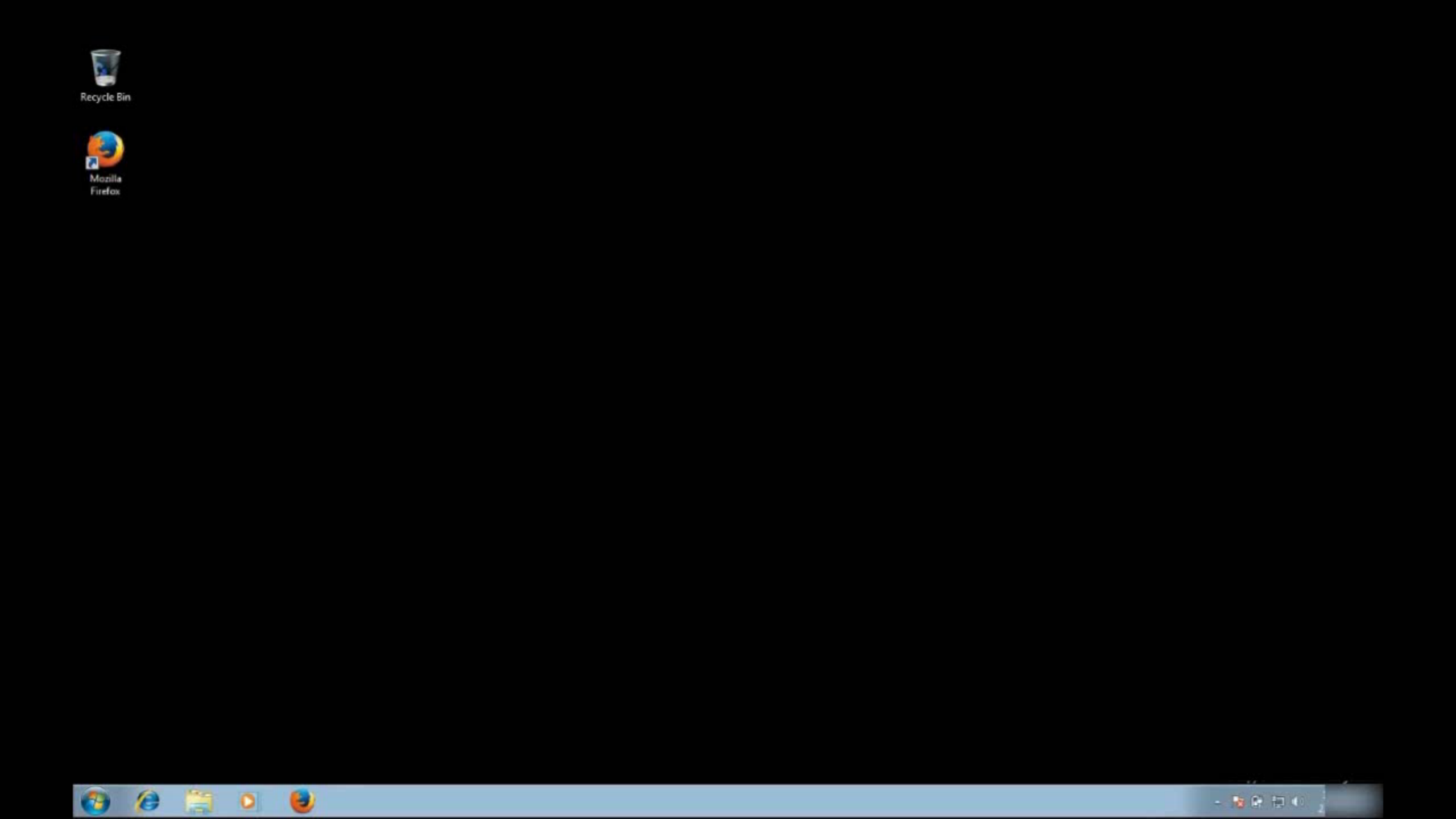
Check Point
SOFTWARE TECHNOLOGIES LTD.

RANSOMWARE:

Evolúcia Zero-Day hrozieb ku kryptografickým útokom

Peter Kovalcik
SE Manager, Check Point

©2016 Check Point Software Technologies Ltd.


Recycle Bin
Mozilla Firefox

Check Point
SOFTWARE TECHNOLOGIES LTD.

CerberRing

An in-depth exposé on Cerber ransomware-as-a-service

Budovanie Ransomware business

Čo potrebujete pre vybudovanie úspešného business:

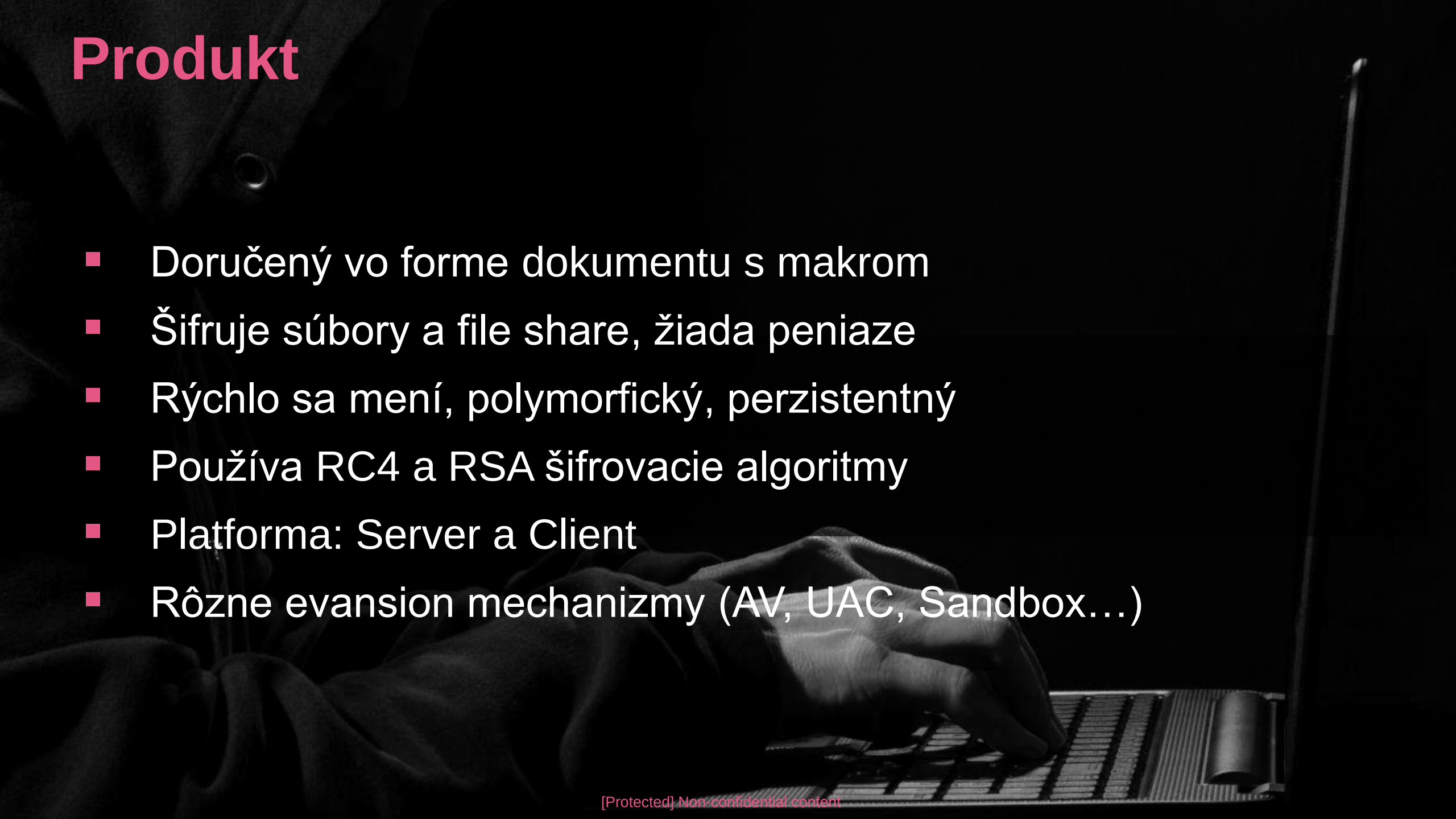
- Produkt
- Business model
- Marketing
- Operations
- Financie

[Protected] Non-confidential content

Cerber Ransomware: Produkt

[Protected] Non-confidential content

Produkt

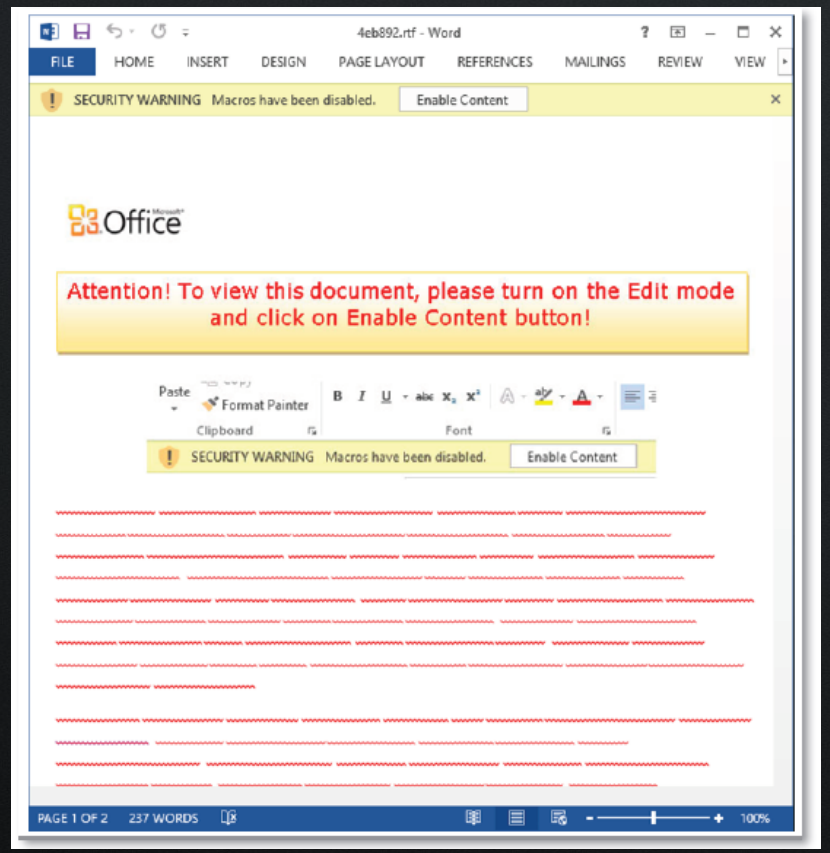


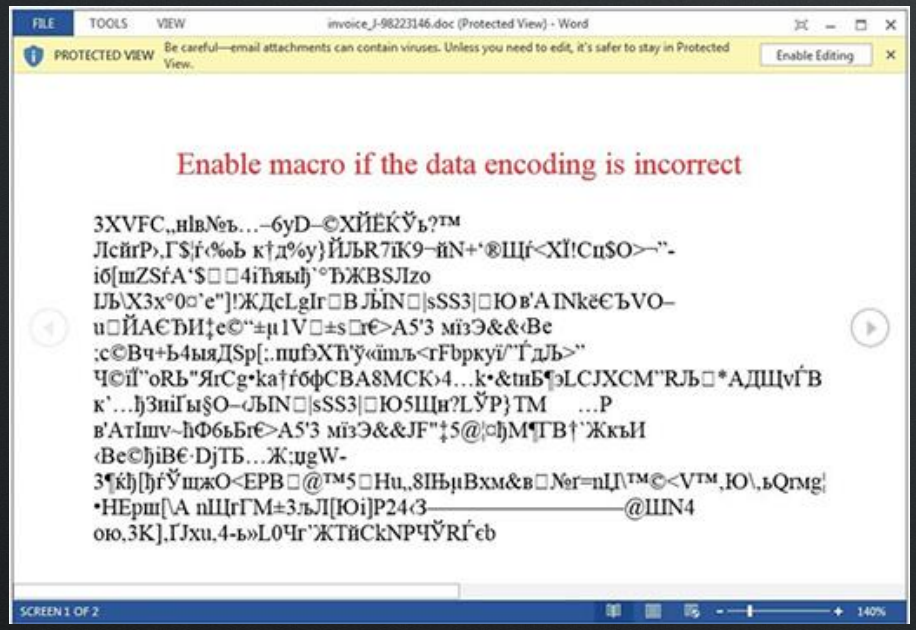
- Doručený vo forme dokumentu s makrom
- Šifruje súbory a file share, žiada peniaze
- Rýchlo sa mení, polymorfický, perzistentný
- Používa RC4 a RSA šifrovacie algoritmy
- Platforma: Server a Client
- Rôzne evansion mechanizmy (AV, UAC, Sandbox…)

[Protected] Non-confidential content

Produkt: ako funguje

Enable Macro





Produkt: ako funguje

Enable Macro ➡ PowerShell download
Cerber executable

A sample JGP file – Cerber ransomware payload is appended to an image data

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	84	00	09	06	07	13	12	12	14	....ÿÛ.„.....
00000020	13	13	13	15	16	15	17	17	1A	19	18	17	18	19	1D	1B	.....
00000030	1F	1B	22	1B	18	1A	1A	1B	23	1E	20	18	20	28	22	1A	.."....#. . (".
00000040	1B	26	1F	1F	1B	22	31	21	25	29	2B	33	2E	2E	18	1F	.&..."1!%)+3....
00000050	33	38	33	2D	37	28	2D	2E	2B	01	0A	0A	0A	0E	0D	0E	383-7(-.+.....
00000060	1B	10	10	1B	2D	26	20	26	32	2D	2D	2F	2D	2D	2F	2D	....-& &2--/--/-
00000070	2D	2D	30	2F	30	2D	2D	2D	2D	2D	2F	2D	2D	2D	2D	2D	--0/0-----/-----
00000080	2D	2B	2D	2D	2D	2D	2D	2F	2D	2E	2D	2D	2D	2E	2D	2D	-+-----/-.---.--
00000090	2D	2D	2D	2D	2D	2D	2D	2D	2D	2D	FF	C0	00	11	08	00	----------ÿÀ....
000000A0	73	00	73	03	01	11	00	02	11	01	03	11	01	FF	C4	00	s.s.........ÿÄ.

JPG image data

000169D0	69	27	00	4C	C2	0E	39	83	19	55	F3	33	61	34	2B	4B	i'.LÂ.9ƒ.Uó3a4+K
000169E0	E5	0E	37	50	E3	27	F8	24	34	7C	C6	C1	14	33	73	93	å.7Pã'ø$4|ÆÁ.3s"
000169F0	45	43	F6	EE	0A	D1	A9	34	42	B9	D6	4C	3F	4F	49	53	ECöî.Ñ©4B¹ÖL?OIS
00016A00	42	E9	5B	2B	35	A5	70	37	C0	17	9F	EC	26	72	FD	2B	Bé[+5¥p7À.Ÿì&rý+

The marked bytes are the beginning of the XOR-ed Cerber executable

[Protected] Non-confidential content

Produkt: ako funguje

Enable Macro → PowerShell download Cerber executable → Bypass UAC

UAC Bypass

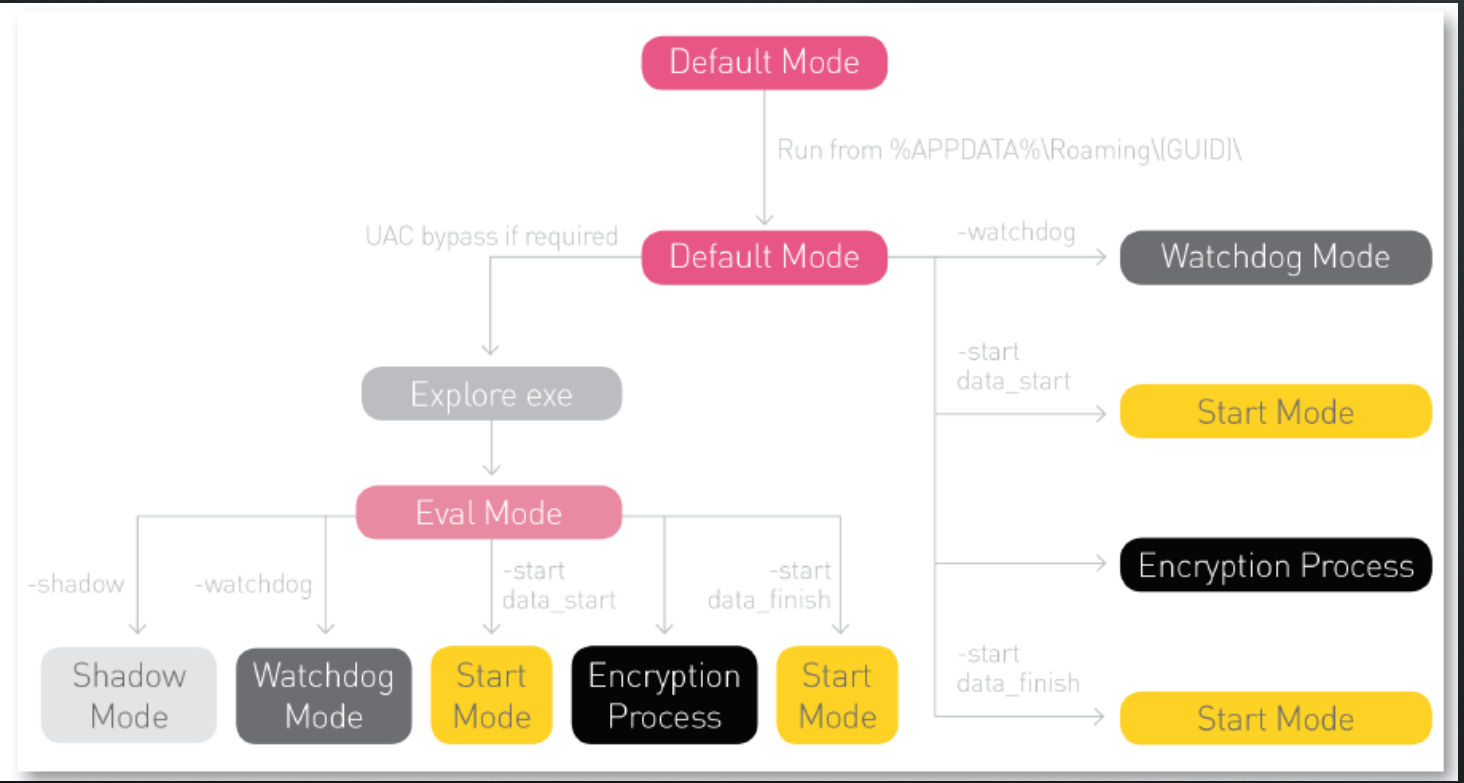
The ransomware tries to bypass UAC and execute with elevated system privileges:

1. Check if the `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLua` flag is set. If not set, Cerber launches in eval mode using the arguments `-eval {CurrentProcessID}` to terminate the current execution mode and start the encryption process. If the `EnableLua` flag is set, Cerber enumerates the `%SYSTEM32%` folder to locate files with the following features:
   - Files with `EXE` extension and none of the `FILE_ATTRIBUTE_SYSTEM` and `FILE_ATTRIBUTE_HIDDEN` file attribute flags. This `EXE` file manifest must also contain the following information:
     ```
     <autoElevate>true</autoElevate>
     <requestedExecutionLevel level="requireAdministrator"/>
     ```
   - The `EXE` files must contain an imported `DLL` whose name does not start with `api-ms-win-` and does not appear in `\KnownDlls` directory object.
2. Copy the matched `DLL` (referenced by the `EXE` file) to the `%TEMP%` directory using a random name with a `tmp` extension. It then patches the first instruction of the `DllEntryPoint`, redirecting the execution flow to the malicious code, which is responsible for running Cerber with elevated privileges.
3. Create a randomly named directory using `[A-Za-z0-9]` characters in the `%SYSTEM32%` directory.
4. Set the `cerber_uac_status` property for the `Shell_TrayWnd` window to FALSE.
5. Create the `explorer.exe` process in `CREATE_SUSPENDED` state and inject malicious code inside the `explorer.exe` process space.

[Protected] Non-confidential content

Produkt: ako funguje

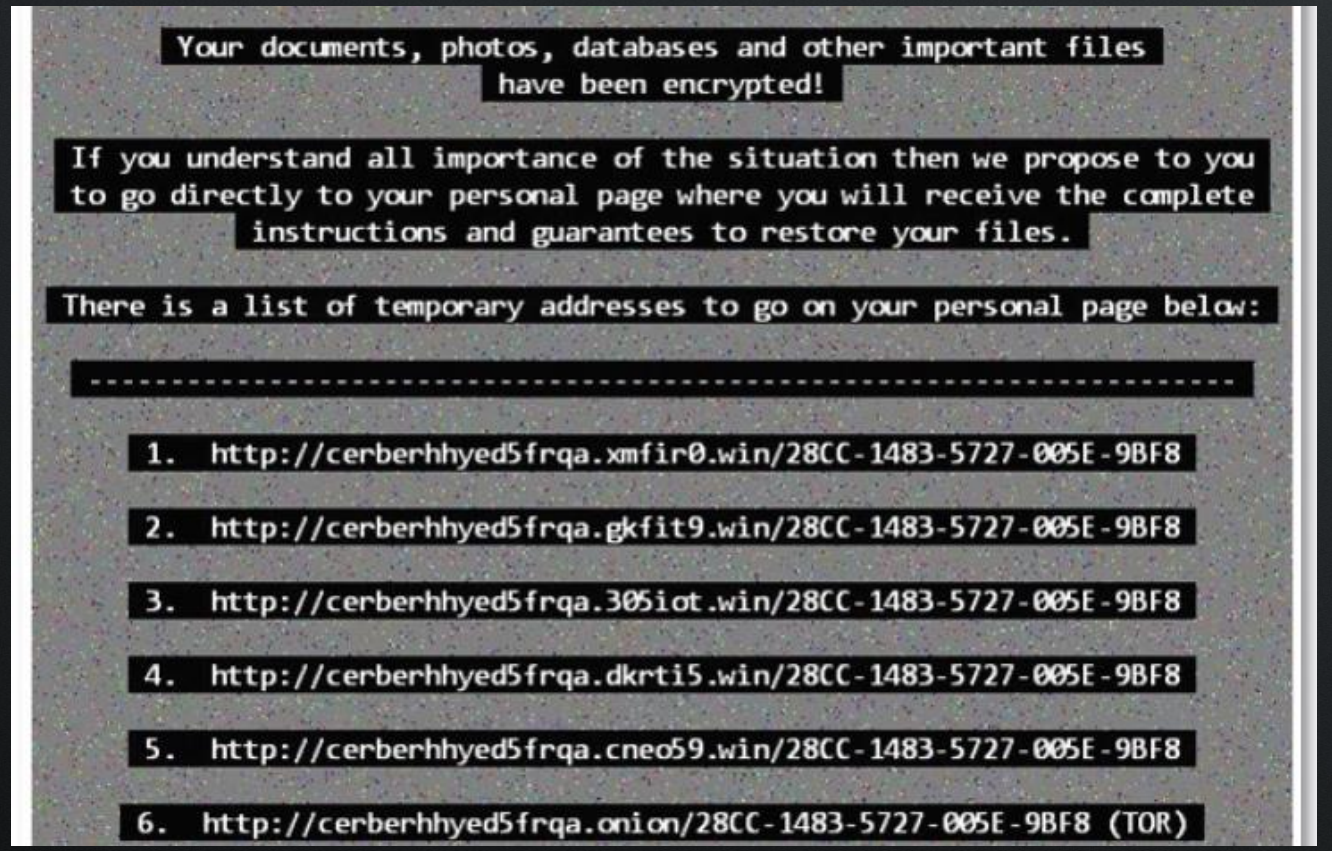
Enable Macro → PowerShell download Cerber executable → Bypass UAC → Execute



[Protected] Non-confidential content

Produkt: ako funguje

Enable Macro → PowerShell download Cerber executable → Bypass UAC → Execute



[Protected] Non-confidential content

Dodatočné nastavenia

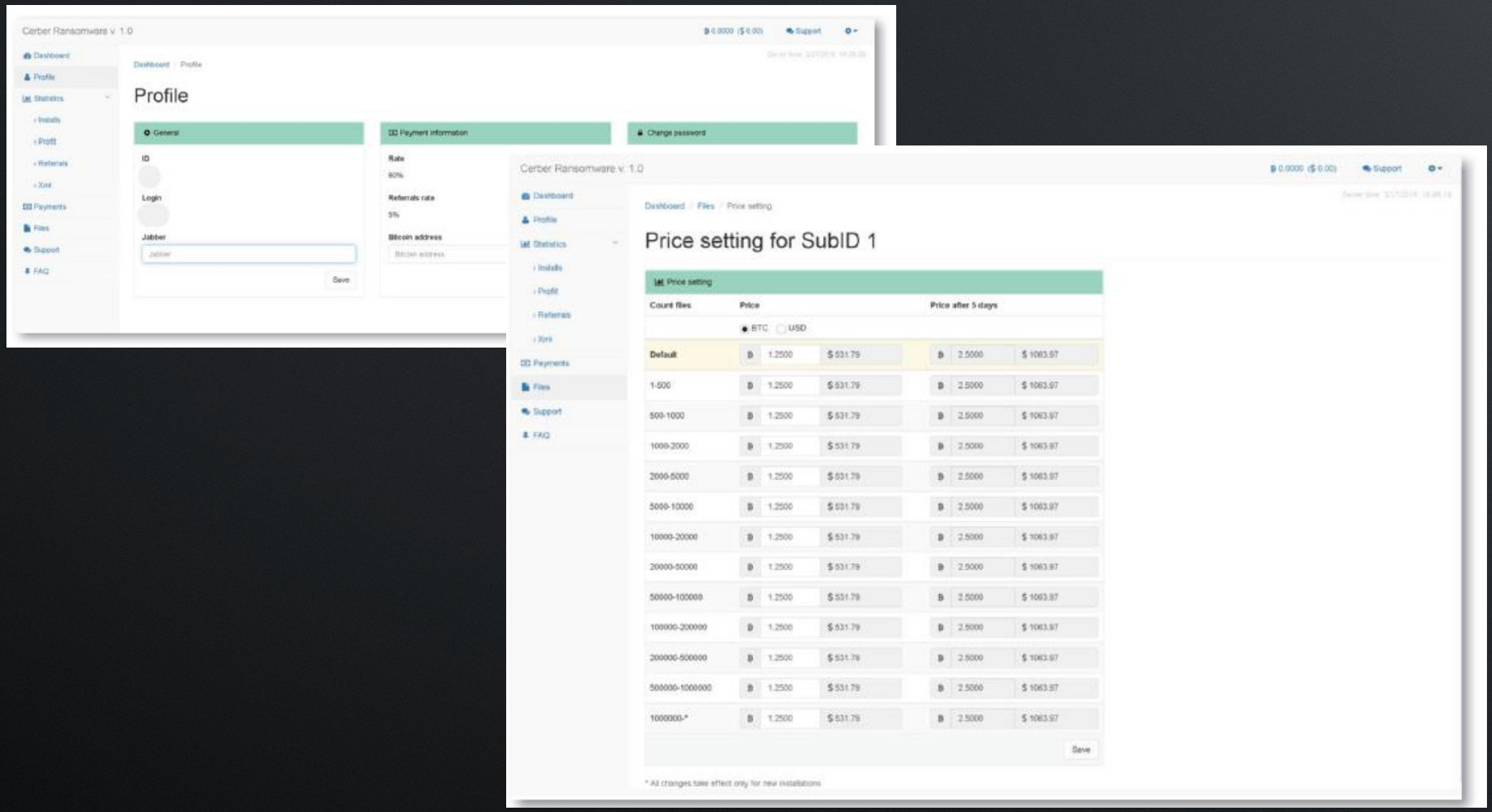
- encrypt.network
- min_file_size
- blacklist.files
- blacklisted.folders
- ip_geo
- blacklist.countries
- servers.send_stat
- virtualization evansion

Virtualization Technology Based Evasions

Virtualization Technology	Evasion Technique Description
Hypervisor	Checks if ECX 31st bit is set after executing cpuid assembly instruction with the EAX register set to 1.
VirtualBox	• `HKLM\HARDWARE\Description\System\SystemBiosVersion` registry key • `HKLM\HARDWARE\Description\System\VideosBiosVersion` registry key • `HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\Identifier` registry key • `HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions` registry key • `\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Enum\PCI` registry key • Check presence of the following file in the filesystem: `C:\WINDOWS\system32\drivers\VBoxMouse.sys`
Parallels	• `HKLM\HARDWARE\Description\System\SystemBiosVersion` registry key • `HKLM\HARDWARE\Description\System\` registry key • `\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Enum\` registry key
QEMU	• `HKLM\HARDWARE\Description\System\SystemBiosVersion` registry key • `HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\Identifier` registry key
VMWare	• `HKLM\HARDWARE\Description\System\SystemBiosVersion` registry key • `HKLM\HARDWARE\Description\System\VideosBiosVersion` registry key • `HKLM\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0\Identifier` registry key • `\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Enum\PCI` registry key • `HKLM\SOFTWARE\VMWARE, Inc.\VMware Tools` registry key • Check presence of the following file in the filesystem: `C:\Windows\system32\drivers\vmmouse.sys or C:\Windows\system32\drivers\vmhgfs.sys`
Wine	Check if `wine_get_unix_file_name` function is present in `"kernel32.dll"`

[Protected] Non-confidential content

Produkt: Server strana



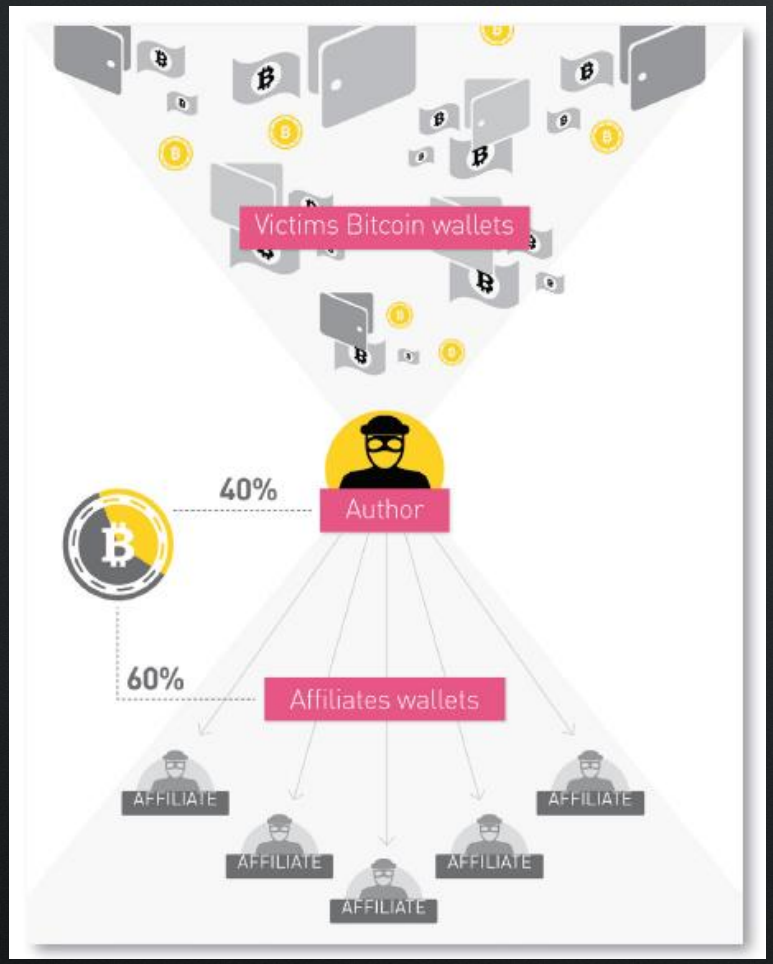
Business Model

[Protected] Non-confidential content

Business Model

RANSOMWARE-AS-A-SERVICE

- 40% k autorovi ransomware
- 60% k „partnerovi/predajcovi“



[Protected] Non-confidential content

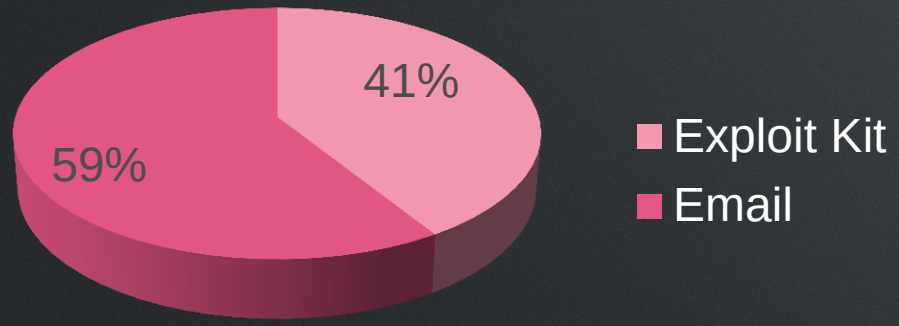
Operations

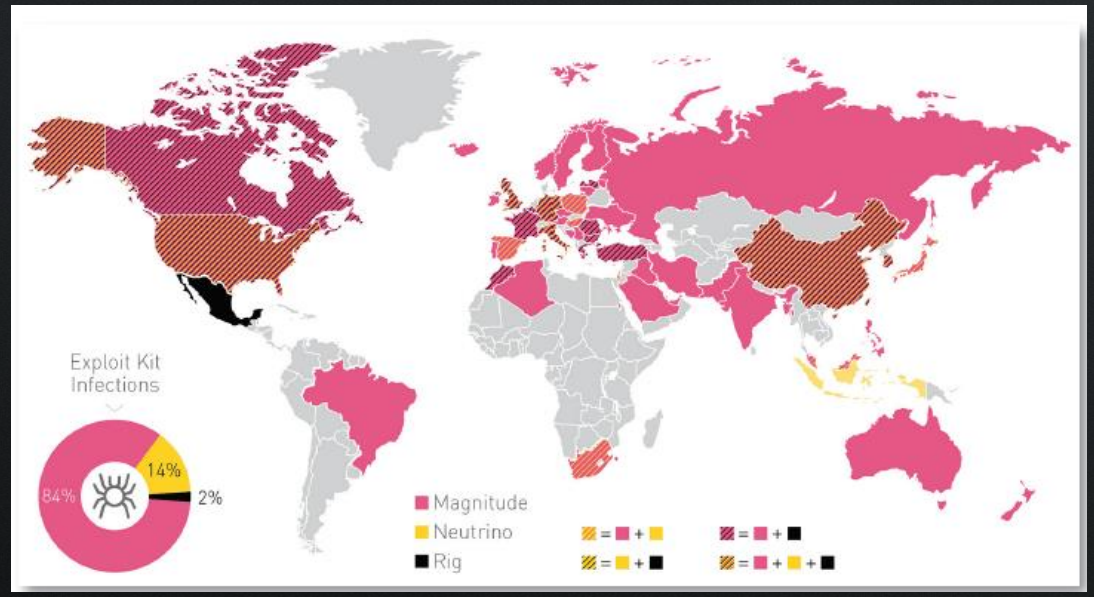
Distribučné kanály:

- Exploit kits*
  - Magnitude
  - Neutrino
  - Rig
- Email

Common vulnerability exploited:
Adobe flash zero day exploit (CVE-2016-1019)

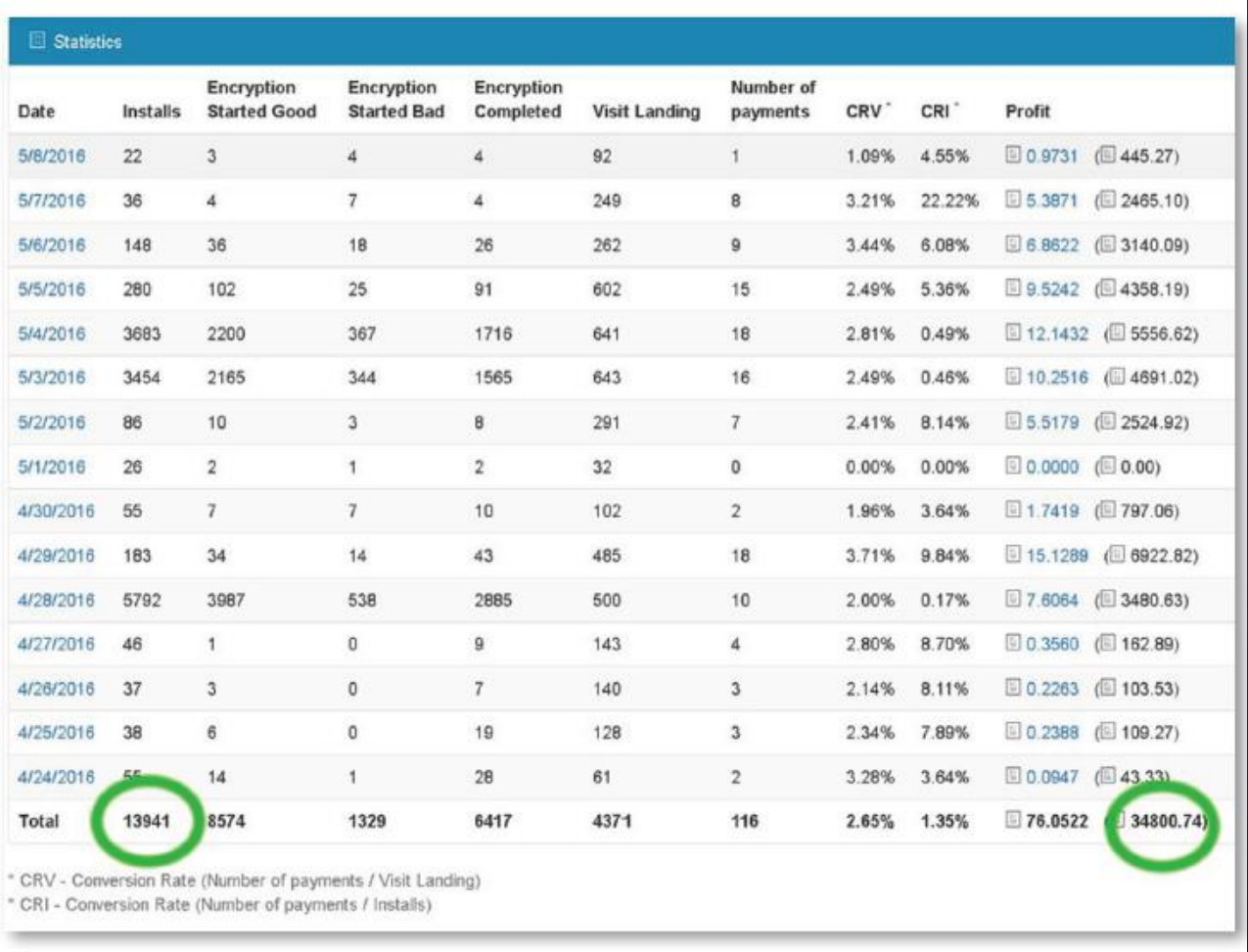
Distribution methods





[Protected] Non-confidential content

Business Model



Statistics

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRI *	Profit
5/8/2016	22	3	4	4	92	1	1.09%	4.55%	0.9731 (445.27)
5/7/2016	36	4	7	4	249	8	3.21%	22.22%	5.3871 (2465.10)
5/6/2016	148	36	18	26	262	9	3.44%	6.08%	6.8622 (3140.09)
5/5/2016	280	102	25	91	602	15	2.49%	5.36%	9.5242 (4358.19)
5/4/2016	3683	2200	367	1716	641	18	2.81%	0.49%	12.1432 (5556.62)
5/3/2016	3454	2165	344	1565	643	16	2.49%	0.46%	10.2516 (4691.02)
5/2/2016	86	10	3	8	291	7	2.41%	8.14%	5.5179 (2524.92)
5/1/2016	26	2	1	2	32	0	0.00%	0.00%	0.0000 (0.00)
4/30/2016	55	7	7	10	102	2	1.96%	3.64%	1.7419 (797.06)
4/29/2016	183	34	14	43	485	18	3.71%	9.84%	15.1289 (6922.82)
4/28/2016	5792	3987	538	2885	500	10	2.00%	0.17%	7.6064 (3480.63)
4/27/2016	46	1	0	9	143	4	2.80%	8.70%	0.3560 (162.89)
4/26/2016	37	3	0	7	140	3	2.14%	8.11%	0.2263 (103.53)
4/25/2016	38	6	0	19	128	3	2.34%	7.89%	0.2388 (109.27)
4/24/2016	55	14	1	28	61	2	3.28%	3.64%	0.0947 (43.33)
Total	**13941**	**8574**	**1329**	**6417**	**4371**	**116**	**2.65%**	**1.35%**	**76.0522 (34800.74)**

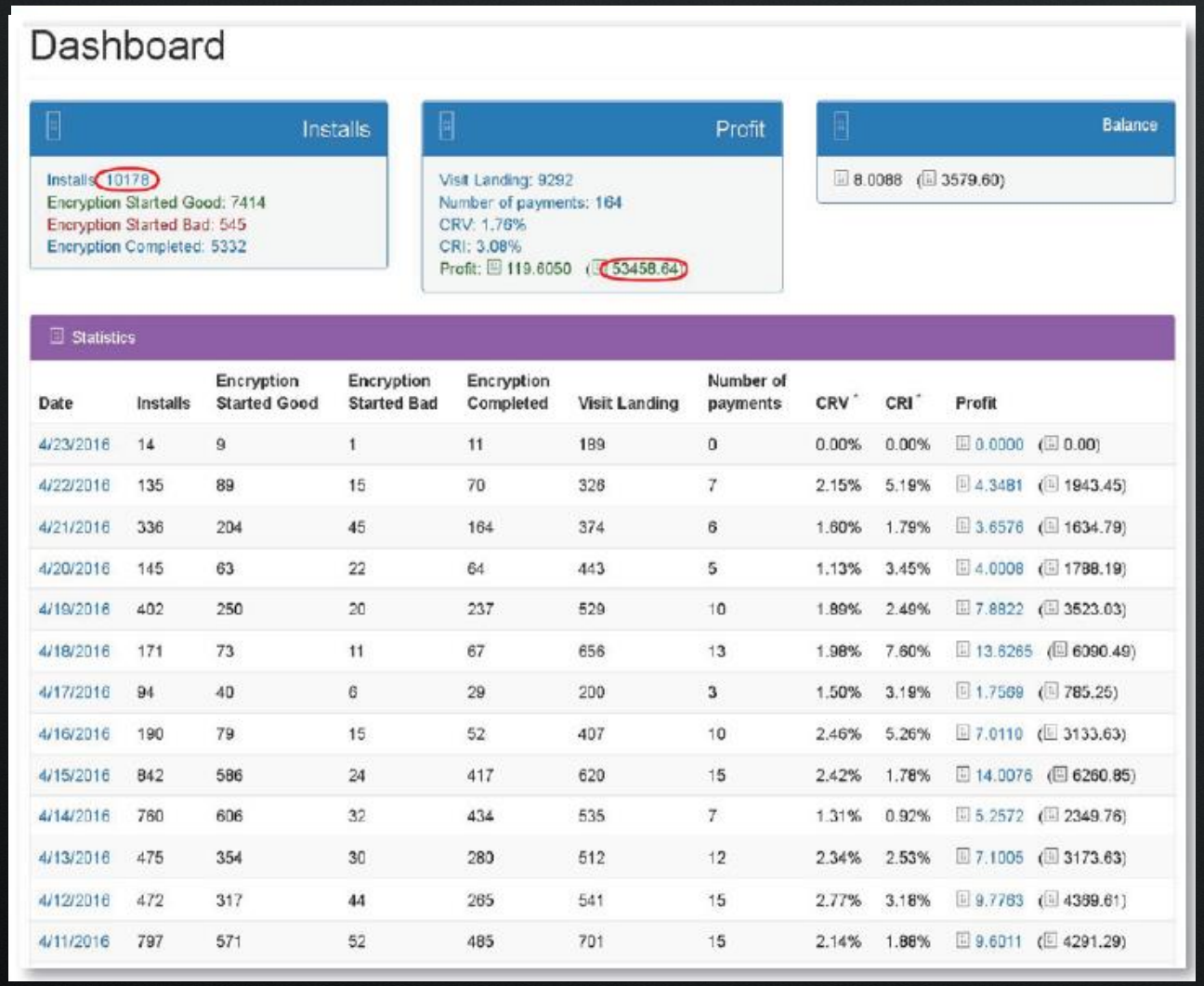
* CRV - Conversion Rate (Number of payments / Visit Landing)
* CRI - Conversion Rate (Number of payments / Installs)

13,491 installed to 116 ransom payments, earning 34,800.74 USD between Apr-May 16

Abbreviations used in the Profit section:
CRI – Conversion Rate Installs (Number of payments/Installs)

[Protected] Non-confidential content

Business Model



Dashboard

Installs

Installs: 10178
Encryption Started Good: 7414
Encryption Started Bad: 545
Encryption Completed: 5332

Profit

Visit Landing: 9292
Number of payments: 164
CRV: 1.76%
CRI: 3.08%
Profit: 119.6050 (53458.64)

Balance

8.0088 (3579.60)

Statistics

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRI *	Profit
4/23/2016	14	9	1	11	189	0	0.00%	0.00%	0.0000 (0.00)
4/22/2016	135	89	15	70	326	7	2.15%	5.19%	4.3481 (1943.45)
4/21/2016	336	204	45	164	374	6	1.60%	1.79%	3.6576 (1634.79)
4/20/2016	145	63	22	64	443	5	1.13%	3.45%	4.0008 (1788.19)
4/19/2016	402	250	20	237	529	10	1.89%	2.49%	7.8822 (3523.03)
4/18/2016	171	73	11	67	656	13	1.98%	7.60%	13.6265 (6090.49)
4/17/2016	94	40	6	29	200	3	1.50%	3.19%	1.7589 (785.25)
4/16/2016	190	79	15	52	407	10	2.46%	5.26%	7.0110 (3133.63)
4/15/2016	842	586	24	417	620	15	2.42%	1.78%	14.0076 (6260.85)
4/14/2016	760	606	32	434	535	7	1.31%	0.92%	5.2572 (2349.76)
4/13/2016	475	354	30	280	512	12	2.34%	2.53%	7.1005 (3173.63)
4/12/2016	472	317	44	265	541	15	2.77%	3.18%	9.7783 (4369.61)
4/11/2016	797	571	52	485	701	15	2.14%	1.88%	9.6011 (4291.29)

10,178 installed to 164 ransom payments, earning 58,458.06 USD between Feb-Apr 16

Abbreviations used in the Profit section:
CRI – Conversion Rate Installs (Number of payments/Installs)

[Protected] Non-confidential content

CerberRing V ČÍSLACH

Aktuálne beží cca 161 aktívnych Cerber kampaní

8 nových kampaní vzniká každý deň

150,000 obetí za Júl (conv. rate ~1.5-3%)

Obete pochádzajú z 201 krajín

Ročný zisk je cca $2.3M

©2016 Check Point Software Technologies Ltd.

[Protected] Non-confidential content

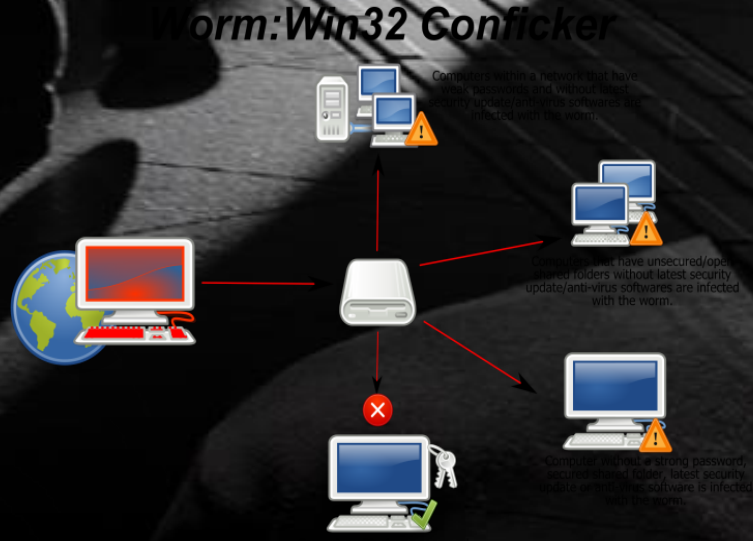
Evolúcia Ransomware

“Tiché šifrovanie”:

- Za pár mesiacov – backupy sú zašifrované

Nové cesty šírenia malware - červ:

- Šírenie ako červ
- Ransomware + Conficter

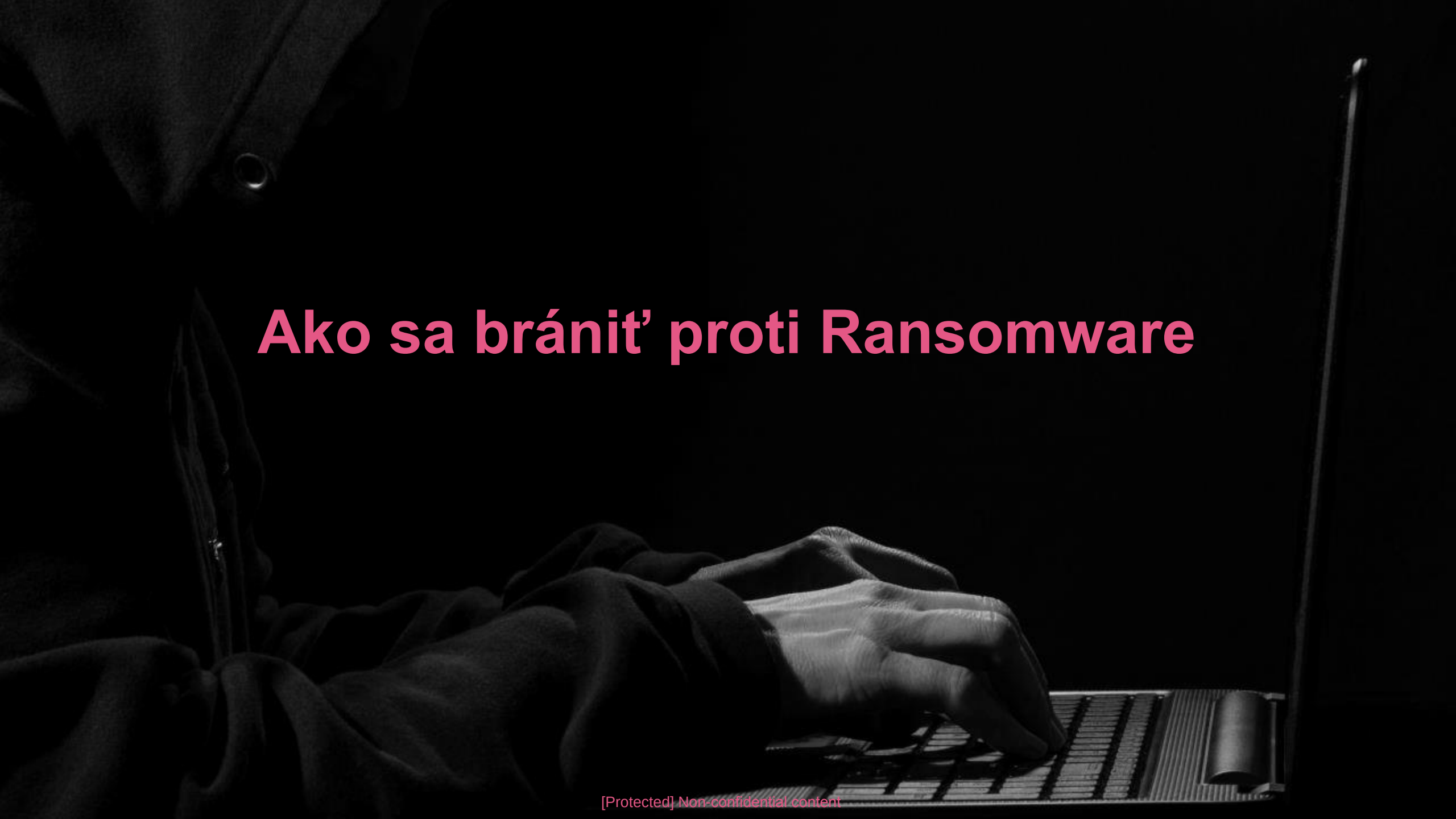


RansomWeb

- Šifruje web aplikačné data
- “Tiché šifrovanie”
- Šifruje DB + backupy

[Protected] Non-confidential content

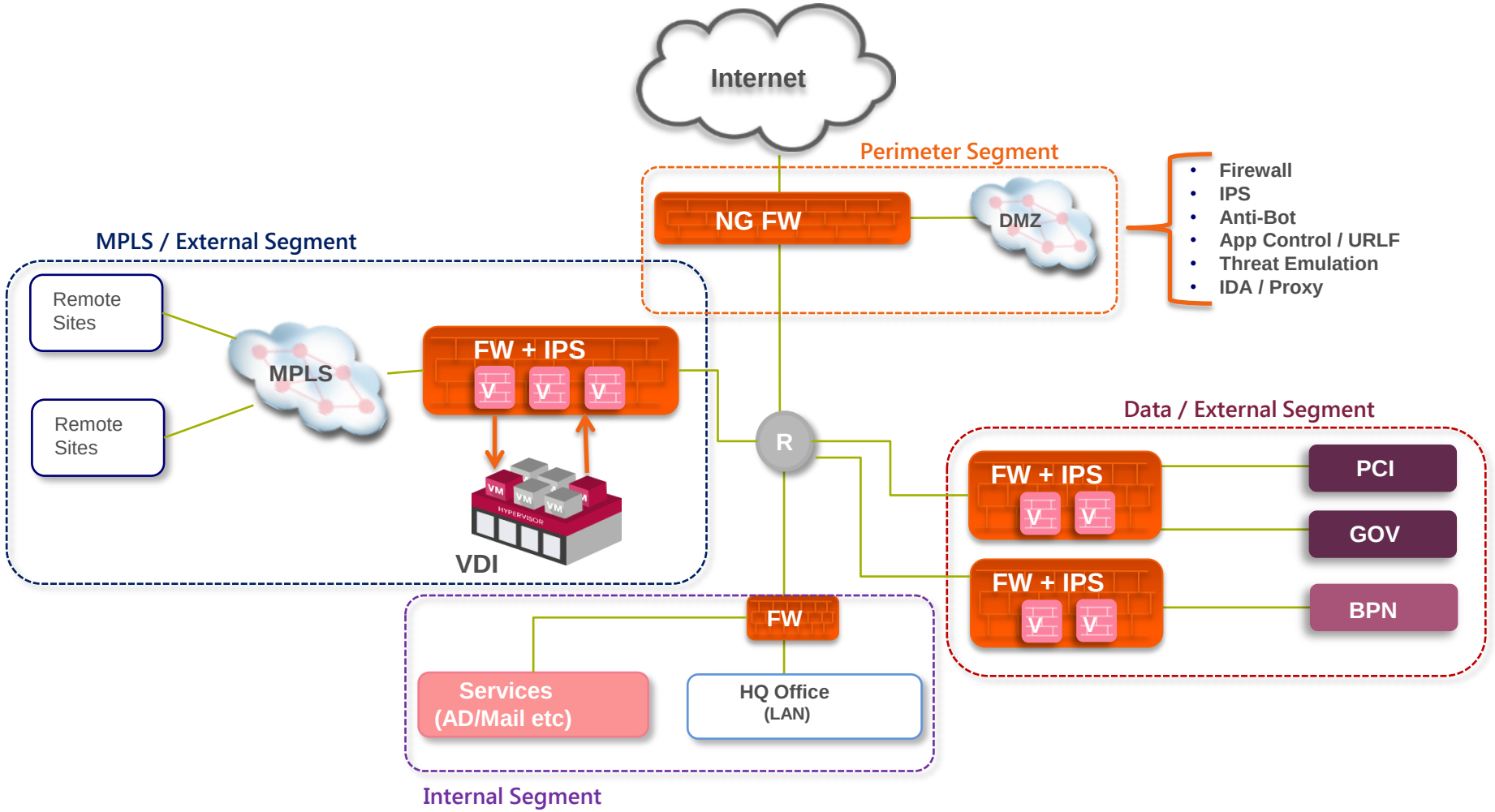
Source: Symantec: The evolution of ransomware

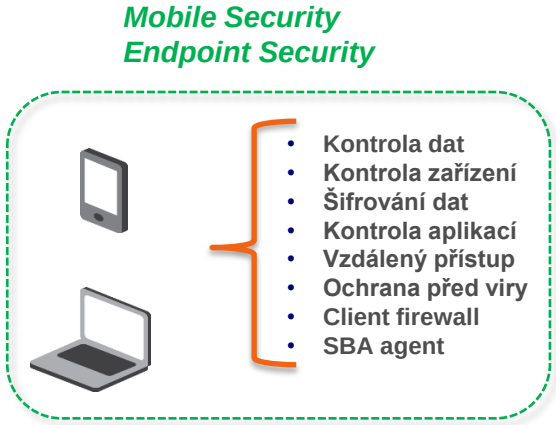


Ako sa brániť proti Ransomware

[Protected] Non-confidential content

Správna Architektura





©2016 Check Point Software Technologies Ltd.

Správna Architektura

Kompletná ochrana

Next Generation Firewall

Firewall

Application Control

IPS

Malware Protection

Web Security

Antivirus

Anti-bot

Zero-day protection

Threat Emulation

Threat Extraction

Data protection

DLP

Document Security

Endpoint and Mobile Protection

Mobile Security

Endpoint Security Suite

Podpora všetkých business platforiem

Security Appliances

Virtual Appliances and SDN

Microsoft

cisco

vmware NSX

vmware

amazon web services

openstack CLOUD SOFTWARE

KVM

APIC ACI

Endpoint and Mobile devices

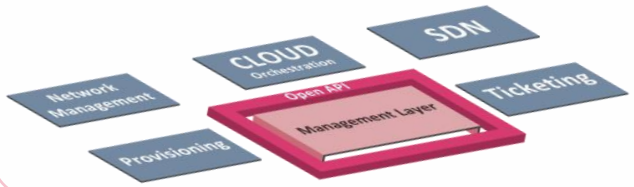
Microsoft

android

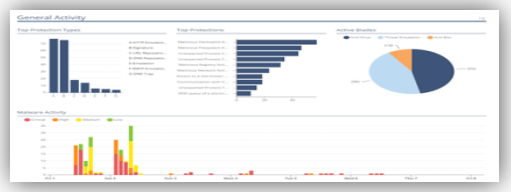
iOS

Centrálny management a Reporting

Centrally Managed & Integrated



Monitoring and Reporting

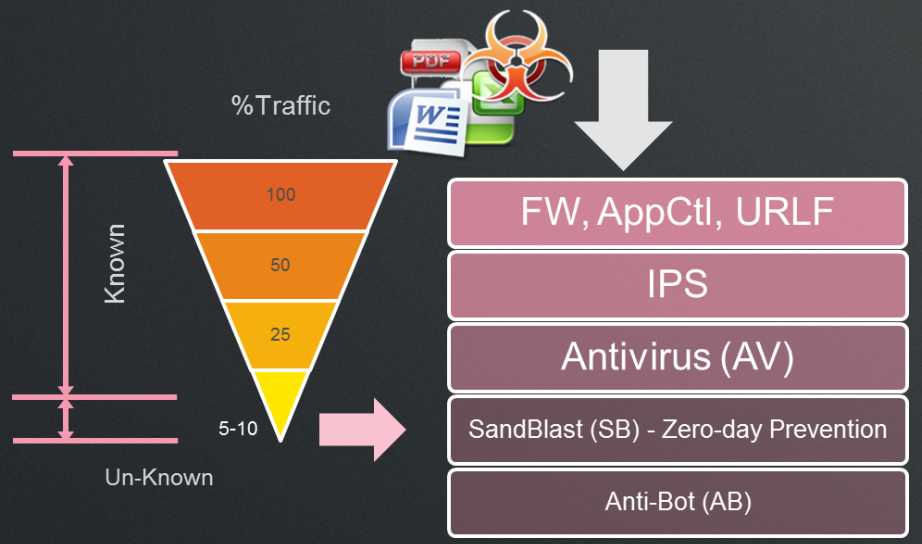


Incident Response

©2015 Check Point Software Technologies Ltd.

Rozvoj technologií

- NGFW sú efektívne z ~75%
- Vzostup nových technologií (Behavior based)
  - Machine Learning / AI
  - 2nd generation Sandboxes
  - Zero-day endpoint protection (NG AV)

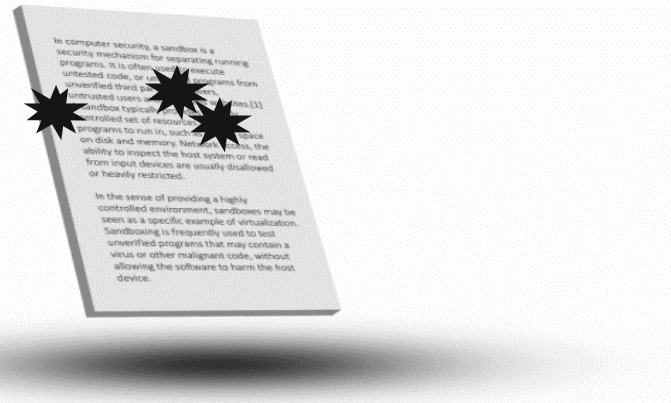


[Protected] Non-confidential content

TRADITIONAL 1ST GENERATION SANDBOX

Check Point
SOFTWARE TECHNOLOGIES LTD.

Open and try to detonate files



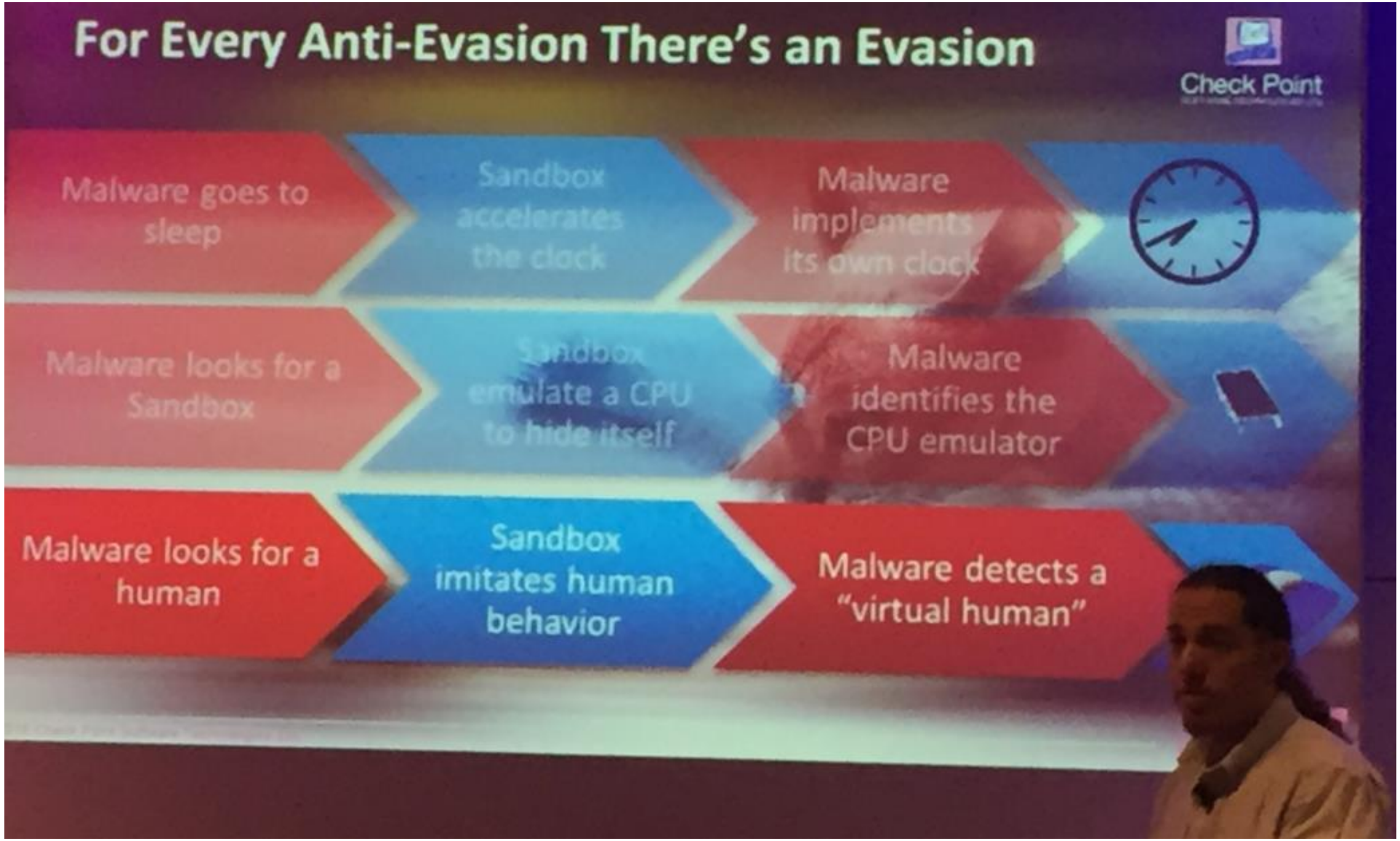
Examine:

- System Registry
- Network Connections
- File System Activity
- System Processes

Watch for telltale signs of malicious code at the Operating System level

©2015 Check Point Software Technologies Ltd.
[Restricted] ONLY for designated groups and individuals

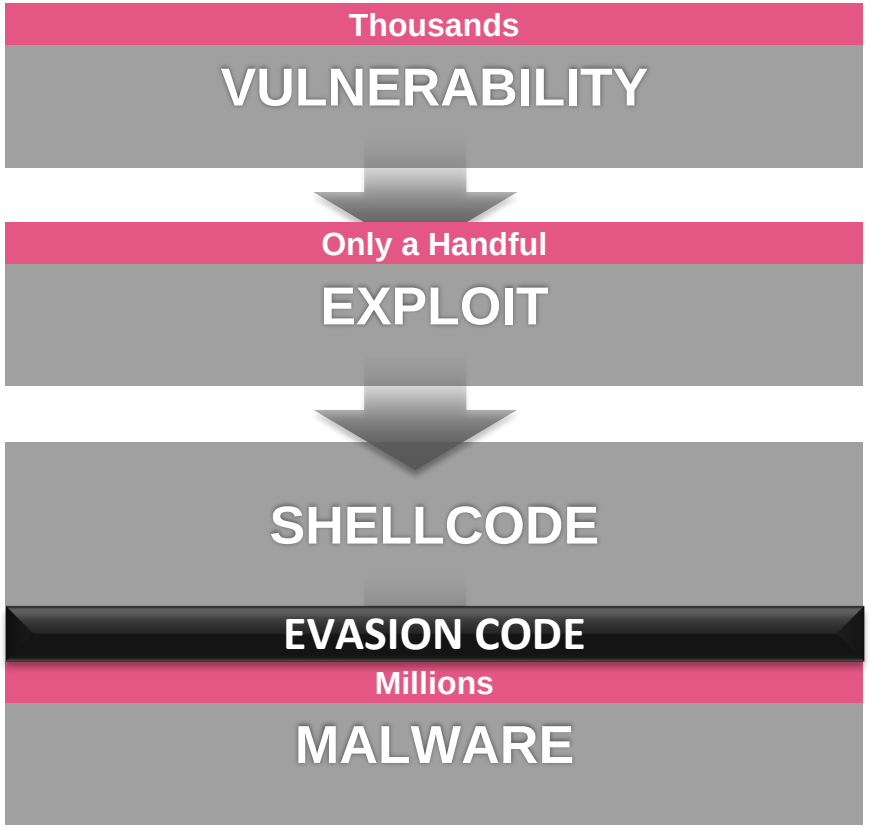
Malware se snaží sandboxů 1. generace vyvarovat



©2015 Check Point Software Technologies Ltd.

Detekce na úrovni CPU (CPU Level)

a dodatečná statická a heuristická analýza



Check Point SandBlast ZERO-DAY PROTECTION

CPUL detekce odhalí malware

Dříve než dojde k jeho stažení….

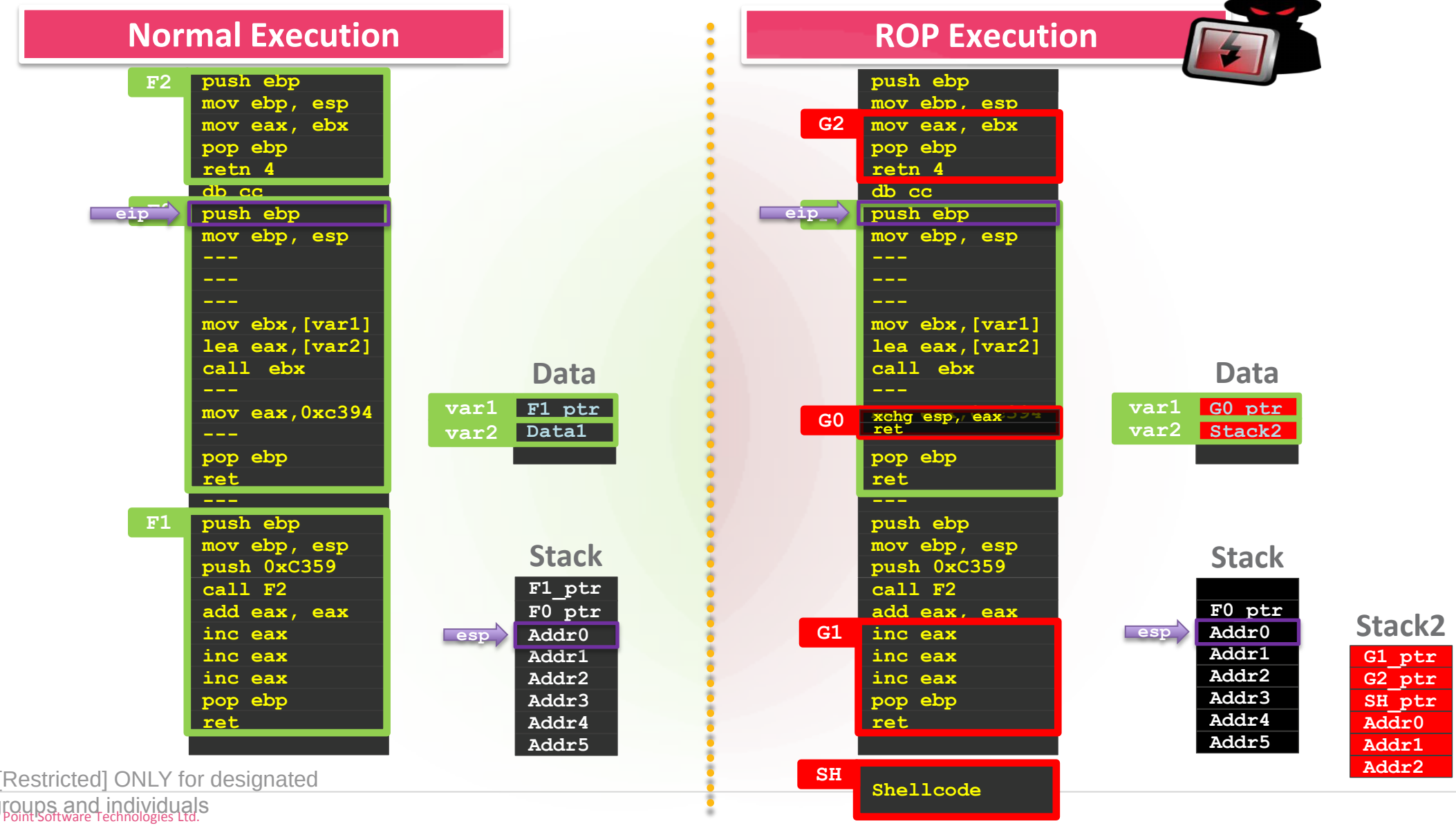
Dříve než dojde na jeho spuštění…

Tradičný sandbox

©2016 Check Point Software Technologies Ltd.

[Confidential] For designated groups and individuals

Building a ROP Gadgets Dictionary -
To gain privileges to run the malware



[Restricted] ONLY for designated groups and individuals

©2016 Check Point Software Technologies Ltd.

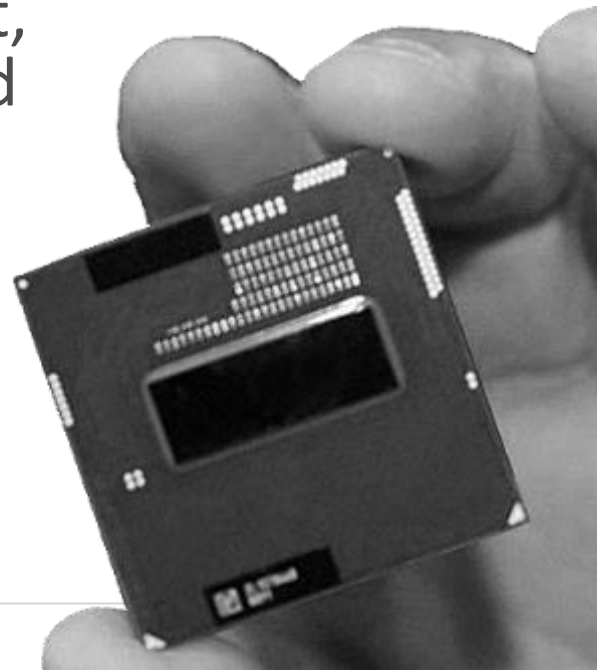
Leveraging the Haswell CPU

Check Point
SOFTWARE TECHNOLOGIES LTD.

Modern processors include sophisticated debug and performance monitoring mechanisms

- Tracks the flow of **branch operations**
  - Operations that change execution flow of a running process
  - Output is usually a trace of records in a FROM->TO format, which represent the branch operations the CPU processed
- Concept of using this to mitigate control flow exploits has been subject of academic research…

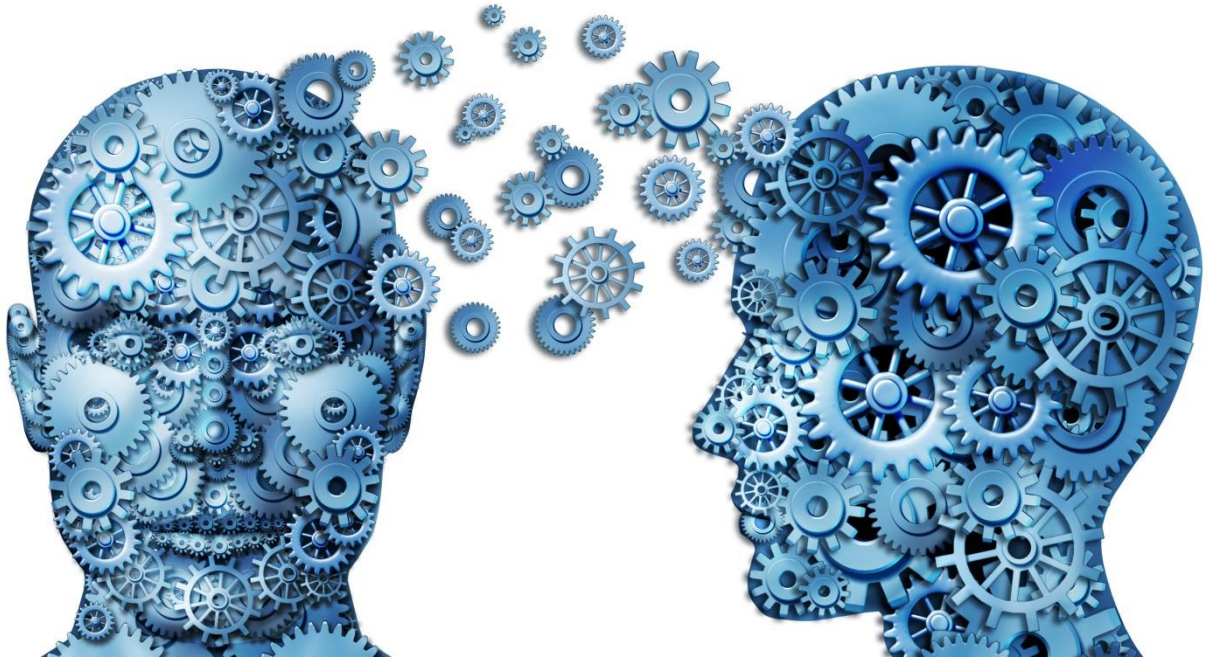
… Haswell makes it feasible for threat prevention

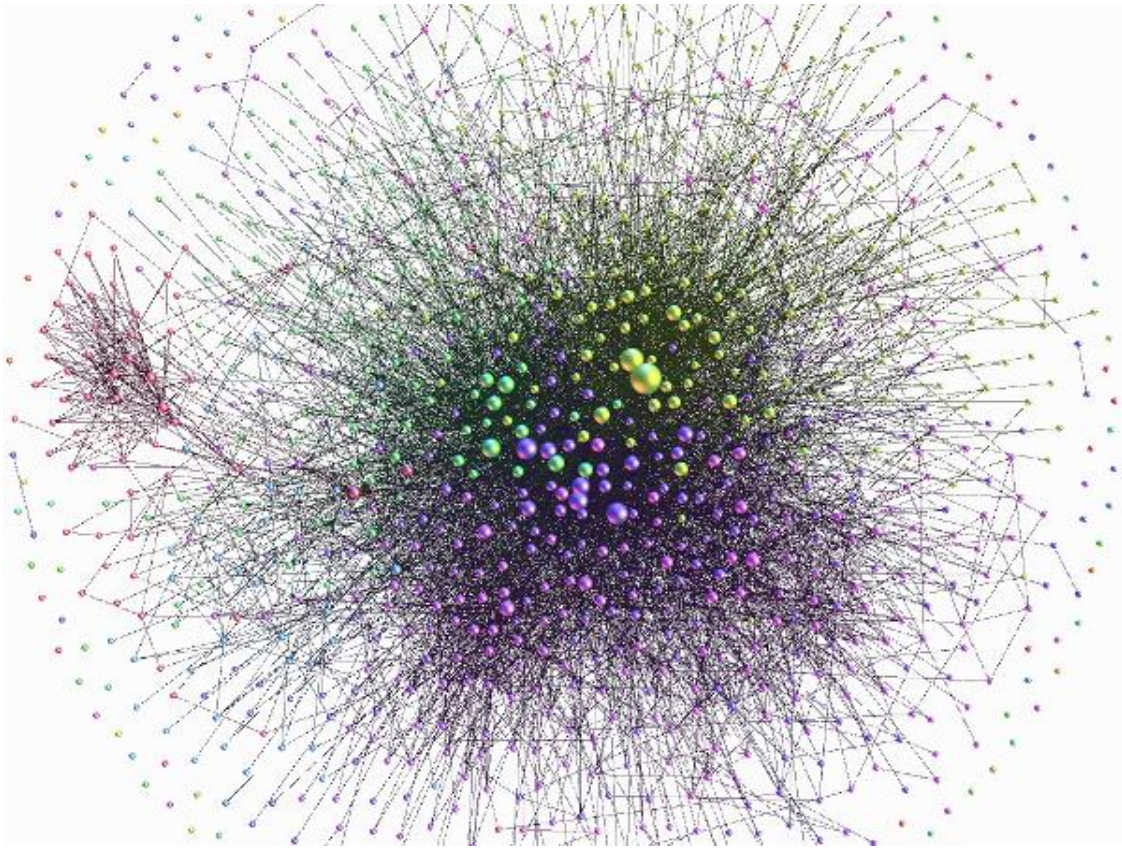


©2016 Check Point Software Technologies Ltd.

Machine Learning inside Sandboxing

Malware detection using Big Data and Machine Learning

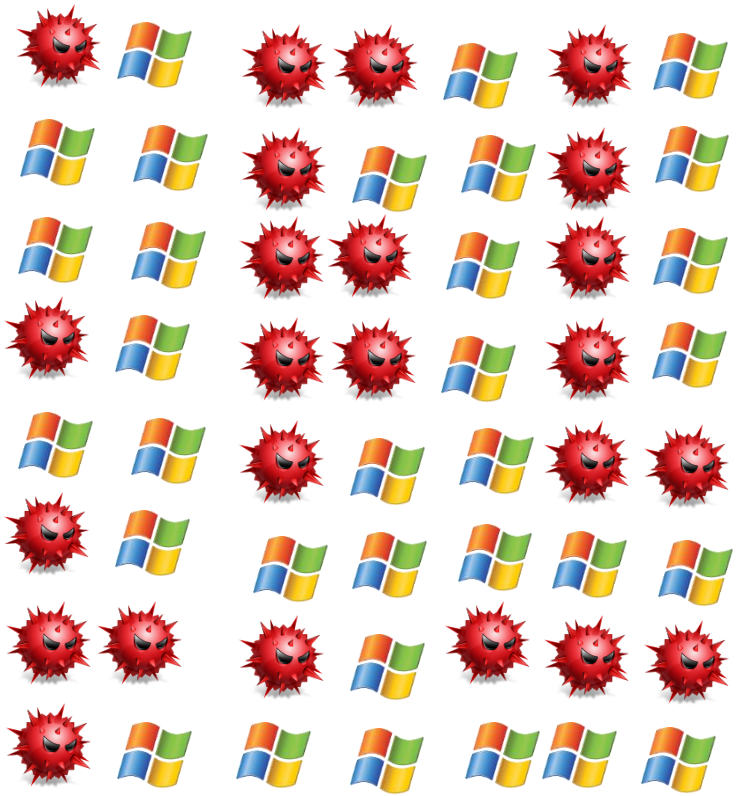


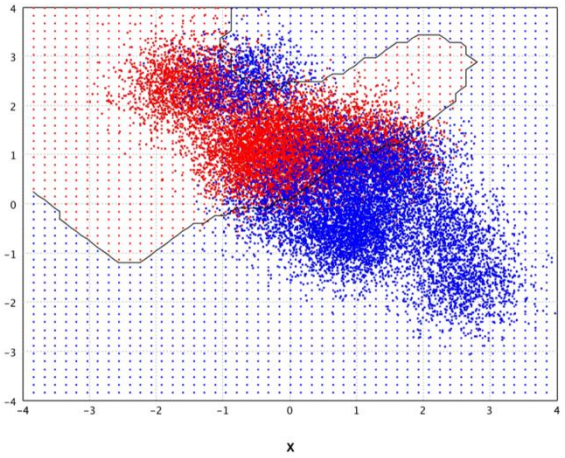


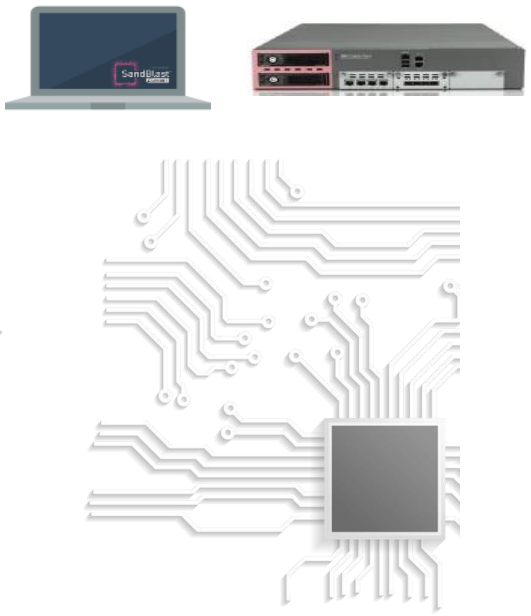
©2016 Check Point Software Technologies Ltd.

Machine Learning inside Sandboxing

Malware detection using Big Data and Machine Learning







©2016 Check Point Software Technologies Ltd.

TRADITIONAL SANDBOXES ARE IN DETECTION or SLOW

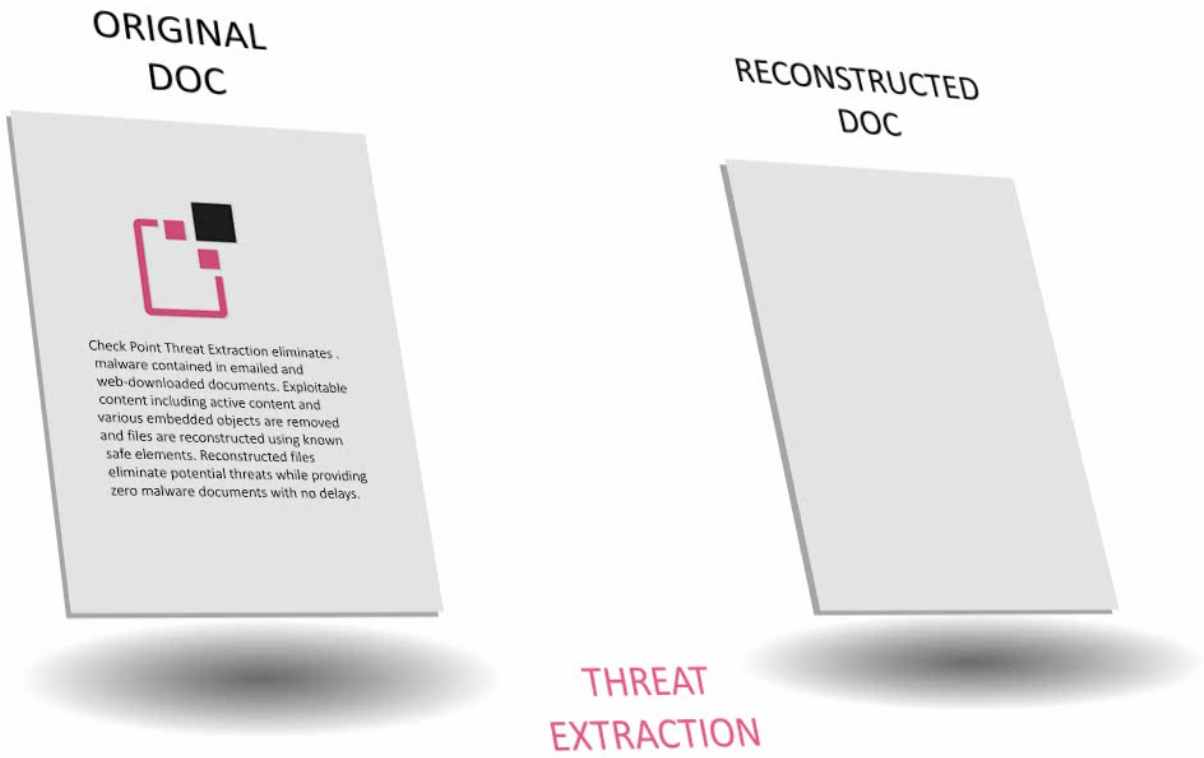
INSPECTION TAKES TIME

- 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

©2016 Check Point Software Technologies Ltd.
[Restricted] ONLY for designated groups and individuals

Sandblast - Check Point Threat Extraction

Clean potentially malicious content from documents



[Protected] Non-confidential content
©2016 Check Point Software Technologies Ltd.

Okamžitá ochrana příloh

Rychlé doručení bezpečné verze

Check Point
SOFTWARE TECHNOLOGIES LTD.

Reply Reply All Forward

Tue 5/4/16 6:03 PM

Yonni Shelmerdine

SECURITY ALERT! Skipped Invoice

To Yonni Shelmerdine

Message invoice.cleaned.pdf

*Check Point SandBlast Threat Extraction has **cleaned** an attachment named **Invoice.doc** as it was determined to contain potentially malicious elements.*

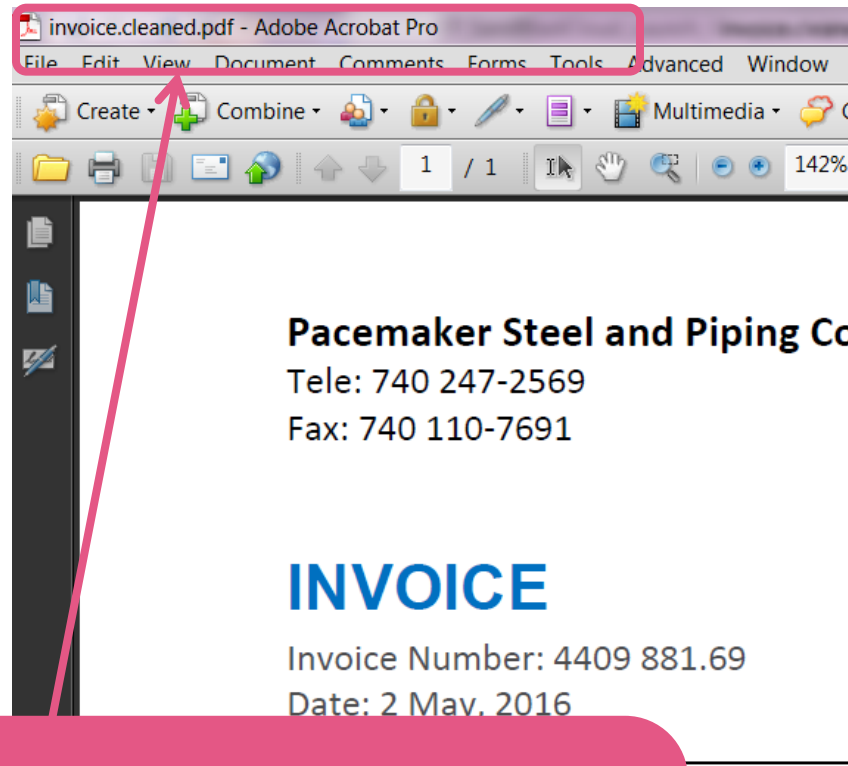
To access the original file, please click here

Hi Yonni,
Attached is invoice #4409 881.69 from May which was missing from the original summary.

I am out of the office tomorrow and Monday, so I'm emailing you now to request that you go over the invoice, submit the detail [Blocked Malicious URL] and complete they payment as soon as possible.

Julia Reyes / Credit Manager
Pacemaker Steel and Piping Co. Inc.
Tele: 740 247-2569
Fax: 740 110-7691

This Email was secured by Check Point SandBlast Connector for Office 365



Vyčištěná verze originálu nebo konvertováno do PDF pro eliminaci rizik

©2016 Check Point Software Technologies Ltd.

Endpoints Require Advanced Zero-Day Protection

[Restricted] ONLY for designated groups and individuals

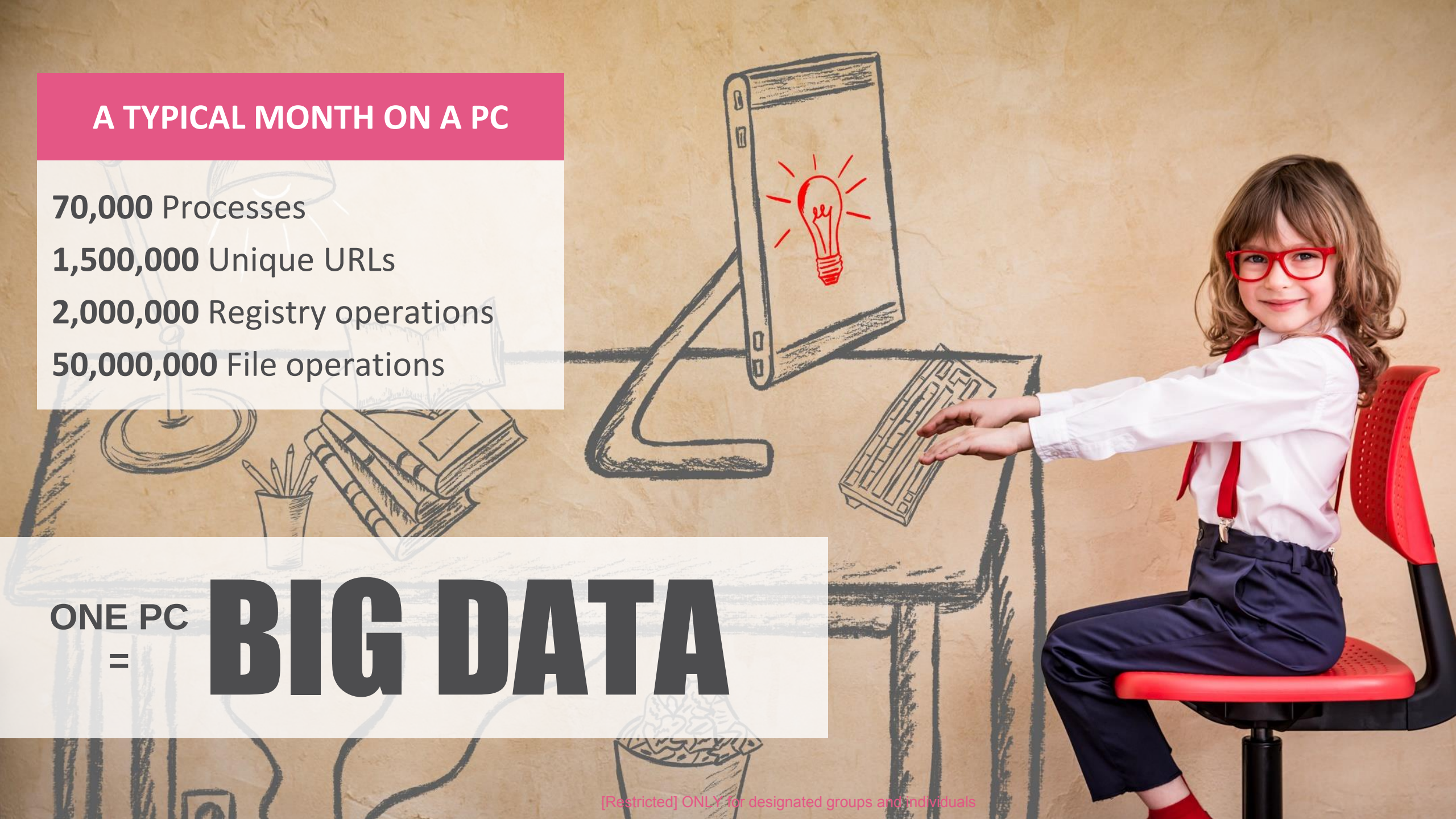
A TYPICAL MONTH ON A PC

70,000 Processes

1,500,000 Unique URLs

2,000,000 Registry operations

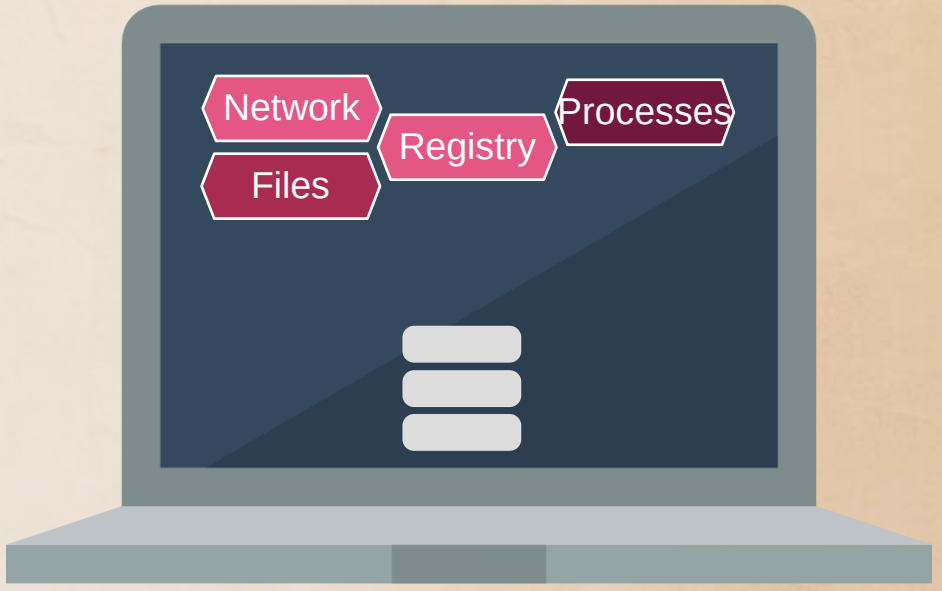
50,000,000 File operations

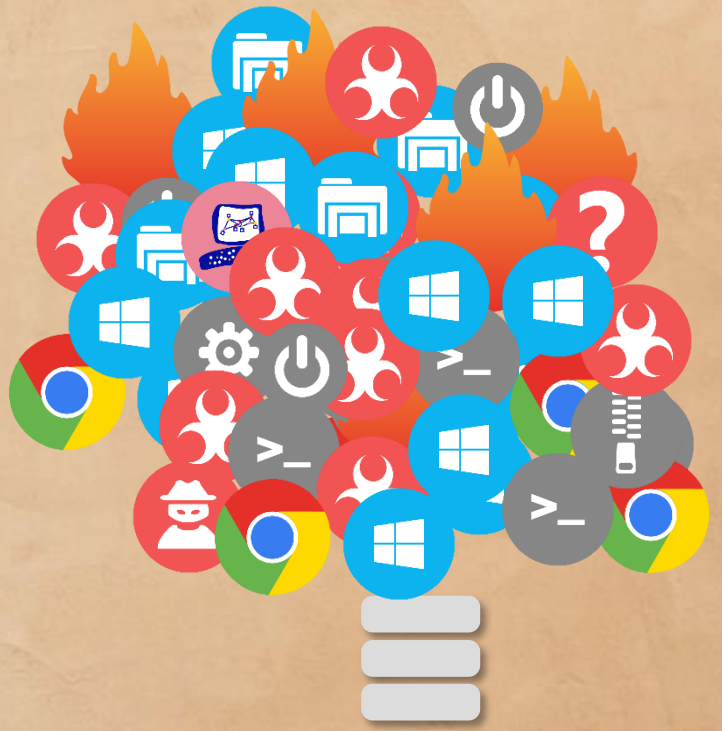


ONE PC
=
BIG DATA

[Restricted] ONLY for designated groups and individuals

Collecting Forensics Data is Easy

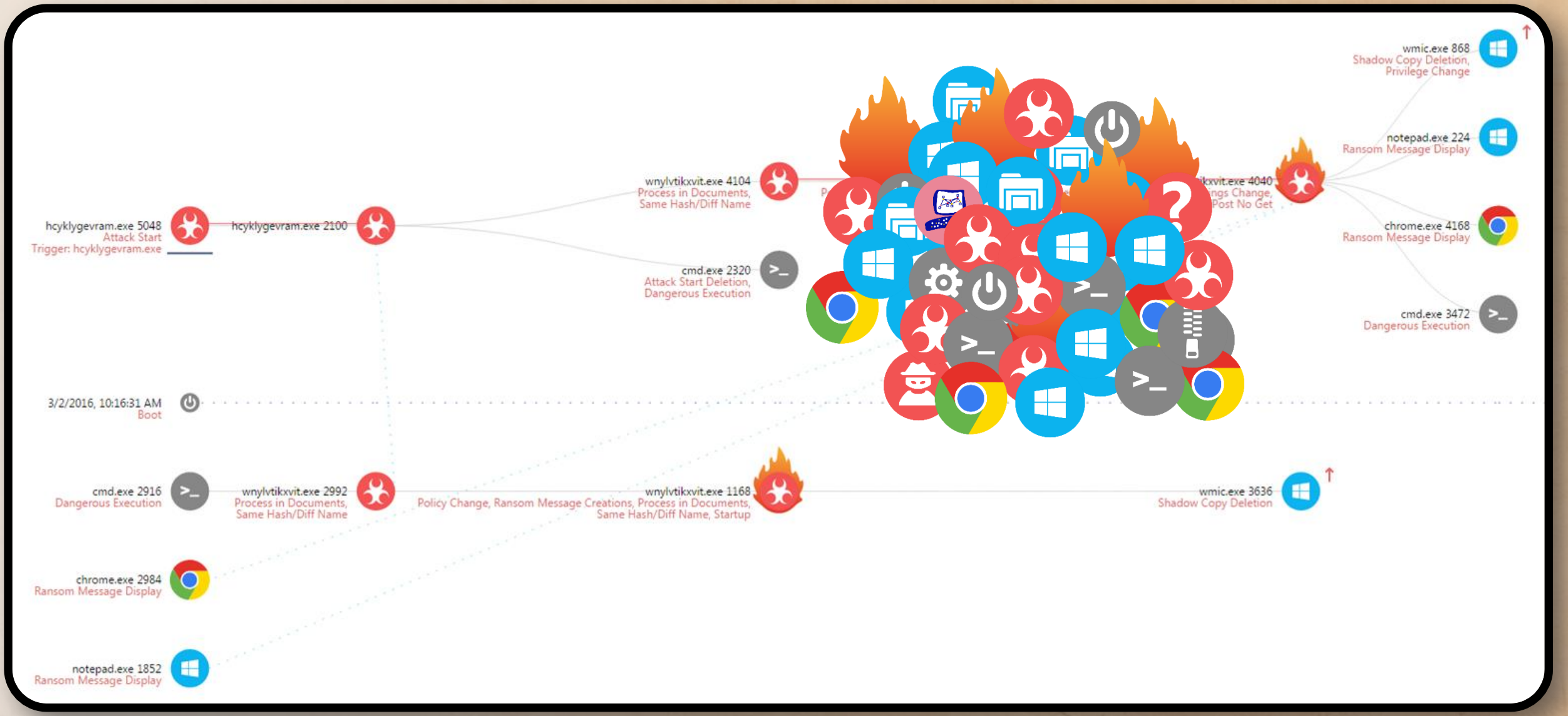




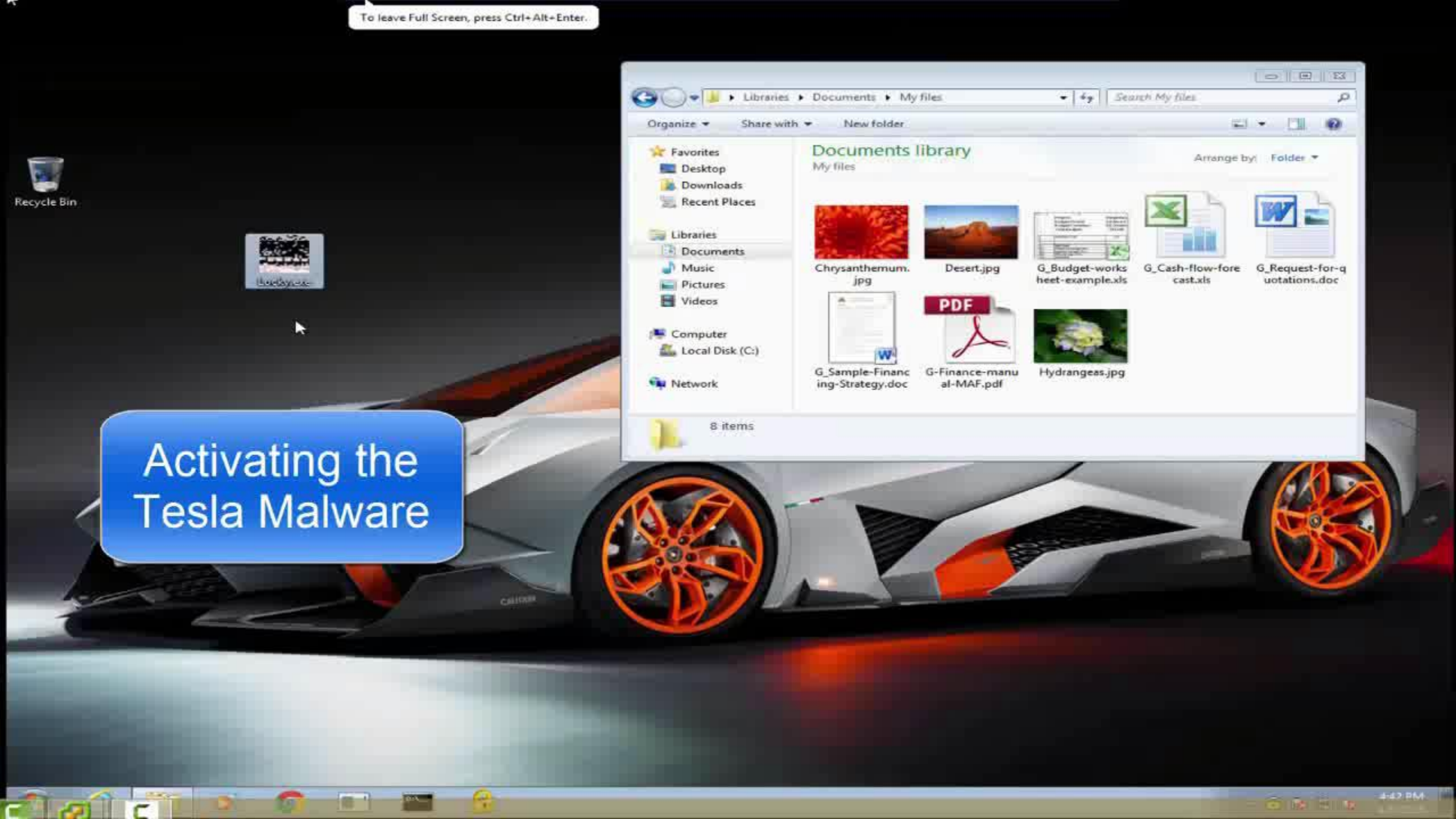
OK... but **NOW WHAT?!**

[Restricted] ONLY for designated groups and individuals

Making Sense out of BIG Forensics Data



[Restricted] ONLY for designated groups and individuals


To leave Full Screen, press Ctrl+Alt+Enter.
Recycle Bin
Libraries ▸ Documents ▸ My files
Search My files
Organize
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Documents library
My files
Arrange by: Folder
Chrysanthemum.jpg
Desert.jpg
G_Budget-worksheet-example.xls
G_Cash-flow-forecast.xls
G_Request-for-quotations.doc
G_Sample-Financing-Strategy.doc
G-Finance-manual-MAF.pdf
Hydrangeas.jpg
8 items
Activating the Tesla Malware

Check Point
SandBlast™
ZERO-DAY PROTECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

EMULATION AND EXTRACTION SERVICE

THREATCLOUD

CHECK POINT CLOUD

SandBlast Service

HOSTED ON PREMISE

SandBlast TE Appliance

NETWORK

AGENT

Office 365

CLOUD

<API>

[Confidential] For designated groups and individuals

Záver

©2015 Check Point Software Technologies Ltd.

[Confidential] For designated groups and individuals

Doporučenie:

Blokujte

Zálohujte

Vzdelávajte

Check Point SOFTWARE TECHNOLOGIES LTD.

Architektúra

Check Point SOFTWARE TECHNOLOGIES LTD.

2nd generation of Sandboxing

Check Point SOFTWARE TECHNOLOGIES LTD.

Zero-Day Endpoint Protection

©2015 Check Point Software Technologies Ltd.

[Confidential] For designated groups and individuals

S čím Vám radi pomôžeme:

- Návrh architektury pre Zero-Day ochranu
- Otestovanie / PoC Sandblast
- Security Check Up – overenie stavu siete
- Rýchle nasadenie / zapožičanie zariadenia v prípade útoku

Tempest

IT makes sense

Check Point®
SOFTWARE TECHNOLOGIES LTD.

[Restricted] ONLY for designated groups and individuals

Check Point
SOFTWARE TECHNOLOGIES LTD.

ĎAKUJEM

©2016 Check Point Software Technologies Ltd.