Check Point
SOFTWARE TECHNOLOGIES LTD

UVEDOMUJTE SI HROZBU VYDIERAČOV, BUĎTE JEDEN KROK PRED NIMI

Tempest
IT makes sense

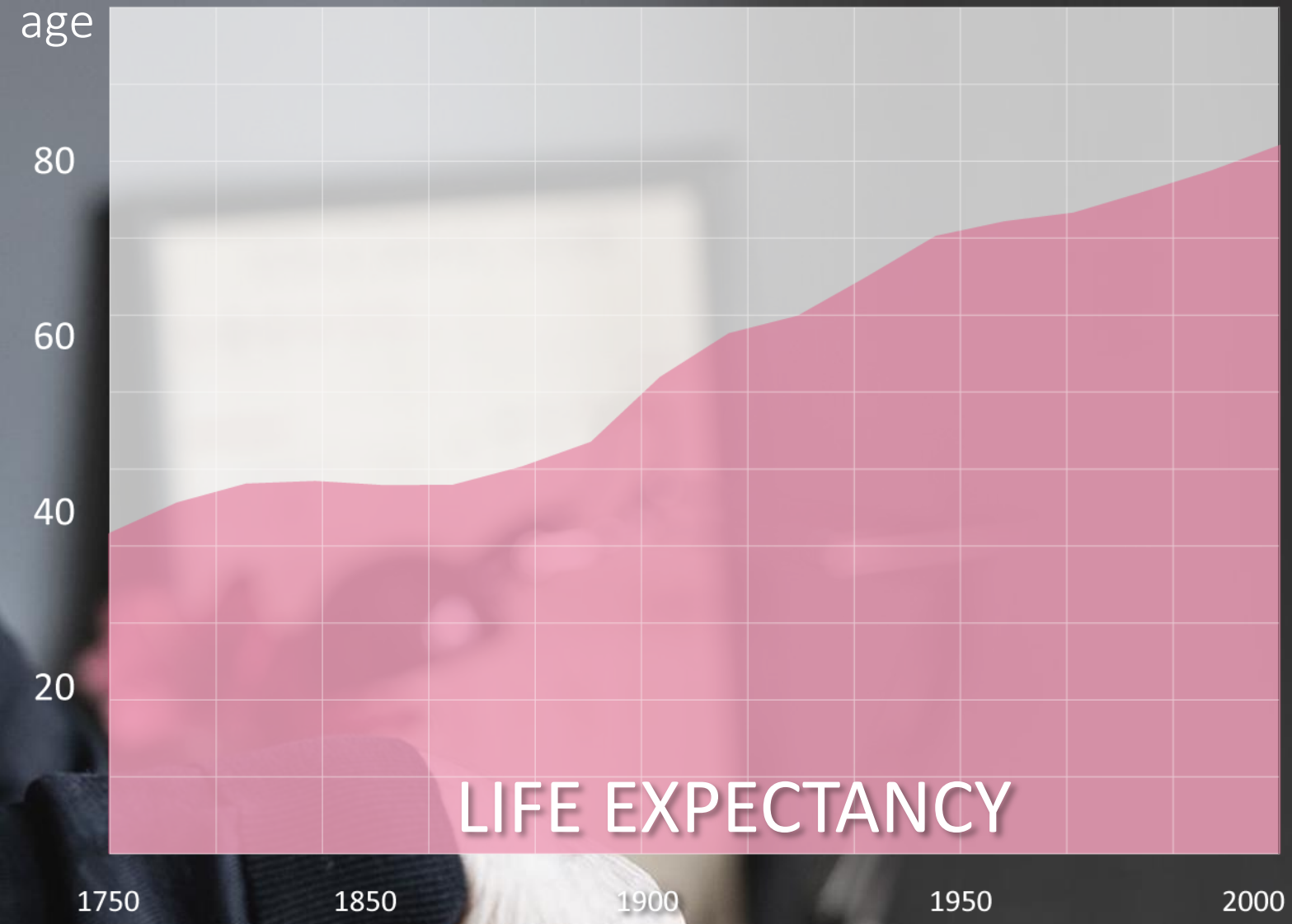
JUDGMENT DAY 12

Peter Kovalčík
SE Manager, Check Point Software Technologies


WE LIVE
IN AN
AMAZING
WORLD

Check Point
SOFTWARE TECHNOLOGIES LTD

WE LIVE LONGER



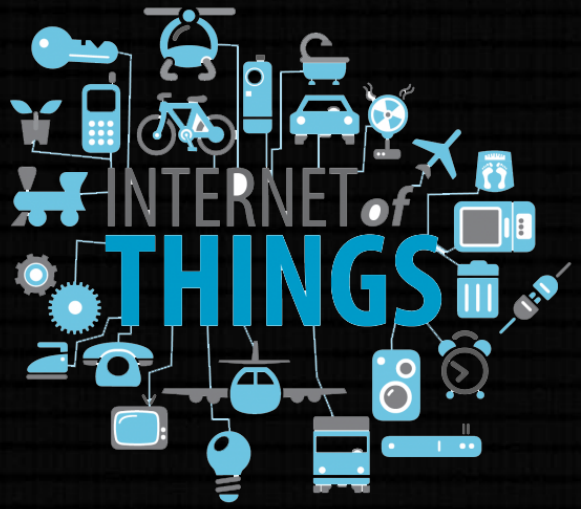
Source: ourworldindata.org

WE GET BETTER EDUCATION

Check Point
SOFTWARE TECHNOLOGIES LTD

OUR LIFE IS MORE COMFORTABLE

Mobile Devices



IOT

Autonomous systems

Check Point
SOFTWARE TECHNOLOGIES LTD

TECHNOLOGY EVOLUTION IS EXPONENTIAL

TAKE **30 LINEAR** PACES…

Check Point
SOFTWARE TECHNOLOGIES LTD

30 Meters

TAKE 30 EXPONENTIAL Steps…

Check Point
SOFTWARE TECHNOLOGIES LTD

26X

Around the Earth!

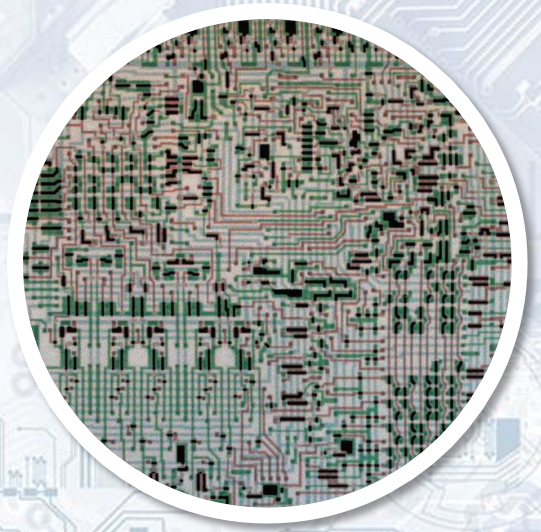
1,073,741,824 Meters

THE FUNDAMENTAL OF EXPONENTIAL TECHNOLOGY

Moore's law

1951

2 Transistors

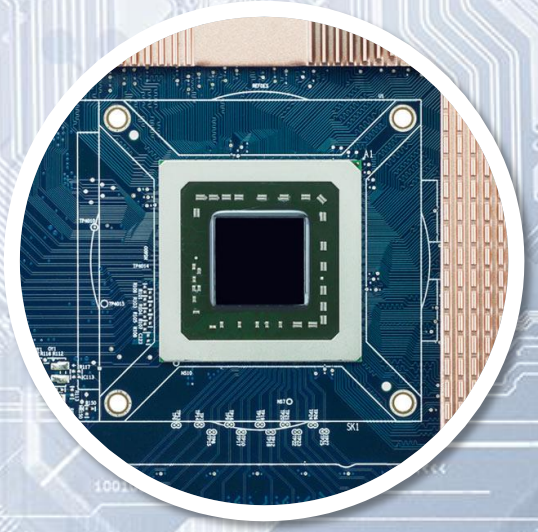


1971

Intel 4004

2300 Transistors

$1



2012

Nvidia GPU

7.1 B Transistors

$0.0000001

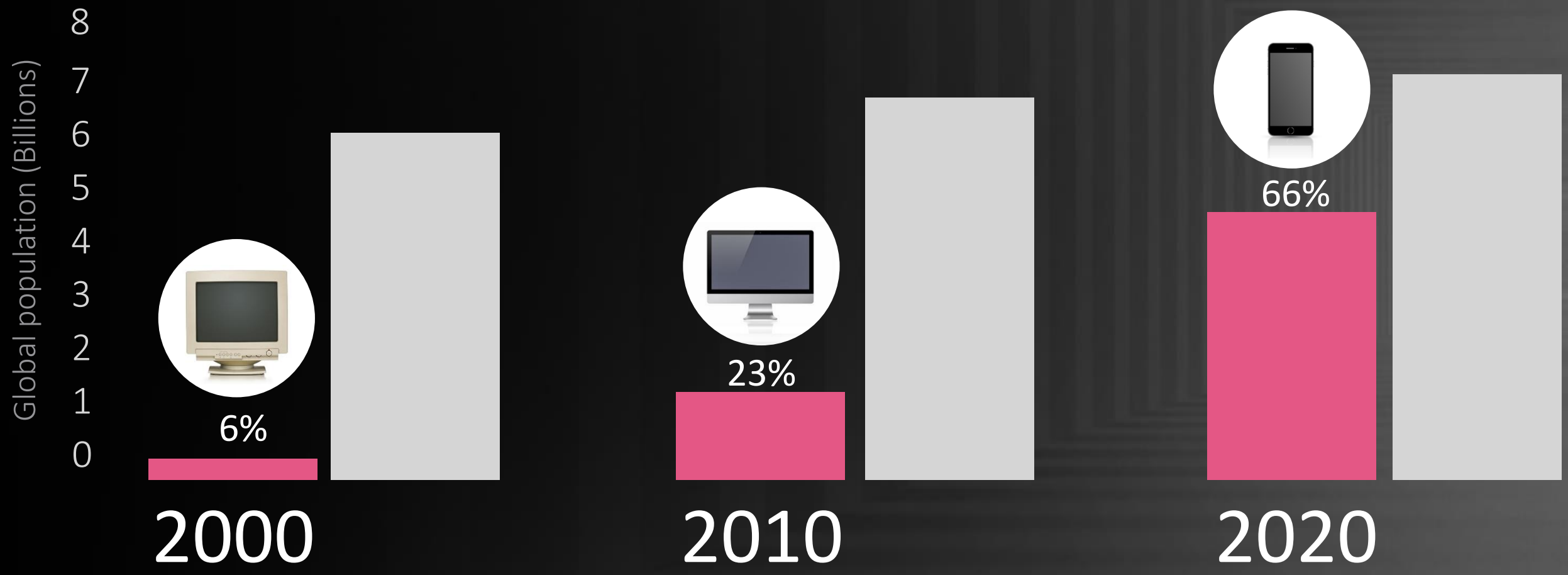
NETWORKED SUPERCOMPUTERS IN OUR POCKET

1 iPhone holds 50,000 of these

THE CONNECTED WORLD
5 BILLION NEW MINDS

Check Point
SOFTWARE TECHNOLOGIES LTD

% world population using internet



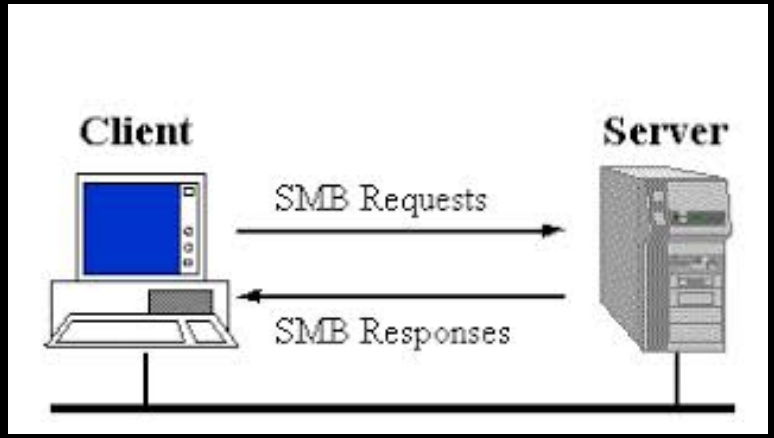
Source: PHD Ventures, Inc.

1 DAY FOR WANNACRY

- More than 150.000 machines infected within single day
- 150 countries affected
- Estimated loss $4 billion USD

Wannacry

- SMB – network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.
- „Weapon-grade“



THE PLAYERS

	CYBER CRIMINALS	STATE SPONSORED CYBER AGENCIES
TARGET	CONSUMERS AND ALL ENTERPRISE Mass infection	CRITICAL INFRASTRUCTURE & LARGE ENTERPRISES Targeted attacks
MOTIVATION	FINANCIAL	POLITICAL
THREATS	UNKNOWN MALWARE	ZERO-DAY
SOPHISTICATION LEVEL	MEDIOCURE	WEAPON GRADE
INVESTMENT	LOW	NATIONAL BUDGETS
EXAMPLES	SAN FRANCISCO MTA, WANNACRY, NOTPETYA, EQUIFAX	UKRAINE POWER GRID, SONY HACK

Monetizácia ?

DoS 2.0 ?

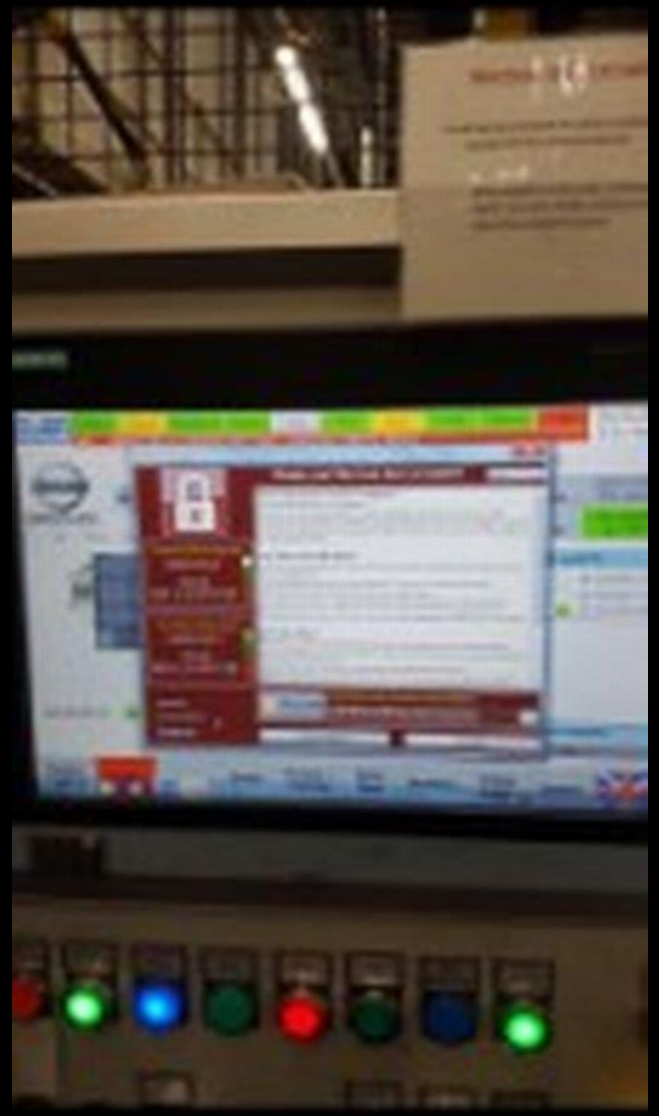
Ransomware

Ransomware

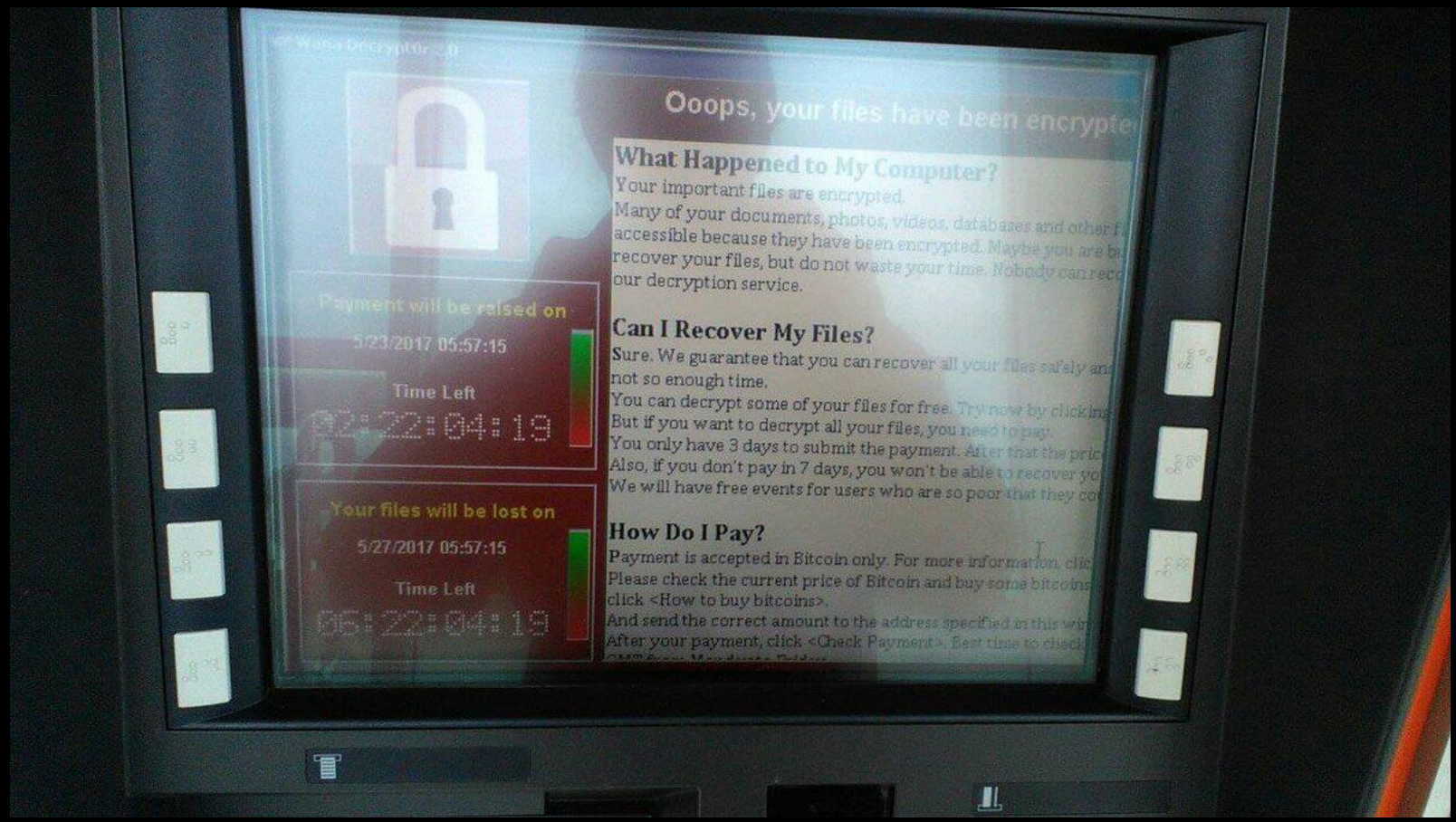

ОЩАДБАНК
терминал тимчасово не працює
терминал временно не работает
temporary out of service
0800 210 800
отримайте
свою картку
безкоштовно
• банк, який вже не ощадить
• близький, зрозумілий та відкрити
• відповідальний та надійний
іністратор

Ransomware

Ransomware



Ransomware


Ooops, your files have been encrypted
What Happened to My Computer?
Your important files are encrypted.
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
5/23/2017 05:57:15
Time Left
02:22:04:19
Your files will be lost on
5/27/2017 05:57:15
Time Left
06:22:04:19

Ransomware


Abfahrt
Linie
Ziel
Zeit
Über
Nach
Gleis
22:10
RB81
Flöha - Pockau-Lengefeld
Olbernhau
8
22:30
RB30
Hohenstein
Hbf
11
22:31
RB30
Flöha - Zsc
(S) Hbf
10
22:36
RB80
g-B. Süd
8
9
2:36
345
Geithain - B
Hbf
5
2:44
6
Einsiedel - Thalheim (Erzgeb)
Aue (Sachs)
14
2:45
Flöha - Freiberg (Sachs) - Tharandt
Dresden Hbf
11
:30
Fährt heute von Gleis 11 -
BMG | MIS

Ransomware

Čo s tým?

PREDCHÁDZAŤ A BLOKOVAŤ !!

PREDCHÁDZAŤ A BLOKOVAŤ !!

Procesy

Technológia

Procesy

- Čo najrýchlejší „Vulnerability patching“ prípadne „virtual patching“
- Nepublikovať SMB do internetu a iné nepotrebné protokoly
- Vysekať (lokálne) privilegované účty na koncových staniciach
- Edukácia užívateľov
- SOC team a reakcia na incidenty, procesy

Technológia

- Blokovať (nie detekovať)
- Segmentácia siete + IPS (primárne internej a DC)
- Chránte koncové body (vektory, protokoly, mobilita)
- Adoptovať nové technológie (Sandboxing, Machine-learning, NG-AV)
- Celková revízia architektury
- Zálohujte

Zhrnutie

- Ransomware = reálna a závažná hrozba „weapon-grade“
- Nie je otázka „či“ ale „kedy“
- Predchádzať a blokovať

„Očakávajte len to najlepšie,
ale budte pripravení na to najhoršie“

Dale Carnegie, spisovateľ a kouč

Tempest
IT makes sense

JUDGMENT DAY 12

Check Point
SOFTWARE TECHNOLOGIES LTD

ĎAKUJEM