奇安信威胁情报中心

MD5	d75e03ebaba0c426d457684c510e8bd0
SHA1	81776da5d6cdcf7cb7566c5c984dba9b37810cd8
SHA256	be2ef75b60cd65b4401204ceb23c83f0504abb52998f90b32a50098ed0877f18
文件名称	a.pptx
文件类型	PowerPoint Microsoft Office Open XML Format Document
文件大小	30470字节
检测环境	Windows 7 x64
文件信誉	未检出
RAS检测	-
基因特征	注入 解压执行 探针 检测沙箱
分析时间	2023-03-24 09:44:38

恶意评分

0

未发现风险

威胁情报

威胁情报 (共计2条，当前展示2条)

IOC对象	情报类型	恶意类型	家族/团伙	标签
d75e03ebaba0c426d457684c510e8bd0	未知	-	-	
d41d8cd98f00b204e9800998ecf8427e	白	-	-	

AV引擎

检出率 **0/18 (0%)**

检测时间 **2023-03-24 09:46:39**

avast	✓	bd	✓
clamav	✓	huorong	✓
jowto	✓	mcafee	✓
microsoft	✓	qde2	✓
qde2-win	✓	qde2m	✓
qowl	✓	qowl-alpha	✓
qowl-beta	✓	ras	✓
symantec	✓	yara	✓
yara-beta	✓	yara-ras	✓

行为异常

全部收起

一个试图延迟分析任务的进程

描述: POWERPNT.EXE tried to sleep 1260 seconds, actually delayed analysis time by 60 seconds

修改非子进程的内存,可能是进程注入

类别: Process injection

入侵指标: Process 556 manipulating memory of non-child process 2504

类型: ioc

类型: call

分配可读、可写、可执行内存空间(通常为了解压自身)

奇安信威胁情报中心

时间&API	参数&栈跟踪	返回状态	返回值	进程ID
2023-03-24 09:43:41.453125 NtProtectVirtualMemory	base_address: 0x6b671000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:41.641125 NtAllocateVirtualMemory	allocation_type: 0x00002000 base_address: 0x03d10000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 65536 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:41.641125 NtAllocateVirtualMemory	allocation_type: 0x00001000 base_address: 0x03d10000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 8192 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:41.703125 NtAllocateVirtualMemory	allocation_type: 0x00001000 base_address: 0x03d12000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:41.750125 NtAllocateVirtualMemory	allocation_type: 0x00001000 base_address: 0x03d13000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:41.750125 NtAllocateVirtualMemory	allocation_type: 0x00001000 base_address: 0x03d14000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:47.187125 NtProtectVirtualMemory	base_address: 0x6b862000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:43:47.250125 NtAllocateVirtualMemory	allocation_type: 0x00001000 base_address: 0x03ed0000 heap_dep_bypass: 0 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 region_size: 8192 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556

2023-03-24 09:44:01.641125 NtProtectVirtualMemory	base_address: 0x5fff0000 heap_dep_bypass: 1 length: 65536 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:44:01.641125 NtProtectVirtualMemory	base_address: 0x76936000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:44:01.641125 NtProtectVirtualMemory	base_address: 0x76844000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:44:01.641125 NtProtectVirtualMemory	base_address: 0x76843000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556
2023-03-24 09:44:01.641125 NtProtectVirtualMemory	base_address: 0x76845000 heap_dep_bypass: 0 length: 4096 process_handle: 0xffffffff process_identifier: 556 protection: 0x00000040 stack_dep_bypass: 0 stack_pivoted: 0	1	0	556

在文件系统中创建(office)文档

类别:	file
入侵指标:	C:\Users\ADMINI~1\AppData\Local\Temp\~$a.pptx
类型:	ioc

收集信息到指纹系统(MachineGuid, DigitalProductId, SystemBiosDate)

类别:	registry
入侵指标:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid
类型:	ioc
类别:	registry
入侵指标:	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\14.0\Registration\{90140000-0011-0000-0000-0000000FF1CE}\DigitalProductID
类型:	ioc

静态分析

基本信息

a.pptx

文件类型	PowerPoint Microsoft Office Open XML Format Document

奇安信威胁情报中心

文件类型匹配度	50.5% (.PRDX/PRVX) SoftMaker Presentations Document 41.7% (.PPTX) PowerPoint Microsoft Office Open XML Format document 6.0% (.ZIP) Open Packaging Conventions container 1.3% (.ZIP) ZIP compressed archive 0.3% (.BIN) PrintFox/Pagefox bitmap (var. P)
文件大小	30470字节
MD5	d75e03ebaba0c426d457684c510e8bd0
SHA1	81776da5d6cdcf7cb7566c5c984dba9b37810cd8
SHA256	be2ef75b60cd65b4401204ceb23c83f0504abb52998f90b32a50098ed0877f18
SHA512	f77b0aca089ac7eecf63b864557deaee88e0989c8b61d93200d810e34744ae4c605ab69efefdd990c2b526ddfd5c5fa0729fe772e827980f0cf559b3fc72c5e1
SSDeep	768:n9T11f3S0yS00SneS0JSnjS0MS0bS02S0dS0EJVILsoScCz70rZTnUZ2fXQHQE6N:nRmMhz7AnUMUbooCDkIr

Exiftool文件元数据

FileAccessDate	2023:03:24 09:43:32+08:00
FileInodeChangeDate	2023:03:24 09:43:32+08:00
FileModifyDate	2023:03:24 09:43:32+08:00
FileSize	30 KiB
FileType	ZIP
FileTypeExtension	zip
MIMEType	application/zip
ZipBitFlag	0x0006
ZipCRC	0xf518ccdf
ZipCompressedSize	429
ZipCompression	Deflated
ZipFileName	[Content_Types].xml
ZipModifyDate	1980:01:01 00:00:00
ZipRequiredVersion	20
ZipUncompressedSize	3142

深度解析

基本信息

	a.pptx
文件类型	pptx
文件大小	30470字节
MD5	d75e03ebaba0c426d457684c510e8bd0
SHA1	81776da5d6cdcf7cb7566c5c984dba9b37810cd8
SHA256	be2ef75b60cd65b4401204ceb23c83f0504abb52998f90b32a50098ed0877f18

奇安信威胁情报中心

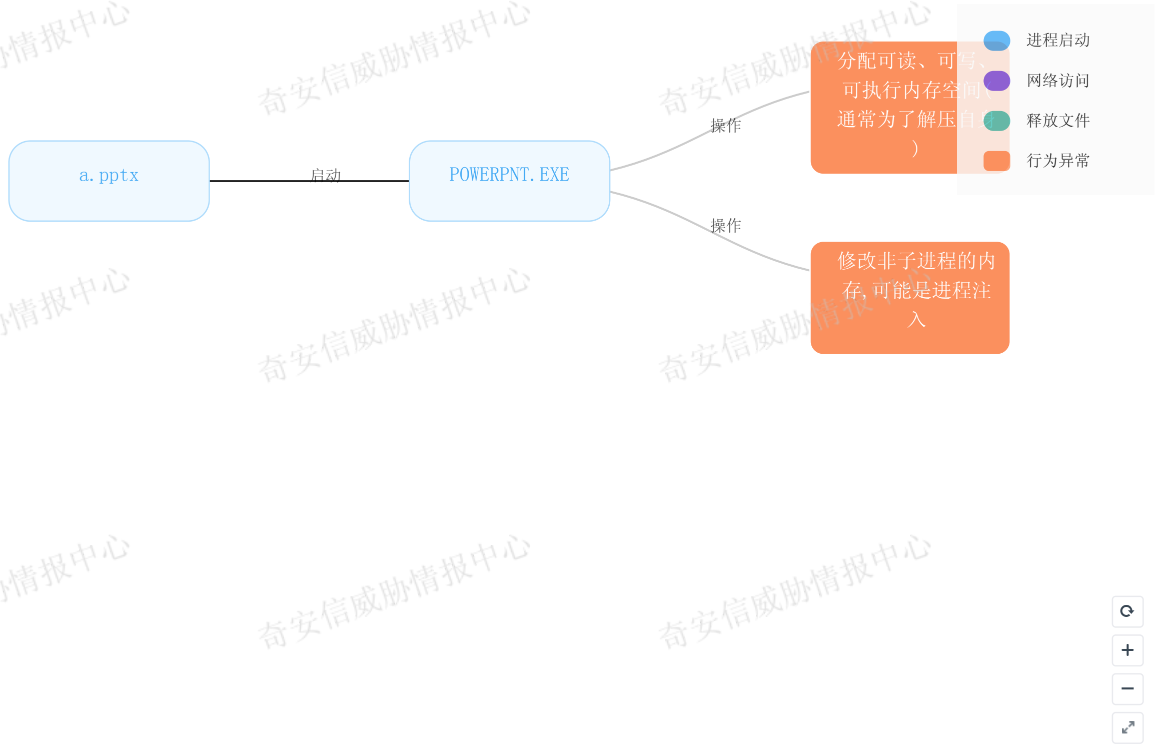
SHA512	f77b0aca089ac7eecf63b864557deaee88e0989c8b61d93200d810e34744ae4c605ab69efefdd990c2b526ddfd5c5fa0729fe772e827980f0cf559b3fc72c5e1
SSDeep	768:n9T11f3S0yS00SneS0JSnjS0MS0bS02S0dS0EJVILsoScCz70rZTnUZ2fXQHQE6N:nRmMhz7AnUMUbooCDkIr

文档摘要信息

创建者	陈学勤01
修改者	陈学勤01
创建时间	2023-03-24 09:41:30
修改时间	2023-03-24 09:41:38
文档标题	啊

主机行为

行为分析图


a.pptx
启动
POWERPNT.EXE
操作
分配可读、可写、可执行内存空间(通常为了解压自身)
操作
修改非子进程的内存,可能是进程注入
进程启动
网络访问
释放文件
行为异常

奇安信威胁情报中心

奇安信威胁情报中心

进程

⊟ POWERPNT.EXE(进程ID: 556) 命令行:"c:\program files (x86)\microsoft office\office14\powerpnt.exe" /S C:\Users\ADMINI~1\AppData\Local\Temp\a.pptx

网络行为

● 会话

DNS (DNS总数0, 当前显示0)

解析域名	IP/域名	归属地	请求类型	ASN
		暂无数据		

会话信息 (会话总数0, 当前显示0)

协议	端口	IP地址	IP归属地	ASN
		暂无数据		

HTTP (URL总数0, 当前显示0)

URL	请求方式	用户代理
暂无数据		

释放文件

释放文件

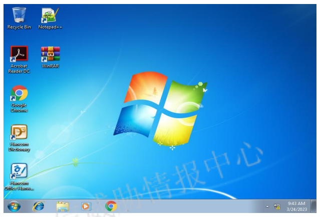
e3b0c44298fc1c14_cvr89bc.tmp.cvr

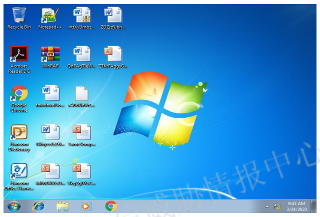
文件名称	e3b0c44298fc1c14_cvr89bc.tmp.cvr
文件路径	c:\users\administrator\appdata\local\temp\cvr89bc.tmp.cvr
进程ID	556
文件类型	empty
MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

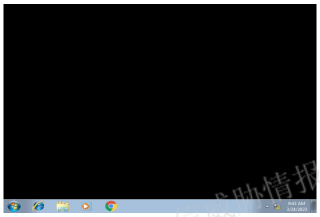
SSDeep	3::

运行截图

运行截图(共7张)







奇安信威胁情报中心