CERT-UA

Рекомендації
5 січня 2015

CUA-15-01M
Опис шкідливого програмного забезпечення Regin

Державна служба спеціального зв'язку та захисту інформації України
Державний центр захисту інформаційно-телекомунікаційних систем
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація 3
1.1 Вразливі системи 3
1.2 Інформація про Regin 3
2. Рекомендації 5
2.1 Загальні рекомендації 5
2.2 Ідентифікація загрози Regin 5
2.3 Сервери контролю та управління бот-мережами Regin 11
3. Корисні посилання 12

1. Загальна інформація

1.1 Вразливі системи

Regin загрожує 32- та 64-бітним версіям операційних систем сімейства Microsoft Windows NT, 2000, XP, Vista та 7.
За даними компанії зараженню підлягають переважно країни (не вичерпний перелік):

- Афганістан
- Алжир
- Бельгія
- Бразилія
- Фіджі
- Німеччина
- Індія
- Індонезія
- Іран
- Кірібаті
- Малайзія
- Пакистан
- Російська Федерація
- Сирія

1.2 Інформація про Regin

Шкідливе програмне забезпечення, що має умовну назву Regin, найбільш вірогідно розроблене іноземними спецслужбами (за даними деяких дослідників - США та Великобританії), для шпигунських цілей та класифікується, як троян з функціями віддаленого доступу (remote access Trojan (RAT)). Модульність складу Regin, широкий функціонал, варіативність поведінки та складність роботи (велика кількість різноманітних векторів атак та широке розповсюдження по країнах світу) дозволяють зробити припущення про велику вартість проекту та його довге існування (орієнтовно, з 2009 року).

Regin, частіше за все, реалізує таргетовані (підлаштовані під кожну окрему жертву) атаки, тобто реалізує APT.

Функціонал загрози

Regin має наступні функціональні (на поточний момент досліджені) можливості:

- організація віддаленого доступу до зараженої системи
- отримання контролю за пристроями вводу-виводу
- перехоплення даних, що вводяться (keylogger, screenshotting)
- відновлення видалених файлів
- перехоплення мережевих інформаційних потоків
- збір даних щодо функціонуючих процесів та використання пам'яті
- збір команд та всієї активності базових станцій сотового зв'язку формату GSM
- організація p2p-мереж заражених систем (розподіл функцій між ними)
- модульність складу та широкий функціонал

Хронологія

- онлайн-сервіс Virustotal.com ідентифікує перші зразки компонентів Regin 07.2008 у звіті
- 9 березня 2011 року вперше викладено інформацію на Malware Encyclopedia компанії Microsoft про один з видів Regin — Regin.A
- 12 грудня 2013 року компанія Symantec опублікувала звіт щодо Regin, який 24 листопада 2014 року оновлено та доповнено
- 24 листопада 2014 про Regin опубліковано звіт антивірусної компанії Kaspersky Lab
- 25 листопада 2014 року американська команда швидкого реагування оприлюднила опис загрози Regin (Alert (TA14-329A))

2. Рекомендації

2.1 Загальні рекомендації

Користувачам та адміністраторам рекомендується вжити наступних превентивних дій для захисту від Regin мереж та систем:

- використовувати та оновлювати антивіруси для захисту від відомих вірусів (детальніше про це читайте тут)
- вчасно оновлювати операційну систему та програмне забезпечення, призначене для захисту (детальніше про це читайте тут)
- спробувати ідентифікувати наявність Regin за відомими ознаками компрометації (Indicators of Compromise (IOCs)), наведеними в п. 2.2

2.2 Ідентифікація загрози Regin

Відомі 5 стадій шкідливого коду, що реалізують Regin:

- **Стадія 1**: дропер (первинний злом та завантаження Regin)
- **Стадія 2**: завантажувач (loader) 1 рівня (необхідні драйвери)
- **Стадія 3**: завантажувач 2 рівня
- **Стадія 4**: динамічна бібліотека рівня ядра операційної системи (реалізація компресії даних, криптографічного захисту, мережевої взаємодії компонентів, управління файловою системою EVFS тощо)
- **Стадія 5**: оркестратор (модуль координації інших модулів, користування EVFS та завантаження інших модулів, в тому числі, модулів функціоналу (payload)

На кожному з етапів є характерні ідентифікатори компрометації, наведені нижче.

Стадія 1

Наступні **md5-суми файлів** є ідентифікаторами компрометації для стадії 1 (дроперу у 32- та 64-бітних операційних системах):

01c2f321b6bfdb9473c079b0797567ba

06665b96e293b23acc80451abb413e50

187044596bc1328efa0ed636d8aa4a5c

1c024e599ac055312a4ab75b3950040a

26297dc3cd0b688de3b846983c5385e5

2c8b9d2885543d7ade3cae98225e263b

47d0e8f9d7a6429920329207a32ecc2e

4b6b86c7fec1c574706cecedf44abded

6662c390b2bbbd291ec7987388fc75d7

744c07e886497f7b68f6f7fe57b7ab54

b269894f434657db2b15949641a67532

b29ca4f22ae7b7b25f79c1d4a421139d

b505d65721bb2453d5039a389113b566

ba7bb65634ce1e30c1e5415be3d1db1d

bfbe8c3ee78750c3a520480700e440f8

d240f06e98c8d3e647cbf4d442d79475

db405ad775ac887a337b02ea8b07fddc

ffb0b9b5b610191051a7bdf0806e1e47

Отримати дані щодо md5-суми файлу та того, як його ідентифікує велика кількість антивірусів, можливо шляхом використання однієї з наявних md5-сум, наприклад, на сайті virustotal.com (Рис. 1):

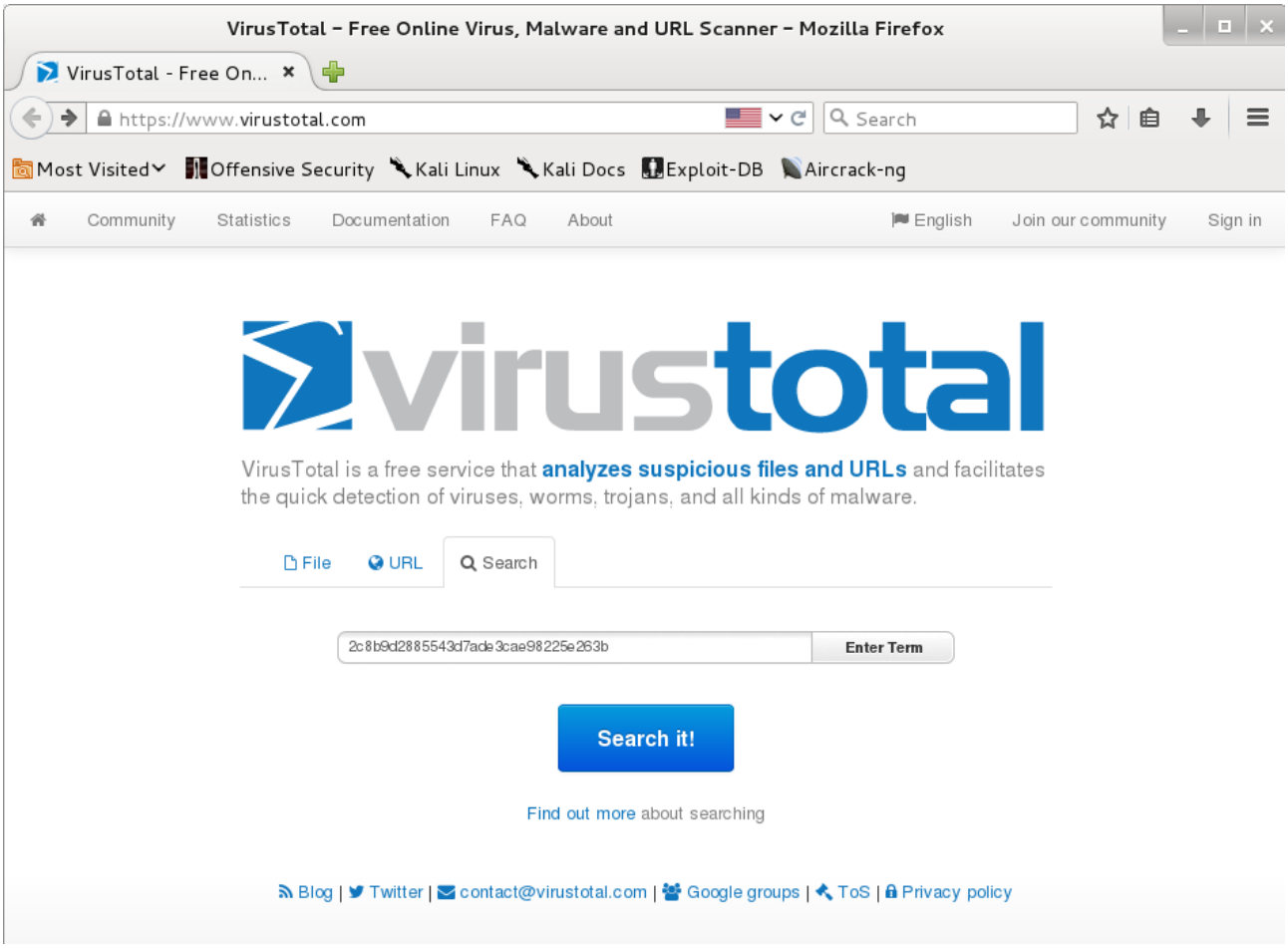

Рис. 1

Стадія 2

Наступні імена файлів та шляхи є ідентифікаторами компрометації для стадії 2 (loader) для **32-бітних** операційних систем:

18d4898d82fcb290dfed2a9f70d66833

b9e4f9d32ce59e7c4daf6b237c330e25

На Стадії 2 створюються маркери у вигляді файлів:

%SYSTEMROOT%\system32\nsreg1.dat

%SYSTEMROOT%\system32\bssec3.dat

%SYSTEMROOT%\system32\msrdc64.dat

Наступні **імена файлів та шляхи** є ідентифікаторами компрометації для стадії 2 (loader) для **64-бітних** операційних систем:

d446b1ed24dad48311f287f3c65aeb80

Стадія 3

Наступні **імена файлів та шляхи** є ідентифікаторами компрометації для стадії 3 (kernel mode manager “VMEM.sys”) для **32-бітних** операційних систем:

8486ec3112e322f9f468bdea3005d7b5

da03648948475b2d0e3e2345d7a9bbbb

Наступні ключі реєстру є ідентифікаторами компрометації:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\RestoreList\VideoBase

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA5A}

\REGISTRY\Machine\System\CurrentControlSet\Control\RestoreList

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{39399744-44FC-AD65-474B-E4DDF-8C7FB97}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{3F90B1B4-58E2-251E-6FFE-4D38C5631A04}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{4F20E605-9452-4787-B793-D0204917CA58}

\REGISTRY\Machine\System\CurrentControlSet\Control\Class\{9B9A8ADB-8864-4BC4-8AD5-B17DFDBB9F58}

Для 64-бітних Windows-систем стадія 3 відсутня. Замість неї на стадії 2 диспетчер завантажується та запускається з диску завантажувачем (без kernel mode manager “VMEM.sys”).

Стадія 4

Стадія 4 (для 32-бітних систем)/стадія 3 (для 64-бітних систем) має наступні **md5-суми файлів** у якості ідентифікаторів компрометації:

32-бітні системи:

1e4076caa08e41a5befc52efd74819ea

68297fde98e9c0c29cecc0ebf38bde95

6cf5dc32e1f6959e7354e85101ec219a

885dcd517faf9fac655b8da66315462d

a1d727340158ec0af81a845abd3963c1

64-бітні системи:

de3547375fbf5f4cb4b14d53f413c503

Найбільш цікавий контент та дані щодо функціоналу Regin на поточний час наявний з **контейнерів**, закритих у закодованих у EVFS (за даними компанії Kaspersky їх отримано 24 з різних країн світу). Ці контейнери, зазвичай, мають довільні імена та розташовані у наступних папках операційної системи:

Папка на диску	**Ім'я файлу**	**Опис**
C:\Windows\System32\config\	SystemAudit.Evt, SystemLog.Evt, SecurityLog.Evt, SecurityAudit.Evt, CACHE, SESSIONMGR	Дані щодо аудиту операційної системи (стара версія Regin)
C:\Windows\System32\	UsrClass.dat	Дані щодо аудиту користувачів системи (стара версія Regin)
C:\WINDOWS\pchealth\helpctr\Database	cdata.dat, cdata.edb	Дані щодо з'єднань системи (стара версія Regin)
C:\Windows\System32\config\	UsrEvent.evt, ApplicationLog.Evt	Дані щодо подій всередині віртуальної файлової системи , побудованої на базі Regin (скоріш за все — журнал взаємодії між ботами)
C:\Windows\Panther\	setup.etl.000	Тільки для 64-бітних систем
C:\Windows\System32\wbem\repository\	INDEX2.DATA, OBJECTS2.DATA	Шифрування нового типу, з травня 2014 року
C:\Windows\System32\	dnscache.dat, mregnx.dat, displn32.dat, dmdskwk.dat, nvwrsnu.dat, tapiscfg.dat	Шифрування нового типу, з травня 2014 року

2.3 Сервери контролю та управління бот-мережами Regin

Виявлені та ідентифіковані наступні сервери контролю та управління бот-мережами Regin:

IP-адреса серверу контролю та управління (C&C)	Місцезнаходження	Опис
61.67.114.73	Taichung, Taiwan	Chwbn
202.71.144.113	Chetput, India	Chennai Network Operations (team-m.co)
203.199.89.80	Thane, India	Internet Service Provider
194.183.237.145	Brussels, Belgium	Perceval S.a.

Цікавим фактом, виявленим дослідниками Regin, стало те, що заражені системи у одній з країн ближнього сходу, що належали адміністрації президента, банківським, науково-освітнім та комерційним установам, обмінювались між собою зашифрованими каналами інформацією та мали сервер контролю та управління в Індії. Це робить команди, які передаються зараженим Regin системам, не доступні нікому, крім саме цього ботнету. Таке є ознакою цільового використання Regin проти певної країни та APT.

УВАГА!

Якщо Ви отримуєте позитивний результат у ході перевірок наявності на Вашій системі однієї з ознак компрометації, що характерні для Regin, будь-ласка зв'яжіться з нами та повідомте про цей випадок!
Це важливо не тільки для нас і Вас, а й для інших користувачів українського сегменту мережі Інтернет, установ і організацій різних секторів.

3. Корисні посилання

[1]https://www.virustotal.com/en/file/b12c7d57507286bbbe36d7acf9b34c22c96606ffd904e3c23008399a4a50c047/analysis/

[2]http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Trojan%3AWinNT%2FRegin.A#tab=1

[3]http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

[4]http://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

[5] https://www.us-cert.gov/ncas/alerts/TA14-329A

[6] https://www.us-cert.gov/ncas/tips/ST04-005

[7] https://www.us-cert.gov/ncas/tips/ST04-006

Зміни до документу

- 05.01.2015 – перший випуск.