itsme

**Cyber Security Operations
The Frontline of Digital Protection**

# Evolution on Cyber Attacks and Consumer Fraud
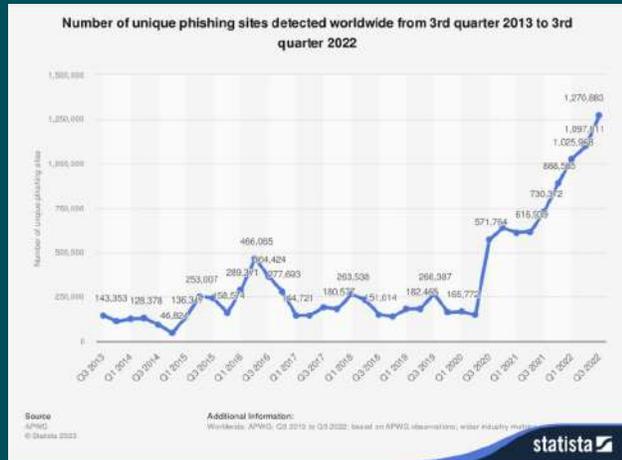
- Dwell time has remained stable ~270 days
- Cycle time has gone down from 270 days to < 10 days in 2024
- Avg time from CVE disclosure to exploit <48h (impact AI!)
- Steep increase in consumer fraud

Security Operations is not an option anymore

- APT's are scanning everybody, not just big organizations and governments
- Vulnerabilities are discovered much faster and in higher numbers
- Attacks become more sophisticated and stealthy (LOTL! – example Spider since mid 2023)
- Thousands of cyber attacks per day
- A proactive approach has become mandatory (note use of CTI in new version ISO27k!)
- MITRE, NIST CSF, CCB provide frameworks
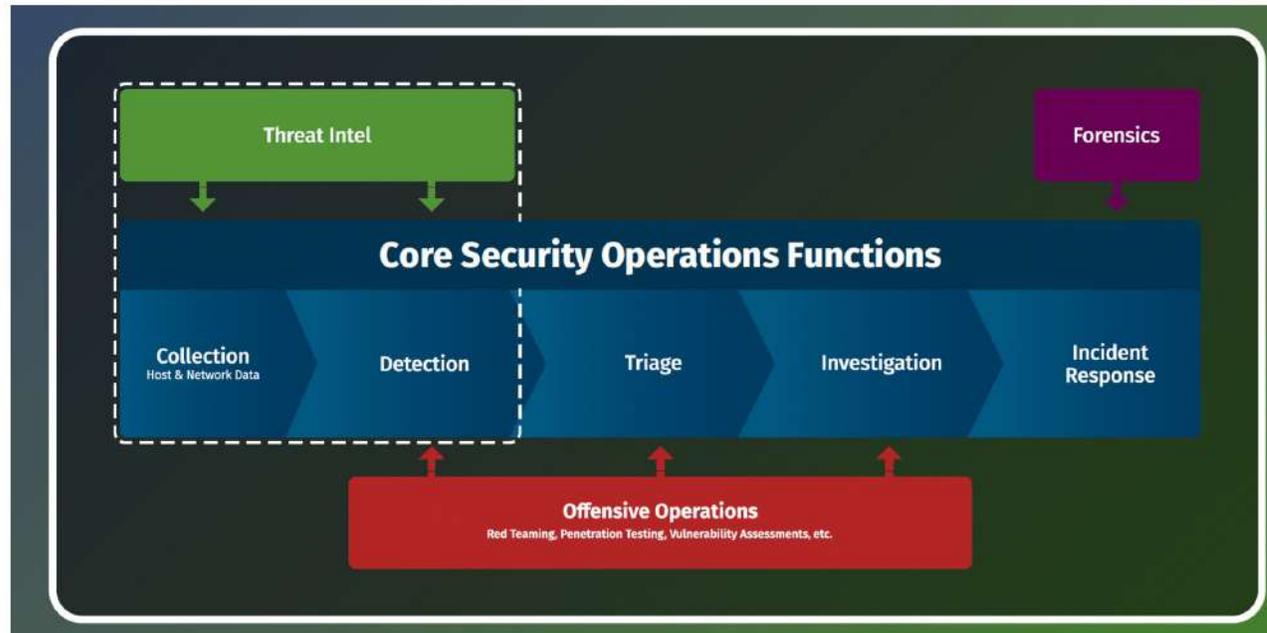
Knowledge landscape becomes gigantic

Operational models

In house   Hybrid   Outsourced
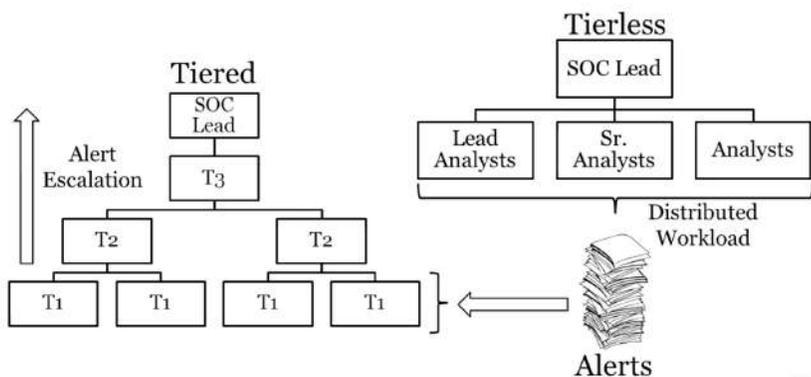
MSSP

Users/Endpoints	Common Solution
0 - 1.000	MSSP + non-dedicated internal security team
1.000 – 10.000	MSSP Hybrid with some functions in-house
10.000 – 100.000	Full internal SOC with possible outsourcing of specialty functions
100.000+	Full-fledged internal SOC with auxiliary/specialty services

Public Private collaboration to strengthen our cyber resilience

- Collaboration with regulators, law enforcements, national security agencies leverages on the different expertise and capabilities of each
- Examples: Cyber Security Coalition, AUSTRAC , GASA, ...
- CCB Cyber Fundamentals, BAPS, Safe On Web

Some examples from itsme® collaboration

- Phishing
- Risk Warning System

Phishing as a service as one of the main drivers

- ~70% of worldwide phishing campaigns are using the UAdmin phishing kit
- The creator sold his kit via TOR and added bank templates and automated features in 2019 making it very easy to use for non-technical criminals
- Criminals are now renting phishing kit and SMS gateways via Telegram as a service, per day/week/month making it even more easy
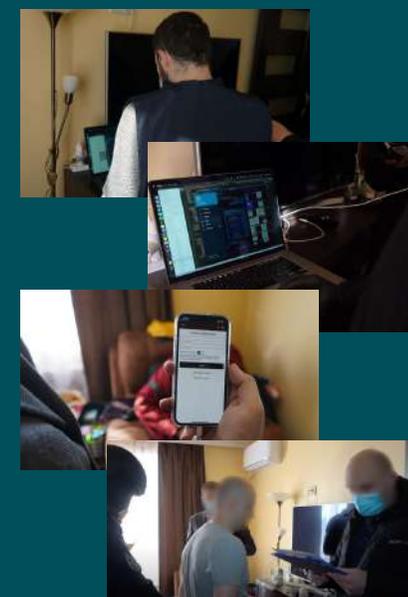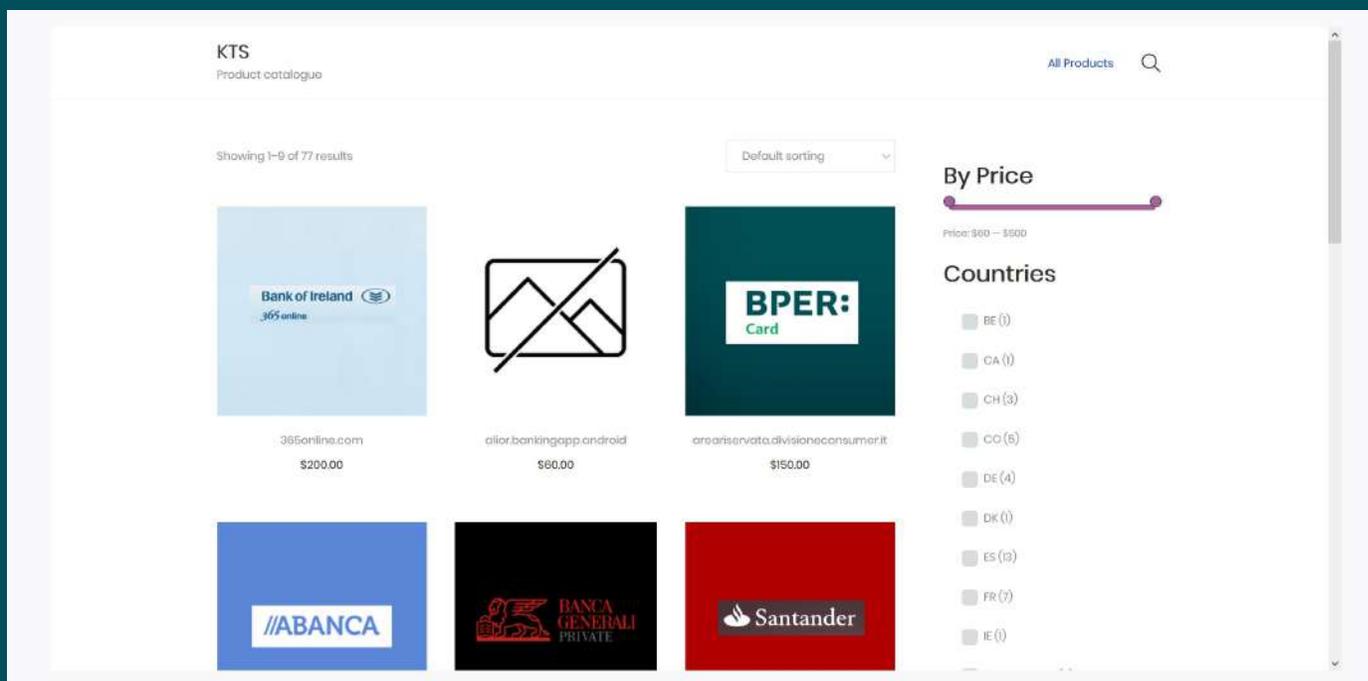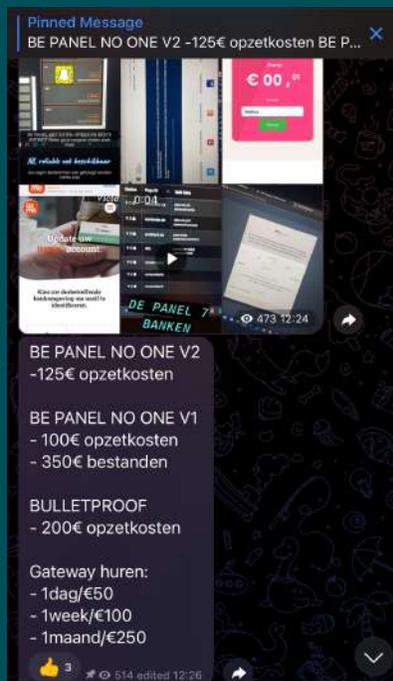
Support in Phishing Scenario

Attacker

Phishing message

Victim

Phishing website

Proxy

Phishing Panel

itsme® SOC

Telco's/banks

Telco's

DNS blacklist

CENTRE FOR **CYBER SECURITY** BELGIUM

WAARSCHUWING – KWAADAARDIGE WEBSITE
De website die u wou bezoeken is onveilig.

AVERTISSEMENT – SITE INTERNET MALVEILLANT
Le site internet que vous souhaitez visiter est dangereux.

WARNUNG – BÖSARTIGE WEBSITE
Die Website, die Sie besuchen wollen, ist nicht sicher.

WARNING – MALICIOUS WEBSITE
The website you want to visit is not safe.

- National phishing detection (directly, via telco smishing detection or banking fraud detection)
- Tracing of attacker infrastructure using vulnerabilities of the phishing kit
- Geolocation of used mobile devices via telco's
- Forensic report to Law Enforcement and Dept Justice (within 10 min of detection)
- Threat Intel & Technical Support for Cyber Crime Units
- Take down of attacker infrastructure (on average within 50 min)
- Live feed to Belgian Anti Phishing Shield (BAPS) warning citizens about malicious websites

New initiative: Risk Warning System

- Objective:
    - National Threat Intel system with indicators for consumer fraud (e.g. MSISDN's/IMEI's used for Smishing, IBAN's of mule accounts)
    - Fast(er) notification and blocking of consumer fraud
- Key stakeholders:
    - National Centre for Cybersecurity (CCB)
    - Belgian Police
    - Banks
    - Telco's
    - Digital ID infrastructure (itsme®)
    - Telco regulator (BIPT)
    - Bank regulator (FSMA)
    - FOD Economie
    - DNS Belgium

Collaboration is key

"It takes a network to fight a network"

Thank you

Remy Knecht
Chief Security Officer
remy.knecht@itsme-id.com

Curriculum lead Security Operations
Solvay Executive Master in Cybersecurity

Financial Action Task Force
Industry Expert AML/CTF
Co-author Guidance on Digital Identity

Founder
Consulting for EU Commission
- Digital Identity
- Cybersecurity

EU CyberNet
Expert Cyber Defense & Intelligence

Advisor

Advisor on Digital Identity Eco-Systems
Co-creator toolkit for governments

CSIRT Focus Group