奇安信威胁情报中心

ti.qianxin.com/blog/articles/Lazarus'-Recent-Attack-Campaign-Targeting-Blockchain-Finance-and-Energy-Sectors/

概述

Lazarus APT组织是疑似具有东北亚背景的APT团伙，该组织攻击活动最早可追溯到2007年，其早期主要针对韩国、美国等政府机构，以窃取敏感情报为目的。自2014年后，该组织开始针对全球金融机构 、虚拟货币交易所等为目标，进行以敛财为目的的攻击活动。

据公开情报显示，2014 年索尼影业遭黑客攻击事件，2016 年孟加拉国银行数据泄露事件，2017年美国国防承包商、美国能源部门及英国、韩国等比特币交易所被攻击等事件都出自APT组织Lazarus之手。

近日，奇安信红雨滴团队使用内部高价值样本狩猎流程捕获多个Lazarus组织新的攻击样本，相关攻击活动具有以下特征：

1. 本次鱼叉式网络攻击活动中，**攻击目标包括区块链与石油天然气等行业**，使用了zip打包Lnk后缀文件或和诱饵文件。
2. Lnk文件使用了的伪装后缀包括txt、pdf、docx等，运行后打开谷歌云盘的诱饵文件或自释放诱饵文件，并同时加载具有后门功能的恶意js代码，将恶意Lnk文件写入到%startup%文件夹中。
3. 近期捕获的诱饵样本标题包括Security Bugs in rigs.zip（钻机安全漏洞），SALT Lending Opportunities.zip （SALT Lenging工作机会），New Development Guidelines.zip （新发展指南），Blockchain Intelligence Group Opportunities.docx.lnk（区块链智囊团工作机会），JP Morgan Chase Job Opportunities.pdf.lnk（摩根大通工作机会）。涉及的企业包括J.P. 摩根大通、SALT Lenging等。
4. **未发现影响国内**，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括威胁情报平台（TIP）、天眼高级威胁检测系统、NGSOC、奇安信态势感知等，都已经支持对此APT攻击团伙攻击活动的精准检测。

样本分析

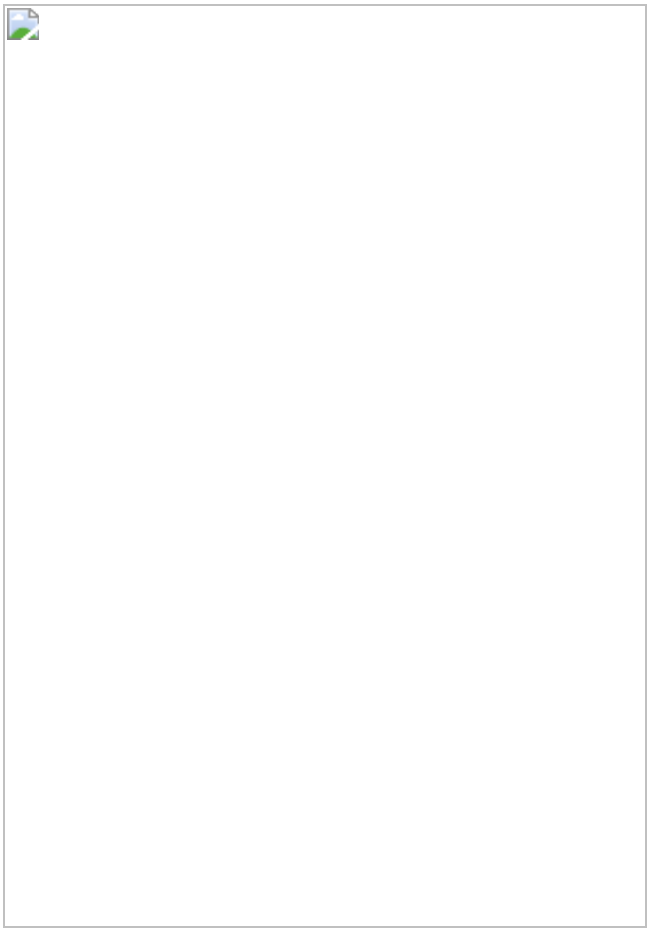
以捕获的最新的LNK样本文件为例，文件名为JP Morgan Chase Job Opportunities.pdf.lnk ，意为摩根大通的工作机会。J.P. 摩根大通，总部位于美国纽约，商业银行部旗下分行5100家，业务涉及投资银行、金融交易处理、投资管理、商业金融服务、私人银行服务等。

涉及样本基础信息如下：

-	-
文件名	JP Morgan Chase Job Opportunities.pdf.lnk
MD5	aefa2caddfeb3bccb1e696cc2cd6955a

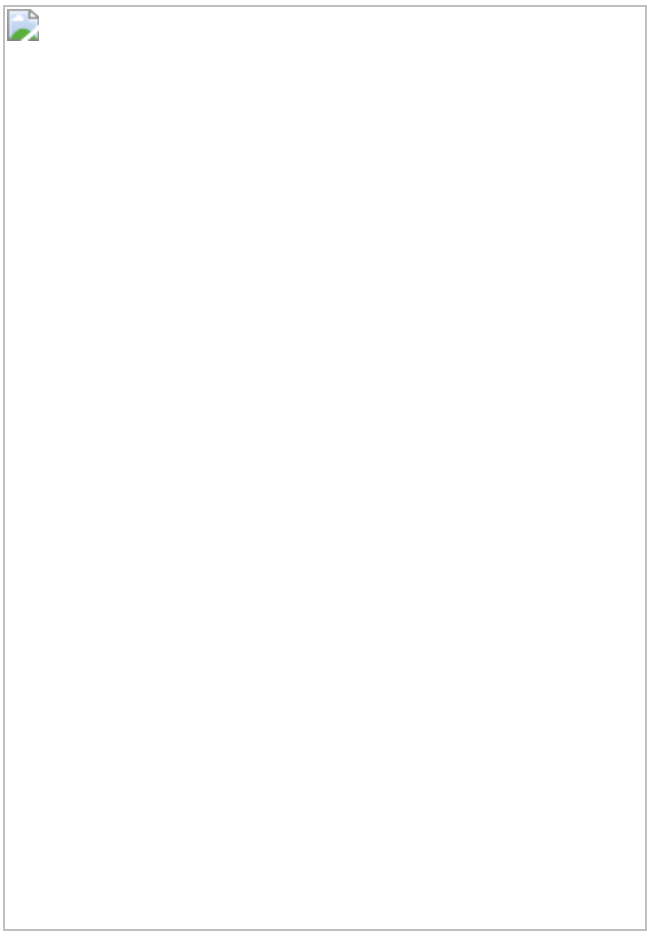
-	-
文件大小	724.64 KB (742035 bytes)
创建日期	2021-04-22 03:38:09
C&C	https[:]//www.googlesheetpage.org

释放的诱饵如下:



详细分析

通过奇安信威胁情报中心自研深度文件解析引擎QOWL解析Lnk文件结果如下：

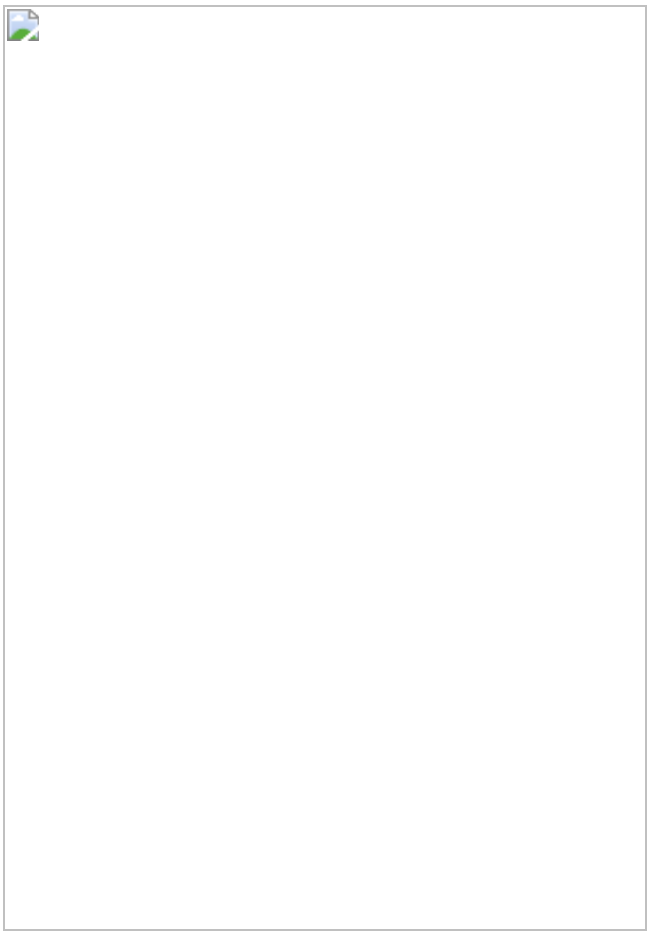


根据解析结果可得到基本信息。该Lnk文件使用cmd.exe运行mshta.exe，参数为https[:]//www.googlesheetpage.org/bSQphSxgStENEhz5Y+PZCpjr/NBSWGWjjhkJi/PvaqE=。使用了EDGE浏览起的图标作为伪装。

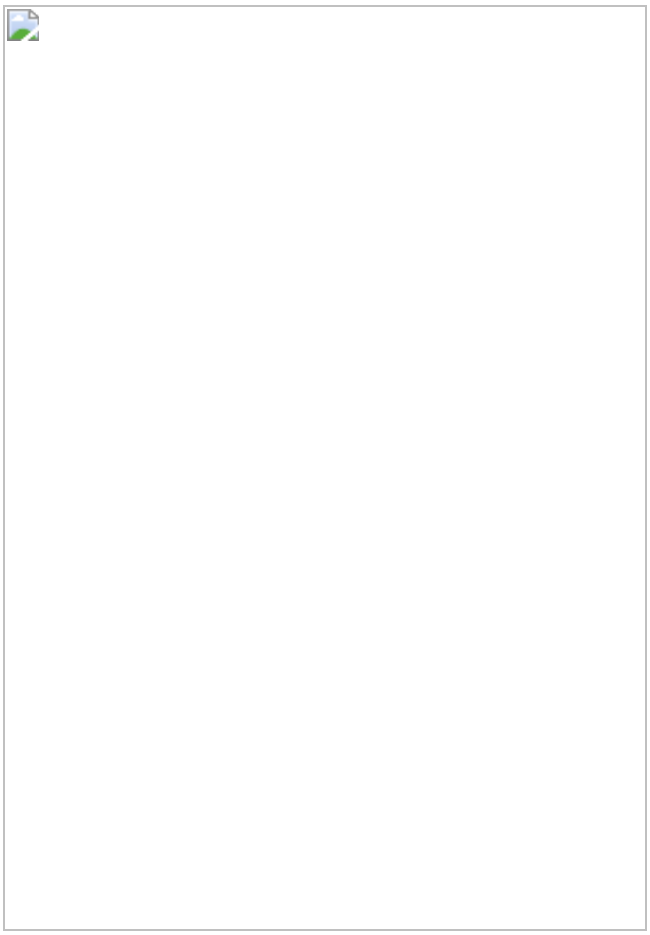
请求的网址数据是一段Jscript代码。Jscript代码为了方便查看和分析进行了一定的去混淆处理。相关样本信息如下：

-	-
MD5	e0d73c941e3792f7c753724c0c064de8
编程语言	Javascript

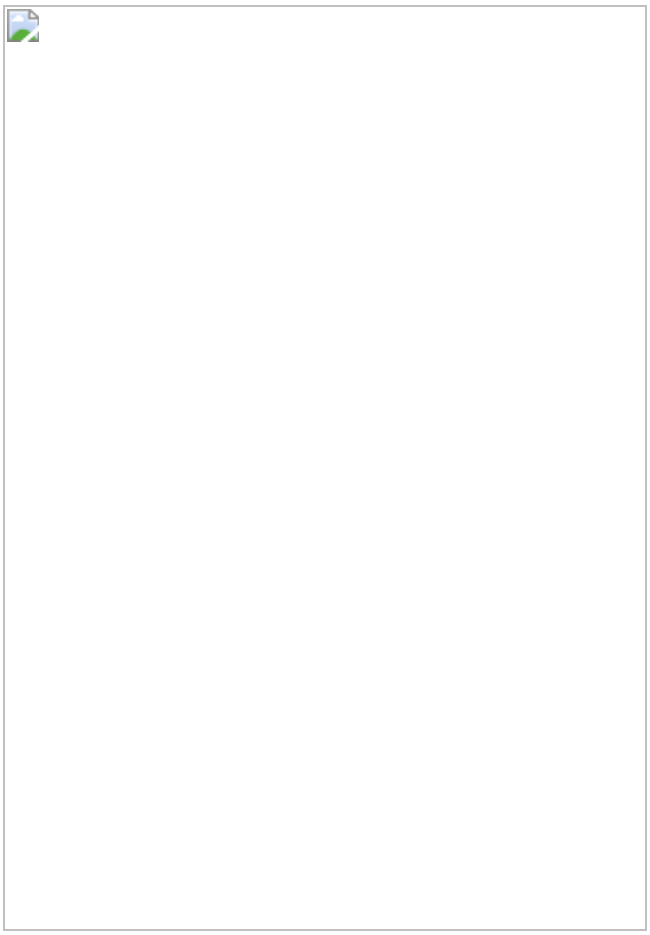
接着会打开base64解码后的谷歌云盘中的诱饵文件。



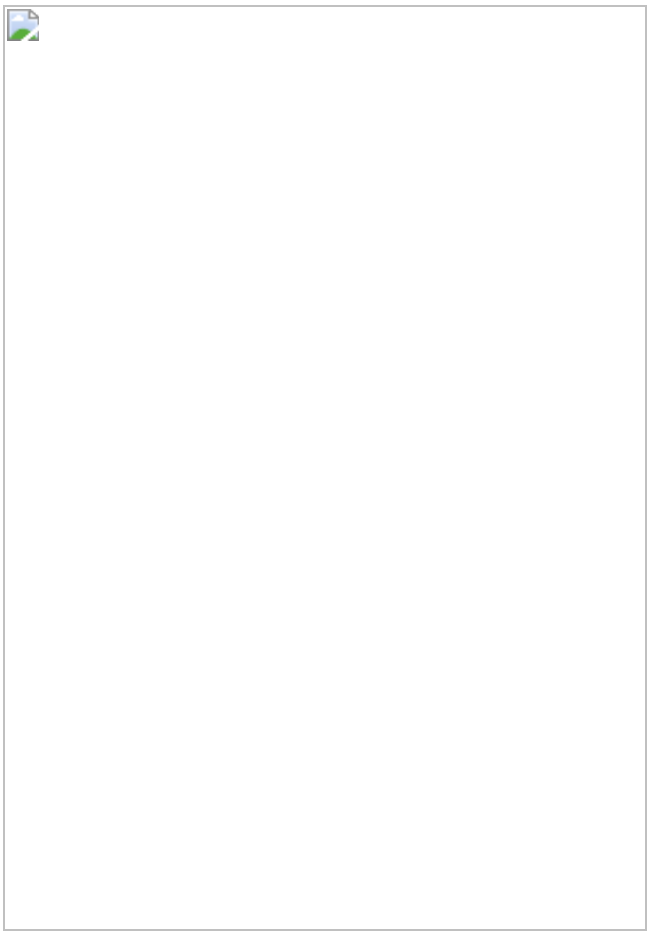
并通过wmi接口遍历当前系统进程，检查杀毒软件。



Bdagent和epsecurityservice为Bitdefender 公司的杀毒组件，ccSvcHst和nortonsecurity为赛门铁克安全公司的杀毒组件。Kwsprot是金山毒霸的组件。Ekrn是ESET的反病毒软件相关程序。Npport是[Net Protector Antivirus](https://www.npav.net/" \t "_blank)[的杀毒组件。](https://www.npav.net/" \t "_blank)



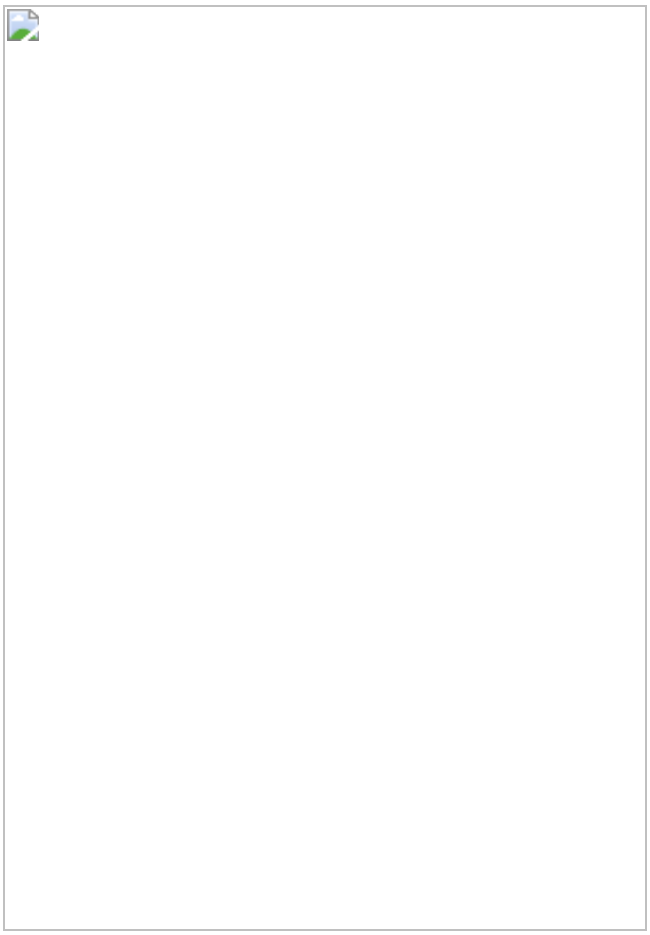
解码一长串base64后，写入到%Temp%\\reqveh.js，并在后续中启动并传入参数 www.googlesheetpage.org/ 与 1或者2。将写好参数的LNK文件复制移动到开机启动文件夹。
短链接指向
https[:]//www.googlesheetpage.org/+Oy4hirVnSwZBtJJuw/rQz82YTYsSH4P4eVS3au1ano=.



对应的reqveh.js文件信息如下：

-	-
文件名	rqveh.js
MD5	C2E62F04D5234BA46A050BDDDF3540CB

通过参数生成uid后请求url，并执行接收到的数据。5秒请求一次。



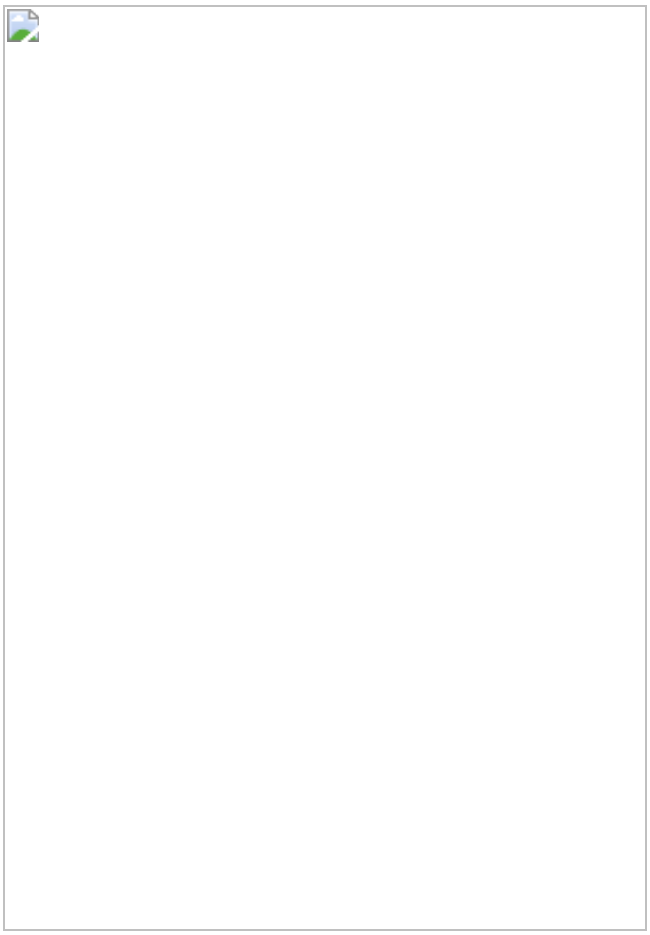
溯源与关联

奇安信威胁情报中心红雨滴团队结合威胁情报中心ALPHA威胁分析平台（https://ti.qianxin.com/），对此次攻击活动的手法、恶意代码等方面关联分析发现：此次攻击活动与Lazarus组织样本存在高度相似性。该样本与此前的Lazarus组织使用的Jscript代码MD5：9d555c1093ff84ac3d442b1a0617f7ef存在一致性。

总结

Lazarus 团伙是一个长期活跃的APT组织，武器库十分强大，拥有对多平台进行攻击的能力，近年来，该团伙多次被安全厂商披露，但从未停止进攻的脚本，反而越发活跃，攻击目标也越发广泛。同时，该团伙也多次针对国内进行攻击活动，企业用户在日常的工作中，切勿随意打开来历不明的邮件附件。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括威胁情报平台（TIP）、天眼高级威胁检测系统、NGSOC、奇安信态势感知等，都已经支持对此APT攻击团伙攻击活动的精准检测。



IOCs

MD5

aefa2caddfeb3bccb1e696cc2cd6955a

e0d73c941e3792f7c753724c0c064de8

9f8e51f4adc007bb0364dfafb19a8c11

db315d7b0d9e8c9ca0aa6892202d498b

f5b14052e15aea78d2da695276f585c8

A2BE99A5AA26155E6E42A17FBE4FD54D

e24bbbd3b32ca2fd3b8fb76f036cb4bb

790a21734604b374cf260d20770bfc96

d3a988a9750cb6582310c806fa32d4f1

805949896d8609412732ee7bfb44900a

1bf36342c0506a58369a3b530b7d0bcc

60214745027c7efa7cc920d43d9c254a

9a06ce2b0b038de9147f93bbb3b3c56c

173edf96e60b3fd520801a6c1adee7e0

2a78bf4487915d91855d0c4661d974a0

071107f7bddc8ca6e8a8c3c94931512c

59c328cd766f6ec0c9141bca7da6b807

5bec2687fd743d23331cd54c987b44de

URL

https://www.googlesheetpage.org

https://product.onlinedoc.dev

https://share.devprocloud.com

https://gsheet.gdocsdown.com

https://signverydn.sharebusiness.xyz

https://dev.sslsharecloud.net

https://sharemanage.elwoodasset.xyz

https://dshellelink.gcloud-share.com

https://page.googledocpage.com