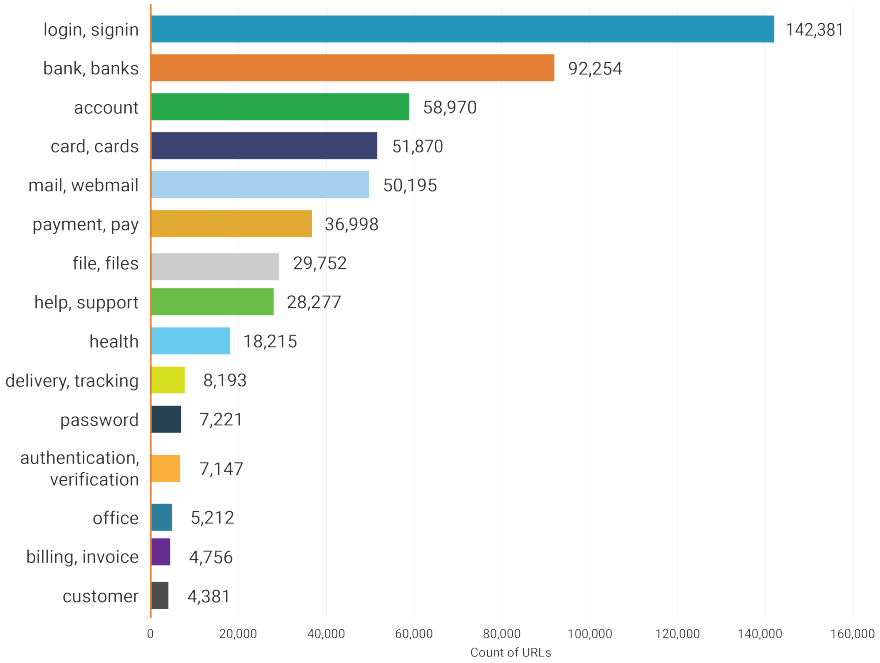
Phishing Trends by the Numbers | Top 15 Common Words by URL Counts

zveloCTI™ 2021 Malicious Trends Report

RESULTING TRENDS OBSERVED

- Top 15 common, and related, words that stood out:
  - Login and signin
  - Bank and banks
  - Account
  - Card and cards
  - Mail and webmail
  - Payment and pay
  - Help and support
  - File and files
  - Health
  - Delivery and tracking
  - Password
  - Authentication and verification
  - Office
  - Billing and invoice
  - Customer
- ~16.5% of the time, MCAs are looking to harvest user credentials.
- ~26% of the time, MCAs have a distinct focus on perpetrating financial crimes.

TOP 15 COMMON WORDS OBSERVED | URL COUNT



Top 15 Common Words Observed in Phishing URLs | zveloCTI™ 2021 Malicious Trends Report

The top 15 common words observed in phishing URLs are represented by URL count in the graph to the left.

TRENDS BY TOP LEVEL DOMAIN (TLD):

As this is the first year that zvelo's Cybersecurity Team has specifically assessed phishing data, it is interesting to note that the .com TLD was seen most frequently (~41%) — similar to what we observed with the malicious URLs.

TOP 15 COMMON URL OBSERVATIONS

Total 946,556	.com 393,208	.ru 46,015	.cn 36,549
.org 34,117	.xyz 31,212	.co 29,941	.net 27,203
.tk 16,422	.ml 13,625	.uk 10,525	.ga 10,150
.cf 9,997	.info 9,481	.de 8,977	.site 7,530

Phishing Trends by the Numbers | Top 15 TLDs by URL Counts zveloCTI™ 2021 Malicious Trends Report

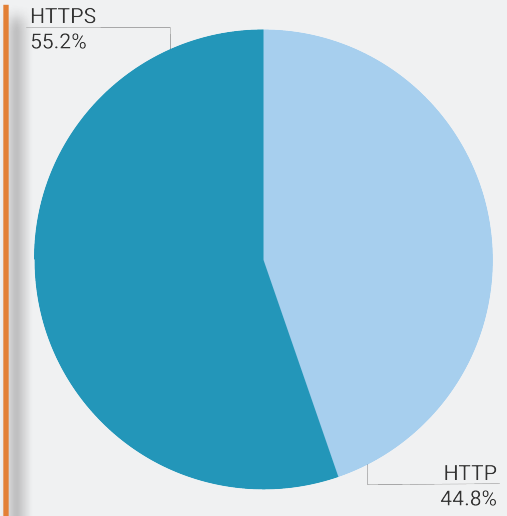
KEY FINDINGS:

- .com, .net, .org, .co (presumably legitimate) URLs make up 484,469 (~51%) of those reviewed.
- .xyz, .info, and .site (usually suspicious) URLs make up 48,223 (~5%) of those reviewed.
- Country-based (.ru, .cn, .tk, .ml, .uk, .ga, .cf, and .de) URLs make up 150,260 (~16%) of those reviewed.

USE OF HTTP vs HTTPS:

The zvelo Cybersecurity Team continued their assessment and found that the majority of phishing URLs surveyed utilized HTTPS as the primary scheme. However, the split is not as wide as expected only ~55% (HTTPS) to ~45% (HTTP). In many cases, the initial HTTP URL will redirect to an HTTPS URL. If that is taken into account the use of HTTPS approaches 90%.

Because this is the first year the Team has assessed phishing specific data, it will be important to see how this trend changes over time. With anywhere from 80% to 90% of internet traffic encrypted, it is reasonable to expect that future analyses will show MCAs trend more toward usage of HTTPS over HTTP.



HTTPS vs HTTP in Phishing URLs
zveloCTI™ 2021 Malicious Trends Report

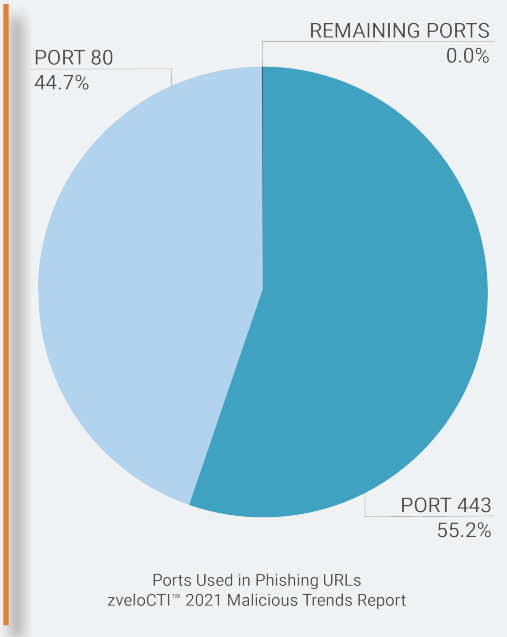
PORTS USED:

In reviewing phishing URLs, the Team found at ~55% of the ports used were Port 80, ~45% were Port 443, with the rest of the ports making up the rest at ~0.001% (185 entries).

PORTS USED

Port 443	Port 80	Remaining Ports
523,368	423,003	185

Ports Used in Phishing URLs zveloCTI™ 2021 Malicious Trends Report



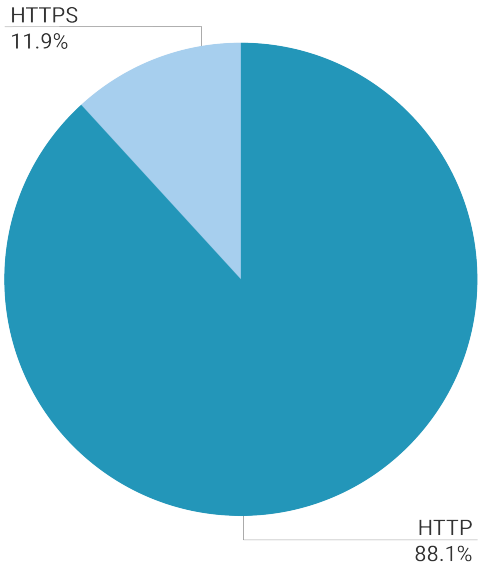
Ports Used in Phishing URLs
zveloCTI™ 2021 Malicious Trends Report

Of the remaining 185 ports, the top two ports were 2096 (24 entries) and 3000 (19 entries). Port 2096 is used by a commercial webmail vendor that hosts email for customers worldwide. Port 3000 is used by several vendors of Voice/Video over IP (VoIP) devices. These specific ports demonstrate that MCAs are aware of the “one off” usage of ports in their targeting.

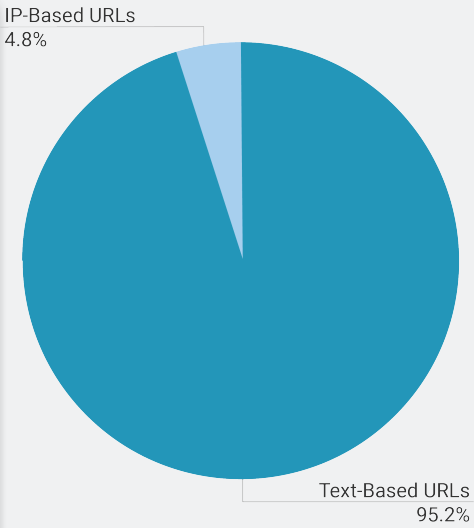
IP ADDRESS URL vs TEXT URL

In addition to text-based URLs in phishing, the zvelo Cybersecurity Team also observed IP address-based URLs. During the investigation of the dataset used for this report, the zvelo Cybersecurity Team discovered that of the ~946K URLs assessed, only ~46K were IP address-based URLs or ~5%.

Behaviorally, this is not surprising as many phishing prevention solutions will automatically filter out IP-based URLs. However, as seen in the data, MCAs are still finding organizations that are not tackling this problem. Of note, 24,213 IP-based URLs use just IP-address as the path, and use the HTTP scheme ~88% of the time.



IP-Based URLs Using HTTP Scheme in Phishing
zveloCTI™ 2021 Malicious Trends Report



IP-Based URLs vs Text-Based URLs in Phishing
zveloCTI™ 2021 Malicious Trends Report

BRAND TARGETS BY VERTICAL:

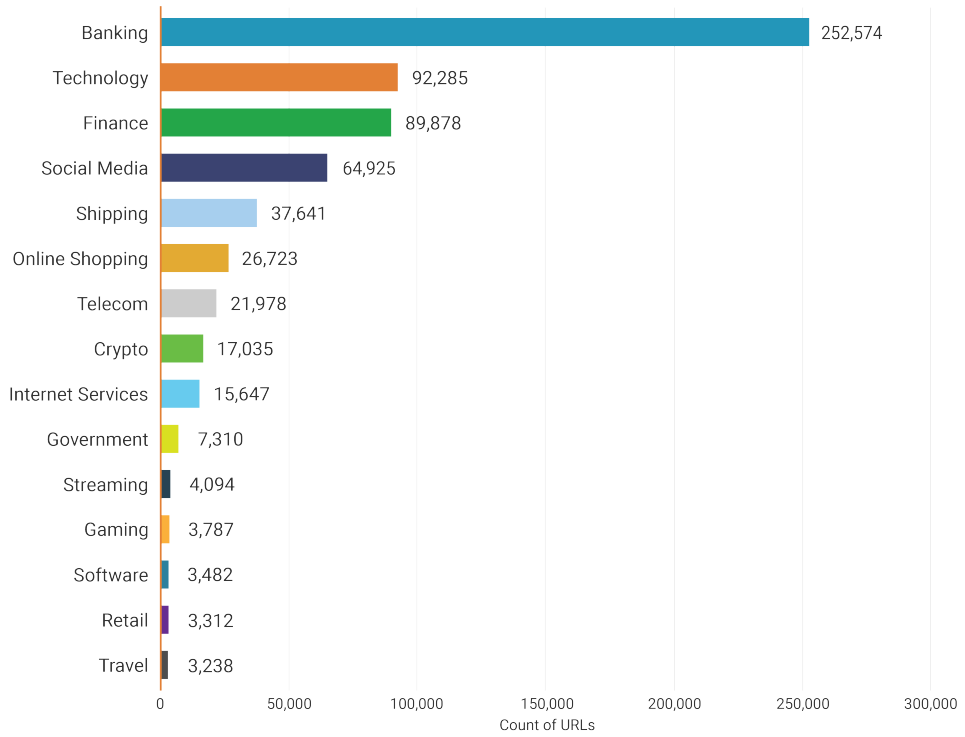
Unique to phishing, there are a wide variety of brands that are being targeted by MCAs. In assessing brands, the zvelo Cybersecurity Team grouped the brands by type to identify the top 15 impacted business areas. This is shown in the following charts.

BRAND TARGETS | TOP 15 IMPACTED VERTICALS

Total 648,208	Banking 252,574	Technology 92,285	Finance 89,878
Social Media 64,925	Shipping 37,641	Online Shopping 26,723	Telecom 21,978
Crypto 17,035	Internet Services 15,647	Government 7,310	Streaming 4,094
Gaming 3,787	Software 3,482	Retail 3,312	Travel 3,238

Phishing Trends | Top 15 Brand Verticals Targeted by URL Counts

zveloCTI™ 2021 Malicious Trends Report



Top 15 Brand Verticals Targeted in Phishing Attacks | zveloCTI™ 2021 Malicious Trends Report

BRAND TARGET FINDINGS:

- Top 15 Impacted Verticals:
  - Banking
  - Technology
  - Finance
  - Social Media
  - Shipping
  - Online Shopping
  - Telecom
  - Crypto
  - Internet Services
  - Government
  - Streaming
  - Gaming
  - Software
  - Retail
  - Travel
- Brands within the Banking and Finance categories make up ~52% (342,452 entries) of those targeted by MCAs.
- Brands within the remaining top 15 categories make up ~46% (301,457 entries) targeted.

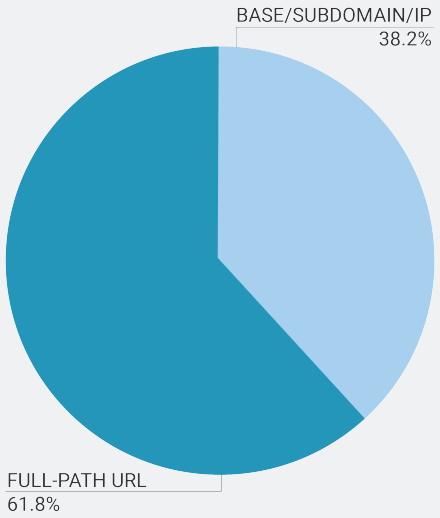
PHISHING CONCLUSIONS

The zvelo Cybersecurity Team makes the following general conclusions from the phishing 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).

- MCAs use the .com, .net, .org, .co TLDs extensively in phishing because organizations rarely inspect traffic from them.
- MCAs use more HTTPS than HTTP in phishing to appear more legitimate to consumers, and because organizations generally presume that encrypted web-traffic is safe.
- In phishing, MCAs do use ports other than 80 and 443, although it accounts for an extremely small percentage observed.
- MCAs rarely use IP-based phishing URLs.
- In phishing, MCAs are targeting end users to gain access to their finances the majority of time. It is likely that even the phishing attempts lacking an obvious financial 'angle' have the same end goal.

THE ZVELO CYBERSECURITY TEAM RECOMMENDS IMPLEMENTING ANY AND ALL AVAILABLE TECHNICAL MITIGATIONS IN AN ORGANIZATION TO PREVENT PHISHING *BEFORE* THESE URLS LAND IN A USER'S INBOX. ADDITIONALLY, ORGANIZATIONS SHOULD ALSO FOCUS ON NON-TECHNICAL MITIGATIONS SUCH AS USER TRAINING, WHICH IS ULTIMATELY THE BEST PREVENTION FOR PHISHING.

- **~62% of phishing threats were detected in full-path URLs vs base domain, subdomain, and IP.**



Phishing URLs Detected at Full-Path vs Base/Subdomain/IP
zveloCTI™ 2021 Malicious Trends Report

COMPARING MALICIOUS AND PHISHING TRENDS

The zvelo Cybersecurity Team compared the trends between the malicious and phishing datasets and made the following assessments.

KEY COMMONALITIES

- Malicious and phishing MCAs both use a mix of HTTP (Port 80) and HTTPS (Port 443).
- The main TLD observed was .com for both malicious (~33%) and phishing (~41%). This is likely because most organizations implicitly trust the .com TLD as always legitimate.

KEY DIFFERENCES

- Malicious MCAs use more HTTP (Port 80), ~82% of the time compared to phishing MCAs at 44% of the time. This is likely due to the fact that encryption can impact the responsiveness of beacons, malware C2, and so on.
- Phishing MCAs use more HTTPS (Port 443), ~55% of the time compared to malicious MCAs at ~18% of the time. This is likely because organizations are beginning to filter traffic (at scale) to accept only HTTPS connections, presuming that HTTP connections are not legitimate or secure.
- Malicious MCAs use more IP-based URLs (~17%) compared to phishing MCAs (~5%). The Team's observations indicate this likely due to the fact that malicious MCAs are specifically targeting IoT devices and exposed Linux-based systems which do not utilize DNS.

zveloCTI solutions are designed to 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 and phishing activities such as those presented in this report.

zveloCTI FEEDS AVAILABLE NOW

- **PhishBlockList (PBL):** Multi-source and proprietary data to disrupt phishing attacks (MITRE T1566). 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 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). zvelo's Malicious Intelligence Dataset identifies, confirms, and enriches malicious URLs and files for direct action by defenders and analysts.

zveloCTI FEEDS AVAILABLE 2022

- **Suspicious New Registration 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"). 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.

zveloCTI REPORTING OFFERED

In addition to CTI, zvelo can help organizations identify and mitigate their cyber risks through detailed threat reporting specific to an organization's unique Cyber Operating Environment (COE).

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

ADDITIONAL OFFERINGS INCLUDE:

- **zveloDB —** URL Classification Database. Market-leading classified URL database with excellent accuracy, coverage, updating and performance. Ideal for integration with web filtering, parental controls, contextual targeting, brand safety, and more where local deployment and very fast lookups are required.
- **zveloCAT —** Real-time, full-path URL classification service. Build custom solutions and applications that take advantage of fast, highly accurate, full-path URL categorizations. Ideal for applications that require classification of content at the page, post or article level.

zvelo

www.zvelo.com
cybersecurity@zvelo.com