Рекомендації щодо захисту комп'ютерів від кібератаки вірусу-вимагача (оновлено)

19:25, 30-06-2017

За даними СБУ, потрапляння шкідливого програмного забезпечення **Petya.A** (відноситься до виду ШПЗ «ransomware», «шифрувальник», «локер») на ЕОМ під управлінням операційних систем Windows державних та комерційних структур відбувалося шляхом експлуатації вразливості MS17-010.

Головним призначенням ШПЗ зазначеного виду є шифрування усіх файлів, що зберігаються на ЕОМ-жертви. Після виконання власного програмного коду виводиться повідомлення про перетворення файлів з пропозицією здійснити оплату ключа дешифрування для розблокування даних. На сьогодні зашифровані дані, на жаль, розшифруванню не підлягають. Триває робота над можливістю дешифрування зашифрованих даних. Кошти, які вимагають здирники не виплачувати - оплата не гарантує відновлення доступу до 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.dat з атрибутом «тільки для читання». Перед початком процеса шифрування вірус перевіряє наявність файлу perfc.dat, якщо файл вже існує вірус завершує роботу і не шифрує файли.**

4. Залежно 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

- See more at: https://ssu.gov.ua/ua/news/1/category/2/view/3643#sthash.fI6Aqvwn.dpuf

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

Якщо з якоїсь причини ви не можете застосувати оновлення, можливим рішенням для зменшення атаки є відключення SMBv1 по кроках, задокументованих у https://support.microsoft.com/ru-RU/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows

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, вихідні коди доступні тут https://github.com/Cisco-Talos/MBRFilter

• зріле рішення Greatis http://www.greatis.com/security/

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

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 зазначити, 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

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 (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 рекомендуємо адміністраторам мереж:

1. Заблокувати запити до наступних ресурсів в мережі Інтернет (дужки біля точок вставлені, щоб не було гіперпосилань):

- 84.200.16[.]242

- 111.90.139[.]247

- 185.165.29[.]78

- 95.141.115[.]108

- 84.200.16[.]242/myguy.xls

- http://french-cooking[.]com/myguy.exe

2. Якщо в мережі вже є заражені робочі станції або сервери необхідно відключити (як мінімум на період перевірки) TCP-порти 1024-1035, 135 і 445.

3. Заблокувати використання облікових записів локальних адміністраторів та адміністраторів домену на робочих станціях, заборонивши для них повноваження локального та віддаленого керування (https://technet.microsoft.com/windows-server-docs/security/securing-privileged-access/securing-privileged-access)

4. Задіяти безкоштовний мережевий сервіс Local Administrator Password Solution (LAPS) для генерації динамічно-змінюваних паролів адміністраторів (https://technet.microsoft.com/en-us/security/jj653751 або http://www.microsoft.com/en-us/download/details.aspx?id=46899).

5. Налаштувати групові політики безпеки AppLocker на контроль списку додатків на робочих станціях (https://technet.microsoft.com/en-us/library/dd723678(v=ws.10).aspx).

6. Скористатись безкоштовним рішенням для запобігання атак 0-дня (http://www.microsoft.com/en-us/download/details.aspx?id=50766 и http://www.microsoft.com/en-us/download/details.aspx?id=50766).

7. У зв'язку з тим, що в ході свого поширення мережею вірус використовує PsExec, доцільно застосувати SIGMA-правило для виявлення використання PsExec, воно може бути автоматично конвертуване в запит Splunk і ElasticSearch, наприклад:

title: PsExec tool execution on destination host

status: experimental

description: Detects PsExec service installation and execution events (service and Sysmon)

author: Thomas Patzke

reference: www.jpcert.or.jp/english/pub/sr/ir_research.html

logsource:

product: windows

detection:

service_installation:

EventID: 7045

ServiceName: 'PSEXESVC'

ServiceFileName: '* \ PSEXESVC.exe'

service_execution:

EventID: 7036

ServiceName: 'PSEXESVC'

sysmon_processcreation:

EventID: 1

Image: '* \ PSEXESVC.exe'

User: 'NT AUTHORITY \ SYSTEM'

condition: service_installation or service_execution or sysmon_processcreation

falsepositives:

- unknown

level: low

Додатково до зазначених рекомендацій можна скористатися рекомендаціями антивірусних компаній:

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

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

а) Виконайте створення логу за допомогою програми ESET Log Collector: Завантажте утиліту ESET Log Collector: http://eset.ua/ua/download/utility?name=logcollector 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.

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.

II. http://zillya.ua/ru/epidemiya-

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. Налаштуйте антиспам системи вашої електронної пошти, щоб відфільтрувати всі потенційно шкідливі вхідні повідомлення. Визначте конкретні обмеження розширення файлів у вашій поштовій системі.

5. Переконайтеся, що додатки з наступними розширеннями містяться в чорному списку: .js, .vbs, .docm, .hta, .exe, .cmd, .scr та .bat. Крім того, обробляйте ZIP архіви в отриманих повідомленнях з особливою обережністю.

6. Регулярне резервне копіювання ваших файлів,

III. *https://www.symantec.com/*

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\perfc/

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 perfc, і встановлення для нього атрибуту «тільки для читання».

IV. *https://www.romadcyber.com*

Можливі сценарії відновлення даних:

1. В ручному режимі:

- Пошук файлів на жорсткому диску по сигнатурам, при цьому ім'я файлів не відновлюється. Можливо лише тільки для нефрагментованих файлів.

- Пошук файлових записів по сигнатурі FILE, отримання списку кластерів, які належать файлу, таким способом відновлюється дані та ім'я файлів.

- Метод відновлення вибіркових файлів за допомогою відновлення нерезидентного списку секторів, що належать файлу (Data Runs). Даний метод базується на наступній концепції: виконується пошук кластера, що містить вихідний файл (пошук здійснюється за сигнатурою), далі номер цього кластера використовується для пошуку нерезидентного списку секторів, що належать файлу.

За допомогою описаних методів, можливо відновити файли більшого розміру, які не можна відновити за допомогою пошукового запиту за сигнатурою та автоматичними засобами.

- Відновлення MBR можливо за командою "bootrec/FixMbr" до перезавантаження системи (Vista +, у випадку з Windows XP можна використовувати команду "fixmbr").

- Відновлення MBR після перезавантаження, але до шифрування. Необхідно видалити оригінальний MBR з 34 секторів (0x4400 зсув на диску, розмір 0x200) розшифровувати (xor 0x07) і записати в початок диска.

2. Напівавтоматичний сценарій відновлення:

Ця проблема вирішується відновленням MBR запису. Використовуємо для цього утиліту «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 (як приклад Universal USB Installer). Завантажитись зі створеної Live-USB та далі слідувати інструкції з відновлення MBR запису.

3. Автоматичний сценарій відновлення даних:

- У тому випадку, якщо фейковий chkdsk Petya відпрацював за своїм сценарієм, то шанси щодо до відновлення даних, на даний час, достатньо малі.

- У тому випадку, якщо живлення комп'ютера було відключено, то рекомендуємо підключити HDD до другого (не враженого) PC та запустити R-Studio або GetDataBack.

Нагадуємо, що при зараженні системи з використанням ШПЗ «PSEXEC» в директоріях Windows можуть присутні наступні файли:

«c:\Windows\perfc.dat»

«c:\Windows\dllhost.dat»

Також для зупинки розповсюдження даного шкідливого ПЗ необхідно заблокувати запуск ПЗ «PSEXEC.EXE» за допомогою засобів локальної або групової політики безпеки на потенційно уразливих машинах, а також, якщо можливо, заблокувати або вимкнути дистанційний доступ до WMI.

В ході дослідження та відповідно до інформації від компетентних вірусних аналітиків було виявлено особливість, що дозволяє запобігти зараженню через PsExec та WMI. Для цього достатньо створити пустий файл "c:\Windows\Perfc".

V. *http://www.microsoft.com*

Антивірусне програмне забезпечення Microsoft виявляє та захищає від вірусу Petya.A. Попередній аналіз показав, що вірус використовує декілька методів для розповсюдження, включаючи ті, що були задіяні в оновленні безпеки (MS17-010), раніше наданому для всіх платформ від Windows XP до Windows 10.

На разі, Windows Defender, System Center Endpoint Protection та Forefront Endpoint Protection визначили ці загрози як Ransom:Win32/Petya.

Переконайтеся, що ваша встановлена версія є однією з перечислених чи більш пізньою:

Встановлена версія загрози: 1.247.197.0

Версія створена о 12:04:25 PM : Вівторок, 27 червня, 2017 (Тихоокеанський час)

Останнє оновлення: 12:04:25 PM : Вівторок, 27 червня, 2017 (Тихоокеанський час)

Крім того, безкоштовний Сканер безпеки Microsoft Safety Scanner http://www.microsoft.com/security/scanner/ розроблений для виявлення цієї загрози, а також для виявлення багатьох інших. Якщо ви використовуєте антивірус не від корпорації Microsoft, будь-ласка, зверніться до компанії-провайдера.

Фотографії

Рекомендувати: