CERT-UA

Загальна інформація

На початку лютого 2022 року Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA від одного з суб'єктів координації отримано інформацію про виявлення потенційно шкідливих програм на комп'ютерах співробітників.

За результатами проведеного аналізу встановлено, що надані об'єкти дослідження містять ознаки шкідливих програм, класифікованих як LightRope та LiteManager. Подальша кореляція індикаторів компрометації, а також тактик, технік та процедур, дозволила асоціювати виявлену активність з діяльністю групи UAC-0008 (Buhtrap). Виходячи з того, що файли шкідливих програм підписані електронним підписом, конкретно розглянута хвиля атаки розпочалася не пізніше 16.01.2022.

Довідково:

Групою Buhtrap у період з 2014 по 2016 рік здійснено низку цільових атак, здебільшого, на фінансові організації Росії. Разом з тим, у 2016 році, в т.ч., після публікації вихідного коду використовуваних шкідливих програм, за невідомих причин група почала проводити атаки виключно у відношенні конкретних державних органів та підприємств України, використовуючи, серед іншого, програмне забезпечення dnscat та LiteManager.

Виходячи з характеру впливу на інформаційно-телекомунікаційні системи атакованих організацій, очевидно, що метою групи є закріплення в корпоративній мережі жертви та налагодження процесу отримання інформації, яка обробляється в спеціалізованих системах організацій.

Для наочної демонстрації способу проникнення та використовуваного групою інструментарію, вжито заходів з дослідження інциденту, що мав місце наприкінці липня 2021 року.

Так, вірогідно, за допомогою електронної пошти зловмисниками здійснено розповсюдження посилання на шкідливий документ "2021-07-30-08-55-07.xlsm". У разі відкриття документу та активації макросу на комп'ютері жертви буде створено та виконано файл "output.exe", що класифіковано як шкідливу програму SourSnack. Останній отримає базову інформацію про комп'ютер, згенерує DNS-запит до серверу управління та, отримавши у відповідь ключ, здійснить декодування вбудованого у вигляді ресурсу конфігураційного файлу і подальше дешифрування пейлоаду, яким виявиться раніше згаданий LightRope (але без ZLIB-компресії).

Надалі, LightRope здійснить декодування вбудованого ресурсу, збереження отриманого файлу на комп'ютері та створення запланованого завдання для забезпечення персистентності та відкладеного запуску останнього. В результаті, на комп'ютері жертви буде виконано програму dnscat, яка надасть зловмисникам можливість віддаленого керування пристроєм, тунелюючи інформаційні потоки за допомогою протоколу DNS.

Зауважимо, що файли-дропери, які використовуються групою, як правило, підписано дійсним цифровим підписом.

Не вичерпний перелік шкідливих програм, що використовуються групою:

dnscat – програмне забезпечення, розроблене з використанням мови програмування C. Призначене для створення шифрованого каналу управління між клієнтом та сервером за допомогою DNS-протоколу. Підтримується операційними системами *nix та Windows. Передбачено функціонал для віддаленого виконання команд на клієнті через термінал.

LiteManager – умовно безкоштовна програма з закритим вихідним кодом для віддаленого адміністрування та управління комп'ютером. Розроблено російською компанією LiteManagerTeam. Проект є офіційним продовженням закритого проекту Remote Office Manager. Клієнтська частина доступна для операційних систем: Windows, Android, Mac OS, iOS, iPhone, iPad.

SourSnack – шкідлива програма, розроблена з використанням мови програмування C. Забезпечує отримання базової інформації про комп'ютер (GetComputerName, GetUserName, GetAdaptersInfo). Здійснює з'єднання з сервером управління для отримання ключа шифрування з метою розшифрування PE-файлу, який міститься у зашифрованому ресурсі, його збереження на комп'ютері в каталозі %APPDATA% та подальшого запуску. Для комунікації з сервером управління використовується DNS-протокол (TXT-записи); інформація про EOM кодується за допомогою hex. Для розшифрування ресурсу застосовується XOR; для розшифрування PE-файлу використовується алгоритм, заснований на математичних операціях (XOR/DIV/MUL), який реалізує перетворення блоків, довжина яких визначається ключем шифрування.

LightRope – шкідлива програма, розроблена з використанням мови програмування C. Виконує роль дропера, здійснюючи ZLIB-декомпресію (може не використовуватись) та XOR-декодування пейлоаду зі вбудованого ресурсу, а також створення запланованого завдання. З метою унікалізації створюваних файлів елементи їхніх ресурсів можуть заповнюватися довільними даними.

NTDSDumpEx – публічно доступне програмне забезпечення, призначене для отримання інформації з бази даних Active Directory %SYSTEMROOT%\NTDS.dit, а саме: даних про доменні облікові записи, членство в групах та хеші паролів.

RDPWrapper – публічно доступне програмне забезпечення, призначене для створення можливості запуску декількох паралельних RDP-сесій на комп'ютері.

Ngrok – публічно доступне програмне забезпечення, призначене для публікації будь-якого сервісу (мережевого порта) в Інтернеті шляхом тунелювання інформаційних потоків.

Індикатори компрометації

Файли:

```
1b5f0425dd76496e715bfa1aa76d306c    facebook.exe (LightRope)
42397efeaf1d971896cdc91ca024974d    lsass.exe (LiteManager)
9297e47fe1b256a8bbcb2b7a20844b2c    svchost.exe (LiteManager)
42397efeaf1d971896cdc91ca024974d    lsass.exe (LiteManager)
43a9a42b9a656d1ca39a3337a841ad5d    NTDSDumpEx.exe (NTDSDumpEx)
```

```
c1f47a14a958e2345ba929afa829c7e7    2021-07-30-08-55-07.xlsm
86926e56e4f6d854161066b5989a350e    output.exe (SourSnack)
3dcec8f6ba15e801b63b7c21a6b966fb    dnsoption.exe (LightRope_v2)
86f322fe52829b8b8094d053ed648a65    CDSSyncReporting.exe (dnscat)
```

Мережеві:

```
hxxps://mail.nais-gov[.]org/2021-07-30-08-55-07.xlsm
widget.forum-pokemon[.]com
ns.ns2-dns[.]com
ns.ns3-dns[.]com
ns3-dns[.]com
ns2-dns[.]com
cs1.wpc-v0cdn[.]org
wpc-v0cdn[.]org
ipv6-wpnc[.]net
alt-2cdn[.]net
nais-gov[.]org
nais-gov[.]com
91[.]240.86.200
89[.]108.101.61
45[.]76.85.232
185[.]162.9.218
95[.]179.135.36
91[.]240.86.200:5651
```

Хостові:

```
Mikael LLC (administrator@mikael-company[.]ru)
George Alan Developments Incorporated

C:\windows\system32\wbem\wmic.exe process where
ExecutablePath='C:\\ProgramData\\lsass.exe' delete
C:\windows\system32\wbem\wmic.exe process where
ExecutablePath='C:\\ProgramData\\svchost.exe' delete
C:\windows\system32\schtasks.exe /delete /tn "Network Security
Update" /f
C:\windows\system32\schtasks.exe /create /sc onstart /tn "Network
Security Update" /tr "C:\ProgramData\lsass.exe" /ru SYSTEM
%PROGRAMDATA%\lsass.exe
%PROGRAMDATA%\svchost.exe
%PROGRAMDATA%\config.xml
%PUBLIC%\output.exe
%APPDATA%\dnsoption.exe
%APPDATA%\Microsoft\Windows\CDSSyncReporting.exe
```

Додаткова інформація

· Рекомендуємо зменшити так звану «поверхню атаки» (attack surface), в тому числі, за рахунок фільтрації мережевих портів для вихідних інформаційних потоків.

· З метою виявлення фактів тунелювання інформаційних потоків за допомогою DNS-протоколу, здійснити перевірку та подальший моніторинг відповідних журнальних файлів на предмет наявності подій з аномальною довжиною DNS-запиту.

· Реалізувати можливість централізованого управління засобами антивірусного захисту на всіх без виключення комп'ютерах; передбачити можливість вжиття заходів захисту на комп'ютерах (запуск Yara-правил, видалення шкідливих файлів, пошук за індикаторами тощо), в першу чергу, в режимі віддаленого доступу.

Графічні зображення

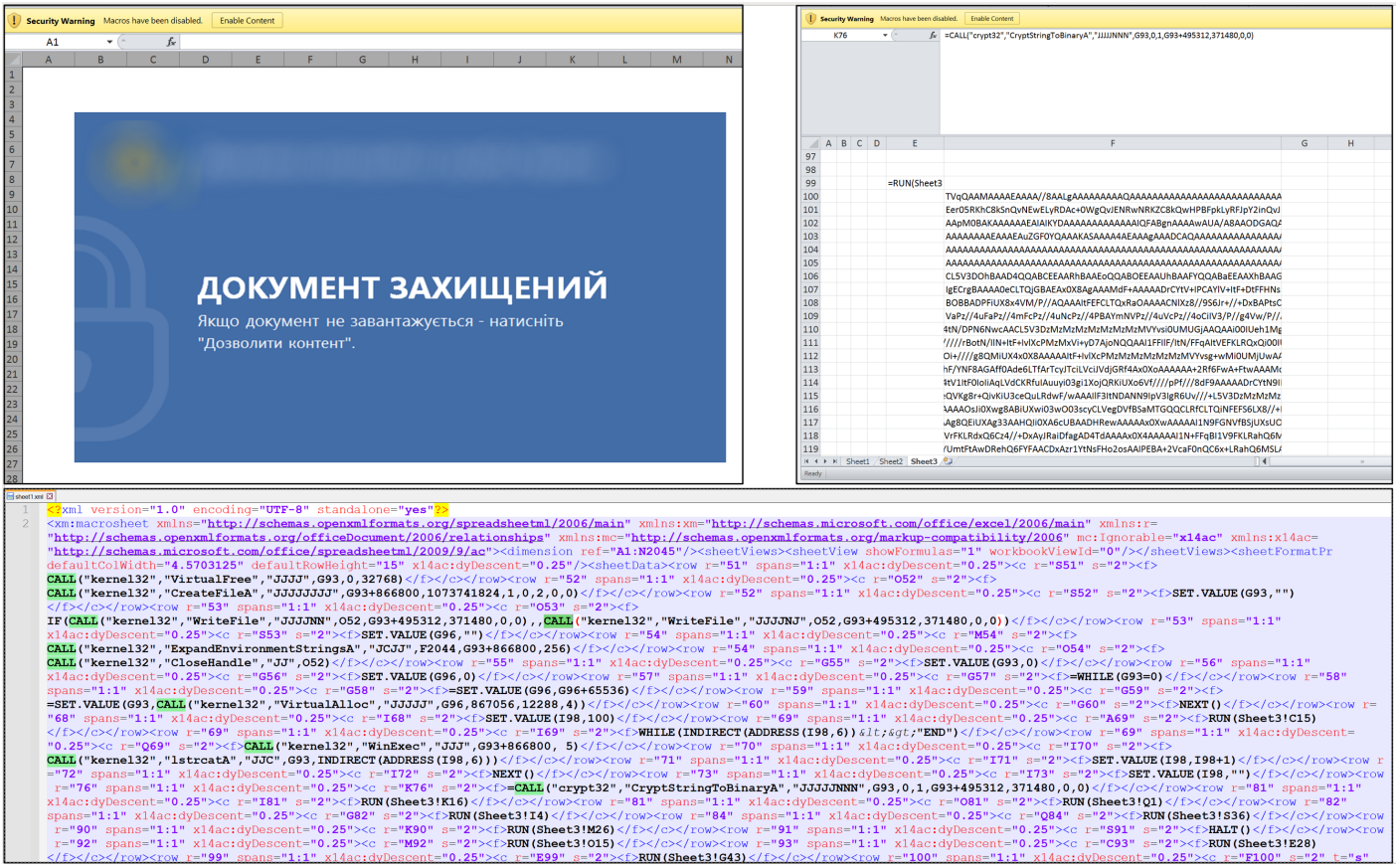

Рис. 1 Приклад шкідливого документу