



بیت‌های اطلاعاتی





The Little Ransomware That Couldn't Dharma

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

۴.....	مقدمه
۵.....	توضیحات اولیه
۵.....	دسترسی اولیه
۵.....	شناسایی
۶.....	اقدام بر روی اهداف (Action on Objectives)
۹.....	حرکت جانبی (Lateral Movement)
۹.....	IOC's





مقدمه

باچ‌افزارها همچنان یکی از جدی‌ترین تهدیدات امنیت سایبری محسوب می‌شوند و با وجود افزایش آگاهی سازمان‌ها و بهبود ابزارهای دفاعی، این نوع حملات بدون وقفه ادامه دارند. مهاجمان سایبری با بهره‌گیری از ابزارهای متنوع و تکنیک‌های مختلف تلاش می‌کنند به شبکه‌ها نفوذ کرده و با رمزگذاری داده‌ها، سازمان‌ها را مجبور به پرداخت باج کنند. اگرچه بسیاری از گزارش‌ها بر فعالیت گروه‌های بزرگ و سازمان‌یافته تمرکز دارند، اما در کنار آن‌ها مهاجمان کوچک‌تر و مستقل نیز حضور دارند که با وجود منابع محدودتر، همچنان قادر به ایجاد اختلال و خسارت قابل توجه در سیستم‌ها هستند.

فرآیند یک حمله باچ‌افزاری معمولاً شامل چند مرحله مشخص است؛ از دسترسی اولیه و شناسایی محیط هدف گرفته تا آماده‌سازی سیستم برای رمزگذاری داده‌ها. در مرحله شناسایی، مهاجم تلاش می‌کند ساختار شبکه، اشتراک‌های فایل و منابع قابل دسترس را بررسی کند تا بتواند اهداف مناسب را انتخاب کند. پس از آن، اقداماتی مانند حذف نسخه‌های پشتیبان سیستمی، پاک‌سازی لاگ‌ها و بستن برنامه‌های فعال انجام می‌شود تا فرآیند رمزگذاری بدون مانع انجام گیرد و امکان بازیابی داده‌ها برای قربانی دشوارتر شود.

در این گزارش، روند یک نمونه حمله باچ‌افزاری مورد بررسی قرار می‌گیرد که در آن مهاجم پس از دسترسی به سیستم، اقدام به شناسایی شبکه، آماده‌سازی محیط و در نهایت اجرای باچ‌افزار کرده است. تحلیل این مراحل می‌تواند دید بهتری نسبت به رفتار مهاجمان، ابزارهای مورد استفاده و تکنیک‌های به‌کاررفته در چنین حملاتی ارائه دهد و به درک بهتر نحوه شناسایی و مقابله با این تهدیدات کمک کند.





توضیحات اولیه

استفاده از باج افزارها همچنان بدون وقفه ادامه دارد، در سالی که فشارها به طور مداوم در حال افزایش هستند. اما در مقابل هر بازیگر بزرگ تهدید که شرکت های فهرست شده در فهرست Fortune را هدف قرار داده و به آنها نفوذ می کند، افراد کوچک تری هم وجود دارند که شاید به همان اندازه ماهر نباشند.

دسترسی اولیه

عامل تهدید در ساعت ۰۸:۵۸ به وقت UTC از آی پی ۲۱۷.۱۳۸.۲۰۲.۱۱۶ با حساب کاربری ادمین محلی وارد سیستم شد.

شناسایی

عامل تهدید مجموعه ابزارهای شخصی خود برای لیست برداری و جابه جایی در شبکه را به همراه داشت؛ ابزاری با نام NS.exe.

ما بارها و بارها مشاهده کرده ایم که از این ابزار برای اسکن کردن و نقشه برداری از File Share ها استفاده شده است.

این ابزار در ساعت ۰۹:۳۶ به وقت UTC اجرا شد.

```

C:\Oc\NS.exe
-----
Scan all network by mask and mount shared folders as drives
+ scan local volumes for unmounted drives.
+disabled restriction on the count of ip's(be careful!)
-----

#####
# Appreciate your time! #
# Network scan and mount include chek for unmounted local volumes. #
# '98' was add for standalone usage! #
#####

Select ip appdres for scan network:

1 Scan by: 10. 0
98 Scan local volumes for unmounted drives

Enter a number to scan:

```

USERPROFILE%\Desktop\Oc\NS.exe%





اقدام بر روی اهداف (Action on Objectives)

در ابتدا فایل batchی به نام shadow.bat اجرا شد که فایل‌های Shadow (نسخه‌های پشتیبان سیستمی) را حذف می‌کند.

```
vssadmin delete shadows /all
```

چند ثانیه بعد، فایل logdelete.bat اجرا شد که تمامی فایل‌های لاگ را پاک می‌کند.

پس از آن، فایل closeapps.bat اجرا شد که در یک حلقه، برنامه‌های رایج مختلف را بررسی و می‌بندد تا از قفل بودن فایل‌های باز جلوگیری کند؛

این کار باعث می‌شود فایل‌های حیاتی بدون مشکل رمزگذاری شوند و باز بودن آن‌ها مانع فرآیند رمزگذاری نشود.





```
Loop
rem VEAM
taskkill /F /IM Veeam.Backup.Agent.ConfigurationService.exe
taskkill /F /IM Veeam.Backup.BrokerService.exe
taskkill /F /IM Veeam.Backup.CatalogDataService.exe
taskkill /F /IM Veeam.Backup.CloudService.exe
taskkill /F /IM Veeam.Backup.Manager.exe
taskkill /F /IM Veeam.Backup.MountService.exe
taskkill /F /IM Veeam.Backup.Service.exe
taskkill /F /IM Veeam.Backup.WmiServer.exe
taskkill /F /IM Veeam.Guest.Interaction.Proxy.exe
taskkill /F /IM VeeamDeploymentSvc.exe
taskkill /F /IM VeeamNFSSvc.exe
taskkill /F /IM VeeamTransportSvc.exe
taskkill /F /IM Veeam.EndPoint.Manager.exe
taskkill /F /IM Veeam.EndPoint.Service.exe
taskkill /F /IM Veeam.EndPoint.Tray.exe
taskkill /F /IM sqlbrowser.exe
taskkill /F /IM sqlceip.exe
taskkill /F /IM sqlservr.exe
taskkill /F /IM sqlwriter.exe
taskkill /F /IM sqlagentc.exe
taskkill /F /IM ReportingServicesService.exe
taskkill /F /IM Ssms.exe
taskkill /F /IM fdhost.exe
taskkill /F /IM fdlauncher.exe
taskkill /F /IM MsDtsSrvr.exe
taskkill /F /IM msmdsrv.exe
taskkill /F /IM mysql.exe
taskkill /F /IM mysqld.exe
taskkill /F /IM w3wp.exe
taskkill /F /IM node.exe
taskkill /F /IM slack.exe
taskkill /F /IM wsusservice.exe
taskkill /F /IM SageCSClient.exe
taskkill /F /IM agent.exe
taskkill /F /IM Dropbox.exe
taskkill /F /IM OneDrive.exe
taskkill /F /IM acrotray.exe

rem MExchange
taskkill /F /IM store.exe
taskkill /F /IM MExchangeMailboxReplication.exe
taskkill /F /IM Microsoft.Exchange.ProtectedServiceHost.exe
taskkill /F /IM MExchangeThrottling.exe
taskkill /F /IM EdgeTransport.exe
taskkill /F /IM MExchangeTransportLogSearch.exe
taskkill /F /IM Microsoft.Exchange.RpcClientAccess.Service.exe
taskkill /F /IM Microsoft.Exchange.AddressBook.Service.exe
taskkill /F /IM DataCollectorSvc.exe
taskkill /F /IM Microsoft.Exchange.ServiceHost.exe
taskkill /F /IM Microsoft.Exchange.ContentFilter.Wrapper.exe
taskkill /F /IM MExchangeMailboxAssistants.exe
taskkill /F /IM msexchangerepl.exe
taskkill /F /IM Microsoft.Exchange.Search.ExSearch.exe
taskkill /F /IM Microsoft.Exchange.EdgeSyncSvc.exe
taskkill /F /IM MsExchangeFDS.exe
taskkill /F /IM MExchangeMailSubmission.exe
taskkill /F /IM MExchangeTransport.exe
taskkill /F /IM Microsoft.Exchange.AntispamUpdateSvc.exe
```





کلیدهای Run در رجیستری و همچنین دو پوشه Startup برای فایل اصلی باج افزار با نام 1pgp.exe ایجاد شدند.

C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1pgp.exe

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\1pgp.exe

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\1pgp.exe

در نهایت، باج افزار اجرا شد و سیستم را قفل کرد.

این باج افزار را می توان بر اساس مسیر PDB موجود در رشته های داخل فایل، به خانواده باج افزار Dharma/Crysis مرتبط دانست.

size	58 (bytes)
format	RSDS
debugger-stamp	0x58B8AF72 (Thu Mar 02 23:49:06 2017)
path	c:\crysis\release\pdb\payload.pdb
guid	906D7E25-96FC-4243-8EC3-87236B61A492

یک یادداشت باج نسبتاً مختصر (با جزئیات کم) بر جای گذاشته شد.

```

FILES ENCRYPTED - Notepad
File Edit Format View Help
all your data has been locked us
You want to return?
Write email openpgp@foxmail.com

```





حرکت جانبی (Lateral Movement)

با وجود اینکه عامل تهدید با سطح دسترسی ادمین دامنه در حال اجرا بود، تلاشی برای حرکت جانبی در شبکه یا گسترش باج افزار خود انجام نداد.

IOC's

MISPPriv

5ee3822c-6828-418c-b619-62de950d210f and 68219.

1pgp.exe

1ebb6bb49ac1077c5e7eba4d56f6a3a1

1a37bb789c7bdda44330fd55aa292f5f76dada5d

2f2e75affe9217c7211043936678fb1777e2db4a8f1986b8805ddb1e84e9e99b

closeapps.bat

9b0d6df42f879ba969f82c7a0ab48bc6

b5d6f94f270a02abedc7484dc7214d15d2cee99e

e25245f98a23596e03e51535beb0f73c000de63e473580c4c26e7b8b01b4e593

Everything.exe

8add121fa398ebf83e8b5db8f17b45e0

c8107e5c5e20349a39d32f424668139a36e6cfd0

35c4a6c1474eb870eec901cef823cc4931919a4e963c432ce9efbb30c2d8a413

LogDelete.bat

fb9c610ba195f9b18a96b84c5e755df7

5e4f2074850cce0eab4d6165807e86c88b5b8c0b

e17ca6c764352c0a74e1e6b80278bb4395588df4bed64833b1b127ea2ca5c5fd

NS.exe

597de376b1f80c06d501415dd973dcec

629c9649ced38fd815124221b80c9d9c59a85e74

f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446

Shadow.bat

df8394082a4e5b362bdcb17390f6676d

5750248ff490ceec03d17ee9811ac70176f46614

da3f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878

217.138.202.116





```
YARA
/*
YARA Rule Set
Author: DFIR Report
Date: 2020-06-12
Identifier: dharmia-06-12-20
Reference: https://thedfirreport.com/
*/
/* Rule Set ----- */
import "pe"
rule vssadmin_Shadow_bat {
  meta:
    description = "dharmia-06-12-20 - file Shadow.bat"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "da3f155cfb98ce0add29a31162d23da7596da44ba2391389517fe1a2790da878"
  strings:
    $s1 = "vssadmin delete shadows /all" fullword ascii
  condition:
    uint16(0) == 0x7376 and filesize < 1KB and
    all of them
}
rule Network_Scanner_post_exploit_enumeration {
  meta:
    description = "dharmia-06-12-20 - file NS.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446"
  strings:
    $s1 = "CreateMutex error: %d" fullword ascii
    $s2 = "--Error mount \\\\$s\%s Code: %d" fullword wide
    $s3 = "-Found share \\\\$s\%s" fullword wide
    $s4 = "--Share \\\\$s\%s successfully mounted" fullword wide
    $s5 = "host %s is up" fullword ascii
    $s6 = "Get ip: %s and mask: %s" fullword wide
    $s7 = "GetAdaptersInfo failed with error: %d" fullword wide
    $s8 = "# Network scan and mount include chek for unmounted local volumes. #"
    fullword wide
}
```





```

    $s9 = "#####"
fullword wide /* reversed goodwill string
'#####' */
    $s10 = "Share %s successfully mounted" fullword wide
    $s11 = "Error mount %s %d" fullword wide
    $s12 = "Failed to create thread." fullword ascii
    $s13 = " start scan for shares. " fullword wide
    $s14 = "# '98' was add for standalone usage!          #" fullword wide
    $s15 = "Error, wrong value." fullword wide
    $s16 = "QueryDosDeviceW failed with error code %d" fullword wide
    $s17 = "FindFirstVolumeW failed with error code %d" fullword wide
    $s18 = "FindNextVolumeW failed with error code %d" fullword wide
    $s19 = "SetVolumeMountPointW failed with error code %d" fullword wide
    $s20 = "| + scan local volumes for unmounted drives.      |" fullword wide
condition:
    uint16(0) == 0x5a4d and filesize < 400KB and
    ( pe.imphash() == "0b0d8152ea7241cce613146b80a998fd" or 8 of them )
}
rule Dharma_ransomware_1pgp {
  meta:
    description = "dharma-06-12-20 - file 1pgp.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "2f2e75affe9217c7211043936678fb1777e2db4a8f1986b8805ddb1e84e9e99b"
  strings:
    $x1 = "C:\\crysis\\Release\\PDB\\payload.pdb" fullword ascii
    $s2 = "sssssbs" fullword ascii
    $s3 = "sssssbs" fullword ascii
    $s4 = "9c%Q%f" fullword ascii
    $s5 = "jNYZO\\" fullword ascii
    $s6 = "RSDS%~m" fullword ascii
    $s7 = "xy ?*5" fullword ascii
    $s8 = "<a-g6J" fullword ascii
    $s9 = "]q)WtH?" fullword ascii
    $s10 = "s=9uo^" fullword ascii
        $s11 = "\"iMw\\e" fullword ascii
        $s12 = "{?nT*}2g" fullword ascii
        $s13 = "h*UqD*" fullword ascii
        $s14 = "b,_f n7" fullword ascii
        $s15 = "+mm7S%!" fullword ascii

```





```
$s16 = "+L]DAb" fullword ascii
$s17 = "nq0<3AD" fullword ascii
$s18 = "U2cUbO" fullword ascii
$s19 = ";C!|E2z" fullword ascii
$s20 = "P)8$X=" fullword ascii
condition:
  uint16(0) == 0x5a4d and filesize < 300KB and
  ( pe.imphash() == "f86dec4a80961955a89e7ed62046cc0e" or ( 1 of ($x*) or 4 of them ) )
}
rule closeapps_bat {
  meta:
    description = "dharma-06-12-20 - file closeapps.bat"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "e25245f98a23596e03e51535beb0f73c000de63e473580c4c26e7b8b01b4e593"
  strings:
    $x1 = "taskkill /F /IM MExchangeTransportLogSearch.exe" fullword ascii
    $x2 = "taskkill /F /IM Veeam.Backup.Agent.ConfigurationService.exe" fullword ascii
    $x3 = "taskkill /F /IM MExchangeTransport.exe" fullword ascii
    $x4 = "taskkill /F /IM EdgeTransport.exe" fullword ascii
    $x5 = "taskkill /F /IM Microsoft.Exchange.ServiceHost.exe" fullword ascii
    $x6 = "taskkill /F /IM Microsoft.Exchange.ProtectedServiceHost.exe" fullword ascii
    $x7 = "taskkill /F /IM agent.exe" fullword ascii
    $x8 = "taskkill /F /IM fdhost.exe" fullword ascii
    $x9 = "taskkill /F /IM MExchangeThrottling.exe" fullword ascii
    $x10 = "taskkill /F /IM sqlagentc.exe" fullword ascii
    $x11 = "taskkill /F /IM Microsoft.Exchange.ContentFilter.Wrapper.exe" fullword ascii
    $x12 = "taskkill /F /IM Veeam.Backup.CatalogDataService.exe" fullword ascii
    $x13 = "taskkill /F /IM cbInterface.exe" fullword ascii
    $x14 = "taskkill /F /IM httpd.exe" fullword ascii
    $x15 = "taskkill /F /IM VeeamTransportSvc.exe" fullword ascii
    $x16 = "taskkill /F /IM cbService.exe" fullword ascii
    $x17 = "taskkill /F /IM Veeam.Backup.BrokerService.exe" fullword ascii
    $x18 = "taskkill /F /IM wsusservice.exe" fullword ascii
    $x19 = "taskkill /F /IM pvxcom.exe" fullword ascii
    $x20 = "taskkill /F /IM Veeam.Backup.MountService.exe" fullword ascii
  condition:
    uint16(0) == 0x6c3a and filesize < 10KB and
    1 of ($x*)
}
```





```
rule LogDelete_bat {
  meta:
    description = "dharma-06-12-20 - file LogDelete.bat"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "e17ca6c764352c0a74e1e6b80278bb4395588df4bed64833b1b127ea2ca5c5fd"
  strings:
    $s1 = "FOR /F \"delims=\" %I IN ('WEVTUTIL EL') DO (WEVTUTIL CL \"%I\") " fullword ascii
  condition:
    uint16(0) == 0x4f46 and filesize < 1KB and
    all of them
}

rule Everything_seach_tool {
  meta:
    description = "dharma-06-12-20 - file Everything.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "35c4a6c1474eb870eec901cef823cc4931919a4e963c432ce9efbb30c2d8a413"
  strings:
    $x1 = "<assembly xmlns=\"urn:schemas-microsoft-com:asm.v1\" manifestVersion=\"1.0\"
xmlns:asmv3=\"urn:schemas-microsoft-com:asm.v3\"><a" ascii
    $s2 = "\" version=\"6.0.0.0\" processorArchitecture=\"*\"
publicKeyToken=\"6595b64144ccf1df\" language=\"*\"></assemblyIdentity></depen" ascii
    $s3 = "http://www.voidtools.com/downloads/" fullword ascii
    $s4 = "http://www.voidtools.com/downloads/#language" fullword ascii
    $s5 = "Folder\\shell\\%s\\command" fullword ascii
    $s6 = "Directory\\background\\shell\\%s\\command" fullword ascii
    $s7 = "Directory\\Background\\shell\\%s\\command" fullword ascii
    $s8 = "yIdentity version=\"1.0.0.0\" processorArchitectur
e=\"*\" name=\"Everything\" type=\"win32\"></assemblyIdentity><description>Eve" ascii
    $s9 = "; settings stored in %APPDATA%\\Everything\\Everything.ini" fullword ascii
    $s10 = "Host the pipe server with the security descriptor." fullword ascii
    $s11 = "http://www.voidtools.com/support/everything/" fullword ascii
    $s12 = "username:password@host:port" fullword ascii
    $s13 = "<html><meta http-equiv=\"Content-Type\" content=\"text/html;
charset=utf-8\"><meta name=\"viewport\" content=\"width=512\"><head" ascii
    $s14 = "\\.\PIPE\\Everything Service" fullword ascii
    $s15 = "Everything Service Debug Log.txt" fullword wide
```





```

    $s16 = "Auto detect will attempt to read file contents with the associated IFilter." fullword
ascii
    $s17 = "processed %l64u / %l64u file records" fullword ascii
    $s18 = "SERVICE_SERVER_COMMAND_REFS_MONITOR_READ_USN_JOURNAL_DATA read
ok %d" fullword ascii
    $s19 = "Store settings and data in %APPDATA%\\Everything?" fullword ascii
    $s20 = "http://www.voidtools.com/donate/" fullword ascii
condition:
    uint16(0) == 0x5a4d and filesize < 5000KB and
    ( pe.imphash() == "e7a8222fca78bde6fe29c9cc10d97ca2" or ( 1 of ($x*) or 4 of them ) )
}
/* Super Rules ----- */
rule Everything_search_tool_super {
meta:
    description = "dharma-06-12-20 - from files Everything.exe, Everything.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-12"
    hash1 = "35c4a6c1474eb870eec901cef823cc4931919a4e963c432ce9efbb30c2d8a413"
    hash2 = "35c4a6c1474eb870eec901cef823cc4931919a4e963c432ce9efbb30c2d8a413"
strings:
    $s1 = "-disable-run-as-admin" fullword ascii /* Goodware String - occured 1 times */
    $s2 = "type=%s;" fullword ascii /* Goodware String - occured 1 times */
    $s3 = "EVERYTHING" fullword ascii /* Goodware String - occured 1 times */
    $s4 = "-install-run-on-system-startup" fullword ascii /* Goodware String - occured 2 times */
    $s5 = "-uninstall-url-protocol" fullword ascii /* Goodware String - occured 2 times */
    $s6 = "-app-data" fullword ascii /* Goodware String - occured 2 times */
    $s7 = "-uninstall-service" fullword ascii /* Goodware String - occured 2 times */
    $s8 = "-uninstall-efu-association" fullword ascii /* Goodware String - occured 2 times */
condition:
    ( uint16(0) == 0x5a4d and filesize < 5000KB and pe.imphash() ==
    "e7a8222fca78bde6fe29c9cc10d97ca2" and ( all of them )
    ) or ( all of them )
}

```

منبع:

<https://thedfirreport.com/2020/06/16/the-little-ransomware-that-couldnt-dharma>

