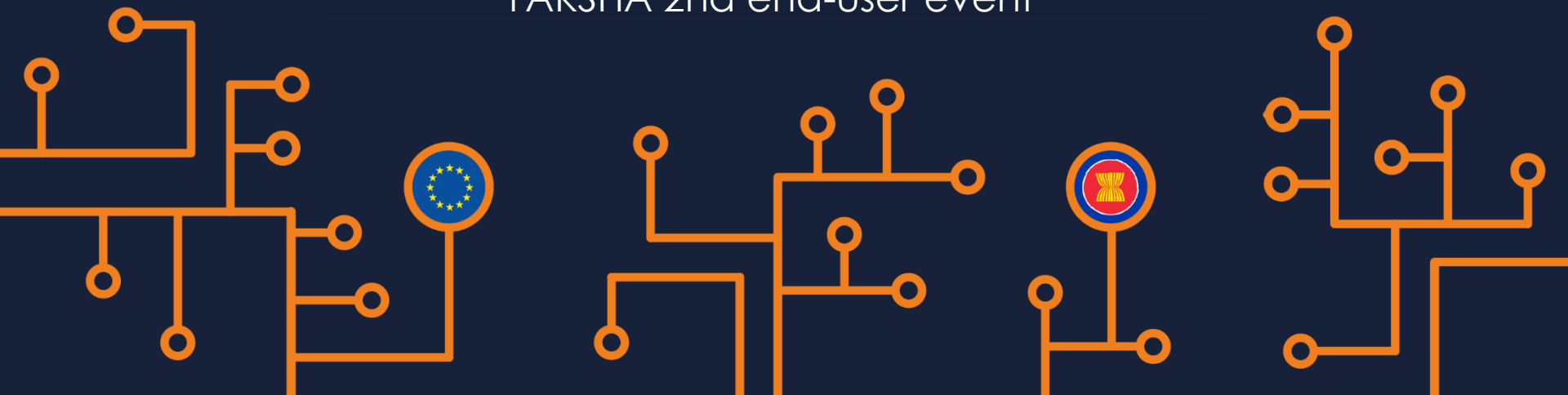
YAKSHA software value proposition

Constantinos Patsakis
Associate Professor
University of Piraeus

YAKSHA 2nd end-user event



Cybersecurity & Cybercrime

- **Quantifying means identifying:** It is easier to understand a problem if you quantify many aspects of the problem

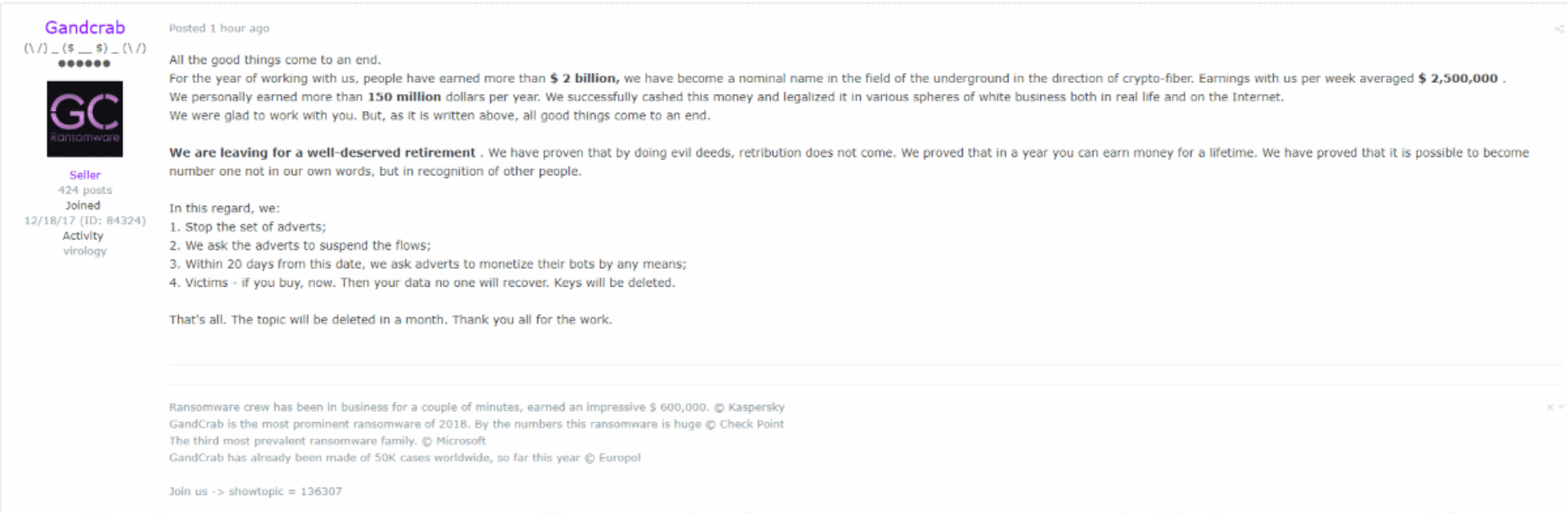
Cybersecurity & Cybercrime

- Its economic impact is devastating [1], with FBI estimating the losses to $3.5 billion only within USA [2]
- The continuous rise is so threatening that it has become the second most-concerning risk for global commerce over the next decade, according to the World Economic Forum [3]
- The recent COVID-19 pandemic resulted in a huge spike in cybercrime activities

Cybersecurity: You vs XXX?

- Individual hackers
- Hacker groups
- Industrial/corporate espionage
- Nation state actors

Cybersecurity: You vs XXX?



Gandcrab
(\ /) _ ($ __ $) _ (\ /)

Seller
424 posts
Joined
12/18/17 (ID: 84324)
Activity
virology

Posted 1 hour ago

All the good things come to an end.
For the year of working with us, people have earned more than **$ 2 billion,** we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **$ 2,500,000** .
We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.
We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:
1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

Ransomware crew has been in business for a couple of minutes, earned an impressive $ 600,000. © Kaspersky
GandCrab is the most prominent ransomware of 2018. By the numbers this ransomware is huge © Check Point
The third most prevalent ransomware family. © Microsoft
GandCrab has already been made of 50K cases worldwide, so far this year © Europol

Join us -> showtopic = 136307

Cybersecurity: You vs XXX?

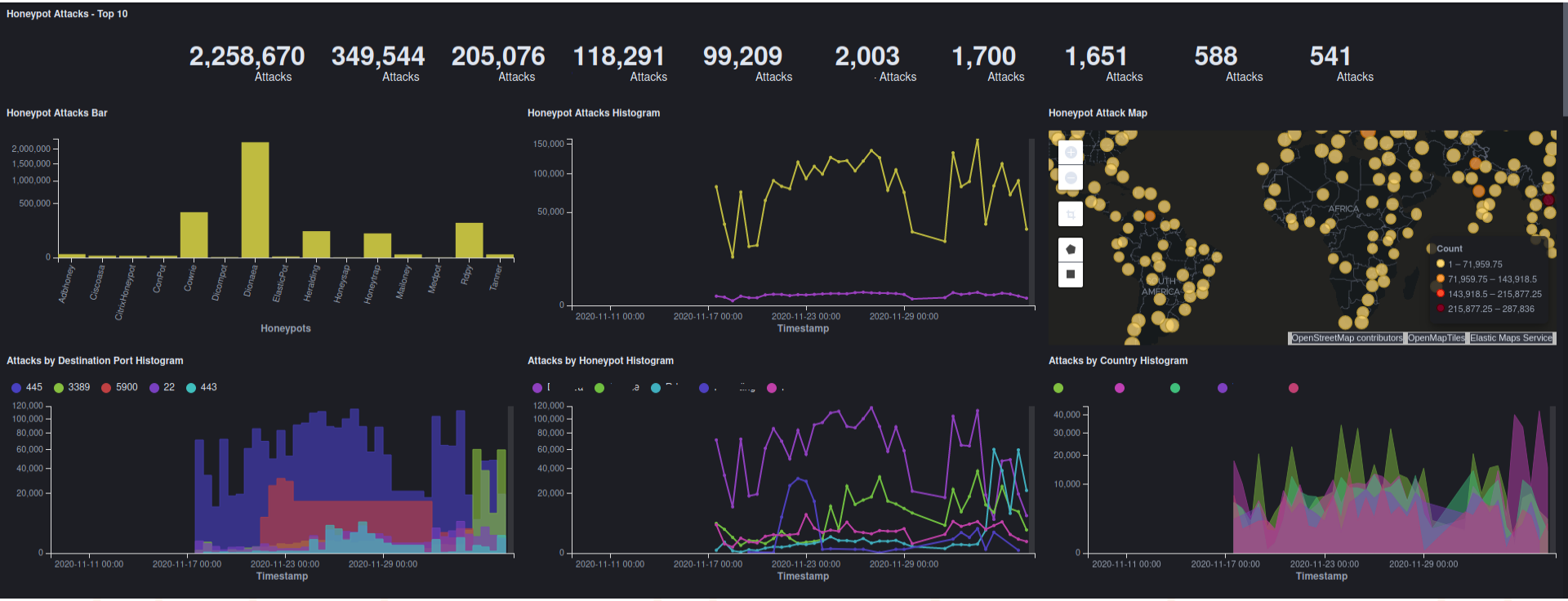
- It's you vs a multi-billion underground economy.

YAKSHA

What are the market tools doing?

- **Firawall:** Block incoming/outgoing traffic
- **Vulnerability assessment tools:** Which are my weak points?
- **Antivirus:** Is there any malware installed in my clients?
- **Honeypot:** How does an attacker act?
- **Threat intelligence:** What are the adversaries doing right now?
- **Sandbox:** What this binary do?

The insight from a honeypot in UPRC



Too much information

- What should I understand from this?
- Too much noise

What about me?

I want to know/assess:

- Which are **my** **weak points** that an adversary would target.
- How an attacker would act in one of **my** **systems**.
- The lateral movement in **my** **premises**.
- What an adversary would do to **my** **systems** now.
- The impact of the adversary's toolkits on **my** **system**

YAKSHA

How should the above be offered?

- In a secure isolated environment
- Automatic deployment and instantiation
- Replication of my infrastructure/systems
- Automated analysis
- Full log access

What about YAKSHA?

- YAKSHA offers the above as a custom honeypot environment which is hosted in an isolated environment, offering real-time overview of what the adversary would do in your system.
- It is a cyber-deception tool to monitor your adversaries

Customising YAKSHA

- Choose your OS: Windows, Linux, Android
- Choose the services: Install your services remotely
- Monitor your systems and attacks
- Revert to stable state

YAKSHA

Insight from YAKSHA

- I don't care about all hackers, but for the ones who would target my infrastructure.
- Collect their toolkits.
- Create IOCs from the logs before they attack the actual environment.
- Monitor botnets as part of them.

Key benefit of YAKSHA

- **Personalisation:** SMEs, Governmental institutions, and public authorities collect information which is tailored to their needs, their exposure, and their adversaries.

YAKSHA

Unique features

- Selective information and threat intelligence sharing
- Use of machine learning: Identify malicious parts automatically from known features.
- Clustering: Identify the binaries you have to study and don't waste time in reviewing many samples to assess their capabilities and your exposure

Thanks for your attendance

Questions?

Constantinos Patsakis
kpatsak@unipi.gr

References

[1] D. Thomas: Cybercrime Losses: An Examination of US Manufacturing and the Total Economy, NIST, 2020

[2] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3): Internet Crime report, 2019

[3] World Economic Forum: Wild Wide Web Consequences of Digital Fragmentation, 2020

[4] https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

[5] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19