



# Summary

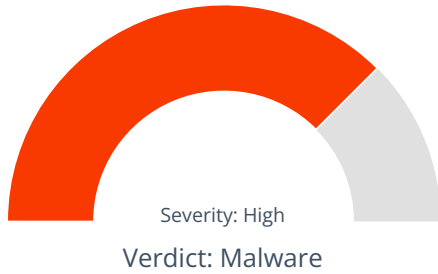
**File Name:** db1666bf21e0ce2110ad319e29edf930a8fec7e2d53b5daa6f4c1eafcea50a79.ex  
**File Type:** PE32 executable (GUI) Intel 80386, for MS Windows  
**SHA1:** 2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c  
**MD5:** 6b4a58489c8865a8033895d4f12ccd3a



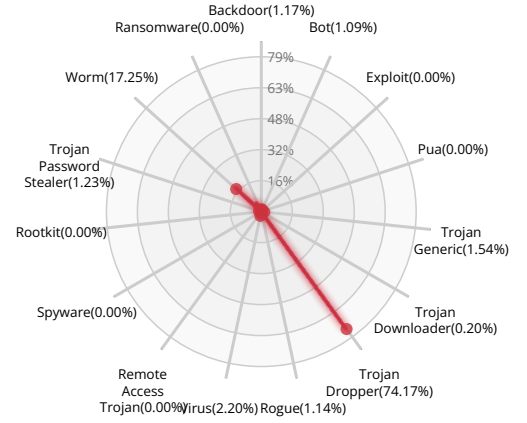
**MALWARE**

Valkyrie Final Verdict

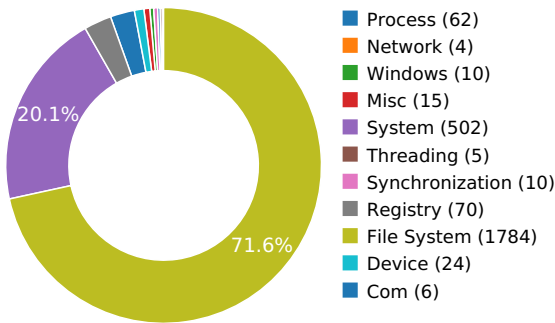
## DETECTION SECTION



## CLASSIFICATION



## HIGH LEVEL BEHAVIOR DISTRIBUTION



## ACTIVITY OVERVIEW



## Activity Details

### INFORMATION DISCOVERY



Reads data out of its own binary image

Show sources

### NETWORKING



Attempts to connect to a dead IP:Port (1 unique times)

Show sources

### LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS



Attempts to disable Windows Auto Updates

Show sources

### DATA OBFUSCATION



Drops a binary and executes it

Show sources

### PERSISTENCE AND INSTALLATION BEHAVIOR



Installs itself for autorun at Windows startup

Show sources

### MALWARE ANALYSIS SYSTEM EVASION



Attempts to modify Explorer settings to prevent hidden files from being displayed

Show sources

Creates a hidden or system file

Show sources



## Behavior Graph

## Behavior Summary

### ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Users\user\AppData\Local\Temp\2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c.exe
C:\Users\user\nioocem.exe
\\?\MountPointManager
\Device\Afd\AsyncSelectHlp
C:\Users\user\nioocem.exe.cfg

### READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation

### MODIFIED FILES

C:\Users\user\nioocem.exe
\Device\Afd\AsyncSelectHlp

**RESOLVED APIS**

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

oleaut32.dll.OleLoadPictureEx

oleaut32.dll.DispCallFunc

oleaut32.dll.LoadTypeLibEx

oleaut32.dll.UnRegisterTypeLib

oleaut32.dll.CreateTypeLib2

oleaut32.dll.VarDateFromUpdate

oleaut32.dll.VarUpdateFromDate

oleaut32.dll.GetAltMonthNames

oleaut32.dll.VarNumFromParseNum

oleaut32.dll.VarParseNumFromStr

oleaut32.dll.VarDecFromR4

oleaut32.dll.VarDecFromR8

oleaut32.dll.VarDecFromDate

oleaut32.dll.VarDecFromI4

oleaut32.dll.VarDecFromCy

oleaut32.dll.VarR4FromDec

oleaut32.dll.GetRecordInfoFromTypeInfo

oleaut32.dll.GetRecordInfoFromGuids

oleaut32.dll.SafeArrayGetRecordInfo

oleaut32.dll.SafeArraySetRecordInfo

oleaut32.dll.SafeArrayGetIID

oleaut32.dll.SafeArraySetIID

oleaut32.dll.SafeArrayCopyData

oleaut32.dll.SafeArrayAllocDescriptorEx

oleaut32.dll.SafeArrayCreateEx

oleaut32.dll.VarFormat

oleaut32.dll.VarFormatDateTime

oleaut32.dll.VarFormatNumber

oleaut32.dll.VarFormatPercent

oleaut32.dll.VarFormatCurrency

oleaut32.dll.VarWeekdayName

oleaut32.dll.VarMonthName

oleaut32.dll.VarAdd

oleaut32.dll.VarAnd

oleaut32.dll.VarCat

oleaut32.dll.VarDiv

oleaut32.dll.VarEqv

oleaut32.dll.VarIdiv

oleaut32.dll.VarImp

oleaut32.dll.VarMod

oleaut32.dll.VarMul

oleaut32.dll.VarOr

oleaut32.dll.VarPow

oleaut32.dll.VarSub

oleaut32.dll.VarXor

oleaut32.dll.VarAbs

oleaut32.dll.VarFix

oleaut32.dll.VarInt

oleaut32.dll.VarNeg

oleaut32.dll.VarNot

oleaut32.dll.VarRound

oleaut32.dll.VarCmp

oleaut32.dll.VarDecAdd

oleaut32.dll.VarDecCmp

oleaut32.dll.VarBstrCat

oleaut32.dll.VarCyMulI4

oleaut32.dll.VarBstrCmp

ole32.dll.CoCreateInstanceEx

ole32.dll.CLSIDFromProgIDEx

sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary

user32.dll.GetSystemMetrics

user32.dll.MonitorFromWindow

user32.dll.MonitorFromRect

user32.dll.MonitorFromPoint

user32.dll.EnumDisplayMonitors

user32.dll.GetMonitorInfoA

user32.dll.GetKeyboardLayoutList

kernel32.dll.GetModuleFileNameW

user32.dll.CallWindowProcW

kernel32.dll.Sleep

shell32.dll.SHGetSpecialFolderPathW

advapi32.dll.GetUserNameW

kernel32.dll.OpenMutexW

## REGISTRY KEYS

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Nls\Codepage

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950

HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\VBA\Monitors

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c.exe

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\nioocem

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate

## READ FILES

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c.exe

\Device\Afd\AsyncSelectHlp

C:\Users\user\nioocem.exe

## MODIFIED REGISTRY KEYS

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\nioocem

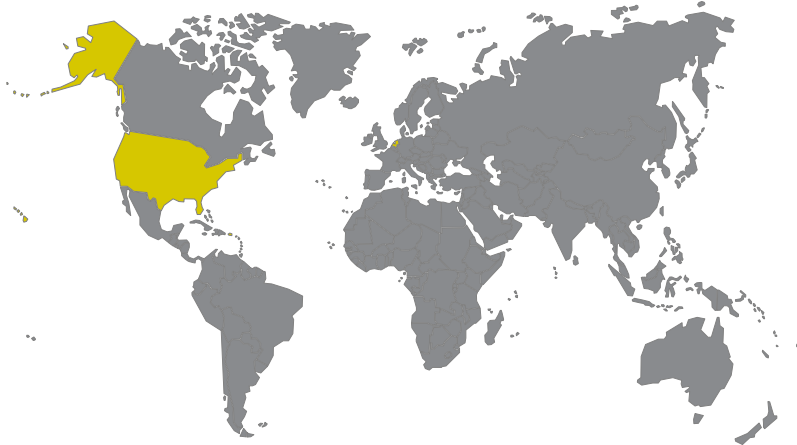
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

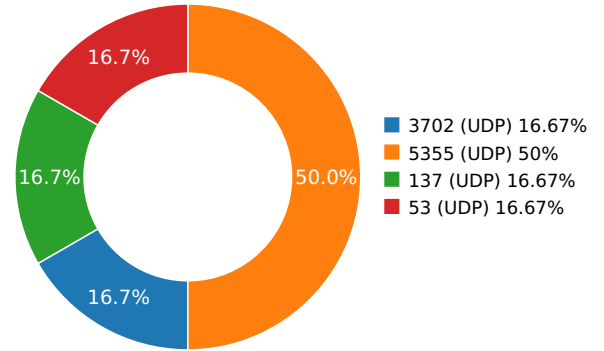
HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate

## Network Behavior

### CONTACTED IPS



### NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	77.247.183.155	Netherlands	43350	Customer 1820	Malware Process
ns1.musiczipz.com	216.245.214.84	United States	46475	Limestone Networks, Inc.	Malware Process

### DNS QUERIES

Request	Type
ns1.musiczipz.com	A
<b>Answers</b>	
- 77.247.183.155 (A)	

### UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.16874909401	Sandbox	224.0.0.252	5355
3.20888805389	Sandbox	192.168.56.255	137
3.21701812744	Sandbox	224.0.0.252	5355
3.22019004822	Sandbox	239.255.255.250	3702
5.81230807304	Sandbox	224.0.0.252	5355
14.8288121223	Sandbox	8.8.4.4	53

## DETAILED FILE INFO

## CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\Nioocem.Exe	<b>Type</b> : PE32 executable (GUI) Intel 80386, for MS Windows <b>MD5</b> : ba77f63da2dc9c435c832fdd27a416f1 <b>SHA-1</b> : 591dd1bcd069a88612673a083e3c3473bebb32da <b>SHA-256</b> : 3b4007cb265448cb3b9611d80d4f5578c94d578c <b>SHA-512</b> : 06a1bccbf7fe4aa2bbd9e9c655656a61eae9bc1a! <b>Size</b> : 315.392 Kilobytes.

## MATCH YARA RULES

MATCH RULES

## STATIC FILE INFO

<b>File Name:</b>	db1666bf21e0ce2110ad319e29edf930a8fec7e2d53b5daa6f4c1eafcea50a79.ex
<b>File Type:</b>	PE32 executable (GUI) Intel 80386, for MS Windows
<b>SHA1:</b>	2fe9b1b874c6bc2bf266e81d3ff9a483b50ec40c
<b>MD5:</b>	6b4a58489c8865a8033895d4f12ccd3a
<b>First Seen Date:</b>	2023-07-07 11:58:41.254154 ( 3 years ago )
<b>Number Of Clients Seen:</b>	6
<b>Last Analysis Date:</b>	2023-07-07 11:58:41.254154 ( 3 years ago )
<b>Human Expert Analysis Date:</b>	2023-07-07 23:16:13.355546 ( 3 years ago )
<b>Human Expert Analysis Result:</b>	Malware

DETAILED FILE INFO

**ADDITIONAL FILE INFORMATION**

**PE Headers**

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	☐
Number Of Sections	3
Trid	☐
Compilation Time Stamp	0x4FAD3A0F [Fri May 11 16:10:55 2012 UTC]
Entry Point	0x401220 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	315392
Ssdeep	
Sha256	db1666bf21e0ce2110ad319e29edf930a8fec7e2d53b5daa6f4c1eafcea50a79
Exifinfo	☐
Mime Type	application/x-dosexec
Imphash	

**PE Sections**

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2a5f4	0x2b000	5.15261668063	b51eeabf470908a19dc8e9aa47405ed4
.data	0x2c000	0x1918	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x2e000	0x1e410	0x1f000	5.27536041721	c676d80a443297261ddb1cf633e335e5

**CERTIFICATE VALIDATION**

- Certificate Validation is not Applicable ?

SCREENSHOTS

