

анализ 15-летней эволюции от 2011 до Node.js

 rt-solar.ru/solar-4rays/blog/6652

January 1, 2001



С конца января 2025 года в инфраструктуре заказчика фиксировалась устойчивая автоматизированная активность, связанная с обращениями к российским онлайн-сервисам. По характеру запросов она выглядела не как набор разрозненных действий, а как работа распределенной бот-инфраструктуры: сценарии повторялись, источники ротировались, а сами запросы со временем становились все менее отличимыми от действий реального пользователя.

В ходе расследования удалось установить, что значительная часть задействованных адресов взаимодействует с инфраструктурой ботнета ProхуСВ, ориентированного на использование зараженных узлов в качестве прокси. Дальнейший анализ показал, что речь идет не об отдельном вредоносном образце, а о полноценной системе с клиентским ботом, выделенными каналами управления и передачи данных, веб-панелью и серверным ядром PCBServer 7.

Эта же инфраструктура использовалась и при обращениях к другим популярным ресурсам в РФ, включая почтовые платформы, маркетплейсы, социальные сети, телеком- и игровые сервисы. Это показало, что ProхуСВ применялся не под один частный сценарий, а как универсальная сеть управляемых прокси-узлов для распределенных операций.

Особый интерес представляет не только сам бот, но и зрелость всей инфраструктуры. Устойчивый бинарный протокол обмена, механизмы централизованного администрирования, элементы многолетней инфраструктуры распространения и возможные пересечения с артефактами, связанными с TeamSpy, позволяют

рассматривать ProxyCV как длительно развивающийся инструмент, адаптированный под практическую эксплуатацию в реальных атаках.

Инцидент у заказчика

Первый пик активности был замечен 29 января 2025 года. На графике показано количество срабатываний аномалии:



График количества срабатываний аномалии

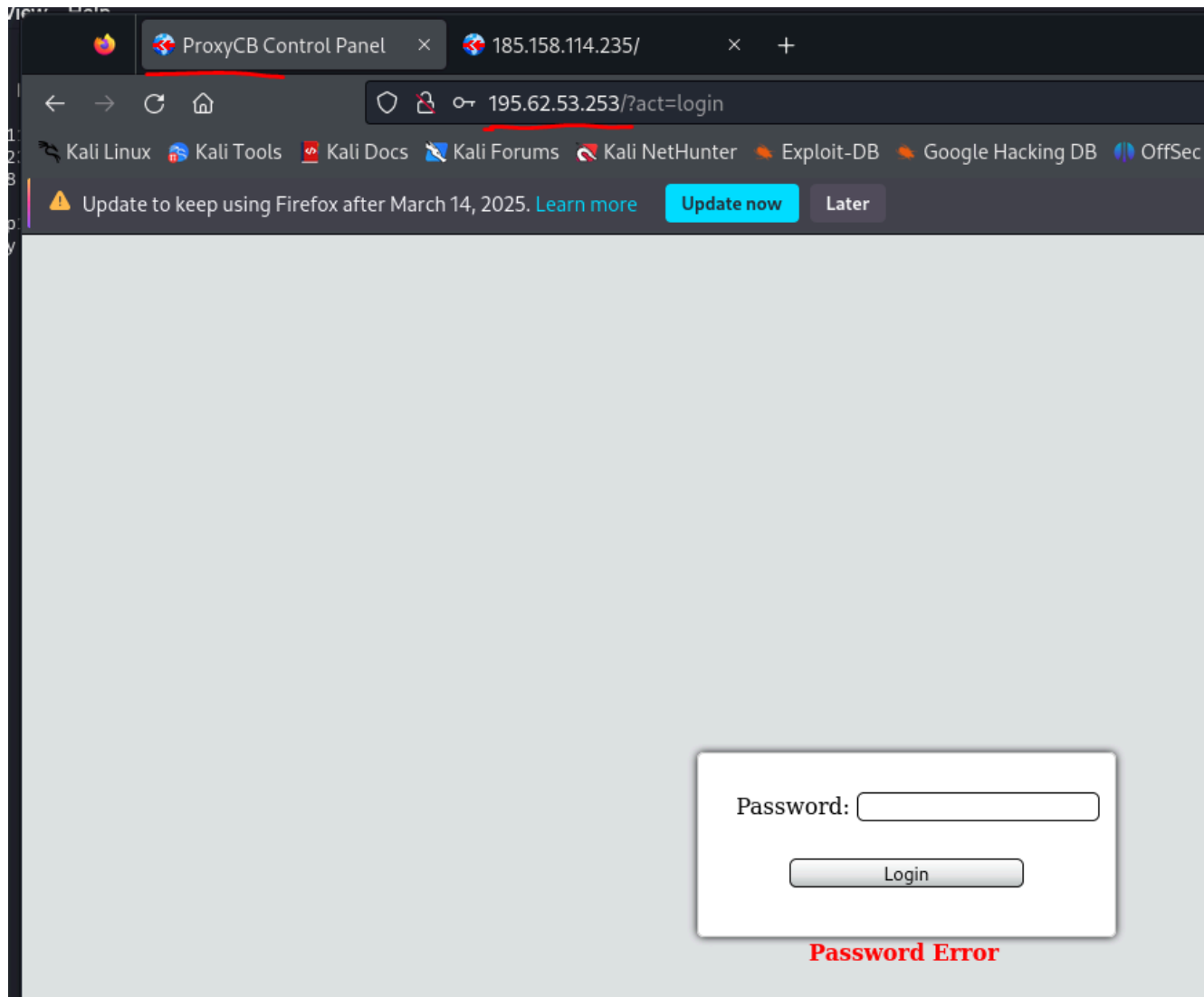
В части запросов используется меньшее количество cookie, чем передает обычный пользователь, некоторые заголовки написаны некорректно и дублируются, также в ответах капчи периодически используется нечитаемый Unicode вперемешку с обычной кодировкой. Например:

```
{"answer": "2\u0428\u04266\u0416", "captchaType": "captcha"}
```

Позже стали попадаться ошибки XEvil (программа для автоматизации прохождения капчи), встречались они только с адресов, проверяющих аккаунты:

```
{"answer": "XEVI+ERROR:+No+handler+for+request+http://rucaptcha.com/in.php",  
"captchaType": "captcha"}
```

В результате анализа сетевых логов одного из участвующих в активности адресов было установлено, что он часто обращается на 195[.]62.53.253 по TCP-портам 1002, 1001. На портах 80 и 443 этого адреса доступна панель авторизации ProxyCV:



Панель авторизации ProxyCB

Общая характеристика ProxyCB

ProxyCB представляет собой ботнет с централизованным управлением зараженными узлами, используемыми в качестве прокси. Его архитектура включает клиентскую часть, управляющий канал на порту 1001, рабочий канал на порту 1002, веб-панель администрирования на 80/443 и серверное ядро PCBServer 7, использующее отдельный административный протокол. Такое разделение говорит о том, что операторы построили не просто канал связи с ботами, а полноценный контур управления инфраструктурой.

На стороне зараженного узла бот формирует идентификатор, предотвращает повторный запуск, устанавливает соединение с C2 и далее работает через отдельные потоки для управляющей и рабочей логики. На стороне сервера доступен интерфейс мониторинга, группировки узлов, настройки конфигурации, ограничения доступа и административных команд. При этом веб-часть выступает скорее оболочкой, тогда как основные механизмы управления скрыты в серверном ядре и бинарном протоколе.

Хронология ботов

Собранные образцы позволяют проследить длительную эволюцию ProхуСВ не столько на уровне самой полезной нагрузки, сколько на уровне упаковки и способов доставки. По имеющимся файлам видно, что прокси-модуль в разных поколениях сохранял общую логику работы, тогда как дропперы, домены управления и технические детали реализации постепенно менялись.

На ранних этапах, судя по временным меткам и встреченным доменам C2, использовались другие серверные адреса, в том числе gogogobaby12[.]com, govenmahen[.]com и grabsfakus[.]com. Более поздние образцы уже связываются с доменами вроде kilo-torrent[.]org и соответствующей серверной частью ProхуСВ. При этом по конечной нагрузке речь идет о том же семействе, поскольку менялись не базовые функции прокси-узла, а способы его доставки, маскировки и отдельные технические детали реализации (PE, DLL или, в наиболее свежих вариантах, Node.js).

Начало

Один из первых найденных образцов ProхуСВ датируется 2011 годом и ориентирован на Windows XP. Мимикрирует он под программу «Знакомство с Windows», которая намеренно завершается ошибкой.

File name	tourstart.exe
MD5	88c96f23ed708f019404f35344206db1
SHA1	ea9413811d93eb47e31fb0fe2559a184834bd131
SHA256	724dabf7e59c1ae2f47d27b20bdf28fc278a8416431d342d12b676b95845910f
File type	PE32 executable
File size	67.00 KB
Compilation timestamp	2005-05-30 19:01:12 UTC (дата компиляции распакованного файла — 2011-11-21 13:44:22)

Анализ образца показал, что файл представляет собой многоступенчатый дроппер, использующий UPX-подобную упаковку. Несмотря на наличие сигнатур UPX, штатная распаковка утилитой UPX не срабатывает.

После распаковки образец создает DLL в каталоге system32, имя которой формируется на основе имени пользователя, и запускает ее через rundll32.exe. В случае ошибки может сам подгрузить созданную DLL и вызывать EntryPoint с вредоносным кодом. Дополнительно реализовано закрепление через ветку HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders (сработает на Windows XP).

Образец создан под работу на Windows XP, поэтому корректная работа на Windows 10 невозможна.

В итоговой DLL содержится бот ПрохуСВ, и значительных отличий от новых версий в нем не обнаружено. Отметить стоит «версию» бота. Для удобной атрибуции кампании в ботах есть параметр group, и в данном образце он равен 4. Удивительно и то, что на нынешних C2 еще остались упоминания подключения ботов с group = 4.

Первая связь с другим вредоносом

Следующее изменение в дроппере датируется 2012–2013 годами.

File name	23391f7d69a883ccd435bcae4d9844114faea9b1223c70984178c11d8e7316f2.exe
MD5	cdf5020d7a7ef2c2ee83a4afdd2413cd
SHA1	2d7f670ee948c1feea2fe1cd3d64f0235025c73f
SHA256	23391f7d69a883ccd435bcae4d9844114faea9b1223c70984178c11d8e7316f2
File type	PE32 executable
File size	68.00 KB
Compilation timestamp	1998-01-13 16:06:20 UTC (модифицирована)

В образце 2013 года основная логика самого бота по-прежнему не отличается от более раннего варианта: сохраняются тот же прокси-модуль ProхуСВ, та же схема сетевого цикла и общий формат работы с С2. При этом меняется сопровождающая обвязка. На уровне инициализации вместе с адресами управления уже используется другой параметр group = 1.

В этот раз бот ProхуСВ поставляется вместе с ботнетом Virut, который работает отдельно и не связан с С2 ProхуСВ. Virut использует более сложный stage-модуль с section-based инъекцией. После запуска он перебирает системные процессы, открывает winlogon.exe, а затем использует именованные секции в BaseNamedObjects для отображения своего кода в память удаленного процесса. После этого в winlogon.exe патчатся несколько Zw*-stub в ntdll, а точка входа внедренного stage запускается через CreateRemoteThread. Уже внутри winlogon.exe (или других процессов) stage начинает загружать сетевые библиотеки и инициирует исходящие соединения.

Бот ProхуСВ при этом ставится через сам дроппер, а не в результате инжекта.

Массовая вредоносная кампания

File name	cerber.exe
MD5	cecdd8e541a6c1c53464792fe75525be
SHA1	e2593f8d5be3d0006c5ba99d3f9a72f175e58c6c
SHA256	5f20a9e19b07572cedd99a5e6ef73cb8b4110929c5b6d94dfcc927be7df6a494
File type	PE32 executable
File size	132.00 KB
Compilation timestamp	2016-04-01 20:19:10 UTC в распакованном боте — 2011-11-21 13:44:22

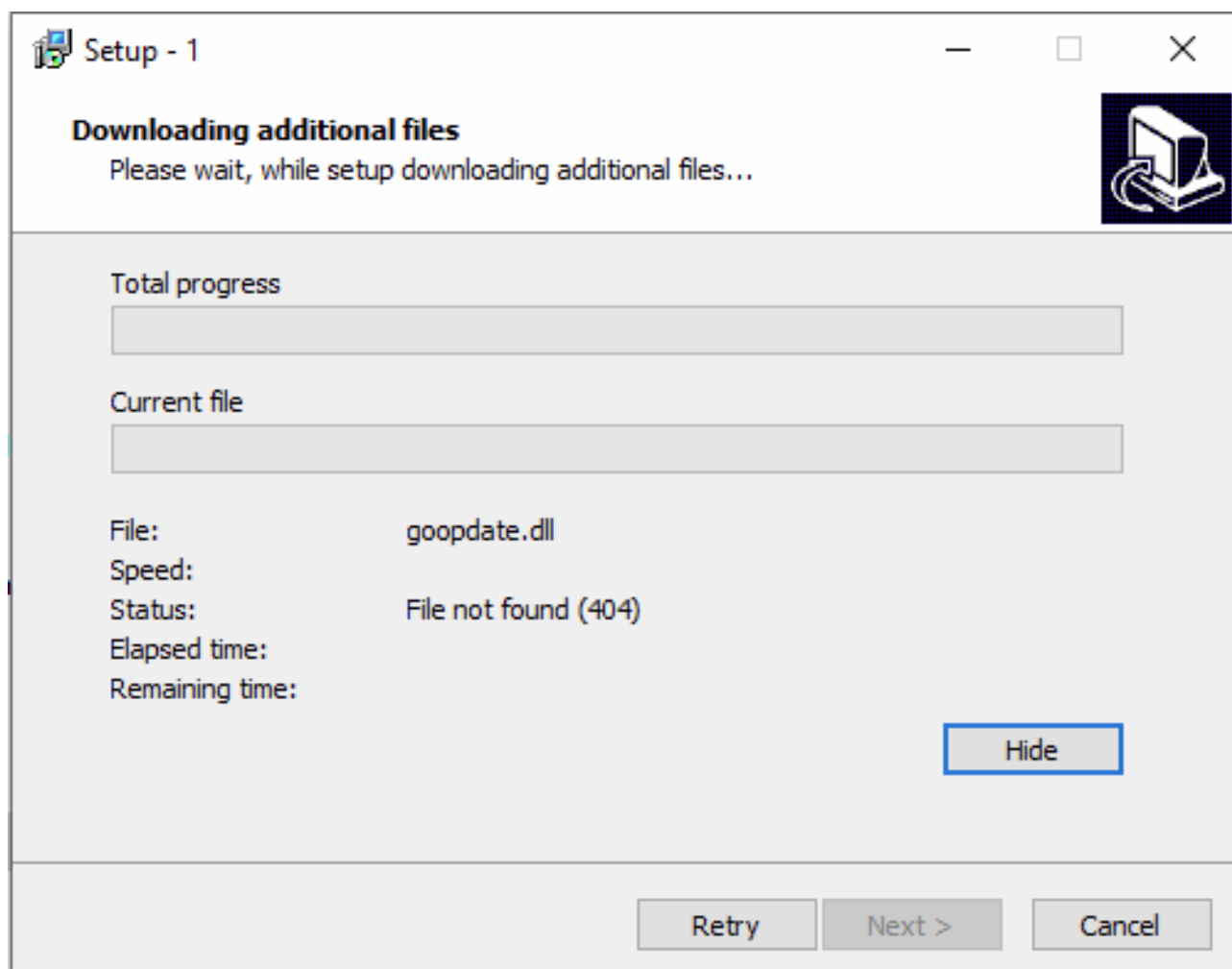
В 2016 году ProхуСВ-боты замечены в составе многоступенчатых цепочек заражения. Первичный JScript-установщик получает первую стадию с uuilouters[.]com, после чего

она обращается к selioprey[.]com за несколькими дополнительными модулями. Один модуль отвечает за кражу учетных данных (Pony stealer), а второй — ProxyCB-бот. На этом фоне сам бот ProxyCB снова остается почти неизменным, а основные изменения приходится на цепочку доставки и разнесение функций по разным payload-модулям.

Современные варианты

File name	setup-235.exe
MD5	ca7b57b87fda8c18354ea6910b20ae73
SHA1	a124d2d6f511298daf6b754213c0146fe8790ad2
SHA256	dc8aaaae4e212ca3c31d94b3a150230e34d1a78544679763e90dc08ee795dadcd
File type	PE32 executable
File size	1.5 MB
Compilation timestamp	2020-05-21 08:56:23 UTC

С 2018 года встречаются новые установщики, маскирующиеся под установщик uTorrent. В них легитимный клиент используется как отвлекающее приложение, тогда как установка ProxyCB происходила параллельно в фоновом режиме, загружая дополнительный модуль с ProxyCB-ботом.



Попытка дроппера установить бота ProxyCB с torrenta[.]top

Примечательно использование Inno Setup, так как этот тип установщиков регулярно встречается в более поздних образцах, связанных с ProxyCB. На этом этапе операторы, по-видимому, делали ставку на правдоподобную установку популярного ПО и вынесение вредоносного модуля в отдельную сетевую стадию.

На одном из форумов с рекламой ботнета администратор сам писал, что может сделать установщик с помощью Inno Setup для программы.



1 июля 2015 г. в 19:31 #7

13

что значит файл всегда чистый? Что софт делает на компе юзера? Будут жалобы на вредное ПО в панель веби

Если юзера начнут спрашивать как де-инсталировать софт, где URL с инструкцией как это сделать?

Сколько детектов на вирустотал? Скрин можно?

- 1) Реклама одного сайта
- 2) Не будут
- 3) Молча.. но могу сделать и установщик с помощью InnoSetup
- 4) В системе они его не найдут, но опять же могу это сделать , если очень надо.
- 5) 1 детектед от заморского антивируса.. Все ссылки в lscq или ЛС.

----- Добавлено 01.07.2015 в 19:32 -----

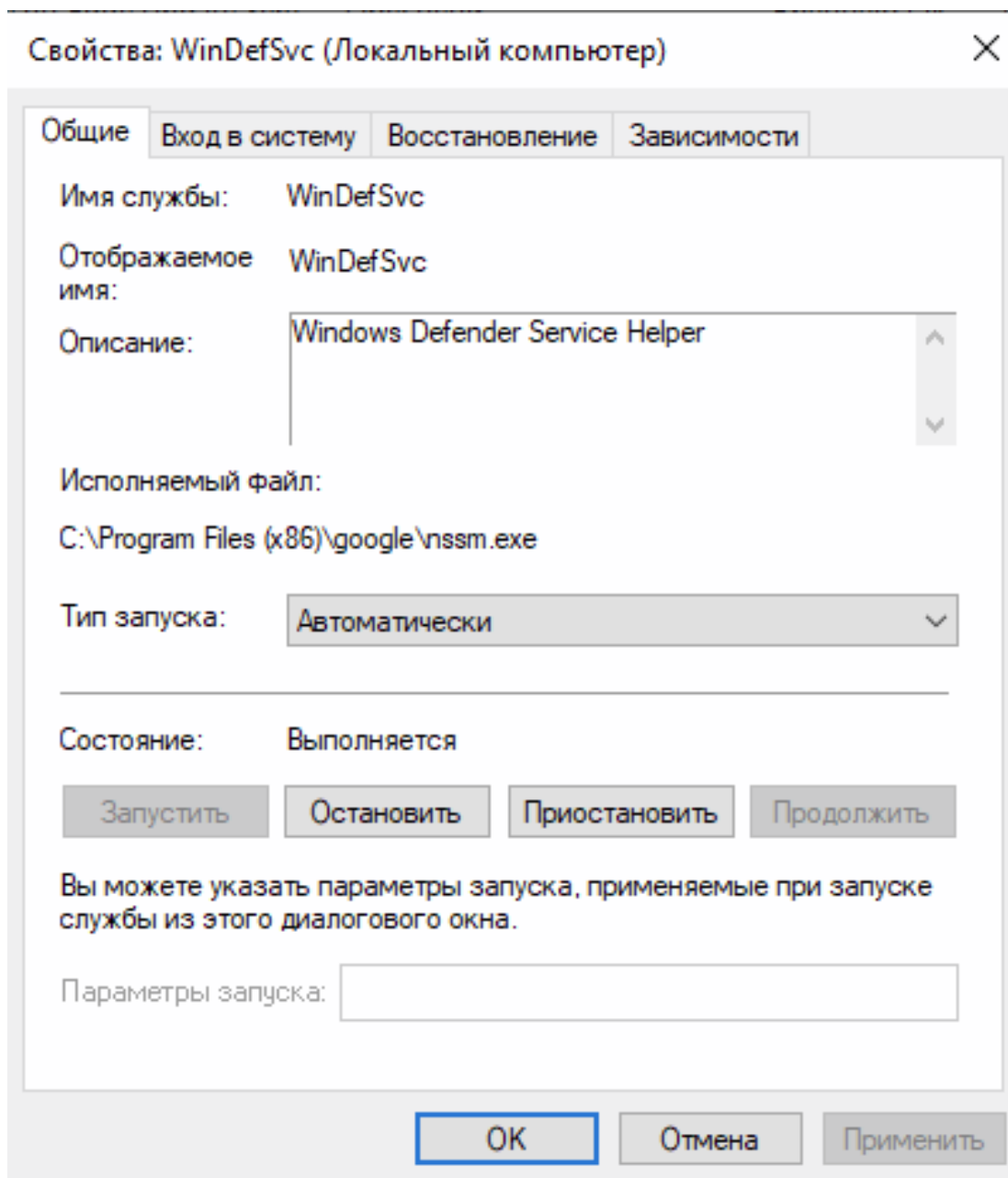
Сообщение от администратора ботнета на форуме

Переход на Node.js

File name	setup.exe
MD5	07353e700edb077cb4de7bd165d0e040
SHA1	f8efadffb89a2c0065ed8864aea8ef4654eb71c6
SHA256	1f708bcd73b114ebf5f59095ff7f7df7cb4b6606054a5e23aa6d36e328bead1e
File type	PE32 executable
File size	18.89 MB
Compilation timestamp	2026-02-11 11:40:27 UTC

Наиболее свежие из найденных вариантов ProхуСВ показывают уже не очередную модификацию дроппера классического PE-бота, а переход к реализации на Node.js. В одном из таких образцов Inno Setup-установщик, маскирующийся под установщик uTorrent, раскладывает в систему node.exe, proxy.js и nssm.exe, после чего через NSSM

создает службу WinDefSvc для запуска бота. При этом полезная нагрузка размещается в каталоге C:\Program Files (x86)\Google, что продолжает характерную для предыдущих поколений ProxycB тактику маскировки под легитимные компоненты (чаще всего Google или uTorrent).



Служба, запускающая бота

Несмотря на смену языка реализации и способа запуска, логика самого бота почти не изменилась. Node.js-вариант сохраняет тот же управляющий цикл, ту же модель разделения main- и data-каналов и тот же набор рабочих режимов: SOCKS4, SOCKS5, HTTP CONNECT, GET и POST. По сути, это очередная упаковка того же прокси-модуля, адаптированная под более современную среду выполнения и новую цепочку доставки.

Технический анализ бота

По сути, боты практически идентичны по своему коду, отличается лишь способ их доставки, поэтому будет рассмотрен один из самых простых вариантов.

File name	23c6e8163646ba03c0a5c6dcd0f0df5688ec4a91c8bd9b663888440254bc12f.exe
MD5	de237777518dc9c0b7a03c536746d878
SHA1	a357466573e35d634a119b7f2e7a8a18f5018811
SHA256	23c6e8163646ba03c0a5c6dcd0f0df5688ec4a91c8bd9b663888440254bc12f
File type	PE32 executable
File size	62.33 KB
Compilation timestamp	2023-11-17 22:20:27 UTC

При старте формируется идентификатор из серийника тома, используется как имя глобального мьютекса и предотвращает повторный запуск на одной системе.

```

tempPathLenOrMutexSeed = GetTempPathA(0x104,tempPath);
if (tempPathLenOrMutexSeed != 0) {
    tempPath[3] = '\\0';
    gotVolumeInfo =
        GetVolumeInformationA
            (tempPath, (LPSTR) 0x0, 0, &volumeSerial, (LPDWORD) 0x0, (LPDWORD) 0x0, (LPSTR) 0x0, 0);
    if (gotVolumeInfo == 0) {
        mutexSeed = 0;
    }
    else {
        mutexSeed = volumeSerial;
    }
    tempPathLenOrMutexSeed = mutexSeed;
}
GenMutexId(mutexId,tempPathLenOrMutexSeed);
g_BotGroup = 728;
lstrcpyA(&g_C2_addr1,"kilo-torrent.org");
lstrcpyA(&g_C2_addr2,"kilo-torrent.org");
WSAStartup(0x202,&wsaData);
g_NetworkReady = 1;
wprintfA(globalMutexName,"Global\\%s",mutexId);
globalMutexHandle = CreateMutexA((LPSECURITY_ATTRIBUTES) 0x0,0,globalMutexName);

```

Начало вредоносной ветки с генерацией мьютекса

Адрес сервера задается на этапе инициализации и сохраняется в глобальных переменных. Далее основной сетевой цикл выносится в отдельный поток **bot_main_thread** и, при успешном создании потока, процесс переходит к установлению соединения с C2.

```

DAT_0040401c = CreateEventW((LPSECURITY_ATTRIBUTES)0x0,0,0,(LPCWSTR)0x0);
if ((DAT_0040401c == (HANDLE)0x0) ||
    (local_28 = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_00401d60,(LPVOID)0x0,0,(LPDWORD)0x0),
    local_28 == (HANDLE)0x0)) {
    mail_availability = 1;
}
else {
    CloseHandle(local_28);
    while (DAT_00404008 != 0) {
        check_C2_diff = lstrcmpiA(&globl_C2_addr,&glob2_C2_addr);
        if (check_C2_diff == 0) {
            while (first_C2_address = FUN_00401bc0(&globl_C2_addr), first_C2_address == 0xffffffff) {
                Sleep(10000);
            }
            mail_availability = check_mail_availability();
            DAT_00404014 = (undefined2)mail_availability;
        }
        else {
            while( true ) {
                first_C2_address = FUN_00401bc0(&globl_C2_addr);
                second_C2_address = FUN_00401bc0(&glob2_C2_addr);
                if (first_C2_address != 0xffffffff) break;
                Sleep(10000);
            }
            mail_availability2 = check_mail_availability();
            DAT_00404014 = (undefined2)mail_availability2;
            if (((mail_availability2 & 0xffff) != 0) && (second_C2_address != 0xffffffff)) {
                first_C2_address = second_C2_address;
            }
        }
    }
    C2_port = 0x3e9;
    C2_address = first_C2_address;
}

```

Основной сетевой цикл

Основной сетевой цикл реализован в **bot_main_thread**. Поток резолвит один или два заранее заданных адреса, после чего устанавливает TCP-соединение на управляющий порт (1001) и обменивается фиксированными 26-байтными сообщениями. В зависимости от **opcode** прокси либо подтверждает успешную авторизацию, либо применяет параметры перенаправления (новый хост/порт) с переподключением, либо запускает отдельный поток обработки задачи (**bot_task_thread**). Отдельно реализована динамическая настройка таймингов, которые сервер может корректировать в ходе работы. Перед соединением с C2 происходит проверка SMTP.

```

undefined4 check_mail_availability(void)
{
    char *mailDomains [4];
    SOCKET smtpSocket;
    int resolveRetry;
    int resolvedMailServerAddr;
    uint domainIndex;

    mailDomains[3] = (char *)0x0;
    mailDomains[0] = "YAhO.Com";
    mailDomains[1] = "HtMaIl.cOM";
    mailDomains[2] = "GMaIl.cOM";
    domainIndex = 0;
    do {
        if (2 < domainIndex) {
            return mailDomains[3];
        }
        resolvedMailServerAddr = -1;
        for (resolveRetry = 0; resolveRetry < 3; resolveRetry = resolveRetry + 1) {
            resolvedMailServerAddr = resolve_mx(mailDomains[domainIndex]);
            if (resolvedMailServerAddr != -1) break;
        }
        if (resolvedMailServerAddr != -1) {
            smtpSocket = safe_connect(resolvedMailServerAddr,25);
            if (smtpSocket != 0xffffffff) {
                closesocket(smtpSocket);
                return 1;
            }
        }
        domainIndex = domainIndex + 1;
    } while( true );
}

```

Проверка SMTP

После получения команды от сервера запускается основной рабочий поток **bot_task_thread**. Поток открывает рабочее соединение (data-канал), выполняет короткое рукопожатие фиксированным сообщением и получает от сервера один байт, определяющий режим работы. Далее выбирается обработчик (сырой TCP, SOCKS или HTTP CONNECT/GET/POST), после чего начинается двунаправленное проксирование данных через общий цикл.

Всего у бота шесть команд от сервера

CMD	Назначение	Что делает бот
0x01	Hello / login	Используется при первичном подключении бота к C2. Бот отправляет hello-пакет, а входящий 0x01 трактуется как успешное подтверждение старта.
0x02	Запуск data-канала	Сервер передает параметры рабочей сессии, после чего бот открывает отдельное соединение и инициализирует worker/data-channel.
0x03	Ошибка	Бот воспринимает такой пакет как ошибочное состояние main-сессии, выходит из цикла и переподключается.
0x04	Keep-alive	Служебный ring-пакет для поддержания main-соединения. Отдельной рабочей логики не несет, но используется для проверки состояния сессии.
0x05	Редирект на новый C2	Бот получает новый IP:port, закрывает текущее main-соединение и переподключается уже к новому адресу. Изменение действует только в памяти работающего бота, без сохранения на диск.
0x06	Закреть main-соединение	Бот явно закрывает текущее управляющее соединение и затем уходит в обычный цикл переподключения.

Сетевое взаимодействие

Обмен между прокси-узлом и сервером на управляющем канале построен на фиксированных сообщениях длиной 26 байт. Каждое такое сообщение начинается с постоянной сигнатуры и версии протокола, после чего следуют поля, смысл которых зависит от типа команды. Таким образом, один и тот же 26-байтный шаблон используется как для начального hello, так и для keep-alive, служебных ответов и команд на запуск рабочего канала.

Общий формат сообщения:

Смещение	Размер	Описание
0x00	4	magic1 = 0x7704B285
0x04	4	magic2 = 0x33E038CE
0x08	1	0x04
0x09	1	cmd
0x0A	2	botnetId / group / port (поле переиспользуется)
0x0C	2	isSmtп / flags (поле переиспользуется)
0x0E	4	v7 (служебный параметр/seed)
0x12	4	serial
0x16	4	creationTime

Структура сообщения остается неизменной по длине и смещениям, однако назначение отдельных полей определяется значением cmd. Поэтому одно и то же смещение в разных пакетах может интерпретироваться как group, data_port, флаг возможностей или идентификатор задачи. Это соответствует наблюдаемому поведению прокси-клиента и логике потоков bot_main_thread и bot_task_thread, где один и тот же буфер используется как для регистрации на main-канале, так и для запуска рабочей сессии.

Начало взаимодействия на управляющем канале

Первым отправляется **hello-пакет** от прокси-узла:

85 b2 04 77 ce 38 e0 33 | 04 | 01 | d8 02 | 00 00 | 00 00 00 00 | 09 80 86 48 | 7c c7 b0 fd

Здесь:

- 85 b2 04 77 ce 38 e0 33 — магическое число,

- 04 — версия,
- 01 — команда hello/login,
- d8 02 — значение group (0x02D8 = 728),
- 00 00 — флаг SMTP/служебное поле (в данном примере — ноль),
- 00 00 00 00 — поле v7, в этом пакете нулевое,
- 09 80 86 48 — serial,
- 7c c7 b0 fd — creationTime.

В ответ сервер отправляет собственный **hello/ack**:

85 b2 04 77 ce 38 e0 33 | 04 | 01 | d8 02 | 00 00 | 00 00 00 00 | 14 00 00 00 | 7c c7 b0 fd

Здесь ключевое отличие состоит в том, что поле 0x12-0x15 уже не несет исходный serial клиента, а используется сервером как параметр управления сессией. В данном примере значение 0x14 соответствует интервалу между keep-alive сообщениями. Поле creationTime при этом сохраняется прежним.

После успешного обмена hello пакеты keep-alive продолжают использовать тот же 26-байтный формат, но с cmd = 0x04. На стороне клиента это соответствует рабочему циклу bot_main_thread, который периодически отправляет пинг и принимает в ответ либо подтверждение, либо команду изменения состояния соединения.

Команда на запуск рабочего канала

Если серверу требуется передать клиентский трафик через конкретный прокси-узел, по управляющему каналу отправляется команда с cmd = 0x02:

85 b2 04 77 ce 38 e0 33 | 04 | 02 | ea 03 | 07 00 | 4c 1a 69 03 | 02 a1 06 00 | 76 f9 bd 1f

В этом случае поля структуры трактуются уже иначе:

- ea 03 — data_port = 1002,
- 07 00 — flags = 0x0007, то есть набор доступных режимов обработки,
- 4c 1a 69 03 — служебный параметр v7, используемый как seed/cookie,
- 02 a1 06 00 и 76 f9 bd 1f — идентификаторы конкретной задачи.

Именно эти значения затем помещаются в структуру, передаваемую в bot_task_thread. Рабочий поток использует их для установления нового TCP-соединения уже не на main-port, а на указанный data_port, после чего повторяет короткое рукопожатие и ожидает режим задачи.

Инициализация data-канала

После получения команды `cmd = 0x02` прокси-узел открывает новое соединение и отправляет первый пакет на рабочий порт:

85 b2 04 77 ce 38 e0 33 | 04 | 02 | d8 02 | 00 00 | 00 00 00 00 | 02 a1 06 00 | 76 f9 bd 1f

Формат тот же, однако поля интерпретируются иначе:

- поле 0x0A-0x0B снова содержит **group** (0x02D8 = 728),
- поле 0x0C-0x11 в данном случае обнуляется,
- последние 8 байт совпадают с идентификаторами задачи, ранее выданными сервером на управляющем канале.

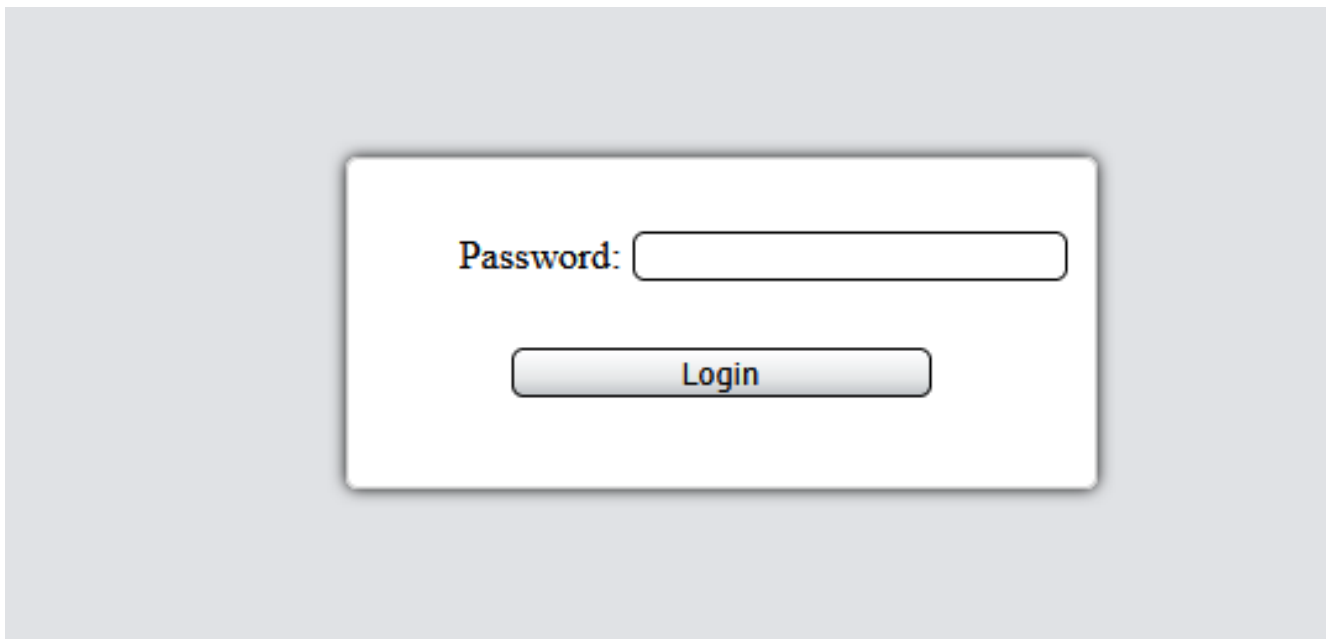
Эта пара значений выполняет функцию синхронизации между командой на `main`-канале и новым рабочим соединением. Управляющий канал используется для выдачи параметров задачи, а рабочий канал — для фактического исполнения проксирования, при этом обе сессии связываются между собой через идентификаторы задачи.

Переход к туннелированию

После успешного рукопожатия на рабочем канале сервер передает один байт, обозначающий режим задачи. В зависимости от значения выбирается один из обработчиков: прямой TCP-туннель, SOCKS-режим или HTTP-режим (CONNECT, GET, POST). Далее выполнение переходит к общему циклу двунаправленного проксирования (`проху_loop`), после чего клиентский трафик уже проходит через цепочку «пользователь → сервер → прокси-узел → целевой ресурс». Именно на этом этапе в сетевом дампе становятся видны обычные прикладные данные, например строка `CONNECT <host>:443` и последующее TLS-рукопожатие.

Панель управления ProхуСВ

На портах 80 или 443 доступна панель авторизации.

A screenshot of a web-based authentication panel for ProxyCV. The panel is a white rectangle with rounded corners and a subtle drop shadow, centered on a light gray background. Inside the panel, the word "Password:" is displayed in a black serif font. To its right is a horizontal text input field with a thin black border. Below the input field is a single button with a light gray gradient and rounded ends, containing the word "Login" in a black serif font.

Панель авторизации ProxyCV

При успешной авторизации происходит переход на страницу с информацией о сервере:

Server Ver	7.1.4
Uptime	0 day 00:02:47
Port Mapper Free	1043765
Port Mapper Wait	328
Port Mapper Work	4483
Port Mapper Used	4811
Allocated Ports	25600
Used Ports	301
Bots In Base	3495
Counters	
transact_count	739637998166
transact_byte	545485283380041
auth_count	42657114
ping_count	61616423
thread_error	81419871
connect_to_close_port	2287769983
client_connect	25555090985
bot_data_connect	19203012719
bot_main_connect	47057461
client_denied	3721277657
admin_pass_error	10176
admin_connect	9999131
bot_send_error_cmd	0

[Clear Stat](#)
[Clear Base](#)
[Reboot](#)
[Show Debug](#)

Структура вкладок и их назначение

Вкладки панели можно условно разделить на три группы:

1. Мониторинг и состояние инфраструктуры

- Server Info — сводка по серверу, счетчики событий и базовые параметры работы.
- Sys Info — статистика по серверным ресурсам.
- Country Info / Group Info — агрегирование прокси-узлов по географии и группам.
- Get List — список активных узлов и их основные атрибуты.

2. Контроль доступа и эксплуатационные ограничения

- Client IP — управление списком IP клиентов.
- API Access — разграничение прав для дополнительных учетных записей API.

3. Управление поведением прокси-узлов

Config — централизованная настройка параметров работы прокси (в т. ч. режимов доступа и других значений конфигурации), а также параметры, связанные с учетными данными панели.

Server InfoBot InfoGroup InfoCountry InfoSys InfoClient IPGet ListConfigApi AccessLogout

Client Ip

Add

DEL IP							
185.107.56.158	149.88.18.25	213.171.17.109	193.233.112.212	193.233.113.18	91.243.31.104	147.45.216.23	193.233.113.48
147.45.199.128	213.171.17.114	212.192.31.249	185.156.3.40	46.17.106.135	178.173.96.76	46.166.182.70	185.159.158.101
185.159.158.58	95.47.189.204	193.233.112.201	185.238.191.34	138.201.17.213	178.63.49.242	168.119.139.232	88.212.207.112
185.9.144.159	185.9.146.97	141.98.189.84	5.79.192.105	185.51.63.200	94.250.254.198	185.108.208.93	192.227.159.237
193.111.117.143	84.20.17.65	178.72.97.181	146.19.207.209	94.141.122.155	46.200.240.127	193.233.126.191	185.143.173.142
79.132.27.219	155.212.216.72	65.21.192.179	213.171.17.111	88.212.206.106	91.142.152.226	176.65.57.205	95.156.77.14
89.188.113.177	46.4.81.149	176.9.64.179	144.76.14.242	144.31.25.61	145.239.87.45	5.8.20.198	158.173.177.236
109.61.108.2	178.207.21.65	136.169.209.138	46.191.182.49	188.187.129.32	144.31.199.88	193.111.117.17	85.209.9.68
1.1.1.1	109.229.184.46	109.252.146.33	193.233.113.224	37.110.91.14	82.143.146.52	38.111.114.28	94.141.122.237
81.30.105.205	135.181.166.12	142.132.154.24	45.129.59.171	65.108.108.57	94.141.160.234	94.141.122.178	91.197.96.238
188.130.132.81	94.141.122.56	84.38.184.234	85.174.195.39	147.45.215.169	109.71.242.250	65.108.122.254	193.233.112.101
185.60.133.115	178.140.157.174	89.250.74.42	5.165.107.209	194.59.40.237	80.66.89.159	185.135.81.58	38.114.102.93
185.46.10.4	88.212.207.115	193.233.113.144	46.175.134.185	188.226.54.54	103.7.54.15	185.177.239.98	91.209.135.253
147.45.198.168	185.209.23.90	37.232.255.86	89.110.93.107	193.58.122.111	94.198.54.51	95.139.91.122	65.108.38.248
147.45.198.80	109.172.89.93	167.148.195.211	85.209.129.57	77.91.65.90	109.252.175.9	176.193.63.198	185.231.155.116
188.255.25.26	217.168.247.151	93.183.90.211	176.65.144.59	190.97.237.72	94.242.55.40	185.135.83.175	37.212.58.101
84.53.236.42	46.191.225.229	185.244.183.67	77.232.37.121	176.192.173.200	51.38.130.131	82.26.193.53	89.110.70.120
77.232.37.134	80.253.249.29	95.220.41.114	192.144.56.78	188.137.225.99	193.37.71.46	94.232.63.0	46.0.112.143
95.52.245.112	213.21.10.109	185.221.162.16	158.173.155.185	152.53.85.249	81.211.41.22	146.158.120.1	95.216.225.116
147.45.198.42	83.147.245.170	195.133.32.155	213.159.77.141	103.112.171.163	5.91.187.18	185.56.162.148	185.175.46.117
5.129.238.115	83.221.200.164	37.9.13.98	93.100.76.222	95.215.56.156	65.21.91.253	85.21.240.163	45.13.187.211
45.12.108.75	95.217.148.157	95.24.33.122	188.165.255.163	81.23.13.96	80.89.239.251	172.67.69.132	94.142.142.99
77.73.67.238	95.24.33.29	45.12.133.18	91.122.97.249	91.223.123.248	185.158.115.191	95.213.200.106	93.85.74.179
144.31.164.129	109.252.27.72	148.253.214.111	109.173.59.19	178.173.252.38	37.187.74.87	141.101.200.237	95.161.221.49
144.31.12.0	65.109.146.177	116.202.162.244	91.122.60.250	193.138.7.144	95.161.157.90	90.188.49.28	95.190.13.156
31.29.197.48	146.59.80.114	135.181.21.158	91.122.15.243	95.217.127.142	37.112.52.42	213.171.17.107	91.204.150.94
188.127.229.116	95.165.158.220	146.70.231.202	168.119.6.153	185.185.181.185	91.214.78.12	5.166.25.78	185.107.136.49
5.44.169.65	79.139.170.240	91.214.78.115					

© 2011 ProxyCB

Вкладка с IP клиентов

Bot Info

Info	Count
All	3495
Online	325
Online %	9.30%
Online per 1 Hour	365
Online per 12 Hours	567
Online per 24 Hours	829
Online per Week	1314
Online per Month	1889

© 2011 ProxyCB

Вкладка с количеством ботов

Server Info	Bot Info	Group Info	Country Info	Sys Info
Client IP	Get List	Config	Api Access	Logout

Group Stat

Group	All	Online	Online %	1 Hour	12 Hours	24 Hours	Week	Month	Get List
473	49	7	14.29%	7	10	12	27	35	Get List
903	328	36	10.98%	37	59	79	139	220	Get List
344	132	0	0.00%	0	2	2	2	8	Get List
9854	10	1	10.00%	1	1	3	4	5	Get List
941	281	28	9.96%	30	47	90	140	197	Get List
701	18	2	11.11%	2	5	6	10	14	Get List
343	591	0	0.00%	0	0	3	6	28	Get List
943	193	22	11.40%	25	42	64	100	147	Get List
947	109	16	14.68%	17	25	35	54	76	Get List
939	46	3	6.52%	3	5	13	23	32	Get List
946	156	21	13.46%	25	36	53	80	108	Get List
621	28	4	14.29%	5	6	9	17	22	Get List
942	99	19	19.19%	19	27	38	54	75	Get List
938	73	10	13.70%	11	13	27	44	54	Get List
940	32	5	15.62%	6	8	14	17	24	Get List
629	32	0	0.00%	1	6	7	15	19	Get List
1	180	20	11.11%	30	46	57	86	121	Get List
714	15	4	26.67%	5	6	6	11	12	Get List
226	7	0	0.00%	0	0	0	0	2	Get List
945	32	6	18.75%	7	9	14	20	24	Get List
630	17	1	5.88%	2	2	5	7	11	Get List
618	23	4	17.39%	4	4	7	11	16	Get List
502	32	3	9.38%	3	4	9	12	22	Get List
708	14	4	28.57%	4	8	8	10	11	Get List
506	17	2	11.76%	2	4	5	8	12	Get List
935	10	2	20.00%	2	3	5	6	6	Get List

Вкладка со списком групп ботов

Группа бота захардкожена и передается в hello-пакете.

Country Stat

Flag	Country	All	Online	Online %	1 Hour	12 Hours	24 Hours	Week	Month	Get List
NONE	--	957	93	9.72%	99	155	224	366	530	Get List
	Europe	8	0	0.00%	1	1	2	4	4	Get List
	United Arab Emirates	1	1	100.00%	1	1	1	1	1	Get List
	Belgium	1	0	0.00%	0	1	1	1	1	Get List
	Bulgaria	1	0	0.00%	0	0	0	0	0	Get List
	Belarus	2	0	0.00%	0	0	0	0	0	Get List
	Switzerland	3	0	0.00%	0	0	2	2	2	Get List
	China	6	0	0.00%	0	0	0	0	0	Get List
	Cyprus	1	0	0.00%	0	0	0	0	0	Get List
	Czech Republic	18	2	11.11%	2	2	5	5	7	Get List
	Germany	9	3	33.33%	3	5	5	7	8	Get List
	Denmark	4	0	0.00%	0	0	0	0	1	Get List
	Spain	2	0	0.00%	0	0	0	0	1	Get List
	Finland	6	0	0.00%	0	0	1	1	3	Get List
	France	7	0	0.00%	1	2	2	4	5	Get List
	United Kingdom	15	2	13.33%	2	3	5	7	8	Get List
	Greece	6	1	16.67%	1	2	2	2	4	Get List
	Iran, Islamic Republic of	2	1	50.00%	1	1	1	1	2	Get List
	Italy	3	0	0.00%	0	0	1	1	1	Get List
	Jordan	1	0	0.00%	0	0	0	0	1	Get List
	Kyrgyzstan	1	0	0.00%	0	0	0	0	0	Get List
	Kazakhstan	3	0	0.00%	0	0	0	1	2	Get List
	Moldova, Republic of	1	0	0.00%	0	0	0	0	1	Get List
	Netherlands	9	0	0.00%	0	1	2	2	3	Get List
	Norway	4	0	0.00%	0	0	0	0	0	Get List
	Poland	1	0	0.00%	0	0	0	1	1	Get List
	Portugal	1	1	100.00%	1	1	1	1	1	Get List
	Romania	16	1	6.25%	1	2	3	4	7	Get List
	Russian Federation	2312	210	9.08%	244	371	547	867	1245	Get List
	Sweden	2	0	0.00%	0	0	1	2	2	Get List
	Tajikistan	1	0	0.00%	0	0	0	0	0	Get List
	Turkmenistan	1	0	0.00%	0	0	0	0	0	Get List
	Turkey	1	0	0.00%	0	0	0	0	0	Get List
	Ukraine	55	5	9.09%	6	12	16	24	32	Get List
	United States	32	2	6.25%	2	6	6	9	15	Get List
	Uzbekistan	2	0	0.00%	0	0	1	1	1	Get List

Вкладка со статистикой по странам

Server Info

Bot Info

Group Info

Country Info

Sys Info

Client IP

Get List

Config

Api Access

Logout

System Info

Name	cpu	Name	cpu0	Name	cpu1	Name	cpu2
Total	20.10%	Total	13.27%	Total	16.83%	Total	12.37%
User	8.42%	User	0.00%	User	0.99%	User	1.03%
System	5.25%	System	4.08%	System	4.95%	System	3.09%
I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%
IRQ	0.00%	IRQ	0.00%	IRQ	0.00%	IRQ	0.00%
Soft-IRQ	6.42%	Soft-IRQ	9.18%	Soft-IRQ	10.89%	Soft-IRQ	8.25%
Nice	0.00%	Nice	0.00%	Nice	0.00%	Nice	0.00%

Name	cpu3	Name	cpu4	Name	cpu5	Name	cpu6
Total	11.34%	Total	17.31%	Total	65.98%	Total	7.00%
User	0.00%	User	0.00%	User	60.82%	User	1.00%
System	4.12%	System	4.81%	System	5.15%	System	6.00%
I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%
IRQ	0.00%	IRQ	0.00%	IRQ	0.00%	IRQ	0.00%
Soft-IRQ	7.22%	Soft-IRQ	12.50%	Soft-IRQ	0.00%	Soft-IRQ	0.00%
Nice	0.00%	Nice	0.00%	Nice	0.00%	Nice	0.00%

Name	cpu7	Name	cpu8	Name	cpu9	Name	cpu10
Total	4.12%	Total	9.09%	Total	16.50%	Total	15.84%
User	1.03%	User	1.01%	User	0.97%	User	0.99%
System	3.09%	System	8.08%	System	6.80%	System	5.94%
I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%	I/O Wait	0.00%
IRQ	0.00%	IRQ	0.00%	IRQ	0.00%	IRQ	0.00%
Soft-IRQ	0.00%	Soft-IRQ	0.00%	Soft-IRQ	8.74%	Soft-IRQ	8.91%
Nice	0.00%	Nice	0.00%	Nice	0.00%	Nice	0.00%

Name	cpu11
Total	49.04%
User	33.65%
System	5.77%
I/O Wait	0.00%
IRQ	0.00%
Soft-IRQ	9.62%
Nice	0.00%

Name	Send	Recv	Send Total	Recv Total	Send Peak	Recv Peak	Read+Send Peak
lo	4.646 KB/sec	4.646 KB/sec	6.407 GB	6.407 GB	60.954 KB/sec	60.954 KB/sec	121.908 KB/sec
enp3s0f0	53.976 MB/sec	53.764 MB/sec	176.332 TB	176.184 TB	69.211 MB/sec	68.709 MB/sec	137.921 MB/sec
enp3s0f1	0 Byte/sec	0 Byte/sec	0 Byte	0 Byte	0 Byte/sec	0 Byte/sec	0 Byte/sec

© 2011 ProxyCB

© 2011 ProxyCB

Вкладка со статистикой по серверным ресурсам

Full List

☒

Show on this page

☒

Group

Country

SMTP

Filtering

Current List As Text

Flag	IP:PORT	Real IP	Group	Country	CCode	CName	SMTP
	185.158.112.116:25607	81.23.203.193	943	185	RU	Russian Federation	GOOD
	185.158.112.116:25625	77.243.117.128	940	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25629	46.235.68.95	621	0	--	--	BAD
NONE	185.158.112.116:25647	37.194.196.66	945	0	--	--	GOOD
	185.158.112.116:25650	95.32.76.190	939	185	RU	Russian Federation	GOOD
	185.158.112.116:25658	178.176.81.12	618	185	RU	Russian Federation	GOOD
	185.158.112.116:25661	95.68.170.174	941	185	RU	Russian Federation	GOOD
	185.158.112.116:25675	85.172.76.80	943	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25721	176.126.30.70	947	0	--	--	BAD
	185.158.112.116:25729	95.26.47.205	947	185	RU	Russian Federation	BAD
	185.158.112.116:25735	212.106.54.150	943	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25743	176.195.78.220	942	0	--	--	GOOD
	185.158.112.116:25751	62.183.17.132	628	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25754	213.109.49.196	701	0	--	--	GOOD
NONE	185.158.112.116:25757	176.52.40.173	1	0	--	--	GOOD
	185.158.112.116:25760	178.66.159.77	701	185	RU	Russian Federation	GOOD
	185.158.112.116:25763	46.164.219.2	619	185	RU	Russian Federation	GOOD
	185.158.112.116:25767	95.25.207.175	572	185	RU	Russian Federation	BAD
	185.158.112.116:25772	95.189.77.78	310	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25775	176.100.118.229	714	0	--	--	GOOD
	185.158.112.116:25788	193.233.122.79	938	185	RU	Russian Federation	GOOD
	185.158.112.116:25792	92.63.188.50	946	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25795	5.16.76.220	903	0	--	--	GOOD
	185.158.112.116:25803	178.34.47.162	946	185	RU	Russian Federation	GOOD
	185.158.112.116:25804	91.215.89.245	902	185	RU	Russian Federation	GOOD
	185.158.112.116:25805	90.154.72.57	310	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25816	176.114.25.46	942	0	--	--	GOOD
	185.158.112.116:25835	109.196.195.32	947	185	RU	Russian Federation	GOOD
	185.158.112.116:25837	2.61.90.169	473	185	RU	Russian Federation	GOOD
NONE	185.158.112.116:25843	37.76.153.104	946	0	--	--	GOOD
	185.158.112.116:25850	188.168.207.63	9855	185	RU	Russian Federation	GOOD

Вкладка со списком ботов

Server Info	Bot Info	Group Info	Country Info	Sys Info
Client IP	Get List	Config	Api Access	Logout

Config

Proxy Access	IP CHECK ▾
Bot Ping Timeout:	60
Bot Ping Timeout Limit:	122
Client Wait Bot Timeout:	10
Inactive Connect Timeout:	120
Allow Socks4 Protocol:	☒
Allow Socks5 Protocol:	☒
Allow HTTP Protocol:	☒
New Admin Pass:	
New Api_1 Pass:	
New Api_2 Pass:	
Current Pass Salt:	57219660

© 2011 ProxyCB

Вкладка с настройкой конфигурации ботов и пароля к панели

Server Info

Bot Info

Group Info

Country Info

Sys Info

Client IP

Get List

Config

Api Access

Logout

Api Access

	Api 1		Api 2
Server Info:	☒	Server Info:	☒
Bot Info:	☒	Bot Info:	☒
Group Info:	☒	Group Info:	☒
Country Info:	☒	Country Info:	☒
Config Get:	☒	Config Get:	☒
Config Set:	☒	Config Set:	☒
Client Add Ip:	☒	Client Add Ip:	☒
Client Del Ip:	☒	Client Del Ip:	☒
Client Get List:	☒	Client Get List:	☒
Get Proxy List:	☒	Get Proxy List:	☒
Reboot:	☒	Reboot:	☒
Clear Base:	☒	Clear Base:	☒
Clear Stat:	☒	Clear Stat:	☒
Api Access Get:	☒	Api Access Get:	☒
Api Access Set:	☒	Api Access Set:	☒
Check Pass:	☒	Check Pass:	☒
Get Performance:	☒	Get Performance:	☒
Gen Pass Salt:	☒	Gen Pass Salt:	☒
Show Debug:	☒	Show Debug:	☒

Save

© 2011 ProxyCB

Вкладка с настройками доступов у двух пользователей (у администратора есть все права)

На самом деле это не единственный способ управления ботнетом. О другом способе мы расскажем дальше.

Анализ ядра C2-сервера

Веб-панель — это лишь обертка над реальным каналом управления. В результате расследования удалось найти два sh-скрипта: первый скрипт отвечает за установку PCBServer 7, второй — за ее полное удаление.

```
C:\Windows\system32>curl -O http://185.158.115.191/1.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  671k  100  671k    0     0   869k      0 --:--:-- --:--:-- --:--:--   869k

C:\Windows\system32>curl -O http://185.158.115.191/2.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100   797  100   797    0     0   3659      0 --:--:-- --:--:-- --:--:--   3655
```

Установка скриптов

Установочный скрипт создает демона под систему на init.d.

```
Verifying archive integrity... All good.
Uncompressing PCB Installer.....
PCBServer 7 INSTALL
Copy geoip.db                OK
Copy pcb                     OK
Copy pcb_x64                 cp: cannot create regular file '/usr/sbin/pcb': Text file busy
Copy pcb_test                OK
Chmod /usr/sbin/pcb          OK
Chmod /usr/sbin/pcb_test     OK
Chmod /etc/init.d/pcb        OK
Make Link /etc/rc1.d/K99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc0.d/K99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc2.d/S99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc3.d/S99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc4.d/S99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc5.d/S99pcb -> /etc/init.d/pcb      OK
Make Link /etc/rc6.d/K99pcb -> /etc/init.d/pcb      OK
./install: 75: insserv: not found
Warning: The unit file, source configuration file or drop-ins of pcb.service changed on disk. Run '
systemctl daemon-reload' to reload units.
PCBServer 7 INSTALL FINISH
```

Запуск установщика

Порты 1001,1002 и 1003 есть в параметрах запуска демона PCB и остаются неизменными.

```
#!/bin/sh
### BEGIN INIT INFO
# Provides:          pcb_mon
# Required-Start:    $remote_fs $network $syslog
# Required-Stop:     $remote_fs $network $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: ProxyCB Control
# Description:       This file ProxyCB Control script
### END INIT INFO

PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="ProxyCB Daemon"
NAME=pcb
DAEMON=/usr/sbin/$NAME
DAEMON_ARGS="--main_port=1001 --data_port=1002 --admin_port=1003 --daemon=1 --log=/var/log/$NAME.log"
PIDFILE=/var/run/$NAME.pid
SCRIPTNAME=/etc/init.d/$NAME
```

Скрипт запуска демона PCB

```
● pcb.service - LSB: ProxyCB Control
   Loaded: loaded (/etc/init.d/pcb; generated)
   Active: active (running) since Thu 2026-02-26 12:30:41 MSK; 3min 9s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3011 ExecStart=/etc/init.d/pcb start (code=exited, status=0/SUCCESS)
    Tasks: 16 (limit: 19098)
   Memory: 185.3M (peak: 187.1M)
      CPU: 447ms
   CGroup: /system.slice/pcb.service
           └─1231 /usr/sbin/pcb --main_port=1001 --data_port=1002 --admin_port=1003 --daemon=1 --log=/var/log/pcb.log
             └─1233 /usr/sbin/pcb --main_port=1001 --data_port=1002 --admin_port=1003 --daemon=1 --log=/var/log/pcb.log

Feb 26 12:30:41 DockerAndNginxReverse systemd[1]: Starting pcb.service - LSB: ProxyCB Control...
Feb 26 12:30:41 DockerAndNginxReverse pcb[3011]: * Starting ProxyCB Daemon
Feb 26 12:30:41 DockerAndNginxReverse pcb[3016]: start-stop-daemon: matching on world-writable pidfile /var/run/pcb.pid is insecure
Feb 26 12:30:41 DockerAndNginxReverse pcb[3011]: ...done.
Feb 26 12:30:41 DockerAndNginxReverse systemd[1]: Started pcb.service - LSB: ProxyCB Control.
```

Рабочий демон ProxyCB

В коде pcb_x64 сразу заметны функции, отражающие функциональность веб-панели:

- DB_AdminAuth
- DB_AuthBot
- DB_BotGetCountry
- DB_BotGetGroup
- DB_BotGetInfo
- MPM_InsertBot
- MPM_InsertClient
- SA_ClientRouteProc
- и т. д.

И множество других функций, часть из которых была показана в устройстве веб-панели.

Административный порт использует собственный бинарный протокол поверх TCP.

Запросы имеют стандартный формат с полями:

1. MAGIC (8 байт) — уникальный идентификатор для синхронизации.

2. LEN (4 байта) — длина полезной нагрузки.
3. CMD (1 байт) — команда для сервера.
4. MD5 (пароль) (32 байта) — MD5-хэш пароля администратора в ASCII-hex.
5. Payload — дополнительные данные, передаваемые в зависимости от команды.

Ответы от сервера всегда начинаются с 13 байт заголовка:

1. MAGIC (8 байт) — проверка на соответствие.
2. LEN (4 байта) — длина ответа.
3. STATUS (1 байт) — статус выполнения команды (0 — успех, другие значения — ошибка).

Всего у панели есть 19 команд. В коде они реализованы через **case**.

```

-----,
case 1:
    DB_BotGetInfo((int *)local_8ab);
    __n = 0x29;
    local_8b0 = 0x1c;
    break;
case 2:
    local_8ab = (undefined1 [4])DB_BotGetGroup(&local_8c8,&local_8bc);
    __n = 0x11;
    local_8b0 = 4;
    break;
case 3:
    uVar6 = DB_BotGetCountry(&local_8c8,&local_8bc);
    local_8ab = SUB84(uVar6,0);
    __n = 0x11;
    local_8b0 = 4;
    break;

```

Пример нескольких команд в коде

Все возможные команды и их привязка к функции представлены в таблице.

0x00	Server Info
0x01	BotGetInfo

0x02	BotGetGroup
0x03	BotGetCountry
0x04	GetConfig
0x05	SetConfig
0x06	DB_AddAccessIp
0x07	DB_DelAccessIp
0x08	DB_GetAccessIpList
0x09	MCP_GetList
0x0A	Reboot (процесса)
0x0B	DB_ClearBotBase
0x0C	Reset admin stats (счетчики Server Info)
0x0D	DB_GetApiAccess
0x0E	DB_SetApiAccess
0x0F	Предположительно ping/check pass т. к. ничего не делает и просто возвращает 0 при удачной авторизации
0x10	Perf_Stat (информация по нагрузке сервера)
0x11	Change Salt

Распространение ботов

В ходе анализа было выявлено несколько доменов, участвовавших в распространении нынешних версий вредоноса с 2018 года.

Ранние образцы связаны с tut-torrent[.]ru и windows-rar[.]com:



Скачать Торрент - бесплатная программа для сетей BitTorrent (P2P), функционирующий под ОС Windows: 98/ME, NT/2000, XP, 2003 и Vista. Главные отличия от прочих Торрент-программ это маленький размер при довольно большом функциональном потенциале и простому, дружелюбному интерфейсу. Занимает менее **220 КБ** на диске, использует минимум системных ресурсов и не капризен к железу, нормально будет работать даже на очень старых PC. На мой взгляд **uTorrent** является лучшей программой для torrent сетей и не вызовет затруднений при скачивание фильмов, игр и музыки с известных **torrent tracker**'ов! Что бы всё это опробовать на деле рекомендуем Вам *скачать торрент бесплатно* с нашего сайта.

Скачайте ТОРРЕНТ 3.4.9 бесплатно

Торрент программа для компьютера

Архиватор RAR

Лучший rar архиватор

- ✓ Поддержка всех форматов архивации - RAR, 7z, ZIP, gz
- ✓ Выбор темы оформления программы
- ✓ WindowsRAR условно-бесплатная программа

БЕСПЛАТНО
СКАЧАТЬ АРХИВАТОР RAR

Windows XP / Vista / 7 / 8 / 10
Версия: 1.4 от 06.12.2019 Размер файла: 27 МБ.



Сайты с вредоносом

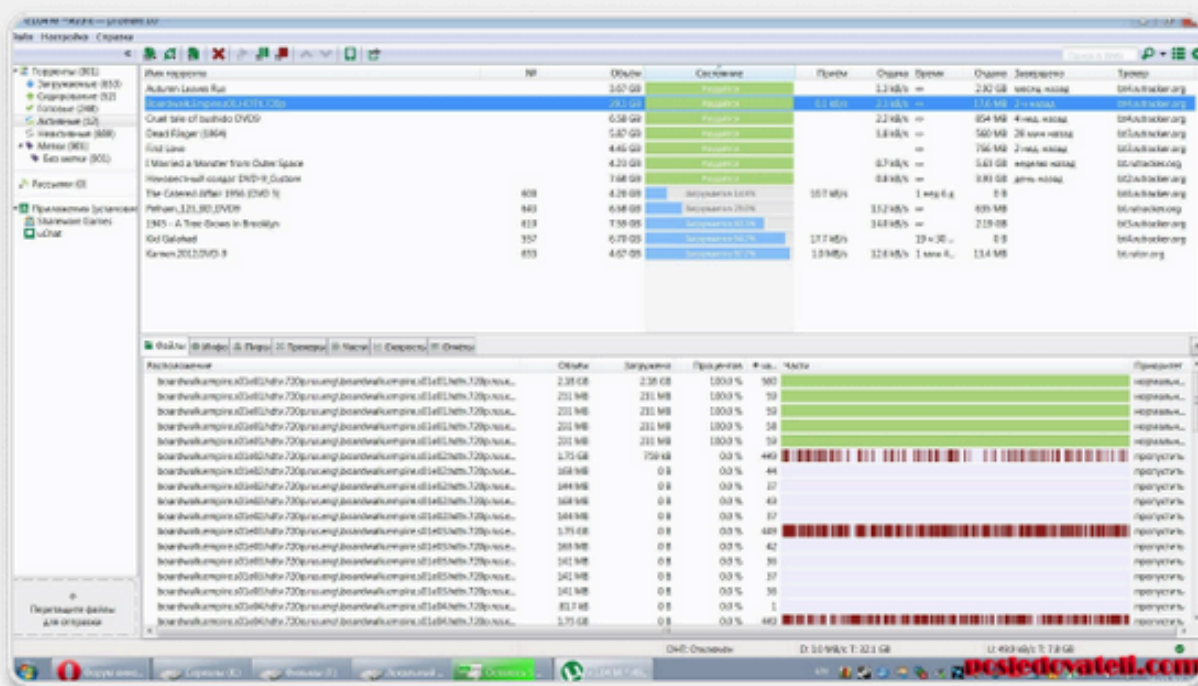
В ноябре 2022 года появился новый домен torrenta[.]top:



Получите лучший в мире классический торрент-клиент.

Быстрое массовое скачивание торрентов на компьютере

Скачать



Новый сайт с вредоносом

Этот домен все еще активен, и через него прошло несколько вариаций дропперов. Часть из них ведет на GitHub-репозиторий, где среди легитимных файлов лежит бот (файл setup.msi).

meyson199502-eng Add files via upload ✓

e4bb5df · last week History

Name	Last commit message	Last commit date
..		
app	fix: use Node.js https module to bypass Reddit HTTP/...	2 weeks ago
public	feat(ai-news-aggregator): initialize ai-news-aggregato...	2 weeks ago
.gitignore	feat(ai-news-aggregator): initialize ai-news-aggregato...	2 weeks ago
README.md	feat(api): implement reddit oauth app-only token flow	2 weeks ago
eslint.config.mjs	feat(ai-news-aggregator): initialize ai-news-aggregato...	2 weeks ago
next.config.js	fix: resolve Reddit posts not loading (#7)	2 weeks ago
package-lock.json	build(deps): add https-proxy-agent to dependencies	2 weeks ago
package.json	build(deps): add https-proxy-agent to dependencies	2 weeks ago
postcss.config.mjs	feat(ai-news-aggregator): initialize ai-news-aggregato...	2 weeks ago
setup.msi	Add files via upload	last week
tsconfig.json	feat(ai-news-aggregator): initialize ai-news-aggregato...	2 weeks ago

Репозиторий с ботом

Через другие дропперы обнаружен более ранний репозиторий с несколькими версиями ботов.

 maik11asa4434 Add files via upload ✖ c7ecf22 · 2 months ago 🕒 54 Commits		
 client	Add files via upload	5 months ago
 server	Add files via upload	2 months ago
 .gitignore	Initial commit	3 years ago
 43	Create 43	7 months ago
 433.zip	Add files via upload	8 months ago
 Dockerfile	Initial commit	3 years ago
 LICENSE	Initial commit	3 years ago
 README.md	Initial commit	3 years ago
 config.json	Initial commit	3 years ago
 docker-compose.yml	Initial commit	3 years ago
 podman-build.sh	Initial commit	3 years ago
 requirements.txt	Initial commit	3 years ago
 run.py	Initial commit	3 years ago
 setup-235.exe	Add files via upload	8 months ago
 setup-235.zip	Add files via upload	8 months ago
 setup.cab	Add files via upload	8 months ago
 setup.exe	Add files via upload	6 months ago
 setup.iso	Add files via upload	8 months ago
 setup.msi	Add files via upload	8 months ago
 setup.zip	Add files via upload	8 months ago
 software.msi.zip	Add files via upload	8 months ago
 uTorrent(42).zip	Add files via upload	2 years ago

Более ранний репозиторий (файлы младше трех лет — это вредоносы)

Связь ботнета с TeamSpy

TeamSpy (или TeamSpy Crew) — это кибершпионская группа, публично описанная в 2013 году. По оценкам исследователей, связанные с ней операции могли вестись с середины 2000-х годов, а к моменту раскрытия кампания продолжалась уже почти десятилетие. Группировка известна тем, что осуществляла скрытные атаки, используя легитимное программное обеспечение для удаленного управления TeamViewer.

В скриптах панели управления обнаружено упоминание домена mir-modov[.]ru. При анализе этого домена выявлено несколько вредоносных файлов, использовавшихся группировкой TeamSpy в своих атаках.

File name	setup.exe
MD5	d711e0af93179af04b050fe08c875df1
SHA1	456c2139c110d442e0a2c513449ab8270185e944
SHA256	9f272806c9626ce7040b73e6ffd489ecc12bb593748b11e55104cf476c195b76
File type	PE32 executable
File size	320.00 КиБ
Compilation timestamp	2014-07-09 07:58:13 UTC

 tvrp	02.09.2016 15:49	Папка с файлами	
 Build.exe	11.10.2016 17:09	Приложение	5 КБ
 game.exe	03.08.2015 17:10	Приложение	2 669 КБ
 msimg32.dll	01.01.2016 0:00	Расширение при...	97 КБ
 SkypeC0SvcService.exe	14.07.2016 22:18	Приложение	7 846 КБ
 TeamViewer_Desktop.exe	14.07.2016 22:18	Приложение	2 234 КБ
 TeamViewer_Resource_en.dll	14.07.2016 22:18	Расширение при...	286 КБ
 TeamViewer_StaticRes.dll	14.07.2016 22:18	Расширение при...	2 529 КБ
 tv_w32.dll	14.07.2016 22:18	Расширение при...	67 КБ
 tv_w32.exe	14.07.2016 22:18	Приложение	105 КБ
 tv_x64.dll	14.07.2016 22:18	Расширение при...	81 КБ
 tv_x64.exe	14.07.2016 22:18	Приложение	127 КБ
 tvr.cfg	05.08.2016 15:59	Файл "CFG"	1 КБ
 vpn64.cab	14.07.2016 22:18	Архив WinRAR	55 КБ
 vpn86.cab	14.07.2016 22:18	Архив WinRAR	43 КБ

Распакованный setup.exe

Результатом запуска этого установщика будет фоновая установка TeamViewer и открытие игры для отвлечения внимания.

В середине 2017 года этот вредонос пропал с доменов mir-modov[.]ru, exe-craft[.]ru и worldoftankist[.]ru, а на различных форумах появилась реклама прокси-сервиса ProxyBunker (он же ProxyTank и ботнет ProxyCB). Стоит отметить, что реклама была и ранее, но в малом количестве, а после середины 2017 года в существующих темах произошли обновления или создались новые темы на новых форумах.

На домене kilo-torrent[.]org также выявлены следы инструментария TeamSpy. В этот раз вредоносный установщик оформлен под клиент uTorrent — приманку, которая неоднократно встречается и в дропперах, связанных с ProxyCB. На момент публикации домен kilo-torrent[.]org остается одним из основных C2 ботнета.

File name uTorrent.zip

MD5 7f846f1b364b1b51528b8461aad5a412

SHA1 9c1af12030dec7afdc8ca014ae182b97175b3d22

SHA256 d973a6054c2952cb14feea309c9063f4aadcee441c4dca5394136bb69f69d232

File type ZIP

File size 8.54 MB

Архив содержит легитимную утилиту TeamViewer, переименованную в setup.exe, вредоносную библиотеку msimg32.dll и архив msimg32.dat. Если распаковать msimg32.dat (пароль: tvratbetabot), то получится тот же инструментарий группировки TeamSpy.

 tvrp	17.01.2017 18:26	Папка с файлами	
 msimg32.dll	13.01.2017 11:26	Расширение при...	135 КБ
 SkypeC0SvcService.exe	14.07.2016 22:18	Приложение	7 846 КБ
 TeamViewer_Desktop.exe	14.07.2016 22:18	Приложение	2 234 КБ
 TeamViewer_Resource_en.dll	14.07.2016 22:18	Расширение при...	286 КБ
 TeamViewer_StaticRes.dll	14.07.2016 22:18	Расширение при...	2 529 КБ
 tv_w32.dll	14.07.2016 22:18	Расширение при...	67 КБ
 tv_w32.exe	14.07.2016 22:18	Приложение	105 КБ
 tv_x64.dll	14.07.2016 22:18	Расширение при...	81 КБ
 tv_x64.exe	14.07.2016 22:18	Приложение	127 КБ
 tvr.cfg	17.01.2017 10:56	Файл "CFG"	1 КБ
 uTorrent.exe	26.10.2016 14:01	Приложение	2 320 КБ
 vpn64.cab	14.07.2016 22:18	Архив WinRAR	55 КБ
 vpn86.cab	14.07.2016 22:18	Архив WinRAR	43 КБ

Распаковка архива

Ранее по этому пути лежал другой архив.

File name uTorrent.zip

MD5 fe495981709d430e806fb217903e07bf

SHA1 de1dd0071972156dc713b7a868018f72c725b649

SHA256 0dc6c8331b3ea5d01295d602696a7ba3d58aa730b66f361accc6a742cd75a514

File type ZIP

File size 8.79 MB

В этот раз пароль от msimg32.dat — это superpass. Пароль superpass использовался TeamSpy в подключениях к зараженным устройствам. Других существенных отличий замечено не было.

Заключение

Исследование ProхуСВ показало, что речь идет не о примитивном боте, а о развитой ботнет-платформе с собственной серверной логикой, панелью управления,

административным бинарным протоколом и устойчивой инфраструктурой распространения.

В ходе анализа удалось связать между собой сетевую активность, устройство вредоносного клиента, серверное ядро и используемые домены, а также выявить возможные пересечения с инструментарием TeamSpy.

Все это указывает на длительное развитие проекта, его устойчивость и способность адаптироваться к изменениям, что, вероятно, позволило ему сохранять активность многие годы и увеличивать количество зараженных узлов.

IoC

Files

MD5

1bad7d07ae90b906e8f744146fdd8c12
6448d436b95b460b6cfb896f9f0fd6a7
1aaf34496209cbd8d5cfb5b932fd0591
4ba2b00487028565829b3abef8b8495a
de237777518dc9c0b7a03c536746d878
95b0e9fcc1025661b6550866d253f6ba
95a57385cfd1870391538c9d791aeaa
9938bb672128f111fa050251d340b008
630064446d988fb8fd9993855ff3f1
cedf8a321ef594fc6ccaa0164001c945
6cf2f25edf83d9e662c385255b473953
915d049345f416bbbd81f3b56d309cd0
bc373714afa689e64d3f248260089cfa
74eefba5d93380e05a66333a5ed9866a
39988c3a8099d5f188751c2e500e6259
6c721f65384687ca25c952597c10bbb7
97231c24b8a7bb48a05d51760f68ef01
5fe66eb2c7b221b334c30b2260e20447
6c491796d2921da1f8dfad182dc6e33e
b99fe489a109498ed19227f76bb40c52
245132ff6ef9a9864069d71b86b285c2
ce66e63723c96ed705c07ff0015e171e
ed72de2c066a58bae0f4a7da5838fbfc

SHA1

44f49b416764edcbe2b9b4a428ee1beaacf76a7b
3629c84165945e7c67ee172e943a0aaaa9d91f5a
1c42f0bbf3c9055c3d20513edc2b69e95df22aa2
d54f13e14b91dc89a18431c9f0b413d4e3db96d4
a357466573e35d634a119b7f2e7a8a18f5018811
e8db6d571a5c243e9c8c2c402a44fb72b768245c
1bd4e4f7832dcd96e52a90b4ed5fe77d8036ec2e
7d9a125013b0726bd9b56b324eb4c7f868c7c1d8
9f1a0d635cd8af4eda188a2c53f08673ec5bc908
511354dfae2b02881fbcbbd6967b2a1468daf2ba
1ab8d0535b2ad173f00a80822f9855c4424cac67
593699f27883c94cf515853e47d2ebccda78bc69
f7e21cbc854e8d6ed8a5df8a0da08ca0f560d1ff
4e725bf77b56cf072a75f447e1c35f0bdc6a2b2a
2ff0c8eae79a8a968fd4f6e0a76c720196f5b36b
eef741044da953f30f91fde22a8309925890e9d1
eb0285af5c7e8bfa8f4e3022f9f03c796bb1ded1
963da37b1ee363f924c1f267cb3004ed5e997a40
1e0b35768b6cf5fdbafb7f2a919469306e87aa7c
074a9ea5ae0f825f5c9b596cfff95252c414a07e
4aaba2a1c2a0e3599a97e5ad837a37e351be326e
769496fbdd02934a7362bcd26c62f8e6cb4d7a86
68c0122742c89aa39da3bed36b9384f7cb64928e

SHA256

173463717e7833c4ed00225ba8cb041d13352778ef22462713e44e3845be6e82
ccd387acb8347ba8ed81d48c115bb40ef43a527a748ffbc78595022a8002cbda
5a43aaf1d8b274c6b41cccead680c9fbd1c2065c5bdac9a65fd3f4f31bd70413
004bf4aa9704664a23dc60721447fc5f17d11855a122365a6835fae868f5eb8c
23c6e8163646ba03c0a5c6dcdff0f0df5688ec4a91c8bd9b663888440254bc12f
6c7495d88efe39e0cd2685a120595d467e7b74e6fd64c828cf0bb6fb7207e704
7440cc0613ad6b8bb08601d42a0830c42f0965c59af3270d5845c256c334397d
f135d690e37b444f7d5a06e36cf68ea7b344e4a66da35e3937171e7a8cf94b75
600b74b215a7b031e7db0e56339032c953d663ccd2deafdc36b682f2cbd2a22a
9236c0d8ac5bac35c686356b7c1fa454078921b91c97783193169636978f268a
ecbb0051cb5e1cc71c638feca660b256903c46603f5295d43c906383b76cf121
fcc5d2361fc0bb2b9c12cac6e7d6d20cf96a02307f2f0c04d1cde84c5326d701

b090ddd90b9c15c5d12236b206d0265789211888c4828282964ee0397a162356
c81f9d4071c353959cde13da2c318c37eeb206fc5347b00011dc52e3bbc4c5e3
6e8edb920d0c68032a165ab3d4a2b43bf348a6b983b788a89ce9e1b0cf474678
f1d5d12bdf95e72e829530784280789a68230cba54e7e8eb3810ea162ad9b122
dffbd79a8bdfcfa5cfe1bdd49c4dc6a1f4a7dd8396d7f75e6ff95c3cee5741d6
33e83b7c18def5e0efebed50d86f45420531b82baf625972c7a9c961c0656044
38a9b8f54902b67132a21614652f728d72be70c3e1a0702659a882307bd2c3be
5d44f21b4a98a42b58a94233af3be2ae54dd6459e733310b02b01d17978dd5f5
08aae0a6003b46aa31c34fe4c64a3227c446b94df026ec5cda27ac092ab600b3
b8976b7cfea692aa77d580d1c03c1e9da4b44cb5cbde18ea3a9c587cdf61f79b
bbc42673786c572c253b3ead897170eb1f3f9f9b1616783ea024f831ff167bda

C2

kilo-torrent.org
kilotorrent.org
ndrpotoki.xyz
rdnmanerr.xyz
rdnmaner.xyz
torrent-trecker4.com
upteambuilding.com
kilo-torrent.ru
aktivator-dlya-windows-10.com
torrenta.top
exe-craft.ru

Арден Трейс

Содержание статьи

Получать новости

-
-

Аналитический отчет по целевым кибератакам за 2025 год

[Читать](#)