# 2021年度热门挖矿木马——JavaXminer

随着近十年来加密货币的兴起和相应数字货币价值的持续走高，这个新领域逐渐地吸引了各方关注，这其中自然也包括黑产行业，一个新的恶意软件类型——挖矿木马应运而生。一旦机器被入侵并被植入了挖矿木马，那只要木马还在运行，便可以为黑客带来源源不断的收益。也因此在短短几年内就催生出一大批的挖矿木马家族，与之一起增加的还有对各个平台机器的大量攻击。

挖矿木马一般需要控制大量设备来实施挖矿，才能保证可观的收益，所以我们经常可以看到挖矿木马与“僵尸网络”相伴而生。而入侵的方式多种多样，比如软件捆绑、服务器类漏洞攻击、口令爆破等。

本文将要介绍的是一个被我们命名为JavaXminer的挖矿木马家族，该家族多使用Web服务类漏洞对OA系统、Web服务器等进行攻击。该木马团伙更新迅速且频繁，善于利用最新公开的各类Web漏洞，从其攻击趋势也可以看出与Web端漏洞的曝出相关。

360高级威胁研究分析中心从2018年开始，便对JavaXminer进行了持续监控。我们发现该家族具备Windows、Linux双平台的攻击能力，导致其攻击量在2020年至2021年有大幅度增加。基于大数据分析发现：与该家族所攻击的主要Web应用目标——如各类OA、Tomcat、Confluence等——受到攻击的整体态势与JavaXminer攻击量变化态势基本吻合，这也佐证了JavaXminer的攻击对整体安全态势的影响力。

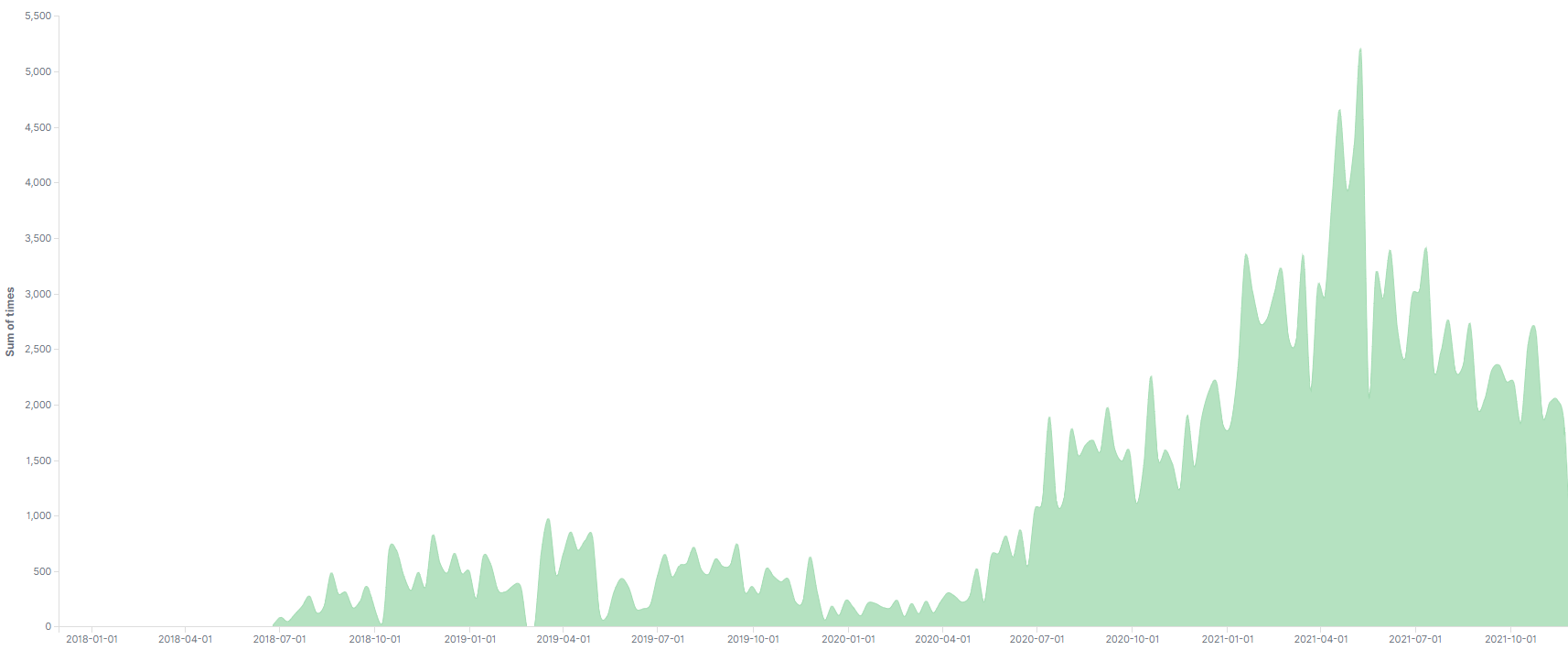


图 1 JavaXminer攻击趋势

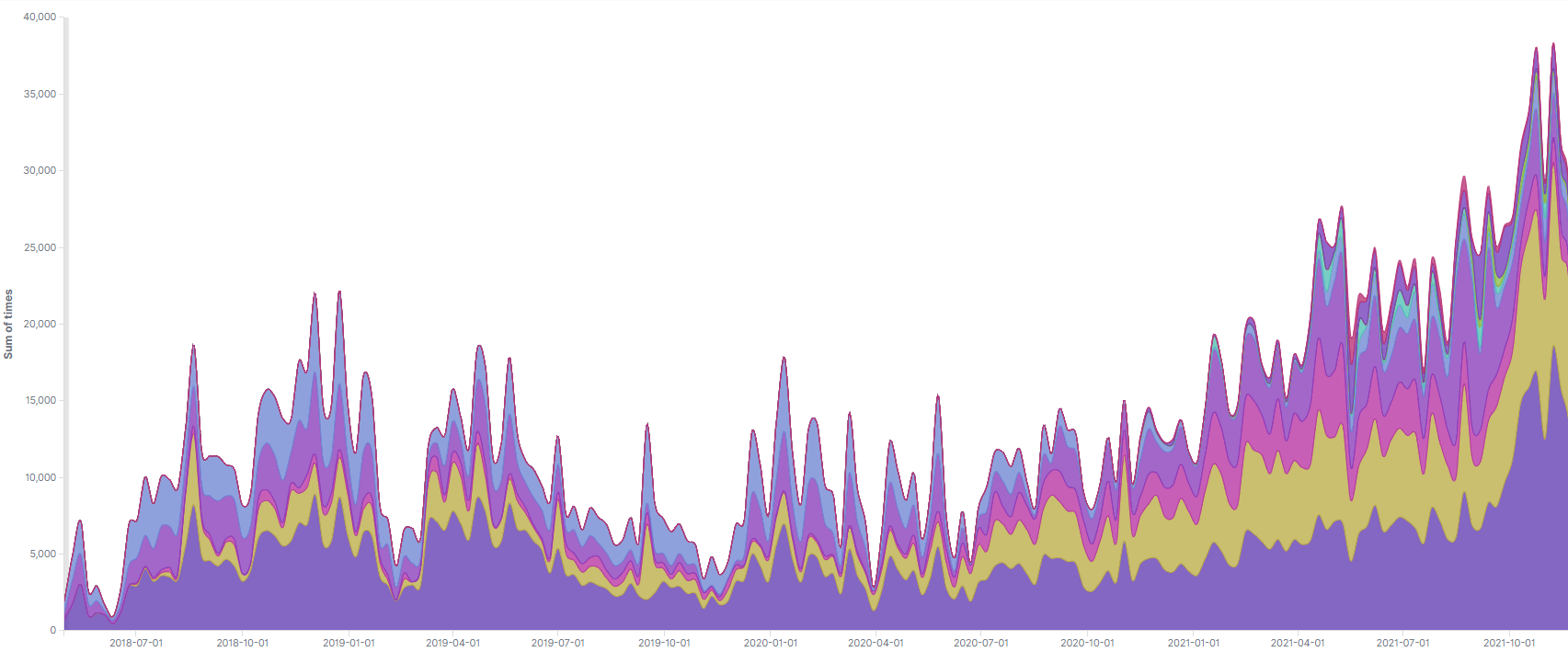


图 2 关联Web应用攻击整体趋势

## 初始访问

JavaXminer的入侵往往会利用新近曝出的Web服务端1Day或是nDay漏洞，成本降低的同时又可以较为轻易的获取未及时修补漏洞的服务器访问权限。比如Atlassian Confluence在今年8月底发布的CVE-2021-26084 RCE漏洞，GitHub上9月1日便出现了相应利用POC，紧接着在9月3日就出现了利用该漏洞对Confluence发起的攻击。

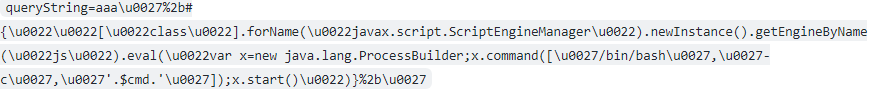


图 3 CVE-2021-26084 公开POC

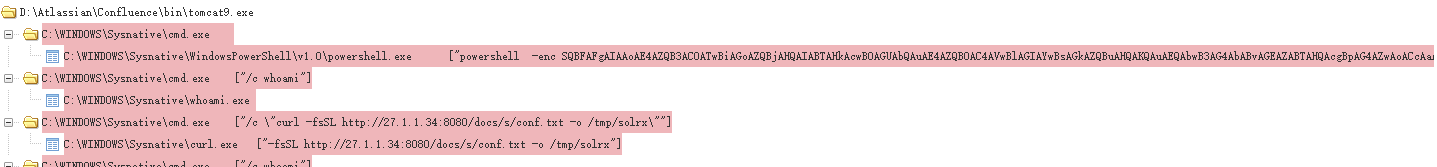
图 4 JavaXminer对Confluence初次攻击

图 5 JavaXminer对Confluence攻击

同样的情况出现在致\*、通\*、泛\*等OA系统上。随着OA系统漏洞的曝光，相应的攻击脚本也积极地被该挖矿家族利用。

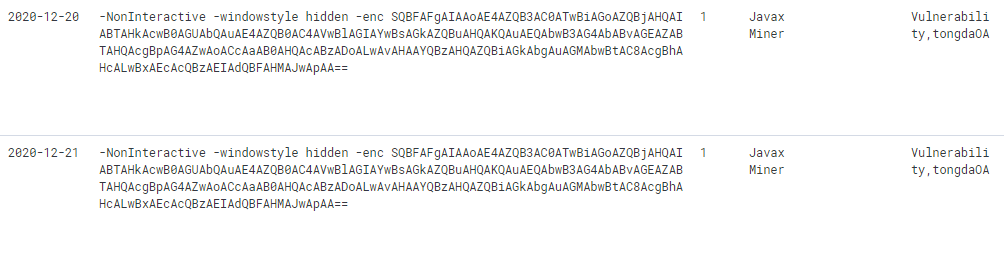


图 6 JavaXminer对通\*OA初次攻击

## 清除竞品

暴露于公网且存在漏洞的服务器很容易被各种木马给盯上。对于挖矿木马来说，在这种机器上常常会碰见自己的“同行”。为了最大程度地占据系统资源挖取货币，对“竞品”的清理工作在所难免——在这一点上JavaXminer也不例外。

被清理的竞品木马都是比较知名的家族，比如Kinsing、watchbog、Mykings、Sysrv-hello、SysUpdate、IMG001等。（注：IMG001之前未被公开报告，该家族出现时间较早，曾使用U盘蠕虫、内网横向渗透进行传播。）

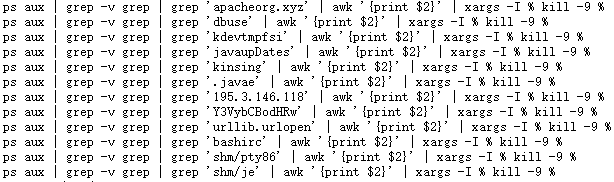


图 8 清除竞品



图 9 清除竞品

## 长期驻留

在入侵成功后的Linux机器上，JavaXminer会通过crontab创建计划任务，每5分钟访问一次hxxps://pastebin[.]com/raw/xxxxxxxx，获取内容执行。

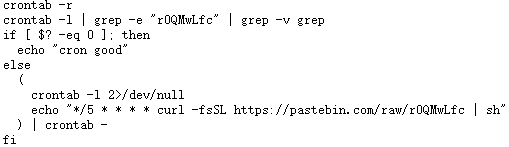


图 10 Linux计划任务

然而这些pastebin粘贴板文本大多为无实质操作的语句，粘贴板名通常与相关脚本url名和攻击手段、目标有关，其中对粘贴板的访问可直观地观察到入侵机器是否活跃和增长。并且创建者ID重复情况较多，可一定程度上作为该家族木马的关联。目前时间较早的粘贴板大部分已被删除，较近时间段（比如10月份）的URL则大多正常。

尽管绝大部分粘贴板未写入恶意命令，但其下发指令的能力是确实存在的。

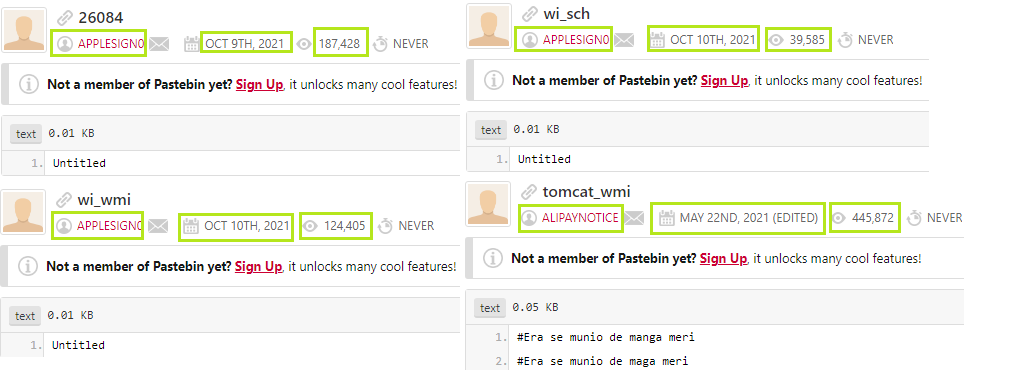


图 11 pastebin内容

在Windows系统的机器上，JavaXminer同样会进行持久化，访问相应pastebin数据执行——即使大部分均为无效指令。创建持久化任务的方式则是采用WMI Subscription事件或是schtasks命令。

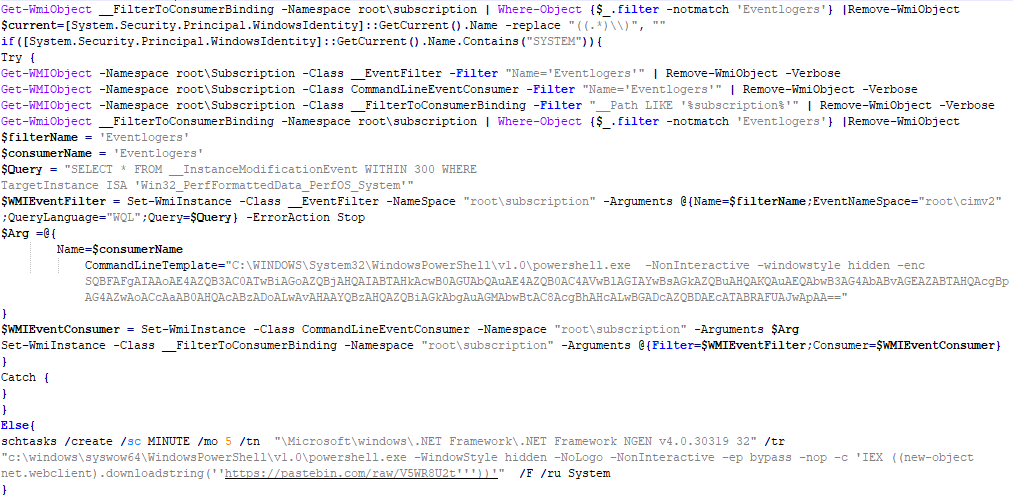


图 12 Windows持久化

## 执行挖矿

JavaXminer挖矿时使用配置文件config.json指定XMRig执行时的各项参数，矿工程序落地文件名也不尽相同。下载时的URL特征之一是路径中常带有/docs/字符串，并且托管文件的服务器通常为Apache Tomcat。



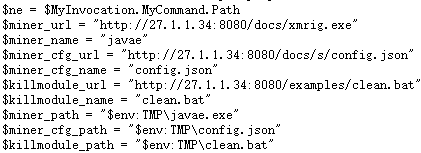
图 13 Linux端执行挖矿程序

图 14 Windows端执行挖矿程序

Config.json配置文件中，指定矿池为pool.supportxmr.com:80，而pass统一为“x”。

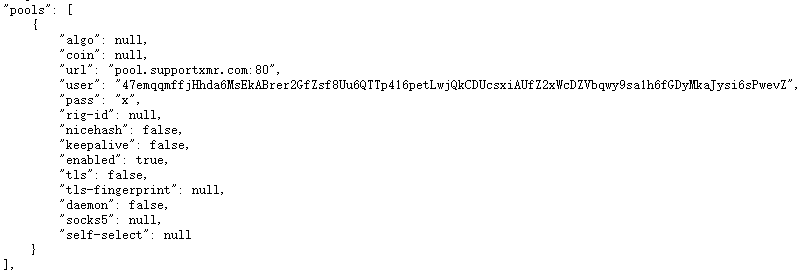


图 15 Config.json Pools配置

## XMR钱包数据

Config.json配置中的钱包地址并不只有一个，我们从钱包地址中取出几个还在活跃的钱包地址，在supportxmr中可以查看其算力和挖取的门罗币数据，以此判断JavaXminer的挖矿能力。



图 16 JavaXminer部分钱包挖矿数据

从上图中可以看出这部分钱包地址依然拥有算力，获取的门罗币也不少。而且这些钱包地址只是其中一部分，由此可以推测受到JavaXminer入侵并成功开挖的机器也也在少数。

在利益驱动下，以挖矿为目的的恶意入侵活动愈发猖獗，作为相关产品的使用用户来说，主动进行产品更新和补丁修补显的尤为重要，以免自身资产沦为挖矿的工具。

360新一代终端检测响应系统（360EDR）通过持续监测终端活动行为、检测安全风险、深度调查威胁风险、提供补救响应手段等方式，补充了传统终端安全产品防御高级威胁能力的不足，能在对抗高级威胁中压缩攻击者的攻击时间，减少高级威胁最终达到目的可能性，获得更快速、高效的防御效果。



图 17 360EDR告警信息展示

通过360EDR能够及时发现和处置各类挖矿攻击，可以通过部署360EDR检查设备使用被JavaXminer入侵。



图 18 360EDR安全事件展示

## IOCs（部分）

**URLs：**

hxxp://159.65.122.137:8080/docs/javas00.txt

hxxp://27.1.1.34:8080/docs/s/wi.txt

hxxp://27.1.1.34:8080/docs/s/kill.sh

hxxp://167.71.197.52:8888/js/ta.txt

hxxp://27.1.1.34:8080/docs/config.json

hxxp://27.1.1.34:8080/docs/s/config.json

hxxp://211.239.117.113:8080/docs/dd1.txt

hxxp://159.65.122.137:8080/docs/javas.txt

hxxp://220.132.202.169:9080/docs/ffma.txt

hxxp://27.1.1.34:8080/docs/s/26084.txt

hxxp://159.65.122.137:8080/docs/zy1.txt

hxxps://pastebin.com/raw/R5c9QFnS

hxxps://pastebin.com/raw/F7eCGLQU

hxxps://pastebin.com/raw/r0QMwLfc

hxxps://pastebin.com/raw/V5WR8U2t

**钱包地址：**

43DAWB7qLHs6ynPP6JkxLUAgQrG8yyFswLef9GzBqz8BYnmbhSUitRYTEfzXxxCA7HisGCvw4u5swJCHGNP42Sx9Jjbdgqp

4BDEgsM9raUWrY2C1ptgnzdC1hVdnaAdu3vQLmrQueK882WBrFvnLL4JWUSpuBAZt4dLMBbKXTmSoPoB6jPUeAuaCCkonTL

47PXdhiZphNHka2K1J9udPj5Nct4zpvCRUMqwVY4Rvyxf3FLmPqyR6J68hDX4fUF65jNxJa43szPM3Ni5zDerArzSkdFp1K

48zfBUeSCupa7hxjWxxGcABqYKAEpM8fCLhhJ34toDHKLQXdxfSPonCDcTFtTQTXxTUCkkCAS28dUSz83H8U6bdr6Hh2Q2d

49r6Mp1fcb4fUT5FPTgaz9E47fZV7n6JiY76c4vdBZvgDm8GmWHTVYM9Azpe4MsA9oXs2RpUNPPfH7oXABr3QnwNQKaP2W7

431Vsm2jFrfaxwwgputHDqVWPq69y2bQhBSrdDzCNR4JjADAfjjyuRTjCkiv3mxAVFG3JWLk4GyxMFM8BqMzmh1uEN6HDP6

48aviohKeqyLCMcWSrvX9BbXWPeZLJps35pMBmFMtxtnXTR9HNPVYU8J1VNHmhhraoDEeZ3nBhdtHDJ2f4wskcbv3rd1f1Z

4BrL51JCc9NGQ71kWhnYoDRffsDZy7m1HUU7MRU4nUMXAHNFBEJhkTZV9HdaL4gfuNBxLPc3BeMkLGaPbF5vWtANQkiTzF2BGMcPSynymf