样本分析报告

文件名称： OneTool开心版.zip

SHA256： c37260a574ab617021733d2f8ab54eaafad7ed17d5be298243eb844de74dd842

文件大小： 36.64 MB

文件类型： Zip archive data, at least v2.0 to extract

分析环境： Win7(32bit,Office2013) Linux(Ubuntu 17.04 64bit)

微步判定： 恶意

云沙箱

目录

OneTool开心版.zip

恶意

首次提交: 2025/02/16　末次提交: 2025/03/26　末次分析: 2025/03/26 14:06:43

文件大小： 36.64 MB　文件类型： Zip archive data, at least v2.0 to extract

引擎检出： 8 / 28　分析环境： Win7(32bit,Office2013)　Linux(Ubuntu 17.04 64bit)

威胁分类： 木马　木马家族： WebShell

HASH

SHA256: c37260a574ab617021733d2f8ab54eaafad7ed17d5be298243eb844de74dd842

MD5: 40081f51c92e9425a5e145722e5b008f

SHA1: 5468670f6edd324de83e4813fff35bb7409df2c8

情报IOC

情报IOC	IOC类型	微步判定	情报内容	发现IOC环境
c37260a574ab617021733d2f8ab54eaafad7ed17d5be298243eb844de74dd842	Hash	恶意	WebShell 木马	2 个分析环境

行为检测

MITRE ATT&CK™ 矩阵（技术）检测到 3 条技术指标。 查看完整结果

全部分析环境签名

可疑行为 (3)

系统环境探测	扫描Windows任务栏，（常用于注入explorer）	Win7(32bit,Office2013)
信息搜集	安装消息钩子	Win7(32bit,Office2013)
系统敏感操作	使用getrlimit系统调用获取系统资源的限制数量	Linux(Ubuntu 17.04 64bit)

通用行为 (3)

系统环境探测	查询计算机名	Win7(32bit,Office2013)
一般行为	访问/etc/ld.so.preload文件	Linux(Ubuntu 17.04 64bit)
系统敏感操作	调用COM相关API	Win7(32bit,Office2013)

多维检测

Yara 规则

全部分析环境签名

初始样本：1

规则	描述	SHA256	匹配项	源	分析环境
shellcode	Matched shellcode byte patterns	c37260a574ab617021733d2f8ab54eaafad7ed17d…	查看	General	2 个分析环境

多引擎检测

检出率：8 / 28

最近检测时间：2025-03-26 14:06:43

引擎	检出	引擎	检出
ESET	PHP/Webshell.NQI trojan	卡巴斯基（Kaspersky）	HEUR:Backdoor.PHP.WebShell.gen
IKARUS	Trojan.PHP.WebShell	大蜘蛛（Dr.Web）	PHP.WebShell.107
Avast	Script:SNH-gen	AVG	Script:SNH-gen
GDATA	Generic.ASP.WebShell.AO.00D3A4A0	OneStatic	WebShell/WebShell.PZK
微软（MSE）	无检出	小红伞（Avira）	无检出
K7	无检出	安天（Antiy）	无检出
江民（JiangMin）	无检出	360（Qihoo 360）	无检出
Baidu	无检出	NANO	无检出
Trustlook	无检出	瑞星（Rising）	无检出
熊猫（Panda）	无检出	Sophos	无检出
ClamAV	无检出	WebShell专杀	无检出
Baidu-China	无检出	MicroAPT	无检出

引擎	检出	引擎	检出
OneAV	无检出	MicroNonPE	无检出
OneAV-PWSH	无检出	ShellPub	无检出

收起全部

静态分析

基础信息

文件名称	c37260a574ab617021733d2f8ab54eaafad7ed17d5be298243eb844de74dd842
文件格式	Zip
文件类型(Magic)	Zip archive data, at least v2.0 to extract
文件大小	36.64MB
SHA256	c37260a574ab617021733d2f8ab54eaafad7ed17d5be298243eb844de74dd842
SHA1	5468670f6edd324de83e4813fff35bb7409df2c8
MD5	40081f51c92e9425a5e145722e5b008f
CRC32	D572AB31
SSDEEP	786432:fxsA/S6ViKWO7AZV7PlBlN7mI0Qx/UCjSkxd0WOobM5:fR/FPal19UBkT0abM5
TLSH	T1ED87F154B2F5B0C0CC92B2B96C6BB1433B35F5D7196396130E7869B40AAEA730B35F19
Tags	zip,contains_pe,contains_zip

元数据

ExifTool

FileType	ZIP
FileTypeExtension	zip
MIMEType	application/zip
ZipRequiredVersion	20
ZipBitFlag	0
ZipCompression	None
ZipModifyDate	2024:10:17 19:17:58
ZipCRC	0x00000000
ZipCompressedSize	0
ZipUncompressedSize	0
ZipFileName	OneTool/

TrID

34.4% (.SH3D)	Sweet Home 3D design (generic) (10500/1/3)
26.2% (.XPI)	Mozilla Firefox browser extension (8000/1/1)
22.9% (.MAFF)	Mozilla Archive Format (gen) (7000/1/1)
13.1% (.ZIP)	ZIP compressed archive (4000/1)
3.2% (.PG/BIN)	PrintFox/Pagefox bitmap (640x800) (1000/1)

格式深度分析

压缩通用

子文件摘要

子文件数量	14938
最早修改时间	2019-08-05 08:17:42.0000000
最晚修改时间	2024-10-17 19:31:00.2901215

子文件扩展名(39)

扩展名	数量	扩展名	数量
svg	1626	php	849
js	129	html	93
css	66	png	50
json	42	md	41
woff2	38	jpg	23

子文件类型(8)

扩展名	数量	扩展名	数量
unknown	13909	PHP	845
IE	83	IMAGE	79
EOT	19	BAT	1
EXEx86	1	Zip	1

子文件详情(100+)

文件	Magic	文件大小	修改时间	
OneTool\app\.htaccess	ASCII text, with no line terminators	13	2022-07-28 20:32:48.0000000	展开
OneTool\app\AppService.php	PHP script, UTF-8 Unicode text	266	2022-07-28 20:32:48.0000000	展开

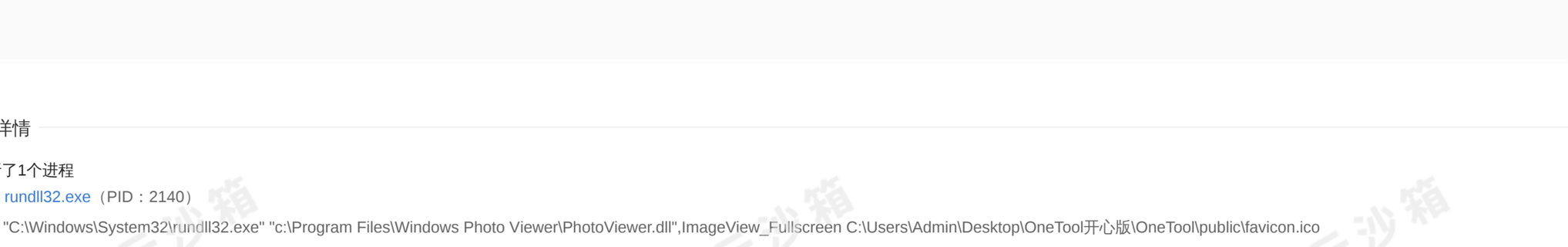
OneTool\app\BaseController.php	PHP script, UTF-8 Unicode text	2082	2022-07-28 20:32:42.00 00000	展开
OneTool\app\ExceptionHandle.php	PHP script, UTF-8 Unicode text	1398	2022-07-28 20:32:50.00 00000	展开
OneTool\app\Request.php	PHP script, UTF-8 Unicode text	88	2022-09-03 21:16:56.00 00000	展开

查看全部

沙箱动态检测

Win7(32bit,Office2013)

执行流程



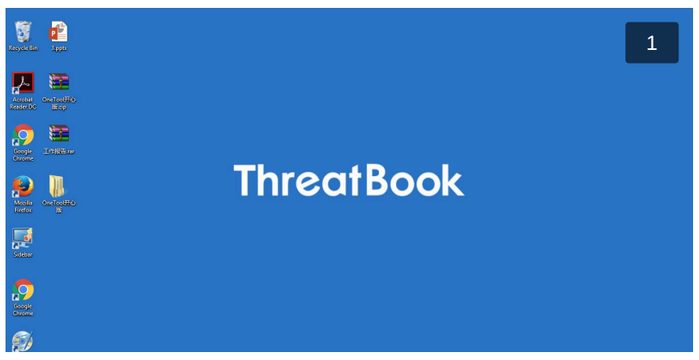
进程详情

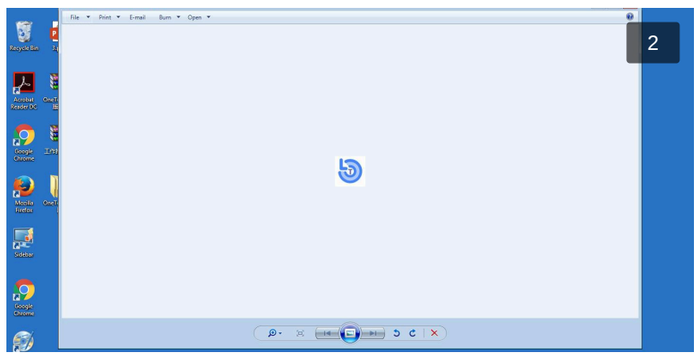
共分析了1个进程

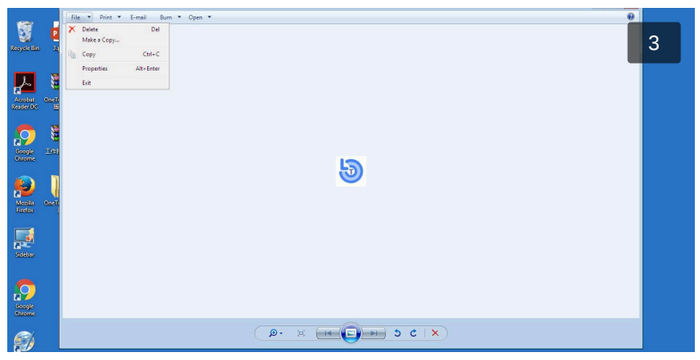
rundll32.exe（PID：2140）

"C:\Windows\System32\rundll32.exe" "c:\Program Files\Windows Photo Viewer\PhotoViewer.dll",ImageView_Fullscreen C:\Users\Admin\Desktop\OneTool开心版\OneTool\public\favicon.ico

运行截图（3）







网络行为

指纹	域名	DNS	HTTP	HTTPS	TCP	UDP	SMTP	ICMP	IRC	Hosts	Dead-Hosts
0	0	0	0	0	0	0	0	0	0	0	0

释放文件

无释放文件

Linux(Ubuntu 17.04 64bit)

执行流程

进程详情

共分析了1个进程

└ php（PID：7862）

php /3TkHJo8/OneTool开心版_Decomp/OneTool/think

运行截图

无运行截图

网络行为

指纹	域名	DNS	HTTP	HTTPS	TCP	UDP	SMTP	ICMP	IRC	Hosts	Dead-Hosts
0	0	0	0	0	0	0	0	0	0	0	0

释放文件

无释放文件