

Масове розповсюдження шкідливої програми JesterStealer з використанням тематики хімічної атаки (CERT-UA#4625)

Загальна інформація

Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA виявлено факт масового розповсюдження електронних листів з тематикою "хімічної атаки" та посиланням на XLS-документ з макросом.

У разі відкриття документу та активації макросу, останній здійснить завантаження і запуск EXE-файлу, що, в подальшому, призведе до ураження комп'ютера шкідливою програмою JesterStealer. Зауважимо, що завантаження виконуваних файлів здійснюється зі скомпрометованих веб-ресурсів.

За функціоналом згадана програма є стилером, що забезпечує викрадення автентифікаційних та інших даних з Інтернет-браузерів, MAIL/FTP/VPN-клієнтів, криптовалютних гаманців, менеджерів паролів, месенджерів, ігрових програм тощо. Викрадені дані через статично визначені адреси проксі (в т.ч., в мережі TOR) передаються зловмиснику в Telegram. Також, реалізовано функціонал протидії аналізу (anti-VM/debug/sandbox). Механізм забезпечення пересистентності відсутній - після завершення роботи програма видаляється.

Активність тимчасово відстежується за ідентифікатором UAC-0104.

Індикатори компрометації

Файли:

d5c9fd40738ac33f59467811c1ceb30b	
5df051b418cd3d51cfcfe17685275e03b0efdf9a80ce237d2deccb3749576092	Map023.xlsb
d80f1d64e07909d29d7a2a1888931af9	
f963ed8559ade984e81a95238c4875d4c0a6ff14a7695630429bf98d4235d596	Map021.xlsb
4742c9d0a6b5b3b10ae7eb8f6b3e2fe6	
ef7ddd544267a8781c99f08146d455aa08beab867e0453b07f1131edcbef92b2	Map026.xlsb
70ef45cb31af0b6f37be051de4170839	
a2234ee40097fa832eb3a533840e86de3933cf216fbf8445d2946cb7b61c887b	Updater-
Microsoft.exe	
8f32a69ecd777f99d67bd18363afa25d	
da0de03004e3ec2711ddc71e119ecc252568b2c9300b98dd2434b8e83ce02dc9	a1.exe
31600c8891e3902a0fe2d2985d25ca34	
f7477c153f861d8c57d4794481445134426d634b9f4ca58d4d8519c4b0cd0085	ckloc
(JesterStealer)	

Мережеві:

tachikawaobs@sv5206.xserver.jp
157[.]112.183.47
igshop[.]net (Скомпрометований веб-ресурс)

dcshost[.]net (Скомпрометований веб-ресурс)
 marmaris.com[.]ua (Скомпрометований веб-ресурс)
 autodoka.com[.]ua (Скомпрометований веб-ресурс)
 lightnogu5owjlllyo4tj2sfos6fchncidlgo6c7e6fz2hgryhfhojd[.]onion
 wasabiwallet[.]online
 ip-api[.]com (Легітимний сервіс)
 hxxps://igshop[.]net/uploads/Map026.xlsb
 hxxps://igshop[.]net/uploads/Map023.xlsb
 hxxps://igshop[.]net/uploads/Map021.xlsb
 hxxps://igshop[.]net/uploads/Updater-Microsoft.exe
 hxxps://dcshost[.]net/mail/OfficeUpdaterNew.exe
 hxxps://marmaris.com[.]ua/misc/Updater-Microsoft.exe
 hxxps://autodoka.com[.]ua/extra/Updater-Microsoft.exe
 hxxp://lightnogu5owjlllyo4tj2sfos6fchncidlgo6c7e6fz2hgryhfhojd[.]onion/stealer/102697744
 hxxp://ip-api[.]com/json (Легітимний сервіс)
 tcp://wasabiwallet[.]online:7777

Хостові:

KCU\SOFTWARE\kxialunboq\state

Графічні зображення

The collage consists of three main parts:

- Top Left:** A screenshot of an email from 'Крістіна Симоненко' with a subject 'Термінова інформація'. The body contains a warning about a chemical attack on June 1st and a link to a map: <https://igshop.net/uploads/Map026.xlsb>.
- Top Right:** A list of browser extensions and their names, including [Vault], [Credman], [Networks], [Screenshots], [Steam], [Gaming], [FilterZilla], [WinSCP], [CoreFTP], [Snowflake], [NordVPN], [EarthVPN], [WindscribeVPN], [AzireVPN], [VPN], [Chrome Passwords], [Chrome CreditCards], [Chrome Tokens], [Chrome Autofill], [Chrome Extensions], [Chrome Bookmarks], [Firefox Passwords], [Firefox Cookies], [Firefox Autofill], [Firefox Bookmarks], [Telegram], [Discord], [Pidgin], [Outlook], [Foxit], [MailBird], [Viber], [WhatsApp], [Signal], [Signal], [Random], [Messengers], [Balance], [MoneroCore], [BitcoinCore], [DashcoinCore], [DogecoinCore], [LitecoinCore], [Electrum], [Exodus], [Atomic], [TonMail], [Jaxx], [Zcash], [Daedalus], [Cosmos], [Wasabi], [Guarda], [BitWarden], [KeepPass], [NordPass], [IPassword], [RoboForm], [Grabber], and [Grabber].
- Bottom:** A screenshot of a Microsoft Excel spreadsheet with columns A-E. Row 1 contains: 'image', 'MSXML2.ServerXMLHTTP.6.0', 'GET', 'https://marmaris.com.ua/misc/Updater-Microsoft.exe', 'ADODB.Stream'. Below the spreadsheet is a network traffic capture showing a request to the map link.