Результаты расследования инцидента в сетевом дампе.

Executive Summary

Злоумышленник собрал данные о правилах аутентификации учётных записей, которые дают ему возможность с большой точностью подобрать пароль. Злоумышленник использовал внутренний компьютер с доступом к инфраструктуре и точно знал логин/пароль учётной записи, с которой зайдёт на него, которая принадлежит Oliver Boomwald (возможно это был сотрудник). При входе на компьютер в 07:49 он запустил автоматический сбор данных (samrdump) и периодическую отправку команд на удалённый сервер (их предназначение неизвестно, т.к. менялись всего раз, а их размер свидетельствует о том, что передал он в разы меньше информации, чем получил) и проверил существование файла автозапуска. Спустя 50 минут, в течении которых происходило скачивание большого трафика с внешних ресурсов и периодические проверки на доступность иных серверов, он получил файлы политик аутентификации, т.к. уже был авторизован и имел к ним полный доступ.

Объекты исследования

Название объекта исследования	Описание объекта исследования
traffic.pcapng	Дамп сетевого трафика Wireshark

Результаты исследования

Временные рамки инцидента

Дата и время события	Краткое описание
07:49 24.11.2024	Авторизация под пользователем oboomwald; начало сбора доменной информации через SAMR, проверка существования Default Domain Policy
05:50 24.11.2024	Начало периодичной отправки POST запросов на сервер злоумышленника
08:39 24.11.2024	Получение GptTmpl.inf, Registry.pol

Вектор(а) атак и подтверждающая информация

Сбор внутренних данных домена был через компьютер (DESKTOP-B8TQK49), находящийся в домене (nemotodes.health) (возможно это был сотрудник) и учётную запись oboomwald.

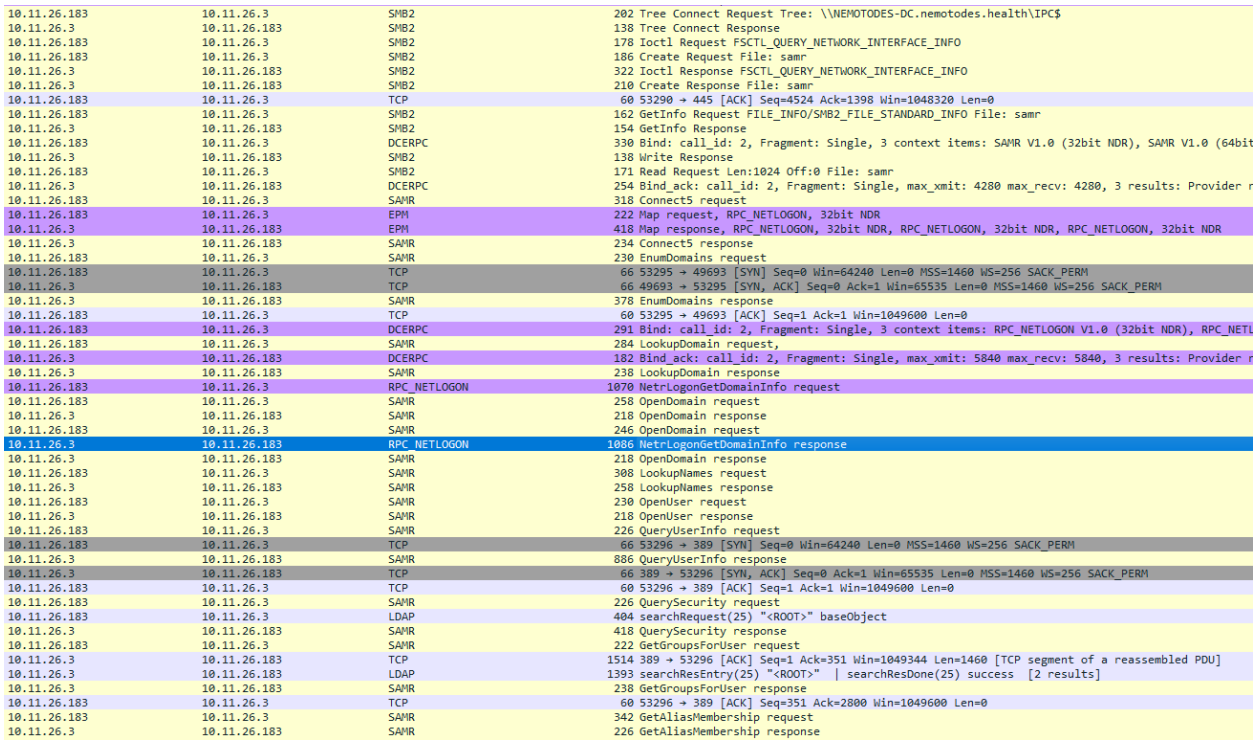
Вероятно, первоначальный сбор данных был при помощи автоматизированного ПО – «*samrdump*», далее при помощи прав доступа были скачаны файлы GptTmpl.inf и Registry.pol, которые позволят узнать уровень безопасности домена (например, требования к паролям и политики блокировки учётных записей). Из GptTmpl.inf известно, что блокировка не

происходит при любом количестве попыток ввода пароля, знание сложности пароля создаёт огромную уязвимость особенно для учётных записей с правами администратора для Brute-Force атак, аналогично для Kerberos-билетов.

Описание последовательности атаки и подтверждающая информация

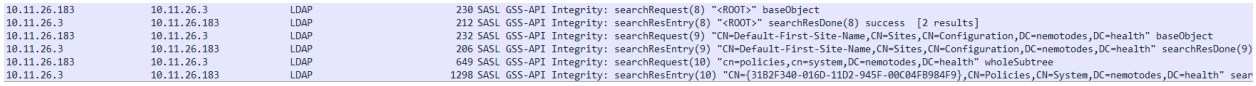
Злоумышленник авторизовался в домене NEMOTODES.HEALTH под пользователем oboomwald.

Выполнив запрос доступа к ldap/NEMOTODES-DC.nemotodes.health, в 07:49:55 он впервые обращается к IPC (named pipe’ам), запрашивает доступ до SAMR вероятно выполняется автоматизированный «samrdump». Через SAMR происходит сбор возможных данных о домене (SID, объекты, имена пользователей), а также информации о пользователе под которым он авторизован и группах, в которые он входит.



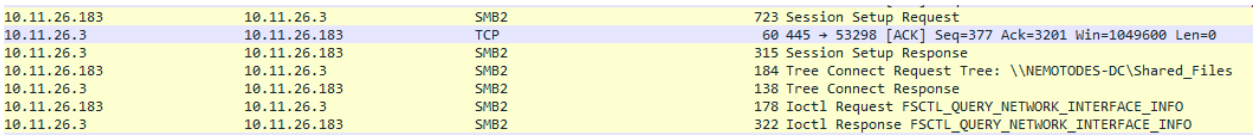
10.11.26.183	10.11.26.3	SMB2	202 Tree Connect Request Tree: \\NEMOTODES-DC.nemotodes.health\IPC$
10.11.26.3	10.11.26.183	SMB2	138 Tree Connect Response
10.11.26.183	10.11.26.3	SMB2	178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.183	10.11.26.3	SMB2	186 Create Request File: samr
10.11.26.3	10.11.26.183	SMB2	322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.3	10.11.26.183	SMB2	210 Create Response File: samr
10.11.26.183	10.11.26.3	TCP	60 53290 → 445 [ACK] Seq=4524 Ack=1398 Win=1048320 Len=0
10.11.26.183	10.11.26.3	SMB2	162 GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: samr
10.11.26.3	10.11.26.183	SMB2	154 GetInfo Response
10.11.26.183	10.11.26.3	DCERPC	330 Bind: call_id: 2, Fragment: Single, 3 context items: SAMR V1.0 (32bit NDR), SAMR V1.0 (64bit
10.11.26.3	10.11.26.183	SMB2	138 Write Response
10.11.26.183	10.11.26.3	SMB2	171 Read Request Len:1024 Off:0 File: samr
10.11.26.3	10.11.26.183	DCERPC	254 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider r
10.11.26.183	10.11.26.3	SAMR	318 Connect5 request
10.11.26.183	10.11.26.3	EPM	222 Map request, RPC_NETLOGON, 32bit NDR
10.11.26.3	10.11.26.183	EPM	418 Map response, RPC_NETLOGON, 32bit NDR, RPC_NETLOGON, 32bit NDR, RPC_NETLOGON, 32bit NDR
10.11.26.3	10.11.26.183	SAMR	234 Connect5 response
10.11.26.183	10.11.26.3	SAMR	230 EnumDomains request
10.11.26.183	10.11.26.3	TCP	66 53295 → 49693 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	10.11.26.183	TCP	66 49693 → 53295 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	10.11.26.183	SAMR	378 EnumDomains response
10.11.26.183	10.11.26.3	TCP	60 53295 → 49693 [ACK] Seq=1 Ack=1 Win=1049600 Len=0
10.11.26.183	10.11.26.3	DCERPC	291 Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETL
10.11.26.183	10.11.26.3	SAMR	284 LookupDomain request,
10.11.26.3	10.11.26.183	DCERPC	182 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider r
10.11.26.3	10.11.26.183	SAMR	238 LookupDomain response
10.11.26.183	10.11.26.3	RPC_NETLOGON	1070 NetrLogonGetDomainInfo request
10.11.26.183	10.11.26.3	SAMR	258 OpenDomain request
10.11.26.3	10.11.26.183	SAMR	218 OpenDomain response
10.11.26.183	10.11.26.3	SAMR	246 OpenDomain request
10.11.26.3	10.11.26.183	RPC_NETLOGON	1086 NetrLogonGetDomainInfo response
10.11.26.3	10.11.26.183	SAMR	218 OpenDomain response
10.11.26.183	10.11.26.3	SAMR	308 LookupNames request
10.11.26.3	10.11.26.183	SAMR	258 LookupNames response
10.11.26.183	10.11.26.3	SAMR	230 OpenUser request
10.11.26.3	10.11.26.183	SAMR	218 OpenUser response
10.11.26.183	10.11.26.3	SAMR	226 QueryUserInfo request
10.11.26.183	10.11.26.3	TCP	66 53296 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	10.11.26.183	SAMR	886 QueryUserInfo response
10.11.26.3	10.11.26.183	TCP	66 389 → 53296 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.183	10.11.26.3	TCP	60 53296 → 389 [ACK] Seq=1 Ack=1 Win=1049600 Len=0
10.11.26.183	10.11.26.3	SAMR	226 QuerySecurity request
10.11.26.183	10.11.26.3	LDAP	404 searchRequest(25) "<ROOT>" baseObject
10.11.26.3	10.11.26.183	SAMR	418 QuerySecurity response
10.11.26.183	10.11.26.3	SAMR	222 GetGroupsForUser request
10.11.26.3	10.11.26.183	TCP	1514 389 → 53296 [ACK] Seq=1 Ack=351 Win=1049344 Len=1460 [TCP segment of a reassembled PDU]
10.11.26.3	10.11.26.183	LDAP	1393 searchResEntry(25) "<ROOT>" | searchResDone(25) success [2 results]
10.11.26.3	10.11.26.183	SAMR	238 GetGroupsForUser response
10.11.26.183	10.11.26.3	TCP	60 53296 → 389 [ACK] Seq=351 Ack=2800 Win=1049600 Len=0
10.11.26.183	10.11.26.3	SAMR	342 GetAliasMembership request
10.11.26.3	10.11.26.183	SAMR	226 GetAliasMembership response

Проверка существования Default Domain Policy групповой политики.

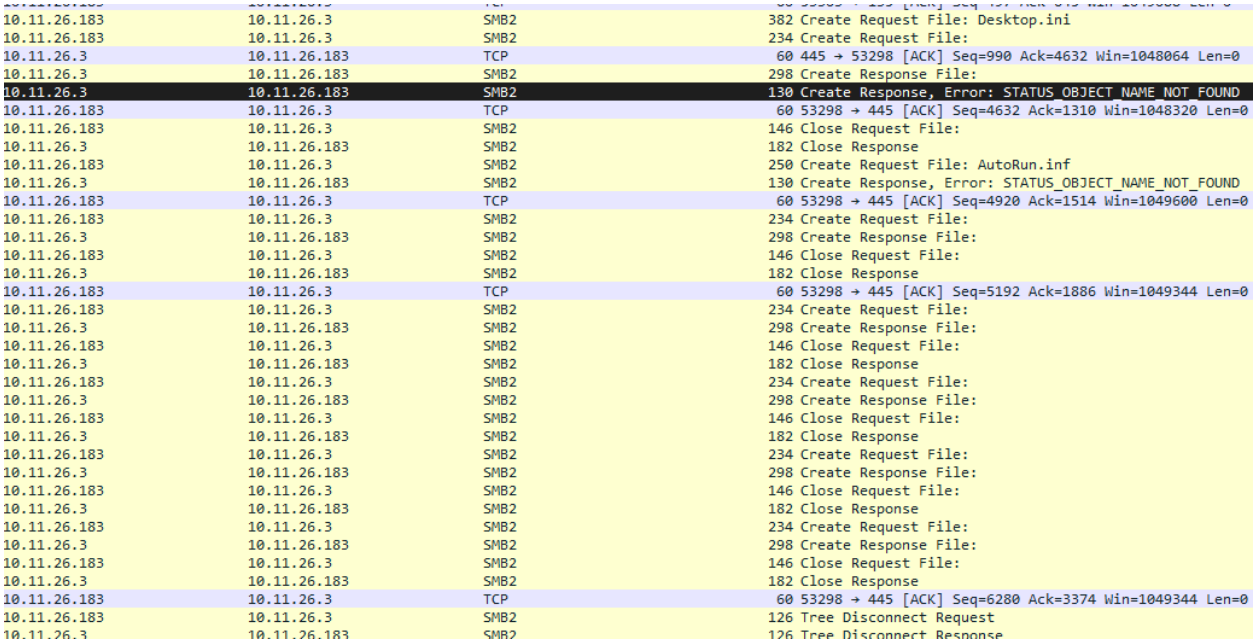


```
10.11.26.183     10.11.26.3       LDAP       230 SASL GSS-API Integrity: searchRequest(8) "<ROOT>" baseObject
10.11.26.3       10.11.26.183     LDAP       212 SASL GSS-API Integrity: searchResEntry(8) "<ROOT>" searchResDone(8) success  [2 results]
10.11.26.183     10.11.26.3       LDAP       232 SASL GSS-API Integrity: searchRequest(9) "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=nemotodes,DC=health" baseObject
10.11.26.3       10.11.26.183     LDAP       206 SASL GSS-API Integrity: searchResEntry(9) "CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=nemotodes,DC=health" searchResDone(9)
10.11.26.183     10.11.26.3       LDAP       649 SASL GSS-API Integrity: searchRequest(10) "cn=policies,cn=system,DC=nemotodes,DC=health" wholeSubtree
10.11.26.3       10.11.26.183     LDAP      1298 SASL GSS-API Integrity: searchResEntry(10) "CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=nemotodes,DC=health" sear
```

Проверка доступа до общего ресурса на контроллере домена \Shared_Files и к файлам desktop.ini, Desktop.ini, AutoRun.inf (файлы не найдены).

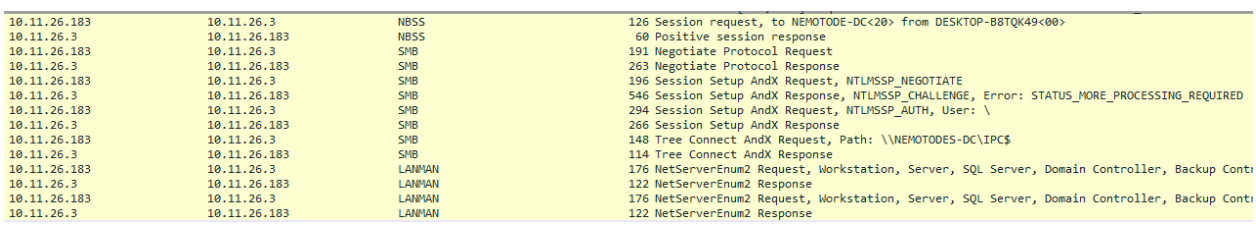


```
10.11.26.183     10.11.26.3       SMB2      723 Session Setup Request
10.11.26.3       10.11.26.183     TCP        60 445 → 53298 [ACK] Seq=377 Ack=3201 Win=1049600 Len=0
10.11.26.3       10.11.26.183     SMB2      315 Session Setup Response
10.11.26.183     10.11.26.3       SMB2      184 Tree Connect Request Tree: \\NEMOTODES-DC\Shared_Files
10.11.26.3       10.11.26.183     SMB2      138 Tree Connect Response
10.11.26.183     10.11.26.3       SMB2      178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.3       10.11.26.183     SMB2      322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
```



```
10.11.26.183     10.11.26.3       SMB2      382 Create Request File: Desktop.ini
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     TCP        60 445 → 53298 [ACK] Seq=990 Ack=4632 Win=1048064 Len=0
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.3       10.11.26.183     SMB2      130 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
10.11.26.183     10.11.26.3       TCP        60 53298 → 445 [ACK] Seq=4632 Ack=1310 Win=1048320 Len=0
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       SMB2      250 Create Request File: AutoRun.inf
10.11.26.3       10.11.26.183     SMB2      130 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
10.11.26.183     10.11.26.3       TCP        60 53298 → 445 [ACK] Seq=4920 Ack=1514 Win=1049600 Len=0
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       TCP        60 53298 → 445 [ACK] Seq=5192 Ack=1886 Win=1049344 Len=0
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       SMB2      234 Create Request File:
10.11.26.3       10.11.26.183     SMB2      298 Create Response File:
10.11.26.183     10.11.26.3       SMB2      146 Close Request File:
10.11.26.3       10.11.26.183     SMB2      182 Close Response
10.11.26.183     10.11.26.3       TCP        60 53298 → 445 [ACK] Seq=6280 Ack=3374 Win=1049344 Len=0
10.11.26.183     10.11.26.3       SMB2      126 Tree Disconnect Request
10.11.26.3       10.11.26.183     SMB2      126 Tree Disconnect Response
```

Попытка поиска всех серверов через NetServerEnum2 со всеми флагами не вернула ничего.



```
10.11.26.183     10.11.26.3       NBSS      126 Session request, to NEMOTODE-DC<20> from DESKTOP-B8TQK49<00>
10.11.26.3       10.11.26.183     NBSS       60 Positive session response
10.11.26.183     10.11.26.3       SMB       191 Negotiate Protocol Request
10.11.26.3       10.11.26.183     SMB       263 Negotiate Protocol Response
10.11.26.183     10.11.26.3       SMB       196 Session Setup AndX Request, NTLMSSP_NEGOTIATE
10.11.26.3       10.11.26.183     SMB       546 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10.11.26.183     10.11.26.3       SMB       294 Session Setup AndX Request, NTLMSSP_AUTH, User: \
10.11.26.3       10.11.26.183     SMB       266 Session Setup AndX Response
10.11.26.183     10.11.26.3       SMB       148 Tree Connect AndX Request, Path: \\NEMOTODES-DC\IPC$
10.11.26.3       10.11.26.183     SMB       114 Tree Connect AndX Response
10.11.26.183     10.11.26.3       LANMAN    176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Contr
10.11.26.3       10.11.26.183     LANMAN    122 NetServerEnum2 Response
10.11.26.183     10.11.26.3       LANMAN    176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Contr
10.11.26.3       10.11.26.183     LANMAN    122 NetServerEnum2 Response
```

Далее проверка доступа до «*desktop.ini*» и повторный скан серверов. Присутствует запрос о DFS.

10.11.26.3	SMB2	382 Create Request File: desktop.ini
10.11.26.183	SMB2	130 Create Response, Error: STATUS_OBJECT_NAME_NOT_FOUND
10.11.26.3	TCP	60 53298 → 445 [ACK] Seq=7152 Ack=4194 Win=1048320 Len=0
10.11.26.3	TCP	66 53357 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.183	TCP	66 445 → 53357 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	TCP	60 53357 → 445 [ACK] Seq=1 Ack=1 Win=1049600 Len=0
10.11.26.3	SMB	213 Negotiate Protocol Request
10.11.26.183	SMB2	306 Negotiate Protocol Response
10.11.26.3	SMB2	374 Negotiate Protocol Request
10.11.26.183	SMB2	430 Negotiate Protocol Response
10.11.26.3	TCP	1514 53357 → 445 [ACK] Seq=480 Ack=629 Win=1049088 Len=1460 [TCP segment of a reassembled PDU]
10.11.26.3	TCP	1514 53357 → 445 [ACK] Seq=1940 Ack=629 Win=1049088 Len=1460 [TCP segment of a reassembled PDU]
10.11.26.3	SMB2	898 Session Setup Request
10.11.26.183	TCP	60 445 → 53357 [ACK] Seq=629 Ack=3400 Win=1049600 Len=0
10.11.26.183	SMB2	315 Session Setup Response
10.11.26.3	SMB2	202 Tree Connect Request Tree: \\NEMOTODES-DC.nemotodes.health\IPC$
10.11.26.183	SMB2	138 Tree Connect Response
10.11.26.3	SMB2	178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.3	SMB2	182 Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
10.11.26.183	SMB2	322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.183	SMB2	272 Ioctl Response FSCTL_DFS_GET_REFERRALS
10.11.26.3	TCP	60 53357 → 445 [ACK] Seq=4644 Ack=1460 Win=1048064 Len=0
10.11.26.3	TCP	66 53359 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.183	TCP	66 139 → 53359 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	NBSS	126 Session request, to NEMOTODE-DC<20> from DESKTOP-B8TQK49<00>
10.11.26.183	NBSS	60 Positive session response
10.11.26.3	SMB	191 Negotiate Protocol Request
10.11.26.183	SMB	263 Negotiate Protocol Response
10.11.26.3	SMB	196 Session Setup AndX Request, NTLMSSP_NEGOTIATE
10.11.26.183	SMB	546 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10.11.26.3	SMB	294 Session Setup AndX Request, NTLMSSP_AUTH, User: \
10.11.26.183	SMB	266 Session Setup AndX Response
10.11.26.3	SMB	148 Tree Connect AndX Request, Path: \\NEMOTODES-DC\IPC$
10.11.26.183	SMB	114 Tree Connect AndX Response
10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.183	LANMAN	122 NetServerEnum2 Response
10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.183	LANMAN	122 NetServerEnum2 Response

Подозрительно огромный трафик с сайта modandcrackapk.com после GET запроса на «*Let’s Encrypt*» с передачей в нём Kerberos AP-REQ. Потом на сервер злоумышленника (нет DNS запросов для получения IP-адреса 194.180.191.64, что подозрительно) идут 2 POST запроса с NetSupport Manager командами управления, у которых совпадают первые 47 байт.

10.11.26.183	10.11.26.3	DNS	80 Standard query 0xbe10 A modandcrackedapk.com
10.11.26.3	10.11.26.183	DNS	96 Standard query response 0xbe10 A modandcrackedapk.com A 193.42.38.139
10.11.26.183	10.11.26.3	DNS	75 Standard query 0xe79e A r10.o.lencr.org
10.11.26.3	10.11.26.183	DNS	174 Standard query response 0xe79e A r10.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net A 104.117.247.99 A 104.117.247.67
10.11.26.183	104.117.247.99	HTTP	294 GET /MFMwUTBPME0wSzAJBgUrDgMCGgUABBRpD%2BQVZ%2B1vf7U0RGQGBm8JZwdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgRSsdGCXQJk1JZNbHi669GH4A%3D%3D HTTP/1.1
104.117.247.99	10.11.26.183	OCSP	944 Response
10.11.26.183	10.11.26.3	DNS	86 Standard query 0x0be4 A geo.netsupportsoftware.com
10.11.26.3	10.11.26.183	DNS	134 Standard query response 0x0be4 A geo.netsupportsoftware.com A 104.26.1.231 A 104.26.0.231 A 172.67.68.212
10.11.26.183	104.26.1.231	HTTP	172 GET /location/loca.asp HTTP/1.1
10.11.26.183	194.180.191.64	HTTP	274 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
194.180.191.64	10.11.26.183	HTTP	269 HTTP/1.1 200 OK (application/x-www-form-urlencoded)
10.11.26.183	194.180.191.64	HTTP	502 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
104.26.1.231	10.11.26.183	HTTP	60 HTTP/1.1 200 OK (text/html)
194.180.191.64	10.11.26.183	HTTP	360 HTTP/1.1 200 OK (application/x-www-form-urlencoded)
10.11.26.183	194.180.191.64	HTTP	328 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
10.11.26.183	194.180.191.64	HTTP	336 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

Далее 3 раза происходит двойной скан серверов через NetServerEnum2, после которых идут NetSupport Manager команды на сервер злоумышленника.

10.11.26.183	10.11.26.3	NBSS	126 Session request, to NEMOTODE-DC<20> from DESKTOP-B8TQK49<00>
10.11.26.3	10.11.26.183	NBSS	60 Positive session response
10.11.26.183	10.11.26.3	SMB	191 Negotiate Protocol Request
10.11.26.3	10.11.26.183	SMB	263 Negotiate Protocol Response
10.11.26.183	10.11.26.3	SMB	196 Session Setup AndX Request, NTLMSSP_NEGOTIATE
10.11.26.3	10.11.26.183	SMB	546 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10.11.26.183	10.11.26.3	SMB	294 Session Setup AndX Request, NTLMSSP_AUTH, User: \
10.11.26.3	10.11.26.183	SMB	266 Session Setup AndX Response
10.11.26.183	10.11.26.3	SMB	148 Tree Connect AndX Request, Path: \\NEMOTODES-DC\IPC$
10.11.26.3	10.11.26.183	SMB	114 Tree Connect AndX Response
10.11.26.183	10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.3	10.11.26.183	LANMAN	122 NetServerEnum2 Response
10.11.26.183	10.11.26.255	BROWSER	228 Request Announcement DESKTOP-B8TQK49
10.11.26.183	10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.3	10.11.26.183	LANMAN	122 NetServerEnum2 Response
10.11.26.183	10.11.26.255	BROWSER	228 Request Announcement DESKTOP-B8TQK49
10.11.26.183	10.11.26.3	TCP	60 53372 → 139 [ACK] Seq=930 Ack=1114 Win=1048576 Len=0
10.11.26.183	10.11.26.3	SMB	93 Tree Disconnect Request
10.11.26.3	10.11.26.183	SMB	93 Tree Disconnect Response
10.11.26.183	10.11.26.3	SMB	97 Logoff AndX Request
10.11.26.3	10.11.26.183	SMB	97 Logoff AndX Response
10.11.26.183	10.11.26.3	TCP	60 53372 → 139 [FIN, ACK] Seq=1012 Ack=1196 Win=1048320 Len=0
10.11.26.3	10.11.26.183	TCP	60 139 → 53372 [FIN, ACK] Seq=1196 Ack=1013 Win=1048320 Len=0
10.11.26.183	10.11.26.3	TCP	60 53372 → 139 [ACK] Seq=1013 Ack=1197 Win=1048320 Len=0
10.11.26.183	10.11.26.3	TCP	60 [TCP Keep-Alive] 53298 → 445 [ACK] Seq=7151 Ack=4194 Win=1048320 Len=1
10.11.26.3	10.11.26.183	TCP	66 [TCP Keep-Alive ACK] 445 → 53298 [ACK] Seq=4194 Ack=7152 Win=1048576 Len=0 SLE=7151 SRE=7152
10.11.26.183	10.11.26.3	TCP	66 53374 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	10.11.26.183	TCP	66 139 → 53374 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.183	10.11.26.3	NBSS	126 Session request, to NEMOTODE-DC<20> from DESKTOP-B8TQK49<00>
10.11.26.3	10.11.26.183	NBSS	60 Positive session response
10.11.26.183	10.11.26.3	SMB	191 Negotiate Protocol Request
10.11.26.3	10.11.26.183	SMB	263 Negotiate Protocol Response
10.11.26.183	10.11.26.3	SMB	196 Session Setup AndX Request, NTLMSSP_NEGOTIATE
10.11.26.3	10.11.26.183	SMB	546 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10.11.26.183	10.11.26.3	SMB	294 Session Setup AndX Request, NTLMSSP_AUTH, User: \
10.11.26.3	10.11.26.183	SMB	266 Session Setup AndX Response
10.11.26.183	10.11.26.3	SMB	148 Tree Connect AndX Request, Path: \\NEMOTODES-DC\IPC$
10.11.26.3	10.11.26.183	SMB	114 Tree Connect AndX Response
10.11.26.183	10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.3	10.11.26.183	LANMAN	122 NetServerEnum2 Response
10.11.26.183	10.11.26.255	BROWSER	228 Request Announcement DESKTOP-B8TQK49
10.11.26.183	10.11.26.3	LANMAN	176 NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller
10.11.26.3	10.11.26.183	LANMAN	122 NetServerEnum2 Response
10.11.26.183	10.11.26.255	BROWSER	228 Request Announcement DESKTOP-B8TQK49
10.11.26.183	10.11.26.3	TCP	60 53374 → 139 [ACK] Seq=930 Ack=1114 Win=1048576 Len=0
10.11.26.183	194.180.191.64	HTTP	288 POST http://194.180.191.64/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

Злоумышленник несколько раз делает проверку на существование конкретного пользователя «*Oliver Boomwald*» (с учётки которого он находится в системе), запрашивались только имя и фамилия. После снова были отправлено несколько NetSupport команд (идентичные последней).

10.11.26.183	10.11.26.3	LDAP	604 bindRequest(8) "<ROOT>" sasl
10.11.26.3	10.11.26.183	TCP	60 389 → 53389 [ACK] Seq=1 Ack=2011 Win=1049600 Len=0
10.11.26.3	10.11.26.183	LDAP	265 bindResponse(8) success
10.11.26.183	10.11.26.3	LDAP	218 SASL GSS-API Integrity: searchRequest(9) "CN=Oliver Q.. Boomwald,CN=Users,DC=nemotodes,DC=health" baseObject
10.11.26.3	10.11.26.183	LDAP	242 SASL GSS-API Integrity: searchResEntry(9) "CN=Oliver Q.. Boomwald,CN=Users,DC=nemotodes,DC=health" searchResDone(9) success [1 result]
10.11.26.183	10.11.26.3	LDAP	97 SASL GSS-API Integrity: unbindRequest(10)

Злоумышленник получил SID пользователей через lsa_LookupNames4 (возможно для получения SID oboomwald@nemotodes).

10.11.26.183	10.11.26.3	DCERPC	214 Bind: call_id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-9812-4540-0300-000000000000)
10.11.26.3	10.11.26.183	DCERPC	162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
10.11.26.183	10.11.26.3	EPM	222 Map request, LSARPC, 32bit NDR
10.11.26.3	10.11.26.183	EPM	322 Map response, LSARPC, 32bit NDR, LSARPC, 32bit NDR
10.11.26.183	10.11.26.3	TCP	66 53420 → 49671 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.3	10.11.26.183	TCP	66 49671 → 53420 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10.11.26.183	10.11.26.3	TCP	60 53420 → 49671 [ACK] Seq=1 Ack=1 Win=131328 Len=0
10.11.26.183	10.11.26.3	DCERPC	291 Bind: call_id: 2, Fragment: Single, 3 context items: LSARPC V0.0 (32bit NDR), LSARPC V0.0 (64bit NDR), LSARPC V0.0 (6cb71c2c-9812-4540-0300-000000000000)
10.11.26.3	10.11.26.183	DCERPC	182 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
10.11.26.183	10.11.26.3	LSARPC	350 lsa_LookupNames4 request
10.11.26.3	10.11.26.183	LSARPC	238 lsa_LookupNames4 response
10.11.26.183	10.11.26.3	DCERPC	203 Alter_context: call_id: 3, Fragment: Single, 1 context items: LSARPC V0.0 (64bit NDR)
10.11.26.3	10.11.26.183	DCERPC	130 Alter_context_resp: call_id: 3, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
10.11.26.183	10.11.26.3	LSARPC	302 lsa_LookupNames4 request
10.11.26.3	10.11.26.183	LSARPC	238 lsa_LookupNames4 response

Получение данных о политике паролей и Kerberos-билетах.

```
10.11.26.183    10.11.26.3      SMB2    206 Tree Connect Request Tree: \\NEMOTODES-DC.nemotodes.health\sysvol
10.11.26.3      10.11.26.183    SMB2    138 Tree Connect Response
10.11.26.183    10.11.26.3      SMB2    178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.3      10.11.26.183    SMB2    322 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
10.11.26.183    10.11.26.3      SMB2    502 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
10.11.26.3      10.11.26.183    SMB2    410 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
10.11.26.183    10.11.26.3      TCP      60 53497 → 445 [ACK] Seq=5029 Ack=1598 Win=131328 Len=0
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    171 Read Request Len:22 Off:0 File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
10.11.26.3      10.11.26.183    SMB2    160 Read Response
10.11.26.183    10.11.26.3      SMB2    446 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine
10.11.26.3      10.11.26.183    SMB2    378 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    260 Find Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: nemotodes.health\Po
10.11.26.3      10.11.26.183    SMB2    682 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
10.11.26.183    10.11.26.3      SMB2    470 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft
10.11.26.3      10.11.26.183    SMB2    378 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    260 Find Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: nemotodes
10.11.26.3      10.11.26.183    SMB2    554 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
10.11.26.183    10.11.26.3      SMB2    494 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT
10.11.26.3      10.11.26.183    SMB2    378 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    260 Find Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File
10.11.26.3      10.11.26.183    SMB2    546 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
10.11.26.183    10.11.26.3      SMB2    510 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit
10.11.26.3      10.11.26.183    SMB2    378 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    260 Find Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Reque
10.11.26.3      10.11.26.183    SMB2    554 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
10.11.26.183    10.11.26.3      SMB2    590 Create Request File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    410 Create Response File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    370 GetInfo Request FILE_INFO/SMB2_FILE_EA_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf;GetInfo Re
10.11.26.3      10.11.26.183    SMB2    346 GetInfo Response;GetInfo Response;GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    186 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_STREAM_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
10.11.26.3      10.11.26.183    SMB2    168 GetInfo Response
10.11.26.183    10.11.26.3      SMB2    162 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
```

Содержание потенциально опасного для эксфильтрации файла GptTmpl.inf:

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
```

Индикаторы компрометации (IOC)

Файловые индикаторы компрометации (sha1sum файлов, связанных с атакой; пути закрепления ВПО)

Файлы, взятые у нас:

1. \\nemotodes-dc.nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
2. \\nemotodes-dc.nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Registry.pol
3. \\nemotodes-dc.nemotodes.health\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini

Сетевые индикаторы компрометации (IP адрес(а) злоумышленника)

10.11.26.183 – машина, через которую происходил сбор данных.

10.11.26.3 – контроллер домена, с которого собирали данные.

194.180.191.64 – сервер (явно принадлежавший злоумышленнику), на который отправлялись подозрительные, редко изменяющиеся команды.