

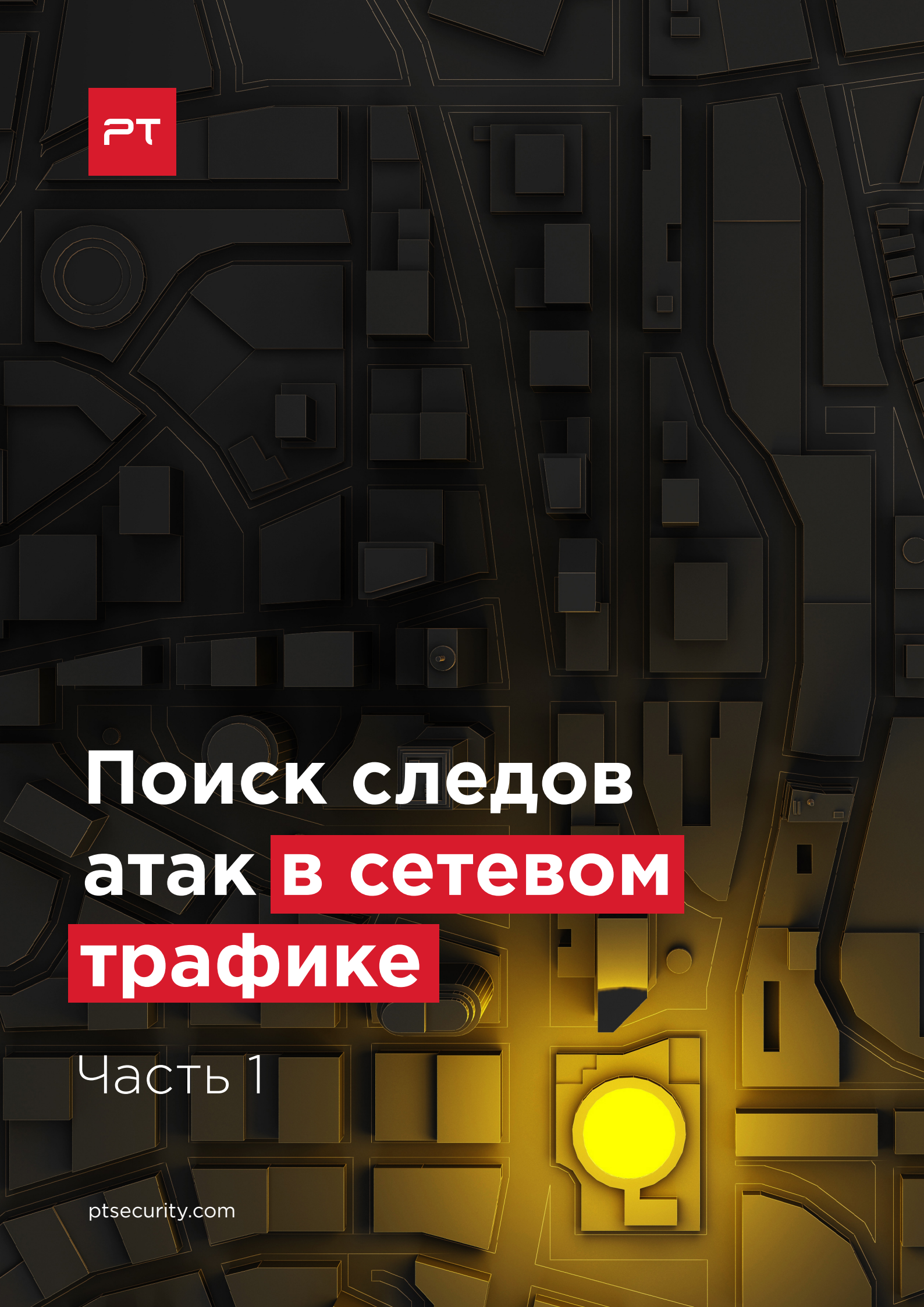


PT

# Поиск следов атак **в сетевом** **трафике**


Часть 1

ptsecurity.com



## **Содержание**

Windows admin shares	3
Windows Management Instrumentation	6
Pass the hash	7
Credential dumping	8
Brute force	9
Подведем итог	10



Г Проводя целенаправленную атаку, нарушитель не может быть уверен, что после проникновения в локальную сеть организации он окажется в нужном ему сегменте сети. Для поиска ключевых серверов и рабочих станций потребуется разведка и ряд подключений между узлами. Такие подключения, или, как обычно говорят, **перемещение хакера внутри периметра**, — непременно оставят следы в сетевом трафике. Их можно отследить, а значит, своевременно обнаружить кибератаку. Если сохранять копию трафика, анализ можно проводить и ретроспективно.

Удаленное выполнение команд на компьютерах с использованием связки из техник Windows admin shares и service execution, а также применение технологии Windows Management Instrumentation (WMI) — одни из распространенных техник перемещения внутри периметра<sup>1</sup>. Эти же техники лежат в основе некоторых утилит для администрирования, которыми также пользуются злоумышленники, в частности psexec и wmicexec из набора Impacket. С их помощью злоумышленники могут осуществлять различные действия, например передавать файлы между узлами (remote file copy), создавать задачи, выполняющиеся по расписанию (scheduled task), или собирать информацию о пользователях (account discovery).

Учетные данные для подключения к удаленным узлам, и в том числе учетные данные администратора домена, злоумышленники, как правило, извлекают из оперативной памяти или реестра ОС. Эта техника называется credential dumping, таким образом злоумышленники получают пароли в открытом виде или их хеши. В свою очередь, техника pass the hash позволяет подключаться к удаленным узлам, зная только хеш пароля пользователя. Впрочем, некоторые атакующие прибегают и к подбору паролей (brute force). Хотя это достаточно грубый подход, существуют методы, с помощью которых атаку можно проводить более незаметно, а благодаря тому, что в компаниях часто используются словарные или простые пароли даже для административных учетных записей ([bit.ly/2PMftnV](https://bit.ly/2PMftnV)), такие методы дают результат.

Рассмотрим, как обнаруживать в трафике признаки использования перечисленных техник.

---

1. В статье используется терминология MITRE ATT&CK.



## Windows admin shares

Для перемещения между компьютерами сети могут использоваться общие сетевые ресурсы, доступ к которым имеют только локальные администраторы узла (техника Windows admin shares). Среди них есть такой сетевой ресурс, как IPC\$ (Inter-Process Communication). Он предоставляет интерфейс для удаленного вызова процедур (RPC), через который можно обратиться к менеджеру сервисов Service Control Manager (SCM). Менеджер сервисов позволяет запускать, останавливать сервисы и взаимодействовать с ними (техника service execution). Эти две техники работают вместе для копирования исполняемого файла на удаленный компьютер и его запуска либо для удаленного выполнения команд через RPC.

Копирование и запуск исполняемого файла происходят следующим образом. Сперва происходит подключение к ресурсу ADMIN\$ (C:\Windows), куда помещается файл. Затем необходимо подключиться к ресурсу IPC\$ и обратиться с его помощью к интерфейсу SCM для создания и старта сервиса, который запустит скопированный файл. Все это происходит поверх протокола SMB.

Protocol	Length	Info
SSDP	215	M-SEARCH * HTTP/1.1
SSDP	215	M-SEARCH * HTTP/1.1
SSDP	215	M-SEARCH * HTTP/1.1
SSDP	215	M-SEARCH * HTTP/1.1
TCP	66	56726 → 445 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
ARP	42	who has 192.168.202.100? Tell 192.168.202.101
ARP	42	192.168.202.100 is at 00:0c:29:c5:12:03
TCP	66	445 → 56726 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP	54	56726 → 445 [ACK] Seq=1 Ack=1 Win=525568 Len=0
SMB	213	Negotiate Protocol Request
SMB2	306	Negotiate Protocol Response
SMB2	232	Negotiate Protocol Request
SMB2	306	Negotiate Protocol Response
TCP	1514	56726 → 445 [ACK] Seq=338 Ack=505 Win=525056 Len=1460 [TCP segment of a reassembled data stream]
SMB2	413	Session Setup Request
TCP	54	445 → 56726 [ACK] Seq=505 Ack=2157 Win=65536 Len=0
SMB2	315	Session Setup Response
SMB2	158	Tree Connect Request Tree: <b>\\WIN01\ADMIN\$</b>
SMB2	138	Tree Connect Response
SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
SMB2	131	Ioctl Response, Error: STATUS_FILE_CLOSED
SMB2	346	Create Request File: PSEXESVC.exe
SMB2	386	Create Response File: PSEXESVC.exe
TCP	1514	56726 → 445 [ACK] Seq=2711 Ack=1259 Win=524288 Len=1460 [TCP segment of a reassembled data stream]
TCP	1514	56726 → 445 [ACK] Seq=4171 Ack=1259 Win=524288 Len=1460 [TCP segment of a reassembled data stream]
TCP	1514	56726 → 445 [ACK] Seq=5631 Ack=1259 Win=524288 Len=1460 [TCP segment of a reassembled data stream]
TCP	1514	56726 → 445 [ACK] Seq=7091 Ack=1259 Win=524288 Len=1460 [TCP segment of a reassembled data stream]

Рисунок 1. Обращение к ресурсу ADMIN\$

RPC может работать не только поверх SMB, но и поверх чистого TCP (без использования протокола прикладного уровня). В этом случае последовательность действий такова: злоумышленник подключается к IPC\$, обращается к какому-либо сервису и отправляет ему команды.



Чтобы выявлять в трафике подключения к общим ресурсам и передачу файлов, нужно уметь разбирать протокол SMB и извлекать передаваемые файлы.



Destination	Protocol	Length	Info
192.168.202.100	SMB2	306	Negotiate Protocol Response
192.168.202.101	SMB2	232	Negotiate Protocol Request
192.168.202.100	SMB2	306	Negotiate Protocol Response
192.168.202.101	SMB2	413	Session Setup Request
192.168.202.100	SMB2	315	Session Setup Response
192.168.202.101	SMB2	158	Tree Connect Request Tree: \\WIN01\ADMIN\$
192.168.202.100	SMB2	138	Tree Connect Response
192.168.202.101	SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
192.168.202.100	SMB2	131	Ioctl Response, Error: STATUS_FILE_CLOSED
192.168.202.101	SMB2	346	Create Request File: PSEXESVC.exe
192.168.202.100	SMB2	386	Create Response File: PSEXESVC.exe
192.168.202.101	SMB2	1466	Write Request Len:65536 Off:0 File: PSEXESVC.exe
192.168.202.101	SMB2	1466	Write Request Len:65536 Off:65536 File: PSEXESVC.exe
192.168.202.100	SMB2	138	Write Response
192.168.202.100	SMB2	138	Write Response
192.168.202.101	SMB2	778	Write Request Len:12288 Off:131072 File: PSEXESVC.exe
192.168.202.100	SMB2	138	Write Response
192.168.202.101	SMB2	918	Write Request Len:2208 Off:143360 File: PSEXESVC.exe
192.168.202.100	SMB2	138	Write Response
192.168.202.101	SMB2	146	Close Request File: PSEXESVC.exe
192.168.202.100	SMB2	182	Close Response

Рисунок 2. Передача файла psexecsvc.exe



Запросы к SCM выявляются в трафике путем разбора вызовов DCE/RPC и поиска обращений к SVCCTL — интерфейсу менеджера сервисов SCM: OpenServiceW(), StartServiceW().

Time	Source	Destination	Protocol	Length	Info
2019-01-23 13:39:15.301693	192.168.202.101	192.168.202.100	SMB2	306	Negotiate Protocol Response
2019-01-23 13:39:15.314294	192.168.202.100	192.168.202.101	SMB2	413	Session Setup Request
2019-01-23 13:39:15.315541	192.168.202.101	192.168.202.100	SMB2	315	Session Setup Response
2019-01-23 13:39:15.316004	192.168.202.100	192.168.202.101	SMB2	154	Tree Connect Request Tree: \\WIN01\IPC\$
2019-01-23 13:39:15.316166	192.168.202.101	192.168.202.100	SMB2	138	Tree Connect Response
2019-01-23 13:39:15.316319	192.168.202.100	192.168.202.101	SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
2019-01-23 13:39:15.316461	192.168.202.101	192.168.202.100	SMB2	131	Ioctl Response, Error: STATUS_FILE_CLOSED
2019-01-23 13:39:15.317171	192.168.202.100	192.168.202.101	SMB2	190	Create Request File: svcctl
2019-01-23 13:39:15.317426	192.168.202.101	192.168.202.100	SMB2	210	Create Response File: svcctl
2019-01-23 13:39:15.317626	192.168.202.100	192.168.202.101	DCE/RPC	200	Bind: call_id: 2, Fragment: Single, 2 context items
2019-01-23 13:39:15.317765	192.168.202.101	192.168.202.100	SMB2	138	Write Response
2019-01-23 13:39:15.317942	192.168.202.100	192.168.202.101	SMB2	171	Read Request Len:1024 Off:0 File: svcctl
2019-01-23 13:39:15.318052	192.168.202.101	192.168.202.100	DCE/RPC	230	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 1024
2019-01-23 13:39:15.318214	192.168.202.100	192.168.202.101	SVCCTL	238	OpenSCManagerW request, WIN01
2019-01-23 13:39:15.318476	192.168.202.101	192.168.202.100	SVCCTL	218	OpenSCManagerW response
2019-01-23 13:39:15.318727	192.168.202.100	192.168.202.101	SVCCTL	398	Unknown operation 45 request
2019-01-23 13:39:15.320312	192.168.202.101	192.168.202.100	SMB2	131	Ioctl Response, Error: STATUS_PENDING
2019-01-23 13:39:15.329962	192.168.202.101	192.168.202.100	SVCCTL	222	Unknown operation 45 response
2019-01-23 13:39:15.330308	192.168.202.100	192.168.202.101	SVCCTL	222	CloseServiceHandle request, (null)
2019-01-23 13:39:15.330582	192.168.202.101	192.168.202.100	SVCCTL	218	CloseServiceHandle response
2019-01-23 13:39:15.330746	192.168.202.100	192.168.202.101	SVCCTL	258	OpenServiceW request
2019-01-23 13:39:15.330928	192.168.202.101	192.168.202.100	SVCCTL	218	OpenServiceW response
2019-01-23 13:39:15.331154	192.168.202.100	192.168.202.101	SVCCTL	238	StartServiceW request
2019-01-23 13:39:15.336318	192.168.202.101	192.168.202.100	SMB2	131	Ioctl Response, Error: STATUS_PENDING
2019-01-23 13:39:15.414881	192.168.202.101	192.168.202.100	SVCCTL	198	StartServiceW response
2019-01-23 13:39:15.415280	192.168.202.100	192.168.202.101	SVCCTL	222	QueryServiceStatus request
2019-01-23 13:39:15.415814	192.168.202.101	192.168.202.100	SVCCTL	226	QueryServiceStatus response

Рисунок 3. Создание нового сервиса с помощью SCM

С помощью RPC реализуются и другие техники, например session discovery. Отправка запросов сервису Security Accounts Manager по протоколу SAMR позволяет получить список пользователей и групп в домене, а перебор идентификаторов SID с помощью сервиса Local Security Authority (LSARPC) позволяет злоумышленнику узнать имена пользователей на удаленном узле.

92	0.178904	192.168.202.154	192.168.202.145	DCERPC	86 Response: call_id: 3, Fragment: Mid, Ctx: 0 [DCE/RPC Mid
93	0.180655	192.168.202.145	192.168.202.154	TCP	66 38098 → 445 [ACK] Seq=39592 Ack=15609 Win=62976 Len=0 TSV
94	0.180655	192.168.202.145	192.168.202.154	SMB2	183 Read Request Len:1048576 Off:0 File: lsarpc
95	0.180822	192.168.202.154	192.168.202.145	TCP	1514 [TCP segment of a reassembled PDU]
96	0.180823	192.168.202.154	192.168.202.145	TCP	1514 [TCP segment of a reassembled PDU]
97	0.180823	192.168.202.154	192.168.202.145	LSARPC	718 Lsa_LookupSids response, STATUS_SOME_NOT_MAPPED, Error: ...
98	0.180823	192.168.202.145	192.168.202.154	TCP	66 38098 → 445 [ACK] Seq=39709 Ack=19157 Win=70016 Len=0 TSV
99	0.484367	192.168.202.145	192.168.202.154	TCP	1514 [TCP segment of a reassembled PDU]

Referent ID: 0x00020000
Domains
Count: 1
Pointer to Domains (lsa_DomainInfo)
Referent ID: 0x00020004
Max Count: 1
Domains
Max Size: 32
Pointer to Names (lsa_TransNameArray)
Names
Count: 1000
Pointer to Names (lsa_TranslatedName)
Referent ID: 0x00020010
Max Count: 1000
Names

00 00 00 00 0d 00 00 00 00 00 00 00 0d 00 00 00	.....
41 00 64 00 6d 00 69 00 6e 00 69 00 73 00 74 00	A.d.m.i. n.i.s.t.
72 00 61 00 74 00 6f 00 72 00 00 00 05 00 00 00	r.a.t.o. r.....
00 00 00 00 05 00 00 00 47 00 75 00 65 00 73 00	..... G.u.e.s.
74 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00	t.....
4e 00 6f 00 6e 00 65 00 03 00 00 00 07 01 00 00	N.o.n.e. ....

Рисунок 4. Получение учетных записей с помощью lookupsids

Один из популярных методов закрепления в системе и продвижения по сети — создание задач, выполняющихся по расписанию (scheduled task), — осуществляется путем отправки запросов сервису планировщика задач ATSVС.

No.	Time	Source	Destination	Protocol	Length	Info
165	2018-09-03 12:34:21.927575	192.168.241.1	192.168.241.203	SMB2	224	Session Setup Request, NTLMSSP_NEGOTIAT
166	2018-09-03 12:34:21.927877	192.168.241.203	192.168.241.1	SMB2	393	Session Setup Response, Error: STATUS_M
167	2018-09-03 12:34:21.930647	192.168.241.1	192.168.241.203	SMB2	536	Session Setup Request, NTLMSSP_AUTH, Us
170	2018-09-03 12:34:21.932674	192.168.241.203	192.168.241.1	SMB2	151	Session Setup Response
171	2018-09-03 12:34:21.934966	192.168.241.1	192.168.241.203	SMB2	186	Tree Connect Request Tree: \\192.168.24
172	2018-09-03 12:34:21.935446	192.168.241.203	192.168.241.1	SMB2	150	Tree Connect Response
173	2018-09-03 12:34:21.936533	192.168.241.1	192.168.241.203	SMB2	20	Create Request File: atsvc
174	2018-09-03 12:34:21.936790	192.168.241.203	192.168.241.1	SMB2	222	Create Response File: atsvc
175	2018-09-03 12:34:21.938665	192.168.241.1	192.168.241.203	DCERPC	294	Bind: call_id: 1, Fragment: Single, 1 c
176	2018-09-03 12:34:21.938844	192.168.241.203	192.168.241.1	SMB2	150	Write Response
177	2018-09-03 12:34:21.939715	192.168.241.1	192.168.241.203	SMB2	183	Read Request Len:1048576 Off:0 File: at
178	2018-09-03 12:34:21.940012	192.168.241.203	192.168.241.1	DCERPC	446	Bind Ack: call_id: 1, Fragment: Single,
179	2018-09-03 12:34:21.943267	192.168.241.1	192.168.241.203	DCERPC	588	AUTH: call_id: 1, Fragment: Single, NT
180	2018-09-03 12:34:21.943479	192.168.241.203	192.168.241.1	SMB2	150	Write Response
183	2018-09-03 12:34:21.945097	192.168.241.1	192.168.241.203	TCP	1514	53344 → 445 [ACK] Seq=1933 Ack=2261 Win
184	2018-09-03 12:34:21.945105	192.168.241.1	192.168.241.203	TCP	1514	53344 → 445 [ACK] Seq=3381 Ack=2261 Win
185	2018-09-03 12:34:21.945118	192.168.241.1	192.168.241.203	DCERPC	1462	Request: call_id: 2, Fragment: 1st, op
186	2018-09-03 12:34:21.945254	192.168.241.203	192.168.241.1	TCP	66	445 → 53344 [ACK] Seq=2261 Ack=6225 Win
187	2018-09-03 12:34:21.945469	192.168.241.203	192.168.241.1	SMB2	150	Write Response
188	2018-09-03 12:34:21.946489	192.168.241.1	192.168.241.203	TCP	1514	53344 → 445 [ACK] Seq=6225 Ack=2345 Win
189	2018-09-03 12:34:21.946497	192.168.241.1	192.168.241.203	TCP	1514	53344 → 445 [ACK] Seq=7673 Ack=2345 Win
190	2018-09-03 12:34:21.946510	192.168.241.1	192.168.241.203	DCERPC	1462	Request: call_id: 2, Fragment: Mid, op
191	2018-09-03 12:34:21.946656	192.168.241.203	192.168.241.1	TCP	66	445 → 53344 [ACK] Seq=2345 Ack=18517 Wi
192	2018-09-03 12:34:21.946718	192.168.241.203	192.168.241.1	SMB2	150	Write Response
193	2018-09-03 12:34:21.947716	192.168.241.1	192.168.241.203	DCERPC	1470	Request: call_id: 2, Fragment: Last, op
194	2018-09-03 12:34:21.947853	192.168.241.203	192.168.241.1	SMB2	150	Write Response
196	2018-09-03 12:34:21.948788	192.168.241.1	192.168.241.203	SMB2	183	Read Request Len:1048576 Off:0 File: at

0000 00 0c 29 56 5f c3 00 50 56 c0 00 08 08 00 45 00	..V..P.V.....E..
0010 00 ba 43 97 40 00 00 06 92 88 c0 a8 f1 01 c0 a8	..C.@.....
0020 f1 cb d0 00 01 bd a7 f2 65 65 2c 57 6e 85 80 18	.....ee,Win.....
0030 00 fe c2 5a 00 00 01 01 00 00 72 a8 6f 05 13 46	.....rHo..F.....
0040 bf 90 00 00 00 82 fe 53 4d 42 40 00 01 00 00 00	.....S.HB.....
0050 00 00 05 00 7f 00 00 00 00 00 00 00 00 05 00	.....
0060 00 00 00 00 00 00 00 00 00 01 00 00 00 45 00	.....E.....
0070 00 04 00 10 00 00 00 00 00 00 00 00 00 00 00	.....
0080 00 00 00 00 00 39 00 00 00 02 00 00 00 00 00	.....9.....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00	.....
00a0 00 00 00 00 00 01 00 00 00 01 00 00 00 40 00	.....@.....
00b0 00 00 78 00 0a 00 00 00 00 00 00 00 00 61 00	.....x.....a.....
00c0 74 00 73 00 76 00 63 00	t.s.v.c.....

Рисунок 5. Создание новой задачи в планировщике задач ATSVС

Описанные сценарии вполне легитимны и могут использоваться в повседневной деятельности администраторов, поэтому нужно создавать вспомогательные правила, которые бы автоматизировали обнаружение RPC-вызовов и обращений к сервисам. Эти действия необходимо анализировать в связи с другими событиями, учитывая общий контекст происходящего. Такой анализ может потребовать больших трудозатрат.

Поэтому более эффективны точечные правила обнаружения, которые анализируют сетевой трафик с учетом порядка команд и значений объектов в запросах, характерных для конкретных инструментов. Например, зная последовательность действий и структуру данных, которые определены в коде утилиты psexec из набора Impacket, можно с большой точностью выявить ее запуск в трафике.

```

tid = s.connectTree('IPCS')
fid_main = self.openPipe(s,tid,'\\RemCom_communicaton',0x12019f)

packet = RemComMessage()
pid = os.getpid()

packet['Machine'] = ''.join([random.choice(string.letters) for _ in range(4)])
if self.__path is not None:
    packet['WorkingDir'] = self.__path
packet['Command'] = self.__command
packet['ProcessID'] = pid

s.writeNamedPipe(tid, fid_main, str(packet))

```

Рисунок 6. Фрагмент кода psexec

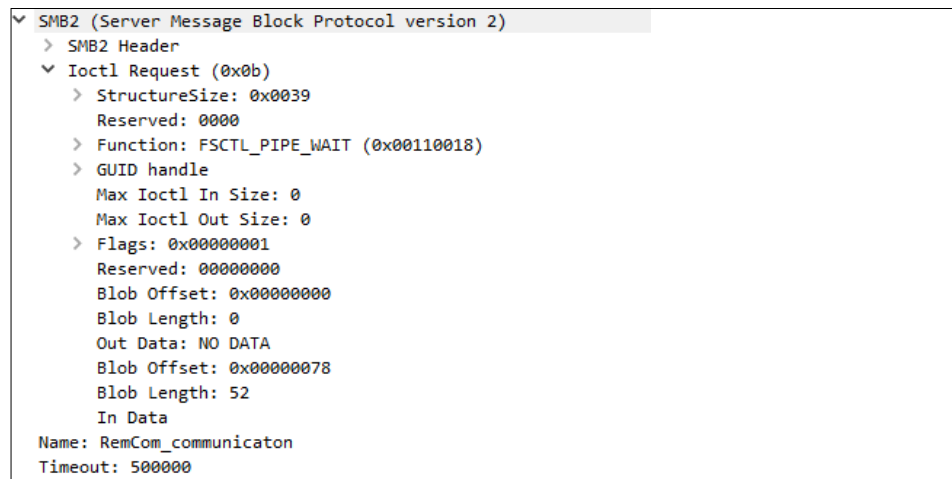


Рисунок 7. SMB-пакет, который отправляется в результате выполнения кода на рис. 6

## Windows Management Instrumentation

Встроенная технология WMI позволяет злоумышленникам воспользоваться уже имеющимися в системе средствами для взаимодействия с удаленными узлами. Когда WMI-команда передается по сети по незашифрованному протоколу DCERPC, в сетевом трафике можно увидеть текстовые строки, где указан класс, к которому происходит обращение, и метод, который вызывается у класса. Чтобы выявить передачу команды на исполнение, необходимо отслеживать вызов метода Create класса Win32\_Process.

```

.....
W.i.n.3.2..P.r.o.c.e.s.s..User.....C.r.e.a.t.e.....|...MEOW.....s...M...K...$...
$.L...xV4.D.....
.....*...s...s.....
...PARAMETERS..abstract.....CommandLine..string.....
7...In.....
7...^.....Win32API|Process and Thread Functions|lpCommandLine ..MappingStrings....
7...^.....ID.....6...
Y...^.....string.....CurrentDirectory..string....
In.....
.....Win32API|Process and Thread Functions|CreateProcess|lpCurrentDirectory ..

```

Рисунок 8. Вызов метода Create класса Win32\_Process

```

.....
.....<.....2.....PARAMETERS..new user /add FindMe
098*()poiIOP.....

```

Рисунок 9. Команда на исполнение

Модули для работы с WMI присутствуют во многих готовых инструментах, например в Impacket, Koadic и Cobalt Strike. В Cobalt Strike есть также модуль WMI event consumer, который создает подписку на WMI-события. Такая подписка позволяет



выполнять определенное действие, когда происходит заданное событие, например когда проходит установленное время с момента старта ОС или пользователь авторизуется в системе. Действием может быть запуск вредоносного ПО или средства удаленного управления. Создание подписки также выявляется в сетевом трафике по специфическим строкам, в частности ROOT\Subscription и EventConsumer.

## Pass the hash

Злоумышленнику необязательно знать пароль пользователя, чтобы получить доступ к какому-либо сервису. Техника pass the hash эксплуатирует особенности протокола аутентификации NTLM, которые позволяют подключаться к ресурсам при наличии хеша пароля. Если же в инфраструктуре используется механизм аутентификации Kerberos, злоумышленник может прибегнуть к атаке overpass the hash, которая является развитием этой техники.

Протокол Kerberos был разработан специально для того, чтобы пароли пользователей не передавались по сети. Для этого на своей машине пользователь хешем своего пароля шифрует запрос на аутентификацию. В ответ Key Distribution Center выдает ему билет на получение других билетов — так называемый Ticket-Granting Ticket (TGT). Теперь клиент считается аутентифицированным и в течение десяти часов может обращаться за билетами для доступа к другим сервисам.

Последовательность действий при атаке overpass the hash состоит в следующем. Злоумышленник получает хеш пароля пользователя, например с помощью техники credential dumping, шифрует им запрос на аутентификацию и выпускает для себя билет TGT. Затем он запрашивает билет для доступа к интересующему его сервису и успешно в нем авторизуется.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.010575	10.10.10.10	10.10.10.10	KRB5	369	AS-REQ
6	0.022675	10.10.10.10	10.10.10.10	KRB5	345	AS-REP
14	0.034916	10.10.10.10	10.10.10.10	KRB5	1829	TGS-REQ
17	0.048151	10.10.10.10	10.10.10.10	KRB5	442	TGS-REP

> Frame 4: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)

> Ethernet II, Src: VMware\_Virtual\_Ethernet\_Adapter\_08:00:27:00:00:00, Dst: VMware\_Virtual\_Ethernet\_Adapter\_08:00:27:00:00:00

> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.10.10.10

> Transmission Control Protocol, Src Port: 49478, Dst Port: 88, Seq: 1, Ack: 1, Len: 315

▼ Kerberos

> Record Mark: 311 bytes

▼ as-req

pverno: 5

msg-type: krb-as-req (10)

▼ padata: 2 items

▼ PA-DATA PA-ENC-TIMESTAMP

▼ padata-type: kRB5-PADATA-ENC-TIMESTAMP (2)

▼ padata-value: 303da003020117a236043476a62254b49cc1c49c31bfe110...

etype: eTYPE-ARCFOUR-HMAC-MD5 (23)

cipher: 76a62254b49cc1c49c31bfe110284088d6ac6d99e7158c89...

▼ PA-DATA PA-PAC-REQUEST

▼ padata-type: kRB5-PADATA-PA-PAC-REQUEST (128)

▼ padata-value: 3005a0030101ff

include-pac: True

> req-body

Рисунок 10. Использование RC4 в атаке pass the hash

7



Атака overpass the hash может выявляться в сетевом трафике, например, на основе следующей аномалии. Microsoft рекомендует использовать и по умолчанию устанавливает для современных доменов AES-128/256 для шифрования запросов на аутентификацию, а утилита mimikatz шифрует их с помощью устаревшего алгоритма RC4. Если, конечно, злоумышленник специально не поменял тип шифрования (bit.ly/2uVT8x7).

При таком способе выявления атаки возможно большое количество ложных «детектов». Чтобы снизить количество ошибок, потребуется дополнительный поведенческий анализ.

Но в трафике можно отслеживать и инструменты, с помощью которых осуществляются атаки credential dumping и pass the hash, например mimikatz. Многие APT-группировки используют в своих целях готовые фреймворки для тестирования на проникновение, которые подгружают дополнительные модули разными способами. Например, Koadic, применяемый в атаках MuddyWater, передает mimikatz на зараженный узел по протоколу HTTP в виде закодированной в Base64 библиотеки, сериализованного .NET-класса, который будет ее внедрять, и аргументов для запуска утилиты. Результат выполнения передается по сети в открытом виде также по протоколу HTTP.

## Credential dumping

Существует несколько подходов к реализации credential dumping, которые можно отследить путем анализа трафика. Один из них — это атака DCSync, то есть репликация или копирование учетных записей пользователей на поддельный домен-контроллер. Выявляется атака с помощью разбора RPC-вызовов, которые передаются по сети, и поиска запросов DsGetNCChanges.

Protocol	Length	Info
DCERPC	220	Bind: call_id: 1, Fragment: Single, 1 context items: DRSUAI
DCERPC	418	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max
DCERPC	546	AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: n
DRSUAPI	240	DsBind request
DRSUAPI	252	DsBind response
DRSUAPI	216	DsGetDomainControllerInfo request
DRSUAPI	660	[TCP Spurious Retransmission] DsGetDomainControllerInfo re:
DRSUAPI	248	DsCrackNames request
DRSUAPI	332	DsCrackNames response
DRSUAPI	448	DsGetNCChanges request
DCERPC	796	[TCP Previous segment not captured] Response: call_id: 5, l
DCERPC	220	Bind: call_id: 1, Fragment: Single, 1 context items: DRSUAI
DCERPC	418	Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max
DCERPC	418	[TCP Spurious Retransmission] Bind_ack: call_id: 1, Fragmei
DCERPC	546	AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: n
DRSUAPI	240	DsBind request
DRSUAPI	252	DsBind response
DRSUAPI	216	DsGetDomainControllerInfo request
DRSUAPI	248	DsCrackNames request
DRSUAPI	332	DsCrackNames response
DRSUAPI	248	[TCP Spurious Retransmission] DsCrackNames request
DRSUAPI	448	DsGetNCChanges request
DRSUAPI	448	[TCP Spurious Retransmission] DsGetNCChanges request
DCERPC	796	Response: call_id: 5, Fragment: Last, Ctx: 0

Рисунок 11. Обнаружение атаки DCSync

Кроме того, злоумышленники могут попытаться скопировать файл NTDS.dit, содержащий данные об учетных записях. Поэтому необходимо отслеживать передачу этого файла по сети. Еще один способ реализовать credential dumping — это удаленный доступ к реестру по протоколу WINREG. Запросы на доступ к ключам SAM, SECURITY и LSA могут свидетельствовать о попытке получить учетные данные.

## Brute force

Microsoft Exchange и Office365 очень популярны как решения для корпоративной почты. Эти сервисы могут быть использованы злоумышленниками для получения доступа к учетным записям пользователей Active Directory. Техника такова: сначала получают список пользователей, а затем подбирают к ним пароль, так чтобы учетная запись не заблокировалась: по одному паролю на всех пользователей вместо слова-паролей для каждого. Такой подход получил название password spraying.



Если в инфраструктуре реализована аутентификация с помощью Kerberos, то для выявления подбора паролей требуется разбирать протокол Kerberos, находить сессии с ошибками, сообщающими, что запрашиваемый пользователь отсутствует, и разделять сессии с точностью до миллисекунд.

Если в трафике присутствует множество сессий с ошибкой KDC\_ERR\_C\_PRINCIPAL\_UNKNOWN с разными учетными записями, это означает, что происходит перебор имен пользователей.

192.168.150.130	KRB5	290 AS-REQ	
192.168.150.132	KRB5	156 KRB Error:	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
192.168.150.130	KRB5	290 AS-REQ	
192.168.150.132	KRB5	156 KRB Error:	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
192.168.150.130	KRB5	290 AS-REQ	
192.168.150.132	KRB5	156 KRB Error:	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
192.168.150.130	KRB5	290 AS-REQ	

Рисунок 12. Сессии с ошибкой KDC\_ERR\_C\_PRINCIPAL\_UNKNOWN

Сессии с малым временем ответа сервера (десятки миллисекунд) по сравнению с другими похожими (сотни миллисекунд) показывают, что в этих сессиях пароли подобрали успешно. В трафике будут также отражены попытки входа с подобранными учетными записями и ошибки Kerberos. Сессии без ошибок с успешными ответами AS\_REP и выданными билетами показывают, к каким учетным записям были подобраны пароли.



192.168.150.130	KRB5	290 AS-REQ	
192.168.150.132	KRB5	156 KRB Error:	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
192.168.150.130	KRB5	290 AS-REQ	
192.168.150.132	KRB5	156 KRB Error:	KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
192.168.150.130	KRB5	286 AS-REQ	
192.168.150.132	KRB5	277 KRB Error:	KRB5KDC_ERR_PREAUTH_REQUIRED
192.168.150.130	KRB5	366 AS-REQ	
192.168.150.132	KRB5	244 KRB Error:	KRB5KDC_ERR_PREAUTH_FAILED
192.168.150.130	KRB5	286 AS-REQ	
192.168.150.132	KRB5	277 KRB Error:	KRB5KDC_ERR_PREAUTH_REQUIRED
192.168.150.130	KRB5	366 AS-REQ	
192.168.150.132	KRB5	244 KRB Error:	KRB5KDC_ERR_PREAUTH_FAILED
192.168.150.130	KRB5	286 AS-REQ	
192.168.150.132	KRB5	277 KRB Error:	KRB5KDC_ERR_PREAUTH_REQUIRED
192.168.150.130	KRB5	366 AS-REQ	
192.168.150.132	KRB5	244 KRB Error:	KRB5KDC_ERR_PREAUTH_FAILED
192.168.150.130	KRB5	286 AS-REQ	
192.168.150.132	KRB5	277 KRB Error:	KRB5KDC_ERR_PREAUTH_REQUIRED
192.168.150.130	KRB5	366 AS-REQ	
192.168.150.132	KRB5	86 AS-REP	
192.168.150.130	KRB5	1575 TGS-REQ	

Рисунок 13. Попытки подбора паролей

Здесь также будет видна цикличность в именах пользователей, потому что атакующие подбирают по одному паролю на все учетные записи. Атаке может предшествовать запрос парольной политики домена: сколько установлено попыток неверного ввода пароля и на какое время блокируется учетная запись.

## Подведем итог

Использование рассмотренных техник атаки можно обнаружить и другими методами (например, с помощью SIEM и анализа журналов событий). Артефакты на конечных узлах будут свидетельствовать о компрометации ресурса, но для того, чтобы раскрутить всю цепочку атаки и определить начальный вектор проникновения или просто проверить гипотезы в рамках threat hunting, может потребоваться проследить перемещения злоумышленника внутри сети, выявить подключения к командным серверам или к узлам в Tor, найти и проанализировать аномалии в сетевом взаимодействии.

Типовые решения для защиты конечных узлов в инфраструктуре и межсетевые экраны не обеспечивают должный уровень контроля, опытные хакеры адаптируют свои инструменты для их обхода. Анализ сетевого трафика станет полезным дополнением к уже зарекомендовавшим себя методам обнаружения и расследования киберинцидентов. Копия сетевого трафика может помочь эксперту по ИБ разобраться в инциденте более детально. А в некоторых случаях, например если дополнительно использовать песочницу для анализа файлов, возможно обнаружить сложные АРТ-атаки (рассмотренные техники применялись, к примеру, такими группировками, как APT27, TaskMasters, Silence).

### О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.