Рекомендації Служби безпеки України щодо захисту комп’ютерів від кібератаки вірусу-вимагача

29.06.2017 09:20

[1]

За даними СБУ, інфікування операційних систем переважно відбувалося через відкриття шкідливих додатків (документів Word, PDF-файлів), які були надіслані на електронні адреси багатьох комерційних та державних структур.

Атака, основною метою якої було розповсюдження шифрувальника файлів Petya.A, використовувала мережеву вразливість MS17-010, внаслідок експлуатації якої на інфіковану машину встановлювався набір скриптів, що використовували зловмисники для запуску згаданого шифрувальника файлів.

Вірус атакує комп'ютери під управлінням ОС Microsoft Windows шляхом шифрування файлів користувача, після чого виводить повідомлення про перетворення файлів з пропозицією здійснити оплату ключа дешифрування у біткоїнах в еквіваленті суми $300 для розблокування даних. На сьогодні зашифровані дані, на жаль, розшифруванню не підлягають. Триває робота над можливістю дешифрування зашифрованих даних. Не виплачувати здирникам кошти, які вони вимагають - оплата не гарантує відновлення доступу до зашифрованих даних.

Рекомендації:

Якщо комп’ютер включений і працює нормально, але ви підозрюєте, що він може бути заражений, ні в якому разі не перезавантажуйте його (якщо ПК вже постраждав – також не перезавантажуйте його) – вірус спрацьовує при перезавантаженні і зашифровує всі файли, які містяться на комп’ютері.
Збережіть всі файли, які найбільш цінні, на окремий не підключений до комп’ютера носій, а в ідеалі – резервну копію разом з операційною системою.
Для ідентифікації шифрувальника файлів необхідно завершити всі локальні задачі та перевірити наявність наступного файлу : C:\Windows\perfc.dat
Залежно від версії ОС Windows встановити патч з ресурсу: https://technet.microsoft.com/ru-ru/library/security/ms17-010.aspx [2], а саме:
- для Windows XP - http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb401... [3]

- для Windows Vista 32 bit - http://download.windowsupdate.com/d/msdownload/update/software/secu/2017... [4]

-для Windows Vista 64 bit -

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017... [5]

- для Windows 7 32 bit -
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017... [6]

- для Windows 7 64 bit -
http://download.windowsupdate.com/d/msdownload/update/software/secu/2017... [7]

- для Windows 8 32 bit -
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017... [8]

- для Windows 8 64 bit -
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017... [9]

- для Windows 10 32 bit -
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017... [10]

- для Windows 10 64 bit -
http://download.windowsupdate.com/c/msdownload/update/software/secu/2017... [11]

Знайти посилання на завантаження відповідних патчів для інших (менш розповсюджених та серверних версій) ОС Windows можна за адресою: https://technet.microsoft.com/ru-ru/library/security/ms17-010.aspx [2]

5. Переконатися, що на всіх комп'ютерних системах встановлене антивірусне програмне забезпечення функціонує належним чином та використовує актуальні бази вірусних сигнатур. За необхідністю встановити та оновити антивірусне програмне забезпечення.

6. Для зменшення ризику зараження, слід уважно відноситися до всієї електронної кореспонденції, не завантажувати та не відкривати додатки у листах, які надіслані з невідомих адрес. У випадку отримання листа з відомої адреси, який викликає підозру щодо його вмісту — зв’язатися із відправником та підтвердити факт відправки листа.

7. Зробити резервні копії усіх критично важливих даних.

8. Коли користувач бачить «синій екран смерті», дані ще не зашифровані, тобто вірус ще не дістався до головної таблиці файлів. Якщо комп’ютер перезавантажуються і запускає check Disk, негайно вимикайте його. На цьому етапі ви можете витягнути свій жорсткий диск, підключити його до іншого комп’ютера (тільки не у якості завантажувального тому) і скопіювати файли.

9. Для унеможливлення шкідливим ПЗ змінювати MBR (в якому в даному випадку і записувалась програма-шифрувальник) рекомендується встановити одне з рішень по забороні доступу до MBR:

• рішення Cisco Talos https://www.talosintelligence.com/mbrfilter [12], вихідні коди доступні тут https://github.com/Cisco-Talos/MBRFilter; [13]

• зріле рішення Greatis http://www.greatis.com/security/; [14]

• свіже рішення SydneyBackups https://www.sydneybackups.com.au/sbguard-anti-ransomware/ [15].

Довести до працівників структурних підрозділів зазначену інформацію та рекомендації, не допускати працівників до роботи із комп’ютерами, на яких не встановлено вказані патчі, незалежно від факту підключення до локальної чи глобальної мереж.

Слід ззначити, що існує можливість спробувати відновити доступ до заблокованого зазначеним вірусом комп’ютера з ОС Windows.

Оскільки зазначене ШПЗ вносить зміни до MBR запису із-за чого замість завантаження операційної системи користувачу показується вікно з текстом про шифрування файлів.

Ця проблема вирішується відновленням MBR запису. Для цього існують спеціальні утиліти. Можна використати для цього утиліту «Boot-Repair». Інструкція https://help.ubuntu.com/community/Boot-Repair [16]

Потрібно завантажити ISO образ «Boot-repair» https://sourceforge.net/p/boot-repair-cd/home/Home/ [17]

Потім за допомогою однієї з вказаних в інструкції утиліт створюємо Live-USB (можна використовувати Universal USB Installer).

Завантажитись зі створеної Live-USB та далі слідувати інструкції з відновлення MBR запису.

Після цього Windows завантажується нормально. Але більшість файлів з розширеннями doc, dox, pdf, і т.д. будуть зашифровані. Для їх розшифрування потрібно чекати поки буде розроблено дешифратор, радимо завантажити потрібні зашифровані файли на USB-носій або диск для подальшого їх розшифрування та перевстановити операційну систему.

З досвіду СБУ, в окремих випадках відновити втрачену інформацію можна за допомогою програми ShadowExplorer, але це стане можливим лише тоді, коли в операційній системі працює служба VSS (Volume Shadow Copy Service), яка створює резервні копії інформації з комп’ютера. Відновлення відбувається не шляхом розшифрування інформації, а за допомогою резервних копій.

Додатково до зазначених рекомендацій можна скористатися рекомендаціями антивірусних компаній:

I. https://eset.ua/download_files/news/ESET_Recommendations_v2.0.pdf [18]

1. Якщо інфікований комп’ютер увімкнений, не перезавантажуйте та не вимикайте його!

a) Виконайте створення логу за допомогою програми ESET Log Collector: Завантажте утиліту ESET Log Collector: http://eset.ua/ua/download/utility?name=logcollector [19] Переконайтеся в тому, що встановлені всі галочки у вікні «Артефакти для збору». У вкладці «Режим збору журналів ESET» встановіть: «Вихідний двійковий код із диска». Натисніть на кнопку: «Зібрати». Надішліть архів з журналами на електронну адресу support@eset.ua [20].

b) У продуктах ESET увімкніть сервіс ESET Live Grid, а також виявлення потенційно небажаних та небезпечних додатків. Дочекайтеся оновлення сигнатур до версії 15653 та проскануйте ПК.

2. Якщо комп’ютер вимкнений, не вмикайте його! Для збору інформації, яка допоможе написати декодер, перейдіть до виконання пункту 3, для сканування системи перейдіть до пункту 4.

3. З уже інфікованого комп'ютера (який не завантажується) потрібно зібрати MBR для подальшого аналізу. Зібрати його можна за допомогою цієї інструкції: • Завантажте ПК з ESET SysRescue Live CD або USB (створення описано в Додатку 1). • Надайте згоду з умовами ліцензії використання. • Натисніть CTRL+ALT+T (відкриється термінал). • Напишіть команду

"parted -l" без лапок, параметром є маленька буква "L" та натисніть . • Перегляньте список дисків та ідентифікуйте заражений (повинен бути один з /dev/sda). • Введіть команду "dd if=/dev/sda of=/home/eset/petya.img bs=4096 count=256" без лапок, замість "/dev/sda" використовуйте диск, який визначили в попередньому кроці, та натисніть (файл /home/eset/petya.img буде створений). • Підключіть USB-флешку і скопіюйте файл /home/eset/petya.img. • Комп'ютер можна вимкнути. • Надішліть файл petya.img на електронну адресу support@eset.ua [20].

II. http://zillya.ua/ru/epidemiya-zarazhenii-svyazana-s-deistviem-wannacry [21]

Методи протидії зараженню:

Відключення застарілого протоколу SMB1. Інструкція з відключення SMB1 в TechBlog компанії Microsoft: https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ [22]
Установлення оновлень безпеки операційної системи Windows з Microsoft Security Bulletin MS17-010: https://support.microsoft.com/en-us/help/4013389/title [23]
Якщо є можливість відмовитися від використання в локальній мережі протоколу NetBios (не використовувати для організації роботи мережеві папки і мережеві диски), в Брандмауері локальних ПК і мережевого обладнання заблокувати TCP/IP порти 135, 139 та 445
Блокування можливості відкриття JS файлів, отриманих електронною поштою.
III. https://www.symantec.com/ [24]

За рекомендаціями антивірусної компанії Symantec, для встановлення факту зараження комп’ютеру шифрувальником файлів, необхідно завершити всі локальні задачі та перевірити наявність наступного файлу C:\Windows\perfect/

Крім того, як швидкий спосіб унеможливлення подальшого поширення вірусу, поки будуть встановлені патчі з п. 4, доцільним є примусове створення в дисковій директорії C:\Windows\ текстового файлу perfect, і встановлення для нього атрибуту «тільки для читання».

Детальніше за посиланням:
https://ssu.gov.ua/ua/news/1/category/2/view/3643#sthash.omVibrez.dpuf [25]

Теги: Petya.A кібератака вірус вимагач [26]

Джерело: http://ndiitt.nau.edu.ua/news/2900-rekomendaciyi-sluzhby-bezpeky-ukrayiny-shchodo-zahystu-kompyuteriv-vid-kiberataky-virusu

Посилання:
[1] http://ndiitt.nau.edu.ua/news/2900-rekomendaciyi-sluzhby-bezpeky-ukrayiny-shchodo-zahystu-kompyuteriv-vid-kiberataky-virusu
[2] https://technet.microsoft.com/ru-ru/library/security/ms17-010.aspx
[3] http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-rus_84397f9eeea668b975c0c2cf9aaf0e2312f50077.exe
[4] http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu
[5] http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu
[6] http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu

[7] http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu
[8] http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu
[9] http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu
[10] http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu
[11] http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu
[12] https://www.talosintelligence.com/mbrfilter
[13] https://github.com/Cisco-Talos/MBRFilter;
[14] http://www.greatis.com/security/;
[15] https://www.sydneybackups.com.au/sbguard-anti-ransomware/
[16] https://help.ubuntu.com/community/Boot-Repair
[17] https://sourceforge.net/p/boot-repair-cd/home/Home/
[18] https://eset.ua/download_files/news/ESET_Recommendations_v2.0.pdf
[19] http://eset.ua/ua/download/utility?name=logcollector
[20] mailto:support@eset.ua
[21] http://zillya.ua/ru/epidemiya-zarazhenii-svyazana-s-deistviem-wannacry
[22] https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
[23] https://support.microsoft.com/en-us/help/4013389/title
[24] https://www.symantec.com/
[25] https://ssu.gov.ua/ua/news/1/category/2/view/3643#sthash.omVibrez.dpuf
[26] http://ndiitt.nau.edu.ua/news/petyaa-kiberataka-virus-vimagach