Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

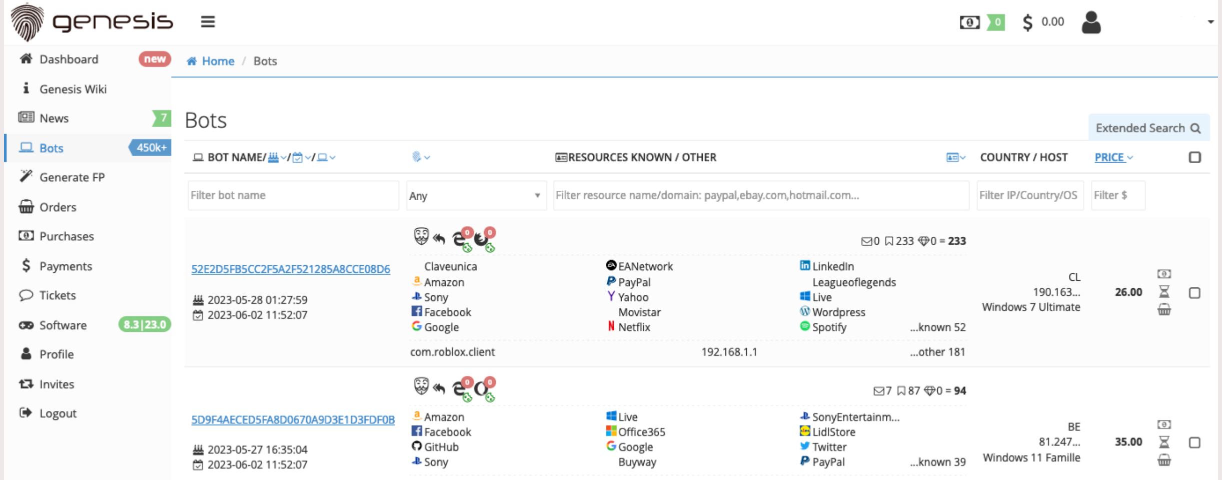
Michele Campobasso & Luca Allodi

Security Group, Mathematics and Computer Science

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

An innovative underground market for user impersonation at scale

Operating under a new threat model affecting victims worldwide: **Impersonation-as-a-Service**[1]



Bots

BOT NAME/ / /		RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE	□
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...	Filter IP/Country/OS	Filter $	
52E2D5FB5CC2F5A2F521285A8CCE08D6 2023-05-28 01:27:59 2023-06-02 11:52:07	0 0	✉0 233 0 = **233** Claveunica, Amazon, Sony, Facebook, Google EANetwork, PayPal, Yahoo, Movistar, Netflix LinkedIn, Leagueoflegends, Live, Wordpress, Spotify ...known 52 com.roblox.client 192.168.1.1 ...other 181	CL 190.163... Windows 7 Ultimate	**26.00**	□
5D9F4AECED5FA8D0670A9D3E1D3FDF0B 2023-05-27 16:35:04 2023-06-02 11:52:07	0 0	✉7 87 0 = **94** Amazon, Facebook, GitHub, Sony Live, Office365, Google, Buyway SonyEntertainm..., LidlStore, Twitter, PayPal ...known 39	BE 81.247... Windows 11 Famille	**35.00**	□

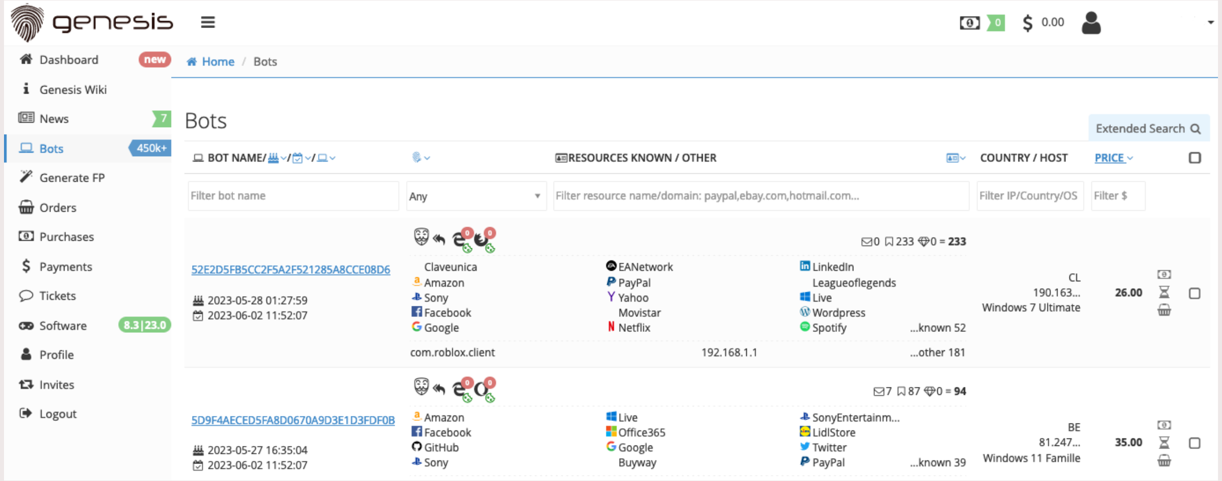
Open gaps:

- Threat size
- Market revenue
- Attacker preferences → *which type of users are most at risk?*

[1] Campobasso, M.; Allodi L., **Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale,** *In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), DOI: 10.1145/3372297.3417892*

An innovative underground market for user impersonation at scale

Operating under a new threat model affecting victims worldwide: **Impersonation-as-a-Service**[1]



Bots

BOT NAME/ / /		RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE	□
Filter bot name	Any ▾	Filter resource name/domain: paypal,ebay.com,hotmail.com...	Filter IP/Country/OS	Filter $	
52E2D5FB5CC2F5A2F521285A8CCE08D6 2023-05-28 01:27:59 2023-06-02 11:52:07		✉0 233 0 = **233** Claveunica Amazon Sony Facebook Google EANetwork PayPal Yahoo Movistar Netflix LinkedIn Leagueoflegends Live Wordpress Spotify ...known 52 com.roblox.client 192.168.1.1 ...other 181	CL 190.163... Windows 7 Ultimate	**26.00**	□
5D9F4AECED5FA8D0670A9D3E1D3FDF0B 2023-05-27 16:35:04 2023-06-02 11:52:07		✉7 87 0 = **94** Amazon Facebook GitHub Sony Live Office365 Google Buyway SonyEntertainm... LidlStore Twitter PayPal ...known 39	BE 81.247... Windows 11 Famille	**35.00**	□

Open gaps:

- Threat size
- Market revenue
- Attacker preferences → *which type of users are most at risk?*

A unique opportunity to directly measure supply & demand to estimate attacker preferences & market size (no proxy – e.g. user feedback)

[1] Campobasso, M.; Allodi L., **Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale,** *In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), DOI: 10.1145/3372297.3417892*

Challenges and solutions to accurately measure Genesis Market’s activity

Challenges	Solutions
Restricted access via invite	Infiltration in affiliated community to obtain 6 invites for 6 accounts

Challenges and solutions to accurately measure Genesis Market’s activity

Challenges	Solutions
Restricted access via invite	Infiltration in affiliated community to obtain 6 invites for 6 accounts
Anti-crawler mechanisms → tradeoff between data completeness & stealth (risking ban)	Browser instrumentation + throttling + 24h sampling + splitting task among 6 crawlers

Challenges and solutions to accurately measure Genesis Market's activity

Challenges	Solutions
Restricted access via invite	Infiltration in affiliated community to obtain 6 invites for 6 accounts
Anti-crawler mechanisms → tradeoff between data completeness & stealth (risking ban)	Browser instrumentation + throttling + 24h sampling + splitting task among 6 crawlers
Data censored due to connectivity limitations (market availability & TOR network congestion)	Retry crawling + collect summary data + statistical evaluation to estimate & recreate missing data

Challenges and solutions to accurately measure Genesis Market’s activity

Challenges	Solutions
Restricted access via invite	Infiltration in affiliated community to obtain 6 invites for 6 accounts
Anti-crawler mechanisms → tradeoff between data completeness & stealth (risking ban)	Browser instrumentation + throttling + 24h sampling + splitting task among 6 crawlers
Data censored due to connectivity limitations (market availability & TOR network congestion)	Retry crawling + collect summary data + statistical evaluation to estimate & recreate missing data

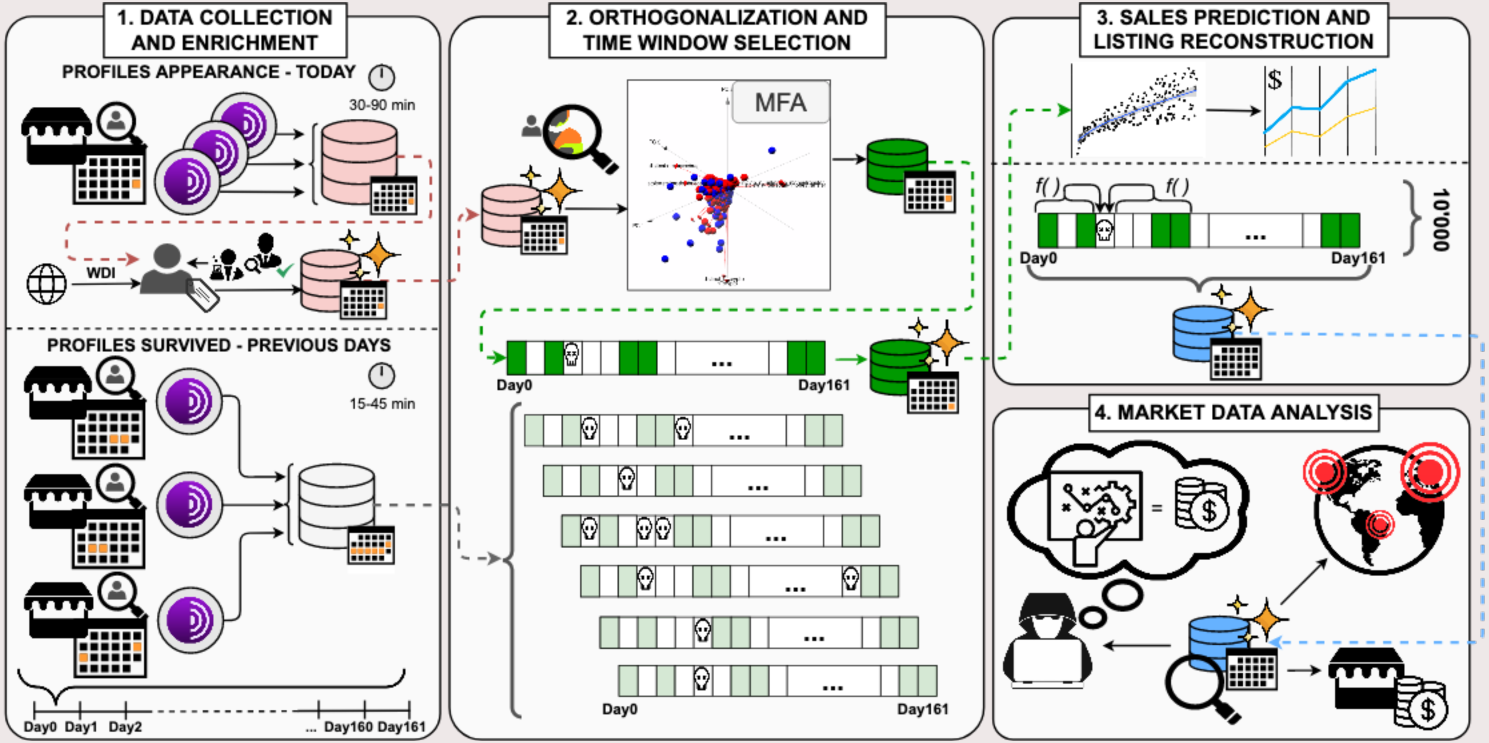
Inc. waking up at night to check if the crawler is working 😤

Challenges and solutions to accurately measure Genesis Market's activity

Challenges	Solutions
Restricted access via invite	Infiltration in affiliated community to obtain 6 invites for 6 accounts
Anti-crawler mechanisms → tradeoff between data completeness & stealth (risking ban)	Browser instrumentation + throttling + 24h sampling + splitting task among 6 crawlers
Data censored due to connectivity limitations (market availability & TOR network congestion)	Retry crawling + collect summary data + statistical evaluation to estimate & recreate missing data
High dimensionality & noisy data	Aggregation of effects with dimensionality reduction, sales prediction model accounting for attacker decisions based on the daily supply

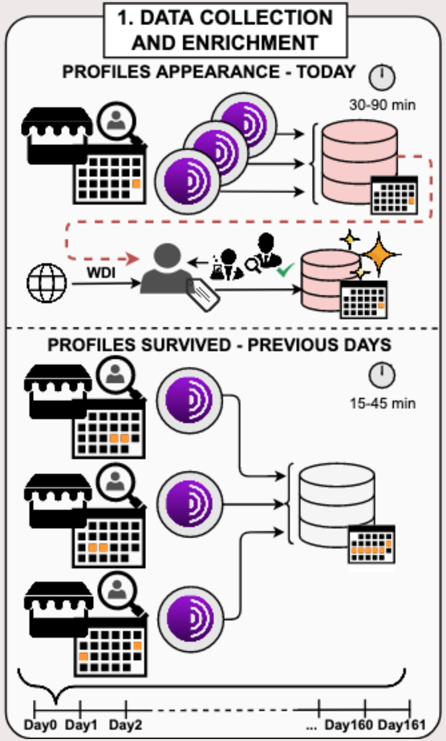
Inc. waking up at night to check if the crawler is working 😤

Measuring attacker preferences from an active market


1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0 Day1 Day2 ... Day160 Day161
2. ORTHOGONALIZATION AND TIME WINDOW SELECTION
MFA
...
Day0
Day161
Day0
Day161
3. SALES PREDICTION AND LISTING RECONSTRUCTION
$
f( )
f( )
...
Day0
Day161
10'000
4. MARKET DATA ANALYSIS
=
$
$

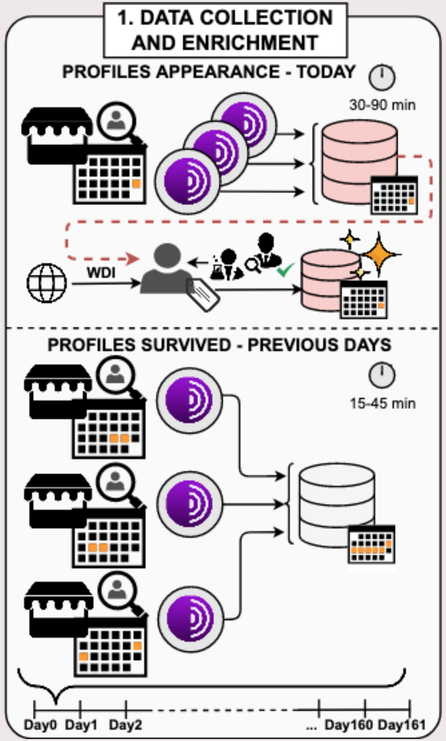
Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Measuring attacker preferences from an active market


1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0
Day1
Day2
...
Day160
Day161

- Data collection from Jan 21st to Jun 30th 2021 (161 days)

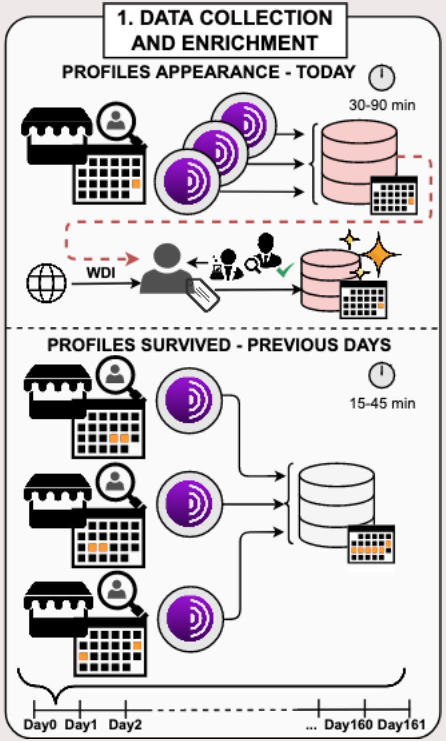
Measuring attacker preferences from an active market


1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0
Day1
Day2
...
Day160
Day161

- Data collection from Jan 21st to Jun 30th 2021 (161 days)

- 3 crawlers sampling 25% of appeared profiles in the last 24h at MSK midnight
- 3 crawlers checking ”survived” profiles over the next 6 days

Measuring attacker preferences from an active market

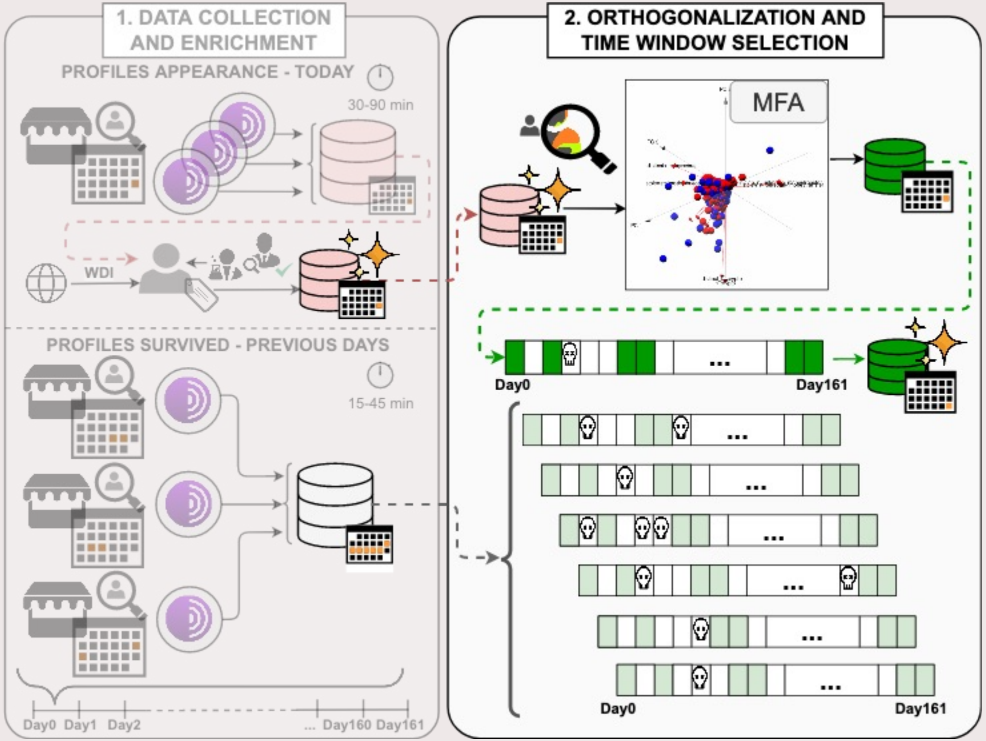

1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0
Day1
Day2
...
Day160
Day161

- Data collection from Jan 21st to Jun 30th 2021 (161 days)

- 3 crawlers sampling 25% of appeared profiles in the last 24h at MSK midnight
- 3 crawlers checking ”survived” profiles over the next 6 days

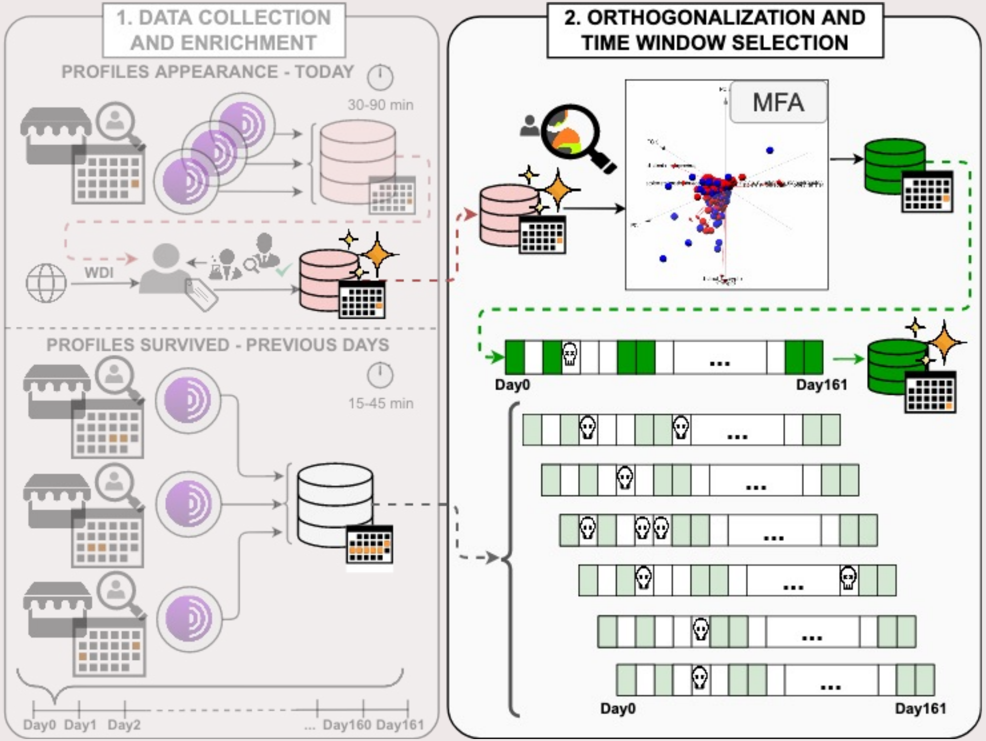
- Complete info for 107/161 days→ 12’149 profiles with detailed info
- Data enriched with GDP/capita based on country of origin
- Classification of available credentials wrt website purpose (moneytransfer, social, commerce, …)

Measuring attacker preferences from an active market


1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0 Day1 Day2
... Day160 Day161
2. ORTHOGONALIZATION AND TIME WINDOW SELECTION
MFA
Day0
Day161
Day0
Day161

- Dimensionality reduction (MFA) on appeared profiles
  - Dimensions are linear combinations of variables (“profile class”)

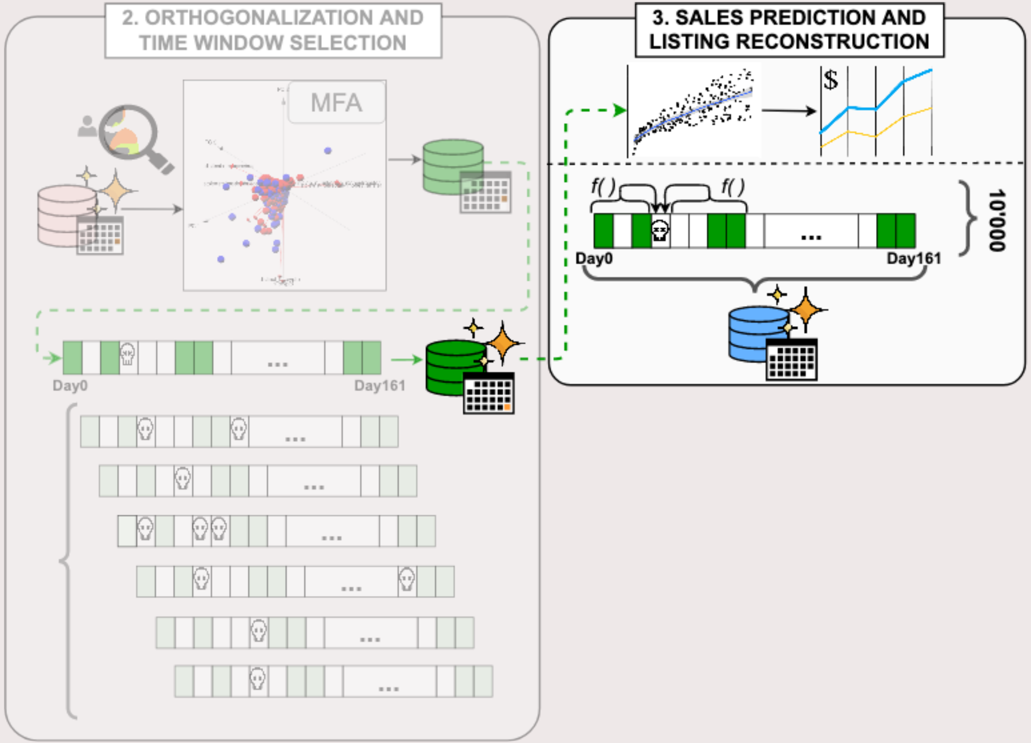
Measuring attacker preferences from an active market


1. DATA COLLECTION AND ENRICHMENT
PROFILES APPEARANCE - TODAY
30-90 min
WDI
PROFILES SURVIVED - PREVIOUS DAYS
15-45 min
Day0 Day1 Day2
... Day160 Day161
2. ORTHOGONALIZATION AND TIME WINDOW SELECTION
MFA
...
Day0
Day161
Day0
Day161

- Dimensionality reduction (MFA) on appeared profiles
  - Dimensions are linear combinations of variables ("profile class")
- First day of sales only → 101/107 days with complete data – 57% total sales (only 6 days for which we cannot measure sales)

Measuring attacker preferences from an active market

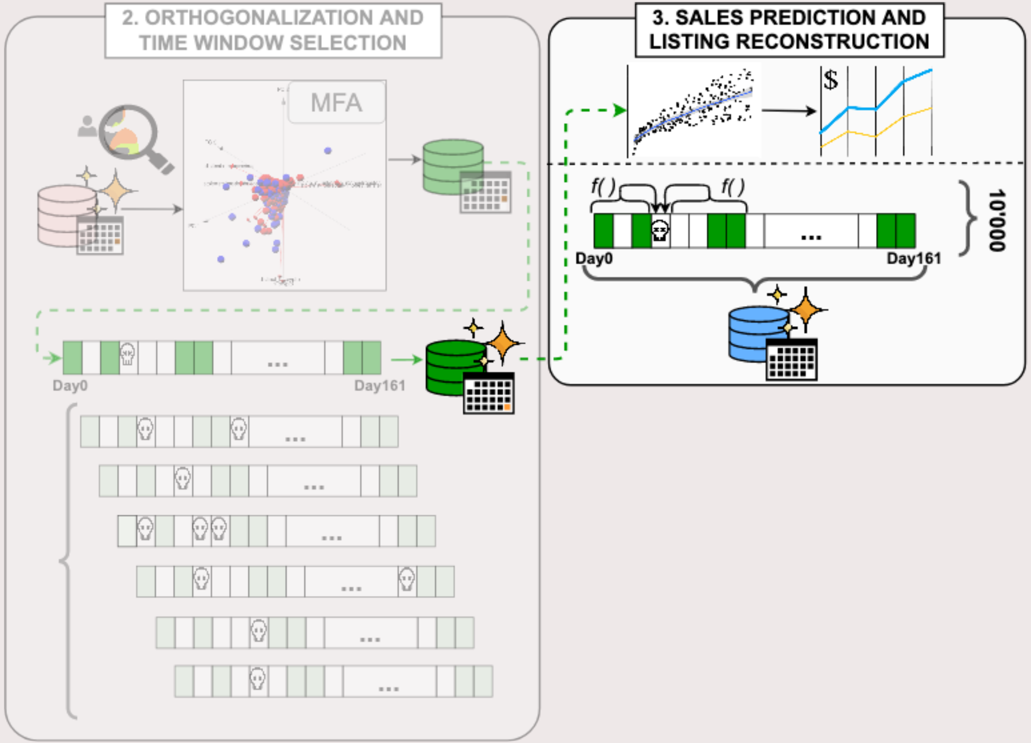
- GLMM sales prediction model (random effect → daily supply) from 101/107 days with complete data
- Predict sales for the 6 days with no information on sales



2. ORTHOGONALIZATION AND TIME WINDOW SELECTION
MFA
Day0
Day161
...
3. SALES PREDICTION AND LISTING RECONSTRUCTION
$
f( )
f( )
...
Day0
Day161
10'000

Measuring attacker preferences from an active market

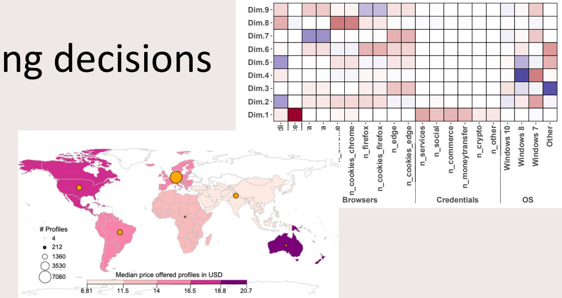
- GLMM sales prediction model (random effect → daily supply) from 101/107 days with complete data
- Predict sales for the 6 days with no information on sales
- Montecarlo sim. to recreate the 161-107=54 missing days


2. ORTHOGONALIZATION AND TIME WINDOW SELECTION
MFA
...
Day0
Day161
3. SALES PREDICTION AND LISTING RECONSTRUCTION
$
f( )
f( )
...
Day0
Day161
10'000

Measuring attacker preferences from an active market

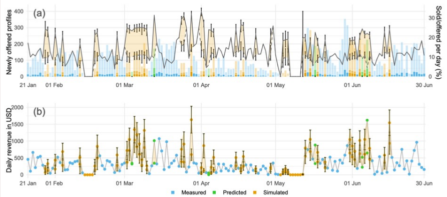
Finally (!), we can study (spoiler alert):

- Attackers' purchasing decisions

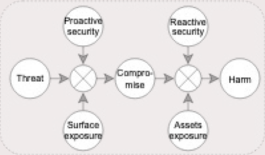


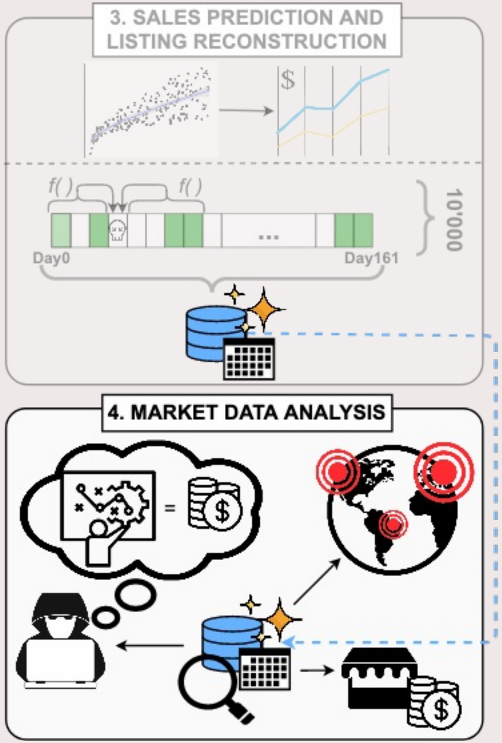
- Scale of the threat

- Market revenues



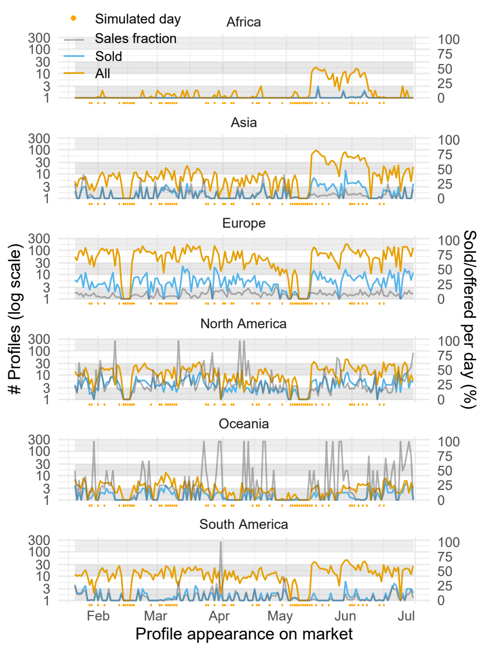
- The relationship between findings and Woods & Böhme's risk model



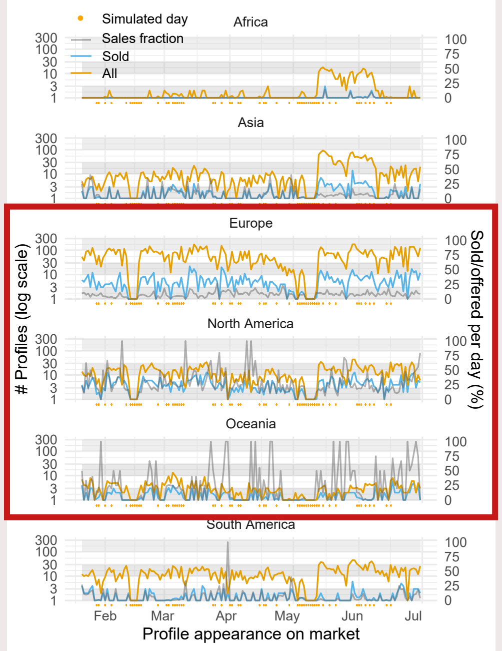


Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Rich nations are targeted, nuanced profiles selection

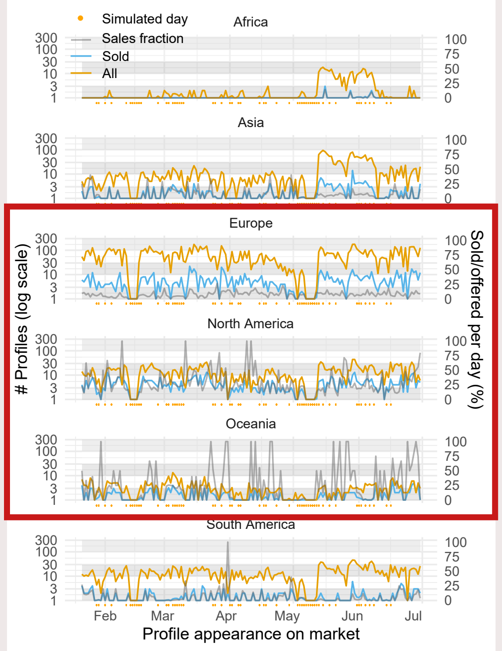


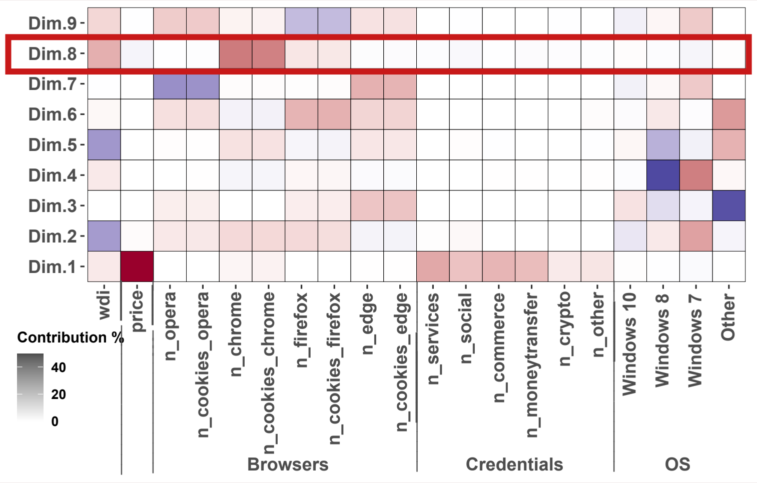
Rich nations are targeted, nuanced profiles selection



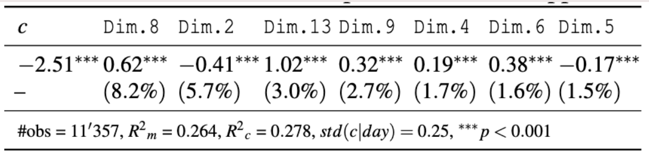
- +60% supply from EU, 12% NA
- Supply ~matches demand in NA & OCE (NA 4x more preferred than EU)

Rich nations are targeted, nuanced profiles selection





Dim8: Profiles from wealthier countries (positive sign wdi) rich in stolen cookies from Chrome (positive sign n_cookies_chrome & n_chrome)

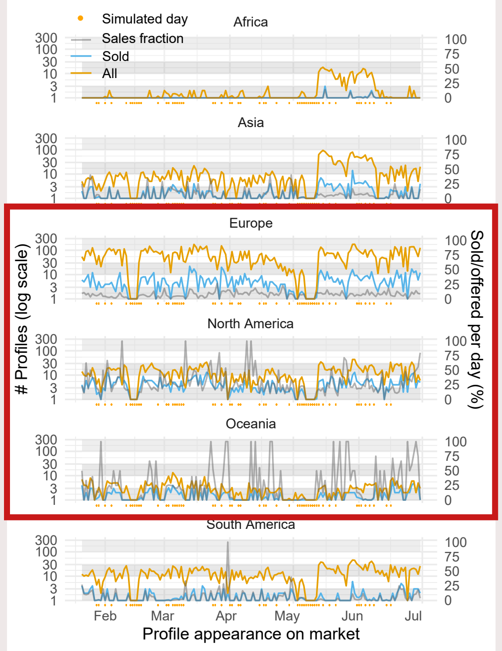


c	Dim.8	Dim.2	Dim.13	Dim.9	Dim.4	Dim.6	Dim.5
-2.51^{***}	0.62^{***}	-0.41^{***}	1.02^{***}	0.32^{***}	0.19^{***}	0.38^{***}	-0.17^{***}
–	(8.2%)	(5.7%)	(3.0%)	(2.7%)	(1.7%)	(1.6%)	(1.5%)

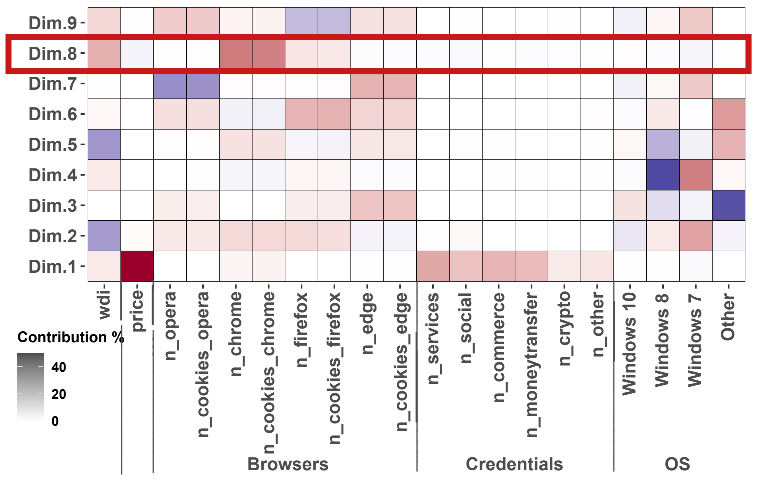
#obs = 11′357, $R^2{}_m = 0.264$, $R^2{}_c = 0.278$, $std(c|day) = 0.25$, $^{***}p < 0.001$

- +60% supply from EU, 12% NA
- Supply ~matches demand in NA & OCE (NA 4x more preferred than EU)

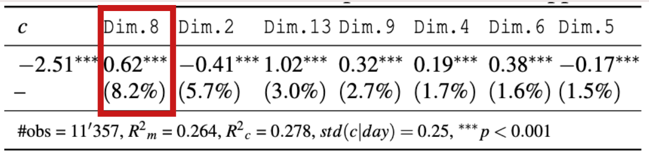
Rich nations are targeted, nuanced profiles selection



- +60% supply from EU, 12% NA
- Supply ~matches demand in NA & OCE (NA 4x more preferred than EU)



Dim8: Profiles from wealthier countries (positive sign wdi) rich in stolen cookies from Chrome (positive sign n_cookies_chrome & n_chrome)

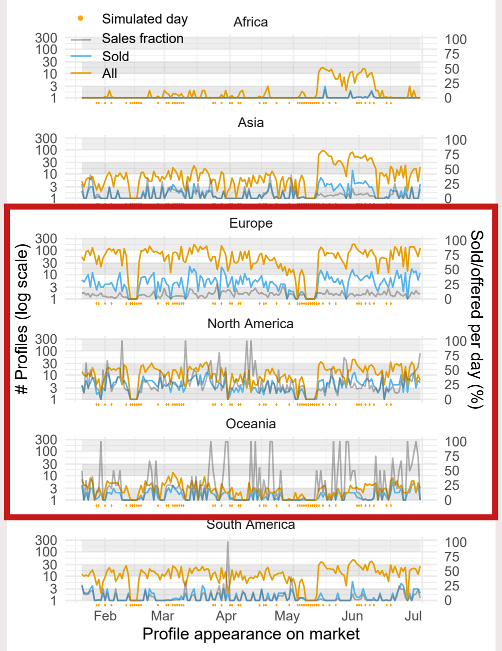


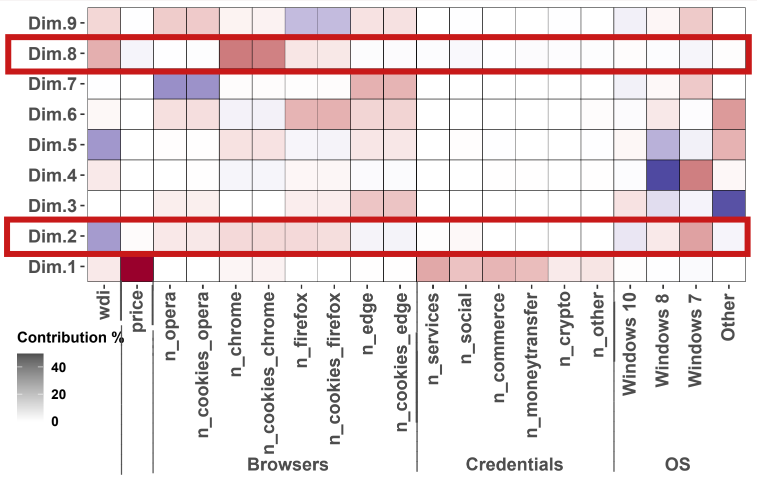
c	Dim.8	Dim.2	Dim.13	Dim.9	Dim.4	Dim.6	Dim.5
-2.51^{***}	0.62^{***}	-0.41^{***}	1.02^{***}	0.32^{***}	0.19^{***}	0.38^{***}	-0.17^{***}
–	(8.2%)	(5.7%)	(3.0%)	(2.7%)	(1.7%)	(1.6%)	(1.5%)

#obs = 11′357, $R^2{}_m = 0.264$, $R^2{}_c = 0.278$, $std(c|day) = 0.25$, $^{***}p < 0.001$

Dim8: are more likely to be sold (positive coefficient)

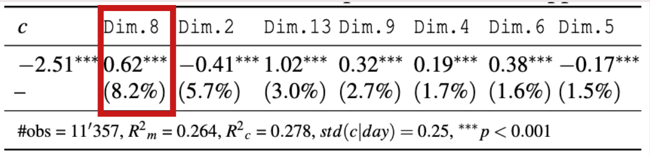
Rich nations are targeted, nuanced profiles selection





Dim8: Profiles from wealthier countries (positive sign wdi) rich in stolen cookies from Chrome (positive sign n_cookies_chrome & n_chrome)

Dim2: Profiles from poorer countries (negative sign wdi) exhibiting older OSs (positive sign win7/8)



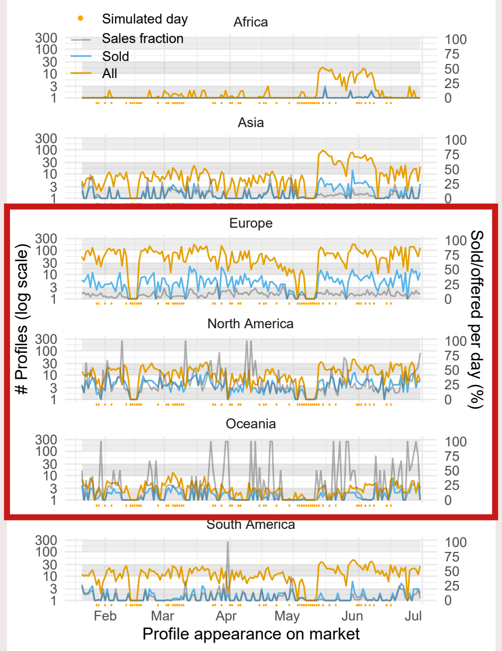
c	Dim.8	Dim.2	Dim.13	Dim.9	Dim.4	Dim.6	Dim.5
-2.51^{***} –	0.62^{***} (8.2%)	-0.41^{***} (5.7%)	1.02^{***} (3.0%)	0.32^{***} (2.7%)	0.19^{***} (1.7%)	0.38^{***} (1.6%)	-0.17^{***} (1.5%)

#obs = 11′357, $R^2{}_m = 0.264$, $R^2{}_c = 0.278$, $std(c|day) = 0.25$, $^{***}p < 0.001$

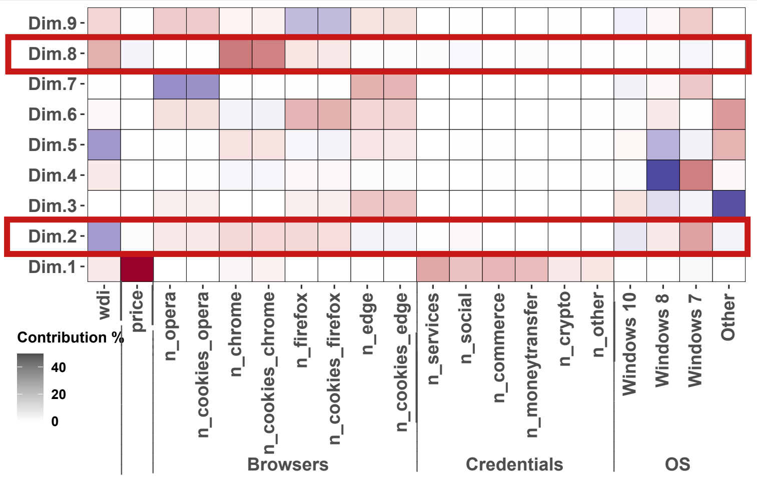
Dim8: are more likely to be sold (positive coefficient)

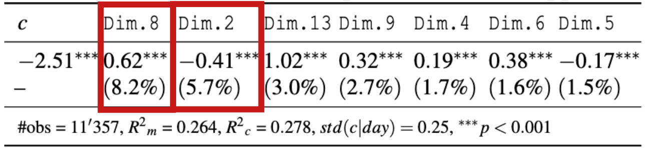
- +60% supply from EU, 12% NA
- Supply ~matches demand in NA & OCE (NA 4x more preferred than EU)

Rich nations are targeted, nuanced profiles selection



- +60% supply from EU, 12% NA
- Supply ~matches demand in NA & OCE (NA 4x more preferred than EU)





c	Dim.8	Dim.2	Dim.13	Dim.9	Dim.4	Dim.6	Dim.5
−2.51***	0.62***	−0.41***	1.02***	0.32***	0.19***	0.38***	−0.17***
–	(8.2%)	(5.7%)	(3.0%)	(2.7%)	(1.7%)	(1.6%)	(1.5%)

#obs = 11′357, $R^2{}_m = 0.264$, $R^2{}_c = 0.278$, $std(c|day) = 0.25$, $^{***}p < 0.001$

Dim8: Profiles from wealthier countries (positive sign wdi) rich in stolen cookies from Chrome (positive sign n_cookies_chrome & n_chrome)

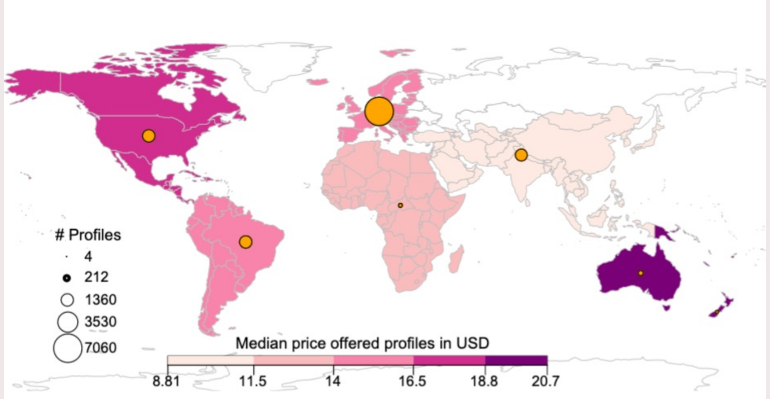
Dim2: Profiles from poorer countries (negative sign wdi) exhibiting older OSs (positive sign win7/8)

Dim8: are more likely to be sold (positive coefficient)

Dim2: are less likely to be sold (negative coefficient)

A lucrative, worldwide scale threat

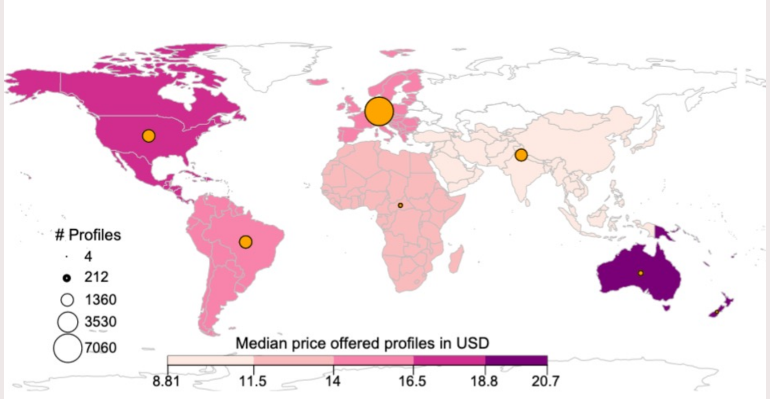
Offered profiles median prices and volume



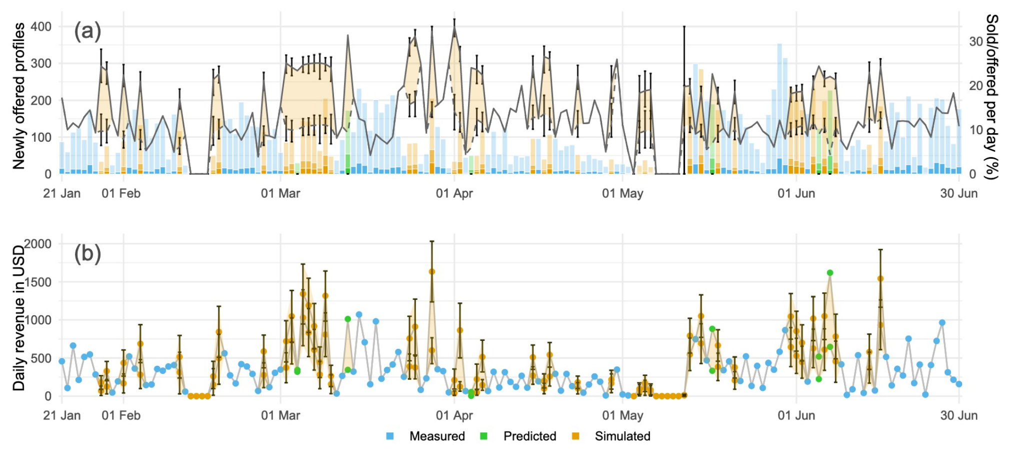
First world regions are main targets, Europe first
Ex-URSS countries are not included

A lucrative, worldwide scale threat

Offered profiles median prices and volume



Supply and demand (i.e., actual affected users) and revenues



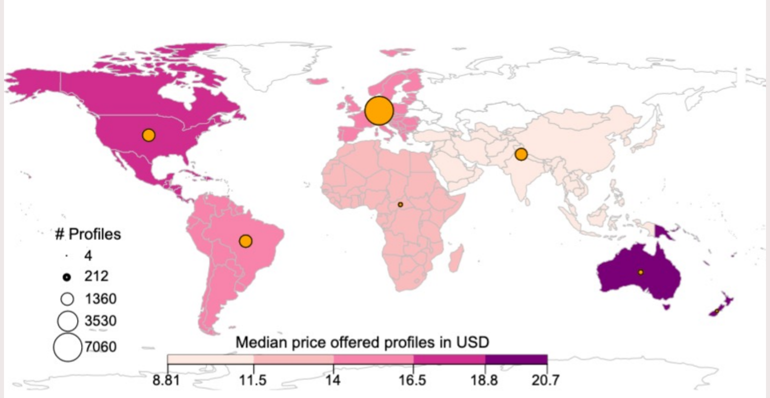
First world regions are main targets, Europe first
Ex-URSS countries are not included

Scaled up numbers (accounting for sampling & data censorship):

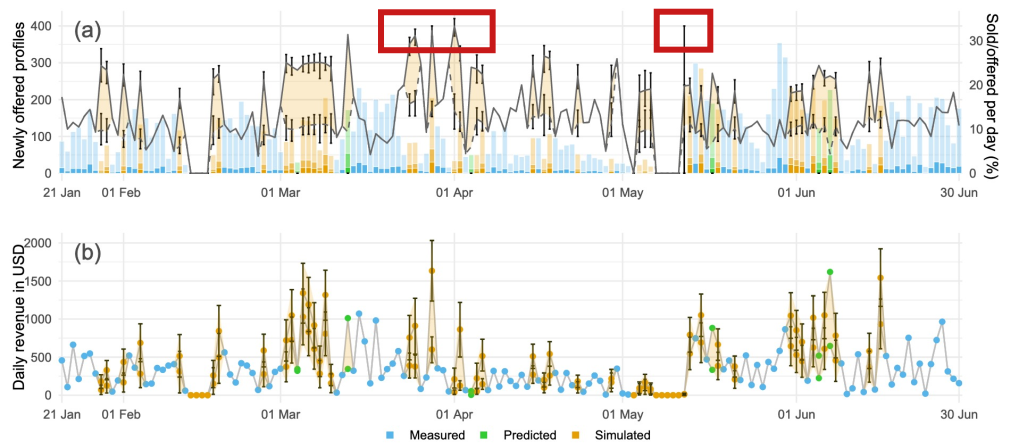
Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

A lucrative, worldwide scale threat

Offered profiles median prices and volume



Supply and demand (i.e., actual affected users) and revenues



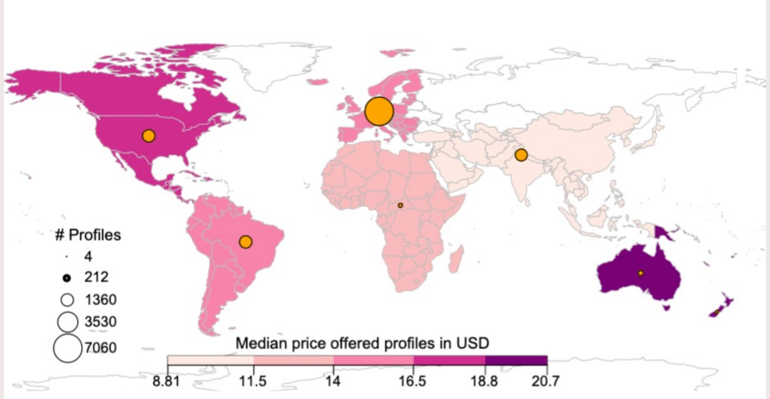
First world regions are main targets, Europe first
Ex-URSS countries are not included

Scaled up numbers (accounting for sampling & data censorship):

- Up to **3’800** new listed profiles daily (**600** on average)

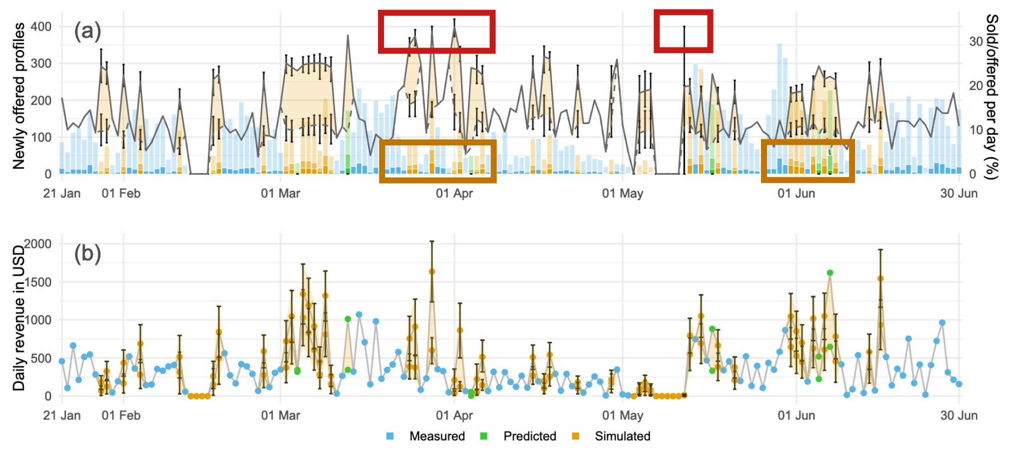
A lucrative, worldwide scale threat

Offered profiles median prices and volume



First world regions are main targets, Europe first
Ex-URSS countries are not included

Supply and demand (i.e., actual affected users) and revenues



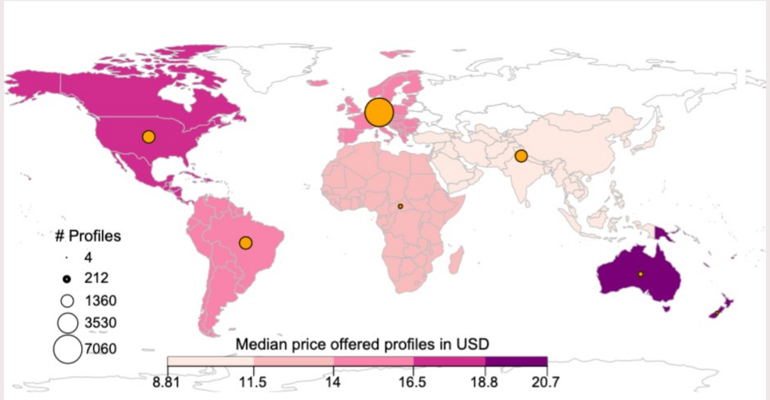
Scaled up numbers (accounting for sampling & data censorship):

- Up to **3’800** new listed profiles daily (**600** on average)
- Up to **430** profiles sold (**actual people attacked**) daily (avg **125**)

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

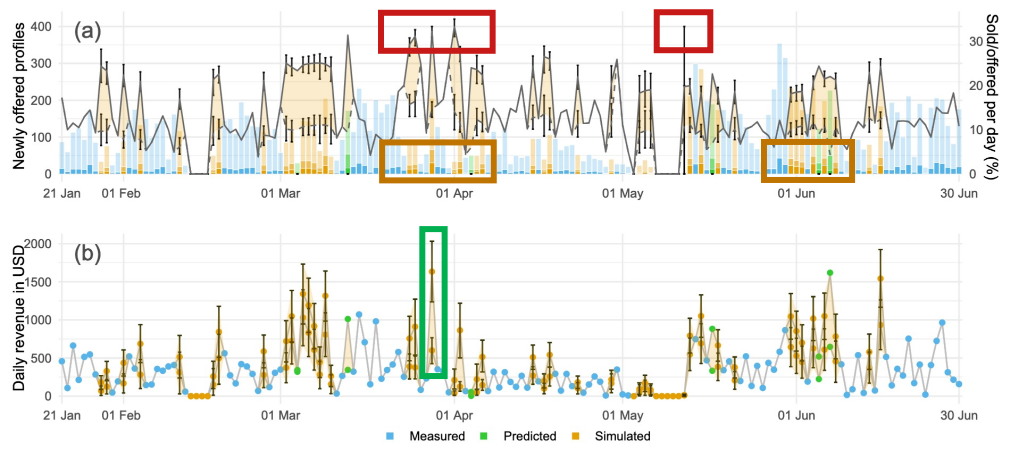
A lucrative, worldwide scale threat

Offered profiles median prices and volume



First world regions are main targets, Europe first
Ex-URSS countries are not included

Supply and demand (i.e., actual affected users) and revenues



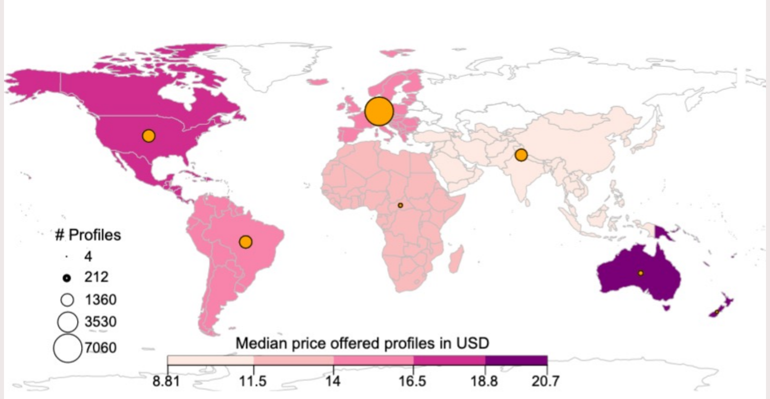
Scaled up numbers (accounting for sampling & data censorship):

- Up to **3'800** new listed profiles daily (**600** on average)
- Up to **430** profiles sold (**actual people attacked**) daily (avg **125**)
- Estimated daily revenues: avg **3'000 – 4'000$**, max: **7'200 – 16'400$**

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

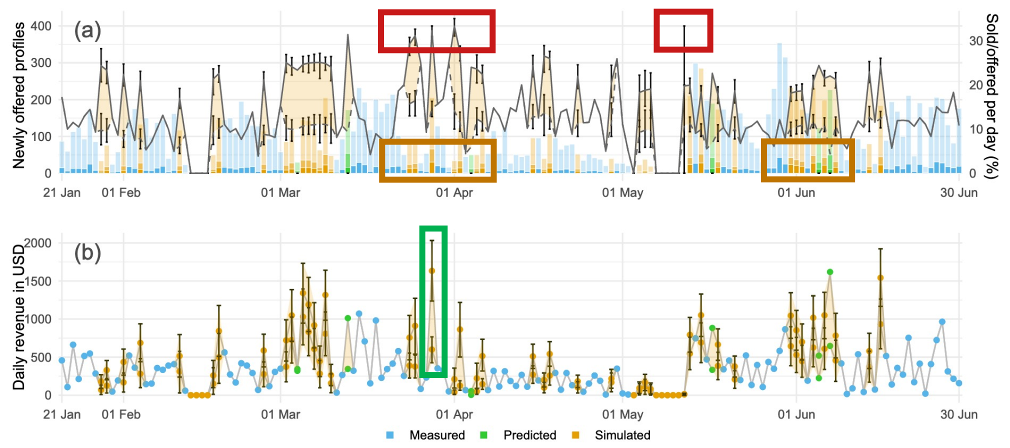
A lucrative, worldwide scale threat

Offered profiles median prices and volume



First world regions are main targets, Europe first
Ex-URSS countries are not included

Supply and demand (i.e., actual affected users) and revenues



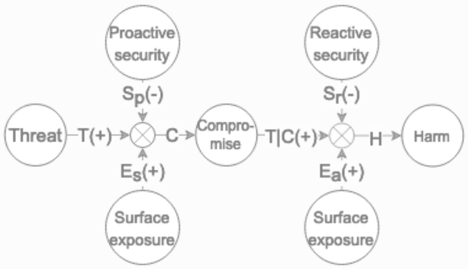
Scaled up numbers (accounting for sampling & data censorship):

- Up to **3’800** new listed profiles daily (**600** on average)
- Up to **430** profiles sold (**actual people attacked**) daily (avg **125**)
- Estimated daily revenues: avg **3’000 – 4’000$**, max: **7’200 – 16’400$**
- Estimated yearly market revenues: **1.2M – 1.6M$**

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme’s cyber risk model

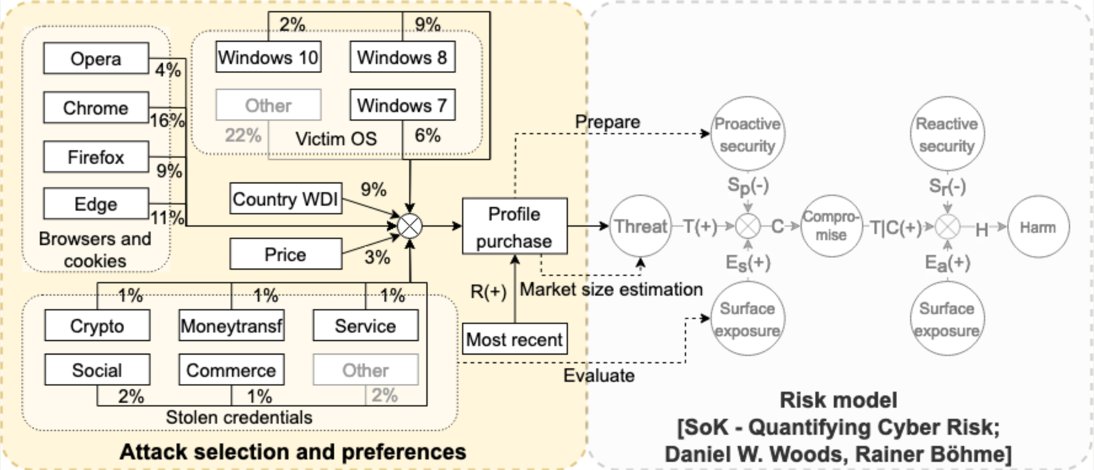
Threat is a consequence of the attackers’ decisions.



Risk model
[SoK - Quantifying Cyber Risk; Daniel W. Woods, Rainer Böhme]

Attacker preferences to inform Woods & Böhme’s cyber risk model

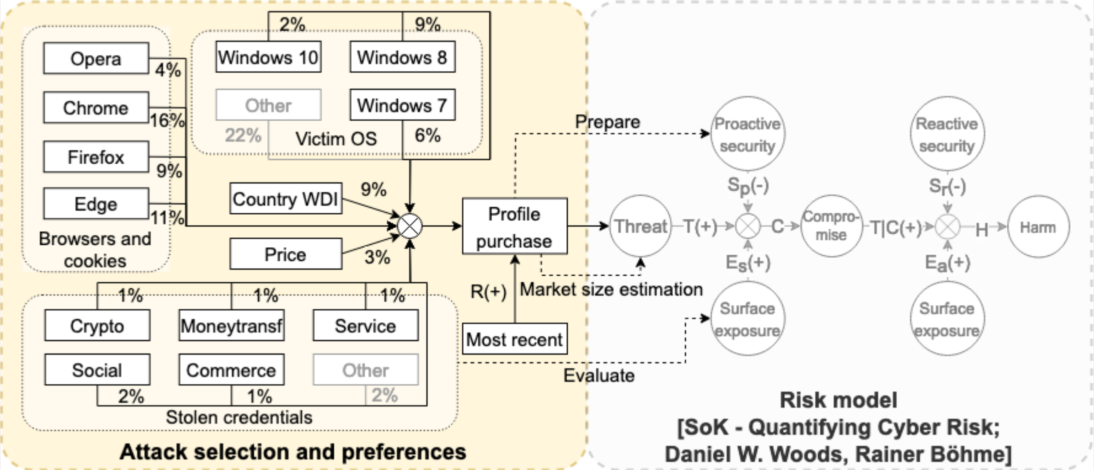
Threat is a consequence of the attackers’ decisions.



Attacker preferences to inform Woods & Böhme’s cyber risk model

Threat is a consequence of the attackers’ decisions.

Purchase decisions are mostly influenced by (but there’s more):



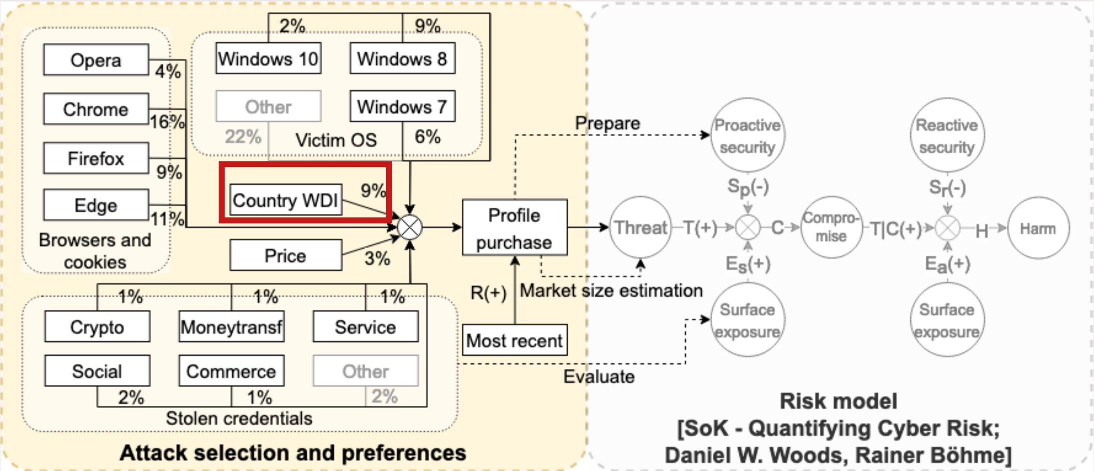
Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme's cyber risk model

Threat is a consequence of the attackers' decisions.

Purchase decisions are mostly influenced by (but there's more):

- expected wealth (country WDI)



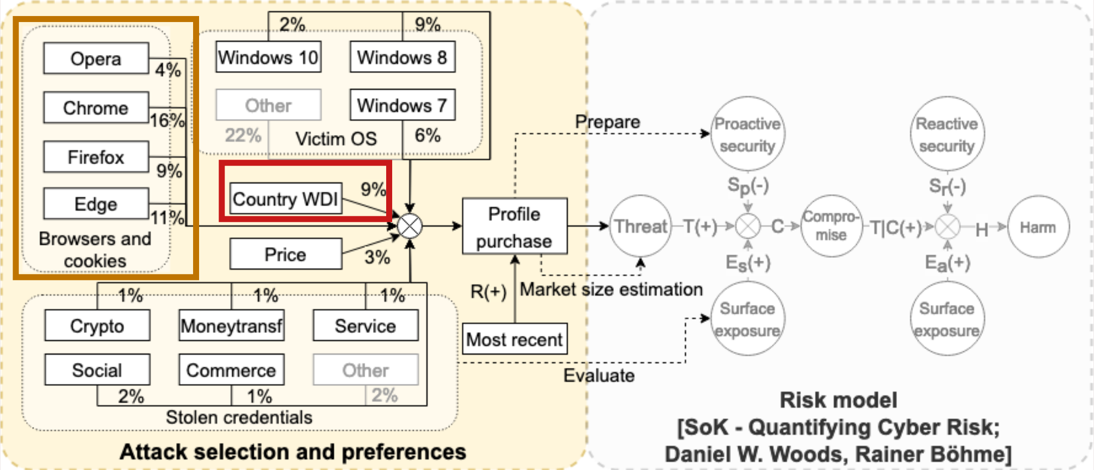
Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme’s cyber risk model

Threat is a consequence of the attackers’ decisions.

Purchase decisions are mostly influenced by (but there’s more):

- expected wealth (country WDI)
- Technical details (mainly browsers)



Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

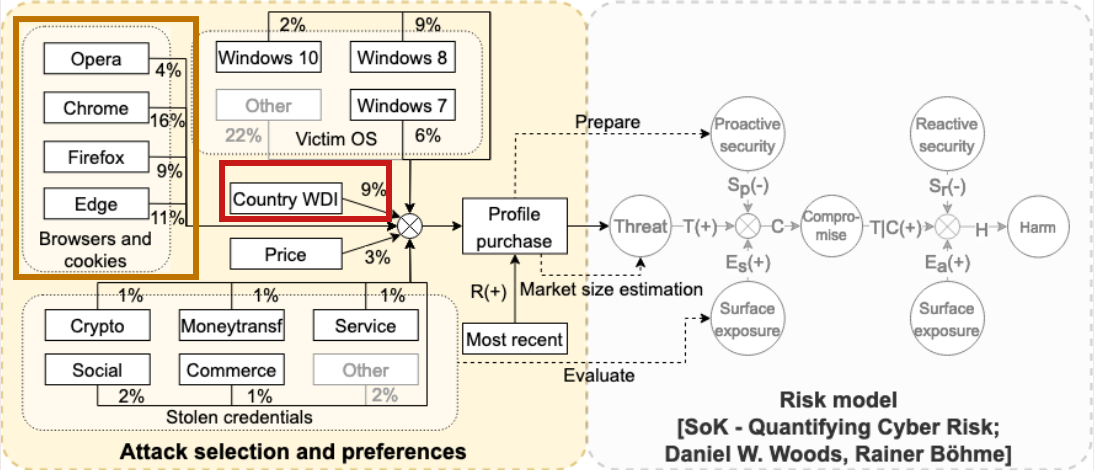
Attacker preferences to inform Woods & Böhme’s cyber risk model

Threat is a consequence of the attackers’ decisions.

Purchase decisions are mostly influenced by (but there’s more):

- expected wealth (country WDI)
- Technical details (mainly browsers)

Stakeholders could monitor market activity to:



Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme’s cyber risk model

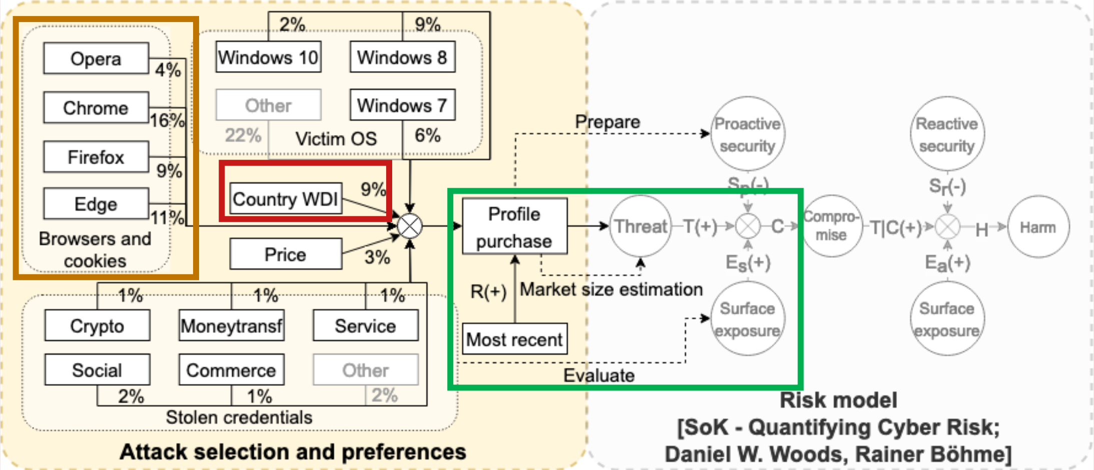
Threat is a consequence of the attackers’ decisions.

Purchase decisions are mostly influenced by (but there’s more):

- expected wealth (country WDI)
- Technical details (mainly browsers)

Stakeholders could monitor market activity to:

- evaluate exposure (market shows affected websites, …)



[SoK - Quantifying Cyber Risk; Daniel W. Woods, Rainer Böhme]

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme's cyber risk model

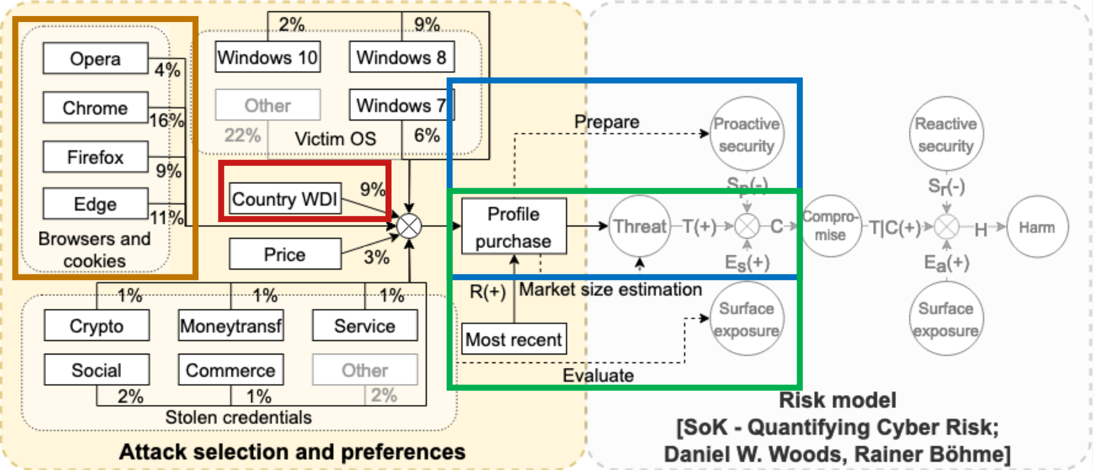
Threat is a consequence of the attackers' decisions.

Purchase decisions are mostly influenced by (but there's more):

- expected wealth (country WDI)
- Technical details (mainly browsers)

Stakeholders could monitor market activity to:

- evaluate exposure (market shows affected websites, …)
- prepare to attacks (revoke creds, mandate 2FA for a week, inform relevant SOC, …)



Risk model
[SoK - Quantifying Cyber Risk; Daniel W. Woods, Rainer Böhme]

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

Attacker preferences to inform Woods & Böhme's cyber risk model

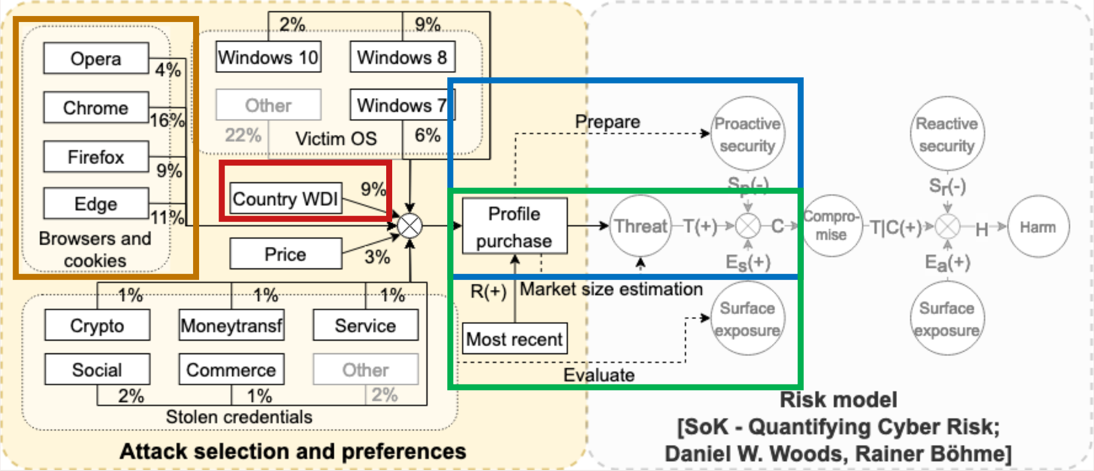
Threat is a consequence of the attackers' decisions.

Purchase decisions are mostly influenced by (but there's more):

- expected wealth (country WDI)
- Technical details (mainly browsers)

Stakeholders could monitor market activity to:

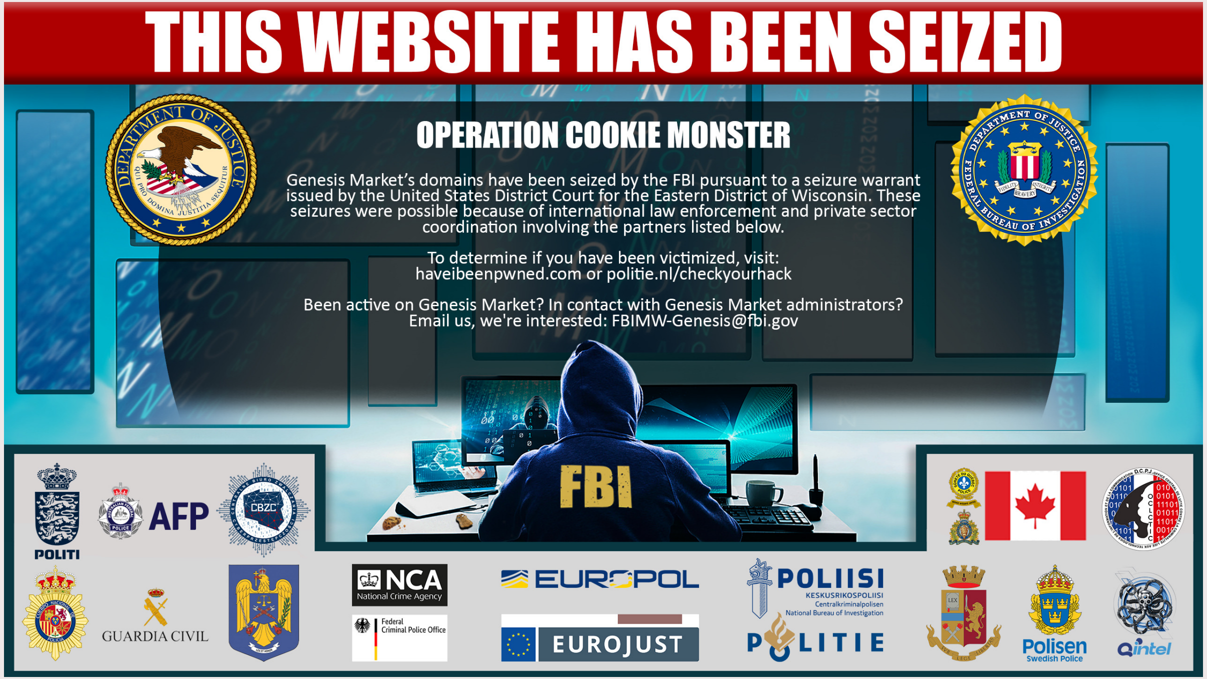
- evaluate exposure (market shows affected websites, …)
- prepare to attacks (revoke creds, mandate 2FA for a week, inform relevant SOC, …)



We should always consider how attackers think to better evaluate risks for the final user.

Know Your Cybercriminal: Evaluating Attacker Preferences by Measuring Profile Sales on an Active, Leading Criminal Market for User Impersonation at Scale

A tale of a market takedown



THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit:
haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov

FBI
POLITI
AFP
CBZC
GUARDIA CIVIL
NCA National Crime Agency
Federal Criminal Police Office
EUROPOL
EUROJUST
POLIISI KESKUSRIKOSPOLIISI Centralkriminalpolisen National Bureau of Investigation
POLITIE
Polisen Swedish Police
Qintel

Check if you were/are a victim: https://politie.nl/checkyourhack

Market takedown in April.

2 months later, Genesis Market has been sold, (inc. infrastructure & impersonation software).

Likely to see another similar market in the near future.

⬇ **Link to the paper** ⬇