Dmitry goes to Hollywood: Criminal Excellence in (Cyber) La La Land

Preliminary frameworks to characaterize excellence in malware markets & social engineering attacks

Luca Allodi
SECurity group @ Department of Mathematics & Computer Science, TU Eindhoven

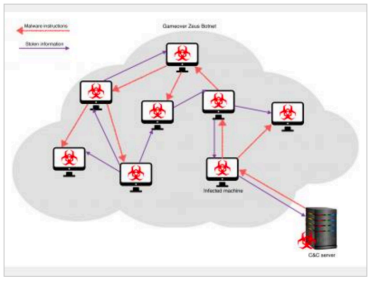
Eindhoven University of Technology

@securescientist

Malware excellence: an example for contrast

Malware in an open "Deep web" marketplace

Vendor	01DigitalDiscount10 (2100) (4.81⭐)
Price	฿0.001234 ($4.16)
Ships to	Worldwide, Worldwide
Ships from	Worldwide
Escrow	Yes



Product description

THIS IS A GUIDE ON HOW TO HACK INTO BANK ACCOUNTS USING THE ZEUS BOT. THIS DOES NOT COME WITH THE BOT

ABOUT ZEUS
Zeus, ZeuS, or Zbot is a Trojan horse malware package that runs on versions of Microsoft Windows. While it can be used to carry out many malicious and criminal tasks, it is often used to steal banking

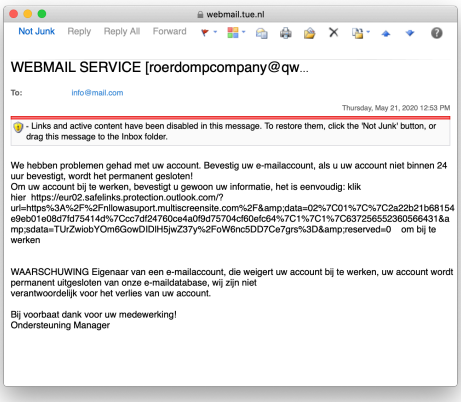
vs

Malware on an "invite-only" forum marketplace

(Here was a screenshot with
A very detailed exploit ad including
Vulnerability characteritistics,
Execution time,
evasion

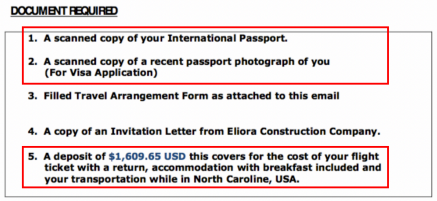
Social Eng. excellence: an example for contrast

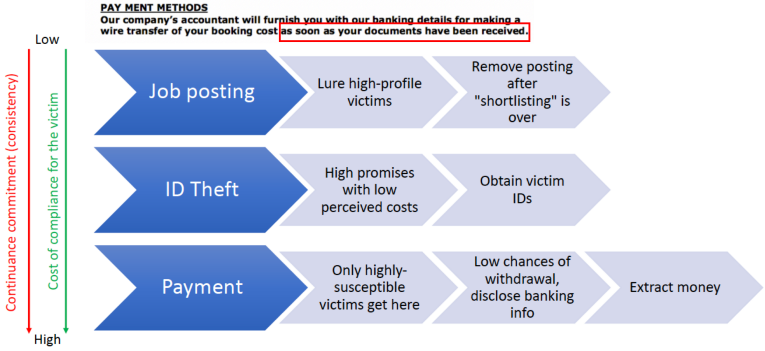
From my spam folder
The classic "webmail problem, click here"



VS

Multi-stage campaign targeting "white-collar" workers on LinkedIn



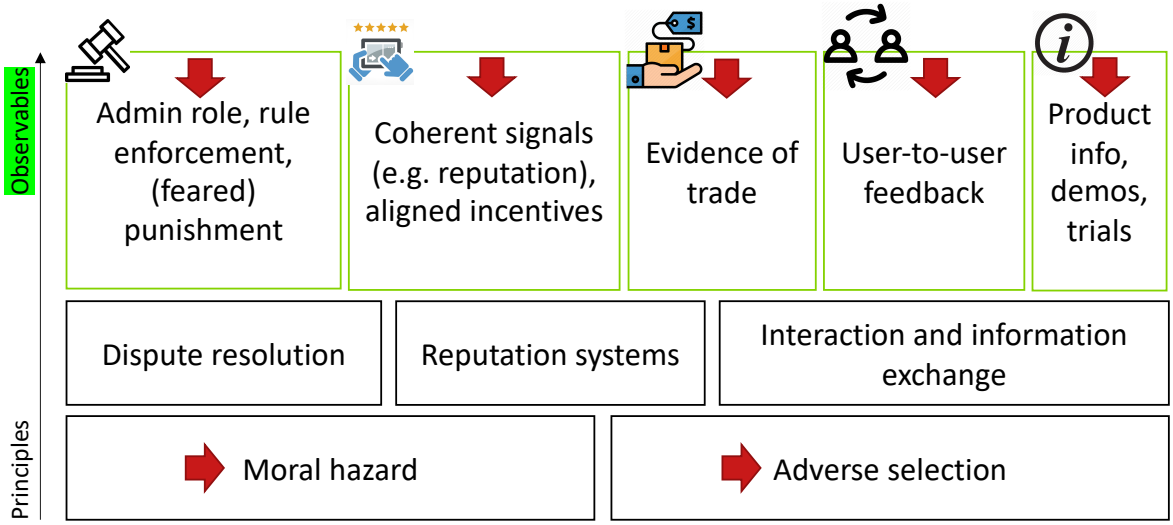


Characterizing excellence in..

Malware criminal endeavours

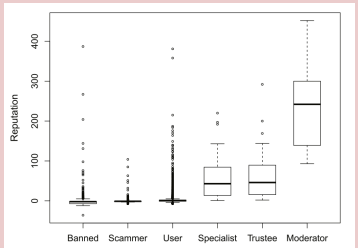
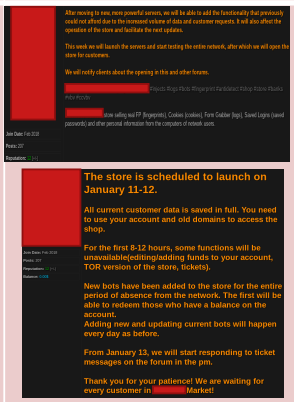
TU/e

Can Dmitry sell his malware kit anywhere?



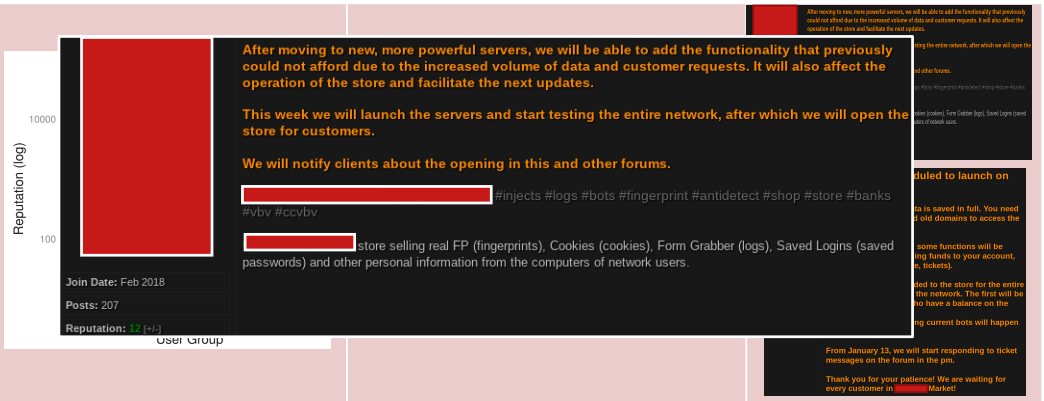
TU/e

Illustrative examples

	Probably not-that-interesting forum market	Probably interesting forum market	Interesting ecrime platform
Coherent signals			

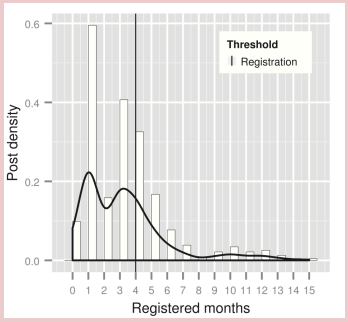
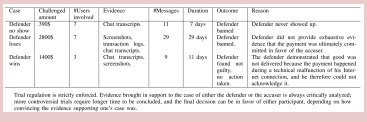
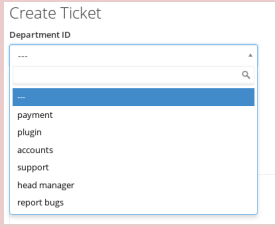
TU/e

Illustrative examples

	Probably not-that-interesting forum market	Probably interesting forum market	Interesting ecrime platform
Coherent signals			

TU/e

Illustrative examples

	Probably not-that-interesting forum market	Probably interesting forum market	Interesting ecrime platform
Rule enforcement	 Rule: access tier 2 after 4 months	 Rule enforcement outcomes	

TU/e

Illustrative examples

	Probably not-that-interesting forum market	Probably interesting forum market	Interesting ecrime platform

Case	Challenged amount	#Users involved	Evidence	#Messages	Duration	Outcome	Reason
Defender no show	390$	7	Chat transcripts	11	7 days	Defender banned	Defender never showed up.
Defender loses	2800$	7	Screenshots, transaction logs, chat transcripts.	29	29 days	Defender banned.	Defender did not provide exhaustive evidence that the payment was ultimately committed in favor of the accuser.
Defender wins	1400$	3	Chat transcripts, screenshots.	9	11 days	Defender found not guilty, no action taken.	The defender demonstrated that good was not delivered because the payment happened during a technical malfunction of his Internet connection, and he therefore could not acknowledge it.

Trial regulation is strictly enforced. Evidence brought in support to the case of either the defender or the accuser is always critically analyzed; more controversial trials require longer time to be concluded, and the final decision can be in favor of either participant, depending on how convincing the evidence supporting one's case was.

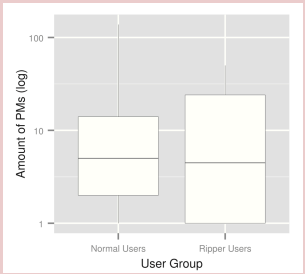
Rule: access tier 2 after 4 months

TU/e

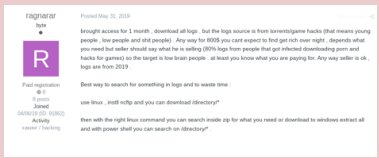
Illustrative examples

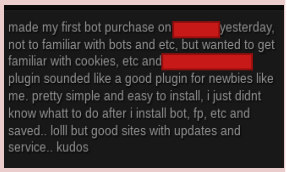
	Probably not-that-interesting forum market	Probably interesting forum market	Interesting ecrime platform

User-to-user feedback & evidence of trade



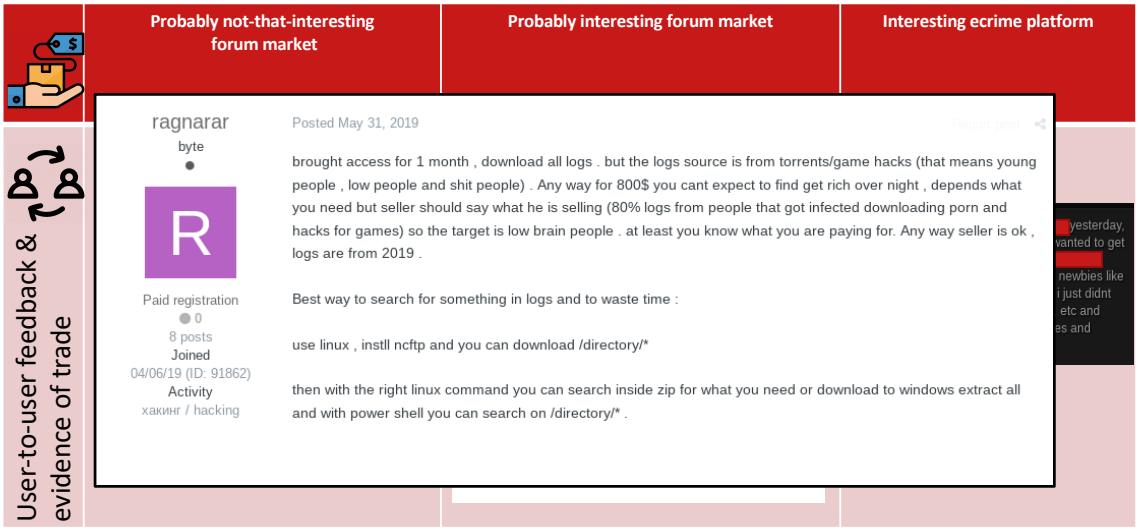
Evidence that participants initiating a trade also often declare to have performed a background check on the seller by either contacting the administrators or by checking the official blacklist of the forum.
e.g., *"[The] admin [of the forum] confirmed me that you [the seller] are not a rookie trader"*.



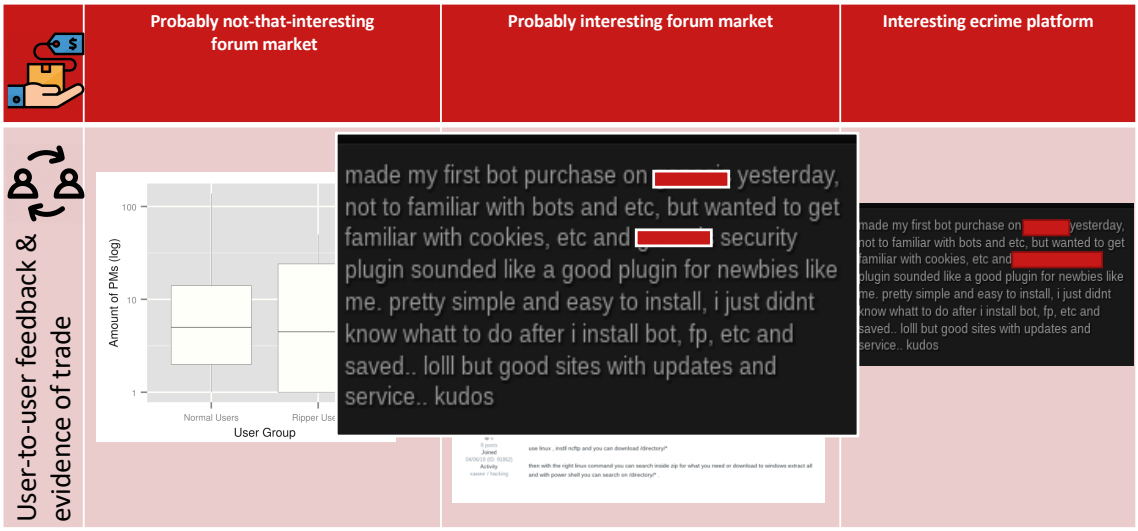


TU/e

Illustrative examples



Illustrative examples



Why all the trouble?

- Usually threat ID comes "after the fact"
  1. Measure activity "in the wild"
  2. Derive corresponding threat model
  3. Identify market/community/criminal initiative that enables it
  4. Take (disruptive) action (sinkhole, jamming, LE actions, ..)

- If we know how to look selectively, we can go the other way around
  - Find the credible "La La Lands" and take selective and pre-emptive action

TU/e

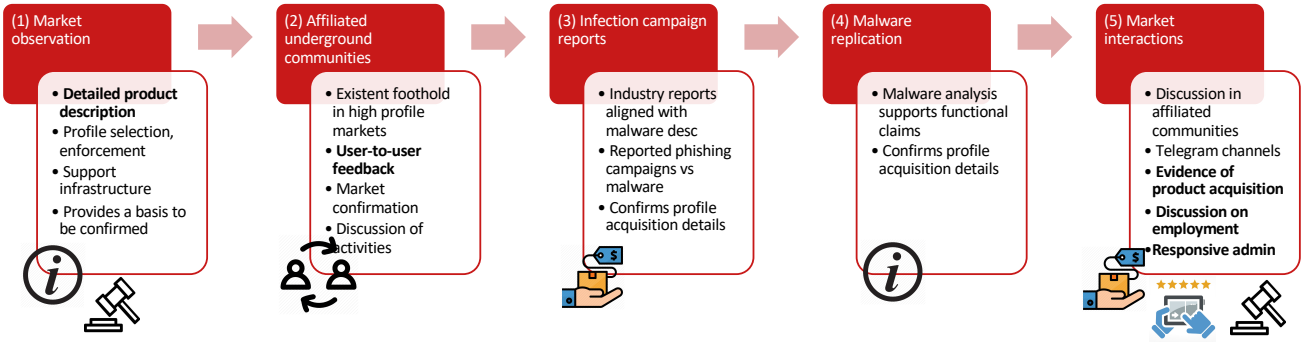
Example of application

- Investigation of the `IMPaaS.ru` criminal platform
- IMPaaS.ru is a Russian **closed access** ecrime platform emerged in Dec'17
  - This platform implements a **new model** to obtain and distribute bundles of **stolen credentials** and **user fingerprints** to cybercriminals
  - Counting 260k+ stolen user profiles at time of infiltration

We infiltrated this market and studied the new threat model that emerges from it

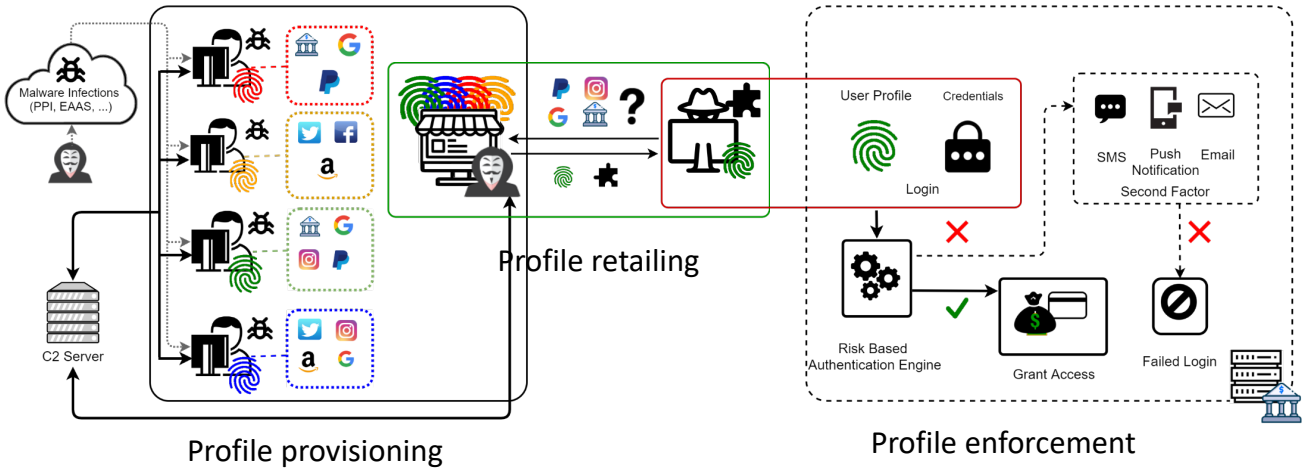
TU/e

Reconstructing attack operations from multiple sources



TU/e

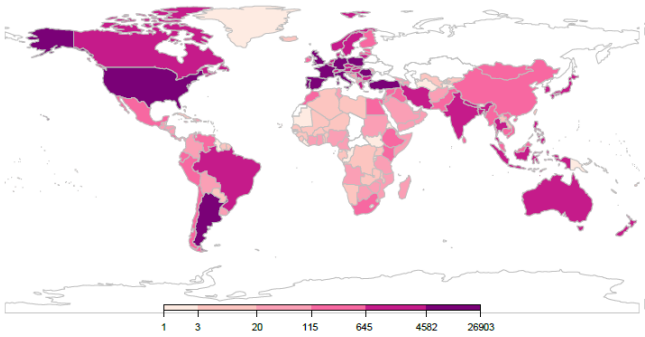
The Impersonation-as-a-Service (IMPaaS) model



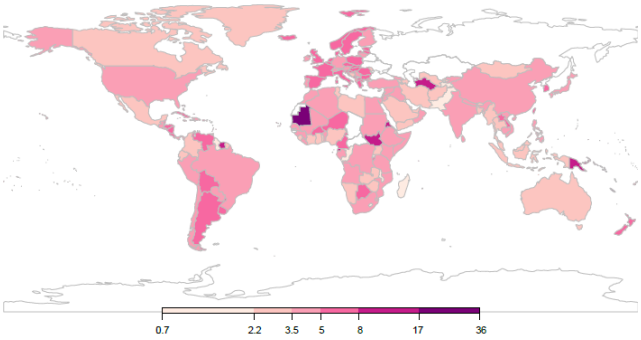
TU/e

Characterizing IMPaaS in the wild – distribution

Amount of profiles available per country



Median price per profile per country in USD

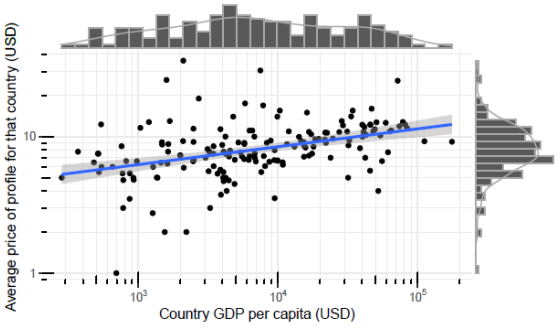


TU/e

Characterizing IMPaaS in the wild – pricing

Moving weekly average price of stolen profiles

Price of profile vs country GDP



Some details:

- Prices range from 0.7 USD to 96 USD
- MNYTRANSF/CRYPTO + 6-10USD over expected price (+150%)
- SOCIAL,SERVICES,COMMERCE not highly valued

Observationally:

- Recent new infra development related to increase in mean price (+15USD)
- pricing structure remained similar.

TU/e