

CNCERT | 关于“FakeSvc”挖矿组织大规模传播恶意程序的风险提示

mp.weixin.qq.com/s

CNCERT



国家互联网应急中心CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称CNCERT或CNCERT/CC），成立于2001年8月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。

感谢安天科技股份有限公司（安天）在本报告的样本分析工作中做出的重要贡献。

一、概述

“FakeSvc”挖矿组织通过SSH弱口令暴力破解入侵Linux服务器后，植入多层攻击载荷：一个极简加载器从指定域名按CPU架构下载对应ELF二进制文件，将其伪装为系统进程静默启动；该二进制文件实为IRC僵尸网络客户端，通过加密信道接收远程控制指令，同时配套的扫描框架

轮询获取密码字典和目标地址，调用多种爆破工具横向扩散；部署定制版门罗币矿机实施挖矿，并通过计划任务实现持久化，形成“暴力破解、入侵、挖矿、继续暴力破解”的蠕虫式自传播闭环。

二、恶意样本分析

1.反弹shell脚本分析

攻击者搭建了一个持久化的交互式Shell入口，建立到C2的反向连接，获取远程Shell。连接方式：依次尝试nc→bash→sh→perl→python→python3，选择一个可用的方式建立反向连接。

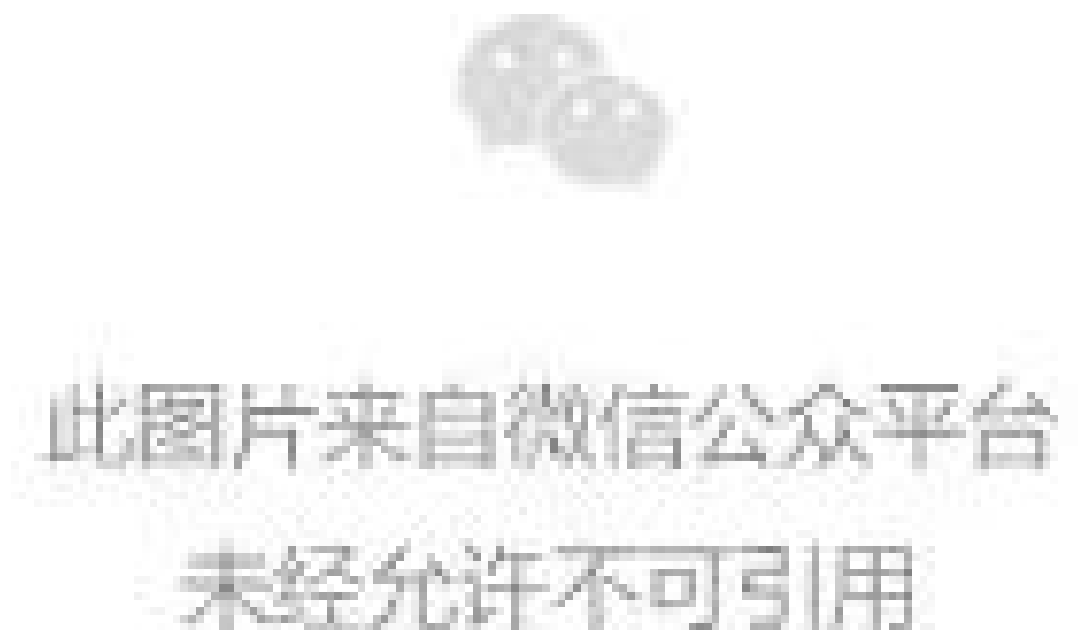


图1 建立反向连接

2.核心扫描暴力破解脚本分析

该脚本是整个样本的核心模块，一个模块化、C2驱动的SSH扫描/暴力破解框架，并且具备自我更新机制。

表1 样本标签

病毒名称	Trojan/Script.FakeSvc
原始文件名	mixscan
MD5	72CB9221703EA28E3289E85724EDAF19
文件大小	43.5KB(44,577字节)
文件格式	Script/Linux.SH

具体各功能模块详解见下表：

表2 脚本各功能模块详解

函数	功能	C2 API参数
get_gmsc	获取扫描配置（密码本文件名、爆破类型、线程数等）	?gmsc=
get_gpwnbst	获取密码本列表	?gpwnbst=
get_gpwnlbn	获取密码本名称	?gpwnlbn=
get_as / get_griplfn	获取目标IP列表	?as= / ?griplfn=
get_giplbfn	下载具体的IP:Port文件	?giplbfn=
get_banner	Banner抓取，识别SSH服务类型和操作系统	调用本地bot二进制
get_pf	下载密码字典文件	?gpwnlbn= / ?gpwlbn=
get_brute	SSH暴力破解	调用本地bot二进制
get_vuln_filter	过滤成功登录的目标	本地处理
get_vuln_upload	POST上传成功结果到C2	?vuln=@filtered.txt

get_gbot	下载/更新bot二进制（主payload）	?gbot=
get_scanbot	下载scanbot子脚本	?gscanbot=
get_scanbot_cron	将scanbot写入crontab持久化	—
get_gsbfbf	下载Spirit扫描器工具包	?gsbf=

支持SOCKS5代理暴力破解、IP列表分割（每1000个IP一批）。

表3 支持的暴力破解工具

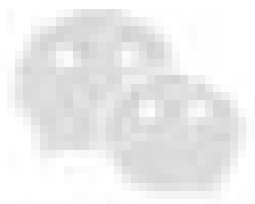
类型	工具名
haiduc	Haiduc SSH爆破器
haita	Haita SSH爆破器
spirit	Spirit SSH爆破器
zhcn	中文SSH爆破器

具备Banner抓取功能，抓取后会过滤掉非目标设备（Cisco、Windows、Mikrotik、防火墙等），保留Linux发行版。

表4 支持的Banner抓取工具

类型	工具	输出文件
bssh	bssh扫描器	banners.log
prg	prg扫描器	banner.log
spirit	Spirit扫描器	b.lst

通过crontab每分钟执行一次scanbot子脚本。



此图片来自微信公众平台
未经允许不可引用

图2 建立计划任务

3.初始投递/下载器脚本分析

初始载荷功能为从C2下载并执行主载荷。

表5 功能概览

步骤	功能
1	收集本机信息：CPU架构(uname-m)、主机名、用户名

2	生成机器唯一ID mid : machine-id+cpuinfo+MAC地址 →sha256→前10位
3	从http://scanbot.me/?gbot=\${arch}下载payload，保存为-bash
4	将ELF载荷以伪装进程名bash静默启动，并携带主机指纹和节点标识向C2注册该肉鸡
5	删除-bash，清理痕迹

4.IRC僵尸网络客户端分析

该组件是一个IRC僵尸网络客户端(IRC Botnet Client)，版本号为v2.0，自称为"botnet"。该组件属于Linux平台下的僵尸网络后门，通过IRC协议与C2服务器通信，接收并执行远程命令。

表6 样本标签

病毒名称	Trojan/Linux.FakeSvcBot
原始文件名	x86_64
MD5	CDB61FE8B0142ABDD4C140B3FF81FEC8
处理器架构	X64
文件大小	171KB(175,432字节)
文件格式	ELF
数字签名	无
加壳类型	UPX

组件使用两层XOR加密来隐藏敏感字符串，解密后IRC频道为“#.botnet.#”，版本号v2.0，SSH用户名为root，C2域名和IP地址等如下表所示。

表7 解密后的C2域名/IP地址

C2域名	IP地址
systems.cmd.systems	
cmd.sshd.services	
cmd.systemctl.cc	
cmd.botnet.vip	
cmd.torservices.download	
cmd.scanbot.me	
cmd.do-dear.com	
	51.79.74.212
	168.235.95.104
	185.106.120.99

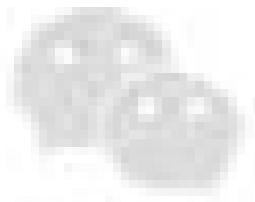
连接时依次尝试每个服务器+端口组合，共计7个可用端口，分别为80、443、6667、6668、7000、8080、22。并且支持丰富的命令行参数，具有高度可定制性，命令行详情如下表所示。

表8 命令行参数说明

参数	说明	默认值
-h	伪装进程名(argv[0])	ssh
-n	IRC昵称	随机生成(BN-机器ID-用户名)
-i	IRC Ident	随机机器架构名
-r	IRC Realname	随机生成的机器ID
-c	IRC频道	#.botnet.#
-k	频道密钥	password
-xu	ChanServ用户名	-
-xp	ChanServ密码	-
-m	自定义机器ID (IPC锁)	自动检测
-nk	禁用杀死旧实例	默认会杀死
-cmd	显示帮助信息	-

5.挖矿程序分析

主要挖矿模块是XMRig（开源Monero矿工）的静态编译定制版本，内部代号“botRig”。连接门罗币矿池地址为services.sshd.services，钱包地址为46emQim8J2i3eWK99jE3MnhbvtDvDkZEBHw2a5gSWA8Zj4K4uX6ATviRXmTqJRe3UxbCnX4cf6GGyQ9N9UYLNjm8AxBLwPk。

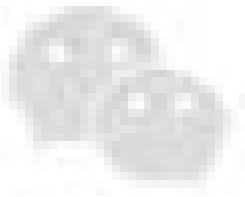


此图片来自微信公众平台
未经允许不可引用

图3 挖矿程序连接矿池挖矿

三、感染规模

通过监测分析发现，境内2026年6月15日至7月22日期间，该组织样本日感染终端数量最高达2511台，累计监测到16054台设备被感染，境内每日感染终端数量情况如下。



此图片来自微信公众平台
未经允许不可引用

图4 境内感染终端数量

四、防范建议

1.强化SSH服务安全加固，杜绝弱口令入侵

本次攻击以SSH弱口令爆破为主要入侵入口。需禁用简单弱口令、默认口令，部署高强度复杂密码并定期更新；优先开启SSH密钥登录，关闭密码登录模式。可修改SSH默认端口，配置运维IP白名单，严格限制远程登录权限，从源头阻断暴力破解攻击。

2.严控主机权限，阻断恶意载荷执行

严格落实服务器最小权限原则，禁止root账户远程登录，日常运维使用低权限账户。定期排查系统陌生bash脚本、无来源ELF可执行文件，严控未知文件执行权限。重点核查伪装为bash、ssh的异常系统进程，及时查杀恶意程序、阻断载荷运行。

3.清理持久化任务，消除驻留后门

该恶意程序通过crontab定时任务实现持久化驻留与自动扫描。需常态化排查服务器计划任务，重点清理每分钟执行的scanbot挖矿、扫描类异常任务，重启服务固化配置。同时监控定时任务新增、修改行为，杜绝恶意后门持久化留存。

4.部署边界防护，拦截恶意网络通信

在防火墙、安全组等边界设备中，封禁本次曝光的恶意IP、C2域名、矿池地址及攻击URL，阻断恶意外联通信。开启网络流量审计，重点监测服务器高频SSH扫描、异常加密外联等可疑行为，实现攻击行为快速预警、拦截处置。

5.常态化安全巡检，及时排查感染风险

建立常态化服务器安全巡检机制，定期核查系统进程、网络连接、登录日志、定时任务等关键内容。依托公开MD5特征，排查XMRig矿机、IRC僵尸客户端、mixscan扫描脚本等恶意样本，及时发现暴力破解入侵、设备感染等风险并快速处置。

五、相关IoC

MD5：

72CB9221703EA28E3289E85724EDAF19

CDB61FE8B0142ABDD4C140B3FF81FEC8

1DE52B717A779D7397BE3083BE575D5E

57285B61386A2FC2BF84B271BEE8D468

95B18DD045F9407E8085A57CB95919F2

IP：

68.183.137[.]83

51.79.74[.]212

168.235.95[.]104

185.106.120[.]99

DOMAIN：

scanbot[.]me

cc.systemctl[.]cc

systems.cmd[.]systems

cmd.sshd[.]services

cmd.systemctl[.]cc

cmd.botnet[.]vip

cmd.torservices[.]download

cmd.scanbot[.]me

cmd.do-dear[.]com

services.sshd[.]services

URL :

[http\[:\]//scanbot.me/pwn/mixscan](http://scanbot.me/pwn/mixscan)

[http\[:\]//scanbot.me/?gbot=x86_64](http://scanbot.me/?gbot=x86_64)

[http\[:\]//scanbot.me/?gbot=aarch64](http://scanbot.me/?gbot=aarch64)

[http\[:\]//scanbot.me/?grig=x86_64](http://scanbot.me/?grig=x86_64)

[http\[:\]//scanbot.me/?gvc](http://scanbot.me/?gvc)

[http\[:\]//scanbot.me/miners/myxmrig.tgz](http://scanbot.me/miners/myxmrig.tgz)

[http\[:\]//scanbot.me/shell/rev.sh](http://scanbot.me/shell/rev.sh)

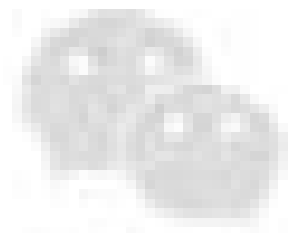
[http\[:\]//cc.systemctl.cc/?gbot=x86_64](http://cc.systemctl.cc/?gbot=x86_64)

[http\[:\]//cc.systemctl.cc/?gbot=aarch64](http://cc.systemctl.cc/?gbot=aarch64)

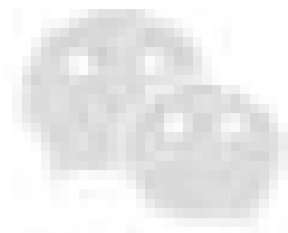
[https\[:\]//cc.systemctl.cc/?gbot=armv7l](https://cc.systemctl.cc/?gbot=armv7l)

[http\[:\]//cc.systemctl.cc/?grig=x86_64](http://cc.systemctl.cc/?grig=x86_64)

[http\[:\]//cc.systemctl.cc/?gvc](http://cc.systemctl.cc/?gvc)



此图片来自微信公众平台
未经允许不可引用



此图片来自微信公众平台
未经允许不可引用