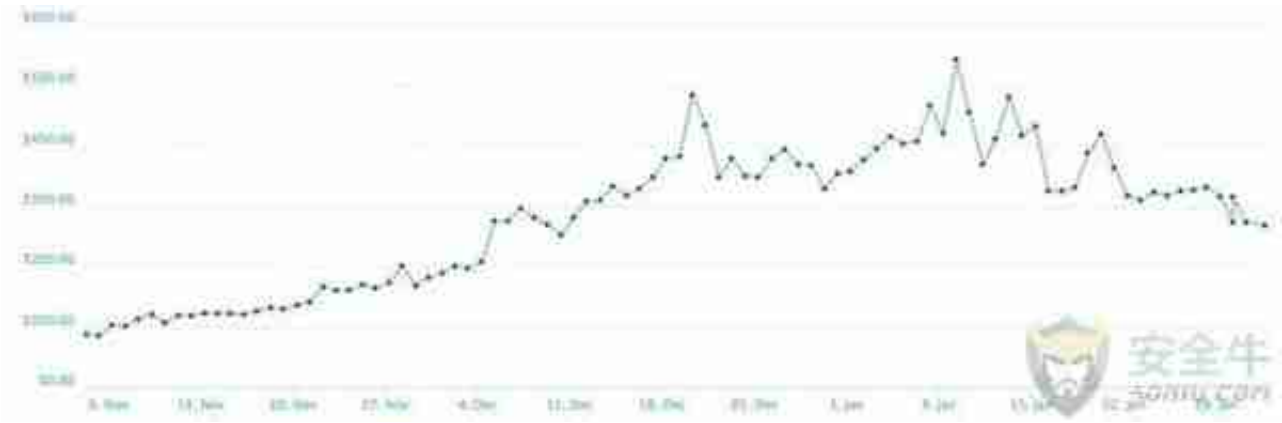


门罗币价格走势图

事件描述

近日，瀚思科技发现黑客利用SSH暴力破解服务器后种植挖矿木马，并且追踪到了其多个后台更新服务器。

黑客攻击服务器与种植挖矿木马过程包括三个步骤：

1. 攻击者探测SSH服务

2. 攻击者对SSH服务账户和密码进行暴力破解

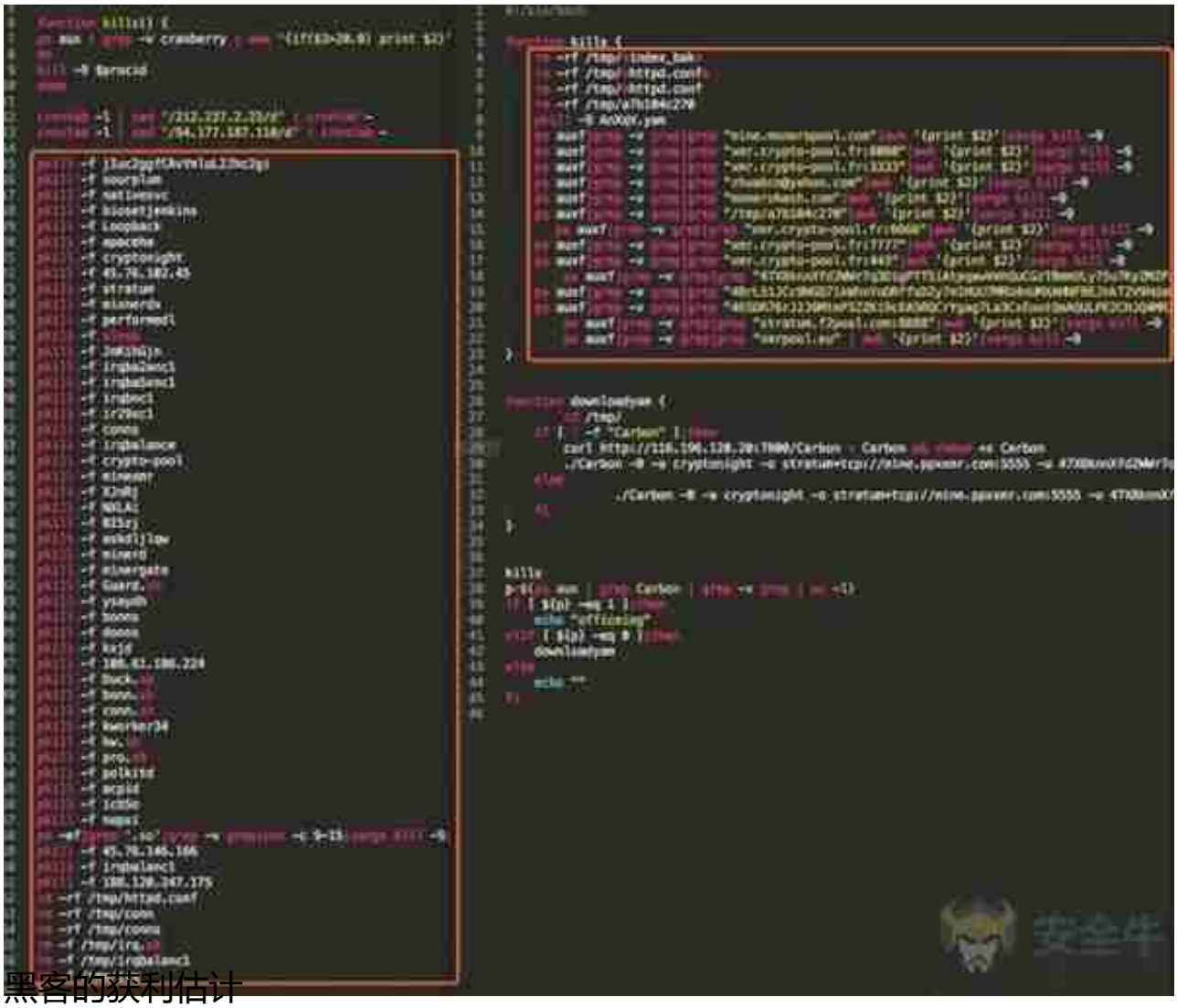
3. 一旦暴力破解成功，攻击者远程下载并运行挖矿程序

下图是一个挖矿木马后台服务器的截图，从图中可以看出116.196.120.20这台服务器从2018年1月26日14点开始，xm.sh(下载器程序)已经被下载过1277次。在对其监控的过程中，发现各个程序也在做频繁的更新。

这段代码包括了三部分：

- 攻击者首先杀掉其他的挖矿程序，来保证自身的收益；
- 远程下载服务器上对应的挖矿程序；
- 配置好矿池以及钱包地址，执行挖矿程序。

3. 文件xmm.sh是更新后的shell程序，与xm.sh相比，修改了矿池链接。目的是选择更高算力的矿池。



黑客的获利估计

从目前的样本获取的钱包地址来看，之前的挖矿币池已经向攻击者的钱包提交了34个XMR（约合8500美元，以当天价格$250计算）。但由于被矿池判定为僵尸网络非法挖矿，该钱包剩余的7个XMR已被冻结：

从目前掌握的情报，综合溯源到的10多台服务器访问信息、钱包地址，该攻击者目

前至少已经控制了3万多台主机，获取了约300多个门罗币，以目前的XMR（门罗币）价格已近10万美元。

挖矿相关IoC：

- IP地址：

116.196.86.246:7800

116.196.120.20:7800

210.76.63.207:3721

182.18.22.71:80

- domain：

dx.777craft.com:7777

钱包地址：

46SDR76rJ2J6MtmP3ZZKi9cEA5RQCrYgag7La3CxEootQeAQULPE2CHJQ4MRZ5wZ1T73Kw6Kx4Lai2dFLAacjerbPzb5Ufg

47X8knnXfd2WWr7q3DigPTTSiAtpqawVmhQuCGzTBmmULy75u7KyZMZPzn1r23oHn3QUJFcwBqp6rbaJAzigr9U5SscpVW8

瀚思威胁情报中心第一时间已更新下发IoC给客户，提供及时的安全检测防护。瀚思大数据安全分析企业版关联分析规则能有效侦测SSH暴力破解,从而在第一时间防护此类攻击的发生。如需瀚思协助检测此类漏洞或者了解瀚思产品防护信息，请直接发邮件至 Contact@HanSight.com。

作者：瀚思科技