目标国防行业：Lazarus使用招聘诱饵结合持续更新的网络武器

By 红雨滴团队

Archived: 2026-04-05 15:24:59 UTC

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。

据公开资料显示，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时间都出自Lazarus之手。

近几个月来，Lazarus组织常用航天，核工业，船舶工业等专业领域头部企业招聘信息为诱饵进行攻击活动，四月中旬红雨滴团队曾披露过《Lazarus APT组织使用西方某航空巨头招聘等信息针对美韩的定向攻击事件分析》，该活动后续被某安全厂商归为北极星行动（OperationNorthStar），近日，奇安信威胁情报中心红雨滴团队在日常的高价值样本挖掘过程，又捕获了一例该类型攻击样本，此次攻击活动中，Lazarus组织以通用（GDMS）公司高级业务经理招聘为诱饵，通过恶意宏释放执行后续Payload。红雨滴团队在捕获该样本的第一时间通过社区进行预警。

除此之外，最近几个月我们检测到在Lazarus也在对其Crat木马架构进行快速迭代，目前已经相当成熟。

样本分析

Operation NorthStar新活动

文件名	MD5	类型
GDLS_2020090392828334.doc	8ed89d14dee005ea59634aade15dba97	宏文档

近期捕获的样本采用word本体嵌套一层word的数据,通过宏进行自身数据读取释放运行招聘文档本体,初始文档无法查看诱饵内容，从而诱导受害者启用宏。

若启用宏后，第一层宏文档将在%temp%目录释放同名第二阶段带诱饵文档释放打开的第二阶段文档以GDMS招聘信息为诱饵,通用动力任务系统公司涉及国防和航空航天,

样本在文字末尾通过白色图形遮盖了招聘文档和控件,字符串采用白色进行隐藏。

恶意宏如下所示。

宏与2018年Lazarus APT组织所使用的部分宏代码一致

在HOMEPATH\Videos下释放名为localdb.db的Loader程序，并在启动目录下释放Recent.lnk，实现持久化。

Lnk命令行如下

调用localdb.db的导出函数ntSystemInfo，参数为“qBzZN42AyWu6Qatd”

文件名	MD5	类型
localdb.db	35545d891ea9370dfef9a8a2ab1cf95d	PE

运行过程中会比较参数是否正确

如果正确则会解密出一段PE，并进行内存加载

内存加载的PE疑似为Lazarus APT组织新型Downloader，核心代码在创建的线程中

解密字符串

解密的字符串如下：

之后进入下载者的流程

获取本机相关信息以“|”相连接

获取正在运行的进程信息

收集的信息如下：

对上述信息进行加密后再进行Base64编码，发送到远程服务器上获取后续

https://www.dronerc.it/shop_testbr/Adapter/Adapter_Config.php

https://www.fabioluciani.com/ae/include/constant.asp

遗憾的是我们没有获取到后续的木马，如果下载到了后续，则会进行解密操作，之后内存加载。

Crat木马

Crat最早出现于今年五月份，Lazarus Group针对韩国证券公司进行APT攻击的活动，由于后门的PDB中存在“Crat Client”的字符串所以将其命名为Crat，从五月份至今，我们一直在对Crat进行跟踪，发现经过了几个月的迭代，目前该木马架构已经较为成熟。

其早期样本中存在大量的调试字符串，功能没有呈现出模块化的趋势

代码中出现了大量的调试字符串

创建的互斥量如下：

在近期捕获的Crat样本中发现已经开始模块化，管道模块、信息收集模块、屏幕监控模块、键盘记录模块、持久化模块等

代码结构发生了细微的改变，调试字符串已经被删除，相关样本及其C2如下：

MD5	**C2**
2a9e49fc80fe5124ac98ff5b874fb4d4	www.advertapp.me/user/invite.php?ts=
6dafaabebf243e1ad2e5b49178230eb6	www.publishapp.co:443/update/check.php?ts=
11eb80efbf659d7a91bd0e1281d01443	www.loonsaloon.com/wp-content/plugins/revslider/hello.php
a3e3886ae43c6e67acf06d8041d8f4d2	www.moonge.cc

总结

2020年以来，疫情肆虐全球，同时网络空间的攻击活动也越发频繁，近期，东亚形势备受关注，而具有该国背景的APT组织近期也活动频繁。

奇安信红雨滴团队提醒广大用户，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行夸张的标题的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台（https://sandbox.ti.qianxin.com/sandbox/page）进行简单判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

IOC

MD5

8ed89d14dee005ea59634aade15dba97

35545d891ea9370dfef9a8a2ab1cf95d

2a9e49fc80fe5124ac98ff5b874fb4d4(Crat)

6dafaabebf243e1ad2e5b49178230eb6

11eb80efbf659d7a91bd0e1281d01443

a3e3886ae43c6e67acf06d8041d8f4d2

C2:

https://www.dronerc.it/shop_testbr/Adapter/Adapter_Config.php

https://www.fabioluciani.com/ae/include/constant.asp

www.advertapp.me/user/invite.php?ts=

www.publishapp.co:443/update/check.php?ts=

www.loonsaloon.com/wp-content/plugins/revslider/hello.php

www.moonge.cc

参考链接

【1】 https://blog.alyac.co.kr/3018

【2】 https://twitter.com/RedDrip7/status/1303186209158492160

【3】 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true

---