Консультація щодо загроз: CaddyWiper

Вівторок, 15 березня 2022 р

ОГЛЯД

14 березня компанія ESET, що спеціалізується на кібербезпеці, оприлюднила ще одну програму Wiper, орієнтовану на Україну, яка отримала назву CaddyWiper. Ця програма порівняно менша за попередні, які можна було спостерігати в Україні, зокрема HermeticWiper і WhisperGate. У скомпільованому вигляді її розмір становить лише 9 КБ.

Виявлена програма Wiper має той же день позначки часу компіляції (14 березня), і початкові звіти припускають, що її було розгорнуто через об'єкт групової політики (Group Policy Object, GPO).

Команда Cisco Talos активно проводить аналіз, щоб підтвердити деталі, включені до цих звітів.

АНАЛІЗ

Програма Wiper порівняно невелика за розміром і динамічно вирішає більшість API-інтерфейсів, які використовує. Наш аналіз не виявив жодних ознак стійкості, саморозповсюдження або коду експлуатації.

Перш ніж починати знищення файлів, програма перевіряє, що система не є контролером домену. Якщо система є контролером домену, програма припиняє процес виконання.

```
obj_DSROLE_PRIMARY_DOMAIN_INFO_BASIC = 0;
result = DsRoleGetPrimaryDomainInformation(0, DsRolePrimaryDomainInfoBasic, &obj_DSROLE_PRIMARY_DOMAIN_INFO_BASIC);
if ( *(_DWORD *)obj_DSROLE_PRIMARY_DOMAIN_INFO_BASIC != DsRole_RolePrimaryDomainController )
{
  LoadLibraryA(&a_advapi32_dll);
  a_C_users = 'C';
  v16 = ':';
  v17 = '\\';
  v18 = 'U';
  v19 = 's';
  v20 = 'e';
  v21 = 'r';
  v22 = 's';
  v23 = 0;
  overwrite_files_with_zeros(&a_C_users);
  drive_letter = 'D';
  v53 = ':';
  v54 = '\\';
  v55 = 0;
  for ( i = 0; i < 0x18; ++i )
  {
    overwrite_files_with_zeros(&drive_letter);
    ++drive_letter;
  }
  result = wipe_physical_drives();
}
```

Псевдокод: CaddyWiper перевіряє наявність у системи ролі контролера домену

Якщо система не є контролером домену, Wiper знищить файли на диску C:\Users, потім усі файли на наступних дисках за алфавітом, доки не досягне диска Z. Це означає, що Wiper також спробує знищити будь-який підключений до мережі диск, поєднаний із системою.

```
                mov     [ebp+a_D_drive], 44h ; 'D'
                mov     [ebp+var_1F], 3Ah ; ':'
                mov     [ebp+var_1E], 5Ch ; '\'
                mov     [ebp+var_1D], 0
                mov     [ebp+ctr], 0
                jmp     short loc_4011A3
; ---------------------------------------------------------------------------

loc_40119A:                             ; CODE XREF: start+1BD↓j
                mov     ecx, [ebp+ctr]
                add     ecx, 1
                mov     [ebp+ctr], ecx

loc_4011A3:                             ; CODE XREF: start+198↑j
                cmp     [ebp+ctr], 24   ;  D drive + 24 next alphabets
                jnb     short loc_4011BF
                lea     edx, [ebp+a_D_drive]
                push    edx
                call    overwrite_files_with_zeros
                add     esp, 4
                mov     al, [ebp+a_D_drive]
                add     al, 1
                mov     [ebp+a_D_drive], al ; increment drive letter
                jmp     short loc_40119A
```

Файли на дисках із літерами від D: перезаписуються нулями

© 2022 Cisco та/або філії компанії. Всі права захищені.

Консультація щодо загроз: CaddyWiper

Завдяки цьому система не вийде з ладу через стирання системних файлів.

АЛГОРИТМ ЗНИЩЕННЯ ФАЙЛІВ

Алгоритм знищення файлів складається із двох етапів: перший етап – перезапис файлів, другий – знищення фізичної схеми диска й таблиць розділів разом із нею. Для знищення файлів програма отримує право власності на файли, змінюючи їхні записи ACL після отримання привілею SeTake-OwnershipPrivilege. Потім знайдені файли просто перезаписуються нулями.

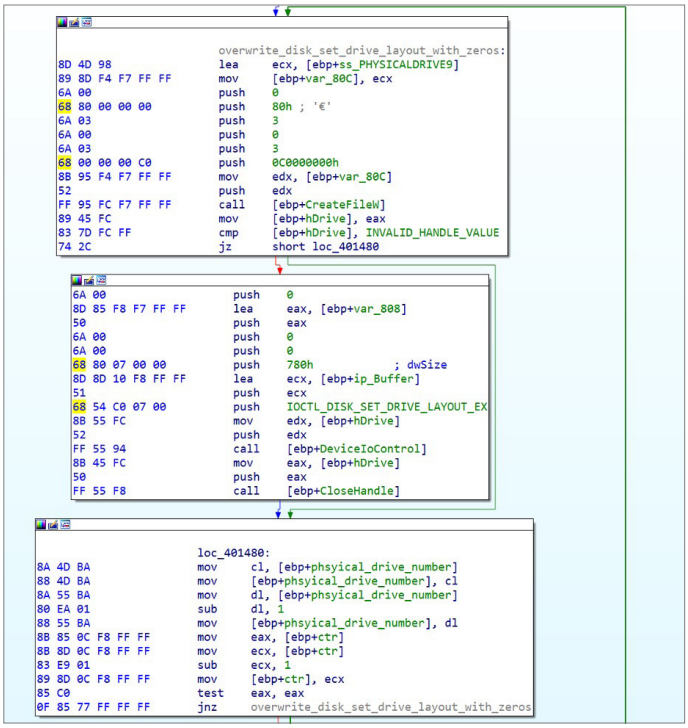
У файлі, розмір якого перевищує 10 485 760 байт (0xA00000), перші 10 485 760 байт буде перезаписано нулями.

```
mov     eax, [ebp+file_size]
push    eax
push    40h ; '@'
call    [ebp+LocalAlloc]
mov     [ebp+buffer], eax
mov     ecx, [ebp+file_size]
push    ecx
mov     edx, [ebp+buffer]
push    edx
call    clear_buffer
add     esp, 8
push    FILE_BEGIN
push    0
push    0
mov     eax, [ebp+hFile]
push    eax
call    [ebp+SetFilePointer]
push    0
lea     ecx, [ebp+lpNumberOfBytesWritten]
push    ecx
mov     edx, [ebp+file_size] ; nNumberOfBytesToWrite = buffer is the same size as the file
push    edx
mov     eax, [ebp+buffer] ; zeroed out buffer
push    eax
mov     ecx, [ebp+hFile]
push    ecx
call    [ebp+WriteFile]
mov     edx, [ebp+buffer]
push    edx
call    [ebp+LocalFree]
mov     eax, [ebp+hFile]
push    eax
call    [ebp+CloseHandle]
```

Файл перезаписується за допомогою буфера з нулів

Потім Wiper переходить до наступного диска системи, починаючи з диска D. Програма рекурсивно отримує права на файли на диску та перезаписує ці файли нулями. Це робиться для наступних 23 дисків в алфавітному порядку (через «Z:\»).

На другому етапі програма Wiper намагається встановити схему розташування всіх фізичних дисків системи з нумерацією від 9 до 0. Це знищить всю розширену інформацію про розділи фізичного диска, зокрема MBR, GPT і записи розділів.



Wiper рекурсивно виконує запити IOCTL_DISK_SET_DRIVE_LAYOUT_EX з обнуленим буфером

Знищення початку файлів і таблиць розділів – це звичайна техніка, що трапляється в інших програмах Wiper, і вона дуже ефективна для запобігання відновленню файлів.

ОХОПЛЕННЯ

Нижче наведено способи, за допомогою яких наші клієнти можуть виявити та блокувати цю загрозу.

Cisco Secure Endpoint (раніше AMP for Endpoints) ідеально підходить для запобігання виконанню шкідливого програмного забезпечення, про яке йдеться в цій публікації. Спробуйте Secure End-

© 2022 Cisco та/або філії компанії. Всі права захищені.

Консультація щодо загроз: CaddyWiper

Продукт	Захист
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	Н/Д
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	Н/Д

point безкоштовно тут. Рішення з вебсканування

Cisco Secure Web Appliance запобігає доступу до шкідливих вебсайтів і виявляє зловмисне програмне забезпечення, яке застосовується в цих атаках.

Cisco Secure Email (раніше Cisco Email Security) може блокувати шкідливі електронні листи, надіслані зловмисниками в межах своєї кампанії. Ви можете спробувати Secure Email безкоштовно тут. Пристрої

Cisco Secure Firewall (раніше Next-Generation Firewall і Firepower NGFW), зокрема Firepower Threat Defense (FTD), Firepower Device Manager (FDM), Threat Defense Virtual і Adaptive Security Appliance, можуть виявити шкідливу активність, пов'язану з цією загрозою.

Cisco Secure Malware Analytics (раніше Threat Grid) виявляє шкідливі двійкові файли та вбудовує захист у всі продукти Cisco Secure.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) автоматично аналізує мережевий трафік і попереджає користувачів про потенційно небажану активність на кожному підключеному пристрої.

Дізнатися, як використовувати Cisco Secure Analytics для реагування на цю загрозу, можна тут. Пристрої

Meraki MX можуть виявляти шкідливу активність, пов'язану з цією загрозою.

Umbrella, захищений інтернет-шлюз (Secure Internet Gateway, SIG), блокує підключення користувачів до шкідливих доменів, IP-адрес і URL-адрес незалежно від того, перебувають користувачі в корпоративній мережі або за її межами. Зареєструйтеся для використання безкоштовної пробної версії Umbrella тут.

Дізнатися про додаткові засоби захисту з урахуванням специфіки вашого середовища та даних про загрози можна в системі керування Firewall Management Center.

Cisco Duo забезпечує багатофакторну автентифікацію користувачів, гарантуючи доступ до вашої мережі лише авторизованим особам.

Користувачі набору правил Snort Subscriber Rule Set із відкритим вихідним кодом можуть завантажити останній пакет правил, наявний у продажу, на сайті Snort.org.

Snort SID: **59268–59269**

Для захисту від цієї загрози доступні такі сигнатури ClamAV:

- Win.Malware.CaddyWiper-9941573-1

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

a294620543334a721a2ae8eaaf9680a0786f-4b9a216d75b55cfd28f39e9430ea

1e87e9b5ee7597bdce796490f3ee09211df48ba1d-11f6e2f5b255f05cc0ba176

ea6a416b320f32261da8dafcf2faf-088924f99a3a84f7b43b964637ea87aef72

f1e8844dbfc812d39f369e7670545a29efef6764d-673038b1c3edd11561d6902

© 2022 Cisco та/або філії компанії. Всі права захищені.