Рекомендації щодо захисту комп'ютерів від кібератаки вірусу-вимагача (Оновлено 18:00 29.06.2017)

27/06/2017

За даними CERT-UA переважна більшість інфікувань операційних систем відбувалася 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, у результаті експлуатації якої на інфіковану машину встановлювався набір скриптів, використовуваних зловмисниками 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 вивчається можливість дешифрування зашифрованих даних.

Рекомендації:

1. 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.

2. Збережіть всі файли, які найбільш цінні, на окремий не підключений до комп'ютера носій, а в ідеалі – резервну копію разом з операційною системою.

3. Для ідентифікації шифрувальника файлів необхідно завершити всі локальні задачі та перевірити наявність наступного файлу : C:\Windows\perfc.dat. Також для попередження шифрування потрібно створити файл C:\Windows\perfc. Перед початком процеса шифрування вірус перевіряє наявність файлу perfc в папці C:\Windows\, якщо файл вже існує вірус завершує роботу і не шифрує файли.

4. В залежності від версії ОС Windows встановити патч з ресурсу: https://technet.microsoft.com/ru-ru/library/security/ms17-010.aspx, а саме:

— для Windows XP — http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-rus_84397f9eeea668b975c0c2cf9aaf0e2312f50077.exe

— для Windows Vista 32 bit — http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x86_13e9b3d77ba5599764c296075a796c16a85c745c.msu

-для Windows Vista 64 bit — http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.0-kb4012598-x64_6a186ba2b2b98b2144b50f88baf33a5fa53b5d76.msu

— для Windows 7 32 bit — http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu

— для Windows 7 64 bit — http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

— для Windows 8 32 bit — http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-x86_a0f1c953a24dd042acc540c59b339f55fb18f594.msu

— для Windows 8 64 bit — http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/05/windows8-rt-kb4012598-

x64_f05841d2e94197c2dca4457f1b895e8f632b7f8e.msu

— для Windows 10 32 bit — http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu

— для Windows 10 64 bit — http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu

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

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.
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.

8. Коли користувач бачить «синій екран смерті», дані ще не зашифровані, тобто вірус ще не дістався до головної таблиці файлів. Якщо ви бачите, що комп'ютер показує вам «синій екран», перезавантажується і запускає Check Disk, негайно вимикайте його. На цьому етапі ви можете витягнути свій жорсткий диск, підключити його до іншого комп'ютера (тільки не в якості завантажувального тому!). І скопіювати свої 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, вихідні коди доступні тут https://github.com/Cisco-Talos/MBRFilter;

Рішення Greatis http://www.greatis.com/security/;

Свіже рішення SydneyBackups https://www.sydneybackups.com.au/sbguard-anti-ransomware/.

Команді CERT-UA вдалося відновити доступ до заблокованого зазначеним вірусом комп'ютера з ОС Windows.

10. На мережевому обладнанні та груповими політиками заблокувати на системах та серверах порти 135, 445, 1024-1035 TCP.
Також заблокувати доступ до таких ресурсів в мережі Інтернет:
— 84.200.16[.]242
— 84.200.16[.]242/myguy.xls
— french-cooking[.]com/myguy.exe
— 111.90.139[.]247
— COFFEINOFFICE[.]XYZ

11. Обмежити можливість запуску виконуваних файлів (*.exe) на комп'ютерах користувачів з директорій %TEMP%, %APPDATA%.

12. Забезпечити неприпустимість відкриття вкладень у підозрілих повідомленнях (у листах від адресантів, щодо яких виникають сумніви; наприклад: автор з невідомих причин змінив мову спілкування; тема листа є нетиповою для автора; спосіб, у який автор звертається до адресата, є нетиповим тощо; а також у повідомленнях з

нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів і т.ін.).

13. Системним адміністраторам і адміністраторам безпеки звернути увагу на фільтруваннявхідних/вихідних інформаційних потоків, зокрема поштового й веб-трафіку.

Насправді, 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. Ми використовували для цього утиліту «Boot-Repair».
Інструкція https://help.ubuntu.com/community/Boot-Repair

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

Потім за допомогою однієї з вказаних в інструкції утиліт створюємо Live-USB (ми використовували 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.
CERT-UA радить завантажити потрібні зашифровані файли на USB-носій або диск для подальшого їх розшифрування та перевстановити операційну систему.

Додатково до зазначених рекомендацій можливо скористатися рекомендаціями антивірусних компаній.
https://eset.ua/ua/news/view/507/-Eset-Guidelines
a). Завантажте утиліту Eset LogCollector: http://eset.ua/ua/download/<s+pan lang=»en-US»>
b). Запустіть і переконайтеся в тому, що були встановлені усі галочки у вікні «Артефакти для збору«.
c). У вкладці «Режим збору журналів Eset» встановіть: Вихідний двійковий код з диску.
d). Натиснить на кнопку: Збирати (Собрать).
e). Надішліть архів з журналами.

Якщо постраждалий ПК включений та ще не виключався, необхідно зробити наступне:
Із вже ураженого ПК (який не завантажується) потрібно зібрати MBR для подальшого аналізу
Зібрати його можливо за наступною інструкцією:
a). Завантажуйте з ESET SysRescue Live CD або USB (інструкція зі створення та оновлення баз сигнатур ESRL)
b). Погодьтесь з ліцензією на користування
c). Натисніть CTRL+ALT+T (відкриється термінал)
d). Напишить команду «parted -l» без лапок, параметр цього маленька буква «L» і натисніть <enter>
e). Перегляньте список дисків та ідентифікуйте уражений ПК (повинен бути один з /dev/sda)
f). Напишіть команду «dd if=/dev/sda of=/home/eset/petya.img bs=4096 count=256» без лапок, замість «/dev/sda» використовуйте диск, який визначили у попередньому кроці і натисніть <enter> (Файл /home/eset/petya.img буде створений)
g). Підключіть флешку і скопіюйте файл /home/eset/petya.img
h). Комп'ютер можна вимкнути.

http://zillya.ua/ru/epidemiya-zarazhenii-svyazana-s-deistviem-wannacry
Методи протидії зараженню
1. Відключення застарілого протоколу SMB1. Інструкція з відключення SMB1 в TechBlog компанії Microsoft:
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
2. Установлення оновлень безпеки операційної системи Windows з Microsoft Security Bulletin MS17-010:
https://support.microsoft.com/en-us/help/4013389/title
3. 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

4. Блокування можливості відкриття JS файлів, отриманих електронною поштою