COMAR: Classification of Compromised versus Maliciously Registered Domains

Sourena Maroofi, Maciej Korczyński, Cristian Hesselman, Benoît Ampeau, Andrzej Duda, Thymen Wabeke

Univ. Grenoble Alpes, SIDN Labs, AFNIC

maciej.korczynski@univ-grenoble-alpes.fr

26 May 2021
ICANN DNS Symposium
Plan

1. Motivation
2. Overview of COMAR
3. Results
4. Conclusions
Overview: DNS reputation systems

DNS reputation systems can detect malicious domains using different techniques and at different phases:

- at the registration time (e.g., PREDATOR\textsuperscript{1})
- domain activity phase (e.g., EXPOSURE\textsuperscript{2})


DNS reputation systems can detect malicious domains using different techniques and at different phases:

- at the registration time (e.g., PREDATOR)\(^1\)
- domain activity phase (e.g., EXPOSURE)\(^2\)

They classify domains as either malicious or benign.

---


Overview: DNS reputation systems

DNS reputation systems can detect malicious domains using different techniques and at different phases:

- at the registration time (e.g., PREDATOR\textsuperscript{1})
- domain activity phase (e.g., EXPOSURE\textsuperscript{2})

- They classify domains as either malicious or benign.
- They do not consider compromised domains.

Why we need to consider compromised domains (hacked websites)?

Compromised domains have also legitimate traffic we may not want to block.

1. The mitigation action for compromised domains (websites) is different from malicious domains

   • Should we block/hold/take down the domain?
   • Should we notify the hosting provider?
Motivation

https://user-paypal.oz4.top/LkQwxCf2/rfFDbZaPR9Ti/ioiuYnPGh/ANWfgiB2vk8b/1

---

Email

Password

Log In

Forgot your email or password?

Sign Up

---

Privacy  Legal

Copyright © 1999-2021 PayPal. All rights reserved.

Consumer advisory: PayPal Pte. Ltd., the holder of PayPal’s stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully.
What can be done to mitigate this abuse?
Motivation

https://user-paypal.oz4.top/LkQwxCf2/rfFDzB9lPR9Ti/loij
YnPgh/ANWfgiB2vk8b/1

http://oz4.top

Forbidden
You don't have permission to access / on this server.

Submission Date: 2021-01-15 18:00:05

WHOIS:
Updated Date: 2021-01-13T15:32:36Z
Creation Date: 2021-01-13T15:26:54Z
Motivation

Technical abuse (maliciously registered domain name) and website content abuse (illegal/abusive content)

https://user-paypal.oz4.top/LkQwxCf2/rfFDbZaPR9Ti/loiujYnPgh/ANWfgiB2vk8b/1

http://oz4.top

Forbidden
You don't have permission to access / on this server.

Submission Date: 2021-01-15 18:00:05

WHOIS:
Updated Date: 2021-01-13T15:32:36Z
Creation Date: 2021-01-13T15:26:54Z
Technical abuse (maliciously registered domain name) and website content abuse (illegal/abusive content)

Action: Block/hold/take down domain name ...and clean the hosting content
Motivation

**Technical abuse** (maliciously registered domain name) and **website content abuse** (illegal/abusive content)

Action: Block/hold/take down domain name ... and clean the hosting content

Intermediary: DNS service operator (registrar, registry) and hosting provider
Motivation

https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html
Motivation

https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html

What can be done to mitigate this abuse?
https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html

WHOIS:
Creation Date: 2014-03-04T00:00:00Z
Registrar Registration Expiration Date: 2022-03-04T00:00:00Z
Website content abuse (illegal/abusive content), benign domain but compromised website...

https://nutribiocorp.com/wp-includes/paypal/paypal/login/update.account-PayPal/account-has-been-limited/logins.html

Motivation

https://nutribiocorp.com

WHOIS:
Creation Date: 2014-03-04T00:00:00Z
Registrar Registration Expiration Date: 2022-03-04T00:00:00Z
Website content abuse (illegal/abusive content), benign domain but compromised website...

Action: Block/hold/take down domain name and clean the hosting content
Website content abuse (illegal/abusive content), benign domain but compromised website...

Action: Block/hold/take-down domain name and clean the hosting content
Website content abuse (illegal/abusive content), benign domain but compromised website...

Action: Block/hold/take down domain name and clean the hosting content
Intermediary: DNS service operator and hosting provider
Website content abuse (illegal/abusive content), benign domain but compromised website...

Action: Block/hold/take down domain name and clean the hosting content
Intermediary: DNS service operator and hosting provider ...and the website owner/administrator
Website structure of compromised vs. malicious domains

- **Compromised domain**
- **Malicious domain**

Legend:
- Red: Non-HTML content
- Green: External hyperlink
- Black: Homepage
- Blue: Malicious page
- White: HTML page or directory
Motivation

Why we need to consider *compromised* domains?

Compromised domains have also legitimate traffic we may not want to block.

1. The mitigation action for compromised domains is different from malicious domains
   - Should we block/hold/take down the domain?
   - Should we notify the hosting provider?
Motivation

Why we need to consider **compromised** domains?

Compromised domains have also legitimate traffic we may not want to block.

1. The mitigation action for compromised domains is different from malicious domains
   - Should we block/hold/take down the domain?
   - Should we notify the hosting provider?

2. Creating more effective domain blacklist feed → better insights into attackers' behavior
   - Do current URL blacklists give us the correct insights?
“Eighty percent of phishing sites have SSL encryption enabled to fool victims.” [1]

“(…) 8.6 percent were OV (Organization Validation) certs, and just 0.1% were Extended Validation (EV)” [1]

“Eighty percent of phishing sites have SSL encryption enabled to fool victims.” [1]

“(...) 8.6 percent were OV (Organization Validation) certs, and just 0.1% were Extended Validation (EV)” [1]

How to interpret the results?

“Eighty percent of phishing sites have SSL encryption enabled to fool victims.” [1]

“(…) 8.6 percent were OV (Organization Validation) certs, and just 0.1% were Extended Validation (EV)” [1]

How to interpret the results?

Distinguishing between compromised and malicious domains can give better insights into attackers' behavior

Contributions

• We developed COMAR, a machine-learning system to classify domains exhibiting malicious behavior as either *compromised* or *maliciously registered* by only using *publicly available* and *readily accessible resources* and achieve 97% accuracy with 2.5% of false positives.

• We leverage 38 features to identify the state of a domain, 14 of which are new and have not been used in previous work.

• We introduce a new method to estimate the domain creation time in cases there is no access to WHOIS information, which outperforms standard statistical methods in filling missing values.

• We show that content-based features are the most important ones in representing the domain status.
Passive information (e.g., lexical patterns of URLs)
Active measurements (e.g., hosting and DNS infrastructure)

COMAR reports:
comp(URL1): 95%
malreg(URL2): 98%
explanation

existing legitimate Site S1
Newly created malicious Site S2

URL1
Automated measurements: spam traps, honeypots, user reports, ...

URL2

URL Blacklist Providers

COMAR Classifier

Registry Dashboard
Registrar
Hosting Provider
Web Master site S1

28
COMAR System Overview

Subdomain
Dynamic DNS
IP Addresses

Blacklist Resources

Malicious URLs

Data collector

Core

WHOIS

screenshots

Host info

Content

Technology

Sitemap

Passive DNS

Content-based

Lexical feature

Popularity feature

Host-based features

Certificate feature

Feature Extractor

LEARNING MODULE

CLASSIFIER
Feature categories

In total we implemented 38 features (14 of them new) in 7 categories:

1. Lexical features
2. Ranking system and popularity features
   • Internet archive, Alexa, Majestic, Umbrella, ...
3. Passive DNS features (DNSDB)
4. Content-based features
   • Internal and external hyperlinks
   • Content length
   • Vulnerable technologies and number of technologies
   • Existence of home page (Is it default or not?)
   • Using redirection techniques
   • ...
5. WHOIS and TLD-based features
   • Spamhaus index
   • Domain age
   • ...
6. TLS certificate features
7. Active DNS features

To make COMAR practical, system uses only publicly available and readily accessible resources, we removed “passive DNS”.
What if we can not collect data for some features?

In practice, there are always missing values when it comes to collecting features. If we can not collect data, we can not classify domains or even worse: misclassification.

We need to fill the missing values appropriately. For example:

- **WHOIS feature:** Some TLDs do not provide registration date (e.g., .de, .tk, .ml, ...)
- **Content features:** We can not fetch the content for any reason (bot detection or host suspension)
Dataset & Machine Learning

Dataset → manually labeled 2,329 domains as maliciously registered, compromised, subdomain/free service, or false positives

1. Number of phishing domain labeled manually: 1,321 (OpenPhish, PhishTank, Anti-Phishing Working Group)
   - 58% maliciously registered - 42% compromised

2. Number of malware domains from URLhaus labeled manually: 1,008
   - 43% maliciously registered - 57% compromised
Machine learning

1. Logistic regression
   • Parametric method known for its efficiency
   • Low computational resources
   • Interpretability

2. Random forest
   • Non-parametric
   • training a non-linear model
   • No feature transformation
Results

Overall results for both classifiers and comparison with method used in Global Phishing Surveys.

Domain is malicious if:
- it is reported “very short time after registration”, or
- contains a brand name or misleading string, or
- registered in batch (challenging after GDPR)

<table>
<thead>
<tr>
<th>Method</th>
<th>DB</th>
<th>Acc</th>
<th>Precision</th>
<th>Recall</th>
<th>F1</th>
<th>MCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF</td>
<td>Phish</td>
<td>97%</td>
<td>95%</td>
<td>97%</td>
<td>96%</td>
<td>0.93</td>
</tr>
<tr>
<td>LR</td>
<td>Phish</td>
<td>96.5%</td>
<td>96.59%</td>
<td>95%</td>
<td>95.7%</td>
<td>0.92</td>
</tr>
<tr>
<td>APWG</td>
<td>Phish</td>
<td>85%</td>
<td>82%</td>
<td>93%</td>
<td>88%</td>
<td>0.69</td>
</tr>
<tr>
<td>RF</td>
<td>Mal</td>
<td>96%</td>
<td>97%</td>
<td>96%</td>
<td>97%</td>
<td>0.92</td>
</tr>
<tr>
<td>LR</td>
<td>Mal</td>
<td>94.5%</td>
<td>95.6%</td>
<td>95.2%</td>
<td>95.4%</td>
<td>0.89</td>
</tr>
</tbody>
</table>

False positive rate:   COMAR → 2.5%  APWG → 26%

False positive: maliciously registered domains classified as compromised
Results

Risk of false negatives

False negative: classifying compromised domains as maliciously registered

Partial cumulative distribution of the compromised domains after registration
Results

Applying logistic regression on the phishing and malware dataset by removing one feature-set at a time.

Phishing dataset

Malware dataset
Results

Distribution of the ‘internal hyperlinks’ (logarithmic scales) and ‘TLD maliciousness index’

Internal hyperlinks

TLD maliciousness index

1https://www.spamhaus.org/statistics/tlds
New anti-phishing evasion technique

http://circlecityflyers.com

http://circlecityflyers.com/lokako/newicn/cust0mers...
New anti-phishing evasion technique

http://circlecityflyers.com

http://circlecityflyers.com/lokako/newicn/custom0mers...
New anti-phishing evasion technique: Google CAPTCHA to hide the real content of the malicious page
COMAR leverages publicly available data and makes classification decisions based on the extracted features.

Registries, registrars, and hosting providers can use it to decide on appropriate mitigation actions for each domain with malicious content.

It can also serve as an effective tool for creating domain blacklists from the existing URL ones.

We showed that the content-based features are the most effective in capturing the ‘amount of beingness’ of domains during their life cycles.

Relatively hard to evade features.
"COMAR: Classification of Compromised versus Maliciously Registered Domains", Sourena Maroofi, Maciej Korczynski, Cristian Hesselman, Benoit Ampeau and Andrzej Duda, IEEE European Symposium on Security and Privacy (EuroS&P 2020), September 2020 (Acceptance rate: 14,6%)

"Are You Human? Resilience of Phishing Detection to Evasion Techniques Based on Human Verification", Sourena Maroofi, Maciej Korczynski, and Andrzej Duda, ACM IMC 2020, Pittsburgh, PA, USA, October 2020 (Acceptance rate: 24,5%)

https://comar-project.univ-grenoble-alpes.fr/
Acknowledgments

This work has been carried out in the framework of the COMAR project funded by SIDN, the .NL Registry and AFNIC, the .FR Registry.

We thank: Anti-Phishing Working Group, OpenPhish, PhishTank, URLhaus for providing access to their URL blacklists;

Farsight Security for sharing DNSDB, and the DNSDB data contributors

This work was partially supported by the ANR projects: the Grenoble Alpes Cybersecurity Institute CYBER@ALPS under contract ANR-15-IDEX-02, PERSYVAL-Lab under contract ANR-11-LABX-0025-01, and DiNS under contract ANR-19-CE25-0009-01.
Thank you for your attention!

Contact:
maciej.korczynski@univ-grenoble-alpes.fr