内存转储文件自动分析报告

基本情况

受理时间	2023-10-30_15:07:56
待检材料	192.168.56.134_2023_10_30_14:49:04
检测时间	2023-10-30_15:07:56
检测方	恶意软件智能检测系统

分析内容

——内存系统信息——

可能的操作系统	Win2008SP1x86, Win7SP1x64, Win7SP0x64
版本	
DTB 目录表基址	1601536
KDBG 信息	2023-04-14_15:07:56
处理器核数	2
Windows 服务包	1
版本	
镜像日期和时间	2023-03-02 05:58:32 UTC+0000
镜像本地日期和	2023-03-02 13:58:32 +0800
时间	

——恶意进程信息——

提供本产品扫描出的恶意进程信息。具体包括**恶意进程命令行信息、恶意进**程 DLL 加载信息、DLL 对应函数加载信息以及恶意 VAD 节点信息

恶意进程命令行信息

提供本产品检测出的**恶意进程的进程 ID、进程名**和**命令行加载信息**

PID	进程名	命令行参数
		<pre>"C:\Program Files (x86)\Mozilla Firefox</pre>
		\firefox.exe" -contentprocchannel="1
		196.20.167375406\430506970" -parentBuil
		dID 20230403170909 -prefsHandle 1928 -p
3488	firefox.exe	refMapHandle 1916 -prefsLen 8036 -prefM
		apSize 216283 -appdir "C:\Program Files
		(x86)\Mozilla Firefox\browser" - 1196
		"\\.\pipe\gecko-crash-server-pipe.1196
		" 1824 rdd
2100	i avel and ave	"C:\Program Files (x86)\Internet Explor
2180	iexplore.exe	er\iexplore.exe"
		"C:\Program Files (x86)\Internet Explor
488	iexplore.exe	er\iexplore.exe" SCODEF:2180 CREDAT:798
		73
1106	C: 100 Co. 100	<pre>"C:\Program Files (x86)\Mozilla Firefox</pre>
1196	firefox.exe	\firefox.exe" -first-startup
		<pre>"C:\Program Files (x86)\Mozilla Firefox</pre>
		\firefox.exe" -contentprocchannel="1
		196.13.1053559141\1653985308" -childID
		2 -isForBrowser -prefsHandle 2124 -pref
1836	firefox.exe	MapHandle 2120 -prefsLen 3486 -prefMapS
		ize 216283 -parentBuildID 2023040317090
		9 -appdir "C:\Program Files (x86)\Mozil
		la Firefox\browser" - 1196 "\\.\pipe\ge
		cko-crash-server-pipe.1196" 2136 tab
2672	firefox.exe	"C:\Program Files (x86)\Mozilla Firefox

		\firefox.exe" -contentprocchannel="1
		196.52.995347841\1174536823" -childID 7
		-isForBrowser -prefsHandle 4752 -prefM
		apHandle 4712 -prefsLen 20398 -prefMapS
		ize 216283 -parentBuildID 2023040317090
		9 -appdir "C:\Program Files (x86)\Mozil
		la Firefox\browser" - 1196 "\\.\pipe\ge
		cko-crash-server-pipe.1196" 4748 tab
		"C:\Program Files (x86)\Mozilla Firefox
		\firefox.exe" -contentprocchannel="1
		196.0.1728630941\770701979" -parentBuil
		dID 20230403170909 -prefsHandle 1424 -p
2808	2808 firefox.exe	refMapHandle 1288 -prefsLen 1 -prefMapS
		ize 216283 -appdir "C:\Program Files (x
		86)\Mozilla Firefox\browser" - 1196 "\
		\.\pipe\gecko-crash-server-pipe.1196" 1
		524 gpu
		"C:\Program Files (x86)\Mozilla Firefox
		\firefox.exe" -contentprocchannel="1
		196.45.826126589\1310194129" -childID 6
		-isForBrowser -prefsHandle 4552 -prefM
2428	firefox.exe	apHandle 4608 -prefsLen 20398 -prefMapS
		ize 216283 -parentBuildID 2023040317090
		9 -appdir "C:\Program Files (x86)\Mozil
		la Firefox\browser" - 1196 "\\.\pipe\ge
		cko-crash-server-pipe.1196" 4532 tab

该部分提供恶意进程加载的动态链接库信息,包括进程 ID、进程名、文件 大小、DLL 加载名称及加载次数

PID	进程名	加载次数	文件大小	DLL 名称				
348	firefox.	CEESE	F22400	Ca) Diagram				
8	exe	65535	532480	C:\Program				
348	firefox.	CEE2E	1740000	C:\Windows\SYSTEM32\ntdll.d				
8	exe	65535	1740800	11				
348	firefox.	2	250040	C:\Windows\SYSTEM32\wow64.d				
8	exe	3	258048	11				
348	firefox.	4	276022	C:\Windows\SYSTEM32\wow64wi				
8	exe	1	376832	n.dll				
348	firefox.	4	22760	C:\Windows\SYSTEM32\wow64cp				
8	exe	1	32768	u.dll				
218	iexplor	CEESE	670036	C.\D.				
0	e.exe	65535	679936	C:\Program				
218	iexplor	CEE2E	1740000	C:\Windows\SYSTEM32\ntdll.d				
0	e.exe	65535	1740800	11				
218	iexplor	2	250040	C:\Windows\SYSTEM32\wow64.d				
0	e.exe	3	258048	11				
218	iexplor	4	276022	C:\Windows\SYSTEM32\wow64wi				
0	e.exe	1	376832	n.dll				
218	iexplor	4	22760	C:\Windows\SYSTEM32\wow64cp				
0	e.exe	1	32768	u.dll				
400	iexplor	65525	670026	C.\ Dnognam				
488	e.exe	65535	679936	C:\Program				
400	iexplor	CEEDE	1740000	C:\Windows\SYSTEM32\ntdll.d				
488	e.exe	65535	1740800	11				
488	iexplor	3	258048	C:\Windows\SYSTEM32\wow64.d				

	e.exe			11				
400	iexplor	1	276022	C:\Windows\SYSTEM32\wow64wi				
488	e.exe	1	376832	n.dll				
400	iexplor	1	22760	C:\Windows\SYSTEM32\wow64cp				
488	e.exe	1	32768	u.dll				
183	firefox.	65535	E22490	C.\ Dnognam				
6	exe	05555	532480	C:\Program				
183	firefox.	65535	1740800	C:\Windows\SYSTEM32\ntdll.d				
6	exe	05555	1740800	11				
183	firefox.	3	258048	C:\Windows\SYSTEM32\wow64.d				
6	exe	3	238048	11				
183	firefox.	1	376832	C:\Windows\SYSTEM32\wow64wi				
6	exe	_	370832	n.dll				
183	firefox.	1	32768	C:\Windows\SYSTEM32\wow64cp				
6	exe	_	32708	u.dll				
119	firefox.	65535	532480	C:\Program				
6	exe	03333	332480	C. (Program				
119	firefox.	65535	1740800	C:\Windows\SYSTEM32\ntdll.d				
6	exe	03333	1740800	11				
119	firefox.	3	258048	C:\Windows\SYSTEM32\wow64.d				
6	exe	3	238048	11				
119	firefox.	1	376832	C:\Windows\SYSTEM32\wow64wi				
6	exe	1	370832	n.dll				
119	firefox.	1	32768	C:\Windows\SYSTEM32\wow64cp				
6	exe	_	32700	u.dll				
267	firefox.	65535	532480	C:\Program				
2	exe	03333	332400	C. (FIOSITAIII				
267	firefox.	65535	1740800	C:\Windows\SYSTEM32\ntdll.d				
2	exe	دورون	1740000	11				

267	C: C			C.\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
267	firefox.	3	258048	C:\Windows\SYSTEM32\wow64.d
2	exe			11
267	firefox.	1	376832	C:\Windows\SYSTEM32\wow64wi
2	exe	_	370032	n.dll
267	firefox.	1	22760	C:\Windows\SYSTEM32\wow64cp
2	exe	1	32768	u.dll
280	firefox.	65525	522400	6.15
8	exe	65535	532480	C:\Program
280	firefox.			C:\Windows\SYSTEM32\ntdll.d
8	exe	65535	1740800	11
280	firefox.			C:\Windows\SYSTEM32\wow64.d
8	exe	3	258048	11
280	firefox.			C:\Windows\SYSTEM32\wow64wi
8	exe	1	376832	n.dll
280	firefox.			C:\Windows\SYSTEM32\wow64cp
8	exe	1	32768	u.dll
242	firefox.			
	exe	65535	532480	C:\Program
	firefox.			C:\Windows\SYSTEM32\ntdll.d
		65535	1740800	11
	exe			
	firefox.	3	258048	C:\Windows\SYSTEM32\wow64.d
8	exe			11
242	firefox.	1	376832	C:\Windows\SYSTEM32\wow64wi
8	exe	-	3,0032	n.dll
242	firefox.	1	22769	C:\Windows\SYSTEM32\wow64cp
8	exe	1	32768	u.dll

加载函数信息

讲程 PID: 2428 讲程名: firefox.exe

[加载 DLL 名称: mozglue.dll]

- | ??2@YAPAXI@Z
- | ??3@YAXPAX@Z
- | ??3@YAXPAXI@Z
- | ?? U@YAPAXI@Z
- | ?? V@YAXPAX@Z
- ?BeginProcessRuntimeInit@detail@mscom@mozilla@@YAAA NXZ
- ?DllBlocklist Initialize@@YAXI@Z
- | ?DllBlocklist_SetBasicDllServices@@YAXPAVDllServicesBase@detail@glue@mozilla@@@Z

恶意节点信息

进程 3488 - VAD 节点地址 0xba0000

000000D0: 00 00 00	00 00 00 00	00 00 00 00 00	00 00 00 00	
000000E0: 00 00 00	00 00 00 00	00 50 45 00 00	4C 01 04 00	PEL
000000F0: 3F 9B D	4D 00 00 00	00 00 00 00 00	E0 00 02 01	?M
进程 2180 - VAD 节	点地址 0x46300	000		
00000000: 4D 5A 90	00 03 00 00	00 04 00 00 00	FF FF 00 00	MZ
00000010: B8 00 00	00 00 00 00	00 40 00 00 00	00 00 00 00	
00000020: 00 00 00	00 00 00 00	00 00 00 00 00	00 00 00 00	• • • • • • • • • • • • • • • • • • • •
00000030: 00 00 00	00 00 00 00	00 00 00 00 00	E8 00 00 00	
00000040: 0E 1F B	A 0E 00 B4 09	CD 21 B8 01 4C	CD 21 54 68	!L.!Th
00000050: 69 73 20	70 72 6F 67	72 61 6D 20 63	61 6E 6E 6F	is program canno
00000060: 74 20 63	2 65 20 72 75	6E 20 69 6E 20	44 4F 53 20	t be run in DOS
00000070: 6D 6F 64	65 2E 0D 0D	0A 24 00 00 00	00 00 00 00	mode\$
00000080: 7E 87 63	3 89 3A E6 0D	DA 3A E6 0D DA	3A E6 0D DA	~.c.::
00000090: D2 F9 09	DA 38 E6 0D	DA B9 FA 03 DA	3B E6 0D DA	8;
000000A0: 1D 20 60	DA 39 E6 0D	DA 1D 20 76 DA	2F E6 0D DA	.`.9 v./
000000B0: 3A E6 00	DA F1 E6 0D	DA 24 B4 89 DA	04 E6 0D DA	:\$
000000C0: 24 B4 90	DA 3B E6 0D	DA 52 69 63 68	3A E6 0D DA	\$;Rich:
000000D0: 00 00 00	00 00 00 00	00 00 00 00 00	00 00 00 00	• • • • • • • • • • • • • • • • • • • •
000000E0: 00 00 00	00 00 00 00	00 50 45 00 00	4C 01 04 00	PEL
000000F0: 3F 9B D	4D 00 00 00	00 00 00 00 00	E0 00 02 01	?M
进程 488 - VAD 节点	地址 0x41f006	00		
00000000: 4D 5A 90	00 03 00 00	00 04 00 00 00	FF FF 00 00	MZ
00000010: B8 00 00	00 00 00 00	00 40 00 00 00	00 00 00 00	
00000020: 00 00 00	00 00 00 00	00 00 00 00 00	00 00 00 00	
00000030: 00 00 00	00 00 00 00	00 00 00 00 00	E8 00 00 00	
00000040: 0E 1F B	A 0E 00 B4 09	CD 21 B8 01 4C	CD 21 54 68	!!
00000050: 69 73 20	70 72 6F 67	72 61 6D 20 63	61 6E 6E 6F	is program canno
00000060: 74 20 62	2 65 20 72 75	6E 20 69 6E 20	44 4F 53 20	t be run in DOS

00000070: 6D 6F	64 65 2E	0D 0D 0A	24 00 0	00 00 00	00 00 00	omode\$
00000080: 7E 87	63 89 3A	E6 0D DA	3A E6 6	0D DA 3A	E6 0D D/	A ~.c.:
00000090: D2 F9	09 DA 38	E6 0D DA	B9 FA 6	03 DA 3B	E6 0D D/	۱;
000000A0: 1D 20	60 DA 39	E6 0D DA	1D 20 7	76 DA 2F	E6 0D D/	A . `.9 v./
000000B0: 3A E6	0C DA F1	E6 0D DA	24 B4 8	89 DA 04	E6 0D D/	A:\$
000000C0: 24 B4	9C DA 3B	E6 0D DA	52 69 6	63 68 3A	E6 0D D	A \$;Rich:
000000D0: 00 00	00 00 00	00 00 00	00 00 0	00 00 00	00 00 00)
000000E0: 00 00	00 00 00	00 00 00	50 45 6	00 00 4C	01 04 00)PEL
000000F0: 3F 9B	D1 4D 00	00 00 00	00 00 0	00 00 E0	00 02 0:	L ?M
进程 1836 - VAD	节点地址 6	0x7600000				
00000000: 4D 5A	90 00 03	00 00 00	04 00 6	00 00 FF	FF 00 00	9 MZ
00000010: B8 00	00 00 00	00 00 00	40 00 6	00 00 00	00 00 00)
00000020: 00 00	00 00 00	00 00 00	00 00 0	00 00 00	00 00 00)
00000030: 00 00	00 00 00	00 00 00	00 00 0	00 00 E8	00 00 00)
00000040: 0E 1F	BA 0E 00	B4 09 CD	21 B8 (01 4C CD	21 54 68	3!L.!Th
00000050: 69 73	20 70 72	6F 67 72	61 6D 2	20 63 61	6E 6E 6I	is program canno
00000060: 74 20	62 65 20	72 75 6E	20 69 6	6E 20 44	4F 53 20) t be run in DOS
00000070: 6D 6F	64 65 2E	0D 0D 0A	24 00 0	00 00 00	00 00 00	mode\$
00000080: 7E 87	63 89 3A	E6 0D DA	3A E6 6	0D DA 3A	E6 0D D/	A ~.c.::
00000090: D2 F9	09 DA 38	E6 0D DA	B9 FA 6	03 DA 3B	E6 0D D/	A8;
000000A0: 1D 20	60 DA 39	E6 0D DA	1D 20 7	76 DA 2F	E6 0D D/	A . `.9 v./
000000B0: 3A E6	0C DA F1	E6 0D DA	24 B4 8	89 DA 04	E6 0D D/	A:\$
000000C0: 24 B4	9C DA 3B	E6 0D DA	52 69 6	63 68 3A	E6 0D D/	A \$;Rich:
000000D0: 00 00	00 00 00	00 00 00	00 00 0	00 00 00	00 00 00	·
000000E0: 00 00	00 00 00	00 00 00	50 45 6	00 00 4C	01 04 00)PEL
000000F0: 3F 9B	D1 4D 00	00 00 00	00 00 0	00 00 E0	00 02 0	L ?M

00000000:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ
00000010:	В8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	
00000020:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	• • • • • • • • • • • • • • • • • • • •
00000030:	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00	• • • • • • • • • • • • • • • • • • • •
00000040:	0E	1F	ВА	0E	00	В4	09	CD	21	В8	01	4C	CD	21	54	68	!L.!Th
00000050:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode\$
00000080:	7E	87	63	89	ЗА	E6	0D	DA	3A	E6	0D	DA	3A	E6	0D	DA	~.c.::
00000090:	D2	F9	09	DA	38	E6	0D	DA	В9	FA	03	DA	3B	E6	0D	DA	8;
000000A0:	1D	20	60	DA	39	E6	0D	DA	1D	20	76	DA	2F	E6	0D	DA	. `.9 v./
000000В0:	3A	E6	0C	DA	F1	E6	0D	DA	24	В4	89	DA	04	E6	0D	DA	:\$
000000C0:	24	В4	9C	DA	3B	E6	0D	DA	52	69	63	68	3A	E6	0D	DA	\$;Rich:
000000D0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	• • • • • • • • • • • • • • • • • • • •
000000E0:	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	PEL
000000F0:	3F	9B	D1	4D	00	00	00	00	00	00	00	00	E0	00	02	01	?M
进程 2672	- V	AD =	节点	地址	止 0	xb4	100	00									
00000000:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ
00000010:	В8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	
00000020:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030:	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00	• • • • • • • • • • • • • • • • • • • •
00000040:	0E	1F	ВА	0E	00	В4	09	CD	21	В8	01	4C	CD	21	54	68	!!Th
00000050:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode\$
00000080:	7E	87	63	89	ЗА	E6	0D	DA	3A	E6	0D	DA	3A	E6	0D	DA	~.C.::
00000090:	D2	F9	09	DA	38	E6	0D	DA	В9	FA	03	DA	3B	E6	0D	DA	8;
000000A0:	1D	20	60	DA	39	E6	0D	DA	1D	20	76	DA	2F	E6	0D	DA	. `.9 v./

000000B0: 3A E6 0C DA F1 E6 0D DA 24	4 B4 89 DA 04 E6 0D DA :\$
00000000: 24 B4 9C DA 3B E6 0D DA 52	2 69 63 68 3A E6 0D DA \$;Rich:
000000D0: 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00
000000E0: 00 00 00 00 00 00 00 50	0 45 00 00 4C 01 04 00PEL
000000F0: 3F 9B D1 4D 00 00 00 00 00	0 00 00 00 E0 00 02 01 ?M
进程 2808 - VAD 节点地址 0xc20000	
00000000: 4D 5A 90 00 03 00 00 00 04	4 00 00 00 FF FF 00 00 MZ
00000010: B8 00 00 00 00 00 00 00 40	0 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00	0 00 00 00 E8 00 00 00
00000040: 0E 1F BA 0E 00 B4 09 CD 23	1 B8 01 4C CD 21 54 68!L.!Th
00000050: 69 73 20 70 72 6F 67 72 65	1 6D 20 63 61 6E 6E 6F is program canno
00000060: 74 20 62 65 20 72 75 6E 20	0 69 6E 20 44 4F 53 20 t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A 24	4 00 00 00 00 00 00 00 mode\$
00000080: 7E 87 63 89 3A E6 0D DA 3/	A E6 0D DA 3A E6 0D DA ~.c.:
00000090: D2 F9 09 DA 38 E6 0D DA B9	9 FA 03 DA 3B E6 0D DA8;
000000A0: 1D 20 60 DA 39 E6 0D DA 10	D 20 76 DA 2F E6 0D DA . `.9 v./
0000000B0: 3A E6 0C DA F1 E6 0D DA 24	4 B4 89 DA 04 E6 0D DA :\$
00000000: 24 B4 9C DA 3B E6 0D DA 52	2 69 63 68 3A E6 0D DA \$;Rich:
000000D0: 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00
000000E0: 00 00 00 00 00 00 00 50	0 45 00 00 4C 01 04 00PEL
000000F0: 3F 9B D1 4D 00 00 00 00 00	0 00 00 00 E0 00 02 01 ?M
进程 2428 - VAD 节点地址 0x8080000	
00000000: 4D 5A 90 00 03 00 00 00 04	4 00 00 00 FF FF 00 00 MZ
00000010: B8 00 00 00 00 00 00 00 40	0 00 00 00 00 00 00 00@
00000020: 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00
00000030: 00 00 00 00 00 00 00 00	0 00 00 00 E8 00 00 00

PS 树状图



——关键注册表信息——

注册表内容	注册表项名称
"C:\Foxmail 7.2\Foxmail.exe" -min	Foxmail
C:\Users\float\AppData\Roaming\Figggl.exe	Figggl

——网络行为信息——

网络连接情况

PID	本地地址	本地端口	协议类型	远程地址	远程端口
1196	10.10.10.26	49350	TCPv4	13.249.165.32	443
1196	10.10.10.26	49346	TCPv4	13.225.163.119	443
1196	10.10.10.26	49358	TCPv4	13.225.163.92	443
1196	10.10.10.26	49341	TCPv4	13.249.165.9	443
1196	Unknown	49289	TCPv4	23.37.124.72	80
2672	127.0.0.1	49277	TCPv4	127.0.0.1	49278
2180	10.10.10.26	49306	TCPv4	212.83.168.196	80
2180	Unknown	0	TCPv4	104.0.25.2	0
2180	10.10.10.26	49336	TCPv4	199.2.137.21	1863

域名及 DGA 域名判断

可疑 IP 域名查询	创建时间	恶意软件家族
bar-espanol-labodeg a-shibuya.com	2023-03-23 06:59:29	无结果
lebeurrenoisettetok yo.com	2023-03-25 15:50:47	None
bidsstalk.com	2023-04-03 02:07:01	None
eang.it	2023-03-26 03:14:21	None
sandbox-saloniris.c	2023-03-20 02:39:35	无结果
protect-my-privacy. org	2023-04-02 02:14:03	None
arajinn.site	2023-03-24 05:51:17	无结果
x3628929.ivps9x.u.a vast.com	2023-03-30 16:59:58	无结果
j8287141.ivps9x.u.a	2023-03-30 16:59:57	无结果

vast.com		
imagec07.247realmed	2023-03-17 21:26:02	无结果
static.inviziads.co m	2023-04-02 21:04:35	无结果
www.recommendation. world	2023-03-30 15:40:21	无结果
api.initialoptimize	2023-04-03 20:27:20	None
config.unityads.uni ty3d.com	2023-03-30 11:17:42	None
imagec16.247realmed ia.com	2023-03-30 21:19:49	None
ucarecdn.com	2023-04-02 21:04:42	无结果
search.expandedkey.	2023-04-01 22:39:53	无结果
api.wipmania.com	2023-04-13 14:57:55	无结果
api8.wipmania.com	2023-01-11 13:53:56	无结果
api7.wipmania.com	2023-01-11 13:53:54	无结果
www.wipmania.com	2019-11-04 20:13:46	无结果
alrond.com	2019-12-13 17:46:13	无结果
napi1.wipmania.com	2019-09-06 16:51:55	无结果
kvnforall.info	2019-08-06 06:32:45	无结果
www.kvnforall.info	2019-12-11 16:53:30	无结果
wipmania.com	2019-12-13 11:25:18	无结果
api2.wipmania.com	2019-09-25 02:03:38	无结果
www.vida-gamer.com	2019-12-28 10:34:55	None
www.pluto.iziger.pl	2023-02-22 00:37:16	None
www.blueverse.kz	2019-12-28 14:23:37	None

www.xxxd1.com	2019-12-28 11:21:34	None
www.xp54823.com	2019-12-28 11:19:34	None
mail.retk03.com	2023-02-22 21:58:26	无结果
mail.n1rx.asia	2023-02-11 21:17:29	无结果
ftp.zuf174.com	2023-01-14 10:35:11	无结果
www.cantvenlinea.bi	2023-02-22 11:45:46	无结果
webmail.pissa.org	2019-12-28 12:35:48	无结果

综合分析

经过系统分析,待检材料 192.168.56.163_2023-12-03 16:11:11 中 存在节点信息恶意软件痕迹。 经检测,恶意进程 ID 如下: 3488, 2180, 488, 1196, 1836, 2672, 2808, 2428,分析人员需要重点关注这些恶意进程的命令行执行信息、D LL 相关信息、 DLL 加载函数以及虚拟地址描述符详细信息。同时本产品提供恶意进程的调用信息, 分析人员可快速把握恶意进程的调用关系。本产品已将恶意进程以可执行文件的形式导出至本地, 分析人员可以在路径/MalProcessResult/192.168.56.163_2023-12-03 16:11:11 下根据需求自行分析查看。 此外,经检测,该恶意软件存在相关网络活动。