

Rocke : 来自中国的门罗币挖矿冠军

[angel010](#) / 2018-09-04 00:46:32 / 浏览数 4374 [技术文章](#) [技术文章 顶\(0\) 踩\(0\)](#)

本文翻译自：

<https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners.html>

思科Talos团队有很多关于加密货币挖矿恶意软件分析和企业如何进行防护的文章。本文分析中国的攻击单元Rocke的加密货币挖矿活动。

Rocke使用不同的工具集来传播和执行加密货币挖矿恶意软件，包括Git、HttpFileServers (HFS)、以及shell脚本、JavaScript后门、以及ELF、PE挖矿机在内的不同的payload。

早期活动

2018年4月，研究人员发现Rocke使用中文和英文的Git库将恶意软件传播到含有Apache Struts漏洞的蜜罐系统中。恶意软件会从中文仓库站点gitee.com（用户名为c-999）下载许多文件到Struts2蜜罐中。随后，Gitee用户页变为c-888。同时，研究人员发现从

而且Gitee和GitLab的仓库是相同的，所有的仓库都有一个含有16个文件名为ss的文件夹。这些文件包括ELF可执行文件、shell脚本、可执行动作的文本文件，文本文件可

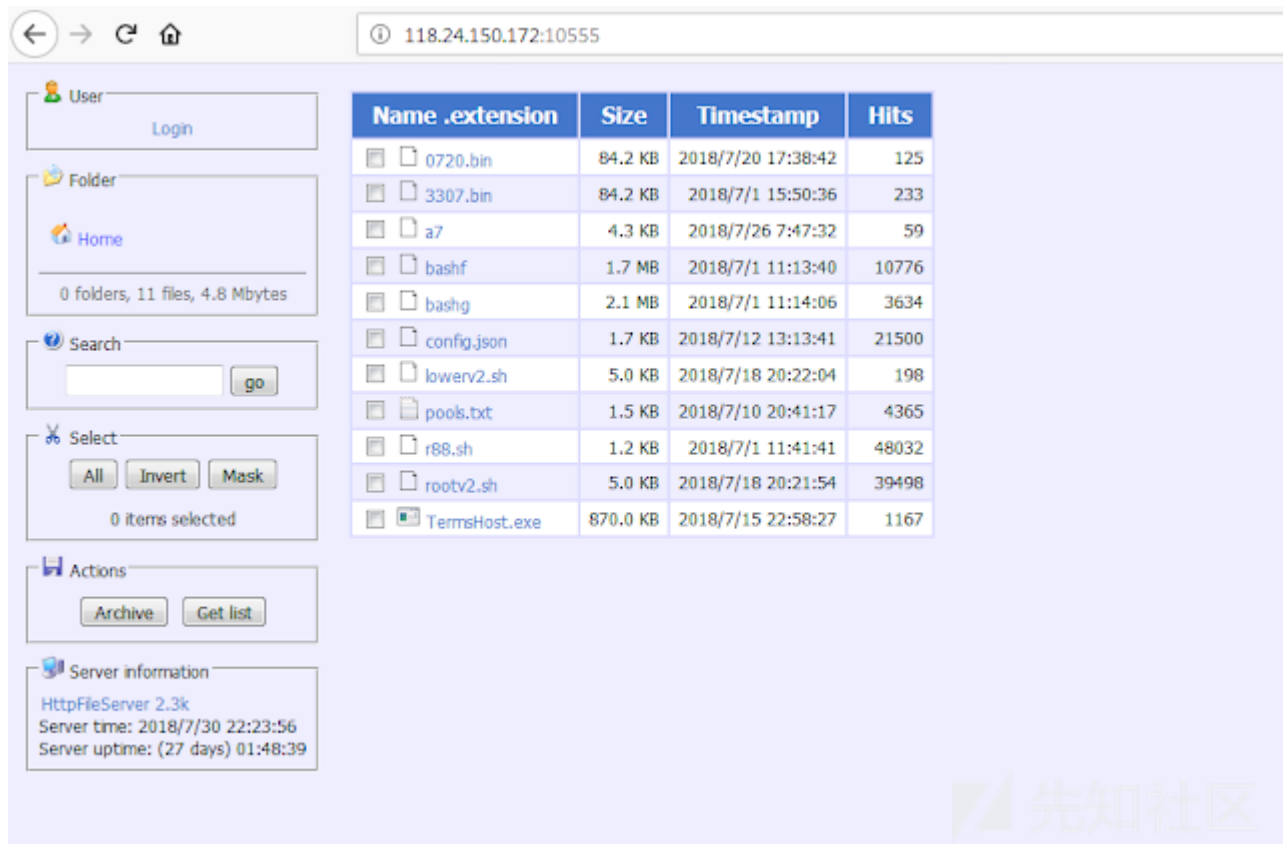
一旦威胁单元入侵一个系统，就会安装一个从3389[.]space下载和执行logo.jpg文件的定时任务来达到驻留的目的。logo.jpg文件实际上是一个shell脚本，会从威胁单元的C

虽然研究人员最早发现其利用的是Apache Struts的漏洞，之后研究人员还发现该威胁单元利用了Oracle WebLogic服务器漏洞（CVE-2017-10271）和Adobe ColdFusion平台的关键Java反序列化漏洞（CVE-2017-3066）。

近期活动

7月底，研究人员发现该组织又参与了另一起类似的活动。通过对这起新攻击活动的调查分析，研究人员发现了关于该威胁单元的更多情况。

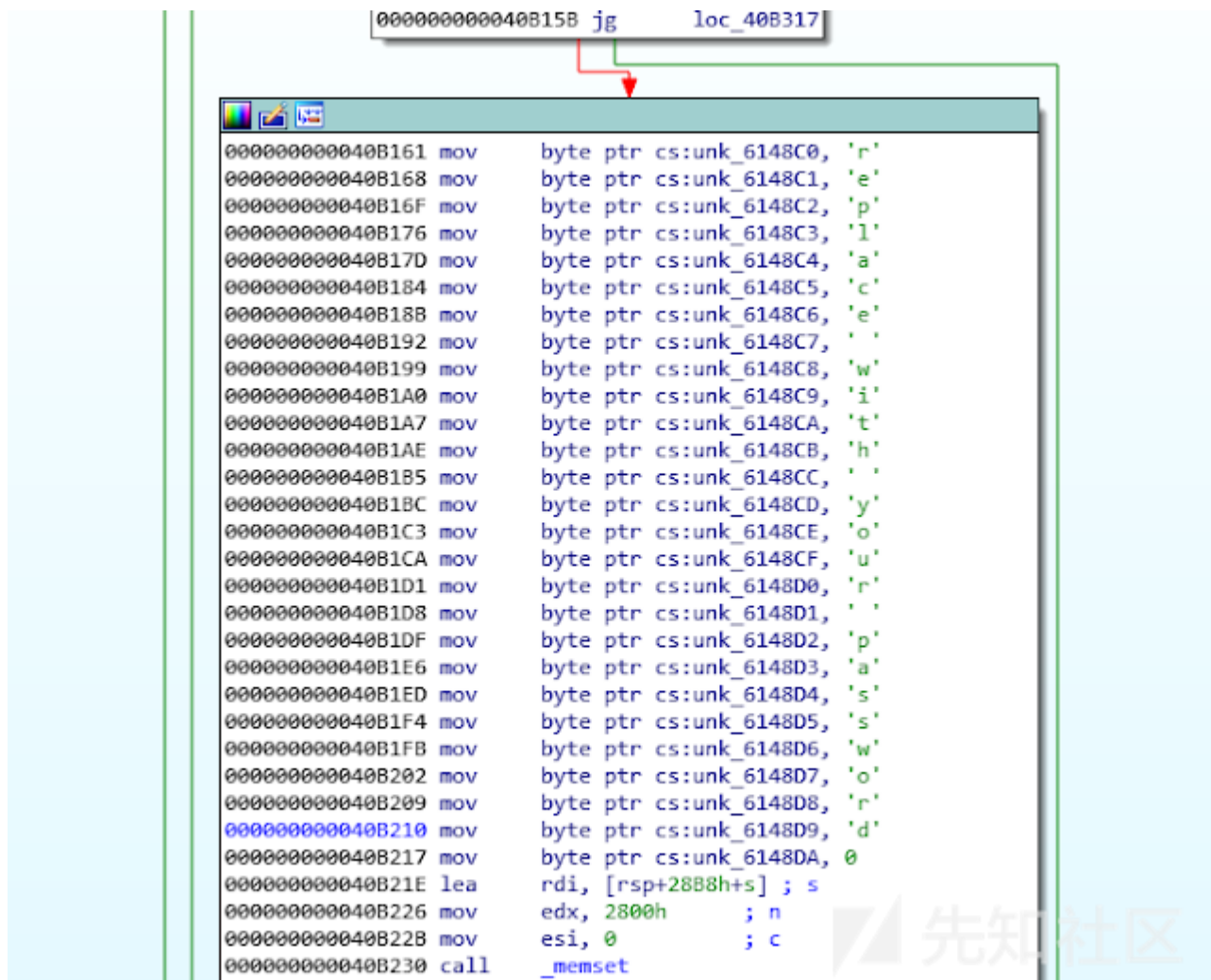
研究人员发现一个Struts2蜜罐的wget请求的是位于118[.]24[.]150[.]172:10555的0720.bin文件。研究人员访问该IP发现这是一个开放HFS，保存的文件有0720.bin、3307



HFS系统截图

研究人员2018年5月就发现该IP扫描过TCP 7001端口，这可能是在扫描Oracle WebLogic服务器，因为Oracle WebLogic服务器的默认端口就是7001。

0720.bin和3307.bin是同样大小（84.19KB）的相同ELF文件，VirusTotal检测该ELF文件是非恶意文件。Morpheus实验室发现了一个连接到相同IP地址的相似文件，如果C Labs发现的那个样本的硬编码密码是相同的，而且偏移量也是相同的。



硬编码的密码

A7是一个shell脚本，可用杀掉与其他加密货币挖矿恶意软件和正常挖矿相关的进程。可用检测和卸载不同种类的国产反病毒软件，并从blog[.]sydwzlj[.]cn (118[.]24[.]150[.]172)的HFS上下载a7之前，该脚本会从known_hosts中寻找IP地址并尝试通过SSH连接并执行。

```
#!/bin/bash
if [ -f /tmp/.a7 ]; then
    exit 101
fi
touch /tmp/.a7
function clean () {
    rm -f /tmp/.a7
}

for f in /var/spool/cron/* /var/spool/cron/crontabs/* /etc/*crontab /etc/cron.d/*; do
    if grep -i -q redis "$f"; then echo > "$f"; fi
done

if [ -f /etc/ld.so.preload ]; then
    mv -f /etc/ld.so.preload /etc/ld.so.pre
fi
chmod -x /etc/xig
chmod -x /root/cranberry /tmp/cranberry /root/yam
chmod -x /etc/root.sh
chmod -x /usr/bin/gpg-agentd
chmod -x /usr/bin/kworker
chmod -x /usr/local/bin/gpg-agentd
killall -9 xig
killall -9 cranberry
killall -9 root.sh
killall -9 gpg-agentd
killall -9 .gpg-agent
killall -9 xmr-stak
killall -9 kworker
killall -9 .gpg
killall -9 pnsan
killall -9 netfs
killall -9 geth
pkill -f stratum
pkill -f nativesvc
pkill -f cryptonight
pkill -f minerd
```

a7源码

Config.json是开源门罗币挖矿机XMRig的挖矿配置文件。配置文件设定的挖矿池是xmr[.]pool[.]MinerGate[.]com:45700，钱包地址为rocke@live.cn。这也是威胁单元Ro
Bashf是XMR-stak的变种，而bashg是XMRig的变种。

Lowerv2.sh和rootv2.sh是两个相同的shell脚本，会尝试下载和执行位于118[.]24[.]150[.]172的挖矿恶意软件组件bashf和bashg。如果shell脚本没有从118[.]24[.]150[.]172
R88.sh是一个shell脚本，会安装定时任务，并且尝试下载lowerv2.sh和rootv2.sh文件。

TermsHost.exe是一个PE32的门罗币挖矿机。根据使用的配置文件可以看出是Monero Silent Miner。该挖矿机的售价为14美元，广告中称该挖矿机可以加入到开始菜单的注册表中，只在空闲时进行挖矿，可以将挖矿机注册到Windows进程中来绕过防火墙。配置文
打包的文件dDNLQrsBUE.ur。该文件看起来与渗透测试软件Cobalt Strike有一些相似之处，攻击者可以用来控制受感染的系统。

恶意软件使用的payload看似与Iron犯罪组织类似。而且Iron和Rocke恶意软件有很多相似之处，而且有系统的基础设施。因此，可以确认payload之间共享了一些代码基础

Rocke

通过Rocke的MinerGate
Monero钱包地址rocke@live.cn，研究人员发现其C2注册的邮箱为jxci@vip.qq.com。而且Freebuf上的用户名rocke关联的邮箱就是jxci@vip.qq.com。

 www.freebuf.com/author/rocke?comment=1



NEW

FB招聘站

分类阅读 ▾

专栏

公开课

HOT

企业服务 ▾

用户服务 ▾



rocke

注册会员 等级：1 级 注册日期：2015年05月12日

个人描述：这家伙太懒了，还未填写个人描述！

先知社区

Rocke注册的网站地址大多位于江西省，一些网站是江西的商业公司，比如belesu[.]com，就是出售婴儿食物的。GitHub也显示Rocke来自江西，而且邮箱中的jx可能也代表

 belesu.com

您好！南昌乐伴食品有限公司欢迎您！



Belesu

贝乐素

——专为中国宝宝研制——

致力于婴幼儿营养辅食

乐伴首页

米粉

清清宝

产品中心

乐伴资讯

先知社区



Overview

Repositories 26

Stars 24

Followers 1

Following 5

Pinned repositories

[XX-net/XX-Net](#)

a web proxy tool

Python

★


 24.5k

🔗

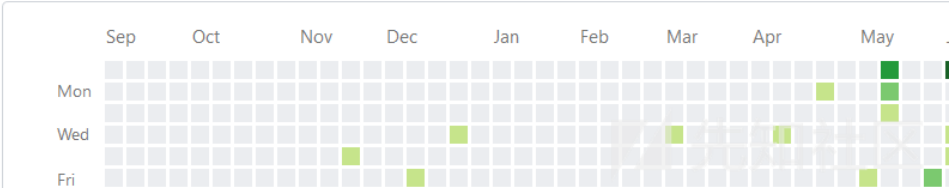
 7k

rocke

Block or report user

 江西师范大学

60 contributions in the last year



GitHub

研究人员还找到一个与Rocke相关的Github主页，主页显示隶属于江西师范大学。其中一个仓库文件夹里有与HFS系统相同的文件，包括shell脚本、钱包信息和挖矿机变种。

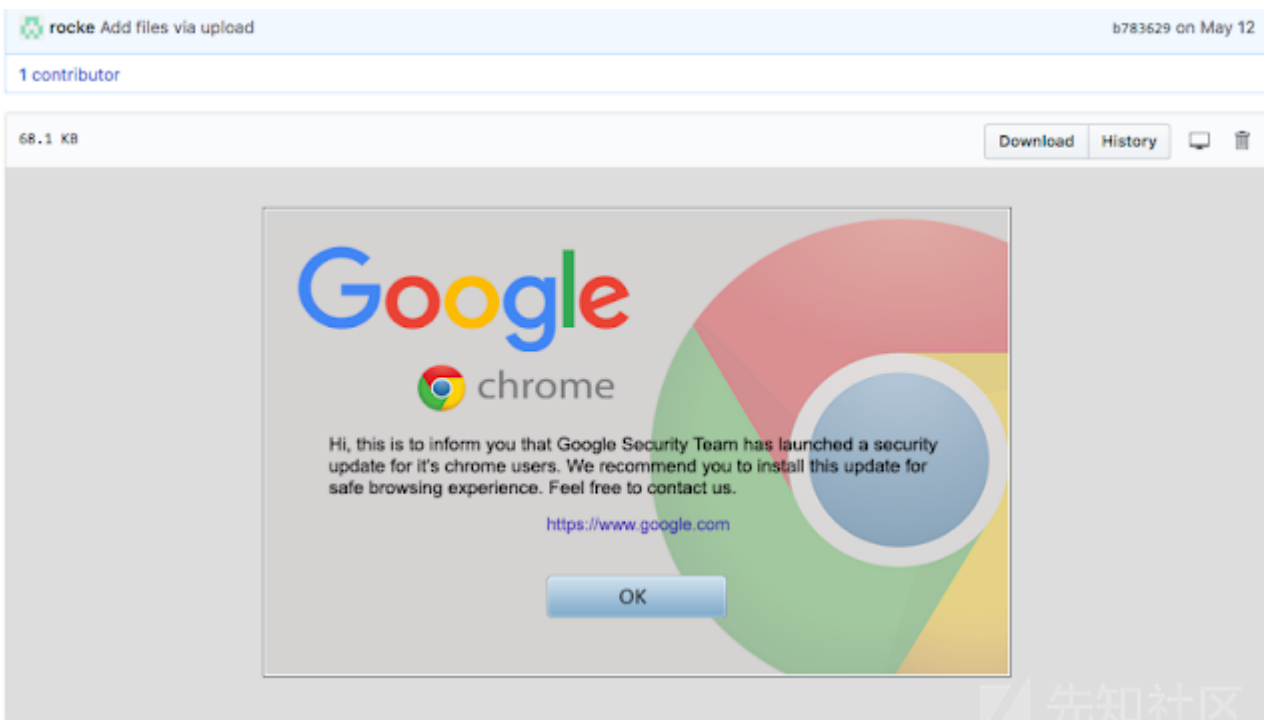
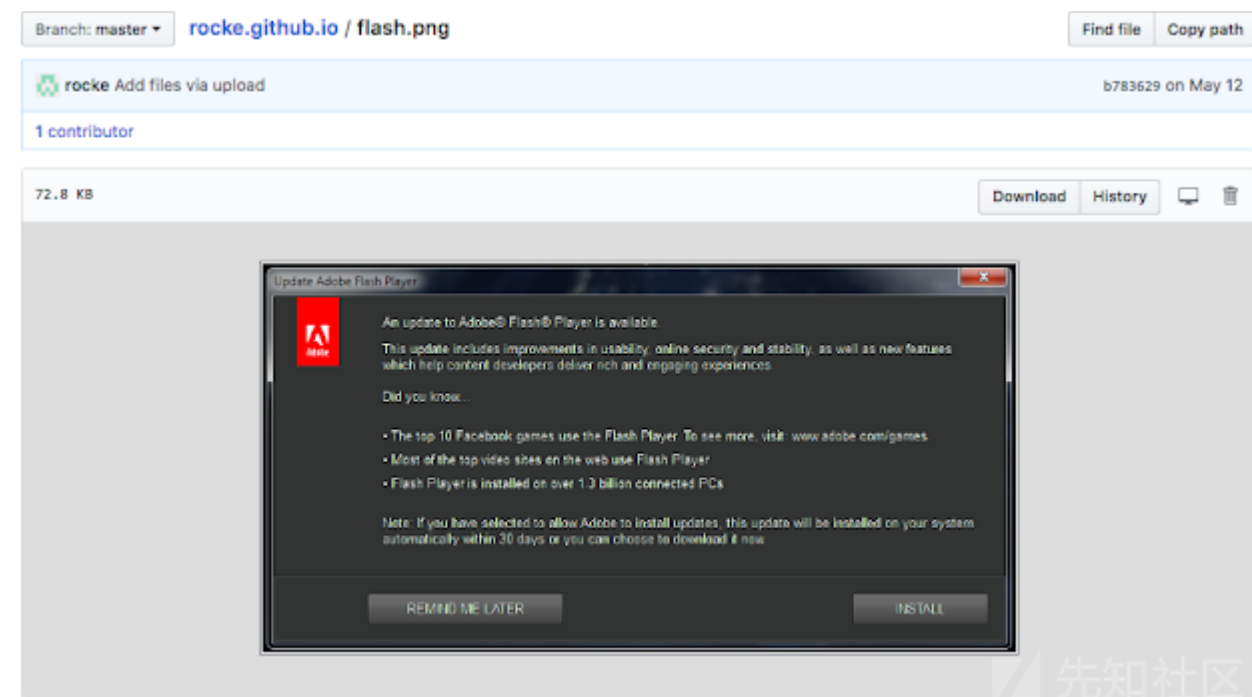
Branch: master | [rocke.github.io / sample /](#) | [Create new file](#) | [Find file](#) | [History](#)

rocke Add files via upload

Latest commit 1294aba on Jun 6

..		
Xshell	Add files via upload	2 months ago
bashd	Add files via upload	3 months ago
bashe	Add files via upload	3 months ago
config.json	Add files via upload	3 months ago
index.html	Create index.html	3 months ago
lowerv2.sh	Add files via upload	3 months ago
pools.txt	Add files via upload	3 months ago
r88.sh	Add files via upload	3 months ago
root.sh	Add files via upload	3 months ago
rootv2.sh	Add files via upload	3 months ago

研究人员通过Rocke的主页找到另一个保存了几乎相同内容但C2不同的仓库。但不能确定该主页是使用者以及使用方式。不同仓库中的文件说明Rocke对通过CryptoNote进行Chrome高警消息、虚假APP、虚假Adobe Flash更新等方式诱使用户下载恶意payload。



仓库中有一个名为commands.js的JS文件，使用隐藏的Iframes来传播位于CloudFront的payload。通过UPX打包的payload的行为与TermsHost.exe释放的文件dNLQrsh

结论

根据过去几个月的分析，Talos研究人员认为rocke会继续利用Git仓库在受害者设备上下载和执行非法加密货币挖矿。Rocke的工具集包括基于浏览器的挖矿机、很难检测的Strike恶意软件等等。除此之外，Rocke还将社会工程作为一个新的感染向量。同时，Rocke的活动说明非法加密货币挖矿活动并没有消亡。

点击收藏 | 0 关注 | 1

[上一篇：从一道线下赛题目看VM类Pwn题目...](#) [下一篇：Bypass Waf 的技巧\(一\)](#)

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](#)