Ботнет Stantinko додає до інструментарію можливість майнінгу криптовалюти

ESET НАСОЛОДЖУЙСЯ БЕЗПЕКОЮ

Дослідники ESET виявили, що кіберзлочинці, які стоять за ботнетом Stantinko, розповсюджують модуль для майнінгу криптовалюти на контрольовані ними комп'ютери.

Оператори ботнету Stantinko додали до свого набору інструментів новий спосіб отримання прибутку з використанням комп'ютерів, які перебувають під їх контролем. Приблизно півмільйонний ботнет, який, як відомо, був активним щонайменше з 2012 року і в основному націлений на користувачів Росії, України, Білорусі та Казахстану, зараз поширює модуль для майнінгу. Майнінг криптовалюти Monero, обмінний курс якої коливається в 2019 році від 50 до 110 доларів США, є функцією монетизації ботнету щонайменше з серпня 2018 року.

У цьому матеріалі спеціалісти ESET опишуть модуль Stantinko для майнінгу та проаналізують його функціонал.

Особливістю цього модуля є спосіб заплутування коду для запобігання аналізу та уникнення виявлення. Завдяки використанню маскування на рівні джерела із частиною випадковості та тому, що оператори Stantinko компілюють цей модуль для кожної нової жертви, кожен зразок є унікальним.

Оскільки Stantinko постійно розробляє нові та вдосконалює існуючі спеціальні маскувальники та приховані модулі, важко відстежити кожне незначне вдосконалення та зміни. Тому спеціалісти ESET вирішили описати сам модуль та тільки суттєві корективи порівняно з попередніми зразками.

Модифікований криптомайнер з відкритим кодом

Модуль Stantinko для майнінгу криптовалют, який витрачає більшість ресурсів компрометованої машини на видобуток криптовалюти, є модифікованою версією криптомайнера з відкритим кодом – xmr-stak. Для уникнення виявлення було видалені усі непотрібні рядки і функції. Рядки і функції, які залишилися, були заплутані. Продукти ESET виявляють це шкідливе програмне забезпечення як Win{32,64}/CoinMiner.Stantinko.

Використання проксі для майнінгу

CoinMiner.Stantinko з'єднується зі своїм майнінг-пулом не безпосередньо, а через проксі, IP-адреси якого отримані з тексту опису YouTube відео. Аналогічну техніку приховування даних в описах відео YouTube використовує банківське шкідливе програмне забезпечення Casbaneiro. Однак ця загроза використовує на вигляд більш легітимні канали та описи, але з тією ж метою – зберігання зашифрованих командних серверів (C&C).

Опис такого відео складається з рядка, створеного з проксі-адрес для майнінгу у шістнадцятковому форматі. Наприклад, відео YouTube, показане на малюнку 1, має опис "03101f1712dec626", що відповідає двом IP-адресам у шістнадцятковому форматі – `03101f17` відповідає 3.16.31[.]23 у десятковому форматі, а `12dec626` – 18.222.198[.]38. На момент написання матеріалу формат був дещо скорегований. Наразі IP-адреси прикріплені до "!!!!", що спрощує сам процес розбору та запобігає можливим змінам HTML-структури відео YouTube, що перетворюють аналізатор в нефункціональний.

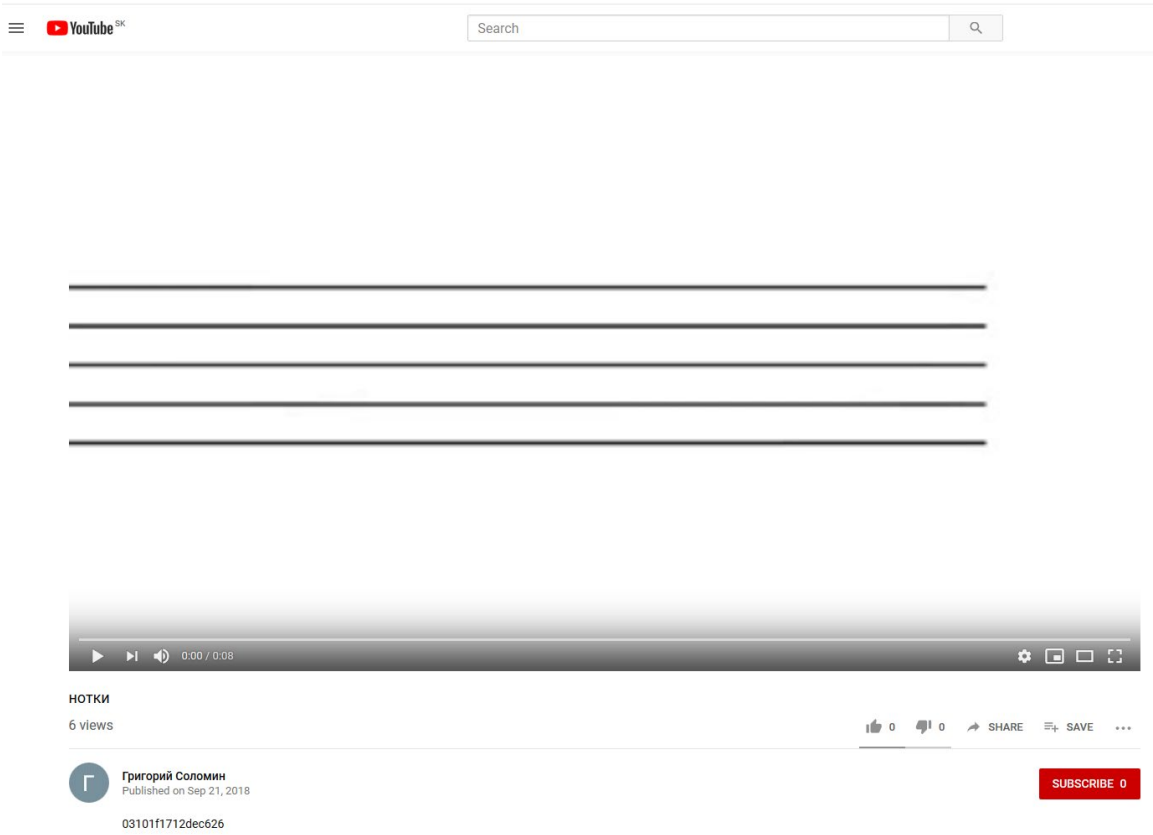

Рисунок 1. Приклад YouTube відео, опис якого містить IP-адресу для з'єднання модуля з майнінг-пулом

У попередніх версіях URL-адресу YouTube було закодовано у бінарному файлі CoinMiner.Stantinko. На даний час модуль натомість отримує відео-ідентифікатор як параметр командного рядка. Цей параметр потім використовується для побудови URL-адреси YouTube у формі `https://www.youtube.com/watch?v=%PARAM%`. Модуль майнінгу криптовалюти виконується або компонентом BEDS Stantinko, або `rundll32.exe` через пакетний файл, при цьому модуль завантажується з локальної файлової системи у формі `%TEMP%\%RANDOM%\%RANDOM_GUID%.dll`.

Спеціалісти ESET повідомили YouTube про цей випадок використання; діяльність всіх каналів, що містять ці відео, були припинена.

Можливості майнінгу криптовалюти

Спеціалісти ESET розділили модуль для майнінгу криптовалюти на чотири логічні частини, які представляють різні набори можливостей. Основна частина виконує майнінг криптовалюти; інші частини модуля відповідають за додаткові функції:

- призупинення інших (конкурентних) програм для майнінгу криптовалюти
- виявлення програмного забезпечення з безпеки
- призупинення функції майнінгу криптовалюти, якщо ПК працює від батареї або коли виявлено диспетчер задач, щоб запобігти виявленню користувачем

Майнінг криптовалюти

В основі функції майнінгу криптовалюти лежить процес хешування та з’єднання з проксі. Спосіб отримання списку проксі для майнінгу описаний вище; CoinMiner.Stantinko з’єднується з першим знайденим проксі для майнінгу.

Це з’єднання відбувається через TCP та шифрується RC4 з ключем, що складається з перших 26 символів числа «пі» (включаючи десяткові значення, тобто «3,14159265358979323846264 3»), а потім кодується base64; той самий ключ використовується у всіх зразках, які зафіксовані раніше.

Код алгоритму хешування завантажується з проксі для майнінгу на початку з’єднання та завантажується в пам'ять — безпосередньо або в попередніх версіях з бібліотеки `libcr64.dll`, яка вперше потрапляє на диск.

Завантаження коду хешування з кожним виконанням дозволяє групі Stantinko змінити цей код під час процесу. Ця зміна дає можливість, наприклад, адаптуватися до коригування алгоритмів у існуючих валютах та перейти до майнінгу інших криптовалют з метою найвигіднішого видобутку криптовалюти на момент виконання. Основна перевага завантаження основної частини модуля з віддаленого сервера та завантаження його безпосередньо в пам'ять полягає в тому, що ця частина коду ніколи не зберігається на диску. Це додаткове коригування, якого немає в попередній версії, спрямоване на ускладнення виявлення, оскільки шаблони в цих алгоритмах легко виявляються продуктами з безпеки.

Усі зразки модуля Stantinko для майнінгу, проаналізовані спеціалістами ESET, видобували криптовалюту Monero. Це стало відомо з завдань, виконаних проксі для майнінгу та алгоритмом хешування. Наприклад, рис. 2 — це завдання, надіслане одним із проксі.

{"error":null,"result":{"status":"OK"}}

{"method":"job","params":{"blob":"0b0bbfdee1e50567042dcfdfe96018227f25672544521f8ee2564cf8b4c3139a6a88c5f0b32664000000a1c8ee5c185ed2661daab9d0c454fd40e9f53f0267fe391bdb4eb4690395deb36018","job_id":"281980000000000a10","target":"67d81500","height":1815711}}

Рис. 2. Приклад майнінгу, отриманого від проксі-сервера для майнінгу

Спеціалісти ESET проаналізували використаний алгоритм хешування і виявили, що це CryptoNight R. Оскільки існує декілька криптовалют, які використовують цей алгоритм, тільки його розпізнання недостатньо. Висота блокчейну на той момент становила 1815711, тому спеціалістам ESET довелося знаходити валюти з використанням CryptoNight R з такою висотою на спеціалізованих оглядачах блоків, які привели до Monero. Аналіз рядка

`0b0bbfdee1e50567042dcfdfe96018227f25672544521f8ee2564cf8b4c3139a6a88c5f0b32664000000a1c8ee5c185ed2661daab9d0c454fd40e9f53f0267fe391bdb4eb4690395deb36018` показує, що хеш попереднього блоку (`67042dcfdfe96018227f25672544521f8ee2564cf8b4c3139a6a88c5f0b32664`) та відмітка часу (`1555590859`) дійсно вписується в блокчейн Monero на висоті 1815711. Можна знайти структуру масиву двійкових даних шляхом дослідження функції генератора у вихідному коді Monero. Функція генератора розкриває іншу структуру, яку називають заголовком блоку, яка містить і хеш попереднього блоку, і часову позначку.

На відміну від решти CoinMiner.Stantinko, алгоритм хешування не заплутаний, оскільки це значно погіршить швидкість обчислення хешу та загальну ефективність та прибутковість. Однак автори все ж переконалися, що не залишають позаду жодних значущих рядків чи артефактів.

Припинення діяльності інших криптомайнерів

Шкідливе програмне забезпечення перераховує запущені процеси пошуку інших криптовалют. У разі знайдення конкурентів Stantinko призупиняє всі їхні дії.

CoinMiner.Stantinko розпізнає процес криптомайнера, якщо його командний рядок містить певний рядок або комбінацію, яка варіюється залежно від зразка, наприклад:

- minerd
- minergate
- xmr
- cpservice
- vidservice та stratum+tcp://
- stratum://
- -u та pool
- "-u та pool
- "-u та xmr
- -u та xmr
- -u та mining
- "-u та mining
- -encodedcommand та powershell.exe
- --donate-level
- windows та -c та cfgi
- regsvr32 та /n та /s та /q
- application data та svchost.exe
- appdata та svchost.exe

Ці рядки стосуються таких легітимних криптомайнерів: https://github.com/pooler/cpuminer, https://minergate.com/, https://github.com/xmrig та навіть https://github.com/fireice-uk/xmr-stak , який і є тим майнером, на якому базується модуль Stantinko. Рядки також приводять до інших зразків шкідливого програмного забезпечення, які містять функцію майнінгу криптовалюти.

Цікавим є той факт, що оператори Stantinko, як відомо, намагалися позбутися конкуруючого коду в минулому. Однак вони покладалися на легітимний інструментарій AVZ Antiviral Toolkit, який надається зі сценарієм, написаним на його вбудованій сценарній мові для цього завдання.

Запобігання виявленню

CoinMiner.Stantinko тимчасово призупиняє майнінг у разі виявлення, що до пристрою не підключено джерело живлення. Ці дії, очевидно, що спрямовані на портативні комп'ютери, запобігають швидкому розряджанню акумулятора, що може викликати підозру у користувача.

Крім цього, він тимчасово призупиняє майнінг, якщо виявлена запущена програма диспетчера завдань (процес під назвою procexp64.exe, procexp.exe або taskmgr.exe).

Шкідливе програмне забезпечення також сканує запущені процеси, щоб знайти програмне забезпечення з безпеки та диспетчер завдань. Загроза обчислює CRC-32 назви процесу, а потім перевіряє його на наявність закодованого списку контрольних сум CRC-32, який міститься у Додатку. Взагалі цей метод допомагає уникнути виявлення, оскільки назви процесів цих продуктів з безпеки не входять в бінарні файли. Це також ускладнює виявлення авторів шкідливих програм, оскільки потрібно зламати ці хеші, що аналогічно процесу зламу пароля. Однак використання списку відомих імен процесів є достатнім для визначення точних імен.

У разі виявлення збігу з CRC-32, CRC записується у журнал файлу (api-ms-win-crt-io-l1-1-0.dll). Журнал файлу, ймовірно, пізніше перекреслюється іншим компонентом Stantinko, який спеціалісти ESET не зафіксували, оскільки в цьому модулі немає жодної іншої функції, пов'язаної з ним.

Обфускація (заплутування коду)

Крім особливостей майнінгу криптовалюти, CoinMiner.Stantinko відомий також методами обфускації (заплутування коду) з метою уникнення виявлення та перешкоджання аналізу. Деякі з цих методів є унікальними.

Висновок

Дослідження показує, що злочинці, які стоять за Stantinko, продовжують розширювати способи використання ботнетів, якими вони управляють. Їх попередніми новими техніками були атаки з використанням «підбору за словником» на веб-сайти Joomla та WordPress, які спрямовані на збирання облікових даних сервера, можливо, з метою їх продажу іншим злочинцям.

Цей дистанційно налаштований модуль для майнінгу криптовалюти розповсюджується щонайменше з серпня 2018 року та досі є активним. Група кіберзлочинців продовжує впроваджувати нові методи та розширювати свої можливості отримання прибутку. Крім стандартних функцій майнінгу криптовалюти, модуль використовує деякі цікаві методи заплутування коду, які спеціалісти ESET опишуть разом із деякими можливими способами захисту від подібних загроз у наступній статті.

Ідентифікатори компрометації

Продукти ESET виявляють загрозу як:

Win32/CoinMiner.Stantinko

Win64/CoinMiner.Stantinko

SHA-1

Повний список понад 1500 хешів доступний у репозиторії GitHub.

00F0AED42011C9DB7807383868AF82EF5454FDD8
01504C2CE8180D3F136DC3C8D6DDDDBD2662A4BF
0177DDD5C60E9A808DB4626AB3161794E08DEF74
01A53BAC150E5727F12E96BE5AAB782CDEF36713
01BFAD430CFA034B039AC9ACC98098EB53A1A703
01FE45376349628ED402D8D74868E463F9047C30

…Назви файлів

api-ms-win-crt-io-l1-1-0.dll

libcr64.dll

C:\Windows\TEMP\%RANDOM%\%RANDOM_GUID%.dll

Назва Mutex та ключ RC4

“3,14159265358979323846264 3”

Адреси YouTube із даними про налаштування проксі для майнінгу

- https://www.youtube[.]com/watch?v=kS1jXg99WiM
- https://www.youtube[.]com/watch?v=70g4kw2iRGo
- https://www.youtube[.]com/watch?v=cAW1xEpyr7Y
- https://www.youtube[.]com/watch?v=6SSKQdE5Vjo
- https://www.youtube[.]com/watch?v=fACKZewW22M
- https://www.youtube[.]com/watch?v=FDQOa5zCv3s
- https://www.youtube[.]com/watch?v=TpyOURRvFmE
- https://www.youtube[.]com/watch?v=2fpiR4NIpsU
- https://www.youtube[.]com/watch?v=TwnD0Kp_Ohc
- https://www.youtube[.]com/watch?v=wJsbj8zPPNs

IP-адреси проксі для майнінгу

- 3.16.150[.]123
- 3.16.152[.]201
- 3.16.152[.]64
- 3.16.167[.]92
- 3.16.30[.]155
- 3.16.31[.]23
- 3.17.167[.]43
- 3.17.23[.]144
- 3.17.25[.]11
- 3.17.59[.]6
- 3.17.61[.]161
- 3.18.108[.]152
- 3.18.223[.]195
- 13.58.182[.]92
- 13.58.22[.]81
- 13.58.77[.]225
- 13.59.31[.]61
- 18.188.122[.]218
- 18.188.126[.]190
- 18.188.249[.]210
- 18.188.47[.]132
- 18.188.93[.]252
- 18.191.104[.]117
- 18.191.173[.]48
- 18.191.216[.]242
- 18.191.230[.]253
- 18.191.241[.]159
- 18.191.47[.]76
- 18.216.127[.]143
- 18.216.37[.]78
- 18.216.55[.]205
- 18.216.71[.]102
- 18.217.146[.]44
- 18.217.177[.]214
- 18.218.20[.]166

- 18.220.29[.]72
- 18.221.25[.]98
- 18.221.46[.]136
- 18.222.10[.]104
- 18.222.187[.]174
- 18.222.198[.]38
- 18.222.213[.]203
- 18.222.253[.]209
- 18.222.56[.]98
- 18.223.111[.]224
- 18.223.112[.]155
- 18.223.131[.]52
- 18.223.136[.]87
- 18.225.31[.]210
- 18.225.32[.]44
- 18.225.7[.]128
- 18.225.8[.]249
- 52.14.103[.]72
- 52.14.221[.]47
- 52.15.184[.]25
- 52.15.222[.]174

Техніки MITRE ATT&CK

Тактика		**Назва**	**Опис**
	HYPERLINK "https:/		Модуль може бути виконаний як `rundll`
	HYPERLINK "https:/		Шкідливе програмне забезпечення може бути виконано як сервіс.
	HYPERLINK "https:/		Модуль здійснює заплутування рядків у своєму коді під час виконання процесу.
	HYPERLINK "https:/		Модуль заплутує код і рядки, намагаючись ускладнити аналіз та виявлення.

	HYPERLINK "https:/		Шкідливе програмне забезпечення отримує дані конфігурації з опису відео на YouTube.
	HYPERLINK "https:/		Шкідливе програмне забезпечення отримує список запущених продуктів з безпеки.
	HYPERLINK "https:/		Модуль використовує проксі для з’єднання з майнінг-пулом.
	HYPERLINK "https:/		Модуль під’єднується до іншого проксі для майнінгу, якщо початковий недоступний.
	HYPERLINK "https:/		Шкідливе програмне забезпечення використовує TCP для власних з’єднань.
	HYPERLINK "https:/		Шкідливе програмне забезпечення передається через порт 443.
	HYPERLINK "https:/		Модуль зашифровує, а потім base64 кодує певний мережевий трафік.
	HYPERLINK "https:/		Модуль шифрує трафік за допомогою RC4.
	HYPE		Отримує конфігураційні дані

	RLINK "https:/		з опису відео на YouTube через
	HYPERLINK "https:/		Модуль здійснює майнінг криптовалюти.

Додаток

Нижче наведено контрольні суми CRC-32, перевірені CoinMiner.Stantinko, та імена файлів, до яких вони прирівнюються.

0xB18362C7	afwserv.exe
0x05838A63	ashdisp.exe
0x36C5019C	ashwebsv.exe
0xB3C17664	aswidsagent.exe
0x648E8307	avastsvc.exe
0x281AC78F	avastui.exe
0xAA0D8BF4	avgcsrva.exe
0x71B621D6	avgcsrvx.exe
0x7D6D668A	avgfws.exe
0x1EF12475	avgidsagent.exe
0x010B6C80	avgmfapx.exe
0x6E691216	avgnsa.exe
0xB5D2B834	avgnsx.exe
0x36602D00	avgnt.exe
0x222EBF57	avgrsa.exe
0xF9951575	avgrsx.exe
0x2377F90C	avgsvc.exe
0x37FAB74F	avgsvca.exe
0xEC411D6D	avgsvcx.exe
0x0BED9FA2	avgtray.exe

0x168022D0	avguard.exe
0x99BA6EAA	avgui.exe
0x7A77BA28	avguix.exe
0x0D22F74A	avgwdsvc.exe
0x98313E09	avira.servicehost.exe
0x507E7C15	avira.systray.exe
0xFF934F08	avp.exe
0x9AC5F806	avpui.exe
0xBD07F203	avshadow.exe
0x64FDC22A	avwebg7.exe
0x0BC69161	avwebgrd.exe
0xBACF2EAC	cureit.exe
0x8FDEA9A9	drwagntd.exe
0xE1856E76	drwagnui.exe
0xF9BF908E	drwcsd.exe
0xC84AB1DA	drwebcom.exe
0x183AA5AC	drwebupw.exe
0xAC255C5E	drwupsrv.exe
0x23B9BE14	dwantispam.exe
0xDAC9F2B7	dwarkdaemon.exe
0x7400E3CB	dwengine.exe
0x73982213	dwnetfilter.exe
0x1C6830BC	dwscanner.exe
0x86D81873	dwservice.exe
0xB1D6E120	dwwatcher.exe
0xD56C1E6F	egui.exe
0x69DD7DB4	ekrn.exe
0xFB1C0526	guardgui.exe
0x5BC1D859	ipmgui.exe

0x07711AAE	ksde.exe
0x479CB9C4	ksdeui.exe
0x6B026A91	nod32cc.exe
0xCFFC2DBB	nod32krn.exe
0x59B8DF4D	nod32kui.exe
0x998B5896	procexp.exe
0xF3EEEFA8	procexp64.exe
0x81C16803	sched.exe
0x31F6B864	spideragent.exe
0x822C2BA2	taskmgr.exe
0x092E6ADA	updrgui.exe
0x09375DFF	wsctool.exe

*Дослідження подано в перекладі. Оригінал доступний за посиланням.