

Learning Malware Analysis

Author XT. Wrote for log learning note.

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

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

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:

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
```

以上安装完毕, labubuntu 切换仅主机模式

LinuxVM config:

1.配置ubuntu静态网络static IP: 192.168.1.100

sudo gedit /etc/network/interfaces

```
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
address 192.168.1.100
netmask 255.255.255.0
```

service networking restart 或者重启ubuntu ifconfig确认

2. 配置ubuntu中的inetsim配置 修改inetsim默认配置: sudo gedit /etc/inetsim/inetsim.conf

在默认配置service_bind区域追加, 并注释掉默认配置:
service_bind_address 192.168.1.100

配置DNS服务, 已用于DNS服务:

在配置dns区域追加以下内容并注释掉原默认配置：
dns_default_ip 192.168.1.100

运行测试： `sudo inetsim` 检查配置

3. 配置第三方软件： python 2.7 (仅限本书)


check point 确认windows主机网段： 192.168.1.105 DNS： 192.168.1.100 测试win和linux之间联通节点

 1555672944518

 1555672906183

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)

 1555673578514 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/utils/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 - 2019-05-21 00', u'In puls
e: Malware dataset 20190307 | Network', u'In pulse: Malware dataset 20190223 | Network']

```

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，还可以在您在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. 在加载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>.

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，转人工分析：

样本邮件

主题:Delivery reports about your e-mail 发件人:"Returned mail" [MAILER-DAEMON@\[.....\]\(脱敏\)](mailto: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)	写入自启动注册表,增加自启动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,以达到将恶意程序隐藏的目的
	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络连接进行数据窃取操作

基本信息

文件名称: 1165539.scr
文件大小: 39KB (40088bytes)
文件类型: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
开始时间: 2019-08-19 05:51:47
MD5: 314c832e02c2501e9d9d8fef1fec3faa[virustotal]
SHA1: c91d5984f8de492fda9b3415ecbab56348542412
壳或编译器信息: UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser

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
<div><div></div></div>	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
<div><div></div></div>	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
<div><div></div><div></div></div>	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
<div><div></div><div></div></div>	1165539.scr[pid=3324]	写入自启动注册表,增加自启动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
<div><div></div></div>	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
<div><div></div><div></div></div>	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
<div><div></div></div>	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
<div><div></div></div>	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
<div><div></div></div>	1165539.scr[pid=3324]	遍历文件	通过文件遍历查找指定目标文件
<div><div></div><div></div><div></div></div>	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。
<div><div></div><div></div></div>	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,以达到混淆视听欺骗用户的目的
<div><div></div><div></div></div>	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络连接进行数据窃取操作

文件行为(Windows XP)

检测有恶意的

lsass.exe Kazaa Lite.exe Winamp 5.0 (en).com

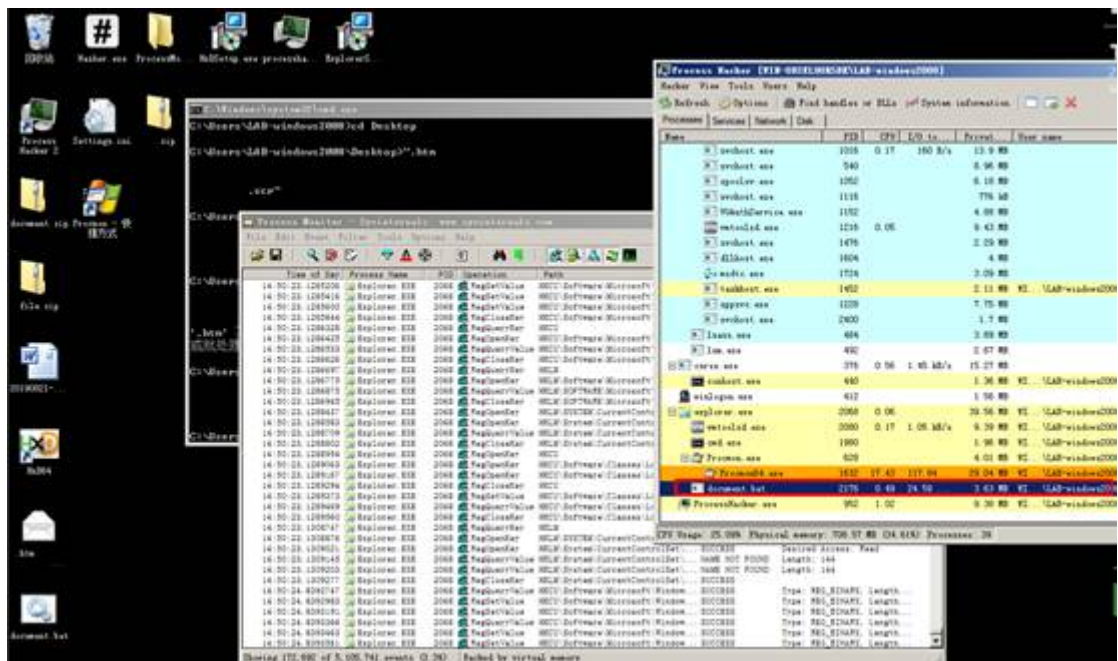
检测安全的

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。

Bounced mail 2019-08-21 17:46 1
发至 none

详情

.....
.....e..
Q.3/.T.|.l.....NU...z..
C.U....K.f8.OV..?..~.D..!...DRV.v..#h..MDJ\$?....
_R.<K..]..'....nj].>.U.F
..WO..K..U.....'1..j...3..4}.vW
.l.l...1...8....
oe,..#.#e..B..`P..b].j...k...`PH)hO*./Ezzu.....^.....).o.....s.gD\,D.,&o1...j2.Q.jc...),.....P..l.,{.}g..9~.
Lx.l...t...7{w.D}.3*...../.....Rk
?.\$.Z.V.V...*..%.
..3...1.S...6X.l.Ex/...>....
..4.C.
~.....\$
akU...tZ..*6[./..H.V....T0C....l8..h...r}f_s...R...f..T&.....#.lk...DJ(. T....1B.dL.q...C...9~.mF[..
<1R....U.C...>1'.gB..d.3...c...?..g.....Ee6Q..y.q..I...G<
V....p]....IV..E..j..A..~.g...>[...~5dVN....B....M..`4..WV..B..k....&c.L#.LV.8A.JQ.b...
.Z....t....B....\..^..>.....4...>.{.3...sd
Q..EM^..}t..1..}..?R.....
..K..cSe..7.7W...v.h9nS..Uh9f...j..O/..[.o...].R...m1w...I.....#
..F6v>F..F45F...n...d..l&GJA...
y6..j.D..G.a
.Ol...n..h7....{>xh...<O}.E
3Y.....HdUNG.D?~&T
*...j...j...U...;y3...W.x.....[.H>.l.Z..rgrO..l..&8.Pkk...WWr.....<Zy.....d_o.
.../.JoS^..0...3r...0..Az
'...-.lFw.tQ..(#....3...K.f>....WI..%v...R....&a..^W.NZ.[7l.Vz.Q.j....0.&o...N.s..Mi.tg..JEQ\$...
D:~FN.E.H.....Oo.K....~.7pK.R.....NE[T...12.J.Y|X.<.....J].9.H..V.M...\$.`P.es...Ex..6...bHf>{...^..^D.Qa....T}
<gH.V....)Iamu.r.Y..a....C.FMIg....\$D.
.....~"3....
...Z..L....XlC'..g1..'.^..tj{.F/..Y.....(J..ow....Z..C./?...)\....)b..A].....v..%..}..Y..&`St{)
.2.....c.b...[....p.
...\$.~.(~.M6..N..#bQ..

附件(1) 保存

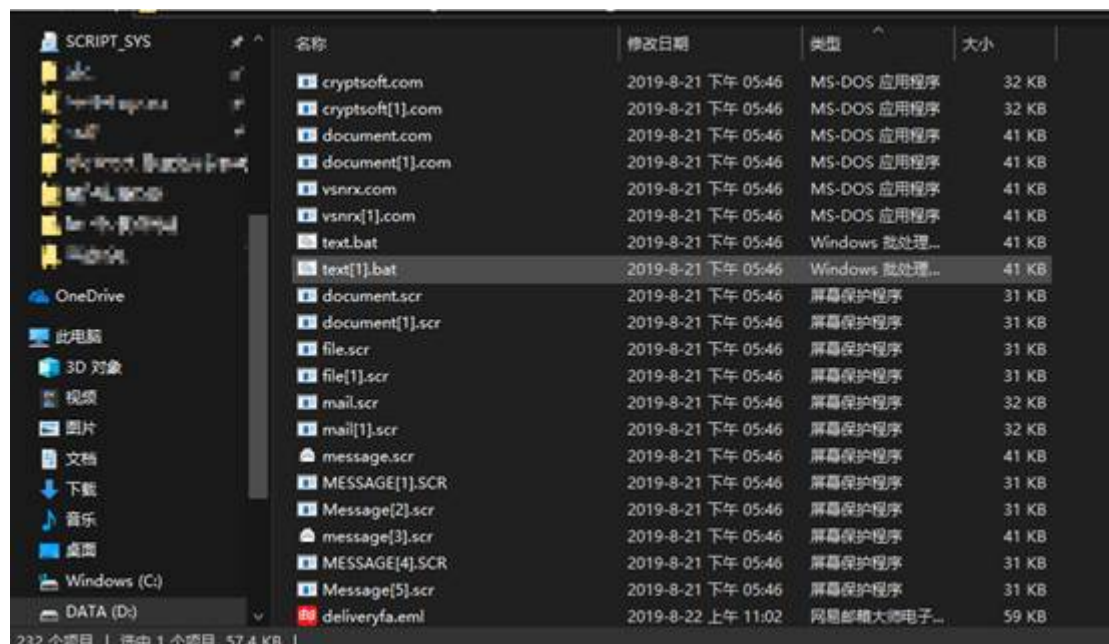


可以看到样本执行后对外发送大量邮件传递信息，或恶意邮件传播。

From	Source host	Destination host	From	To	Subject	From	To	Subject	
104	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	104	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
408	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Delivery failed	408	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Delivery failed
584	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: See message for details	584	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
585	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	585	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
676	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'MAILER-DAEMON' (postmaster@exchange.org)	postmaster@exchange.org	Delivery failed	676	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Delivery failed
936	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Returned mail' (postmaster@exchange.org)	postmaster@exchange.org	Delivery failed	936	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Delivery failed
1040	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Delivery reports about your email	1040	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Delivery reports about your email
1243	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Message could not be delivered	1243	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Message could not be delivered
1276	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: See message for details	1276	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
1380	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	1380	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
1513	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'MAILER-DAEMON' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	1513	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
1730	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	1730	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
1741	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	1741	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
1881	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (MAILER-DAEMON)	postmaster@exchange.org	Returned mail: Data format error	1881	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
1975	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	1975	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2084	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: See message for details	2084	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
2108	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	2108	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2311	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (MAILER-DAEMON)	postmaster@exchange.org	Returned mail: Data format error	2311	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2442	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	2442	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2512	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Mail Administrator' (MAILER-DAEMON)	postmaster@exchange.org	Returned mail: Data format error	2512	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2638	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: Data format error	2638	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2839	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: Data format error	2839	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
2880	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Mail Delivery Subsystem' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	2880	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3000	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	3000	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3112	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	3112	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3315	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	3315	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3318	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'MAILER-DAEMON' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	3318	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3404	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Mail Administrator' (postmaster@exchange.org)	postmaster@exchange.org	Returned mail: Data format error	3404	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3508	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	3508	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3608	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	3608	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3784	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	3784	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
3888	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	3888	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4032	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	4032	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4107	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	4107	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4220	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: See message for details	4220	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
4475	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	4475	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4495	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	4495	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4720	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	4720	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4851	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	4851	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
4942	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	4942	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5274	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5274	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5323	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5323	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5338	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5338	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5425	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5425	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5447	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5447	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5580	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	5580	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
5744	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: See message for details	5744	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
5879	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'The Post Office' (MAILER-DAEMON)	postoffice@exchange.org	Returned mail: See message for details	5879	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: See message for details
5881	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	5881	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
6108	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	6108	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
6208	192.168.1.106 (Windows)	192.168.1.100 (Linux)	'Automatic Mail Delivery Software' (postmaster)	postmaster@exchange.org	Returned mail: Data format error	6208	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
6340	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	6340	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error
6484	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Internet-Exchange.org	mail@exchange.org	Returned mail: Data format error	6484	192.168.1.106 (Windows)	192.168.1.100 (Linux)	Returned mail: Data format error



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：

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>

邮件内容:

Dear Sir/ Madam

Please find enclosed our PO No.021 for the attached products specifications

Kindly acknowledge the receipt and execute the order.

Chvan

Purchase / R & D Nordyne

Normand Group

117, Boulevard Eugène THOMAS

ZI apple tree

<http://www.groupe-normand.com>

F - 62110 HENIN BEAUMONT

GPS: 50.39837N / 2.969699E

Tel: 00 33 (0) 3 91 83 00 93

Fax: 00 33 (0) 3 91 83 00 99

Ce message et ses pieces jointes peuvent contenir des informations confidentielles ou privilegiees et ne doivent donc pas etre diffuses, exploites ou copies sans autorisation. Si vous avez recu ce message par erreur, veuillez le signaler a l'expediteur et le detruire ainsi que les pieces jointes. Les messages electroniques etant susceptibles d'alteration, Orange decline toute responsabilite si ce message a ete altere, deforme ou falsifie. Merci.

This message and its attachments may contain confidential or privileged information that may be protected by law; they should not be distributed, used or copied without authorisation. If you have received this email in error, please notify the sender and delete this message and its attachments. As emails may be altered, Orange is not liable for messages that have been modified, changed or falsified.

Thank you.

邮件内容:

Dear Sir/ Madam

Please find enclosed our PO No.021 for the attached products specifications
Kindly acknowledge the receipt and execute the order.

xtpeeps.cn

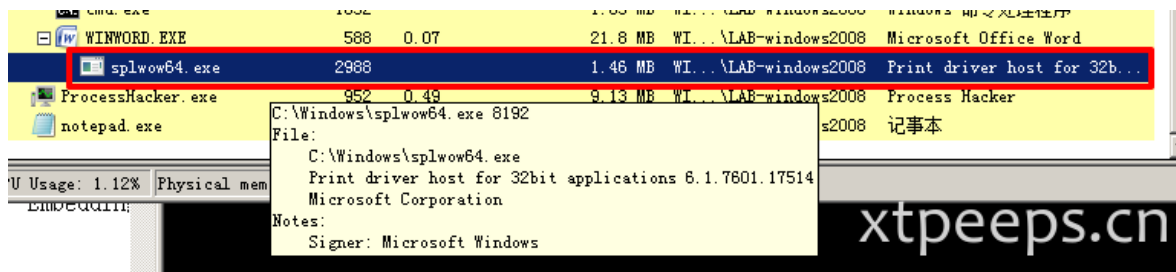
quotation_PO_No.021.doc

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:c3KIZARvYj1HJcuL2hoykm7QvdfOguQy0DKteo:WKIOvYtBHmElOguQRKV 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



回链请求如下所示:

70.10.100.100	192.168.211.131	47.88.102.244	DNS	72 Standard query response 0x08f6 A evaglobal.eu A 47.88.102.244
97.16.605296	192.168.211.2	192.168.211.131	DNS	88 Standard query response 0x08f6 A evaglobal.eu A 47.88.102.244
98.16.607063	192.168.211.131	47.88.102.244	TCP	66 49165 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
99.16.789611	47.88.102.244	192.168.211.131	TCP	58 80 → 49165 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
100.16.789820	192.168.211.131	47.88.102.244	TCP	54 49165 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
101.16.789987	192.168.211.131	47.88.102.244	HTTP	360 GET /donstanz/donstanz.exe HTTP/1.1
102.16.790070	47.88.102.244	192.168.211.131	TCP	54 80 → 49165 [ACK] Seq=1 Ack=307 Win=64240 Len=0
103.17.272611	47.88.102.244	192.168.211.131	HTTP	1100 HTTP/1.1 404 Not Found (text/html)
104.17.272900	192.168.211.131	47.88.102.244	TCP	54 49165 → 80 [ACK] Seq=307 Ack=1048 Win=63194 Len=0
105.17.272974	192.168.211.131	47.88.102.244	TCP	54 49165 → 80 [ACK] Seq=307 Ack=1048 Win=63194 Len=0
106.17.413178	192.168.211.131	192.168.211.2	DNS	78 Standard query 0xf2aa A isatap.localdomain
107.17.413835	192.168.211.1	224.0.0.251	MDNS	72 Standard query 0x0000 A isatap.local, "QM" question
108.17.413992	fe80::95f:1a15:1979::ff02:fb	224.0.0.251	MDNS	92 Standard query 0x0000 A isatap.local, "QM" question
109.17.414639	192.168.211.1	224.0.0.251	MDNS	72 Standard query 0x0000 A isatap.local, "QM" question
110.17.414747	fe80::95f:1a15:1979::ff02:fb	224.0.0.251	MDNS	92 Standard query 0x0000 A isatap.local, "QM" question
111.17.415271	fe80::95f:1a15:1979::ff02:1:3	224.0.0.252	LLMNR	86 Standard query 0x5406 A isatap
112.17.415359	192.168.211.1	224.0.0.252	LLMNR	66 Standard query 0x5406 A isatap
113.17.826102	fe80::95f:1a15:1979::ff02:1:3	224.0.0.252	LLMNR	86 Standard query 0x5406 A isatap
114.17.826161	192.168.211.1	224.0.0.252	LLMNR	66 Standard query 0x5406 A isatap
115.18.413924	192.168.211.1	224.0.0.251	MDNS	72 Standard query 0x0000 A isatap.local, "QM" question
116.18.414061	fe80::95f:1a15:1979::ff02:fb	224.0.0.251	MDNS	92 Standard query 0x0000 A isatap.local, "QM" question

> Frame 101: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0
> Ethernet II, Src: Vmware_00:0d:8d (00:0c:29:00:0d:8d), Dst: Vmware_eb:5a:4c (00:50:56:eb:5a:4c)
> Internet Protocol Version 4, Src: 192.168.211.131, Dst: 47.88.102.244
> Transmission Control Protocol, Src Port: 49165, Dst Port: 80, Seq: 1, Ack: 1, Len: 306
> Hypertext Transfer Protocol
 > GET /donstanz/donstanz.exe HTTP/1.1\r\n
 Accept: */*\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3)\r\n
 Host: evaglobal.eu\r\n
 Connection: Keep-Alive\r\n
 \r\n
 [Full request URI: http://evaglobal.eu/donstanz/donstanz.exe]
 [HTTP request 1/1]
 [Response in frame: 103]

回链请求地址为: <http://evaglobal.eu/donstanz/donstanz.exe>

13 / 72

13 engines detected this URL.

<http://evaglobal.eu/donstanz/donstanz.exe>

200 Status

application/x-msdownload Content Type

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

Community Score

DETECTION	DETAILS	COMMUNITY
AegisLab WebGuard	Malicious	BitDefender Malware
CyRadar	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

样本地址:

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