Консультація щодо загроз: DoubleZero



Четвер, 24 березня 2022 р

ОГЛЯД

22 березня 2022 року команда реагування на комп'ютерні надзвичайні події України (Computer Emergency Response Team of Ukraine, CERT-UA) випустила інформаційне попередження, в якому повідомлялося про шкідливе програмне забезпечення Wiper під назвою DoubleZero, націлене на українські підприємства під час вторгнення Росії в Україну. Цю програму Wiper було виявлено ще 17 березня 2022 року. DoubleZero – це ще одна програма Wiper на додаток до виявлених раніше атак, які ми бачили в Україні протягом останніх двох місяців, як-от CaddyWiper, HermeticWiper і WhisperGate.

DoubleZero – це імплантат на базі платформи .NET, який знищує файли, розділи реєстру та дерева на зараженій кінцевій точці.

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

АНАЛІЗ АЛГОРИТМУ ДІЇ WIPER

Спочатку шкідлива програма перевіряє, чи є поточна кінцева точка одним із контролерів домену. Якщо ім'я кінцевої точки знайдено, Wiper просто припиняє виконання.

Wiper починає роботу з отримання таких привілеїв на кінцевій точці:

- SeTakeOwnershipPrivilege
- SeRestorePrivilege
- SeBackupPrivilege
- SeShutdownPrivilege

Ціль програми – перезаписати всі файли шляхом знищення всіх файлів на всіх дисках, за винятком певного списку місць, жорстко закодованих у Wiper. Шкідлива програма має намір спочатку знищити несистемні файли, а потім файли, пов'язані із системою. Знищення системних файлів під час перезаписування інших файлів може створити нестабільність і призвести до блокування системи, перш ніж файли користувача буде повністю знищено. У подібному випадку можна відновити файли з диска, які ще не було перезаписано.

Системні папки, зарезервовані для знищення *після* знищення всіх інших файлів:

- <Кореневий_диск>\Windows\Microsoft.NET
- <Кореневий_диск>\Windows
- <Кореневий_диск>\\Users\\\\.*?\\\\Local Settings.*
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Application Data.*
- <Кореневий_диск>\\Users\\\\.*?\\\\Start Menu.*
- <Кореневий_диск>\\Users\\\\.*?\\\\Application Data.*
- <Кореневий_диск>\\ProgramData\\\\Microsoft.*
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Microsoft.*
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Roaming\\\\Microsoft.*
- <Кореневий_диск>\Documents and Settings
- <Кореневий_диск>\ProgramData\Application

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

Консультація щодо загроз: DoubleZero

Data

- <Кореневий_диск>\Users\All Users
- <Кореневий_диск>\Users\Default User
- <Кореневий_диск>\system\drivers
- <Кореневий_диск>\Windows\NTDS

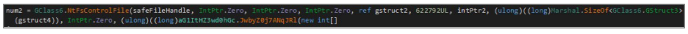
Wiper перерахує всі шляхи до файлів і вирішить, чи файл є «безпечним» для негайного знищення, тобто чи він не є системним файлом.

Для кожного файлу, який вважається «безпечним» для знищення (тобто не входить до винятків, перелічених вище), програма:

- змінить контроль доступу до файлів, надавши обліковому запису локальної системи (WellKnownSidType.LocalSystemSid) повний контроль над файлом;
- використовуватиме одну з двох функцій Wiper для знищення файлів.

ФУНКЦІЯ WIPER № 1

У цій процедурі використовуватимуться API, як-от NtfsControlFile із керівним кодом FSCTL_SET_ZERO_DATA (0x980C8), щоб заповнити весь файл нульовими байтами.



До файлу застосовується функція NtfsControlFile для його обнулення

ФУНКЦІЯ WIPER № 2

Друга процедура, яка використовується для перезапису файлів, є порівняно простішою. Програма відкриває цільовий файл як FileStream і просто перезаписує його масивом, що містить усі нулі.

```
fileStream.Write(array2, xH2BZMNfuO.ivFpj3d4f16Ef(new int[]
```

Файл перезаписується масивом, що містить усі нулі

Потім Wiper переходить до знищення системних файлів, яке виконується двома функціями Wiper, показаними вище. Нижче наведено порядок знищення системних файлів.

Перший етап:

- <Кореневий_диск>\system\drivers

Другий етап:

- <Кореневий_диск>\\Users\\\\.*?\\\\Local Settings.*
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Application Data.*
- <Кореневий_диск>\Windows\NTDS
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Local\\\\Microsoft.*
- <Кореневий_диск>\\Users\\\\.*?\\\\AppData\\\\Roaming\\\\Microsoft.*

Третій етап:

- <Кореневий_диск>\Windows

Потім Wiper починає знищення записів у гілках реєстру:

- HKLM
- HKCU
- HKU

Спочатку програма знищить усі процеси в системі з ім'ям lsass. Потім вона встановить поточного користувача як власника розділів реєстру під цими гілками, змінить права доступу, щоб отримати повний контроль над розділами реєстру, а потім перезапише їхні значення. Wiper також рекурсивно видалить дерева підрозділів.

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

Консультація щодо загроз: DoubleZero

Wiper створює правило для отримання повного доступу до розділів реєстру

```
registryKey.DeleteSubKeyTree(OqA84Tq0.Cx0rwbl251W(new byte[]
```

Wiper видаляє дерева підрозділів у реєстрі

Після завершення всіх руйнівних дій програма Wiper вимикає систему за допомогою API-виклику ExitWindowsEx.

ОХОПЛЕННЯ

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

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

Cisco Secure Endpoint (раніше AMP for Endpoints) ідеально підходить для запобігання виконанню шкідливого програмного забезпечення, про яке йдеться в цій публікації. Спробуйте Secure Endpoint 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 Threat Defense Virtual, Adaptive Security Appliance і Meraki MX, можуть виявити шкідливу активність, пов'язану з цією загрозою.

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

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

Umbrella, захищений інтернет-шлюз (Secure Internet Gateway, SIG) компанії Cisco, 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.

Cisco Secure Web Appliance (раніше Web Security Appliance) автоматично блокує потенційно небезпечні сайти та перевіряє підозрілі сайти, перш ніж користувачі отримають доступ до них.

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.

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

Консультація щодо загроз: DoubleZero

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

Для захисту від цієї загрози доступні такі сигнатури ClamAV:

- Win.Malware.DoubleZeroWiper-9942171-0

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

d897f07ae6f42de8f35e2b05f5ef5733d7ec599d5e-786d3225e66ca605a48f53

8dd8b9bd94de1e72f0c400c5f32dcefc114cc0a5b-f14b74ba6edc19fd4aeb2a5

3b2e708eaa4744c76a633391cf2c983f4a-098b46436525619e5ea44e105355fe

30b3cbe8817ed75d8221059e4be35d5624bd6b5dc-921d4991a7adc4c3eb5de4a

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