伸向中亚地区的触手——DustSquad APT组织针对乌兹别克斯坦的活动分析

By 追影小组

Archived: 2026-04-05 18:03:11 UTC

一.介绍

近日,Gcow安全团队的追影APT分析小组在公共的文件分析平台上捕获到了名为DustSpuad的APT组织,针对乌兹别克斯坦的外交部进行的一起网络攻击活动.所使用的正是名叫Octopus的Windows恶意程序

Octopus恶意程序的名称最初由ESET在2017年由APT组织在其旧C2服务器上使用的0ct0pus3.php脚本之后创造。卡巴斯基通过其监控平台发现Octopus恶意程序与DustSquad有关.在遥测中,我们发现这个组织对中亚共和国以及俄语系的国家产生着浓厚的兴趣

此外,该组织专注于中亚用户以及外交实体,并且通过文件中的特殊字符,以及其手法,推断该组织可能来源于俄罗斯

二.样本分析

(一).释放者:

样本MD5	98b1c326572110a4c88c6741575910c2
样本SHA-1	081fa600a82793cf78e61e0b5dabb46f6ec1e565
样本SHA-256	139b40267aa028c8f4f509abdd88932167754ec863d26cb8e8352ab1d61ffa9f
样本名称	исправленный вариан_18.11.2019г.rar (固定版_2019.11.18)

(二).压缩包所包含的文件:

(Octopus 加载器)

样本MD5	62fb5aa21f62e92586829520078c2561
样本SHA-1	bbf8eaee7ce7c04562e618c0e45f11b060f99662
样本SHA-256	f5941f3d8dc8d60581d4915d06d56acba74f3ffad543680a85037a8d3bf3f8bc
样本名称	исправленный вариан_18.11.2019г.exe (固定版_2019.11.18)

伪装成word文件,拥有word的图标.对于一些安全意识差的人员。这种伪造手段的成功几率较高

通过ExeInfoPE工具查看样本信息,发现该程序由Delphi编写

根据我们的分析,该样本的主要恶意部分在start()函数内

现在我们将利用ollydbg的动态调试以针对该样本进行分析

1).通过GetTickCount()和QueryPerformanceCounter()函数获取当前系统运行时间

2).信息收集部分

1.收集本地IP地址:

通过初始化WSAStartup通过调用gethhostname()获取本地主机名称,再通过gethostbyname()传入获取的本地主机名称以获取本地IP地址

并且将收集好的地址以Local IP Addr:{本地IP地址}的形式进行拼接

2.本地计算机名称

通过GetComputerNameW()函数获取本地计算机的名称

并且将收集好的地址以Computer Name:{本地计算机名称}的形式进行拼接

3.收集当前用户名称

利用GetUserNameW()函数收集当前用户名称

并且将收集好的地址以User Name:{当前用户名称}的形式进行拼接

4.收集Windows文件夹目录

利用GetWindowsDirectoryW()函数获取当前系统的windows文件夹目录

并且将收集好的地址以Windows Dir:{Windows文件夹目录}的形式进行拼接

5.收集恶意样本所在的当前目录

调用GetMouduleFileNameW()函数获取恶意软件当前目录的完整路径

并且将收集好的地址以Current Dir:{文件所在目录}的形式进行拼接

6.获取盘符信息

利用GetDriveTypeW()函数获取各个盘符的属性以及名称

并且将收集好的地址以Volume list:{盘符名称加盘符大小}的形式进行拼接

最后将信息以

Start

Local IP Addr:{本地IP地址}

Computer Name:{本地计算机名称}

User Name:{当前用户名称}

Windows Dir:{Windows文件夹目录}

Current Dir:{文件所在目录}

Volume list:{盘符名称加盘符大小}

3).C2中转:

向http[:]//poisonfight[.]com/idea.php发送Post请求

check=c558838690881fa7f75807cfa94b3713

接受json格式的回显{"status":"ok"}

判断是否返回为ok

接收到ok后,对远程C2服务器发起第二段post请求

http[:]//poisonfight[.]com/idea.php发送Post请求

servers=c558838690881fa7f75807cfa94b3713

返回的json结果为:

{"servers":[{"ip_addr":"cookiesqueen.com\/innovative"}]}

将回显的json进行截取拼接得到C2:http[:]//cookiesqueen[.]com/innovative.php

向C2端发送编码后的系统信息

S=sess_{随机字母组合} check={令牌编码}

(OD:)

(Anyrun)

加密规则是先进行了一次base64加密,再通过URL编码过滤掉敏感字符,解密如下:

为了方便大家理解这一过程,笔者浅显的画了一个草图

4).文件下载

向http[:]//cookiesqueen[.]com/innovative.php

发送post请求

l=ZG93bmxvYWQ%3D以及

s=sess_{随机字母组合} check={令牌编码}

(OD:)

(Anyrun:)

在上文中我们得知了该组织的报文解密方法,对此进行解密

下载文件于%Temp%\{随机字母组合}

5).载荷解压

通过expand –d 命令获取当前cab压缩包中的内容

发现其中包含着java7.exe

利用extrac32.exe提取压缩包里的java7.exe于自启动文件夹下

此外,其会针对系统进行判断,若不属于其侦测范围的则不执行释放诱饵文档于桌面的行为

但我们在anyrun沙箱中看到了这个操作

释放的doc文档名为:èñïðàâëåíûé âàðèàíò_18.11.2019ã.doc

并且执行

诱饵界面为

部分译文为:

由此可见该活动针对的是乌兹别克斯坦的外交部门

并且恶意样本会记录该信息,base64编码后以Post形式反馈给C2

(OD:)

(Anyrun:)

收集之前的解压cab文件记录,以及解压后的文件路径以及遍历启动文件夹内的存在,确保后门的持久化运行

6).载荷清理

释放s.bat于%Temp%\下

写入s.bat

如下图所示

主要内容是判断你所运行的exe是否存在,若存在则删除,若不存在则删除自身

为了方便大家看着方便,笔者画了一幅流程图便于大家方便理解

（三）.网络模块

(Octopus 被控端)

样本MD5	bbb701630f30c5c85cebbc953b98ff38
样本SHA-1	aab83db6b4682694fa972bb2aad982557d8e1afc
样本SHA-256	105402dd65ec1c53b6db68a0e21fcee5b72e161bc3b53e644695a4c9fae32909
样本名称	Java7.exe

经过exeinfo PE查壳后发现其依旧使用delphi编写

(一).获取%AppData%路径,并且释放.setting.ini,写入配置

(二）.像中转c2发出中转请求

和加载器的手段一样,不再赘述

发送check请求,判断存活

发送Servers请求获得中转C2的json格式

拼凑字符串得到C2

(三).收集信息

1).收集当前计算机名称

执行命令

C:\windows\system32\wbem\WMIC.exe computersystem get name /format:list

2).收集系统安装时间

执行

C:\windows\system32\wbem\WMIC.exe os get installdate /format:list

3).获取本地盘符

执行

C:\windows\system32\wbem\WMIC.exe path CIM_LogicalDiskBasedOnPartition get Antecedent,Dependent

4).收集序列号

执行

C:\windows\system32\wbem\WMIC.exe path win32_physicalmedia where tag="\\\\.\\PHYSICALDRIVE0" get serialnumber /format:list

此外,被控端拥有与记载器类同的收集信息部分,这里就不再赘述

(四)发送报文并接受回显

将收集到的信息以如下方式组成json格式

Base64编码后以Post方式向http[:]//cookiesqueen[.]com/innovative.php

?query=c558838690881fa7f75807cfa94b3713发送报文

报文解密后

接受返回指令为{“rt”:”30”}

三.组织关联

根据卡巴斯基于2018.10.15发布的关于DustSquad组织使用Octopus恶意软件攻击中亚地区的报告来看

(链接放在附录部分)

该活动与本活动有以下的几点共性

1).释放于自启动文件夹的被控端都拥有相同的Java图标

2).拥有部分重合的代码逻辑

3).相似的C2报文格式

4).类似的C2中转方式

5).相同的信息收集指令

根据以上信息我们基本上可以判断这次的攻击属于DustSquad组织利用Octopus恶意软件攻击乌兹比克斯坦的外交实体

四.总结

该组织能够熟练的进行投递rar文件的信息对目标进行攻击,并且使用Delphi的恶意软件,以及通过入侵一些正常网站,上传C2中转的PHP文件做到中转C2的操作,这样既可以避免了杀毒软件的静态查杀,又可以随时撤走载荷。

五.IOCs

样本Hash	文件名称
98b1c326572110a4c88c6741575910c2	исправленный вариан_18.11.2019г.rar
62fb5aa21f62e92586829520078c2561	исправленный вариан_18.11.2019г.exe
bbb701630f30c5c85cebbc953b98ff38	Java7.exe

C2:

http[:]//cookiesqueen[.]com/innovative.php

http[:]//poisonfight[.]com/idea.php

URL:

http[:]//poisonfight[.]com/idea.php?check= c558838690881fa7f75807cfa94b3713

http[:]//poisonfight[.]com/idea.php?servers= c558838690881fa7f75807cfa94b3713

http[:]//poisonfight[.]com/idea.php?servers= c558838690881fa7f75807cfa94b3713

http[:]//poisonfight[.]com/idea.php?query= c558838690881fa7f75807cfa94b3713

执行命令:

WMIC.exe computersystem get name /format:list

WMIC.exe os get installdate /format:list

WMIC.exe path CIM_LogicalDiskBasedOnPartition get Antecedent,Dependent

WMIC.exe path win32_physicalmedia where tag="\\\\.\\PHYSICALDRIVE0" get serialnumber /format:list

释放文件:

{自启动文件夹}/Java7.exe

%AppData%\.settings.ini

%userprofile%\Desktop\èñïðàâëåííûé âàðèàíò_18.11.2019ã.doc

%Temp%\{随机字符}

[附录]
https://securelist.com/octopus-infested-seas-of-central-asia/88200/
