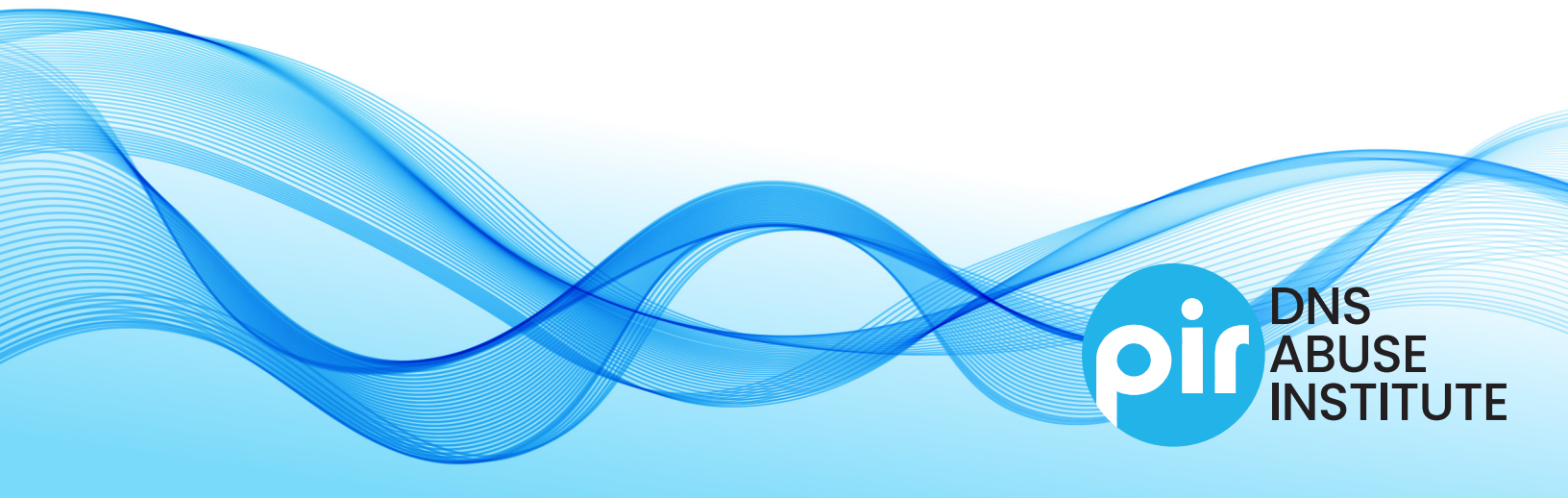
NOVEMBER 2022 REPORT



DNS ABUSE INSTITUTE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report is the third publication from the DNS Abuse Institute's measurement initiative: **DNSAI Compass**.

In previous reports, our methodology identified a decreasing number of unique domains engaged in the distribution of malware. This report sees an increase in levels of malware, returning to, and slightly exceeding those of May 2022, our first month of reporting. We offer some information shared with us from the research community as to why this might be and will continue to monitor.

Our outreach work continues across the DNS Community. We encourage all registrars and registries to get in contact with us and take the opportunity to view the data associated with their registrar or registry. These meetings typically yield insights for both the registry or registrar and the DNSAI.

We have also engaged across the wider community on our measurements, including virtual and in-person presentations at the **Global Forum on Cyber Expertise (GFCE) Triple-I Day** hosted in India, the Latin American and Caribbean Top-Level Domains (LACTLD) Workshop, the **ICANN Contracted Parties Summit**, and the 'State of the DNS' eco Workshop with the European Commission.

This engagement has reinforced the importance of DNS Abuse measurement in current DNS Community discussions. One recurring theme we observed in our outreach is the importance of using specific language and granular measurement. Sometimes 'DNS Abuse' can be used as shorthand for 'mitigation is appropriate at the DNS level'. This isn't always the case and to move the conversation forwards, we need to get more granular. We can do this, for example, by recognising the need to determine whether the registration is malicious or compromised, understanding the evidence available, and considering the potential for collateral damage.

We look forward to continuing these discussions and encourage anyone interested to get in touch.

The **methodology** for this report is the same as all other reports (v1.0) and we encourage readers to consider this detailed methodology and contact us with questions, ideas, or suggestions to help us improve this initiative. After all, we are here to support the DNS Community and make it better equipped to tackle DNS Abuse.

The DNS Abuse Institute will periodically publish reports on **DNSAI Compass**.

ABOUT

The **DNS Abuse Institute** (DNSAI or the "Institute") was created in 2021 by **Public Interest Registry** ("PIR") in pursuit of its non-profit mission. The Institute aims to reduce DNS Abuse and empower the DNS community.

The Institute created DNSAI Compass ("Compass") as a reliable, independent, transparent, and sufficiently granular way of measuring DNS Abuse in order to ultimately reduce it at the DNS level.

Compass is a collaboration with **KOR Labs**, led by **Maciej Korczynski** from Grenoble INP-UGA. This data is then provided to the DNSAI. DNSAI then works with PIR's Data Analytics team to create the interactive charts and for the purposes of writing this report.

Our priorities for Compass are:

- **Transparency**: The methodology that collects, cleans, and aggregates the data must be as transparent as possible. To the extent that anyone should wish to, they could replicate the process.
- **Credibility and Independence**: We aim to have an academically robust and independent approach, separate from commercial interests.
- **Accuracy and Reliability**: The goal of these reports is to enable focused conversations, and to identify opportunities for abuse reduction. The data needs to be of high enough quality to serve as the foundation for meaningful changes to the ecosystem.

Our first report from **September 2022** [1] provides the methodology and further context on the background and development of this initiative.

Our approach is one of collaboration and engagement, and we endeavor to speak to interested parties and provide them with early access to data that concerns their organization. We are committed to refining this project as work continues and welcome insights from across the industry to help us iterate and improve. If you would like to review your data, please **contact us**.

For clarity, Compass exists completely independently of **NetBeacon**, the centralized abuse reporting service we created for the benefit of the DNS. Reports from NetBeacon do not go into our measurement work with Compass. This is a conscious choice to optimize and encourage usage of NetBeacon and prevent any abuse of NetBeacon as an attempt to influence Compass data. See the **methodology** for more information on how domains are included in Compass.

[1] Available at: https://dnsabuseinstitute.org/dnsai-compass/

Understanding this Report

This report is the third publication from the DNS Abuse Institute's measurement initiative: **DNSAI Compass**.

This report shows high level aggregate data from **May to September 2022.**

It focuses on the use of the DNS for phishing and malware:

- **Phishing** is an attempt to trick people into sharing important personal information— banking information, logins, passwords, credit card numbers.
- **Malware** is malicious software designed to compromise a device on which it is installed.

It includes the following charts:

- **Chart 1: Aggregate Trends**
- **Chart 2: Mitigation**
- **Chart 3: Registrar Median Mitigation Time**
- **Chart 4: Malicious vs. Compromised**

Our **methodology** provides important context and we recommend it is read in full.

Each chart is accompanied by:

- '**About this Chart**' to help the reader understand the data being displayed, and;
- '**Commentary**' where we have added any observations on the data.

Where we are showing data over time, the intent is to try and demonstrate trends, year over year, and we are therefore hoping to be able to display about two years of data depending on functionality and viewability.

GENERAL DNS ABUSE TRENDS

These charts are available in an interactive format on our **website**. They provide a broad overview of our findings on DNS Abuse trends.

Chart 1: Aggregate Trends

About this Chart

This chart provides a high level view on how much DNS Abuse has been identified by our methodology, and how it's changing over time. It shows the absolute volume of unique domains our methodology has identified are engaged in phishing and malware, broken out by category.

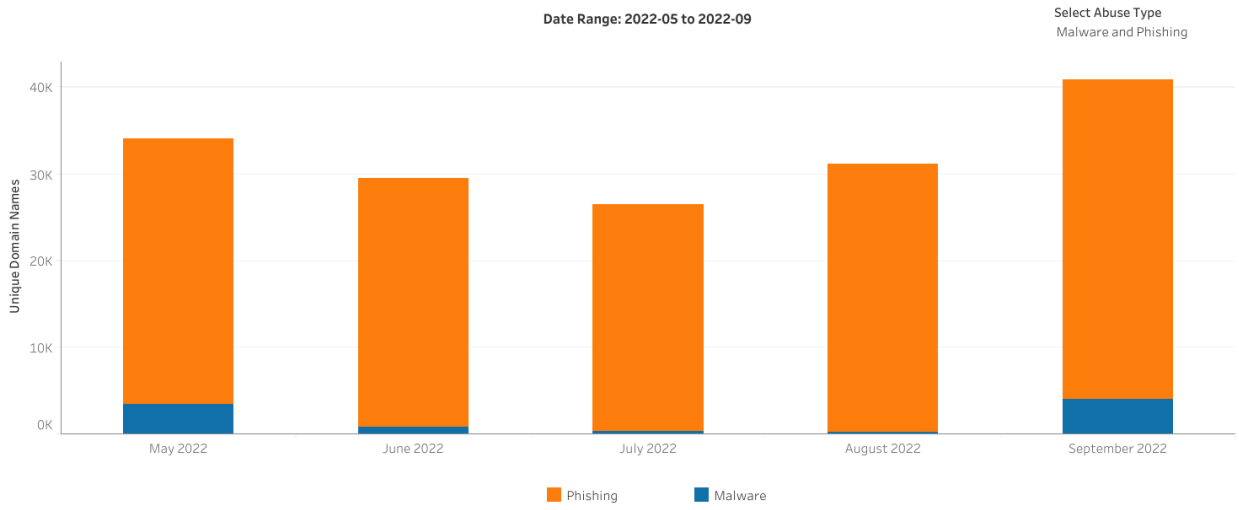


*Figure 1: Aggregate Trends - **Phishing and Malware***

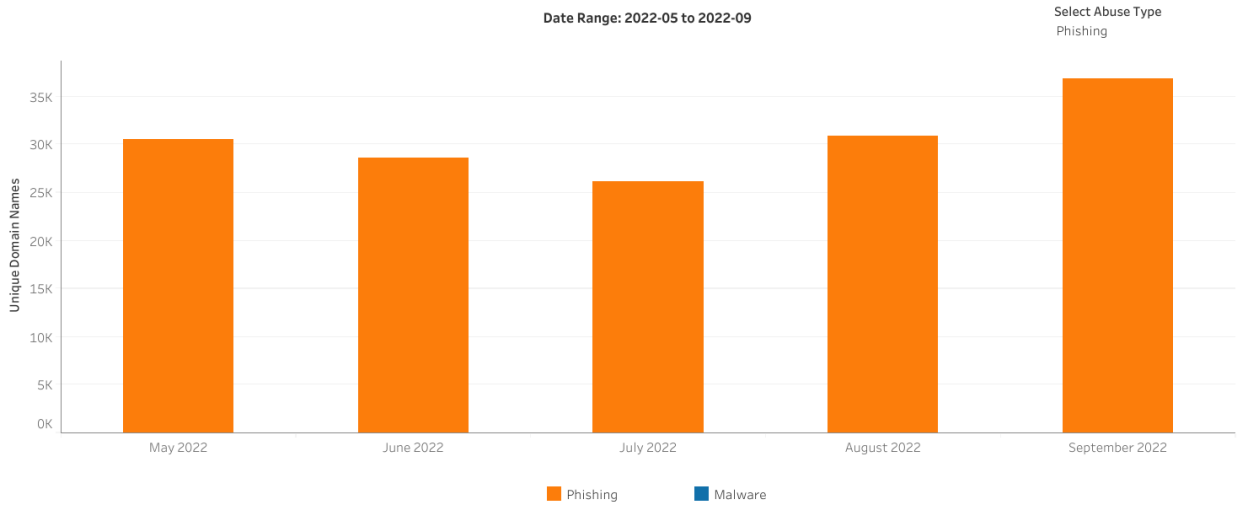


*Figure 2: Aggregate Trends - **Phishing***

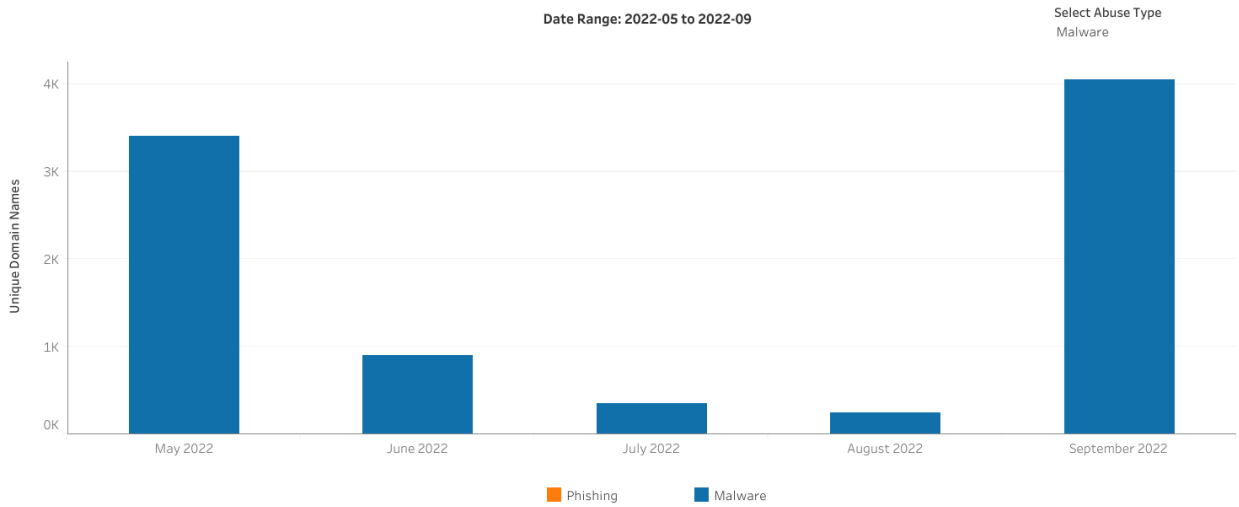


*Figure 3: Aggregate Trends - **Malware***

Commentary

In previous reports we observed a drop in the number of malware domains identified by our methodology. This month, the number of malware domains we observed increased substantially, returning to similar levels seen in May.

A discussion with Roman Huessy (abuse.ch), who kindly provides the URLHaus malware feed for our Compass reports, indicated that the observed decline between June and August may be related to the temporary inactivity of the EMOTET malware. According to security group Cryptolaemus, one of the leading reporters of malicious URLs to URLhaus[2], EMOTET started new email phishing campaigns in early November 2022,[3] which may be linked to the increase in malware delivery URLs observed in URLHaus beginning from September.

Our methodology continues to identify more occurrences of phishing than malware. This is inline with existing measurement reporting initiatives, such as ICANN's DAAR project.

2 https://urlhaus.abuse.ch/statistics/
3 https://www.techspot.com/news/96560-emotet-botnet-came-back-dead.html

Chart 2: Mitigation

About this Chart

This chart provides a high level view on how much DNS Abuse mitigation has been identified by our methodology, and how it's changing over time. The methodology includes a process to determine whether any mitigation has been observed. This involves taking an initial measurement of various factors related to the URL and repeating these measurements for one month. Further details are set out in the **methodology**.

This results in four labels:

- **Mitigated**: We detected that a mitigating action has occurred. This action could have been taken by a registrar, registry, a hosting provider, or another relevant actor, including the registrant.
- **Not Mitigated:** We did not detect any indication of mitigation.
- **Uncategorized**: We were unable to determine whether or not mitigation occurred.
- **Unprocessed**: The domains were not processed due to network connectivity, server problems, or other similar issues.

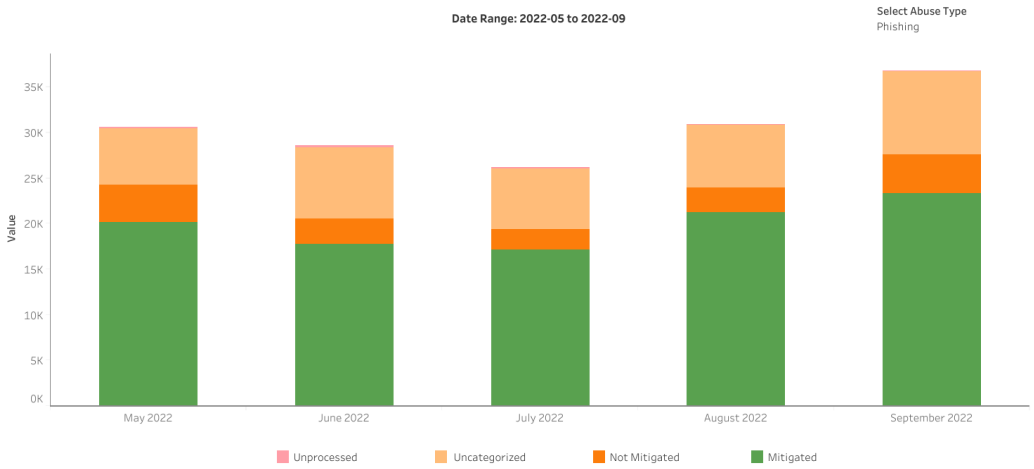


*Figure 4: Mitigation - **Phishing***

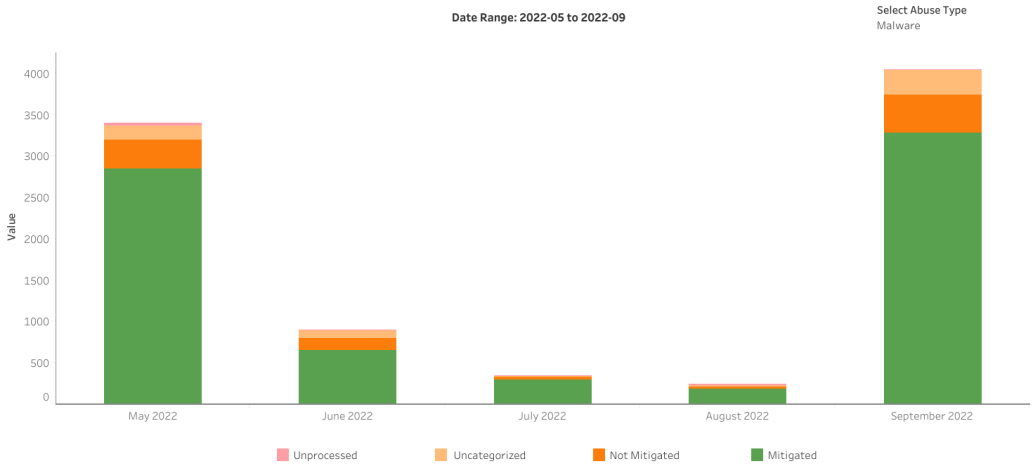


*Figure 5: Mitigation - **Malware***

Commentary

The proportion of domains for which we were unable to categorize as malicious or compromised is higher for phishing than malware. One possible reason for this is the evasion techniques outlined in the **methodology**.

Missing or limited data is challenging to manage in any data-driven project. In the pursuit of transparency, we have identified the number of domains that we were unable to categorize or unable to process.

For future reports, we are working to balance the principles of accuracy and reliability with the desire to compare trends over time. We want this to be a project of iterative improvement with increasing accuracy . However, we also want the ability to compare trends over months and years. We are working on improving the breadth of coverage for categorization of mitigation activity, while avoiding significant changes to the existing categorization methodology for domains that could be categorized. See the **methodology** for further details.

Chart 3: Registrar Median Mitigation Time

About this Chart

This chart is intended to show the observed time taken to mitigate phishing and malware, and how it is changing over time. For the domains that our methodology determined were mitigated, this chart shows how many registrars had a median time to mitigation in each category.

After an initial measurement, KOR Labs repeats measurements for one month to determine if mitigation has occurred. The intervals used are (starting at the time of acquiring the URL from the blocklist): 5m, 15m, 30m, 1hr, 2hr, 3hr, 4hr, 5hr, 6hr, 12hr, 24hr, 36hr, 48hr, and then once every 12 hours for one month.

While we are describing this information as a "median registrar mitigation time", it should be noted that we do not know definitively that it was the registrar that took action. This data could include mitigation taken by the registry, the host, or any other relevant party. The reference to a registrar is indicative that the domain is under their management.

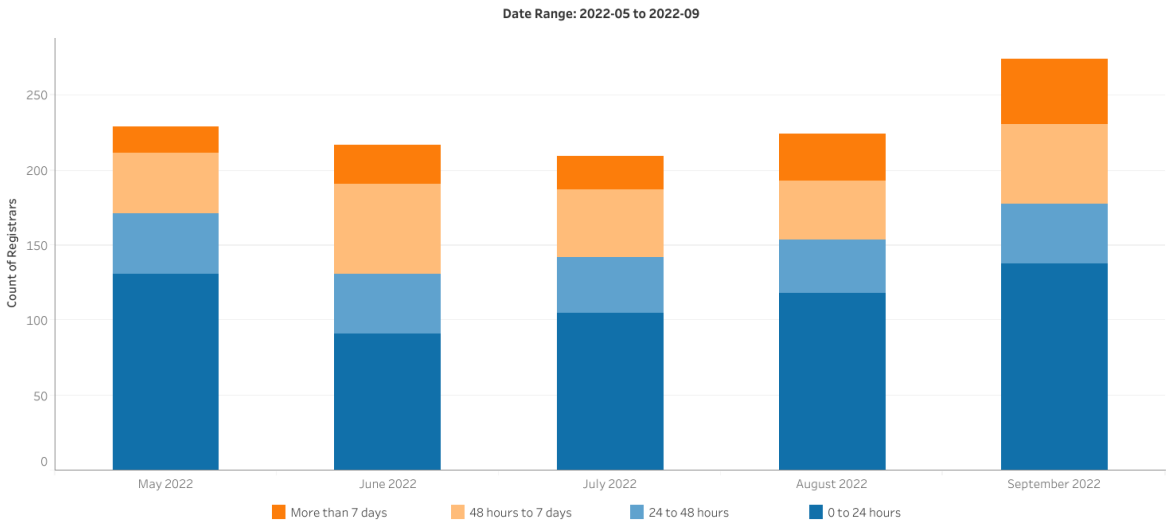


Figure 6: Registrar Median Mitigation Time

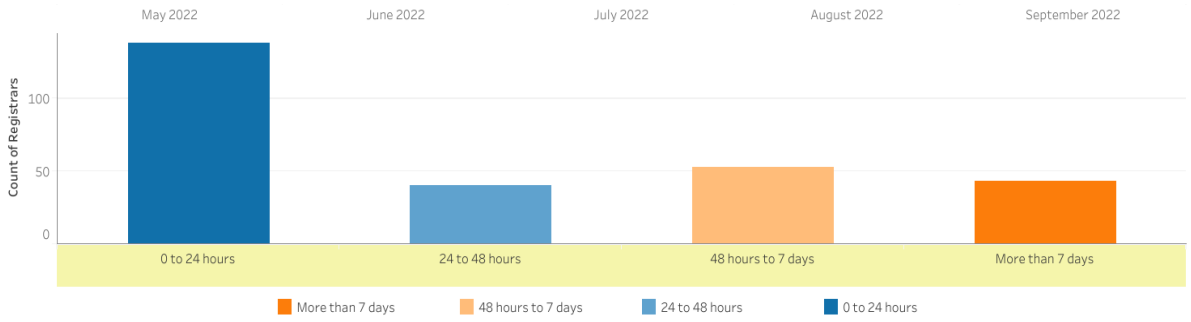


*Figure 7: Registrar Median Mitigation Time - **September 2022***

Commentary

There is no agreed upon industry standard for how quickly mitigation should occur. This makes the presentation of mitigation time challenging. We believe there is a general industry view that mitigation within 24 hours is considered a quick response to sufficient evidence of phishing or malware. As phishing and malware are quite time-sensitive issues, with most harm happening at the start of the attack, we believe that mitigation after 7 days is not quick enough to prevent and disrupt harm, which is why we have included "More than 7 days" as a specific category.

Chart 4: Malicious vs. Compromised

About this Chart

This chart is intended to show the observed registration type (malicious vs. compromised) and how this is changing over time.

Our methodology includes three labels:

- **Malicious**: a domain registered for malicious purposes (i.e., to carry out DNS Abuse).
- **Compromised**: A benign domain name that has been compromised at the website, hosting, or DNS level.
- **Uncategorized**: A domain that our methodology was unable to categorize for a number of reasons, including problems in collecting the metadata necessary to categorize domain names accurately.

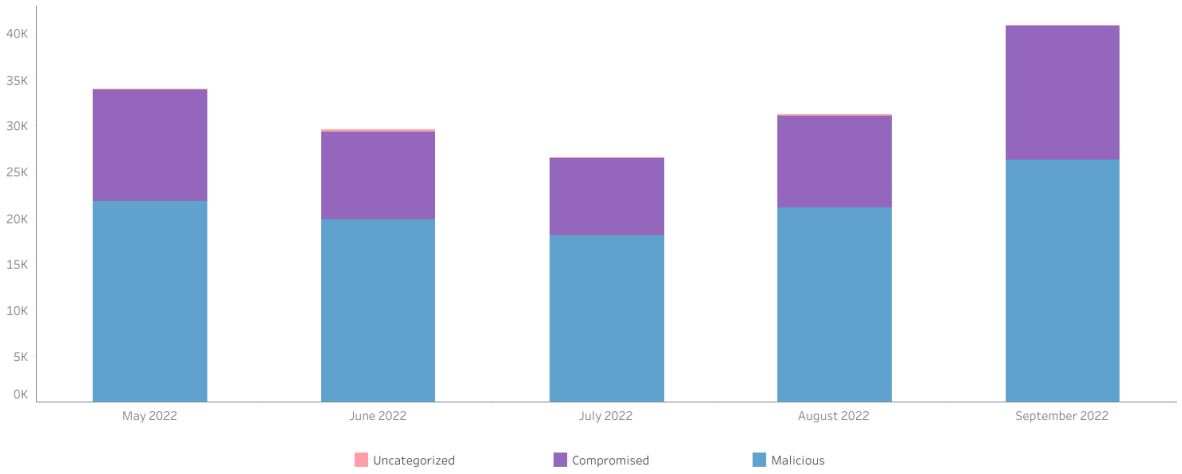


*Figure 8: Compromised vs Malicious - **Phishing and Malware***

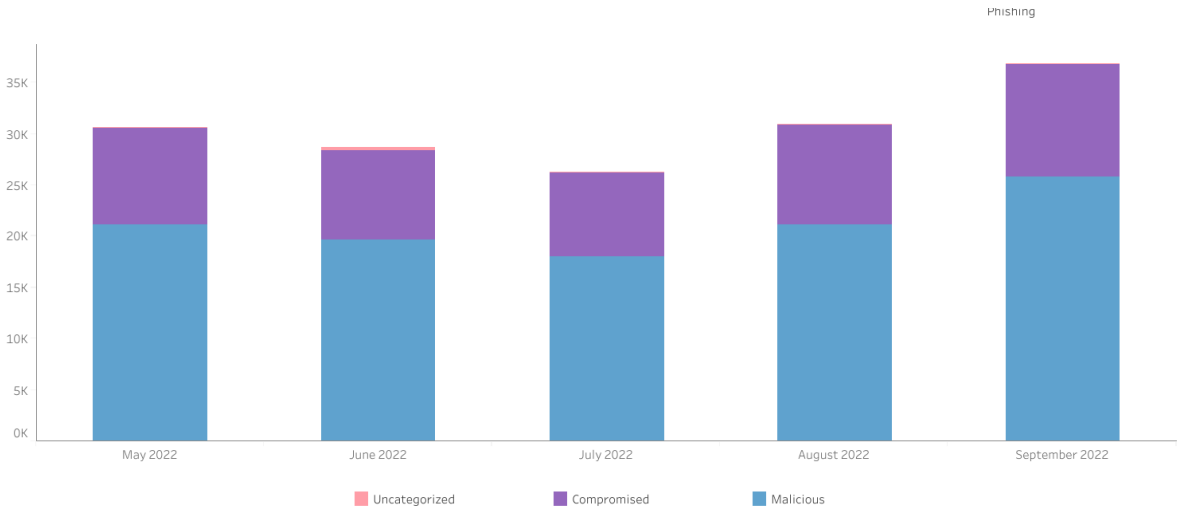


*Figure 9: Compromised vs Malicious - **Phishing***

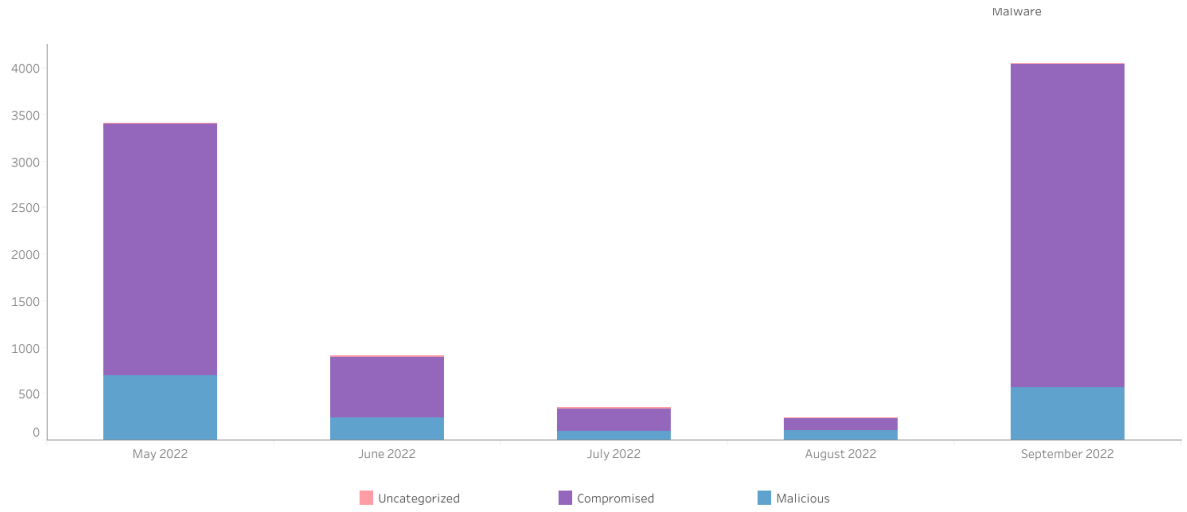


*Figure 10: Compromised vs Malicious - **Malware***

Commentary

In line with our methodology, we have updated our approach to compromised and malicious registrations to improve its accuracy. We have applied this retrospectively to the existing months of data. The result was that our methodology identified more malicious registrations for May to August. More detailed information is available in the interactive charts on our **website**.

DNSAI COMPASS

DNS ABUSE INSTITUTE

www.dnsabuseinstitute.org