Zero-Day Protection mit Sandboxing in der Cloud oder doch lieber lokal

Thomas Hesse

Westcon Comstor
Delivering Results Together
powered by WestconGroup

Agenda

1. Anatomie einer Attacke am Beispiel WannaCry
2. Warum Sandboxing?
3. Angebot verschiedener Hersteller
4. Vor und Nachteile von Cloud Lösungen
5. Worauf ist beim Design zu achten

Microsoft Security Bulletin MS17-010 - Critical

- **Security Update for Microsoft Windows SMB Server (4013389)**
- Published: March 14, 2017

Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146	Windows SMB Information Disclosure Vulnerability – CVE-2017-0147	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148
Critical Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution

Infos zu CVE-2017-0143 SMB Remote Code Execution

Mitigations

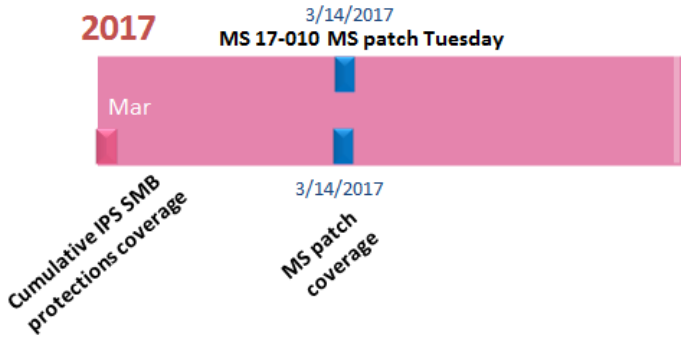
Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

Microsoft has not identified any workarounds for this vulnerability.

Acknowledgments

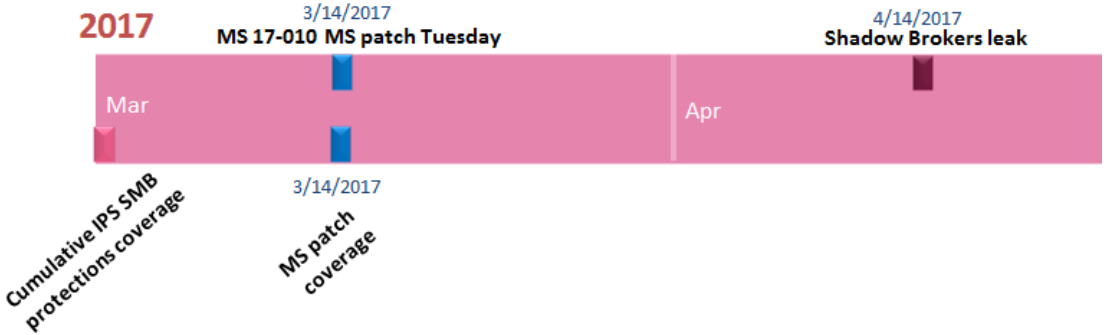
Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure.



Shadow Brokers Fifth leak: "Lost in Translation"

April 14, 2017

Die Shadow Brokers haben über einen Twitter Account einen Tweet mit einem Link zu den geleakten Dateien, verschlüsselt mit dem Password Reeeeeeeeeeeeeee geposted.



14 April 2017

the mysterious "Shadow Brokers" posted some hacking tools for Windows that were allegedly stolen from the NSA. **All of them were at least a few years** old, but exploited flaws in several versions of the operating system to move across networks and infect systems. early Saturday morning, Microsoft has responded with a blog post, saying it has evaluated all of the exploits listed. Its response to the release is surprisingly simple: most of them have already been fixed.

What's particularly curious is that four of the exploits -- **EternalBlue, EternalChampion, EternalRomance and EternalSynergy -- were fixed in an update just last month, on March 14th**. Because "The Shadow Brokers" listed what tools they had in January, it seemed like the NSA had to know this release could happen. Despite a long list of acknowledgments for security issues discovered and fixed in the March 2017 update, …, there's no name listed for the MS17-010 patch that fixed these.

https://www.engadget.com/2017/04/15/microsoft-says-it-already-patched-several-shadow-brokers-nsa-l/

DoublePulsar

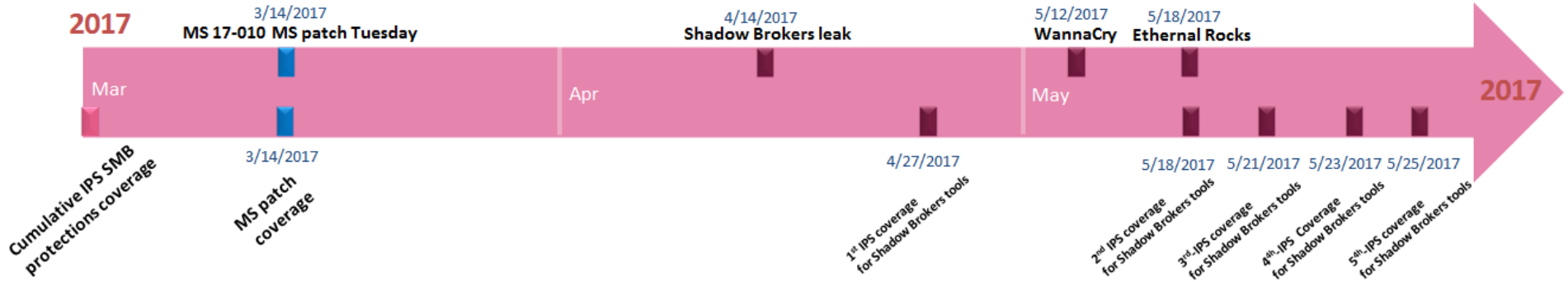
is a backdoor implant tool supposedly developed by the U.S. National Security Agency's (**NSA**) Equation Group that was leaked by The Shadow Brokers in **early 2017**.

Sean Dillon is a senior analyst of security company RiskSense Inc. who first dissected and inspected DoublePulsar. He said that the NSA exploits are **"10 times worse" than the Heartbleed** security bug, and use DoublePulsar as the primary payload. DoublePulsar runs in kernel mode which grants hackers a high level of control over the computer system. Once installed, it has 3 commands: ping, kill, and exec, the latter of which

https://en.wikipedia.org/wiki/DoublePulsar

WannaCry

großer Cyber-Angriff, bei dem über 230.000 Computer in 150 Ländern infiziert wurden



EternalRocks

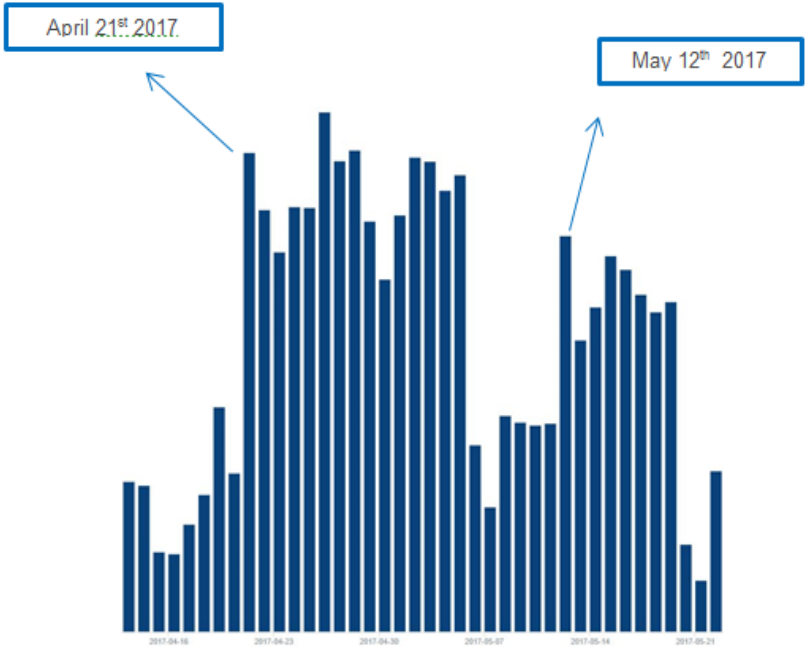
NSA-Exploits: EternalRocks nutzt mehr Schwachstellen als WannaCry

Der Wurm kombiniert sieben der von den Shadow Brokers veröffentlichten NSA-Exploits. Anders als WannaCry transportiert er bislang keine Ransomware oder dergleichen. Die Hintermänner könnten möglichst zahlreiche Infektionen anstreben - um erst dann ihre bösartigen Ziele umzusetzen.

Entdeckt hat den Wurm, der ein ganzes Sammelsurium von Schwachstellen nutzt, Sicherheitsexperte Miroslav Stampar vom kroatischen CERT. EternalRocks machte sich sogar schon am 3. Mai erstmals bemerkbar, berichtet er in seiner Beschreibung auf GitHub. Auf den Wurm aufmerksam wurde er, als dieser eine Honeypot-Falle infizierte.

http://www.zdnet.de/88297887/nsa-exploits-eternalrocks-nutzt-mehr-schwachstellen-als-wannacry/

SMB Attacken monitored by Check Point



IPS SMB protections block rate by date

Total cumulative number of DoublePulsar infections worldwide:

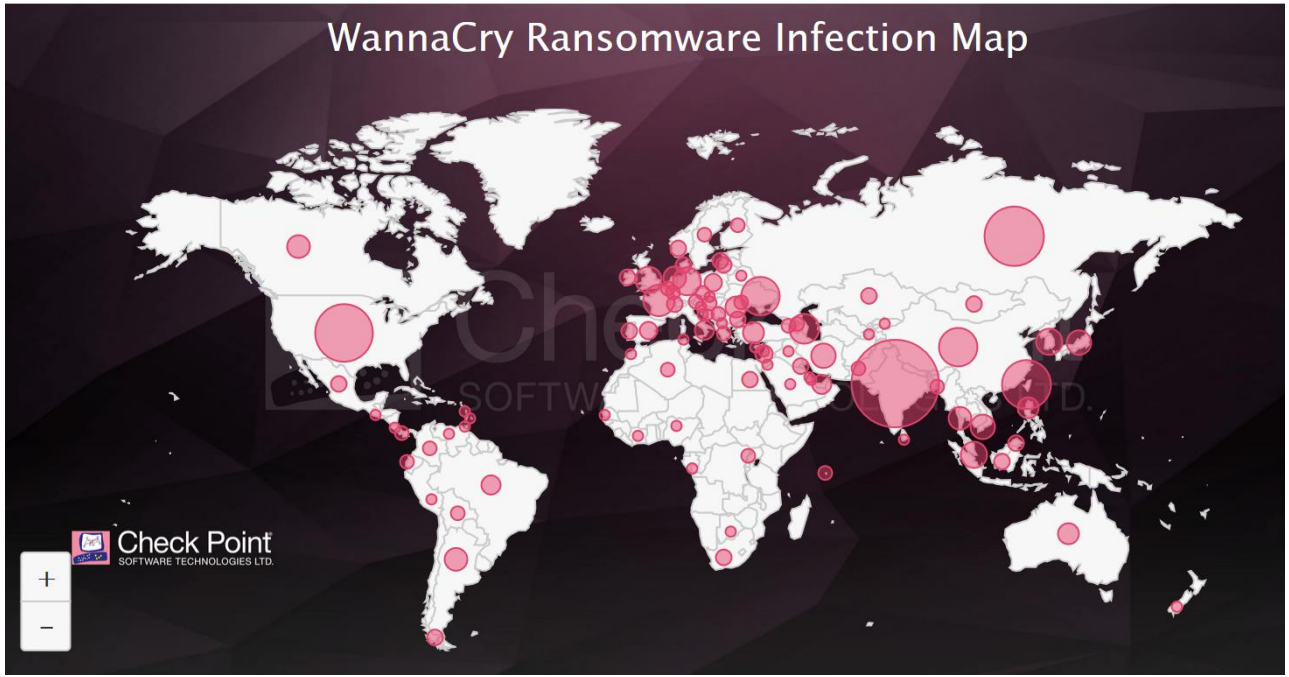
April 21st	106,410
April 22nd	116,074
April 23rd	164,715
April 24th	183,107
April 25th	243,894
April 26th	344,881
April 27th	428,827

https://blog.binaryedge.io/2017/04/21/doublepulsar/

Westcon Comstor

Infektionen Aktuell

- https://attacks.mgmt.cloud/



Eine genaue Analyse der Attacke

- Reconnaissance:
  - **SMBTouch**
  - ArchiTouch
- Exploitation:
  - EternalBlue
  - EternalChampion
  - EternalSynergy
  - EternalRomance
- Backdoor:
  - DoublePulsar

The SMBTouch Reconnaissance tool scans the targets before the attack is launched, and later attaches a detailed report on the target.
The tool **collects its info using legitimate SMB messages** which provide relevant Information about the victim machines.

```
SMB (Server Message Block Protocol)
⊟ SMB Header
    Server Component: SMB
    [Response to: 8]
    [Time from request: 0.000416000 seconds]
    SMB Command: Session Setup AndX (0x73)
    NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016
  ⊞ Flags: 0x98
  ⊞ Flags2: 0xc803
    Process ID High: 0
    Signature: 0000000000000000
    Reserved: 0000
    Tree ID: 0
    Process ID: 65279
    User ID: 4098
    Multiplex ID: 11418
⊟ Session Setup AndX Response (0x73)
    Word Count (WCT): 4
    AndXCommand: No further commands (0xff)
    Reserved: 00
    AndXOffset: 261
  ⊞ Action: 0x0000
    Security Blob Length: 144
    Byte Count (BCC): 218
  ⊞ Security Blob: 4e544c4d5353500002000000c000c003800000
    Native OS: Windows 5.1
    Native LAN Manager: Windows 2000 LAN Manager
```

```
[*] Connecting to target...
        [+] Initiated SMB connection

[+] Target OS Version 5.1 build 2600
    Windows 5.1

[!] Target could be either SP2 or SP3,
[!] for these SMB exploits they are equivalent

[*] Trying pipes...
        [+] spoolss     - Success!

[+] Target is 32-bit

[Not Supported]
        ETERNALSYNERGY  - Target OS version not supported

[Vulnerable]
        ETERNALBLUE     - DANE
        ETERNALROMANCE  - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 3 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded
```

Eine genaue Analyse der Attacke

- Reconnaissance:
  - SMBTouch
  - ArchiTouch
- Exploitation:
  - **EternalBlue**
  - EternalChampion
  - EternalSynergy
  - EternalRomance
- Backdoor:
  - DoublePulsar

EternalBlue exploits (MS17-010) CVE-2017-0144

There is a **buffer overflow** caused by a memmove operation, which leads to a mathematical error, where a DWORD is being cast to a WORD.

The vulnerability exists at SMB_COM_TRANSACTION2_SECONDARY (0x33) request using the malformed fields: Parameters Offset, Data Count and Parameter count. These allow the exploit to inject the DoublePulsar backdoor into the target machine.

19	5.117663	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request
24	5.117860	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
28	5.118052	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
33	5.118274	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
37	5.118460	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
42	5.118661	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
46	5.118831	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
51	5.119048	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
55	5.119244	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
60	5.119446	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
64	5.119624	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
69	5.119824	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
73	5.120009	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
78	5.120231	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
82	5.120409	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]
203	6.345650	10.1.1.82	10.1.1.81	SMB	1287	Trans2 Secondary Request[Malformed Packet]

Eine genaue Analyse der Attacke

- Reconnaissance:
  - SMBTouch
  - ArchiTouch
- Exploitation:
  - **EternalBlue**
  - EternalChampion
  - EternalSynergy
  - EternalRomance
- Backdoor:
  - DoublePulsar

```
◢ SMB (Server Message Block Protocol)
  ◢ SMB Header
      Server Component: SMB
      Continuation to: <unknown frame>
      SMB Command: Trans2 Secondary (0x33)
      NT Status: STATUS_SUCCESS (0x00000000)
    ▷ Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
    ▷ Flags2: 0xc007, Unicode Strings, Error Code Type, Security Signatures, Extended Attributes, Long Names Allowed
      Process ID High: 0
      Signature: 0000000000000000
      Reserved: 0000
    ▷ Tree ID: 2048  (\\10.1.1.81\IPC$)
      Process ID: 65279
      User ID: 2048
      Multiplex ID: 64
  ◢ Trans2 Secondary Request (0x33)
      Word Count (WCT): 9
      Total Parameter Count: 0
      Total Data Count: 4096
      Max Parameter Count: 0
      Max Data Count: 0
      Max Setup Count: 0
      Reserved: 00
    ▷ Flags: 0x1000
      Timeout: 3 days, 20 hours, 19 minutes, 58.645 seconds
      Reserved: 0000
      Parameter Count: 4096
      Parameter Offset: 29747
      Data Count: 30063
      Data Offset: 30072
      ount: 47
      d: 41
      Byte Count (BCC): 21594
```

Total Parameter Count < Parameter Count

Parameter Offset > transaction parameter bytes – SMB Headers

Total Data Count < Data Count

Eine genaue Analyse der Attacke

- Reconnaissance:
  - SMBTouch
  - ArchiTouch
- Exploitation:
  - EternalBlue
  - EternalChampion
  - EternalSynergy
  - EternalRomance
- Backdoor:
  - **DoublePulsar**

Using the above, **DoublePulsar** backdoor is delivered to the target machine encoded in base64:

```
0000261B  00 00 10 35 ff 53 4d 42  33 00 00 00 00 18 07 c0  ...5.SMB 3.......
0000262B  00 00 00 00 00 00 00 00  00 00 00 00 00 08 ff fe  ........ ........
0000263B  00 08 40 00 09 00 00 00  10 00 00 00 00 00 00 00  ..@..... ........
0000264B  10 35 00 d0 23 00 00 00  10 58 46 43 63 38 36 49  .5..#... .XFCc86I
0000265B  72 67 53 37 4c 69 55 6a  58 34 71 78 32 39 55 4e  rgS7LiUj X4qx29UN
0000266B  63 36 70 7a 52 63 43 79  75 49 39 46 4a 69 49 2f  c6pzRcCy uI9FJiI/
0000267B  42 50 6c 4c 59 39 6a 67  73 70 59 70 4f 6a 64 42  BPlLY9jg spYpOjdB
0000268B  36 51 39 63 68 78 41 4d  6c 4d 74 53 75 41 68 54  6Q9chxAM lMtSuAhT
0000269B  6d 68 43 4d 56 76 57 48  70 37 32 71 59 74 53 47  mhCMVvWH p72qYtSG
000026AB  30 52 61 45 76 67 58 6e  4d 63 49 6d 70 6f 36 48  0RaEvgXn McImpo6H
000026BB  48 30 53 74 73 4f 4a 57  31 49 42 33 57 5a 6f 50  H0StsOJW 1IB3WZoP
000026CB  4b 37 6d 55 64 2f 59 4a  4e 41 34 47 63 39 39 79  K7mUd/YJ NA4Gc99y
000026DB  61 46 63 36 39 45 6f 79  55 34 59 63 5a 2f 6b 79  aFc69Eoy U4YcZ/ky
000026EB  74 2b 6a 5a 65 6a 30 59  70 50 70 4a 2b 7a 64 6c  t+jZej0Y pPpJ+zdl
000026FB  47 35 43 68 6a 62 4a 32  62 33 4c 42 34 77 70 2f  G5ChjbJ2 b3LB4wp/
0000270B  62 69 73 34 58 63 77 47  57 53 66 79 33 6b 32 31  bis4XcwG WSfy3k21
0000271B  59 5a 61 5a 53 61 55 65  41 2b 70 63 51 52 55 6c  YZaZSaUe A+pcQRUl
0000272B  5a 62 31 37 51 68 6e 6d  53 4a 76 31 57 6f 5a 59  Zb17Qhnm SJv1WoZY
0000273B  74 6e 6c 55 37 74 43 44  6d 69 54 44 74 46 2b 30  tnlU7tCD miTDtF+0
0000274B  58 75 4f 70 55 35 72 54  79 4e 37 59 4e 4e 42 47  XuOpU5rT yN7YNNBG
0000275B  37 62 31 63 4d 45 6f 71  71 56 59 51 4f 54 6c 67  7b1cMEoq qVYQOTlg
0000276B  70 43 44 77 4d 6c 30 6a  65 4e 45 47 77 44 68 48  pCDwMl0j eNEGwDhH
0000277B  37 37 39 6c 62 76 4f 54  79 30 64 46 6a 38 78 47  779lbvOT y0dFj8xG
0000278B  48 55 30 36 55 4e 6a 32  78 61 43 36 52 69 51 2b  HU06UNj2 xaC6RiQ+
```

This leads us to the 3 basic commands
1.0x23 – Checks if a backdoor is installed.
2.0xc8 – Loads DLL or Executes shell code.
3.0x77 – Uninstalls the backdoor.

http://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/

Warum Sandboxing?

Styx Crypt — first online F

https://styx-crypt.com/?language=en

2012-10-23
At the current time we do maintenance work. Normal operation of the service will be restored in a few days.

2012-10-15
Service is now in maintenance mode.

2012-10-14
chk4me.com check has been temporarily disabled due to service unavailability.

2012-10-08
IFrame / JS cryptor is clear.

2012-09-07
Payments via Liberty Reserve is temporarily unavailable due to technical reasons.

2012-09-05
Update is complete, service is active.

Our services

HTML Morphing (FUD)
HTML, PHP, ASP polymorphing obfuscation. Quick and stable. Now with JavaScript obfuscation.

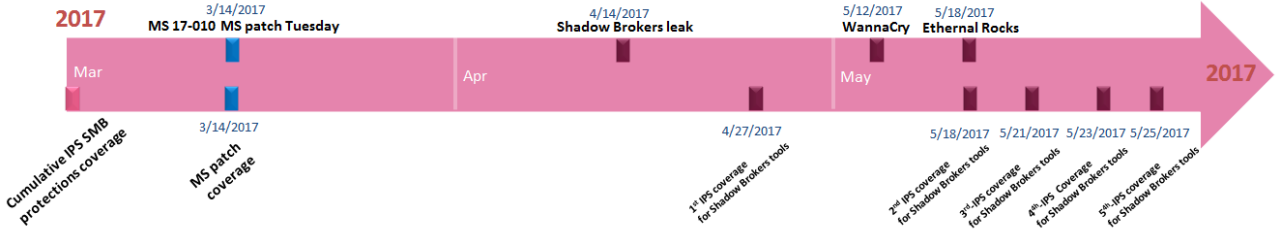
JavaScript Morphing (FUD)
First stable JavaScript polymorphic obfuscation. Every time clean. Every time fast.

EXE / DLL FUD Morphing (Coff PE)
Unique engine. x32 and x64 architecture support. Three times a day update. EXEs < 160 Kib. Small stub. We have private crypt.

PDF FUD Morphing
Your documents protection. Internal scripts obfuscation.

Adobe Flash FUD / Morphing
SWF (Action Script) Obfuscation. First on market.

IFrame FUD / Morphing
IFrame morphing. New level. Now polymorphic.



Sandbox Lösungen einzelner Hersteller

- Paloalto
  - WildFire™ cloud-based threat analysis
  - TRAPS ADVANCED ENDPOINT PROTECTION
- Checkpoint
  - Sandblast
- FireEye
  - AX-Serie forensische Analyseplattform
- Trendmicro
  - Deep Discovery Sandboxing + Smart Protection Network™
  - DEEP DISCOVERY ANALYZER is an open custom sandbox analysis server

WannaCry Report aus der Sandbox

Malware Report

Check Point SOFTWARE TECHNOLOGIES LTD.

Emulated On: Microsoft Windows 7 32 bit, Office 2013, Adobe Acrobat Reader 11.0, Adobe Flash Player 12, Java SE 1.7.0

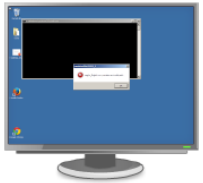
1

@WanaDecryptor@.exe

Malicious Activity Detected

Type	exe
Size	240.0 KB
MD5	7bf2b57f2a205768755c07f238fb32cc
SHA1	45356a9dd616ed7161a3b9192e2f318d0ab5ad10

Download malicious file



Emulation Screenshot

3 Suspicious Activities

Behaves like a known malware (Generic.MALWARE.764b)
Malware detected (Generic.Ransom.HydraCrypt.C8B435F4)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.qyfrf)

0 Affected Processes

0 Processes Created | 0 Processes Terminated | 0 Processes Crashed

3 Affected Registry Keys

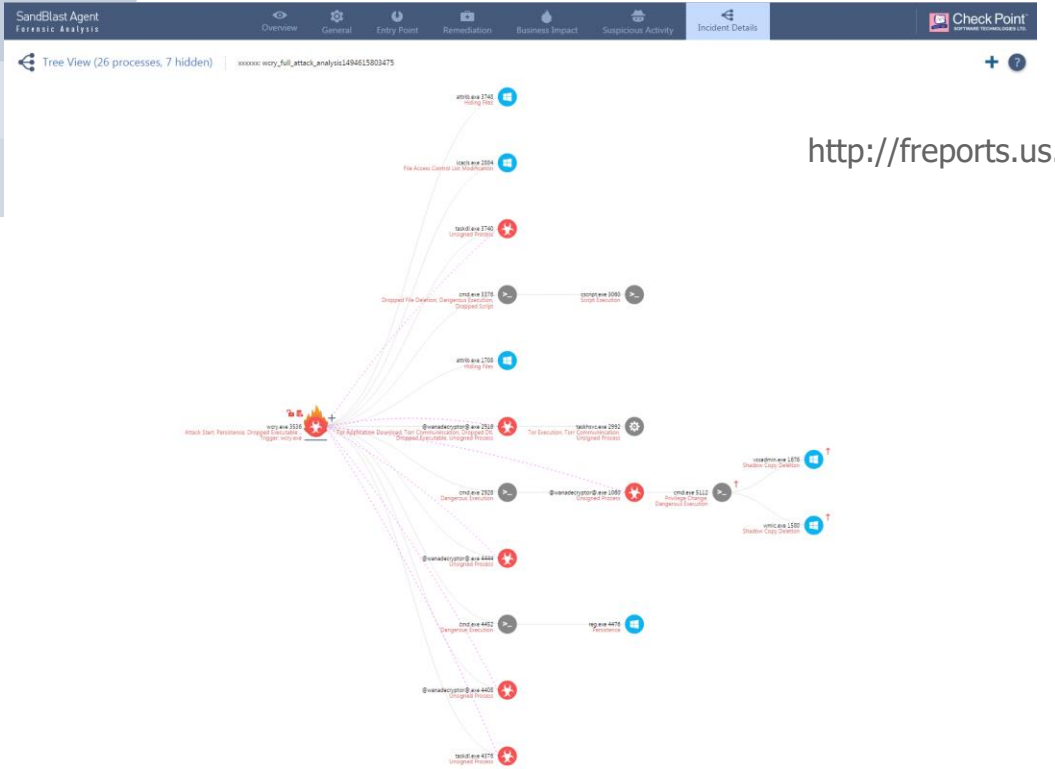
3 Entries Set | 0 Entries Deleted

HKCU\Control Panel\Desktop\Wallpaper
HKCU\Software\WanaCrypt0r
\Registry\User\S-1-5-21-292738990-2461527479-3432112557-1000_Classes\Vir...

0 Affected Files

0 Files Created | 0 Files Modified | 0 Files Deleted

1/6



http://freports.us.checkpoint.com/wannacryptor2_1/index.html

WildFire Report

1 File Information

File Type	PE
File Signer	
SHA-256	bd93a2c673bf90a08bd9ff31f1c023da2d722d3c0ca5bb09462865580e7a41ac
MD5	d11931c7016a350cbf5e0da0352ae514
File Size	739884 bytes
First Seen Timestamp	2013-09-26 23:45:24 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Dynamic Analysis

2.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

2.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior
Created a file in the Windows folder
Created or modified files
Installed a browser helper object
Spawned new processes
Modified Windows registries
Changed security settings of Internet Explorer
Created an executable file in a user document folder

2.1.2. Network Activity

No network data available.

2.1.3. Host Activity

Process Name - .\4IR4OuzYg.exe

(command: .\4IR4OuzYg.exe)

File Activity

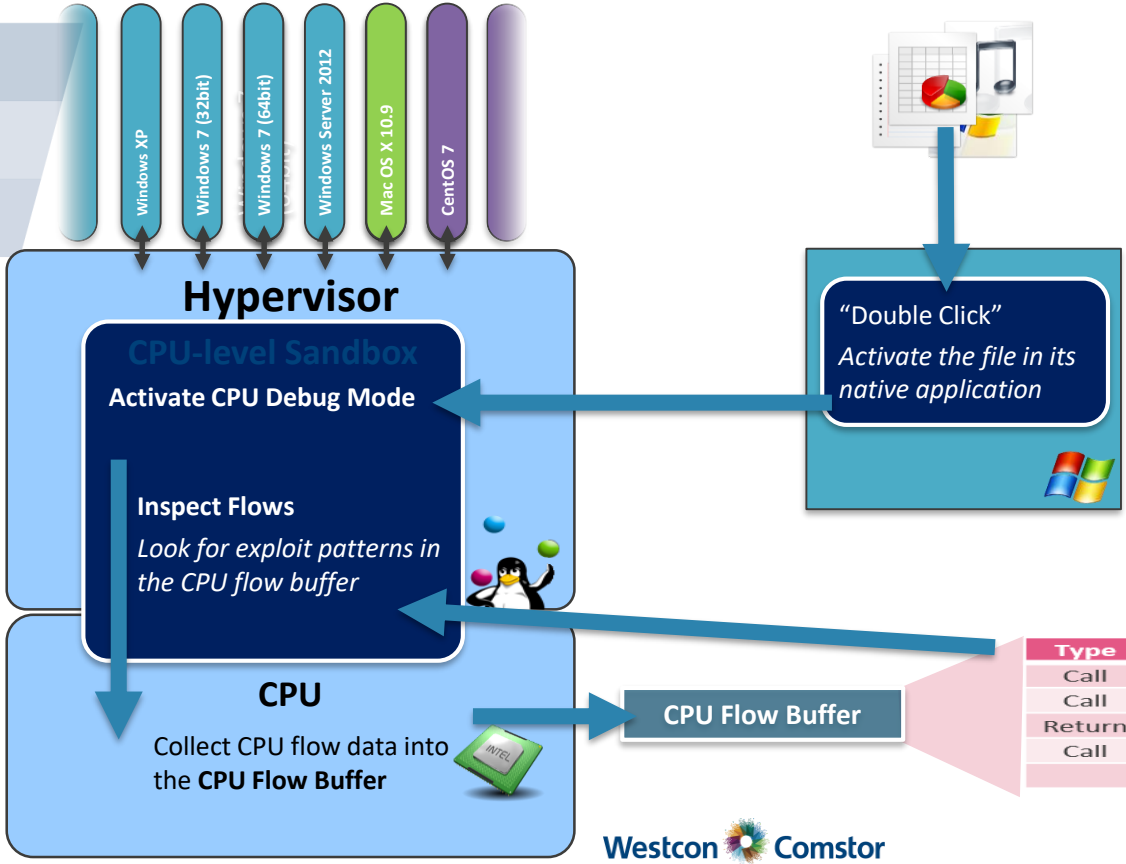
File	Action
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\bootstrap.js	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\chrome.manifest	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\content\bg.js	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\install.rdf	Create
C:\Documents and Settings\All Users\Application Data\WXDownlooAed\mqJ4V1qD.dll	Create

Check Point Tool-B-Gone Root Kit

SandBlast – Superior Anti-Evasion

- Malware usually cannot detect Rootkit!
- The solution is to Install a rootkit on the analysis machine
  - Hide files/processes/drivers
  - Hide open ports
  - Hide registry values
- Malware is not aware that it is being subverted

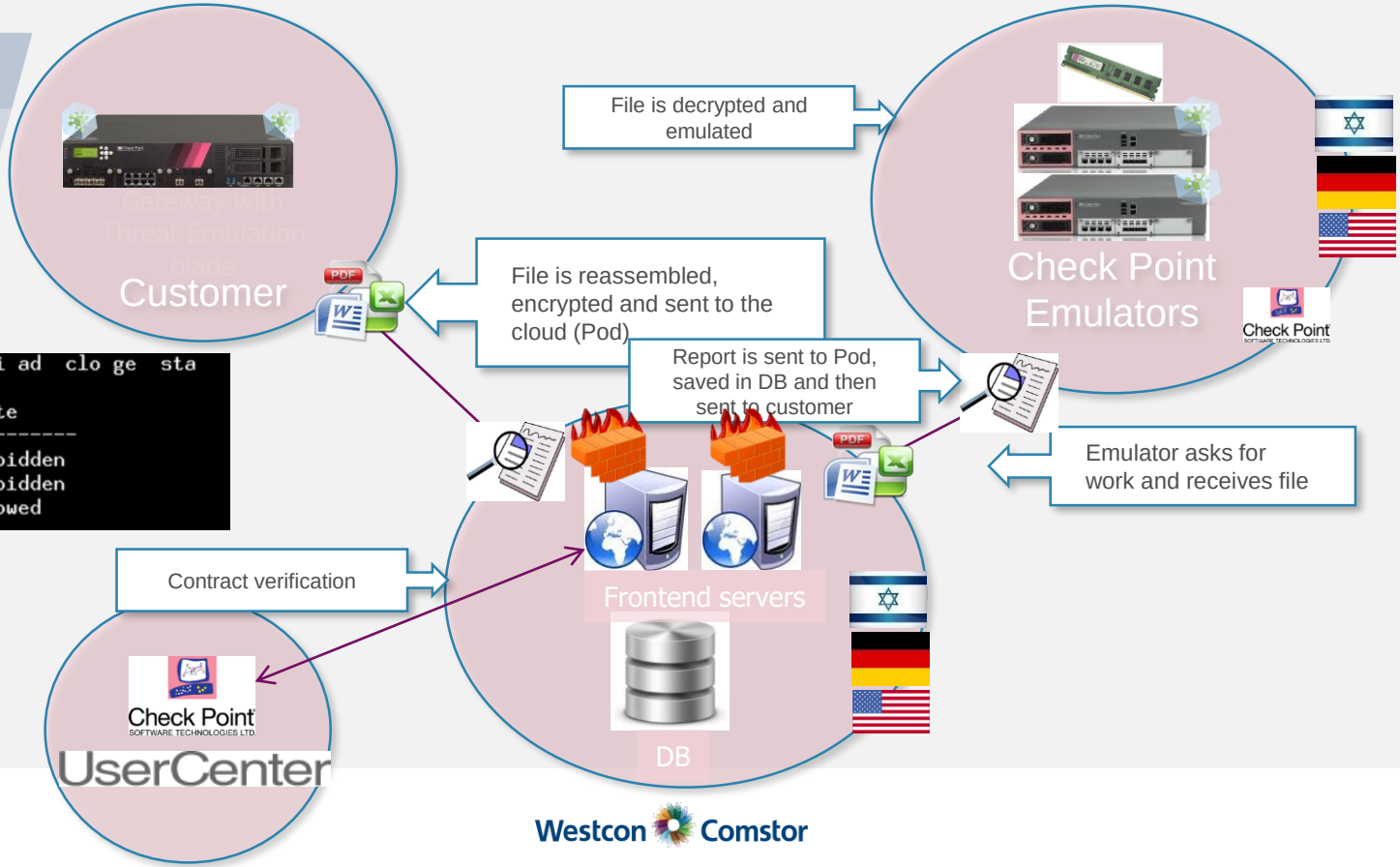
CPU-Level Sandbox



Type	From	To
Call	from_addr_1	to_addr_1
Call	from_addr_2	to_addr_2
Return	from_addr_3	to_addr_3
Call	from_addr_4	to_addr_4
	...	...

Westcon Comstor

SandBlast Cloud Overview




```
[Expert@HOT:0]# tecli ad  clo ge  sta

|Country        |State
|---------------|----------
|Germany        |forbidden
|Israel         |forbidden
|USA            |allowed
```

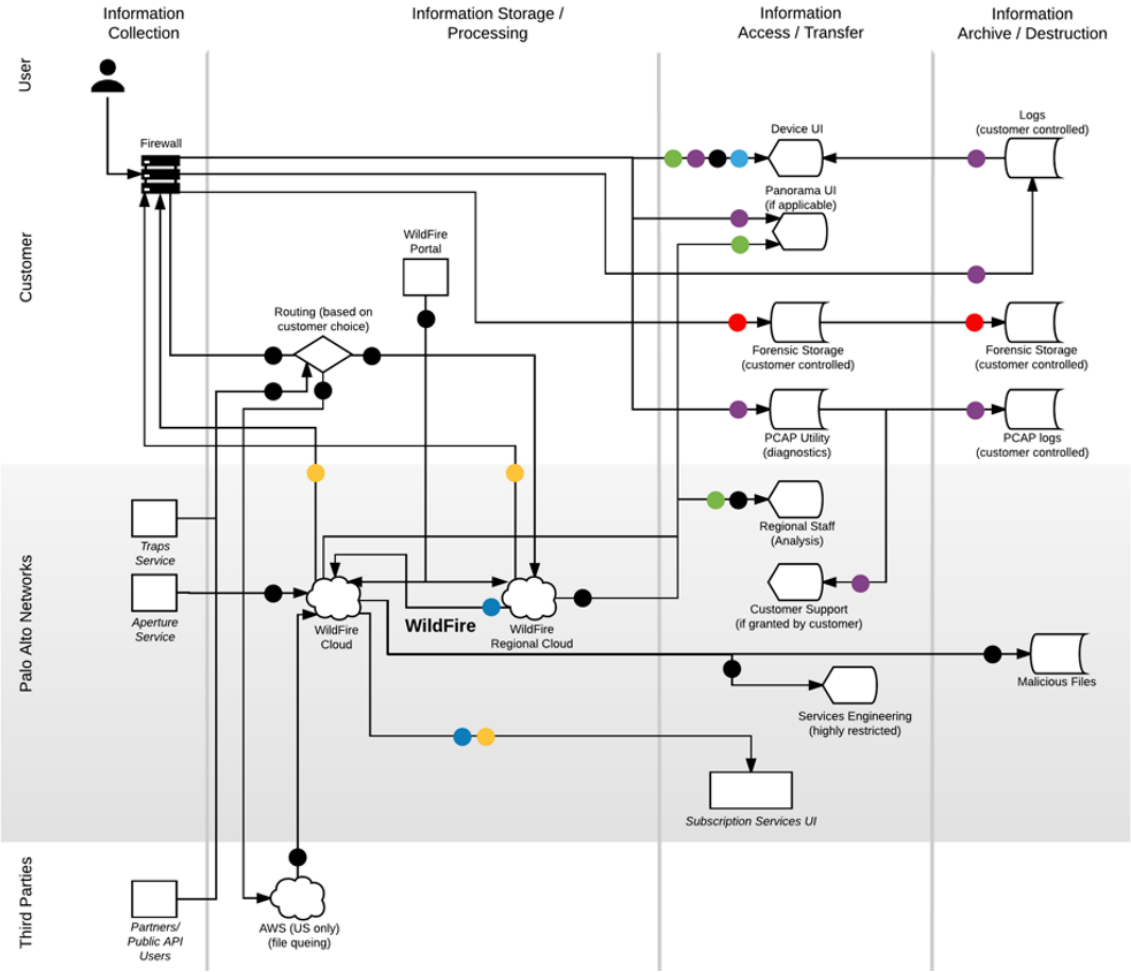
Fluss der Daten

WildFire

Legend

- Files and Session data (source and destination IP addresses and ports, username (if enabled by customer), filename (may include path), email sender/recipients/subject)
- Protections & analysis reports available globally (contains no PII)
- All data passing through firewall (unencrypted)
- Verdict
- Device/Service-specific or UI log data (see reference links for complete specifications)
- Analysis reports, usage statistics and system logs (may contain PII) (see service data sheets for more information)

wildfire-privacy-datasheet.pdf

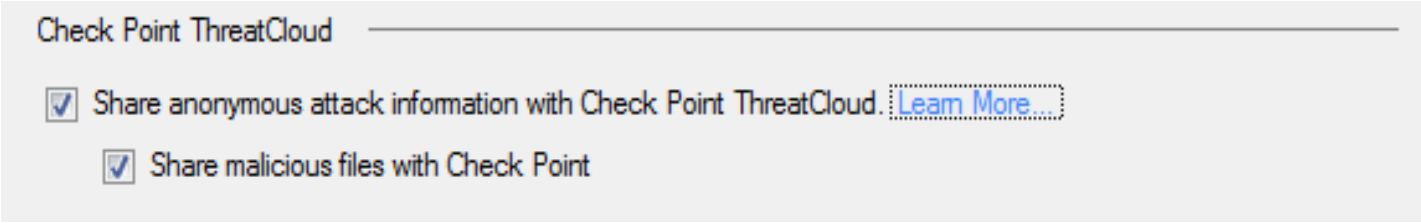


Welche Informationen wandern in die Cloud?

Data type (May be shared with Palo Alto Networks based on customer's configuration)	
Source IP = IP address that sent the unknown file	Filename = the name of the unknown file
Destination IP = destination IP address for the unknown file	Email sender/ recipient/ subject) = the sender of an unknown email link (the name of the email sender also appears in WildFire logs and reports)
Port = source port that sent the unknown file	
Virtual system = virtual system that detected the unknown file	Application/User agent = the user application that transmitted the unknown file
User/User group = targeted user	URL = the URL associated with the unknown file

Threat Emulation Sharing with Check Point

- There are two levels of sharing
  - **Anonymous attack information**
    - Includes – MD5, SHA1, file type, execution report
  - **Malicious files information**
    - Includes – File name, file, sender, recipient, mail subject and URL
- Sharing information with AB/AV
  - When one of the sharing options is enabled the attack information is also being sent to our AV/AB so they will detect these indicators as malicious as well.



Sicherheits Erklärungen der Hersteller

Paloalto Wildfire

- Security of Data in Wildfire Session data sent from firewalls to the WildFire cloud is encrypted in transit. In the EU the transit does not involve any third party. All data received into the cloud is encrypted while at rest. Palo Alto Networks has also achieved SOC2 certification for its WildFire U.S.-based data centers to demonstrate its strong security policies and internal controls environment

How do we assure privacy with the SandBlast Cloud Service?

- Please read and refer to Check Point privacy statement and the Check Point Cloud Services Security Statement pdf.

Aber was passiert im Falle einer infizierten Datei?

- **Malware Research** Files that are detected as malicious may be stored by Check Point to enable vulnerability research. Detected malicious files are made available to designated Check Point security researchers, for in-depth threat analysis of infected files. [1]

- **Access by Palo Alto Networks** Within Palo Alto Networks, access to the WildFire production system is restricted to the teams that perform the analysis of the samples, generate reports and signatures, and test signatures for efficacy. This may include team members from WildFire threat research and engineering [2]

[1] Check_Point_Cloud_Services_Security_Statement_2015_UP.pdf
[2] wildfire-privacy-datasheet.pdf

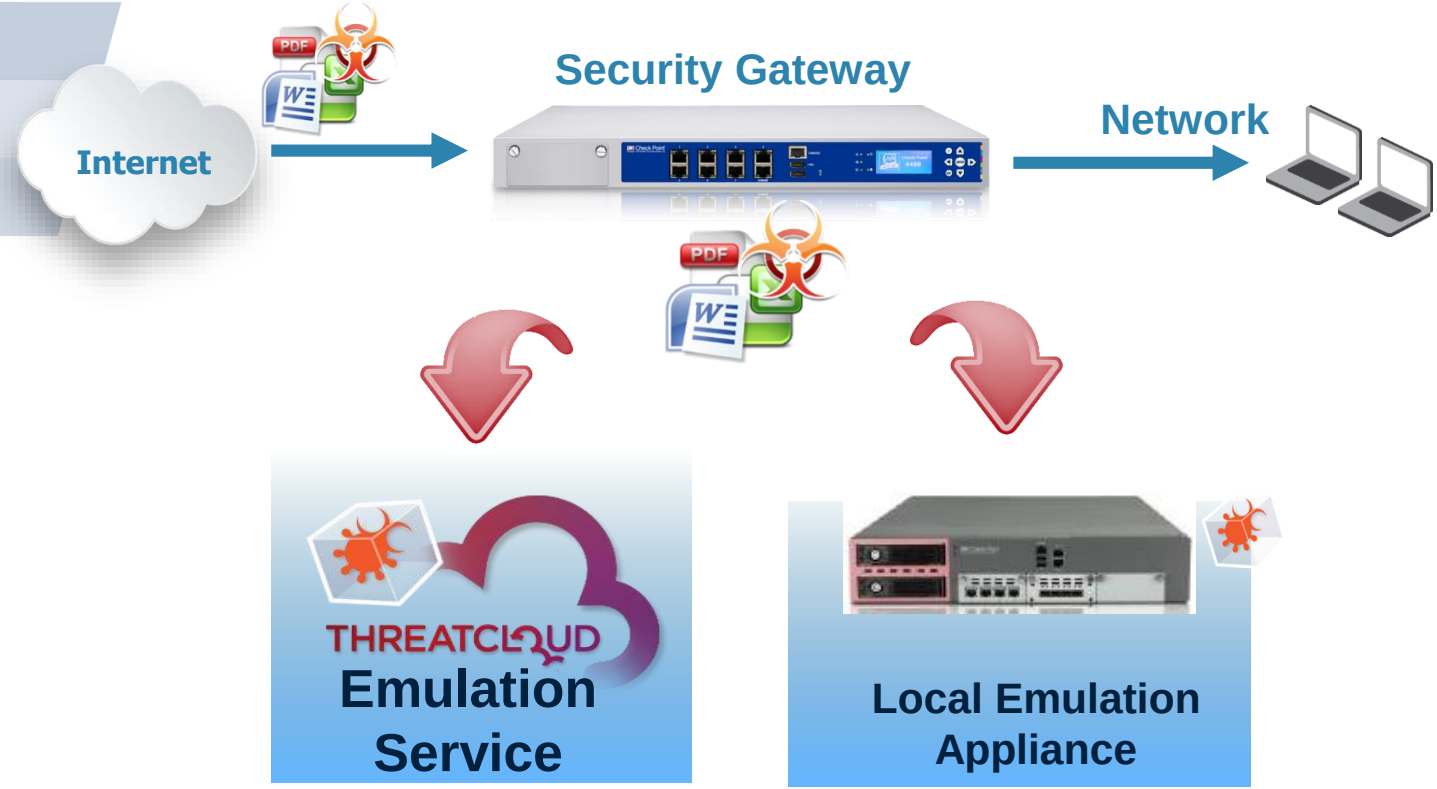
Who Do you Trust

Sharing expertise and threat intelligence within the "commons" -- resources affecting an entire community -- **enhances the ability of the good guys to respond to the bad guys**. Rather than operating in isolated silos, the "sharing" -- sourcing from the crowd -- enables a collective defense that, though not tipping the balance totally in favor of the good guys, certainly improves the potential for a more powerful defense.

The challenge, of course, is how to source from the crowd when trust and transparency are the watchwords of cyber security. **How do you ensure the veracity of submissions ("attribution"), represented as the work of good guys and not a potential "Trojan Horse,"** in a world where anonymity is the norm and may in fact be a legal requirement? How do you establish an audit trail of accountability to ensure trust and transparency? How do you create an incentive system that rewards contributions from the best and brightest

http://www.darkreading.com/analytics/crowdsourcing-and-cyber-security-who-do-you-trust/a/d-id/1278747

Sandblast TE Appliance



Cloud/Local pros and cons

Feature	Cloud Pro	Cloud Con	Local Pro	Local Con
Privacy	N/A	Not everyone can use cloud. Files must be shared	Files are kept on site, control what is shared	N/A
Latency	Previous malicious verdicts are in cloud (fast response)	Files need to be uploaded (often slower than download)	Ethernet speed from collection to SandBlast Appliance	
Data samples	Huge data sample set	N/A	Local gateway knows your files best	Dataset is smaller

Cloud/Local pros and cons

Feature	Cloud Pro	Cloud Con	Local Pro	Local Con
Custom images	N/A	Cant be done	Possible	N/A
Alternative OS images (e.g. OSX)	Possible, with licensing permission	N/A	N/A	Not possible due to licensing
Image updates	Automatic and transparent	N/A	N/A	Must be downloaded and scheduled to not disrupt scanning
Multi Site deployment	Cloud can work with any size CP gateway	Some gateways perform too many emulations, and need local	Can offer appliances for all business sizes and TE can be load balanced	More hardware

Performance deep discovery analyzer Model 100 (Trend)

- Capacity
  - 20,000 samples/day
- supported File types
  - exe, dll, swf, lnk, doc, docx, ppt, pptx, xls, pdf, hwp, cell, jtd, rtf, gul, jar, chm

Performance FireEye

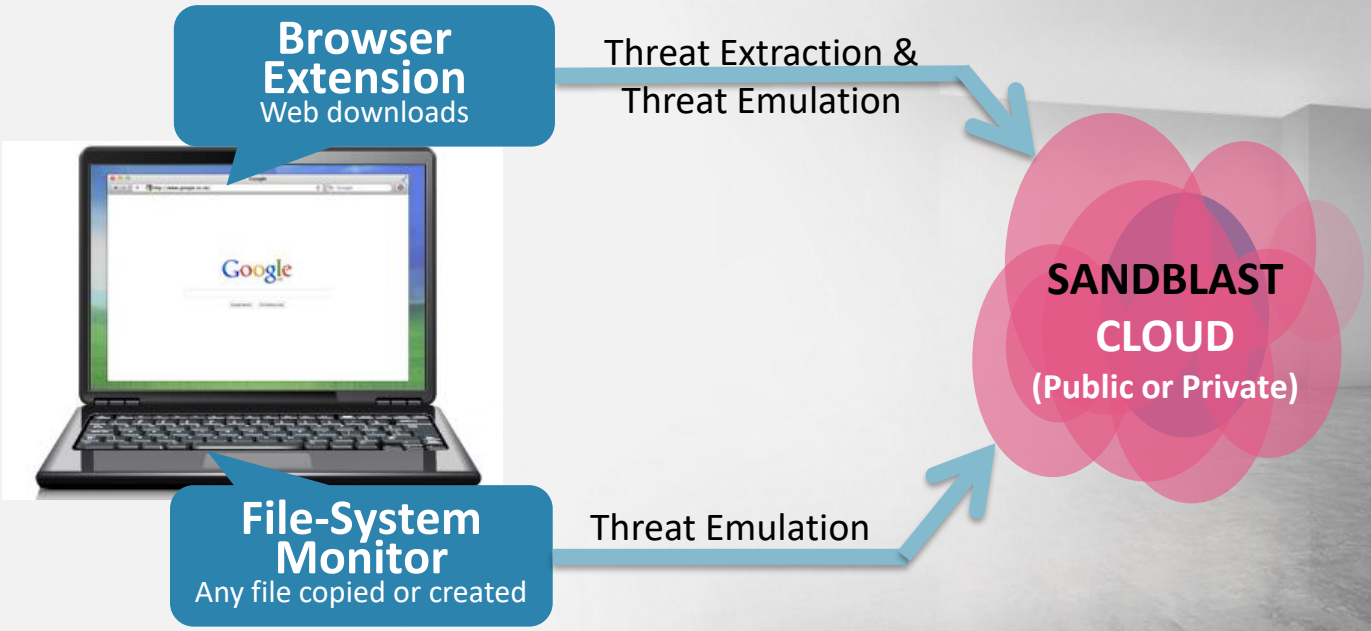
	AX 5400	AX 5500	AX 8400
Leistung*	Bis zu 8.200 Analysen pro Tag	Bis zu 8.000 Analysen pro Tag	Bis zu 16.000 Analysen pro Tag
Unterstützte Betriebssysteme	Microsoft Windows	Microsoft Windows Apple Mac OS X	Microsoft Windows

Performance Check Point

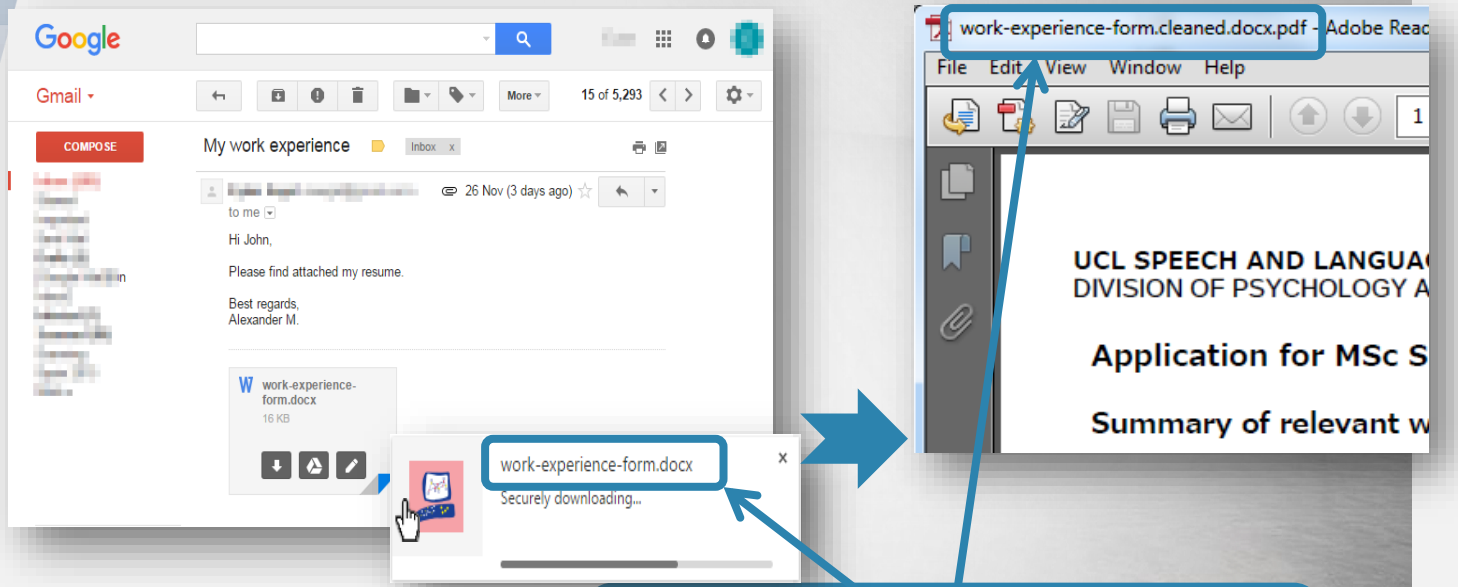
How much time does it take to emulate a file?
Full emulation takes 60-70 seconds. The system can hold files until emulation has completed in the following configurations:
- For web downloads when the system is configured in-line
- For mail attachments when using a “Message Transport Agent” (MTA) topology on the Security Gateway
- For mail attachments when using the agent for exchange server

	TE100X	TE250X	TE1000X	TE2000X	TE2000X HPP
					
Performance					
Recommended files/month	100K	250K	1M	1.5M	2M
Recommended users	Up to 1,000	Up to 3,000	Up to 10,000	Up to 20,000	
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps	
Virtual machines	4	8	28	40	56

Zero-day Protection für den Client



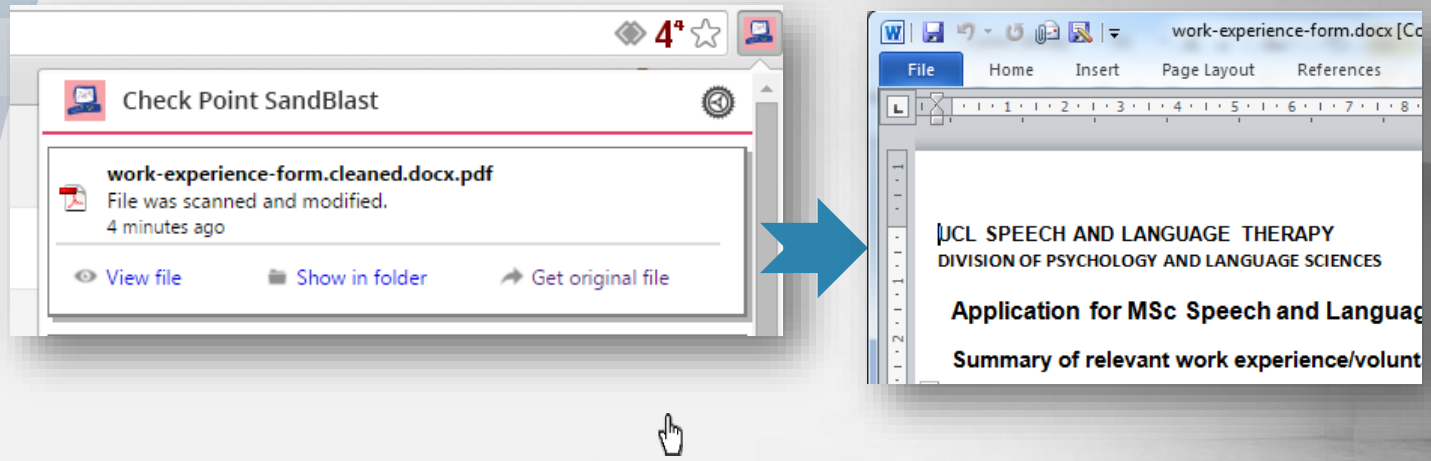
Instant Protection für Web Downloads



Konvertiert Datei in ein PDF

Zugriff auf das Original

After Threat Emulation is Completed



Automatisiert
kein Helpdesk notwendig

Vielen Dank

Thomas Hesse
Senior System Engineer
Thomas.Hesse@westcon.com
+49 5251 14560

Westcon Comstor
Delivering Results Together
powered by WestconGroup

Cloud Global Deployment Services

Security UCC Networking Data Center

Westcon Comstor

Delivering Results Together

powered by WestconGroup

Cloud Global Deployment Services

Security UCC Networking Data Center