АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Petya и другие. ESET раскрывает детали кибератак на корпоративные сети

1 июля 2017 года

Эпидемия шифратора Petya в центре внимания. Проблема в том, что это лишь последний инцидент в серии атак на украинские компании. Отчет ESET раскрывает некоторые возможности Diskcoder.C (он же ExPetr, PetrWrap, Petya или NotPetya) и включает информацию о ранее неосвещенных атаках.

TeleBots

В декабре 2016 года мы опубликовали исследование деструктивных атак, выполненных кибергруппой, которую мы называем TeleBots. Группировка атаковала финансовые учреждения и использовала версию деструктивного компонента KillDisk для Linux. Кроме того, TeleBots могут иметь отношение к группе BlackEnergy, связанной с кибератаками на энергетические компании.

Вредоносная программа KillDisk использовалась группой TeleBots на заключительном этапе атак, чтобы перезаписать файлы с определенными расширениями на диске жертвы. Забегая вперед, выкуп никогда не был приоритетом для этой группы.

В первой волне атак в декабре 2016 года KillDisk переписывал целевые файлы, вместо шифрования данных. Жертва не получала контакты для связи с атакующими, вредоносная программа просто выводила на экран изображение, отсылающее к сериалу «Мистер Робот».

Рисунок 1. Изображение, которое выводил на экран KillDisk в ходе первой волны атак в декабре 2016 года.

Во второй волне атак злоумышленники доработали KillDisk, добавив шифрование и контактную информацию в сообщение о выкупе, что придавало сходство с типичной программой-вымогателем. При этом авторы запросили за восстановление данных рекордную сумму – 222 биткоина (около 250 тысяч долларов по нынешнему курсу). Это может указывать на то, что хакеры не были заинтересованы в получении выкупа, а стремились нанести ущерб атакуемым компаниям.

Рисунок 2. Требование выкупа KillDisk, версия второй волны атак в декабре 2016 года.

В 2017 году группа TeleBots продолжила атаки, которые стали более изощренными. С января по март 2017 года группа скомпрометировала украинскую компанию, разрабатывающую программное обеспечение (не M.E.Doc) и, используя VPN-туннели, получила доступ к внутренним сетям нескольких финансовых учреждений.

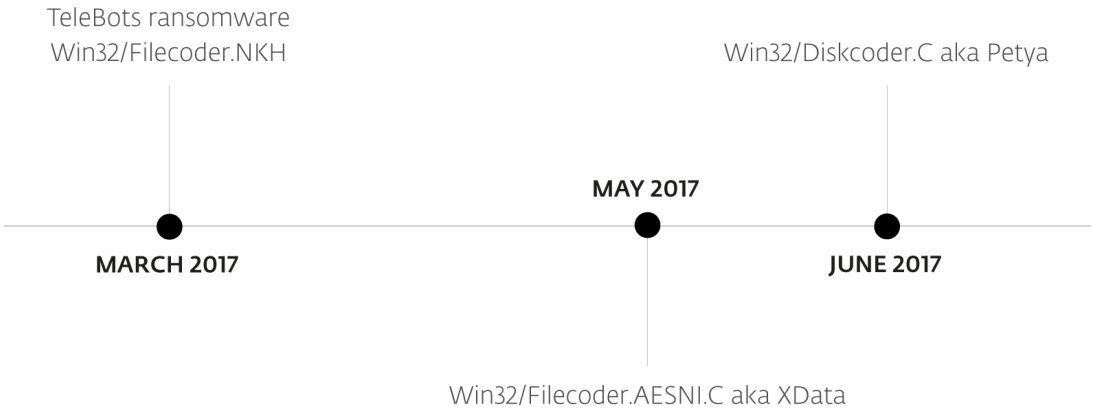

Рисунок 3. Атаки на цепи поставок (supply-chain attacks) в 2017 году

В ходе этой атаки TeleBots пополнили арсенал двумя образцами шифраторов и обновленными версиями инструментов, упомянутых в наших предыдущих отчетах.

Первый бэкдор, на который в значительной степени полагалась группа, – Python/TeleBot.A, который был переписан с языка программирования Python на Rust. Функции не изменились – это стандартный бэкдор, который использует Telegram Bot API, чтобы получать команды от операторов и отправлять ответы.

```
.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
```

Рисунок 4. Дизассемблированный код Win32/TeleBot.AB trojan.

Второй бэкдор, написанный на VBS и упакованный с помощью программы script2exe, был сильно обфусцирован, но его функциональность осталась такой же, как в прежних атаках.

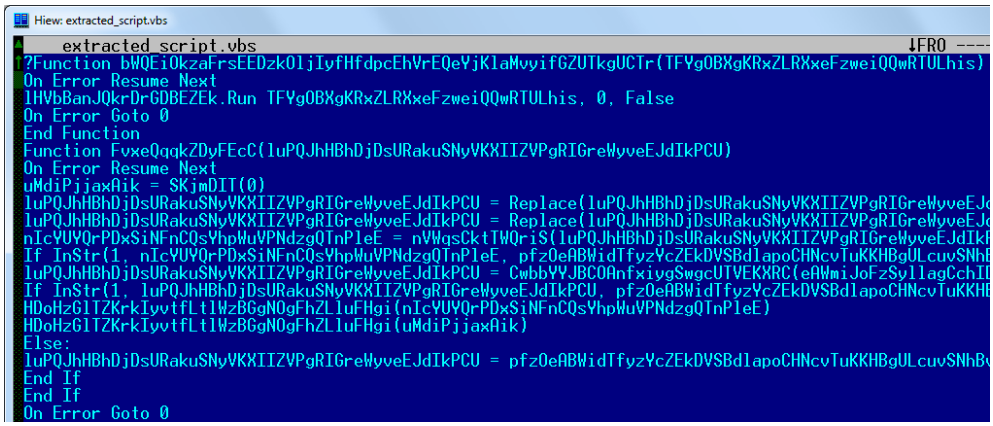

Рисунок 5. Обфусцированная версия VBS-бэкдора.

На этот раз VBS-бэкдор использует командный C&C-сервер 130.185.250[.]171. Чтобы сделать соединения менее подозрительными для тех, кто проверяет журналы фаервола, атакующие зарегистрировали домен **transfinance.com[.]ua** и разместили его на этом IP-адресе. Как видно на рисунке 6, также был запущен почтовый сервер с именем severalwdadwajunior, который работал в сети Tor.

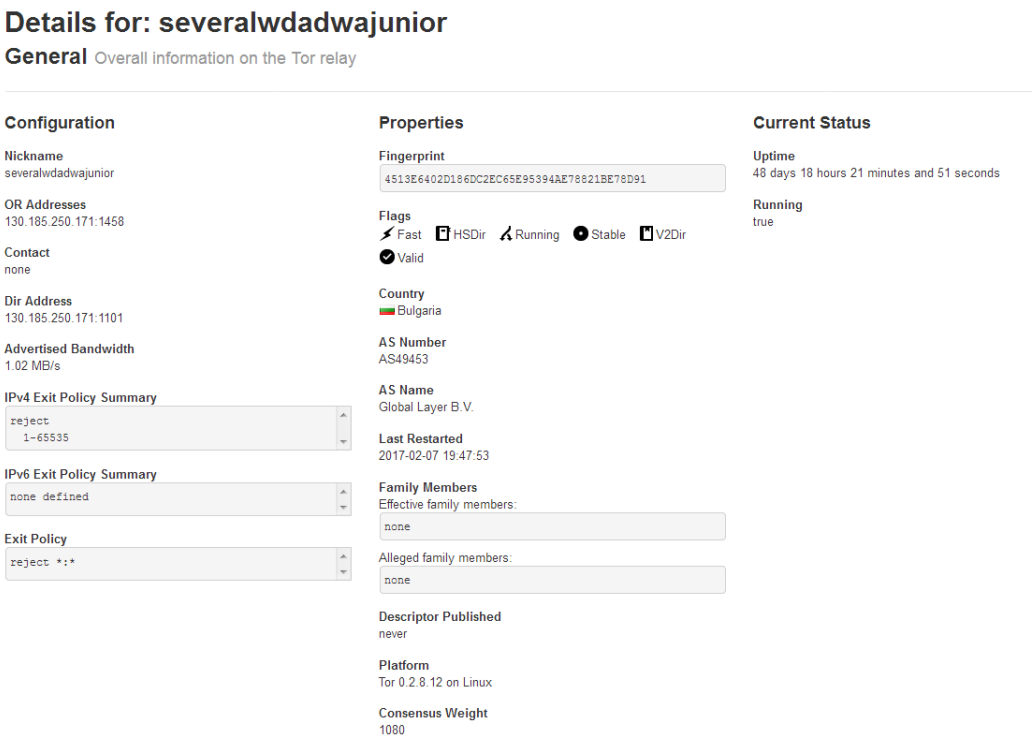

Рисунок 6. Информация о сервере группы TeleBots.

Кроме того, атакующие использовали следующие инструменты:

- CredRaptor (кража паролей)
- Plainpwd (модифицированный Mimikatz используется для восстановления учетных данных Windows из памяти)
- SysInternals' PsExec (используется для распространения угрозы внутри сети)

Как сказано ранее, на завершающей стадии атаки TeleBots распространяют шифратор, используя PsExec и украденные учетные данные Windows. Антивирусные продукты ESET детектируют его как Win32/Filecoder.NKH. После выполнения малварь шифрует все файлы (за исключением расположенных в C:\Windows) с применением алгоритмов AES-128 и RSA-1024. Вредоносная программа добавляет к зашифрованным файлам расширение .xcrypted

Когда шифрование завершено, программа создает текстовый файл readme.txt со следующим содержанием:

Please contact us: openy0urm1nd@protonmail.ch

Помимо вредоносного ПО для Windows, группа TeleBots использовала Linux-шифратор для других ОС. ESET детектирует угрозу как Python/Filecoder.R, она написана на Python. На этот раз атакующие используют для шифрования файлов сторонние утилиты, такие как openssl. Шифрование осуществляется с помощью алгоритмов RSA-2048 и 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
```

Рисунок 7. Код на Python Linux-шифратора Python/Filecoder.R, используемого группой TeleBots.

В коде скрипта на Python атакующие оставляют свой комментарий, включающий следующий текст:
feedback: openy0urm1nd[@]protonmail.ch

Win32/Filecoder.AESNI.C

18 мая мы зафиксировали активность шифратора другого семейства – Win32/Filecoder.AESNI.C, также известного как XData.

Программа-вымогатель распространялась преимущественно на Украине, что связано с интересным начальным вектором заражения. По данным телеметрии ESET, шифратор появлялся на компьютере сразу после запуска программного обеспечения для отчетности и документооборота M.E.Doc, широко распространенного в украинских компаниях.

Функционал Win32/Filecoder.AESNI.C позволял шифратору автоматически распространяться в локальной сети компании. В частности, встроенная DLL Mimikatz использовалась для извлечения учетных записей Windows из памяти скомпрометированного компьютера. С помощью учетных данных малварь распространялась внутри сети, используя утилиту PsExec.

Похоже на то, что атакующие не достигли своей цели в ходе этой атаки, либо провели тестирование перед более эффективным ударом. В любом случае, мастер-ключи были опубликованы на форуме BleepingComputer, там же появилось заявление о том, что исходный код AESNI был украден у настоящего автора и использовался в украинском инциденте.

ESET выпустила дешифратор для жертв Win32/Filecoder.AESNI.

Эпидемия Diskcoder.C (более известного как Petya)

Что действительно получило широкое освещение в СМИ, так это эпидемия Petya, начавшаяся 27 июня. Вредоносная программа скомпрометировала множество систем в критических инфраструктурах и корпоративных сетях на Украине и за ее пределами.

Шифратор, который используется в этой атаке, может подменять главную загрузочную запись (MBR) собственным вредоносным кодом. Код позаимствован у программы-вымогателя Win32/Diskcoder.Petya, поэтому некоторые исследователи называют угрозу ExPetr, PetrWrap, Petya или NotPetya. В отличие от оригинального Petya, авторы Diskcoder.C изменили код MBR таким образом, что восстановить данные стало невозможно. Точнее, атакующие не могут отправить жертве ключ расшифровки, и его невозможно ввести в соответствующее поле, поскольку он содержит недопустимые символы.

Визуально MBR часть Diskcoder.C выглядит как слегка модифицированная версия Petya: сначала она показывает сообщение, в котором выдает себя за CHKDSK – утилиту проверки диска от Microsoft. В процессе фейкового сканирования Diskcoder.C на самом деле шифрует данные.

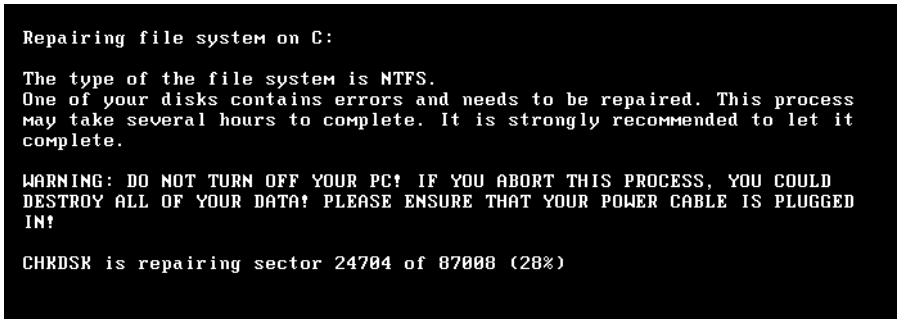

Рисунок 8. Фейковое сообщение CHKDSK, отображаемое Diskcoder.C.

Когда шифрование завершено, код MBR отображает следующее сообщение с инструкциями для оплаты, но, как уже было доказано, эта информация бесполезна.

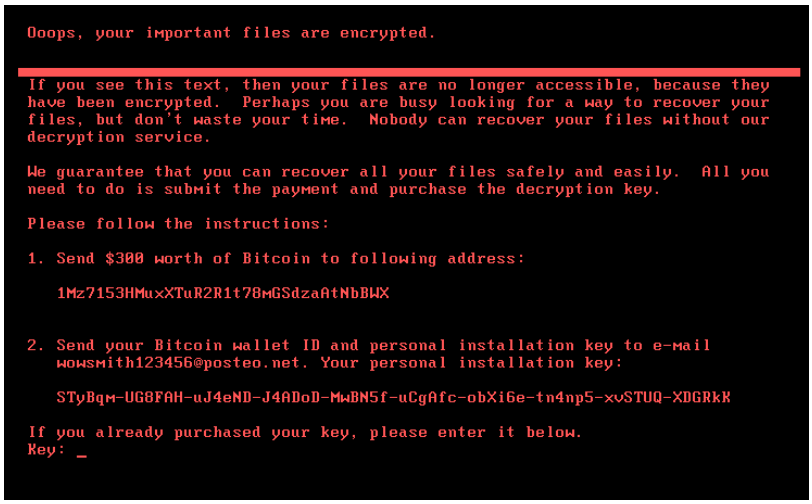

Рисунок 9. Сообщение Diskcoder.C с инструкциями для оплаты выкупа.

Остальной код, помимо заимствованного MBR, написан авторами вредоносной программы. Он включает шифратор файлов, который может использоваться в дополнение к шифрующей диск MBR. Вредоносная программа использует алгоритмы AES-128 и RSA-2048.

Стоит отметить, что авторы допустили ошибки, что сократило возможности дешифровки файлов. Например, Diskcoder.C шифрует только первый 1 Мб данных и не записывает header и footer, только исходные зашифрованные данные. Малварь не переименовывает файлы, поэтому сложно сказать, какие файлы зашифрованы, а какие нет.

Интересно, что список целевых расширений хотя и не полностью идентичен, но очень похож на используемый в атаках KillDisk в декабре 2016 года.

```
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
```

Рисунок 10. Список целевых расширений Diskcoder.C.

После выполнения Diskcoder.C пытается увеличить охват при помощи эксплойта EternalBlue, который использует бэкдор DoublePulsar, работающий в режиме ядра. Точно такой же метод использовался в вымогателе WannaCryptor.D.

Diskcoder.C также использовал метод, позаимствованный у Win32/Filecoder.AESNI.C (XData) – он использует упрощенную версию Mimikatz, чтобы получить учетные данные, а затем исполняет вредоносное ПО на других машинах локальной сети с помощью SysInternals PsExec.

Наконец, авторы Diskcoder.C использовали третий метод распространения – механизм WMI.

Все три метода применялись для распространения Diskcoder.C внутри сетей. В отличие от WannaCryptor, новый шифратор использовал эксплойт EternalBlue только на компьютерах в диапазоне адресов локальной сети.

Почему эпидемия вышла за пределы Украины? Наше исследование показало, что зараженные компании в других странах подключались через VPN к своим украинским филиалам или бизнес-партнерам.

Начальный вектор заражения

И Diskcoder.C, и Win32/Filecoder.AESNI.C использовали атаки на цепь поставок (supply-chain attack) в качестве начального вектора заражения. Эти семейства вредоносного ПО передавались при помощи программного обеспечения для отчетности и документооборота M.E.Doc, которое широко используется в бухгалтерском учете.

Существует несколько вариантов проведения этих атак. У M.E.Doc есть внутренняя система обмена документами и сообщениями, так что хакеры могли использовать фишинг. В этом случае необходимо взаимодействие с пользователем, возможно, не обошлось без социальной инженерии. Поскольку Win32/Filecoder.AESNI.C не распространился слишком широко, мы сначала решили, что были задействованы именно эти методы.

Но последующая эпидемия Diskcoder.C дает основания предполагать, что у хакеров был доступ к серверу обновлений легитимного ПО M.E.Doc. С его помощью атакующие могли направлять вредоносные обновления с их установкой автоматически без участия пользователя. Поэтому так много систем на Украине пострадало от этой атаки. Кажется, что создатели малвари недооценили способности Diskcoder.C к экспансии.

Исследователи ESET нашли подтверждение этой теории. Мы обнаружили PHP-бэкдор в файле medoc_online.php в одной из директорий на сервере FTP M.E.Doc. Доступ к бэкдору можно было получить через HTTP, хотя он был зашифрован, и атакующему нужен был пароль для его использования.

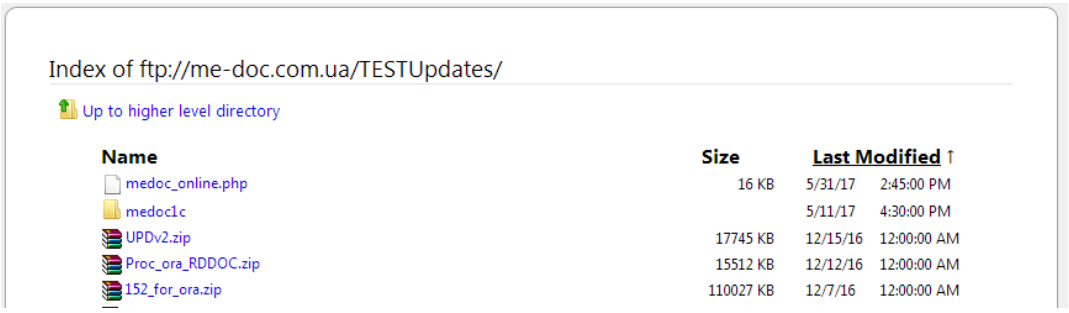

Рисунок 11. Директория с PHP-бэкдором на FTP.

Надо сказать, что есть признаки, указывающие на то, что Diskcoder.C и Win32/Filecoder.AESNI.C – не единственные семейства вредоносных программ, которые использовали этот вектор. Можем предположить, что вредоносные обновления были применены для скрытого проникновения в компьютерные сети, принадлежащие приоритетным объектам.

Одной из вредоносных программ, распространявшихся с помощью скомпрометированного

механизма обновлений M.E.Doc, был VBS-бэкдор, который использует группа TeleBots. На этот раз атакующие снова использовали доменные имена, связанные с финансовой темой: **bankstat.kiev[.]ua**.

В день начала эпидемии Diskcoder.C A-запись этого домена была изменена на 10.0.0.1.

Выводы

Группа TeleBots совершенствует инструменты деструктивных атак. Вместо направленных фишинговых писем с документами, содержащими вредоносные макросы, они использовали более сложную схему, известную как кибератаки на цепи поставок (supply-chain attack). До начала эпидемии группа атаковала преимущественно финансовый сектор. Вероятно, что последняя кампания была нацелена на украинский бизнес, но атакующие недооценили возможности вредоносной программы – малварь вышла из-под контроля.

Индикаторы заражения (IoC)

Детектирование продуктами ESET:
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:
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)

Легитимные серверы, используемые авторами вредоносной программы:
api.telegram.org (IP: 149.154.167.200, 149.154.167.197, 149.154.167.198, 149.154.167.199)

VBS-бэкдор:
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