

金眼狗（APT-Q-27）滥用AWS S3存储桶分发最新恶意载荷

ctfiot.com/286193.html

文章首发地址：https://xz.aliyun.com/news/90793文章首发作者：筱一

概述

近日，笔者基于威胁情报挖掘发现了金眼狗（APT-Q-27）组织的最新攻击活动，基于样本分析、关联扩线等技术，笔者对此次攻击活动进行了详细梳理：

- 攻击者使用了大量携带正常数字签名的文件进行木马传播
 - 山西荣升源科贸有限公司
 - Shandong Saibo Information Technology Co., Ltd.（山东赛博信息技术有限公司）
 - Kingston Technology Company, Inc（金士顿科技）
 - RichQuest Network Technology Ltd.
- 木马使用了多种反沙箱、反调试技术进行安全技术对抗
 - 网络中部分在线沙箱平台无法触发木马的恶意功能
- 木马将外联亚马逊的AWS S3存储桶下载并执行最新恶意载荷
 - 最终远控样本与历史金眼狗（APT-Q-27）组织使用的远控样本同源，且远控指令更丰富

photo20251208698m.exe

文件名称：photo20251208698m.exe文件大小：209792 字节文件版本：8.0.401.0MD5：4B70F3B7BD86678722BC1843517CD4A2SHA1：3B8652142A0CA2DD94C70E2ED1621AD1785231CBCRC32：CCBE07BASHA256：06531922fdad68677036e45406c8a283ed20d07f6ae80ddd4f29053dca846809

国内数字签名

样本携带了国内数字签名，数字签名信息为：山西荣升源科贸有限公司

相关截图如下：



判断文件名

样本运行后，将判断当前进程的文件名是否包含“m”字符串，若不含有“m”字符串，则将弹窗“系统不兼容”，然后直接退出程序。

弹窗截图如下：

相关代码截图如下：

解密字符串

通过分析，发现样本运行过程中，将通过调用Class1.smethod_0()函数解密获取字符串。相关代码截图如下：

尝试修改样本代码，批量解密字符串，所有解密字符串如下：

"JavaUpdate.Properties.Resources""Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0""Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36""Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0""User-Agent""Accept""text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8""Accept-Language""en-US,en;q=0.5""Accept-Encoding""gzip, deflate, br""DNT""1""Connection""keep-alive""Upgrade-Insecure-Requests""1""Sec-Fetch-Dest""document""Sec-Fetch-Mode""navigate""Sec-Fetch-Site""none""Sec-Fetch-User""?1""Cache-Control""max-age=0""Oracle""Java""Updates""N""@27"@HARDWAREDEVICETREESYSTEM"@HARDWAREDESCRIPTIONSystem"@SYSTEMCurrentControlSetServicesDiskEnum""vmware""virtual""vbox""qemu""xen""vboxservice""vboxtray""vmwaretray""vmwareuser""vmacthlp""vmsrvc""vmusrvc""prl_cc""prl_tools""00:05:69""00:0C:29""00:1C:14""00:50:56""08:00:27""0A:00:27""00:1C:42""00:03:FF""System""System Up Time""sandbox""malware""analy""virus""test""ollydbg""ida""x32dbg""x64dbg""windbg""procmon""wireshark""processhacker""tcpview""wireshark""fiddler""procmon""process explorer""regshot""apatedns""netresolver""Memory""Available MBytes""Processor""% Processor Time""_Total""DataReport.exe"@SOFTWAREMicrosoftWindowsCurrentVersionRun""JavaService_""N""runas""YUhsMGNITTZMeTlrWVhSaGntVndiM0owYm1wM0xuTXpMbUZ3TFc1dmNuUm9aV0Z6ZEMweUxtRnRZWHB2Ym1GM2N5NwpiMjB2ZFhVdWRlAa=""file_""-""exe""/download/""png""image""jpg""jpeg""tmp""jpg""png""exe""file_{0:N}.tmp""exe""DataReport.exe""runas""png""jpg""jpeg""gif""bmp""txt""pdf""doc""docx""DataReport.exe""exe""DataReport.exe""runas""png""jpg""jpeg""gif""bmp""txt""pdf""doc""docx""runas""系统不兼容。""m"

反沙箱、反调试

通过分析，发现样本在执行核心功能前，将采用多种技术手段进行反沙箱、反调试。

检查注册表

样本运行后，将检查如下注册表中是否存在“vmware”、“virtual”、“vbox”、“qemu”、“xen”虚拟机名：

- “HKLMHARDWAREDEVICETREESYSTEM”
- “HKLMHARDWAREDESCRIPTIONSystem”
- “HKLMSYSTEMCurrentControlSetServicesDiskEnum”

相关代码截图如下：

检查虚拟机进程

样本运行后，将检查当前进程列表中是否存在如下虚拟机进程名：

- “vboxservice”
- “vboxtray”
- “vmwaretray”
- “vmwareuser”
- “vmacthlp”
- “vmsrvc”
- “vmusrvc”
- “prl_cc”
- “prl_tools”

相关代码截图如下：

检查虚拟网卡

样本运行后，将检查主机MAC地址是否为虚拟网卡MAC地址：

- “00:05:69”
- “00:0C:29”
- “00:1C:14”
- “00:50:56”
- “08:00:27”
- “0A:00:27”
- “00:1C:42”
- “00:03:FF”

相关代码截图如下：

检查CPU核心数及内存大小

样本运行后，将检测运行环境是否符合如下要求：

- CPU核心数 < 2
- 内存大小 < 2GB

相关代码截图如下：

检查系统启动时间

样本运行后，将检测系统启动时间是否少于120秒。相关代码截图如下：

检查运行进程数

样本运行后，将检测当前系统中运行的进程总数是否少于20个。相关代码截图如下：

检查用户名

样本运行后，将检测当前用户名是否包含如下名称：

- “sandbox”
- “malware”
- “analy”
- “virus”
- “test”

相关代码截图如下：

检查硬盘容量

样本运行后，将检查磁盘容量是否小于20GB。相关代码截图如下：

检查是否被调试

样本运行后，将检查当前进程是否被调试。相关代码截图如下：

检查安全工具进程

样本运行后，将检查当前进程列表中是否存在如下安全工具进程名：

- “ollydbg”
- “ida”
- “x32dbg”
- “x64dbg”
- “windbg”
- “procmon”
- “wireshark”
- “processhacker”
- “tcpview”
- “wireshark”
- “fiddler”
- “procmon”
- “process explorer”
- “regshot”
- “apatedns”
- “netresolver”

相关代码截图如下：

外联下载

样本运行后，将Base64解码“YUhSMGNITTZMeTlrWVhSaGNtVndiM0owYm1WM0xuTXpMbUZ3TFc1dmNuUm9aV0Z6ZEMweUxtRnRZWHB2Ym1GM2N5NWpiMjB2ZFhVdWRlID”字符串，获取外联地址<https://datareportnew.s3.ap-northeast-2.amazonaws.com/uu.txt>。

进一步分析，发现样本将发起外联请求，然后根据返回内容下载后续载荷，下载文件将保存至“C:\Users\admin\AppData\Local\Oracle\Java\Updates\xxxxxxxxxxxxxxxxx@27”目录中。

相关代码截图如下：

网页截图如下：

下载后样本信息如下：

文件名	Hash	备注
DataReport.exe	3151B934F1F285211AF6D4C816881900	

文件名	Hash	备注
DataReport.dll	FD260E4849FA91414439CED74B1A25E2	恶意
DataReport.log	B591EE37860F35A788B10531A00BBBD2	恶意
vcruntime140.dll	4113057339D9E4E376BDED9074D20C17	
msvcp140.dll	7E8BDD2C2304E204B44A3BEC09D66062	
image.jpg	4DE8079431D85D3A37FD77FB26E8328F	

DataReport.dll

文件名称：DataReport.dll 文件大小：11768 字节 MD5：FD260E4849FA91414439CED74B1A25E2 SHA1：7093E8B50804C5F3F6DD4106B396D148EF203841CRC32：E7004853SHA256：ec355f76ff1e54054f660e86853bfed9f825f2aa21ae85831eb2d3e6930fec25

解密并执行DataReport.log

通过分析，发现样本运行后，将解密当前目录下的DataReport.log文件，随后直接加载解密后的载荷内容。相关代码截图如下：

DataReport.log

文件名称：DataReport.log 文件大小：162674 字节 MD5：B591EE37860F35A788B10531A00BBBD2 SHA1：79BC7620D08D7A22F3371858EEC1568FA39BE761CRC32：67AEF741

shellcode

通过分析，发现解密后的DataReport.log文件实际是一段shellcode。

shellcode载荷中，还存在一段压缩后的PE文件。相关截图如下：

解密PE文件

进一步分析，发现shellcode运行后，将在内存中解压缩PE文件，然后加载运行PE文件。

相关截图如下：

内存PE文件

文件名称：01220000_upx.mem 文件大小：161792 字节 MD5：69CECF2549EAF971FA04212EC4A121D SHA1：77B1CD225984B727D13E6F320027AA6BD5AE6A84 CRC32：0394B11E

UPX加壳

通过分析，发现此样本携带了UPX壳，直接对其脱壳，即可得到实际样本，相关截图如下：

检查运行环境

样本运行后，将首先检查运行环境，若不满足运行环境要求，则直接退出程序。

运行要求如下：

- 样本未被调试
- CPU 核心数 ≥ 3
- 物理内存 ≥ 3 GB

相关代码截图如下：

内置C&C地址

通过分析，发现样本中内置了大量加密C&C字符串，主要用于后续样本自动化选择C&C。

C&C字符串解密函数如下：

解密后C&C字符串如下：

构建IDAPython解密脚本如下：

```
importidautilsimportida_bytesimportidcdefget_key(enc_addr): data = [] max_len =1024 foriinrange(max_len): b =
ida_bytes.get_byte(enc_addr + i) ifb ==0: break data.append(b) returndatadefxor_decrypt(data: bytes, key: bytes)-> bytes:
iflen(key) ==1: returnbytes(b ^ key[0]forbindata) else: returnbytes(data[i] ^ key[i % len(key)]foriinrange(len(data))) defmain():
target_addr =0x1000148E max_steps =5 found_any =False forref_eainidautils.CodeRefsTo(target_addr,0): current = ref_ea found_push
=False forstepinrange(max_steps): prev_ea = idc.prev_head(current) ifprev_ea == idc.BADADDR: break data =
ida_bytes.get_bytes(prev_ea,5) ifnotdataorlen(data) <5: current = prev_ea continue ifdata[0] ==0x68: imm32 =
int.from_bytes(data[1:5], byteorder='little', signed=False) enc_str = get_key(imm32) xorkey = get_key(0x10046160)
dec_str = xor_decrypt(enc_str,xorkey) print(f"[PUSH] 0x{imm32:08X}@ 0x{prev_ea:08X}, Decode Data : {dec_str}") current =
prev_eaif__name__ == "__main__": main()
```

解密效果如下：

判断管理员权限

样本运行后，将判断当前程序是否以管理员权限运行：

- 若无管理员权限，则尝试调用ShellExecuteExA函数以管理员权限重新运行；
- 若有管理员权限，则尝试创建服务，以实现持久化驻留；

相关代码截图如下：

创建服务

样本运行后，将首先判断系统是否存在Windows Eventn服务：

- 若不存在Windows Eventn服务，则将样本复制至C:UsersadminVideosXXXXXXXXX@27目录，然后创建Windows Eventn服务；
- 若存在Windows Eventn服务，则启动对应服务；

相关代码截图如下：

远控指令

通过分析，发现样本存在大量远控指令，相关代码截图如下：

梳理远控指令功能如下：

远控指令	功能
5430	
5431	DllFile插件
5477	DllScreen插件
5452	DllScreenHide插件
3214	空
5492	DllKeybo插件
5513	DllShell插件
5496、5487	空
5511	DllMsgBox插件
5497	DllSyste插件
5548	空
3217	fnProxy插件
2446	ConnSocks插件
3216	终止explorer.exe进程
3215	以管理员身份重新运行该程序
5527	DllSerSt插件
5520、5521、5522	写入并执行文件
3210	从C2服务器下载插件

远控指令	功能
2447	从C2服务器下载插件
5515	清理攻击痕迹并退出程序
5514	退出程序
5525	设置注册表
5512	ConnectGroup插件
5516	清除Windows日志
5519	运行指定程序
5524	DllOpenURLSHOW插件
5523	DllOpenURLHIDE插件
3221	结束指定进程
3222	删除指定目录的文件
3225	获取指定进程的文件路径
2448	从C2服务器下载插件
2449	onBootup插件
3223	若cmd.exe进程不存在，则运行特定的bat脚本
3224	若cmd.exe进程存在，则结束cmd.exe进程
3227	清除IE浏览器历史记录
3228	清除Skype数据
3229	清除Chrome浏览器数据
3230	清除Firefox浏览器数据
3231	清除360se6浏览器数据
3232	清除360Chrome浏览器数据
3233	清除Sogou浏览器数据
3234	清除QQ浏览器数据

部分远控指令代码截图如下：

5431-DllFile插件
 3216-终止explorer.exe进程
 3215-以管理员身份重新运行该程序
 5522-写入并执行文件
 5515-清理攻击痕迹并退出程序
 5516-清除Windows日志

其他外联

基于静态分析，发现样本中还存在其他可疑外联字符串，相关代码截图如下：

背景溯源

为了确定此样本的木马家族背景，笔者尝试基于网络调研对样本家族进行溯源，最终定位此次攻击活动的木马家族为金眼狗（APT-Q-27）。

溯源过程如下：

- 此次攻击活动与奇安信威胁情报中心于2024年4月3日发布的《VPN安装包“引狼入室”：疑似金眼狗（APT-Q-27）团伙的窃密行动》报告中的最终木马载荷同源，加密C2信息、远控指令等功能均大部分相同；
- 此次攻击活动中的文件行为、进程行为、服务行为、e.nkking.com外联地址与《金眼狗APT后门处置》报告中的描述一致。

相关报告截图如下：

关联扩线

为了更详细的剖析此次攻击活动，笔者尝试基于关联扩线，挖掘发现此次攻击活动中使用的其他样本及数字签名。

数字签名信息如下：

- Shandong Saibo Information Technology Co., Ltd.（山东赛博信息技术有限公司）
- Kingston Technology Company, Inc
- RichQuest Network Technology Ltd.
- 山西荣升源科贸有限公司

关联扩线列表如下：

Hash	文件名	Creation Time	数字签名
3d8bcd5c17425d8a97de0ffeb8addb8d	BusinessDataProcessor.exe	2025-11-30 20:12:48 UTC	Shandong Saibo Information Technology Co., Ltd.
c7082bdd27233200550c3a6dcd4161e6	DataReport.dll	2025-11-30 17:51:05 UTC	Shandong Saibo Information Technology Co., Ltd.
ef776e404e39e89ee326af4252bc8a61	JavaUpdateService.exe	2025-12-01 11:27:12 UTC	Shandong Saibo Information Technology Co., Ltd.
df150002991d77dd1718ce35ea3552a1	JavaUpdateService.exe	2025-12-02 11:45:43 UTC	Shandong Saibo Information Technology Co., Ltd.
8b6f6d2a5c3684827f658321fb994a36	JavaUpdateService.exe	2025-12-02 17:09:18 UTC	Shandong Saibo Information Technology Co., Ltd.
2e0dfc4df82c0fd5e30f24683bef9016	JavaUpdateService.exe	2025-12-03 13:36:44 UTC	RichQuest Network Technology Ltd.
066564533becb4f9c7a8cac1ffbd832a	JavaUpdateService.exe	2025-12-03 15:38:15 UTC	Kingston Technology Company, Inc
32545e9391230b76d480fd06842edb51	JavaUpdateService.exe	2025-12-04 16:02:09 UTC	Kingston Technology Company, Inc
aa4596e4bb9e9c187e93f4950acf4769	photo20251206898.zip	2025-12-06 18:27:30 UTC	
15c94d7fc6ff83e06daa551e155bbb21	photo20251206898m.exe	2025-12-05 14:10:42 UTC	Kingston Technology Company, Inc
c93ee3f63097c2c3f4f80ebb93f011b4	photo20251206896m.exe	2025-12-06 13:42:59 UTC	山西荣升源科贸有限公司
f6cef55bb2ed2f1f8be688cf6609c1e8	photo20251206898.zip	2025-12-07 09:33:16 UTC	
4b70f3b7bd86678722bc1843517cd4a2	photo20251208698m.exe	2025-12-07 15:05:58 UTC	山西荣升源科贸有限公司

外联地址

梳理此次攻击活动中的外联地址信息如下：

外联地址	IP归属地
1.32.250.21	中国香港
1.32.250.227	中国香港
103.145.87.143	中国香港
103.145.87.3	中国香港

外联地址	IP归属地
103.151.44.6	印度.北方邦.诺伊达
103.151.44.82	印度.北方邦.诺伊达
103.215.49.173	中国香港
103.97.228.178	美国.艾奥瓦州.埃德尔
104.233.164.136	日本.东京都.东京
107.148.52.201	中国香港
134.122.190.220	中国香港
134.122.205.97	中国香港
139.28.232.90	美国.加利福尼亚州.旧金山
143.92.32.243	中国香港
143.92.56.224	中国香港
143.92.57.46	中国香港
143.92.61.121	中国香港
154.55.135.212	中国香港
154.91.84.174	中国香港
18.166.142.167	中国香港
18.167.137.104	中国香港
192.252.182.53	中国香港
192.253.225.162	中国香港
202.79.175.78	中国香港
202.94.68.2	中国香港
27.124.41.140	中国香港
27.124.44.76	中国香港
27.124.45.181	中国香港
27.124.7.23	中国香港
43.154.170.196	中国香港
45.120.80.106	中国香港
45.145.73.105	美国.华盛顿州.西雅图
45.195.148.73	菲律宾.马尼拉大都会.马尼拉
8.210.94.213	中国香港
8.217.110.88	中国香港
8.217.69.130	中国香港
8.218.138.126	中国香港
uu.goldeyeuu.io (185.135.79.196)	日本东京
e.nkking.com	

© 版权声明

文章版权归作者所有，未经允许请勿转载。