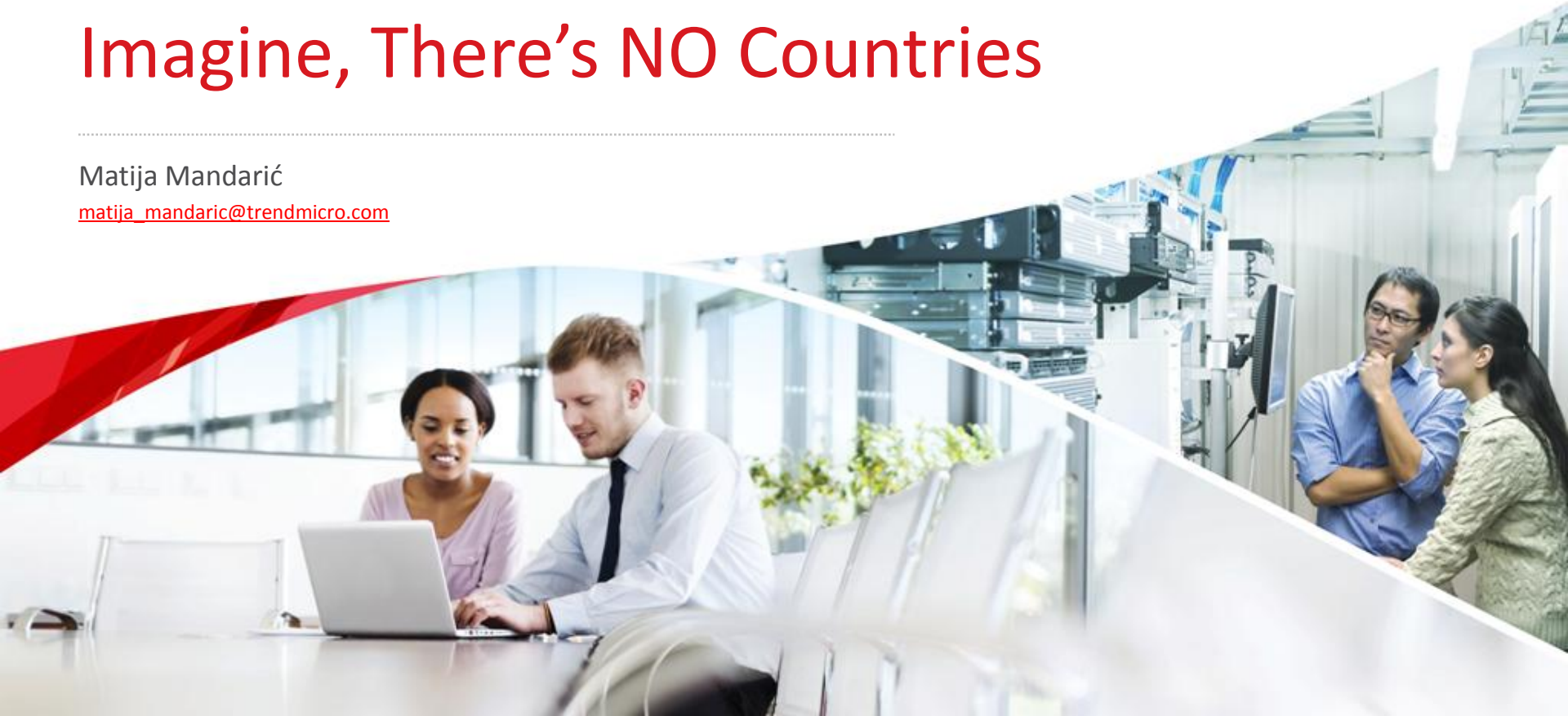
Imagine, There’s NO Countries

Matija Mandarić
matija_mandaric@trendmicro.com



Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

2. Send your Bitcoin wallet ID and personal installation key to e-mail
Your personal installation key:

If you already purchased your key, please enter it below.
Key: _

Jun 2017.

- 27.06.2017. server za nadogradnje Ukrajinskog knjigovodstvenog softvera M.E. Doc šalje kompromitovani update svim korisnicima;
- Unutar manje od 4h, nova varijanta naizgled postojećeg malwarea zahvaća:
  - 4 bolnice;
  - 22 banke;
  - 2 aerodroma;
  - Mrežu card procesora i bankomata;
  - Elektroprivredu i povezane kompanije.

Rezultat?

- Preko 300 zaraženih firmi;
- 10% svih računara u državi onesposobljeno;
- Povratak u kameno doba:
  - Bankomati ne rade, kao ni POS terminali
  - Ne postoje zapisi unutar firmi, bazi
  - Gubitak podataka u državnim institucijama

Daleko je Ukrajina

NotPetya se nekontrolirano širi u firme izvan Ukrajine:

- VPN, predstavništva međunarodnih firmi;
- Uz spomenute tu su još Saint-Gobain, Beiersdorf, Mondelez i mnoge druge;
- Ukupna šteta se procenjuje na **10 mlrd USD**

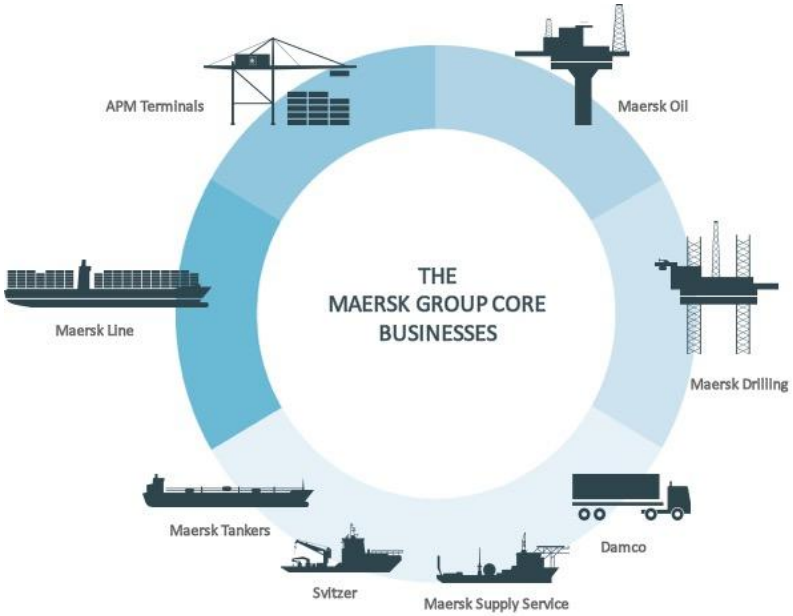
Po prvi put nakon dugog niza godina pojavio se destruktivni malware.

Maersk

- 800 brodova, 76 teretnih luka pod upravljanjem, 574 office-a u 130 država;
- 80000 računara;

27.6.2017.

- 150 DC-a, 1 preživio infekciju (offline radi gubitka struje u Ghani);
- 2 nedelje za osnovni oporavak;
- 2 meseca za potpuni oporavak mreže;
- Procena štete 300 mil USD (trošak sanacije, pravni troškovi, penali, izgubljen promet).



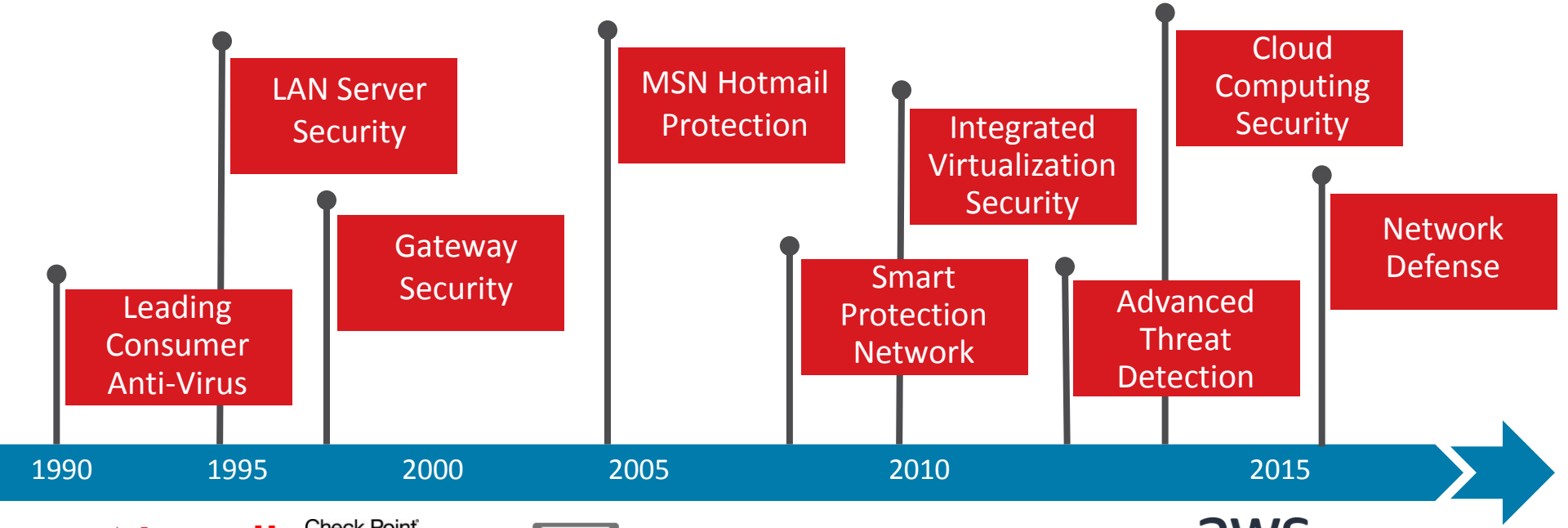
Pogled ”ispod haube”

- Čisti “network exploit” preko SMB protokola
- Ethernal Blue u kombinaciji sa Mimikatz
- NIJE 0-day
- Korisnik nema uticaja na infekciju
- Very unfocused and unpredictable spreading
- Technically - Same “virus” as 15 years ago
- Destructive purpose

Lesson learned – ne postoji sigurna okolina

- U dobi cyber ratovanja granice ne postoje
- Pravovremena primena zakrpi i uopšte patch management su krucijalni za smanjivanje opsega potencijalne štete;
  - Tehnologija tzv. virtualnih zakrpi je podjednako primjenjivo rešenje za sve sisteme koje je nemoguće ažurirati ili postoji rizik od zaustavljanja poslovnog/proizvodnog procesa;
- Korišćenje Multi Factor Autentikacije gde god to procesi dopuštaju, username i password je homeopatsko/placebo delovanje;
- Kontrola porta 445 (SMB group policy management), tj. mrežna segmentacija i kontrola CIFS/SMB komunikacije;
- Korišćenje antimalware sistema višestrukih slojeva zaštite (detekcija anomalija aplikacija i procesa, pokušaja neovlašćenog kriptiovanja diska, virtualne zakrpe te visoka stopa detekcije i zaustavljanje malwarea).

30 Years of Innovation



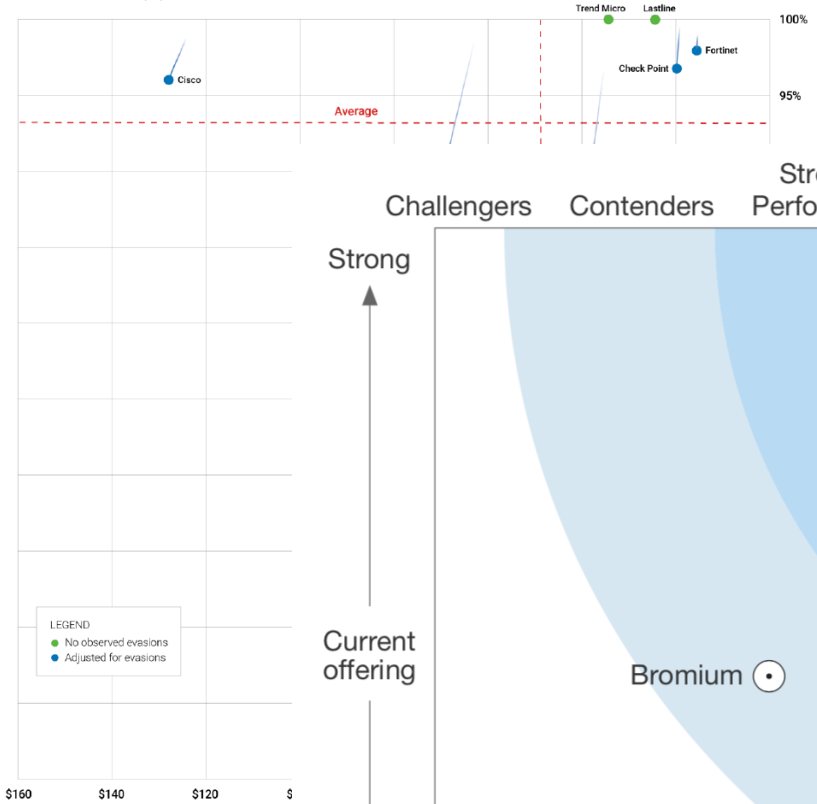
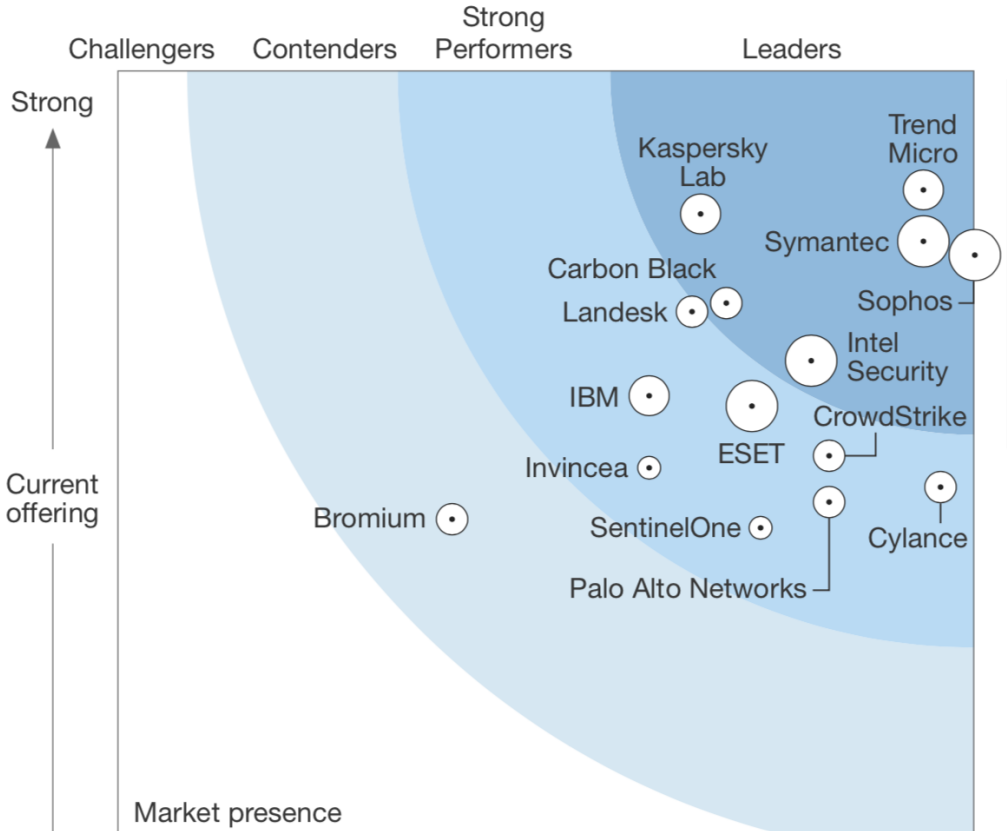
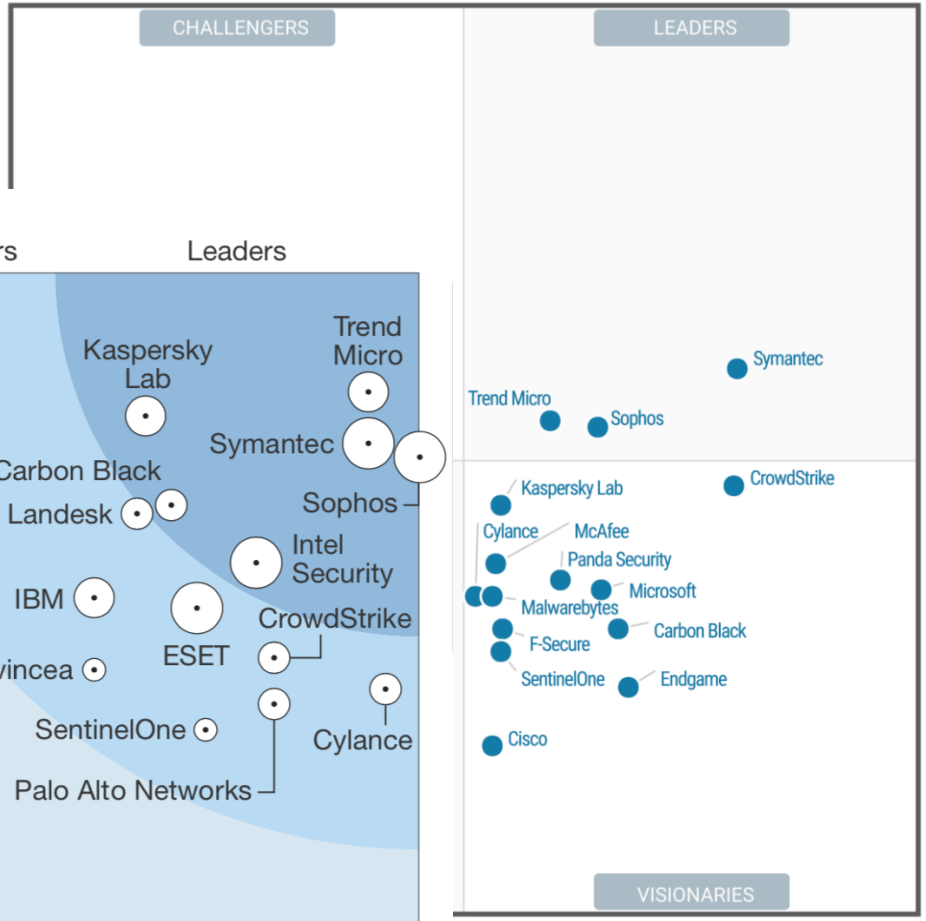


Figure 1 – NSS Labs 2017





As of January 2018 © Gartner, Inc

Market Leadership Position

IDC

The **market leader** in server security for the **7 straight years**

Gartner

Trend Micro delivers **the most cloud security controls (16 of 21)** of all evaluated vendors.

- IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116
- Gartner "Market Guide for Cloud Workload Protection Platforms", Neil MacDonald, March 22, 2017

NSS LABS

Recommended Breach Detection System for **4 straight years**, and **Recommended** Next-generation IPS

Gartner

Leader in Gartner Magic Quadrant for Intrusion Detection and Prevention Systems, January 2018

- NSS Labs Breach Detection Test Results (2014-2017); NSS NGIPS Test Results, 2017
- http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/

Gartner

Highest and Furthest to the Right in the Leader's Quadrant in the Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2017

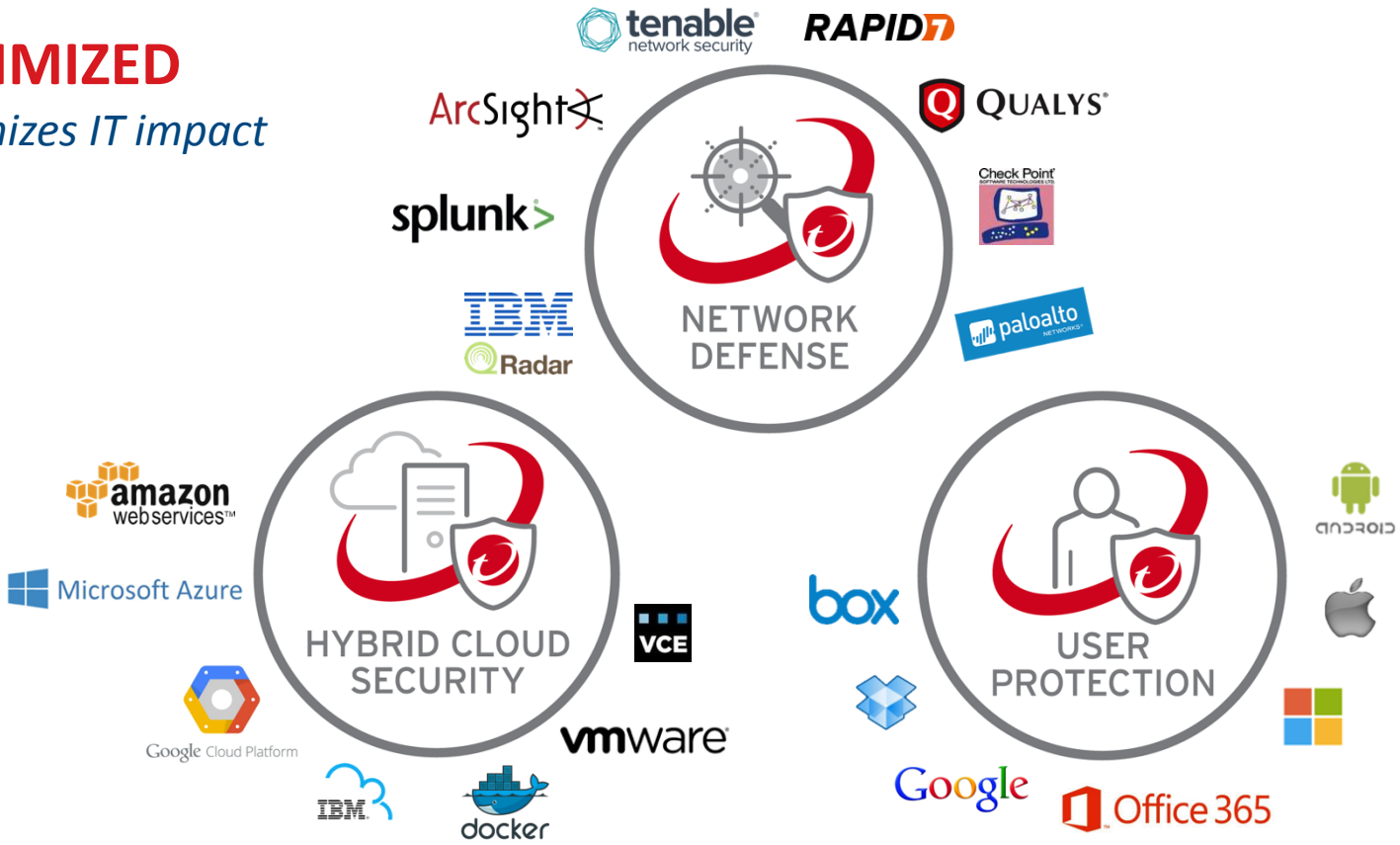
AV-TEST

#1 in protection and performance

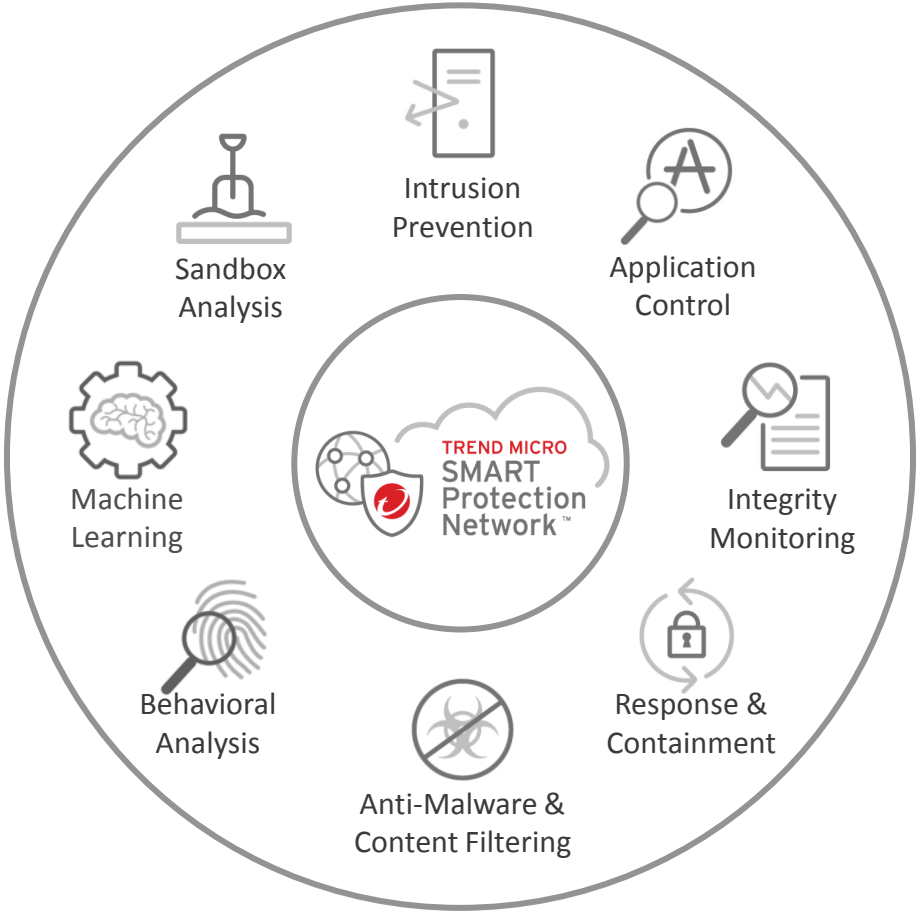
- https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html
- av-test.org (Jan 2014 to Oct 2017)

OPTIMIZED

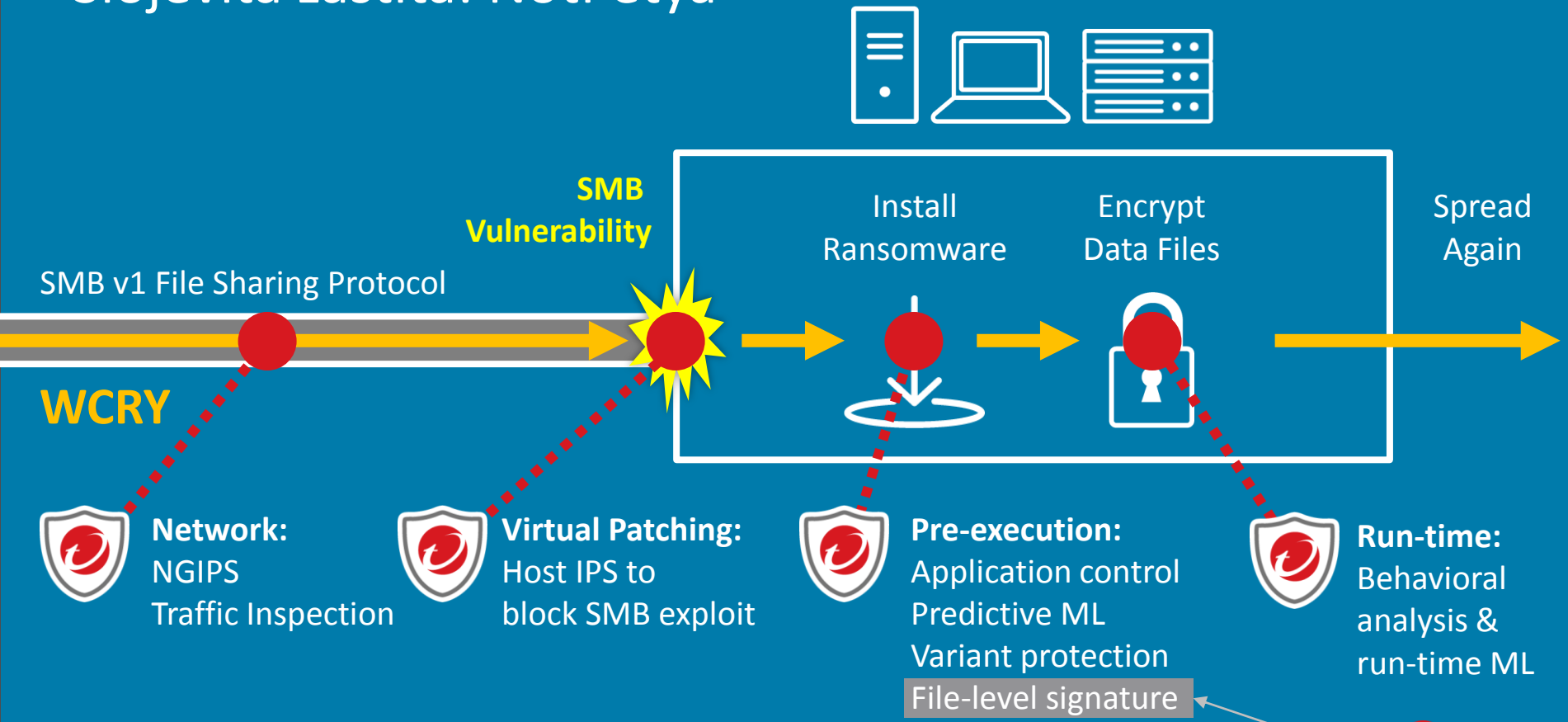
Minimizes IT impact



Slojevita zaštita



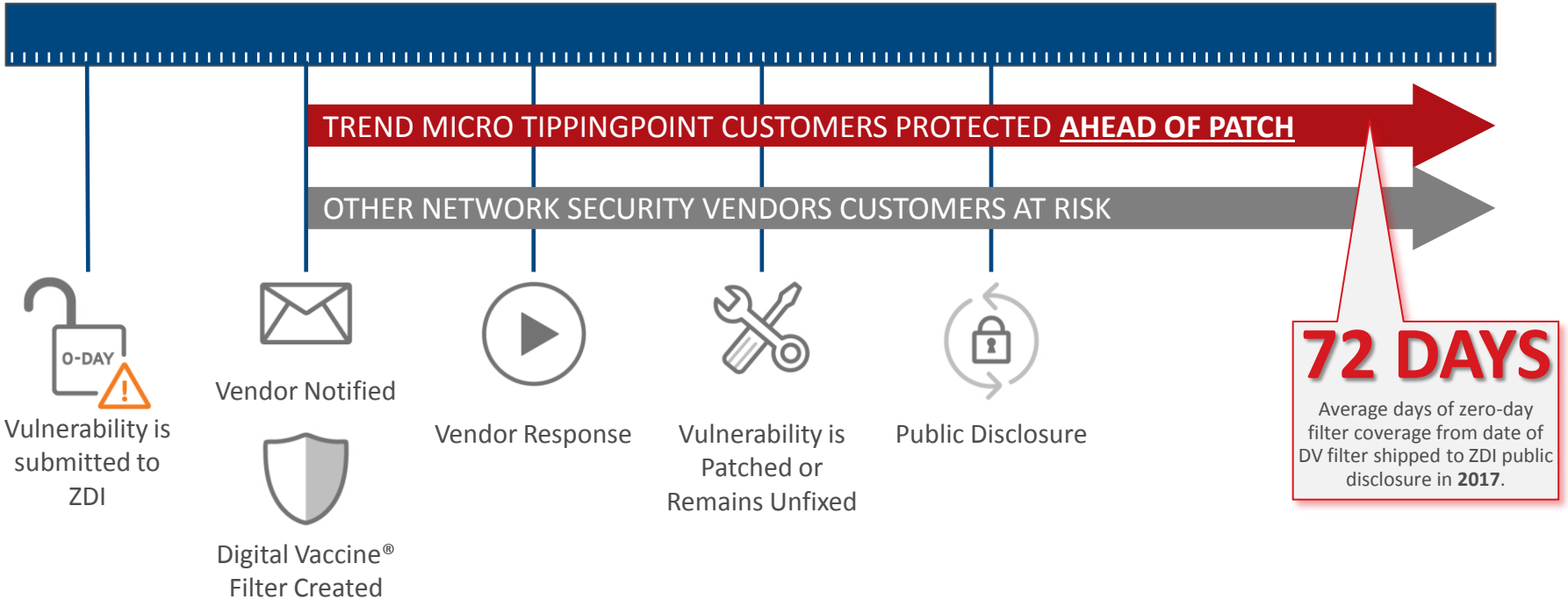
Slojevita zaštita: NotPetya



The Undisclosed: Zero Day Initiative

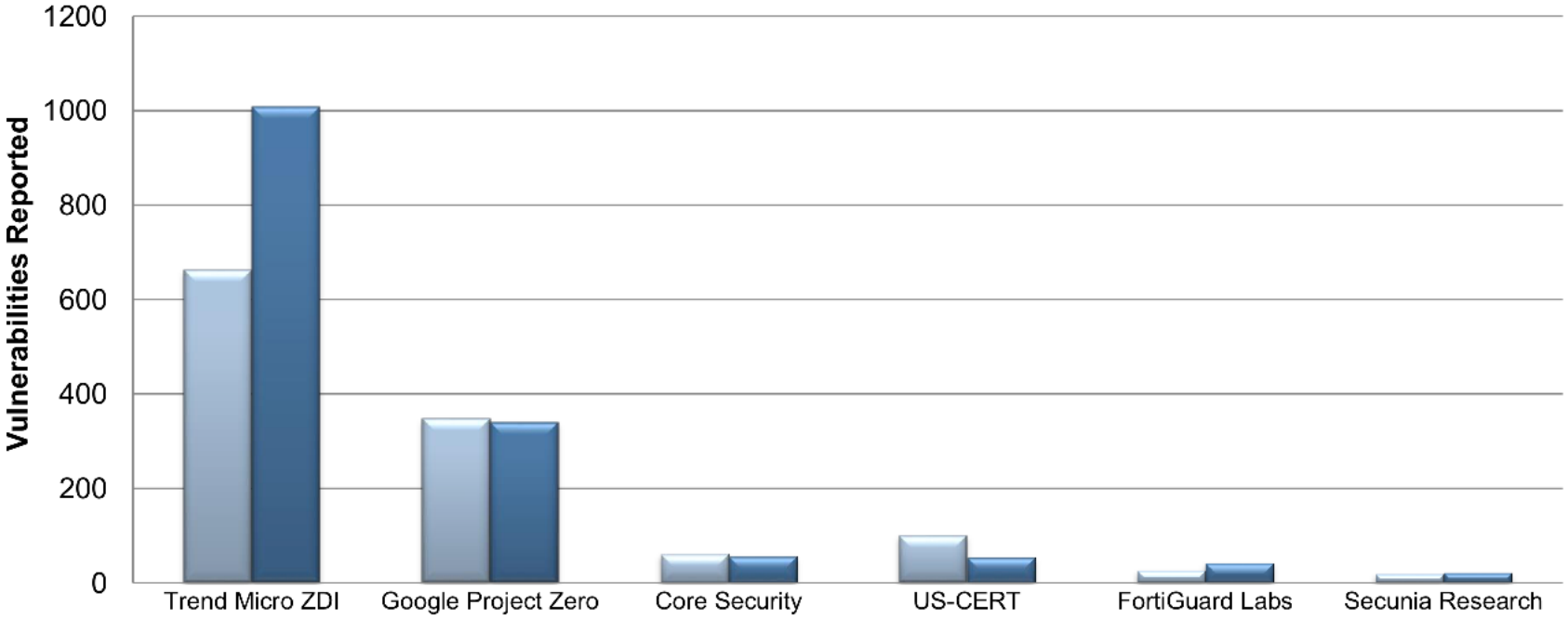
Preemptive Protection for “Undisclosed” Vulnerabilities

ZERO DAY INITIATIVE



TREND MICRO

Public Vulnerability Research Market: Total Vulnerabilities by Disclosing Institutions, Global, 2016 and 2017

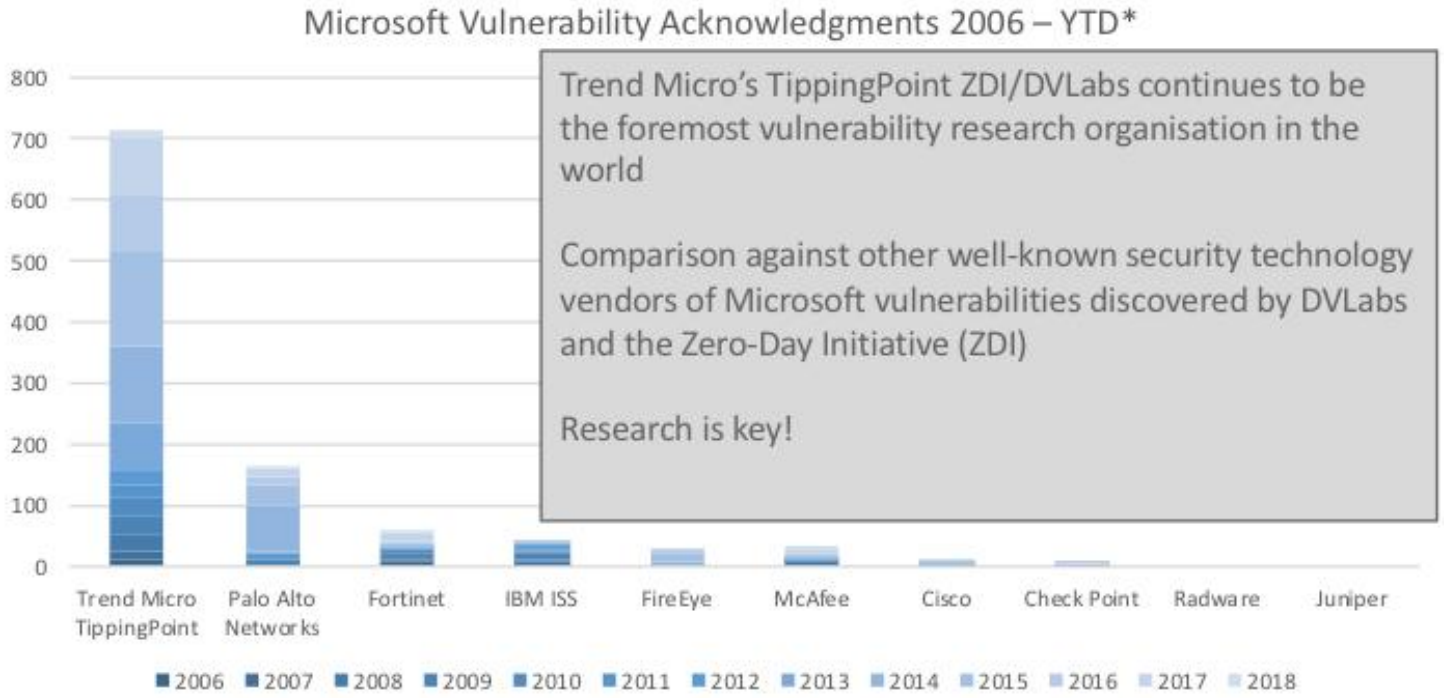


	Trend Micro ZDI	Google Project Zero	Core Security	US-CERT	FortiGuard Labs	Secunia Research
2016	663	348	61	100	26	19
2017	1009	340	56	54	42	21

Disclosing Institutions

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Microsoft Vulnerability discovery 2006-2018



Trend Micro's TippingPoint ZDI/DVLabs continues to be the foremost vulnerability research organisation in the world

Comparison against other well-known security technology vendors of Microsoft vulnerabilities discovered by DVLabs and the Zero-Day Initiative (ZDI)

Research is key!

*From publicly available data at https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Zaštita i sledivost

Performanse

Operativna efikasnost

Cloud i virtualizacija

Poslovni sistemi

Skriveni napadi

Različite tačke kompromitacije (npr. kompromitovani servisi)

Ljudski faktor rizika

Široki spektar napada (email, web, usb, itd)

Ograničena vidljivost

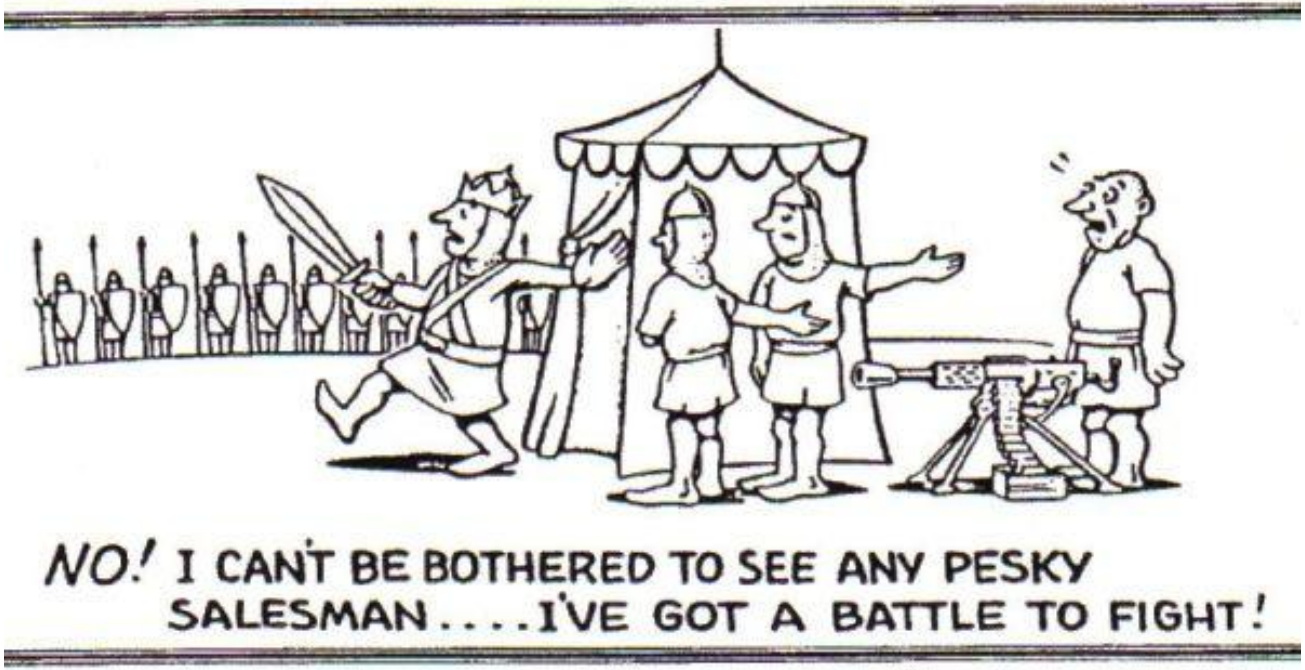
Klijenti

Za one koji žele znati više:

- Trend Micro blog:
  - https://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/
- Wired članak:
  - https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Veracomp blog:
  - https://veracompadria.com/hr/notpetya-ransomware-nastavak-wannacry-price-uz-bitnu-inovaciju/
- Phish Insight, besplatni alat za testiranje znanja vaših korisnika emaila:

  https://phishinsight.trendmicro.com

Don’t work hard, work SMART!



Hvala!

matija_mandaric@trendmicro.com