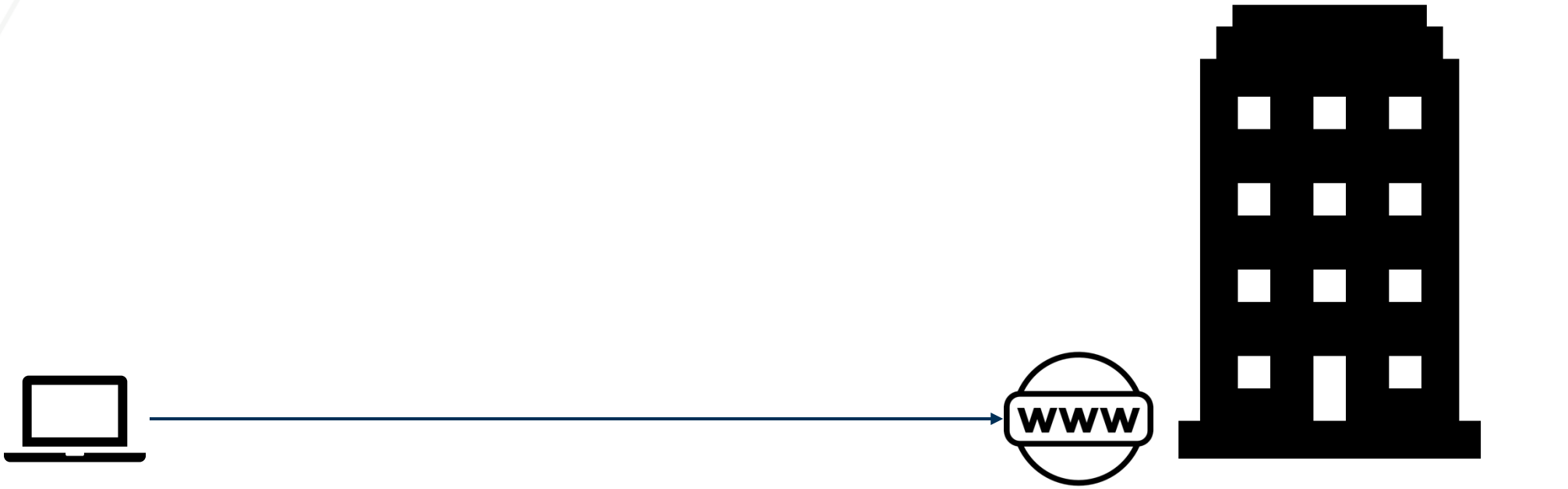
The Guardians of Name Street: Studying the Defensive Registration Practices of the Fortune 500

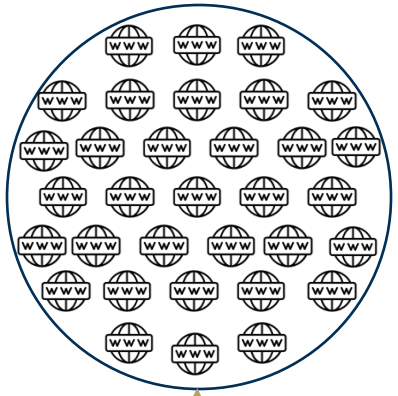
Boladji Vinny Adjibi, Athanasios Avgetidis, Manos Antonakakis, Michael Bailey and Fabian Monrose

Georgia Tech



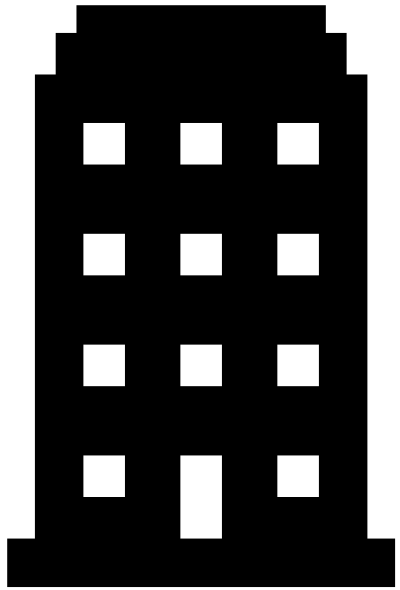
End User

Company and their domain name



Domain names similar to the company’s domain name

End User



Company and their domain name

Georgia Tech

The space of “similar” domain names

The space of “similar” domain names

Typo-squatting (Wang et al., 2006)

The space of “similar” domain names

Typo-squatting (Wang et al., 2006)

Bit-squatting (Nikiforakis et al., 2013)

The space of “similar” domain names

Typo-squatting (Wang et al., 2006)

Bit-squatting (Nikiforakis et al., 2013)

Sound-squatting (Nikiforakis et al., 2014)

TLD-squatting (Halvorson et al., 2015)

Combo-squatting (Kintis et al., 2017)

Abbreviation squatting (Lv et al., 2018)

Homograph squatting (Quinkert et al., 2019)

Level-squatting (Du et al., 2019)

Target embedding (Roberts et al., 2019)

Brand name squatting (Kumar et al., 2021)

The space of “similar” domain names

Typo-squatting (Wang et al., 2006)

Bit-squatting (Nikiforakis et al., 2013)

Sound-squatting (Nikiforakis et al., 2014)

TLD-squatting (Halvorson et al., 2015)

Combo-squatting (Kintis et al., 2017)

Abbreviation squatting (Lv et al., 2018)

Homograph squatting (Quinkert et al., 2019)

Level-squatting (Du et al., 2019)

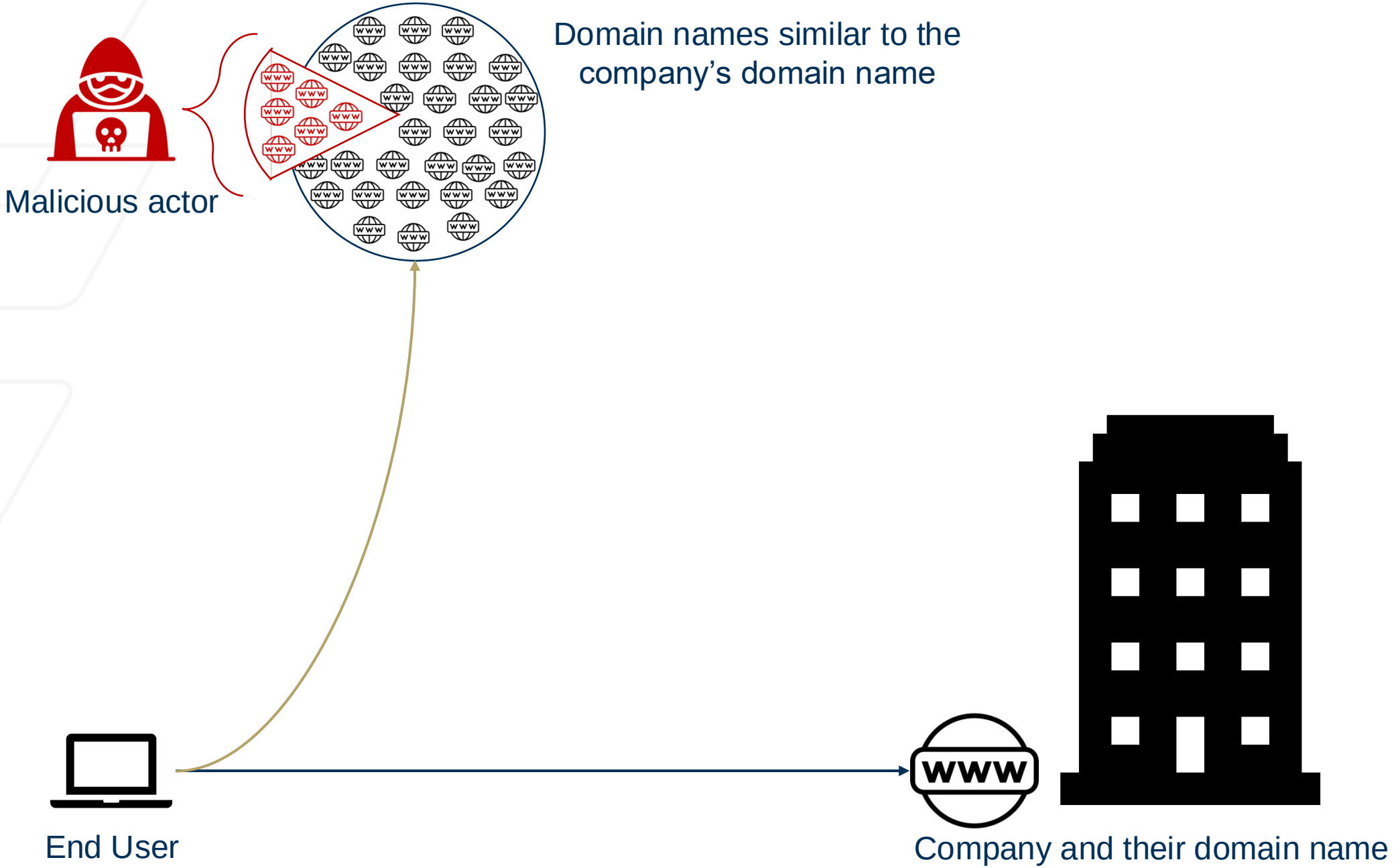
Target embedding (Roberts et al., 2019)

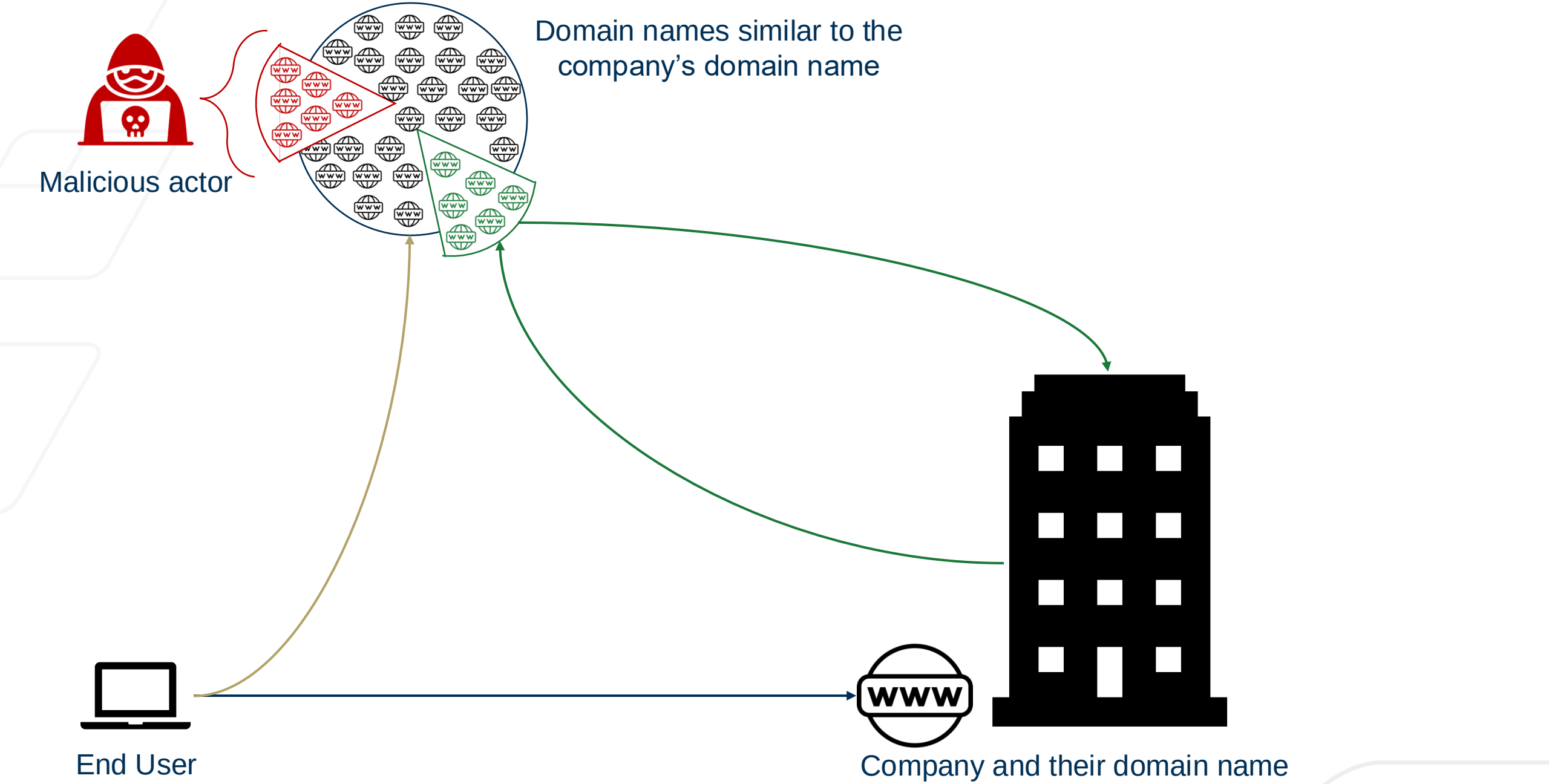
Brand name squatting (Kumar et al., 2021)

×

1,500+
Top-Level Domains

Georgia Tech


Domain names similar to the company's domain name
Malicious actor
End User
Company and their domain name


Domain names similar to the company's domain name
Malicious actor
End User
Company and their domain name

Base domains

Operations

Domain names

Fortune 500’s

Corporate domains

Capital One Financial Corp | capitalone.com | COF

Fortune 500's
Corporate domains

Abbreviation squatting
conef.com

Bit-squatting
capitanone.com

Brand name squatting
capitalonefinancialcorp.com

Homograph squatting
capital0ne.com

Sound-squatting
capitalwon.com

Stock name squatting NEW
cof.com

TLD-squatting
capitalone.net

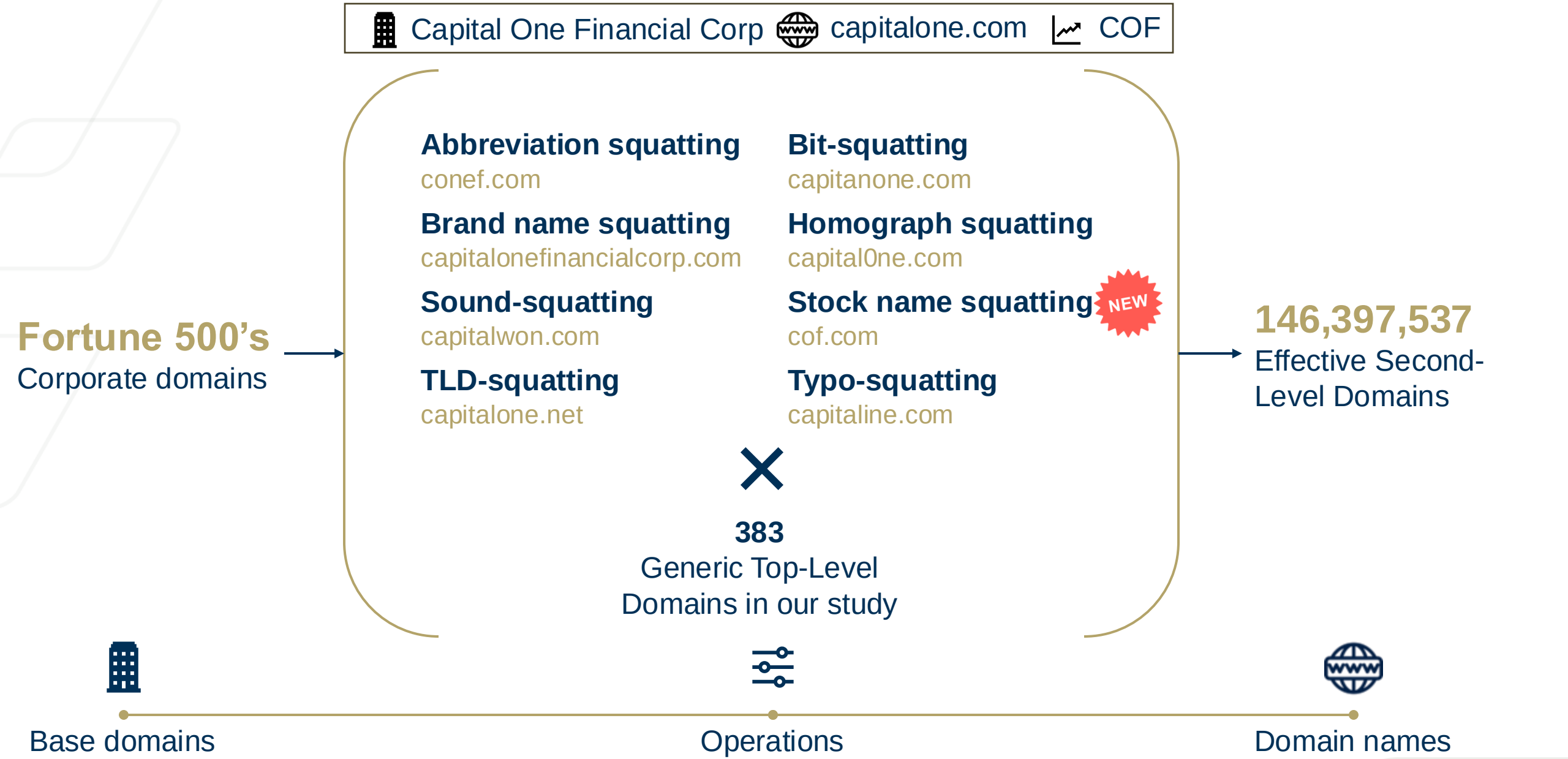
Typo-squatting
capitaline.com

×

383
Generic Top-Level
Domains in our study

Base domains — Operations — Domain names

Georgia Tech



Georgia Tech

Identifying defensive registrations

Georgia Tech

Identifying defensive registrations

CHALLENGES

- Prevalence of external name servers
- Redacted WHOIS records
- Mergers and name changes

SOLUTIONS

- Careful check to find name servers operated exclusively internally
- Conservative matching of Registrant Org. in WHOIS records
- Finding alternative names using SEC and Wikipedia data

CZDS

U.S. Securities and Exchange Commission

WHOIS Records

Georgia Tech

What is a defensive registration?

Georgia Tech

What is a defensive registration?

1

Authoritative name servers CZDS

All the name servers are **subdomains** of the base domain name.

Georgia Tech

What is a defensive registration?

1

Authoritative name servers CZDS

All the name servers are **subdomains** of the base domain name.

2

Alternative name servers CZDS

All the name servers are subdomains of domain names **owned by subsidiaries**.

Georgia Tech

What is a defensive registration?

1

Authoritative name servers CZDS

All the name servers are **subdomains** of the base domain name.

2

Alternative name servers CZDS

All the name servers are subdomains of domain names **owned by subsidiaries**.

3

Registrant information

The **registrant organization** in the WHOIS record refers to a subsidiary.

Georgia Tech

What is a defensive registration?

1

Authoritative name servers CZDS

All the name servers are **subdomains** of the base domain name.

2

Alternative name servers CZDS

All the name servers are subdomains of domain names **owned by subsidiaries**.

3

Registrant information

The **registrant organization** in the WHOIS record refers to a subsidiary.

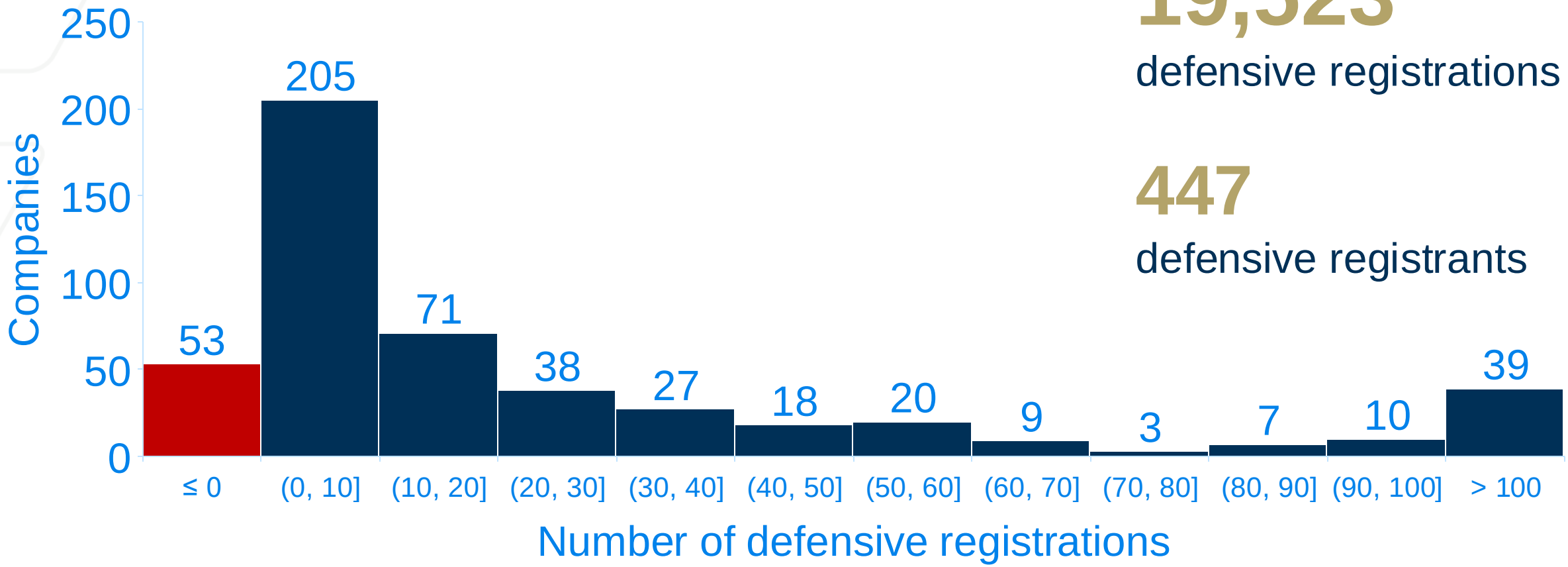
4

Contact details

The **WHOIS email address'** domain name is owned by subsidiaries.

Georgia Tech

Defensive registrations

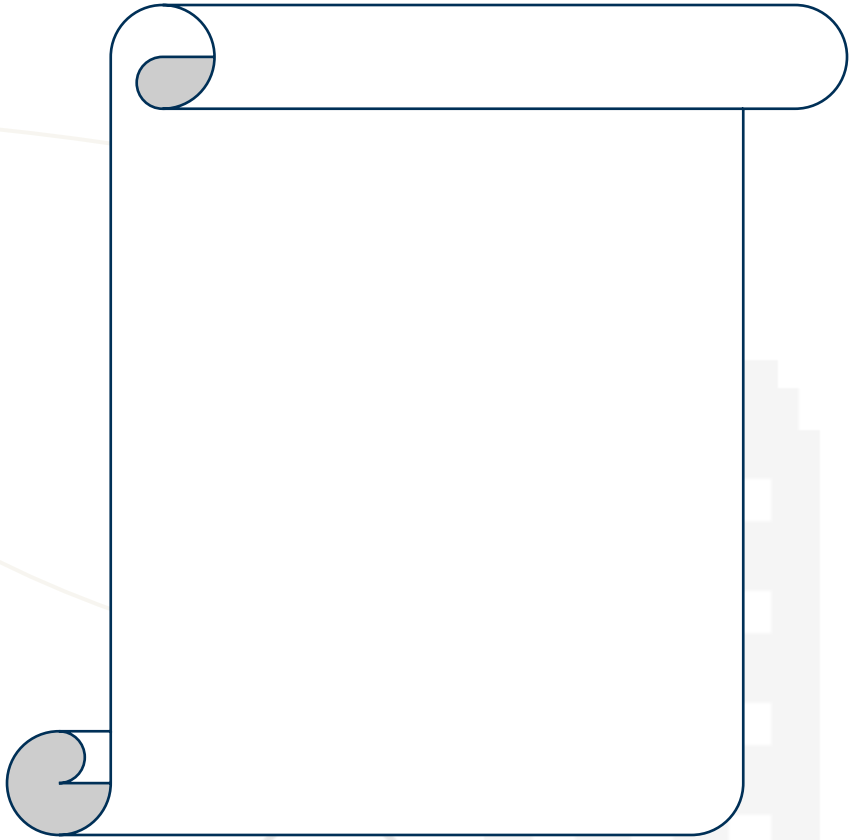


19,523
defensive registrations

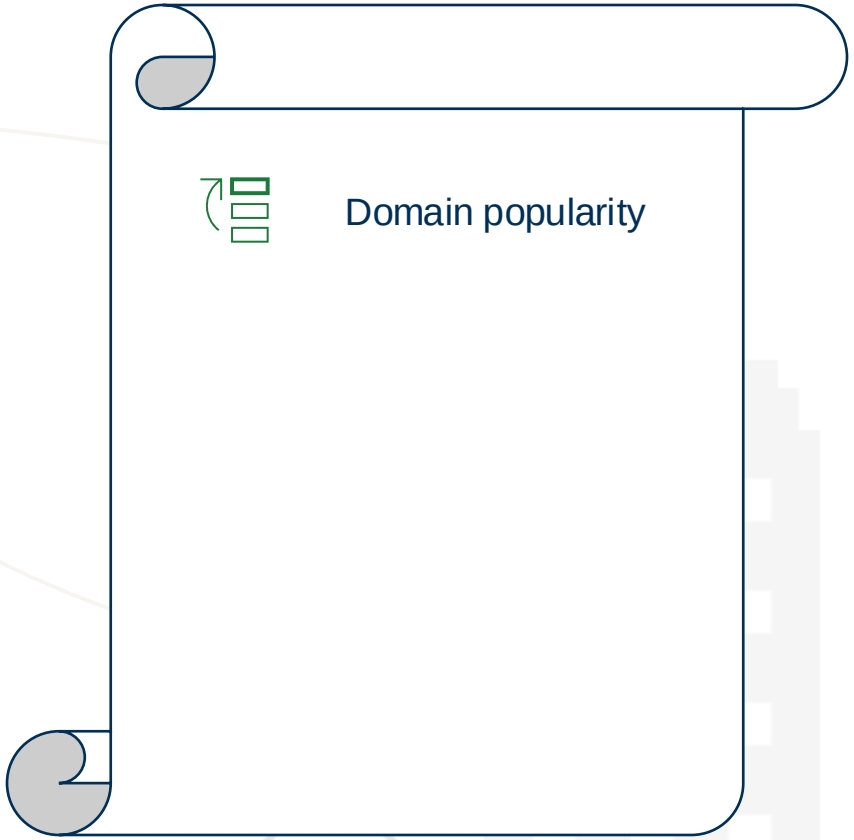
447
defensive registrants

Georgia Tech

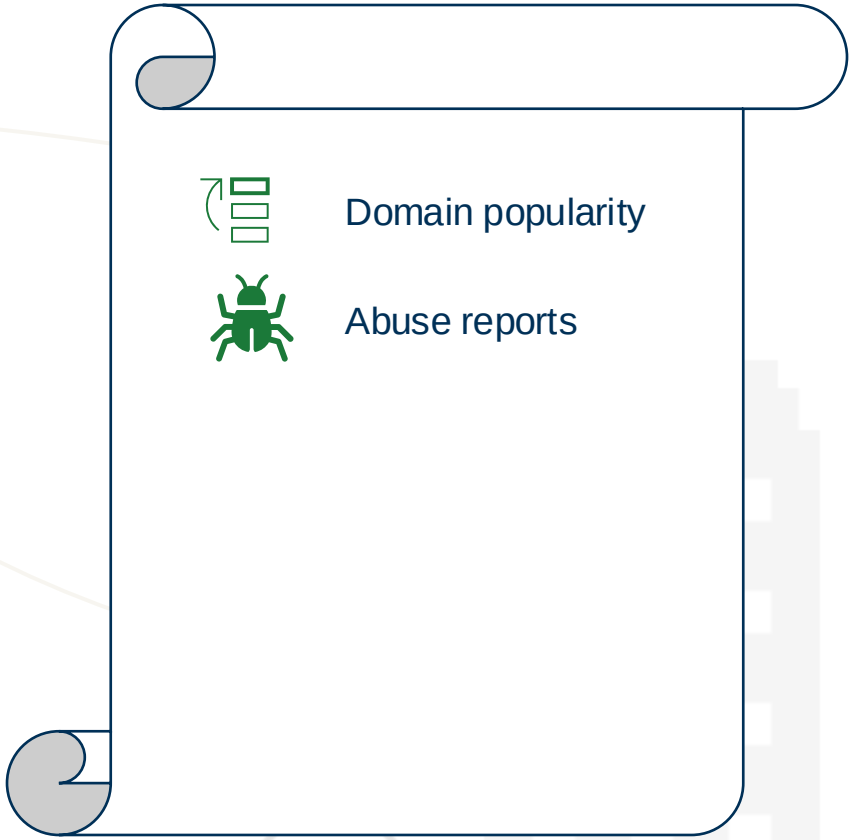
Correlations with number of defensive registrations



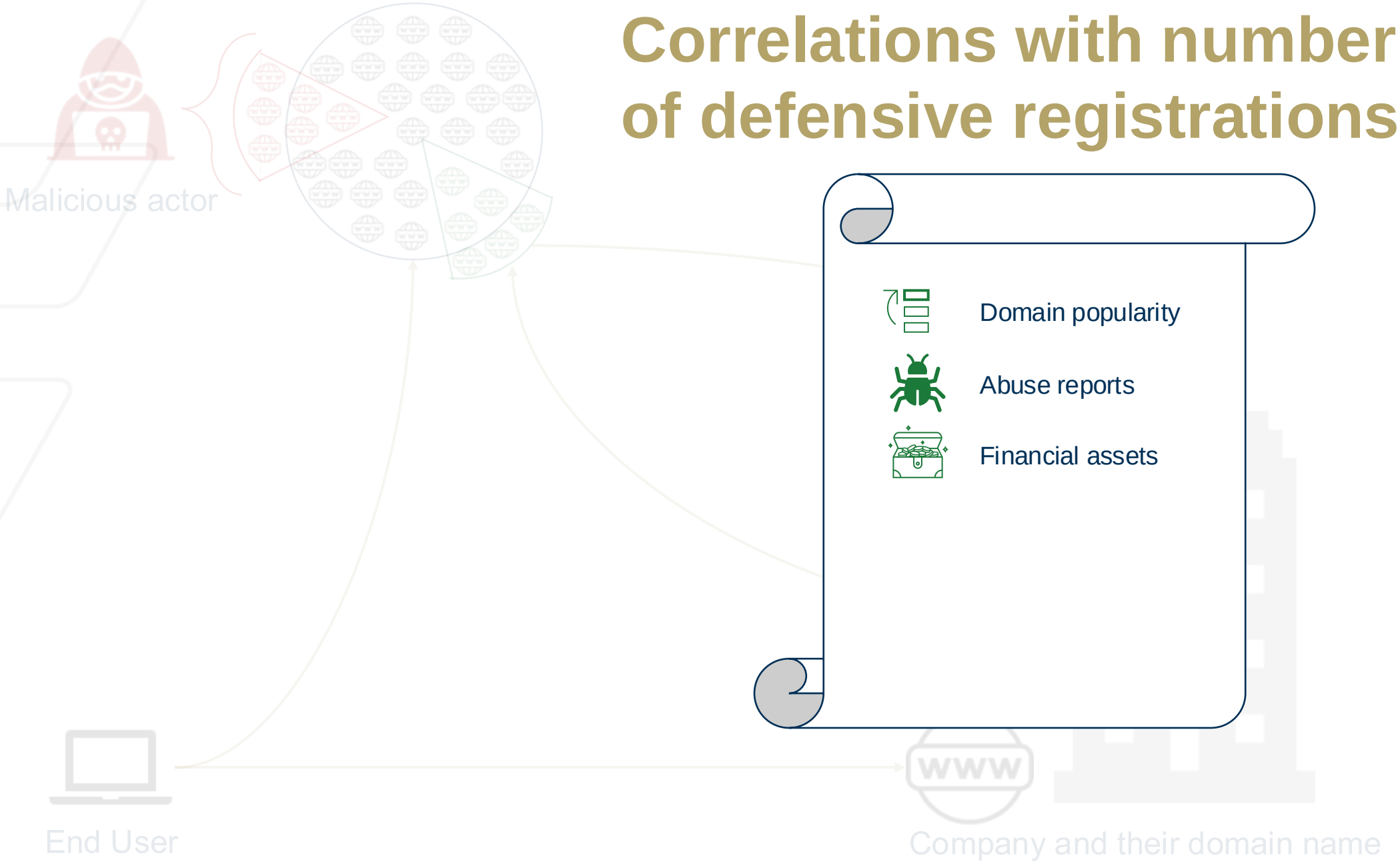
Correlations with number of defensive registrations



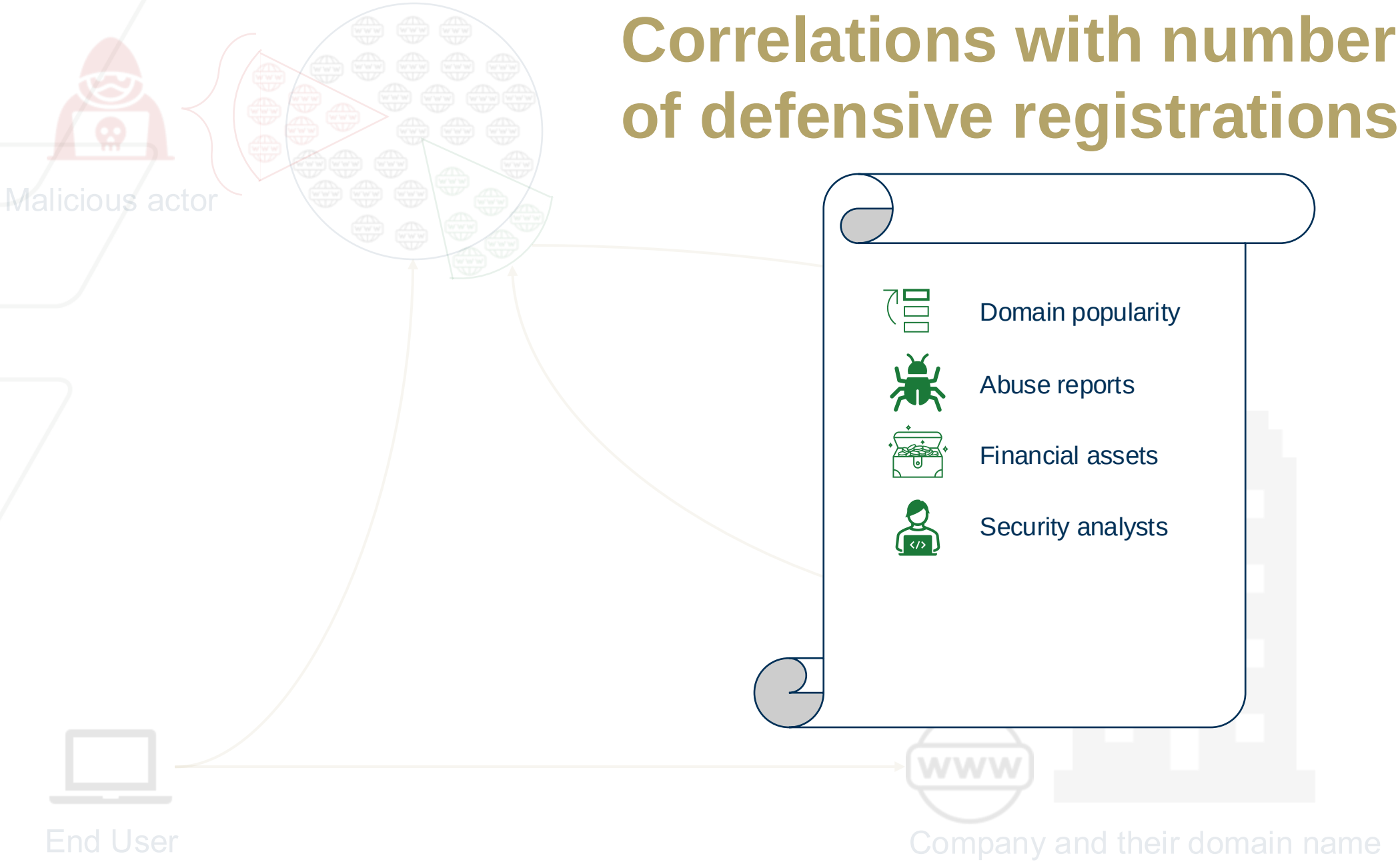
Correlations with number of defensive registrations



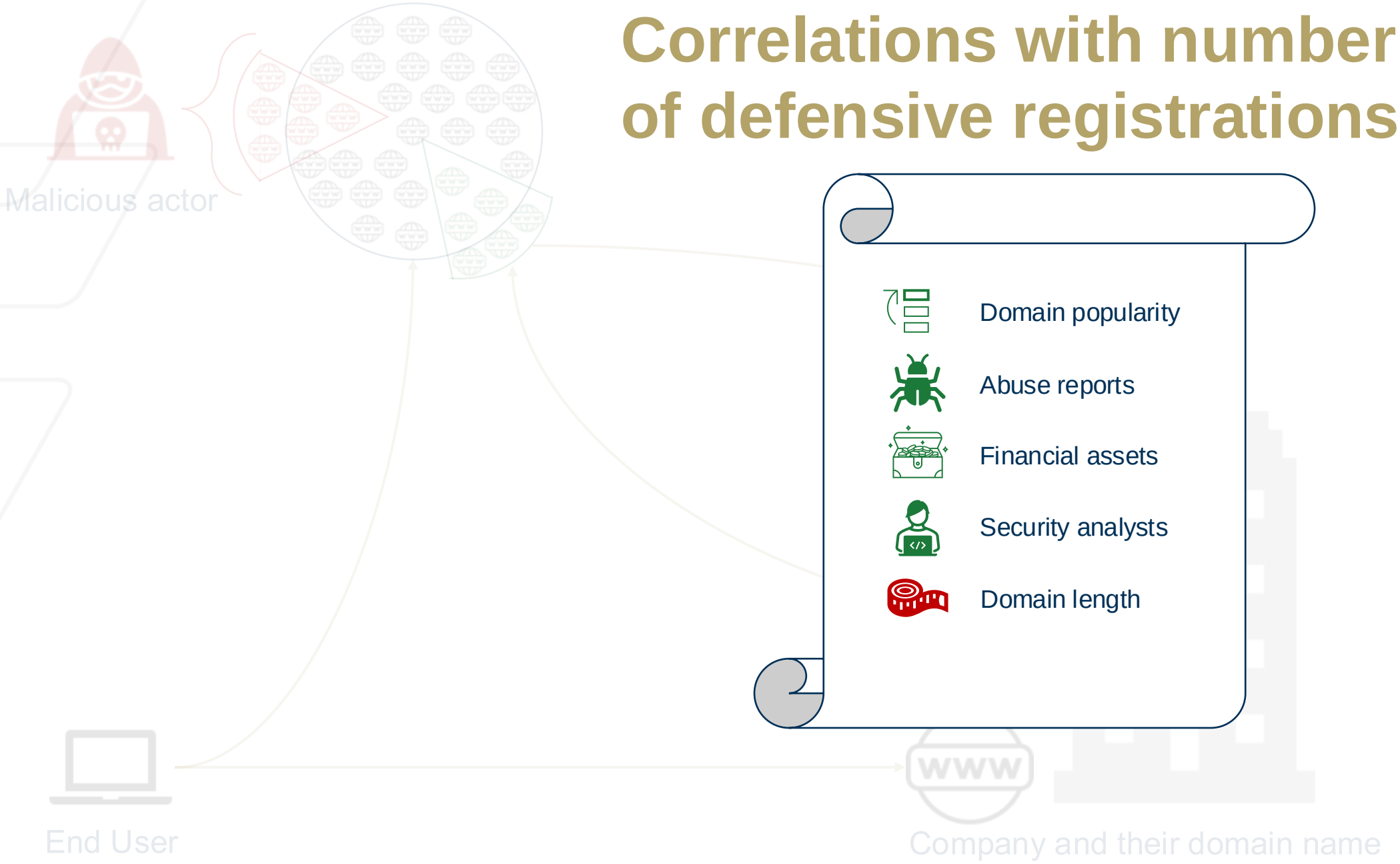
Correlations with number of defensive registrations



Correlations with number of defensive registrations

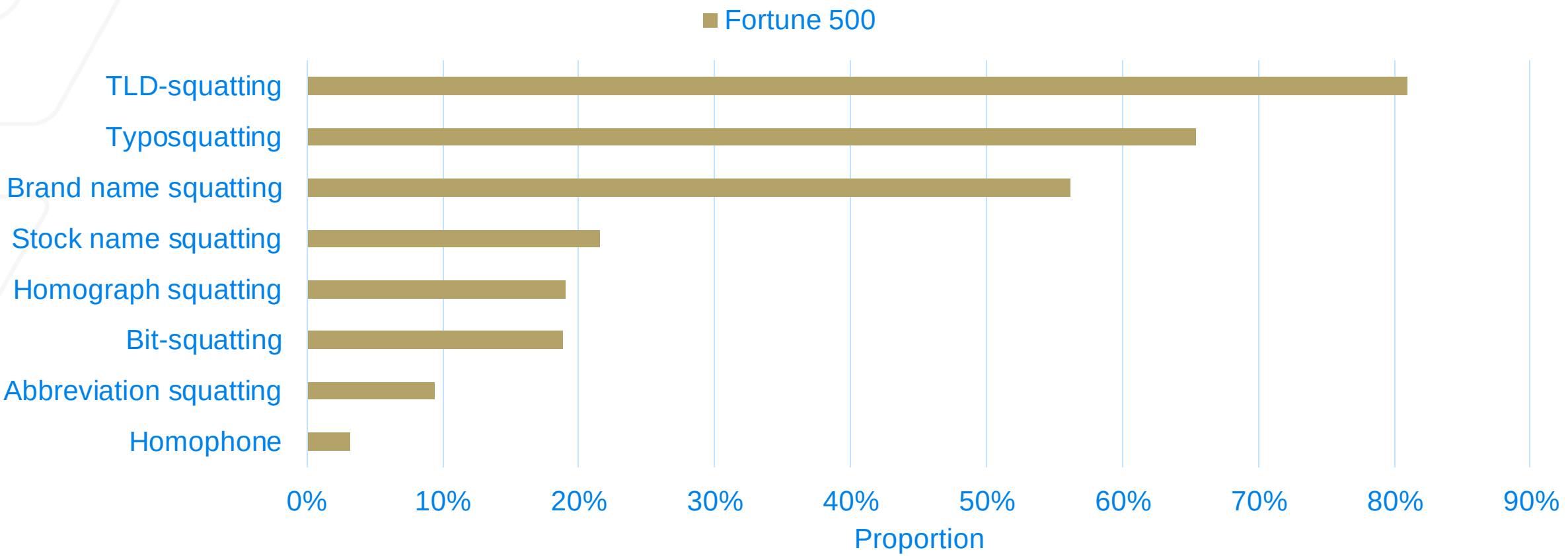


Correlations with number of defensive registrations



Georgia Tech

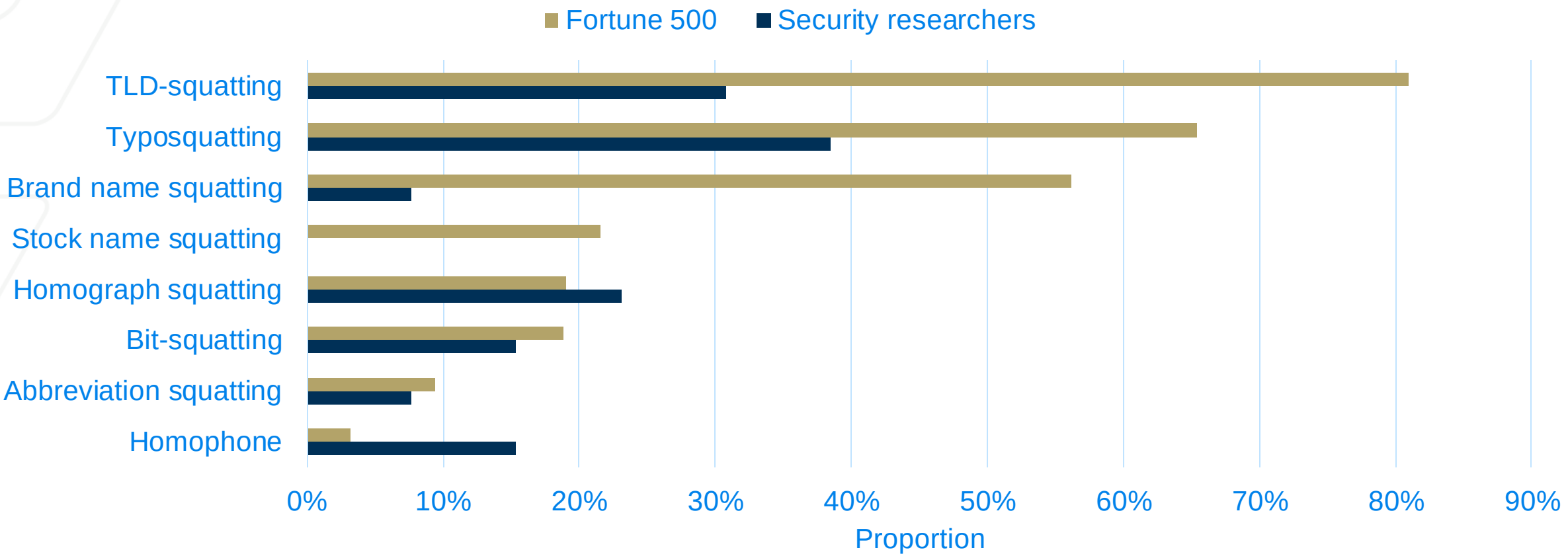
Portfolio of defensive registrations



Proportion of companies registering domains from the transformation.

Georgia Tech

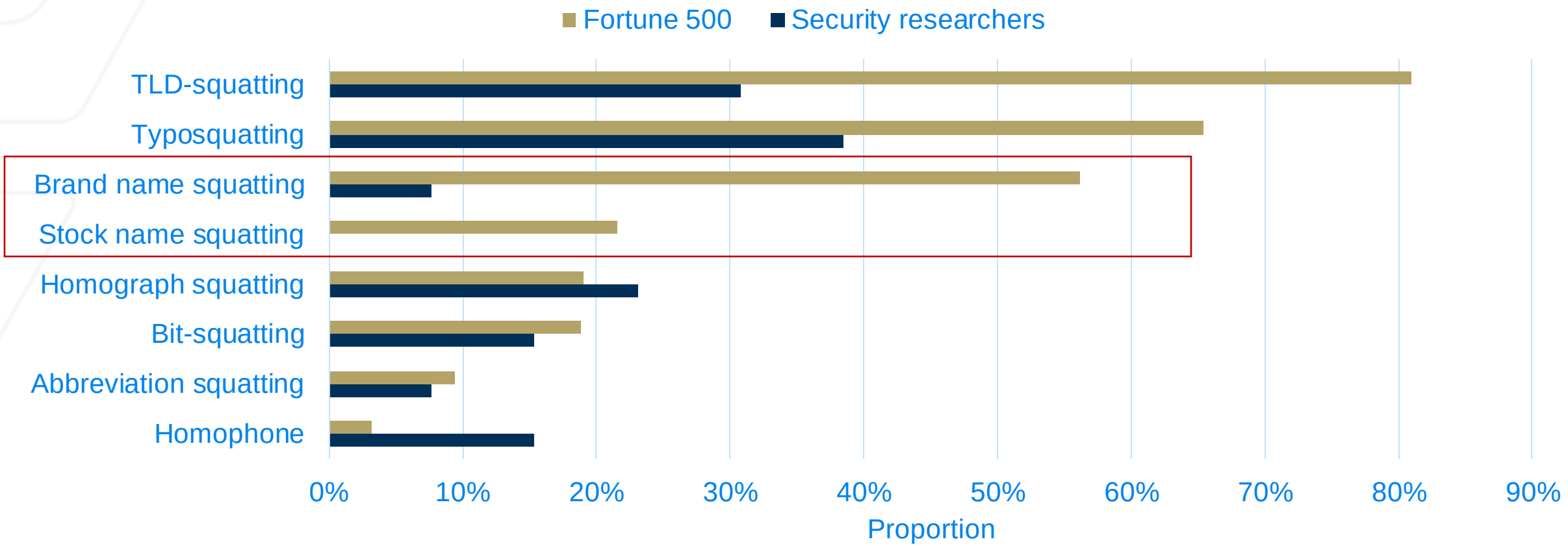
Portfolio of defensive registrations



- Proportion of companies registering domains from the transformation.
- Proportion of peer-reviewed security papers discussing defensive registrations of the transformation

Georgia Tech

Portfolio of defensive registrations

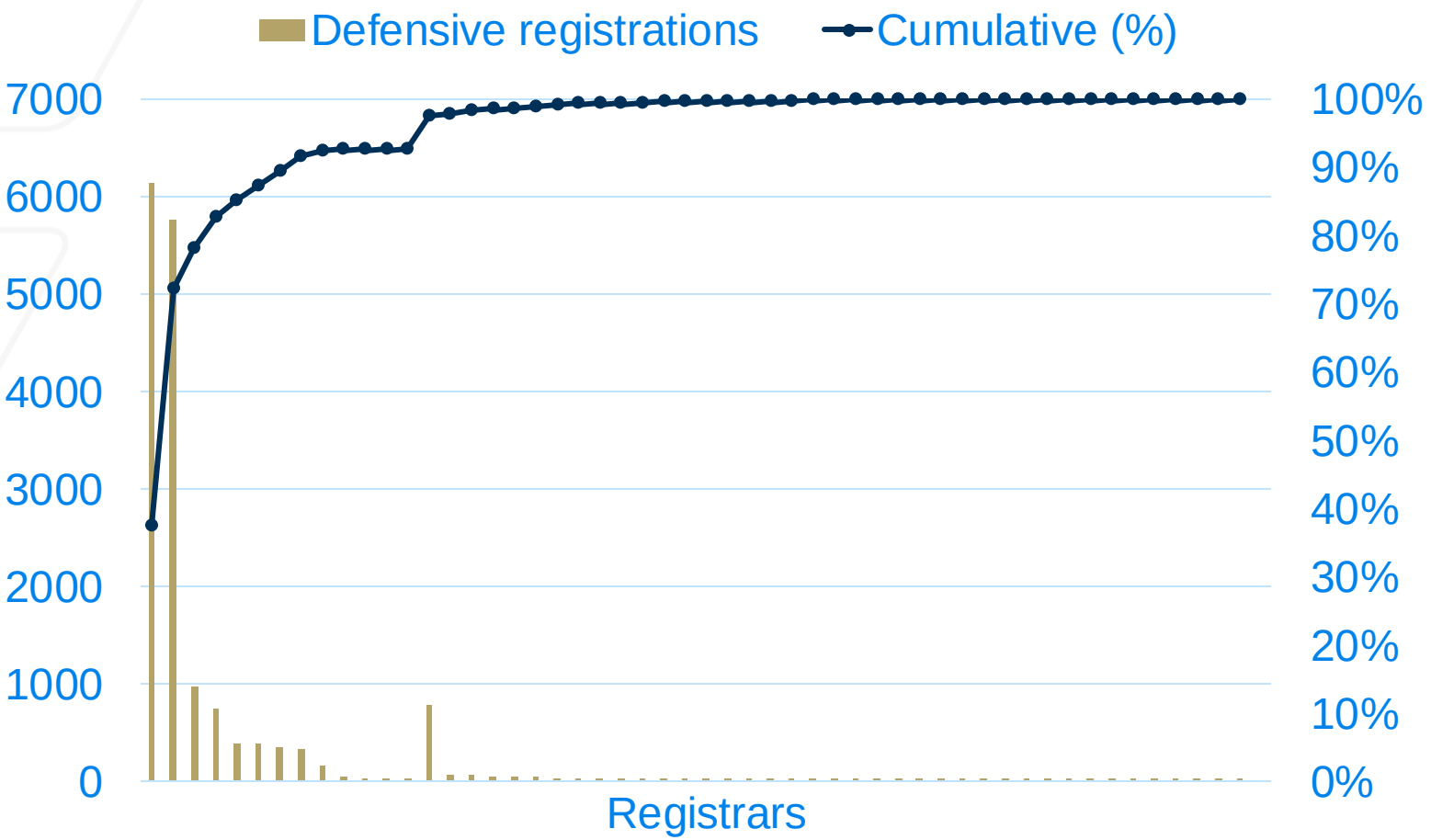


Proportion of companies registering domains from the transformation.

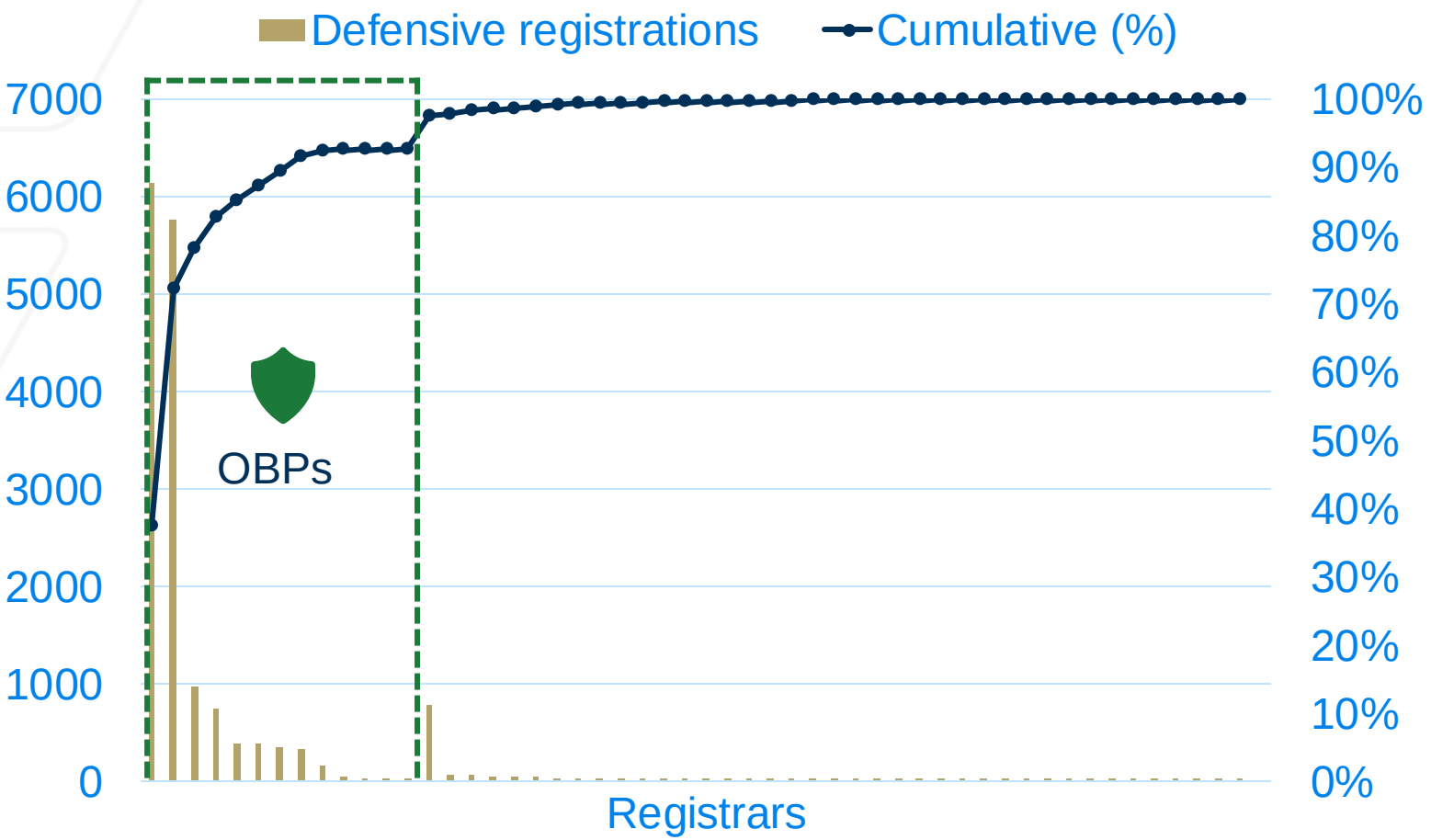
Proportion of peer-reviewed security papers discussing defensive registrations of the transformation

Georgia Tech

Registrars for defensive registrations



Registrars for defensive registrations

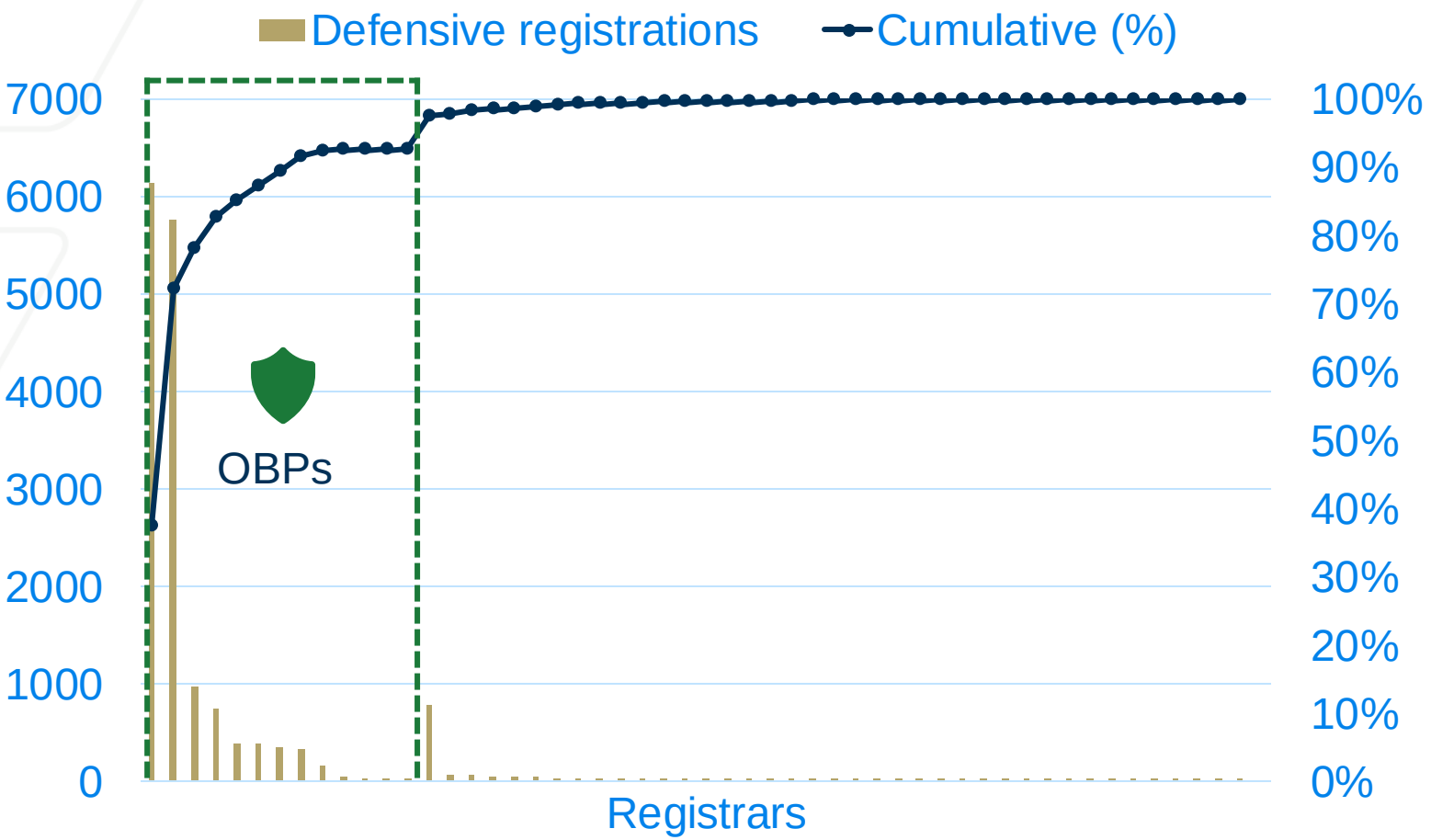


97%

of defensive registrations made by **Online Brand Protection Service Providers**

Georgia Tech

Registrars for defensive registrations



97%

of defensive registrations made by **Online Brand Protection Service Providers**

How **effective** are their strategies?

Georgia Tech

Effectiveness of OBPs' defensive registrations

Large U.S. ISP
109,180,596 records
Oct. 2020 – Dec. 2023

Effectiveness of OBPs' defensive registrations

Large U.S. ISP
109,180,596 records
Oct. 2020 – Dec. 2023

Protection of current customers

What proportion of traffic goes to the OBPs' chosen domain names vs. available domains?

Georgia Tech

Effectiveness of OBPs' defensive registrations

Large U.S. ISP
109,180,596 records
Oct. 2020 – Dec. 2023

Protection of current customers

What proportion of traffic goes to the OBPs' chosen domain names vs. available domains?

Protection of prospective customers

How likely is the OBP to register the most valuable domain names for a new customer?

Georgia Tech

Effectiveness of OBPs' defensive registrations

Large U.S. ISP
109,180,596 records
Oct. 2020 – Dec. 2023

Protection of current customers

What proportion of traffic goes to the OBPs' chosen domain names vs. available domains?

Protection of prospective customers

How likely is the OBP to register the most valuable domain names for a new customer?

Georgia Tech

Predicted performance for prospective customers

Generate transformations for the 53 companies without defensive registrations.

Predicted performance for prospective customers

Generate transformations for the 53 companies without defensive registrations.

Identify domain names that were historically available for registration

Affinito et al. *Domain name lifetimes: Baseline and threats,* Traffic Monitoring and Analysis, 2022

Georgia Tech

Predicted performance for prospective customers

Generate
transformations for the 53 companies without defensive registrations.

Identify
domain names that were historically available for registration

Predict
each OBP's ranking of the domain names by learning from their observed selections

Georgia Tech

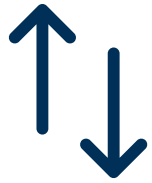
Reverse engineering of OBPs' strategies

Online Brand Protection Service Provider	Performance with top 5% guesses
MarkMonitor Inc.	98.12%
CSC Corporate Domains, Inc.	97.79%
SafeNames Ltd.	96.14%
Nom-iq Ltd. dba COM LAUDE	94.58%
GoDaddy Corporate Domains, Inc.	88.37%
Network Solutions LLC	80.96%

Predicted performance for prospective customers

Generate
transformations for the 53 companies without defensive registrations.

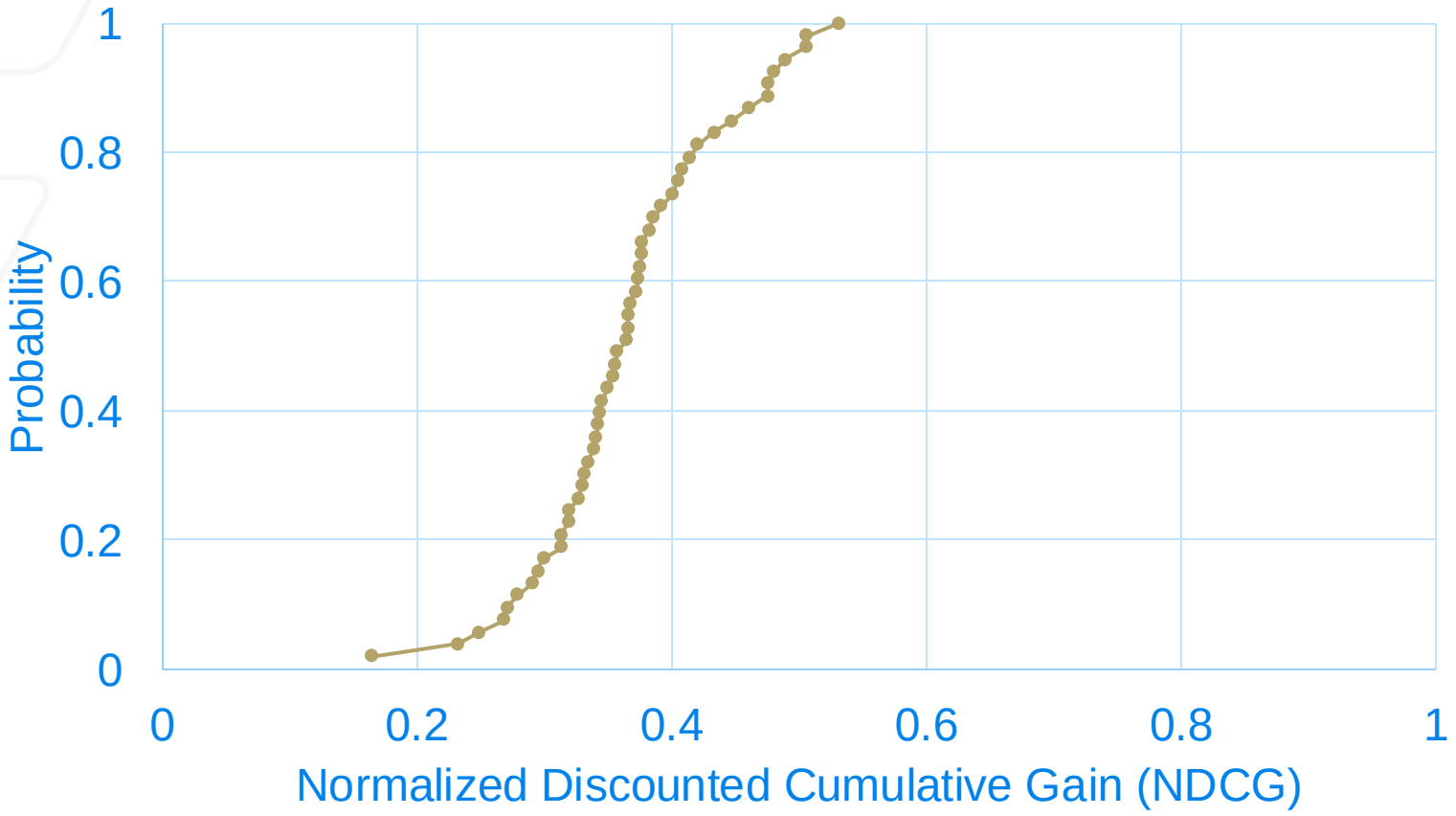
Identify
domain names that were historically available for registration



Predict
each OBP's ranking of the domain names by learning from their observed selections

Assess
the alignment between predicted rankings and real-world traffic data

Predicted performance for prospective customers



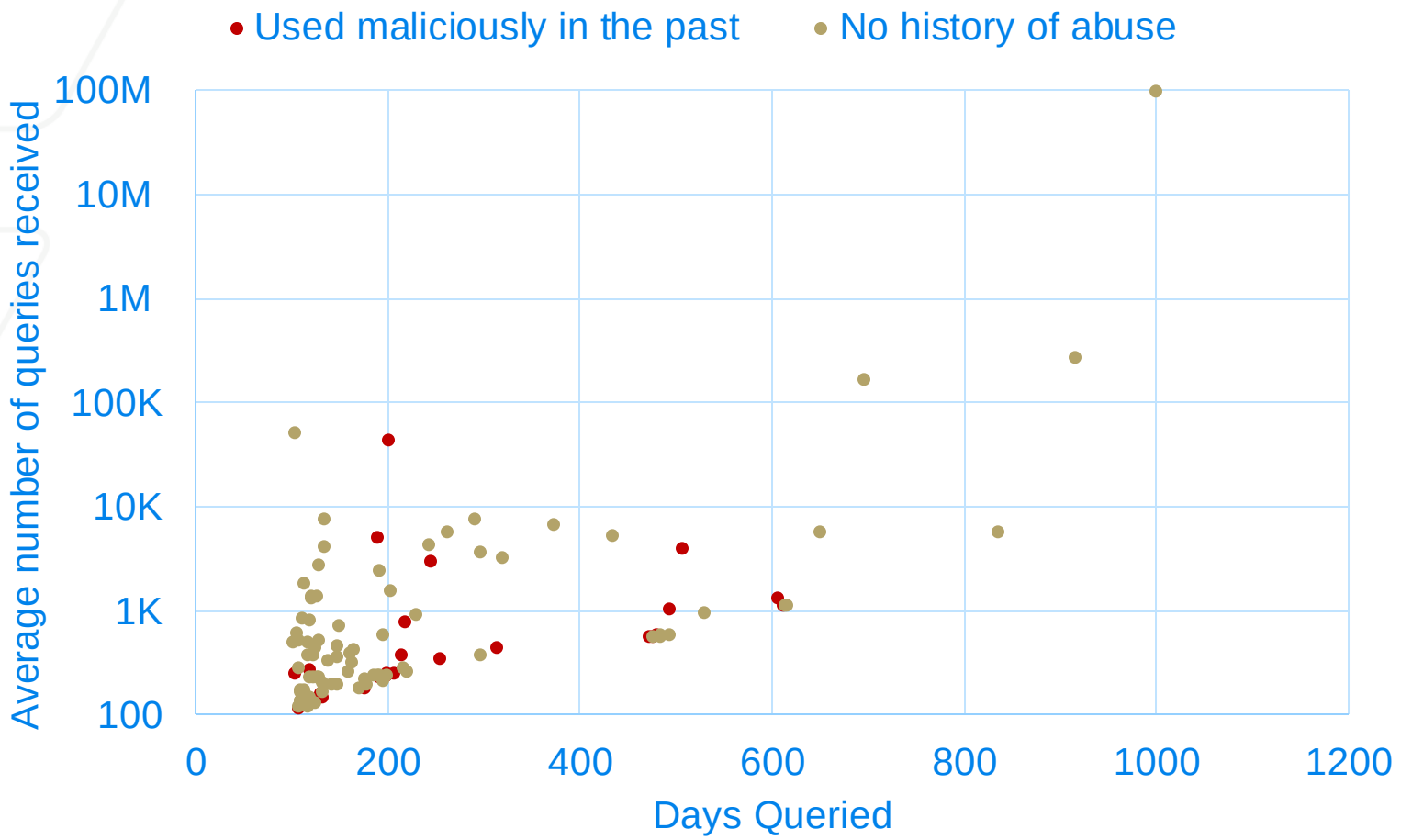
The **best median** score:

0.36

There is still **room for improvement** for their strategies.

Georgia Tech

Queries received by available domains



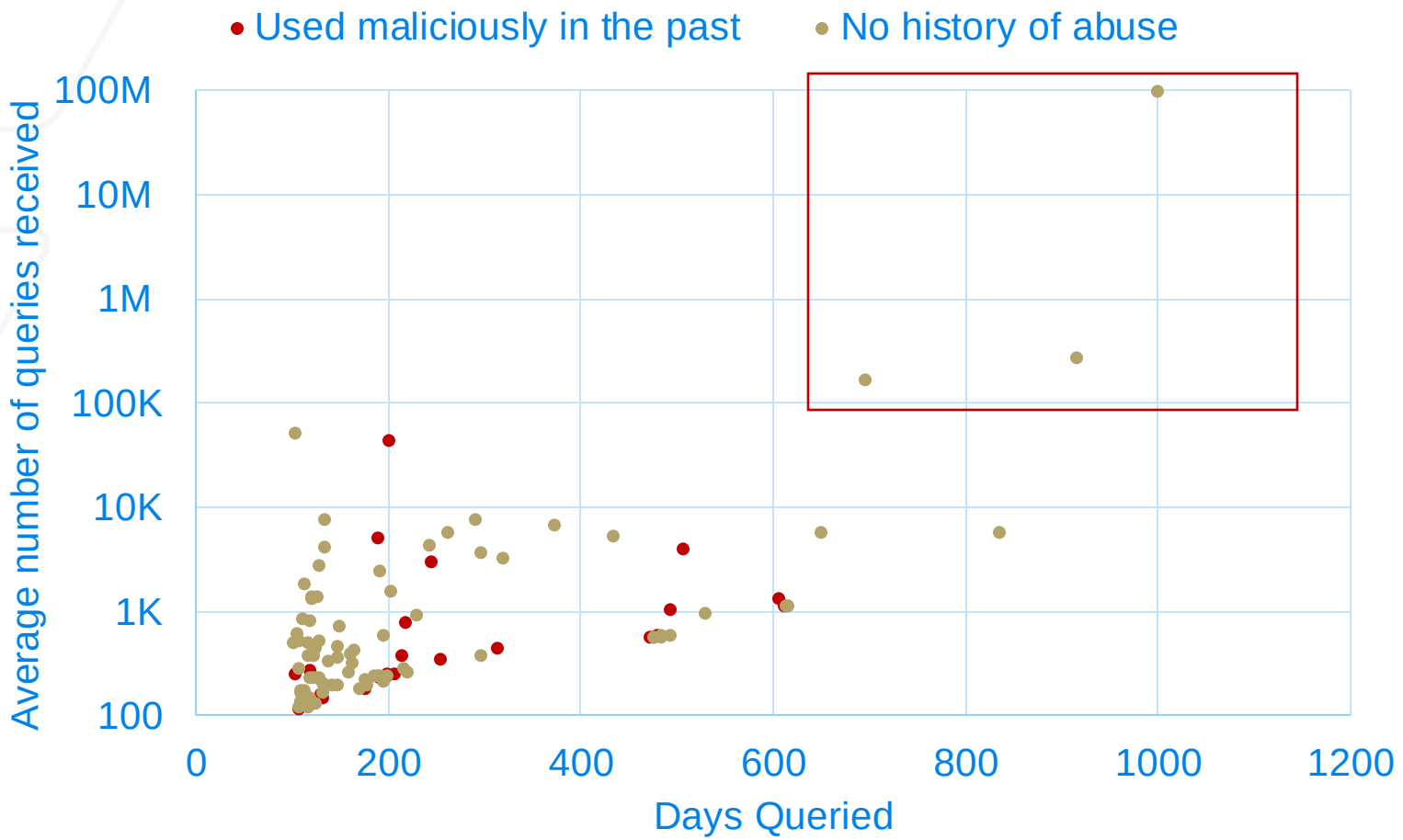
110

available domains queried for **more than 100 days**.

Adversaries can use those domain names maliciously.

Georgia Tech

Queries received by available domains



110

available domains queried for **more than 100 days**.

Adversaries can use those domain names maliciously.

Georgia Tech

Summary

1

Comprehensive study of defensive registrations

Georgia Tech

Summary

2

Assessment of the adequacy of observed defensive strategies

1

Comprehensive study of defensive registrations

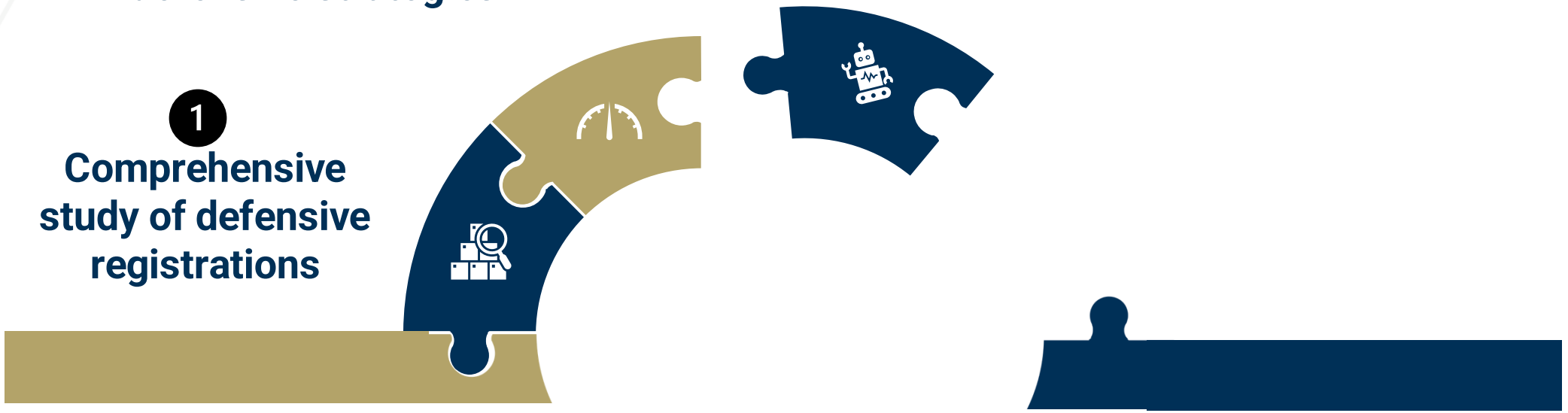
Georgia Tech

Summary

2
Assessment of the adequacy of observed defensive strategies

3
Better recommender models for defensive registrations

1
Comprehensive study of defensive registrations



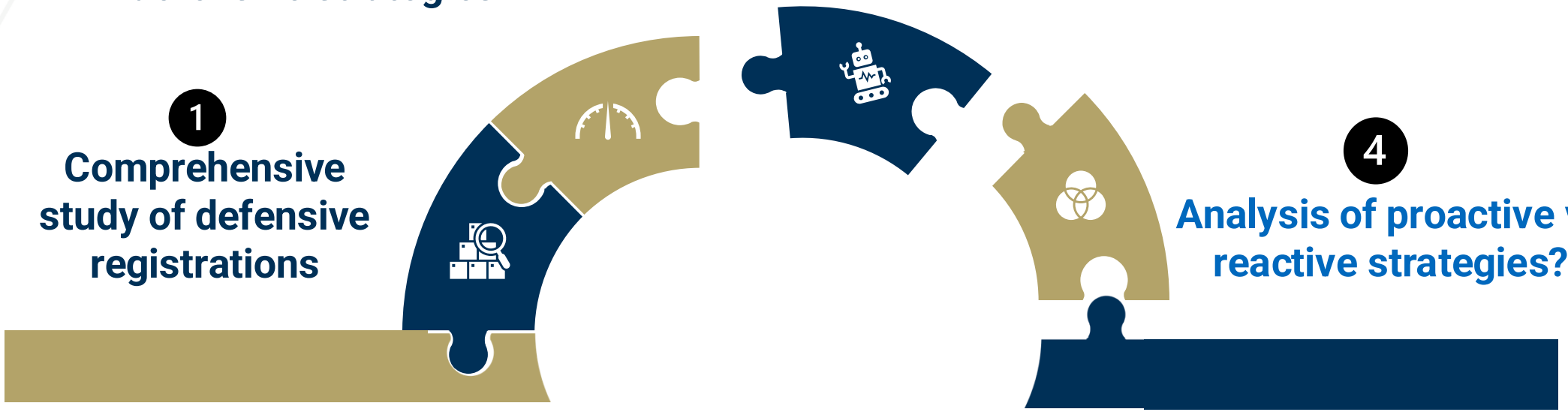
Georgia Tech

Summary

2
Assessment of the adequacy of observed defensive strategies

3
Better recommender models for defensive registrations

1
Comprehensive study of defensive registrations



4
Analysis of proactive vs reactive strategies?

Thanks

Vinny Adjibi
vinny.adjibi@gatech.edu

Georgia Tech