Статья Gozi: Малварь с тысячами лиц

В большинстве случаев связь между кампаниями по борьбе с киберпреступностью и разновидностями вредоносного ПО проста. Некоторые штаммы вредоносного ПО, такие как пропавший-но-не-забытый GandCrab, тесно связаны с одним субъектом, который использует вредоносное ПО напрямую или распространяет его через партнерскую программу. Другие штаммы, такие как Quasar RAT с открытым исходным кодом, являются вредоносными программами "общественного достояния"; они оставались неизменными так долго и использовались как часть Lego так часто, что было бы фундаментальной ошибкой пытаться приписать их действующему лицу, кампании, жертве или временным рамкам.

Приятно думать о вредоносном ПО только в вышеуказанных терминах. Затем штаммы вредоносных программ аккуратно сопоставляются с субъектами, о которых нам удобно рассуждать; и любое вредоносное ПО, не привязанное к субъекту, является просто обезличенным инструментом, которое само по себе не несет серьезного багажа, за которым исследователи должны следить.

Увы, в действительности все гораздо сложнее. Некоторые виды вредоносных программ попадают в серую зону. Нет единого субъекта, контролирующего базу вредоносного кода или двоичные файлы, но также нет и повсеместного распространения вредоносного ПО в качестве стандартного инструмента. Нет никого, кто бы делал все возможное, но есть много не связанных между собой людей, каждый из которых делает некоторые из этого ПО, помещая каждую ветвь вредоносной программы в состояние постоянного расходящегося развития. Это странный и вызывающий головную боль мир вредоносных программ, из которых произошла утечка исходного кода, и это касается не только исследователей и аналитиков; возникающая путаница и фрагментация имеют серьезные последствия для конечных пользователей. Исследователь, который в замешательстве машет руками где-нибудь в Китае, через несколько недель может привести к урагану заражения программами-вымогателями в Карибском бассейне, и очень сердитому менеджеру говорят: "Да, мы прикрыли семейство MalBot, но видите ли, этот MalBot не совсем тот MalBot... послушайте, это сложно".

В этой статье мы разберемся с одним из злейших злоумышленников в категории вредоносного ПО с дивергентной эволюцией: Gozi.

2. Краткая генеалогия Гози

Сегодня люди знают, что Gozi - это тяжеловес вредоносного ПО, которое может похвастаться множеством сложных функций, о которых мы подробно расскажем ниже, и очень широким охватом. Только одна разновидность Gozi, Dreambot, в какой-то момент унесла под свою власть 450 000 жертв; при мониторинге другой разновидности, которая сейчас активна, мы можем видеть тысячи новых несчастных жертв в неделю, зарегистрированных на вредоносных панелях C&C. Учтите, что одну жертву можно монетизировать на сумму в сотни долларов, и вы быстро придете к выводу, что в целом Gozi был пугающе прибыльным, даже по сравнению с и без того прибыльным рынком киберпреступности.

Естественно, Gozi не всегда был таким джаггернаутом. Первоначально это был простой банковский троянец - в некоторых аспектах даже более примитивный, чем первая версия ZeuS, из-за заметного отсутствия в нем функций веб-инъекций. Увлекательная статья от PhishLabs (https://info.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak) 2014 года представляет собой интимный взгляд на первые дни Gozi:

> Никита Кузьмин, 25-летний гражданин России [..] работал над кодированием шпионского ПО и троянских программ удаленного доступа (RAT). Он заимствовал исходный код из существующих популярных в то время семейств [..] UrSnif (разработал Алексей Иванов, "subbsta"), а также функции управления ботнетом C2 и внутренний код от Nuclear Grabber [..] Кузьмин тесно сотрудничал с [автор вредоносным ПО] суперзвездами того времени: Corpse, Владислав Хорошорин (BadB), команда Василия Горшкова и Алексея Иванова (Suidroot, Eliga, XTZ, Skylack, Kotenok). Он знал некоторых из них со времен ShadowCrew. Он был моложе большинства своих сверстников и в то время писал, что с нетерпением ждал получения [прав на мотоцикл] и надеялся вскоре заработать достаточно денег на новенький, "настоящий" мотоцикл [..] Несмотря на его молодость ему доверяли, уважали за его практические технические навыки и талант кодинга, а также был известен своим энтузиазмом по поводу того, что интернет-мошенничество, особенно против западных целей, было законной профессией с более высокой оплатой и льготами, чем работа на местном компьютере, в магазине программного обеспечения, лаборатории университета и у интернет-провайдера. [..] Кузьмин имел доступ к исходному коду нескольких наборов криминального ПО с частично совпадающими возможностями, каждое из которых делало что-то исключительно умное в одной ключевой области по сравнению с другими. [Он и команда HangUP] создали репозиторий под контролем версий для кодовой базы набора криминального ПО, включающий все эти лучшие функции - это то, что стало известно как Gozi. Команда HangUP была националистической группировкой, которая обычно придерживалась "киберфашизма", разделяла российские и нацистские образы и являлась общей темой ведения финансовой войны против интересов Запада с использованием Интернета для совершения мошенничества.

В первый год Gozi действовал незамеченным; В 2007 году компания SecureWorks (https://www.secureworks.com/research/gozi) разоблачила этот штамм вредоносного ПО с кратким описанием его внутреннего состава и формы лежащей в основе финансовой операции. Изначально Gozi - как и Emotet - превратился в многомодульную многоцелевую вредоносную платформу, и многие современные производные от оригинальной работы Кузьмина по-прежнему активно используются во вредоносных кампаниях по состоянию на 2020 год. Это 14 лет активности - в несколько раз больше, чем средний срок жизни вредоносного ПО.

Это не совпадение. По всей вероятности, долголетие Gozi можно проследить до одного несчастного случая.

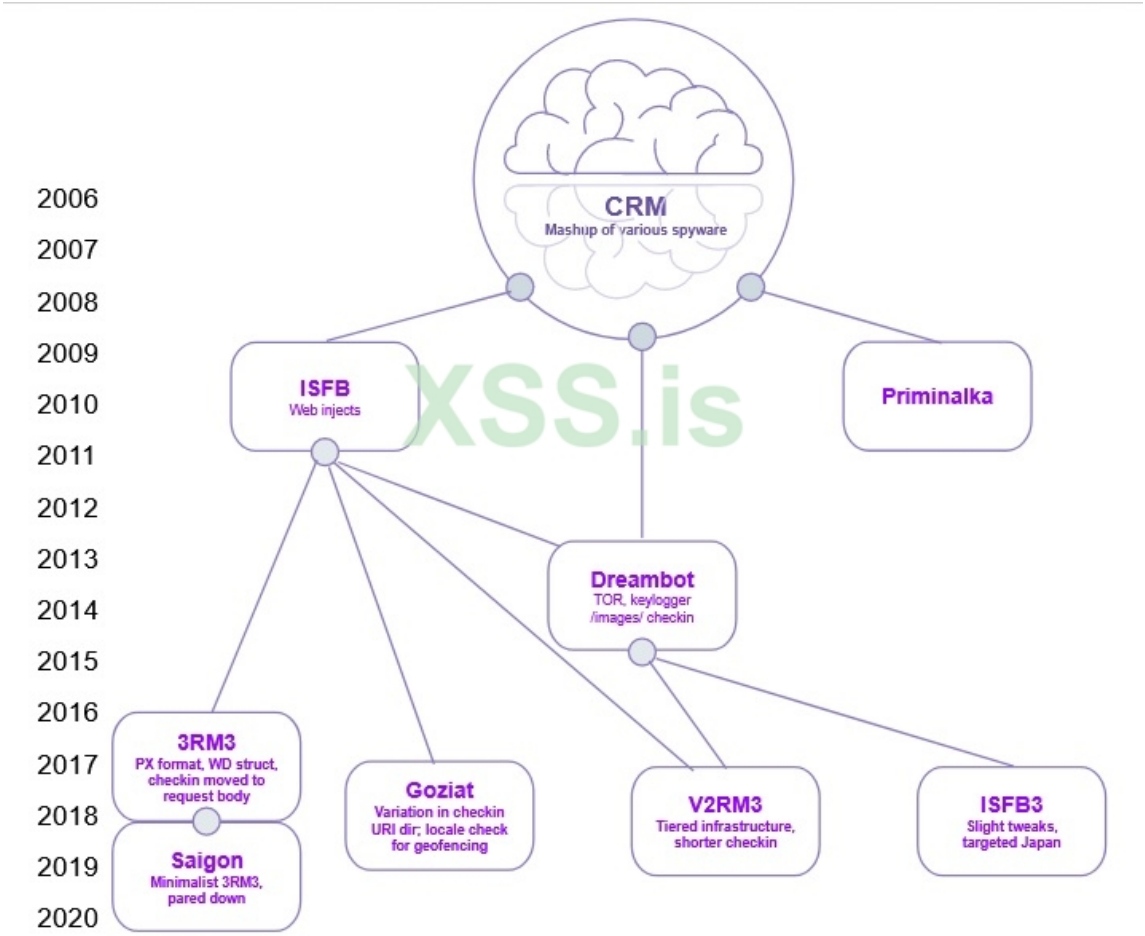
Еще три года после публичного дебюта в 2007 году Gozi представляла собой классическую вредоносную кампанию - единую кодовую базу, предназначенную для плотно закрытой группы киберпреступников. Затем, в 2010 году, просочились исходники для этой первой версии Gozi (эта версия называлась Gozi CRM - что означает "Управление взаимоотношениями с клиентами", а именно управление вашими банковскими учетными данными в состоянии, в котором они находятся у киберпреступников). Другие участники взяли код и запустили его, создав две новые версии: Gozi Prinimalka (которая впоследствии (https://securityintelligence.com/pr...ck-the-planned-prinimalka-gozi-trojan-attack/) слилась с Pony и стала Neverquest(https://securityintelligence.com/neverquest-gang-takes-leave-is-it-the-end-of-the-quest/)) и Gozi «ISFB» (смысл которой, очевидно, был утерян во времени). Одни только эти ранние мутации уже подорвали способность отрасли отслеживать Gozi. Один поставщик назвал ISFB "Gozi2"; другие называли его "Ursnif" или "Snifula" в честь той шпионской программы начала 2000-х, код которой заимствован в оригинальной Gozi CRM. Некоторые другие производители стали называть вредоносное ПО "Rovnix" в честь упаковщика, который обычно использовался для обфускации его двоичных файлов.

Мы знаем, что "ISFB" - собственное имя для этой производной от Gozi, поскольку внутренние двоичные строки содержат ссылки на "проект ISFB". Первоначальный акт дублирования вредоносного ПО Ursnif был связан с давней и гордой традицией произвольного именования вредоносных программ, восходящей, по крайней мере, к вирусу Микеланджело 1991 года, названному таким образом наблюдателями, потому что он запускался в определенный день, который случайно был днем рождения этого художника. По сути, в этом нет ничего плохого, но многочисленные прозвища и заблуждения, окружающие зарождающееся генеалогическое древо Gozi, посеяли путаницу и создали трещины в сфере знаний о вредоносном ПО. "Rovnix" и "Snifula", к счастью, вышли из моды в номенклатуре, но "Ursnif" остался. Фактически, оно прижилось настолько хорошо, что даже в 2020 году, спустя полных два десятилетия после публикации оригинального инструмента Иванова, имя Ursnif - артефакт давно минувшей эпохи - все еще часто используется как коллективный синоним современных воплощений Gozi.

Несколько лет спустя произошла утечка исходного кода ISFB. Источники противоречат друг другу относительно точного времени здесь; большинство свидетельств указывает на то, что эта вторая утечка произошла в 2015 году, но некоторые источники утверждают, что она произошла еще в 2013 году (эта путаница может быть связана с существованием нескольких утечек, произошедших некоторое время отдельно друг от друга). Одна из образовавшихся веток была объединена с Nymaim, где она использовалась в качестве основного кода для гибридного потомка двух семейств вредоносных программ, GozNym. Еще одним ответвлением стал Dreambot, который в значительной степени полагался на код из исходной утечки CRM 2010 года, изменил формат регистрации ISFB и добавил поддержку связи C&C по сети TOR. Другой филиал породил множество успешных кампаний, но так и не получил общего названия, что не оставило нам выбора, кроме как назвать его самим - "Goziat", в честь близости его операторов к австрийскому домену верхнего уровня .at

Когда Gozi второй волны существовал достаточно долго, некоторые участники чувствовали, что рынок созрел для новой основной версии, что привело к рождению Goziv3 (загрузчик RM3), ISFB3 и Gozi2RM3 (IAP 2.0). В каждом из них были внесены свои изменения в механизм обфускации вредоносного ПО, поток управления и схему связи C&C. В частности, эти кампании "третьей волны Gozi" отличались новыми функциями, такими как подписанные двоичные файлы, связь по протоколу HTTPS и многоуровневый двухэтапный процесс регистрации клиента (о котором мы подробнее поговорим ниже).

К этому моменту вам должно стать очевидно, что эти люди никогда не удосужились создать надлежащий регулирующий орган для управления именами для различных ветвей Gozi. Учитывая значительную мигрень, которую мы испытали при усвоении всего вышеперечисленного, возможно, это скорее не ошибка, а скорее особенность.



2. Основной опыт Gozi

Мы так подчеркнули расходящуюся эволюцию Gozi, что вы могли ожидать, что каждый вариант будет делать свое дело, а поведение вредоносных программ будет настолько отличаться от одного варианта к другому, что их общее происхождение едва заметно. На самом деле верно и обратное: если вы не знакомы с садом разветвленных штаммов Gozi, довольно легко принять один вариант за другой, особенно при проведении поведенческого анализа методом черного ящика.

Ниже мы перечисляем некоторые особенности поведения, которые характерны для большинства, если не для всех, штаммов гози.

- Строки содержатся в зашифрованном виде в секции .bss двоичного файла. В процессе дешифрования используется строка ключа, которая представляет собой метку времени компиляции в строковом формате (например, 20 апреля 2019 г.).

```
.text:10008398
.text:10008398
.text:10008398 ; Attributes: bp-based frame
.text:10008398
.text:10008398 CsGetKey proc near
.text:10008398
.text:10008398 puTime_0= dword ptr -0Ch
.text:10008398 puTime_1= dword ptr -8
.text:10008398
.text:10008398 push    ebp
.text:10008399 mov     ebp, esp
.text:1000839B sub     esp, 0Ch
.text:1000839E push    esi
.text:1000839F push    edi
.text:100083A0 mov     esi, offset aJun252020 ; "Jun 25 2020"
.text:100083A5 lea     edi, [ebp+puTime_0]
.text:100083A8 movsd
.text:100083A9 movsd
.text:100083AA movsd
.text:100083AB mov     eax, [ebp+puTime_0]
.text:100083AE xor     eax, [ebp+puTime_1]
.text:100083B1 pop     edi
.text:100083B2 pop     esi
.text:100083B3 leave
.text:100083B4 retn
.text:100083B4 CsGetKey endp
.text:100083B4
```


- Атака типа "злоумышленник в браузере" крадет учетные данные жертвы для списка предварительно настроенных веб-сайтов (обычно это банки, но это устанавливается на уровне кампании и не является особенностью вредоносного ПО как такового). В ISFB и его производных были введены веб-инъекции - они модифицируют веб-сайты, добавляя в них поля ввода, которых раньше не было, например, PIN-код банка, чтобы побудить жертву предоставить эту информацию.

- Особый формат регистрации C&C, который отображается либо в заголовке, либо в теле запроса. Типичный пример: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=% x, хотя есть небольшие различия в используемых параметрах и их порядке.

- Продуманная схема, используемая для обфускации регистрации C&C. Это, в частности, является постоянным среди вариантов - мы нигде не видели никаких изменений. Обфускация работает следующим образом:
-- Шифрует регистрацию с помощью встроенного симметричного ключа (более ранние варианты использовали RC6, новые варианты используют Serpent
-- Кодирует с использованием кодировки base64
-- Экранирует символы, отличные от буквенно-цифровых, с помощью символа "_". Например, "+" становится _2B.
-- Случайным образом перемежает результат символами косой черты ("/").

```
CHAR *__stdcall ObfuscateParamStr(const CHAR *SourceStr, int pKey)
{
  CHAR *DestStr; // edi
  char *fake_param; // eax
  char *_fake_param; // ebx
  int SourceStr_len; // eax
  char *NewStr; // eax
  CHAR *_NewStr; // esi
  LPCSTR _DestStr; // esi
  char *__DestStr; // esi
  const CHAR *v11; // [esp+0h] [ebp-10h]
  int fake_param_len; // [esp+Ch] [ebp-4h]

  DestStr = 0;
  fake_param = GenScriptLine(v11);
  _fake_param = fake_param;
  if ( fake_param )
  {
    fake_param_len = lstrlenA(fake_param);
    SourceStr_len = lstrlenA(SourceStr);
    NewStr = ig_heapAlloc(fake_param_len + SourceStr_len + 1);
    _NewStr = NewStr;
    if ( NewStr )
    {
      strcpy(NewStr, _fake_param);
      lstrcatA(_NewStr, SourceStr);
      DestStr = SerpentEncryptStringToB64(_NewStr, pKey);
      ig_HeapFree(_NewStr);
      StrTrimA(DestStr, "\r\n=");
      _DestStr = UnescapeSpecialBytes(DestStr);
      if ( _DestStr )
      {
        ig_HeapFree(DestStr);
        DestStr = _DestStr;
      }
      __DestStr = PutRandomSlashes(DestStr);
```


- Разделение на уровне процессов между вредоносным модулем, который выполняет атаку "злоумышленник в браузере", и модулем, который принимает фактические решения о том, что вводить и куда, где последний вводится в explorer.exe. Эти два процесса взаимодействуют с помощью именованного канала, хотя некоторая информация о времени выполнения вредоносного ПО хранится в глобальном доступе в реестре (например, значение CRC последнего списка задач, полученного от C&C сервера).

- Широкий спектр стандартных функций кражи информации, таких как ведение журнала ключей, электронная почта, учетные записи ftp, получение данных IM и получение сертификатов, а также захват видео с экрана. Они дополнены поддержкой дополнительных подключаемых модулей формата DLL, которые C&C-сервер может дать указание зараженной машине загрузить и запустить во время выполнения.

- Использование довольно громоздкого формата, называемого "объединенные ресурсы", для различного рода жестко закодированной информации. Тип жестко запрограммированной информации также не записывается на простом английском языке и обозначается тегом CRC32. Известно, что они различаются.

- В вариантах используются одни и те же элементы и один и тот же формат для хранения веб-инъекций.

CRC32 TAG	Readable Name
0x556aed8f	server
0xea9ea760	bootstrap
0xacf9fc81	screenshot
0x602c2c26	keyloglist
0x656b798a	botnet
0xacc79a02	knockertimeout
0x955879a6	sendtimeout
0x31277bd5	tasktimeout
0x18a632bb	configfailtimeout
0xd7a003c9	configtimeout
0x4fa8693e	key
0xd0665bf6	domains
0x75e6145c	domains
0x6de85128	bctimeout
0xefc574ae	dga_seed
0xcd850e68	dga_crc
0x73177345	dga_base_url
0x11271c7f	timer
0x584e5925	timer
0x48295783	timer
0xdf351e24	tor32_dll
0x4b214f54	tor64_dll
0x510f22d2	tor_domains
0xdf2e7488	dga_season
0xc61efa7a	dga_tld
0xec99df2e	ip_service

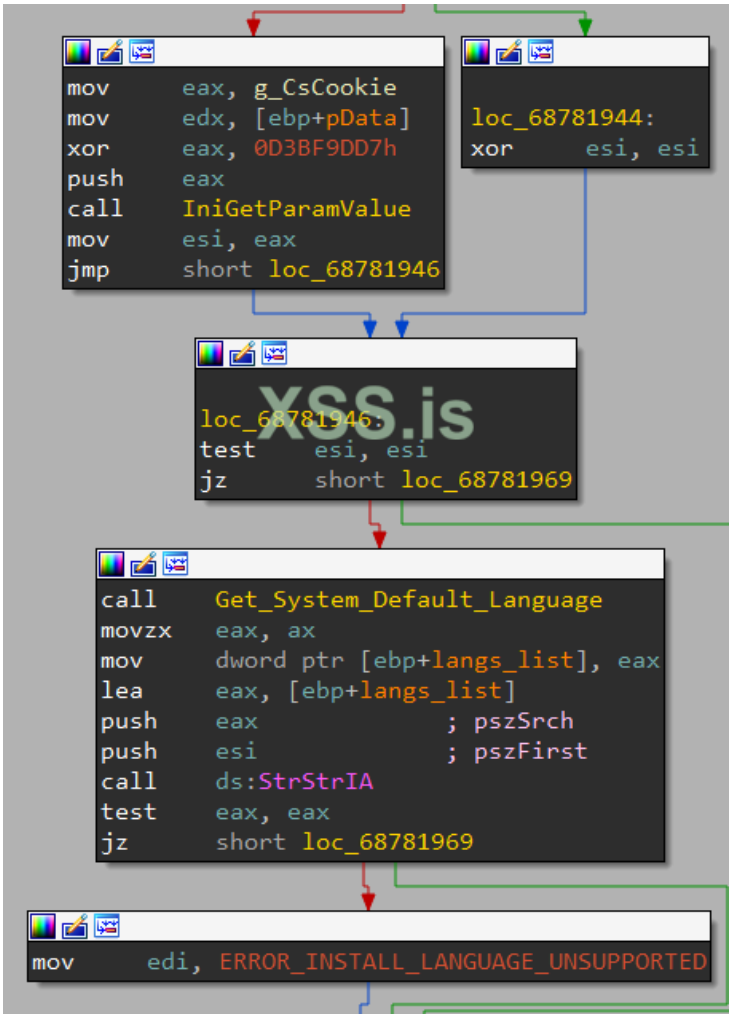
@ID@ -> идентификатор бота (идентификатор хоста жертвы)
@GROUP@ -> group id (идентификатор группы бота)
@RANDSTR@ -> случайная строка
@URL=@ -> целевые финансовые учреждения
@CONFIG=@ -> конфигурация
@VIDEO=@ -> видео для записи, когда жертва посещает интересующую страницу
@SOCKS=@ -> подключить сервер SOCKS
@VNC=@ -> подключить VNC

3. В центре внимания Gozi

3.1 Goziat

Этот Gozi , кажется, дебютировал через несколько лет после утечки ISFB. Его самая отличительная черта по сравнению с другими вариантами - это странность при регистрации C&C; большинство других версий Gozi имитируют HTTP-запрос на получение изображения и поэтому заканчиваются некоторым вариантом /images/, за которым следует длинный и громоздкий BASE64-двоичный объект, завершенный расширением файла .gif или .jpeg. Эта обфускация довольно сложна для решений безопасности, но не невозможна - вероятно, поэтому goziat вместо «образов» использует другой каталог ресурсов, который можно настроить в процессе сборки вредоносного ПО. Так как goziat не заботится о том, что его регистрация является законным запросом на образ, он также отказывается от уловки "расширения файлов обозов как закодированных запросов", популяризируемой Dreambot и копируемой многими другими вариантами. Вместо этого он использует простой формат запроса action = <action>.

Небольшое количество исследователей окрестили этот вариант LOLSnif после его «Living Off the Land» (с использованием предустановленных утилит Windows, таких как mshta.exe и powershell.exe).

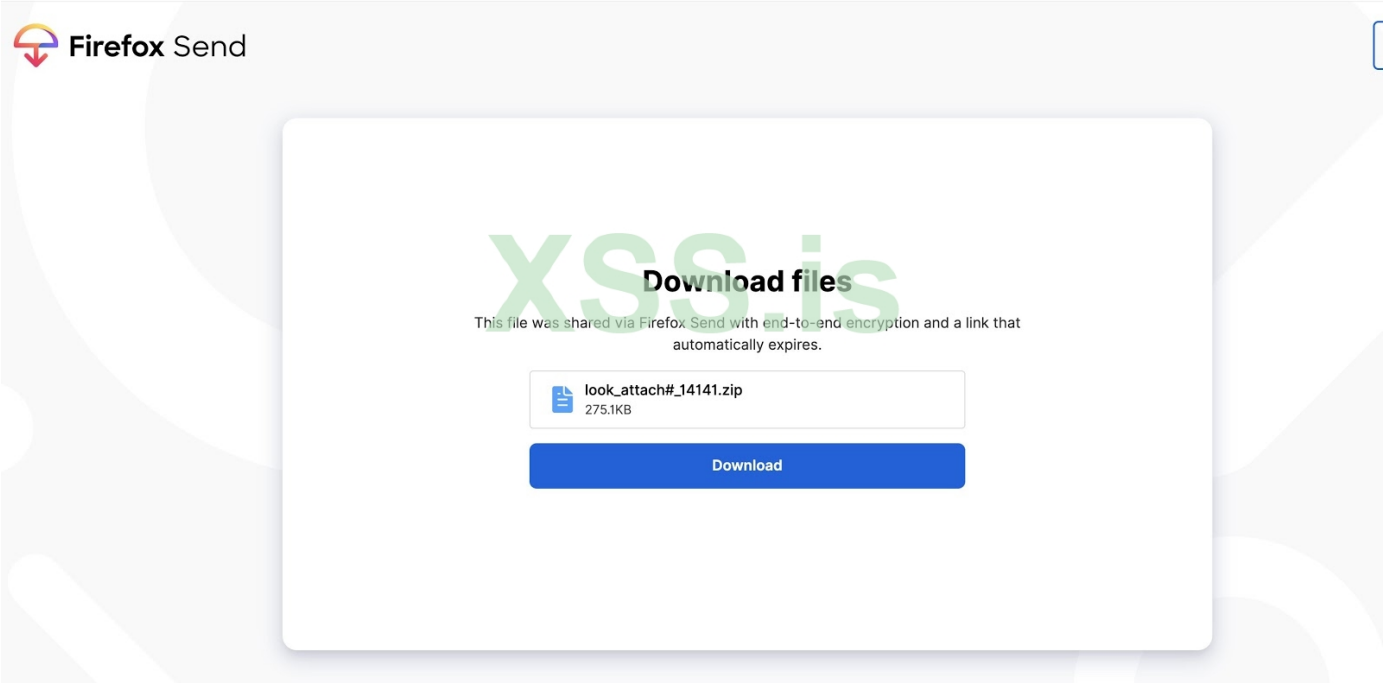


Несмотря на то, что существует несколько различных кампаний, использующих Goziat, они, как правило, используют домены с доменом верхнего уровня .at (отсюда и название, которое мы выбрали для этого варианта). Это, наряду с некоторым перекрытием IP-адресов и даже используемых поддоменов, в совокупности намекает на некоторую общность на уровне операций кампании. Эти кампании, как правило, привязаны к одним и тем же доменам и IP-адресам в течение относительно длительного времени, что может быть не лучшим выбором с точки зрения opsec. В следующей таблице перечислены некоторые кампании, которые мы и другие поставщики смогли отследить, в которых использовалась эта конкретная версия Gozi.

Group ID	Serpent Key(s)	Resource Directory	Target	Domain examples /notes	General Notes

100020003000	W7fx3j0lFvOxT2kFU7yKaYwFde7YtppY	api1	Italy	pipen.at Laurela.atcalag.at	Кампания по рассылке спама, распространяющая защищенные паролем архивы, размещенные на Google Диске, и отправка через firefox. Архивы (обычно с паролем 7777) содержали сильно обфусцированный файл JavaScript с именем presentation _ ????. Js, который, в свою очередь, отбрасывал DLL, запущенную с помощью команды regsvr32.exe -s. Домены первого этапа живут долго
1000	F1cl1tAcbPsStUtM	rpc	USAEurope India Russia	dicin.at kartop.at	По всей видимости, не существует с 2018 года, возможно, раньше. Распространяется вредоносным спамом, а также эксплойт-китом GrandSoft. Определенная общая область предполагает, что участник этой кампании, возможно, также экспериментировал с развертыванием DreamBot для атаки целей в Японии.
1000	K2u7G0lE4u1VoS0V Nf6lU8d5X0i1Wr7V	wpapi	USA Canada Italy	evama.at mobipot.at	Похоже, он взлетел примерно в марте 2018 года.Искусственный спам, очевидно, рассылаемый DHL, используемый для привлечения жертв на целевую страницу Grandsoft Exploit Kit.

20001500	Gwe9HMygngWe8kPKTEJopj7WLDojJKx4	webstore		sorna.at Rivier.atexplik.at	Запущен в конце 2018 года .Выпущено компанией Hancitor, которая перешла на распространение также через тематические электронные письма COVID-19 в начале 2020 года. На основе общих доменов этот объект, похоже, также провел несколько кампаний с использованием загрузчика Hancitor, EvilPony и CobaltStrike.
40005000	Ni8wR0zp1Ak5FoOW Xio4U7r3MlO7FwcQ	wpx	Italy	deepmoler.cn eromov.at	Кажется, началась в 2018 году; распространяется через QuantLoader, набор эксплойтов GrandSoft и вредоносный спам Hancitor.



Помимо доменов, перечисленных выше, каждая кампания также поддерживала домены TOR.

- Api1: 6buzj3jmnvrak4lh.onion, g4xp7aanksu6qgci.onion, l35sr5h5jl7xrh2q.onion
- Rpc: v6ekxns6ldq5uai3.onion, uaoyiluezum43ect.onion, tjiqtwzewnkbqxmh.onion
- Wpapi: 4fsq3wnmms6xqybt.onion, em2eddryi6ptkcnh.onion, nap7zb4gtnzwmxsv.onion, t7yz3cihrrzalznq.onion
- Webstore: vo5vuw5tdkqetax4.onion , zq4aggr2i6hmklgd.onion
- Wpx: pzgxy5elkuywloqc.onion, q7nxkpgras35dwxk.onion, rbhqdxwdwrlp67g6.onion, jesteoq7glp3cpkf.onion

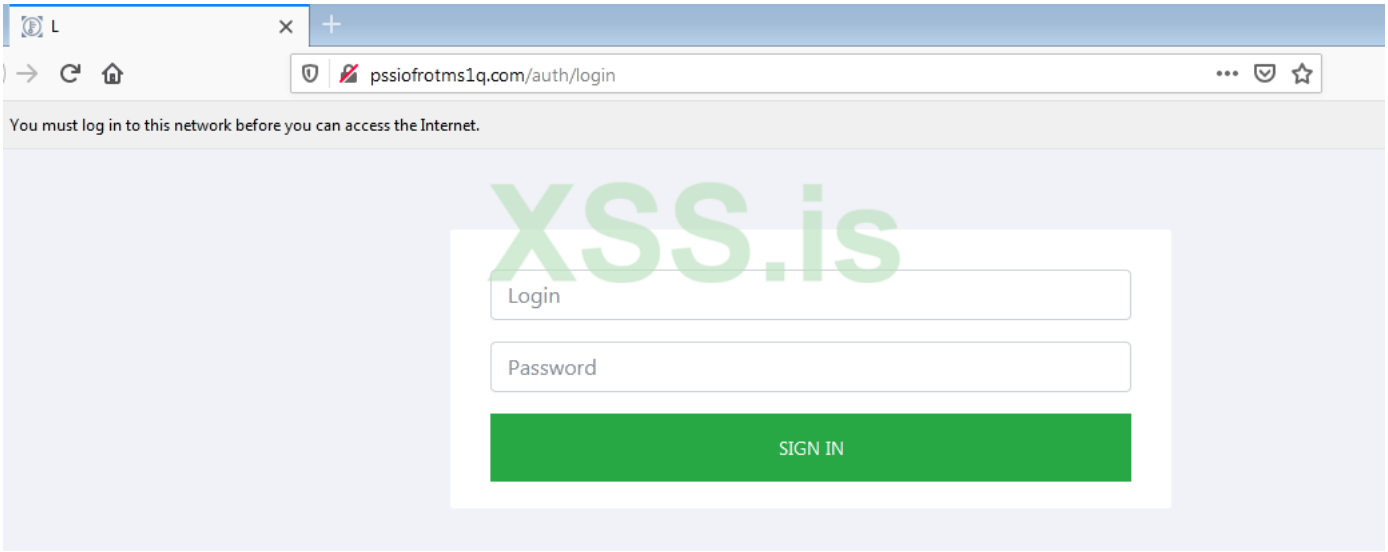
3.2 Gozi2RM3 / Gozi IAP2.0

Эта версия Gozi не содержит никаких настроек связи C&C (в отличие от других Gozi третьей волны, о которых мы поговорим позже); на основе обмена данными и двоичных метаданных, их можно легко принять за другие варианты версии 2. Наиболее существенное различие между Gozi2RM3 и Gozi более раннего поколения заключается на уровне инфраструктуры кампании, которая реализует процесс тщательной проверки.

Инфраструктура C&C кампании Gozi2RM3 подразделяется на 2 этапа, где адрес C&C этапа 1 жестко запрограммирован в исходный двоичный файл, который заражает жертву. На первом этапе C&C предварительно настроен список запрещенных интернет-провайдеров/геолокации, который используется для предварительной фильтрации соединений, подозреваемых в использовании любопытных исследователей, а не настоящих жертв. В некоторых случаях, даже когда эти проверки пройдены, жертва должна доказать, что она хорошая жертва, постоянно отправляя данные; только тогда сервер второго этапа рассмотрит возможность отправки основной полезной нагрузки кампании и отправки истинной конфигурации.

Этот хитрый выбор дизайна - заслуженная запись в нашем списке причин, по которым мы каждый день благодарим Господа за то, что авторы вредоносных программ никогда не учатся на достижениях друг друга. К счастью, существует по крайней мере ключ шифрования по умолчанию для связи с C2 (10291029JSJUYNHG), который многие кампании никогда не удосужились изменить.

Хотя эти различия в инфраструктуре являются основными, есть также некоторые различия в функциональности. Есть панель C&C, которая заставляет нас думать, что этот вариант, вероятно, где-то выставлен на продажу.



Также есть более сжатая строка формата URI (без os, size, hash). Протокол для указания того, какой ресурс запрашивается у C&C, - это протокол «симулирующий запрос на образ», взятый непосредственно из Dreambot.

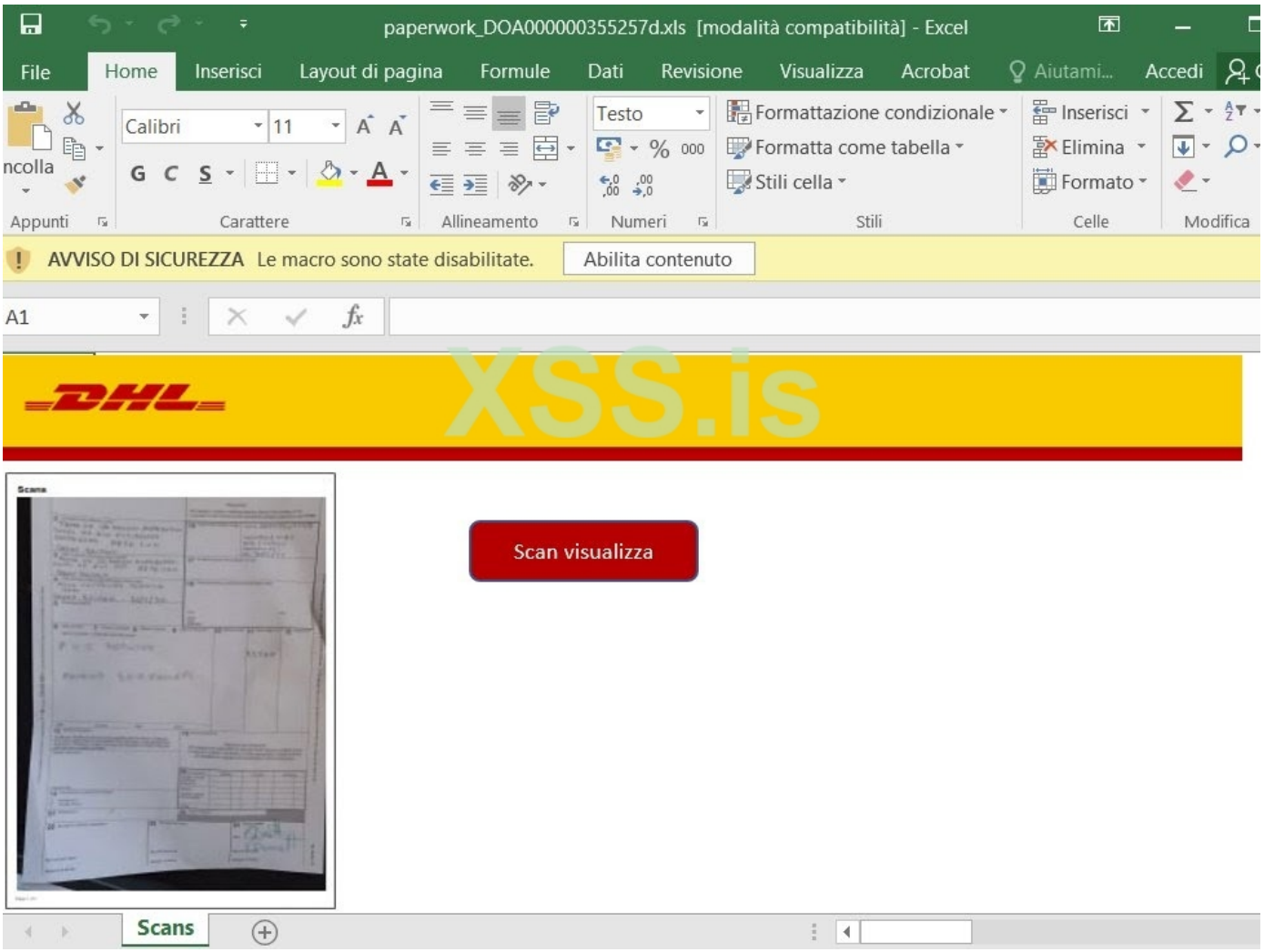
Control Mask	Request Type	Comment
/t*php	get new task	Used until Sep 2015
/c*php	get new config	Used until Sep 2015
/d*php	send stolen data	Used until Sep 2015
/images/*.gif	get new task	current format
/images/*.jpeg	get new config	current format
/images/*.bmp	send stolen data	current format
/images/*/.avi	download 2nd stage dll	not every c&c

Похоже, существует связь между субъектами Goziat и Gozi2RM3. Оба варианта изменили способ расшифровки полезной нагрузки, добавив еще один шаг шифрования - открытый RSA-ключ злонамеренного сервера дополнительно зашифровывается с помощью ключа, который сам собирается только во время выполнения. Тот факт, что оба этих варианта изменили свой поток одинаково и за такой короткий промежуток времени, кажется, означает, что они либо добровольно делятся кодом, либо одна из групп действительно бдительно подражает другой.

В следующей таблице перечислены некоторые из отслеживаемых нами кампаний, в которых использовалась эта конкретная версия Gozi. Это лишь краткий список недавно начавшихся кампаний среди очень длинного списка давно умерших. Некоторые общие черты между кампаниями позволяют предположить, что количество активных участников, использующих Gozi2RM3, может быть меньше, чем кажется на первый взгляд.

Group ID	**Serpent Key(s)**	**Target**	**Domain examples /notes**	**General Notes**
3xxx (varies)	10291029JSJUYNHG	USA Canada Germany, Australia, Italy	TLD of drop site is .cab	Кампания постоянно использовала дропперы первого этапа с именем info_date.doc, распространяемые с использованием перехвата цепочки ответов. Слабое соединение с вредоносным ПО Valak с помощью того же дроппера.
44444343 205x	10291029JSJUYUON 21291029JSJUXMPP	Italy	bizzznez.com Consaltin.orgredflash.org	Распространяется через стандартный вредоносный спам (также замеченный Cutwail), иногда с тематикой COVID-19 или под видом от DHL. Специально ориентирован на кражу учетных данных клиентов итальянских банков.
89897979989893938182	10291029JSJUYNHG	Italy	Sub domains gstat[.] and line[.]	Распространяется через файлы Excel со скрытыми листами. подключен к 3xxx кампании. Наверное, тот же субъект.
5555400040105600	78347829JSDUKLHG	USA Japan	TLD is .today, .website and .space	Распространяется с помощью наборов эксплойтов (RIGEK, GrandSoftEK, FallOutEK), похоже, началось примерно в ноябре 2019 года.

416x		10291029JSJUYNHG	Czech, USA, Italy	*lokoloppo4.com, 38.132.124.193*	Распространяется через спам и документы с макросами. Например, doc выдает себя за Хубату Черноску (большой магазин на чешском языке). Конфигурация веб-инъекции очень похожа на 21291029JSJUXMPP.



В образовательных целях мы включаем конфигурацию перехваченных и скрытых URL-адресов, используемых в одной из кампаний (идентификатор группы 4444, ключ 21291029JSJUXMPP) в приложении B.

3.3 Goziv3 RM3

Этот вариант находится в дикой среде как минимум с лета 2017 года. Группа, стоящая за этим вариантом, довольно сложна и прилагает приличные усилия, чтобы оставаться незамеченной, атакуя в основном Австралию, Италию и США.

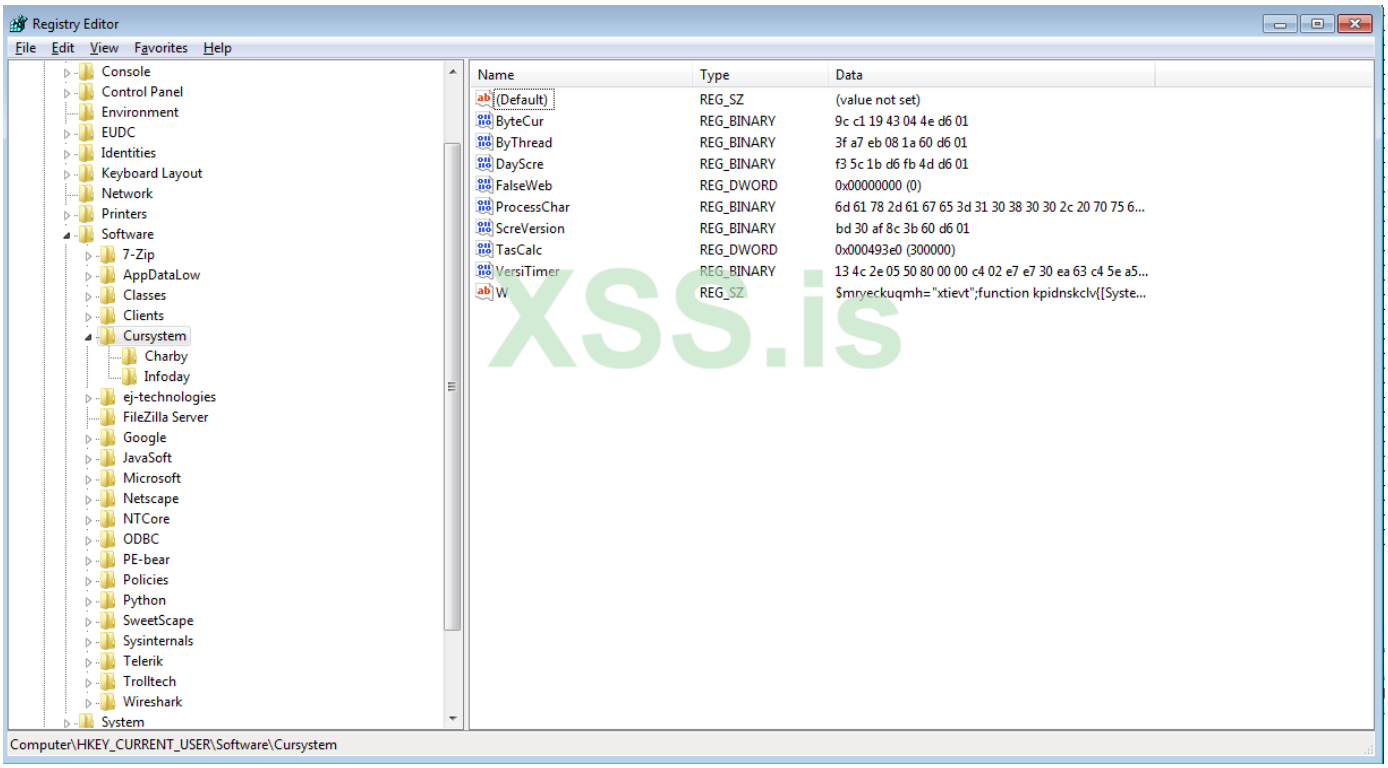
Между этим вариантом и Gozi второй волны есть некоторые существенные технические различия:

- Загрузчик RM3 использует уникальный формат файла, который называется "формат PX". Каждая dll загружается с помощью самодельного загрузчика для этого формата. Инструмент для обработки файлов формата PX можно найти здесь.

- Структура объединенных ресурсов ("JJ") была отклонена в пользу структуры "WD", которая имеет другой формат. Кроме того, структура хранится не сразу после заголовков PE, как раньше, а вместо этого в каталоге безопасности.

```
00000000 WD_struct       struc ; (sizeof=0x18, ma
00000000 size            dd ?
00000004 magic           dw ?
00000006 flags           dw ?
00000008 inner_WD_struct In_WD_Struct ?
00000018 WD_struct       ends
00000018
00000000 ; ---------------------------------------
00000000
00000000 In_WD_Struct    struc ; (sizeof=0x10, ma
00000000
00000000 xor_key         dd ?
00000004 crc32_name      dd ?
00000008 size            dd ?
0000000C addr            dd ?
00000010 In_WD_Struct    ends
```


- В этом варианте используется список слов, который хранится в одной из структур WD для псевдослучайной генерации имен ключей реестра. Это затрудняет обнаружение этого варианта с помощью IOC ключей реестра по сравнению с предыдущими вариантами.



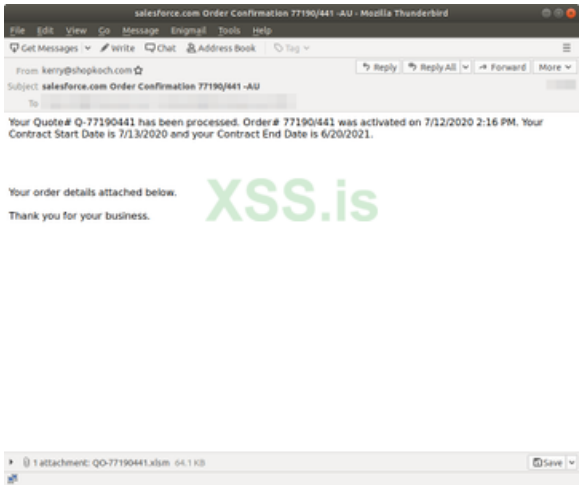
- Этот вариант использует forfiles.exe для выполнения сценария PowerShell, который загружает шелл-код в память, а затем выполняет этот шелл-код с использованием APC-инъекции. Добавляя исполняемый файл forfiles во время цепочки заражения, этот вариант может избежать механизмов обнаружения, которые ищут постоянство более известных механизмов сценариев, таких как PowerShell и mshta.

- Вероятно, разница, которая сначала бросится в глаза аналитику, - это настройка метода общения. Хотя схема обфускации для регистрации C&C остается той же самой, что и глобально используемая в вариантах Gozi, в этом варианте она помещается в тело запроса вместо URI (который становится просто index.htm). Кроме того, обычная регистрация имеет немного другой формат:

> {rand1}={rand2}&type={type}&soft={soft}&version={version}&user={user}&group={group}&id={id}&arc={arc}&crc={crc}&uptime={uptime}

Хотя эти технические различия действительно существуют, как и в случае с Gozi2 RM3, группа, стоящая за этим вариантом, похоже, сосредоточила свои инновации на способах предотвращения взаимодействия исследователей с C2 и получения полезной нагрузки. Они делают это, ограничивая доставку полезной нагрузки на стороне сервера - когда клиенты пытаются подключиться к серверу C2, они проверяют геолокации и отклоняются, если местоположение не соответствует целевому региону текущей кампании. Что еще более важно, первый этап C2 остается в сети в течение очень короткого периода времени - ровно столько, чтобы обслужить большое количество жертв и исчезнуть, прежде чем подвергнуться нежелательному анализу. Gozi3 RM3 обычно распространяется в виде спама, содержащего обфусцированный файл VGS или макрос xls4.0 в качестве вложения. По крайней мере, с 2017 года этот вариант Gozi, как известно, связан с популярным загрузчиком, который также используется в некоторых кампаниях Emotet и Dridex (https://blog.trendmicro.com/trendla...d-bitpaymer-gangs-linked-by-a-similar-loader/).

Доменом верхнего уровня C&C серверов обычно является .xyz, и образцы обычно подписываются Verisign (на практике это означает, что когда жертва запускает эти образцы, она должна нажать "OK" в одном диалоговом окне, которое предупреждает их что, возможно, им не следует запускать случайные файлы, переданные им незнакомцами в Интернете).



Люди, стоящие за этой операцией, похоже, ценят баланс между работой и личной жизнью - кампании несколько далеки от времени и неактивны по выходным. Вы можете прочитать здесь о возможной связи с группой "Evil Corp". Отсутствие различий во всех вышеупомянутых характеристиках, кажется, предполагает, что этот вариант Gozi в основном используется одним субъектом.

4. Наследие Gozi

Это варианты Гози, которые, кажется, вышли из употребления. Группы, которые их продвигают, либо перешли на более современные вредоносные программы, либо полностью отказались от вредоносного ПО.

4.1 Dreambot

Эта ветвь утекших источников ISFB была впервые обнаружена вскоре после утечки ISFB (многие источники говорят, что в 2014 году, некоторые - в 2015 году). Некоторое время он оставался в активной разработке и добавил много новых функций; Наиболее важными среди них были серверы управления и контроля, размещенные в Tor, возможность кейлоггинга, возможность кражи файлов cookie браузера и данных из почтовых клиентов, функция создания снимков экрана, возможность записи экрана жертвы и функция удаленного доступа VNC. У Dreambot как денежная модель Cybercrime-as-a-Service (CaaS), и она была доступна любому начинающему киберпреступнику по разумной цене.

Многие из этих функций были уникальны даже среди более новых вариантов, но в конечном итоге Dreambot был продуктом второй волны эпохи Gozi. Чтобы избежать посторонних взглядов, он полагался на проверки C2, имитирующие GET-запрос изображения - уловка, которая резко потеряла свою ценность, как только стала

общеизвестной, и не могла конкурировать с изощренными передовыми методами скрытных операций третьей волны Gozi, такими как подписанные двоичные файлы и многоуровневая модель C2. После долгой и плодотворной работы в марте 2020 года Dreambot, похоже, наконец замолчал (https://medium.com/csis-techblog/the-end-of-dreambot-a-loved-piece-of-gozi-24cc9bfc8122).

4.2 Saigon

Этот форк Goziv3 RM3 был идентифицирован FireEye (https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html) в сентябре 2019 года. Он внес различные изменения в базовый Goziv3 RM3, в том числе:

- Новые аргументы для регистрации C2. Среди них был заметен стук, который закодировал количество секунд, в течение которых клиент будет ждать между выполнением последующих запросов.

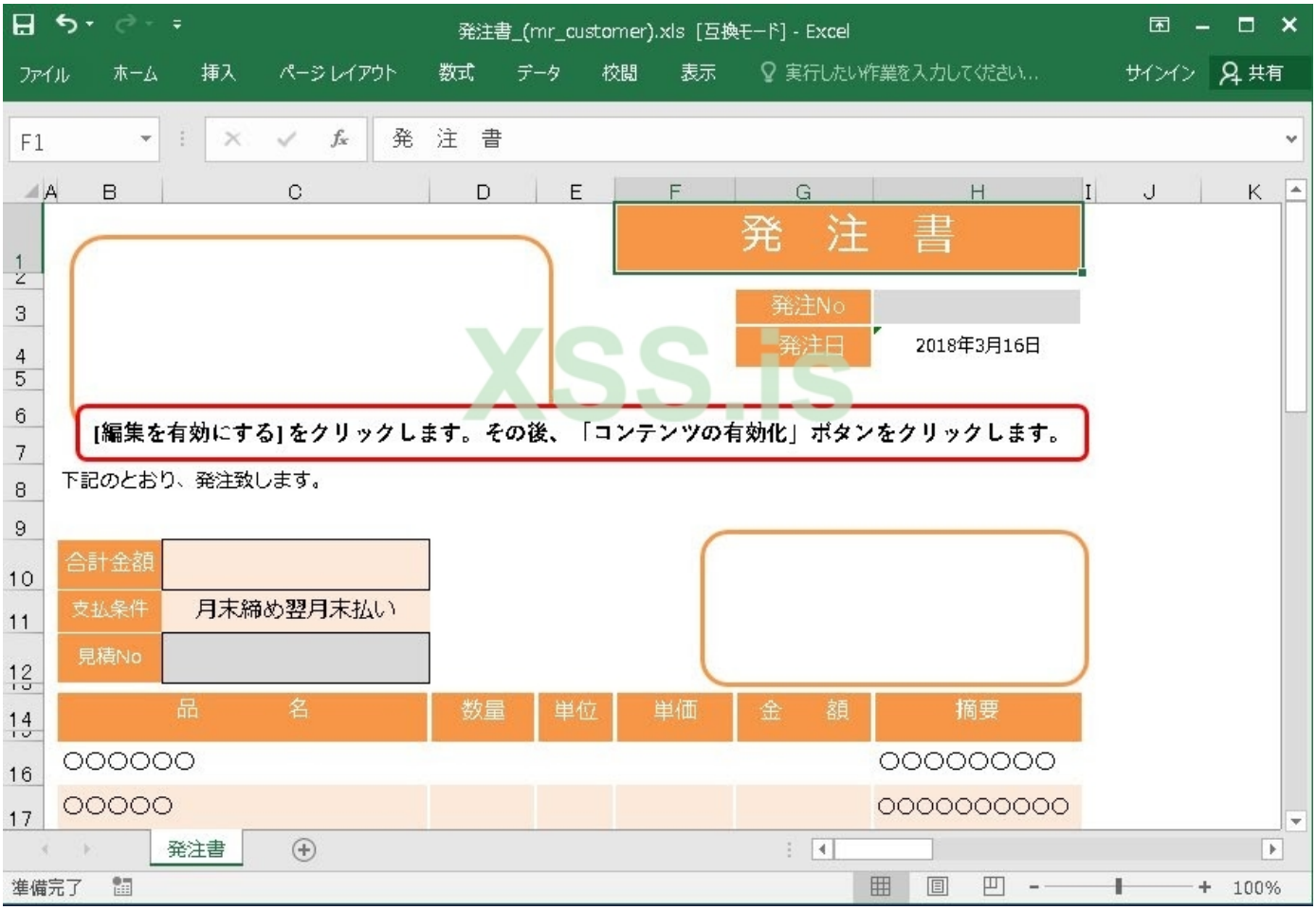
- В режиме работы ECB используется шифрование SERPENT вместо CBC. В реальной криптографии это будет считаться переходом на более раннюю версию, но общее правило состоит в том, что никто никогда не запускает криптоанализ вредоносных программ, и это всего лишь одна прославленная схема обфускации, замененная другой.

- Не используется формат PX.

Как можно видеть, большинство изменений, по-видимому, направлены на удаление функций, упрощение вредоносного ПО и возврат к чему-то более похожему на Gozi второй волны.

4.3 ISFB3 / Ursnif-A

Этот вариант имел очень ограниченное и точное применение, атакуя японских жертв в течение 2018-2019 годов. Из-за общности метода распространения предполагается, что он связан с злоумышленником TA544. Как типично для Gozi в целом, он распространялся с помощью вредоносного спама (в частности, через Cutwail) с прикрепленными офисными документами и использовал геолокацию, чтобы блокировать любые запросы, выходящие за пределы его целей (обычно клиентов местных японских банков). Спам часто содержал загрузчик Bebloh, который только после этого извлекал настоящий Gozi.



Имя "ISFB3" происходит от явного пути к pdb во вредоносных двоичных файлах - c:\isfb3\x64\Release\client.pdb - но, хотя в названии стоит цифра "3", это не Gozi третьей волны. Запрос GET для получения фиктивных образов все еще существует, и отсутствуют какие-либо новаторские функции, препятствующие исследованию кампании. Множество незначительных технических отличий отличают этот вариант от других разновидностей: "J1" используется в качестве магического префикса в объединенных ресурсах (это возврат к ранним версиям Dreambot), некоторые изменения в работе его модулей кражи информации, а также несколько настроек его методов для сохранения и уклонения

5. Вывод

Когда мы имеем дело с вредоносным ПО, мы часто стоим на плечах гигантов. Консенсус производителя быстро сообщит нам название вредоносной программы, с которой мы имеем дело, и если это не так, некоторые Google, ищущие уникальные на первый взгляд индикаторы, быстро покажут нам с трудом добытые идеи исследователей, которые работали до нас и должны были иметь дело с одним и тем же вредоносным ПО. Как только мы узнаем настоящее имя вредоносной программы, мы получаем власть над ней. Мы можем писать сигнатуры, искать больше образцов и использовать наши точные знания для защиты потенциальных жертв.

Предположим, что у вас есть вредоносный образец или кампания, и после небольшого расследования вы определили, что имеете дело с “Gozi”, “ISFB” или “Ursnif”, которые все одинаковы, но каким-то образом разные. Затем вам придется столкнуться со списком вариантов, которые взаимозаменяемо называются этими именами, все с слегка разными методами коммуникации, моделями поведения и инфраструктурой кампании. Что Вы будете делать сейчас? Для базовой работы по сортировке можно сказать: «Это Gozi, банковский троян, который превратился в платформу доставки вредоносного контента». Но для всего, что носит более технический характер, эти тонкие различия - рецепт головной боли. Если ваш прицел - *все* версии Gozi, вам будет очень плохо.

Кажется, нет простого решения этой проблемы. Солнце встает на востоке, море устремляется к берегу, киберпреступники создают новые вредоносные программы, а исследователи придумывают им новые названия. Все, что мы можем сделать, - это производить очень запоздалые обзоры, такие как этот, которые пытаются внести некоторый порядок в всеобъемлющий хаос. Помимо этого, нас может утешать тот факт, что таких случаев, когда вредоносное ПО с несколькими ветками происходит редко, поскольку у киберпреступников нет финансовых мотивов делиться вредоносным кодом. Когда происходит фрагментация в стиле Gozi, обычно это происходит из-за утечки. В заключение мы хотели бы обратиться к киберпреступникам: защитите свои кодовые базы, ради Бога!

Источник: https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
Автор перевода: yashechka
Переведено специально для портала XSS.is (c)