За даними СБУ, 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.

Для ідентифікації шифрувальника файлів необхідно завершити всі локальні задачі та перевірити наявність наступного файлу : C:\Windows\perfc.dat

1. 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

2. 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.

3. 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.

4. Зробити резервні копії усіх критично важливих даних.

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