恶意程序

"3847361739.scr"分析报告

文件被批量文件上报工具发现，经由美国软件交叉索引(NSRL)鉴定器、数字证书鉴定器、动态行为(Windows7)鉴定器、静态分析鉴定器、动态行为(默认环境)鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

"安天追影高级威胁鉴定器"依据动态行为鉴定器最终将文件判定为恶意程序。

该文件具有以下行为：其他进程写入可疑数据;创建特定窗体;填充导入表（疑似壳）;访问文件尾部;获取驱动器类型;获取计算机名称;获取系统内存;查找特定窗体;独占打开文件;打开自身进程文件;获取系统版本;隐藏文件;请求加载驱动的权限;连接网络;获取socket本地名称;获取主机用户名称。

文件名:	3847361739.scr
文件类型:	BinExecute/Microsoft.EXE[:X86]
大小:	112 KB
MD5:	E1E275C70D1BE514C2F774DD9E782E0D
首次发现时间:	2015-04-30 09:51
末次发现时间:	2015-04-30 09:51
病毒类型:	恶意程序
恶意判定/病毒名称:	malware/gen
判定依据:	动态行为
下次鉴定时间:	约2周

运行环境

操作系统	内置软件
Windows 7 6.1.7600 Build 7600	默认,ie9,office 2007,flash,wps,FoxitReader,adobe reader

危险行为

行为描述:	其他进程写入可疑数据	
附加信息:	ImagePath	target.exe
危险等级:	★★★	

其他行为

行为描述:	创建特定窗体	
附加信息:	ClassName	(null)
	WindowName	OleMainThreadWndName
	ClassName	WorkerW
	WindowName	(null)
	ClassName	OpusApp
	WindowName	Microsoft Word
	ClassName	Task Pool Notification Window
	WindowName	(null)
	ClassName	_WwO
	WindowName	(null)
	ClassName	CicMarshalWndClass
	WindowName	CicMarshalWnd
	ClassName	NUIPane
	WindowName	(null)
	ClassName	NetUIHWND
	WindowName	(null)
	ClassName	NetUI_Hidden
	WindowName	(null)
	ClassName	NetUICtrlNotifySink
	WindowName	(null)
	ClassName	_WwF
	WindowName	(null)
	ClassName	MSCTFIME UI
	WindowName	MSCTFIME UI
	ClassName	(null)
	WindowName	DDE Server Window
	ClassName	{157E7179-6C00-44A9-808F-1E9B5F83A226}.message
	WindowName	(null)
	ClassName	_WwB
	WindowName	Winword_1
	ClassName	_WwB
	WindowName	(null)
	ClassName	_WwG
	WindowName	(null)
	ClassName	NUIScrollbar
	WindowName	(null)
	ClassName	_WwC
	WindowName	(null)
	ClassName	CLIPBRDWNDCLASS
	WindowName	(null)
危险等级:	★	

行为描述:	打开自身进程文件	
附加信息:	FileName	C:\target.exe
	FileName	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE.config
危险等级:	★	

行为描述:	填充导入表（疑似壳）	
附加信息:		
危险等级:	★★	

行为描述:	访问文件尾部	
附加信息:	FilePath	\??\C:\Program Files\Microsoft Office\Office12\WINWORD.EXE
	FilePath	\??\C:\Program Files\Common Files\Microsoft Shared\office12\MSO.DLL
	FilePath	\??\C:\PROGRA~1\COMMON~1\MICROS~1\VBA\VBA6\VBE6.DLL
危险等级:	★	

行为描述:	获取驱动器类型	
附加信息:	RootPathName	C:\
	RootPathName	D:\
危险等级:	★	

行为描述:	获取计算机名称	
附加信息:	Buffer	KS32-PC
危险等级:	★	

行为描述:	获取系统内存	
附加信息:		
危险等级:	★★	

行为描述:	查找特定窗体	
附加信息:	ClassName	mspim_wnd32
	WindowName	(null)
	ClassName	MSOBALLOON
	WindowName	(null)
	ClassName	MsoHelp10
	WindowName	(null)
	ClassName	AgentAnim
	WindowName	(null)
	ClassName	CicLoaderWndClass
	WindowName	(null)
危险等级:	★	

行为描述:	独占打开文件	
附加信息:	FileName	C:\Users\ks32\AppData\Roaming\Foxit Software\Foxit PDF Creator\FoxitReaderPrinterProfile_CS.xml
	FileName	C:\Users\ks32\AppData\Roaming\Microsoft\Templates\Normal.dotm
	FileName	C:\Users\ks32\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC
危险等级:	★	

文件操作

操作	文件路径
新建	c:\users\ks32\appdata\local\temp\pofuxix.cab
新建	c:\users\ks32\appdata\local\temp\target.rtf
新建	c:\users\ks32\appdata\local\temp\cvr6810.tmp.cvr
新建	c:\users\ks32\appdata\local\temp\26656.od
新建	c:\progra~2\micros~1\office\data\opa12.dat
新建	c:\users\ks32\appdata\roaming\microsoft\templates\~$normal.dotm
新建	c:\users\ks32\appdata\local\microsoft\windows\temporary internet files\content.word\~wrs{6b66e4ce-b71e-4509-8e7f-4d3f79f003bc}.tmp
新建	c:\users\ks32\appdata\local\temp\~$target.rtf
新建	c:\users\ks32\appdata\local\microsoft\windows\temporary internet files\content.word\~wrs{f136f3db-e4c5-4c14-958e-566aee8e43eb}.tmp
新建	c:\users\ks32\appdata\local\microsoft\windows\temporary internet files\content.word\~wrf{04e4ff19-b194-4edd-a9dd-507c520694e0}.tmp

进程监控

PID：1744	创建：C:\Program Files\Microsoft Office\Office12\WINWORD.EXE
	命令行："C:\Program Files\Microsoft Office\Office12\WINWORD.EXE" /n /dde

进程衍生关系

- target.exe
  - "C:\Program Files\Microsoft Office\Office12\WINWORD.EXE" /n /dde

运行环境

操作系统	内置软件
Windows xp 5.1.2600 Service Pack 3 Build 2600	默认,ie6,office 2003,flash,wps,FoxitReader,adobe reader

危险行为

行为描述:	其他进程写入可疑数据	
附加信息:	ImagePath	target.exe
危险等级:	★★★	

其他行为

行为描述:	创建特定窗体	
附加信息:	ClassName	(null)
	WindowName	OleMainThreadWndName
	ClassName	WorkerW
	WindowName	(null)
	ClassName	OpusApp
	WindowName	Microsoft Word
	ClassName	MSCTFIME UI
	WindowName	MSCTFIME UI
	ClassName	(null)
	WindowName	DDE Server Window
	ClassName	PINTLGNT
	WindowName	PINTLGNT
	ClassName	_WwB
	WindowName	Winword_1
	ClassName	_WwB
	WindowName	(null)
	ClassName	_WwG
	WindowName	(null)
	ClassName	CLIPBRDWNDCLASS
	WindowName	(null)
危险等级:	★	

行为描述:	获取驱动器类型	
附加信息:	RootPathName	C:\
	RootPathName	D:\
	RootPathName	C:\Documents and Settings\Administrator\Local Settings\Temp\
	RootPathName	C:\Documents and Settings\Administrator\Local Settings\
危险等级:	★	

行为描述:	获取系统内存	
附加信息:		
危险等级:	★★	

行为描述:	打开自身进程文件	
附加信息:	FileName	C:\target.exe
危险等级:	★	

行为描述:	获取系统版本	
附加信息:	SubKey	System\CurrentControlSet\Control\ProductOptions
危险等级:	★★	

行为描述:	隐藏文件	
附加信息:	FileName	C:\Documents and Settings\Administrator\Application Data\Microsoft\Office\Recent\index.dat
危险等级:	★★	

行为描述:	请求加载驱动的权限	
附加信息:	Name	SeLoadDriverPrivilege
危险等级:	★	

行为描述:	连接网络	
附加信息:	addr	119.81.64.59
	port	80
	addr	195.32.69.75
	port	80
	addr	46.30.212.236
	port	80
	addr	91.121.104.100
	port	80
	addr	212.47.208.158
	port	80
	addr	148.251.142.65
	port	80
	addr	195.128.174.141
	port	80
危险等级:	★	

行为描述:	获取计算机名称	
附加信息:	Buffer	AZ
危险等级:	★	

行为描述:	填充导入表（疑似壳）	
附加信息:		
危险等级:	★★	

行为描述:	获取socket本地名称	
附加信息:		
危险等级:	★	

行为描述:	查找特定窗体	
附加信息:	ClassName	MSOBALLOON
	WindowName	(null)
	ClassName	MsoHelp10
	WindowName	(null)
	ClassName	AgentAnim
	WindowName	(null)
	ClassName	Shell_TrayWnd
	WindowName	(null)
	ClassName	CicLoaderWndClass
	WindowName	(null)
危险等级:	★	

行为描述:	获取主机用户名称	
附加信息:	NameBuffer	Administrator
危险等级:	★	

文件操作

操作	文件路径
新建	c:\docume~1\admini~1\locals~1\temp\fykilypy.cab
新建	c:\docume~1\admini~1\locals~1\temp\target.rtf
新建	c:\docume~1\admini~1\locals~1\temp\~df86a1.tmp
新建	c:\documents and settings\administrator\application data\microsoft\templates\~$normal.dot
新建	c:\docume~1\alluse~1\applic~1\micros~1\office\data\opa11.dat
新建	c:\docume~1\admini~1\locals~1\temp\~$target.rtf
新建	c:\documents and settings\administrator\application data\microsoft\office\recent\target.rtf.lnk
新建	\??\c:\documents and settings\administrator\application data\microsoft\office\recent\index.dat
新建	c:\documents and settings\administrator\application data\microsoft\office\recent\temp.lnk

网络监控

IP

IP地址	端口
119.81.64.59	80
195.32.69.75	80
46.30.212.236	80
91.121.104.100	80
212.47.208.158	80
148.251.142.65	80
195.128.174.141	80

DNS域名解析

域名	IP	归属地
lasertek.com.sg	119.81.64.59	新加坡
malagadetectives.es	217.76.132.193	西班牙
puntocan.com	148.251.142.65	德国
shaneproject.org.uk	46.30.212.236	丹麦
empuriadata.es	91.121.104.100	法国
vesterlin.eu	212.47.208.158	德国
lars-laursen.dk	195.128.174.141	丹麦

UDP通讯信息

源	目的
192.168.122.1:53	192.168.122.221:1053

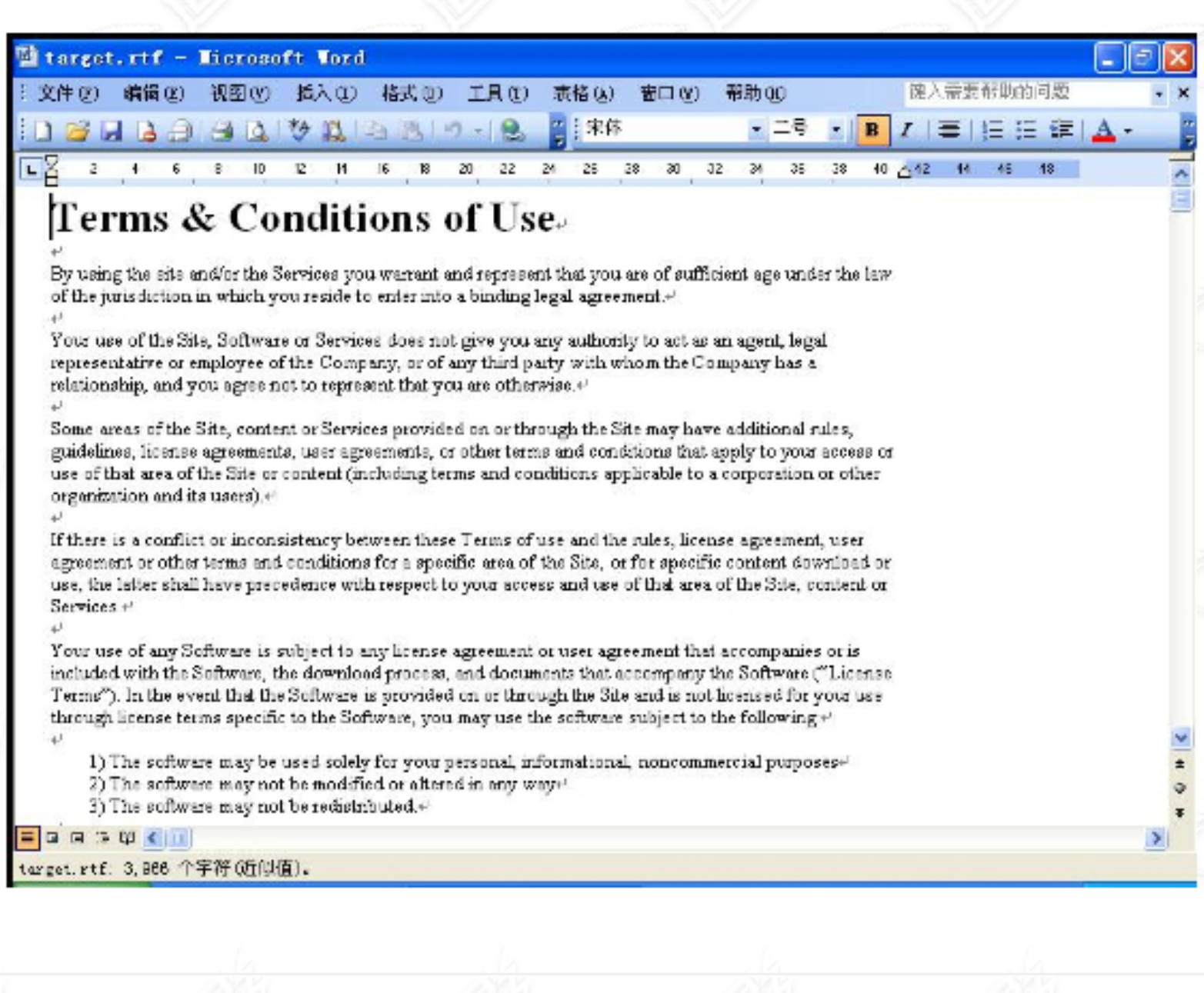
进程监控

PID：1224	创建：C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE
	命令行："C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde

进程衍生关系

- target.exe
  - "C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE" /n /dde

动态截屏



Terms & Conditions of Use

By using the site and/or the Services you warrant and represent that you are of sufficient age under the law of the jurisdiction in which you reside to enter into a binding legal agreement.

Your use of the Site, Software or Services does not give you any authority to act as an agent, legal representative or employee of the Company, or of any third party with whom the Company has a relationship, and you agree not to represent that you are otherwise.

Some areas of the Site, content or Services provided on or through the Site may have additional rules, guidelines, license agreements, user agreements, or other terms and conditions that apply to your access or use of that area of the Site or content (including terms and conditions applicable to a corporation or other organization and its users).

If there is a conflict or inconsistency between these Terms of use and the rules, license agreement, user agreement or other terms and conditions for a specific area of the Site, or for specific content download or use, the latter shall have precedence with respect to your access and use of that area of the Site, content or Services.

Your use of any Software is subject to any license agreement or user agreement that accompanies or is included with the Software, the download process, and documents that accompany the Software ("License Terms"). In the event that the Software is provided on or through the Site and is not licensed for your use through license terms specific to the Software, you may use the software subject to the following:

1) The software may be used solely for your personal, informational, noncommercial purposes.
2) The software may not be modified or altered in any way.
3) The software may not be redistributed.

target.rtf 3,866 个字符(近似值)。

静态启发式检测

检测类型	检测点	详细说明
编译指令	未知壳	未被公开的壳，经常被恶意代码使用，用来保护恶意程序被查杀。
PE结构	无版本信息并且不是GCC编译器	除GCC编译器外，常规编译器均默认包含版本信息。如果不是GCC编译器，并且不包含版本信息，显然是作者故意抹掉版本信息，逃避追查。

EXIF信息

描述	值
File Size	112 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2005:11:13 10:40:58+08:00
PE Type	PE32
Linker Version	6.0
Code Size	65536
Initialized Data Size	45056
Uninitialized Data Size	0
Entry Point	0x1ac1
OS Version	4.0
Image Version	0.0
Subsystem Version	4.0
Subsystem	Windows GUI