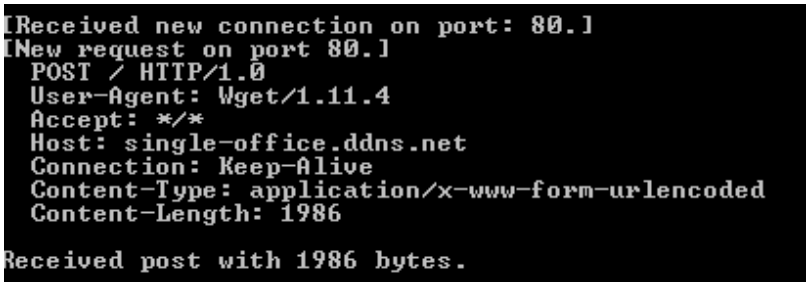
CERT-UA

Archived: 2026-04-05 13:36:43 UTC

Виявлено розсилку шпигунського програмного забезпечення типу Pterodo, яке розповсюджується за допомогою електронної пошти під виглядом офіційної кореспонденції з доменів .gov.ua. Насправді, адреси відправників змінено, а листи відправляються з електронних адрес porohman@i.ua та porohwoman@i.ua.

До електронних листів прикріплений архів, який містить spisok_24.08.2018.com та НПУ.docx файли. За результатами аналізу встановлено, що при активації виконуваних файлів з архіву НПУ.rar виконувана компонента spisok_24.08.2018.com (exe файл) автоматично розпаковується на виконувані (Icloud.exe, Iclouding.exe, ipad.system) та командні файли (iclouds.cmd, iclouds.cmd), метою яких є збір даних враженої системи та передача даних програмою *Iclouding.exe* до командного серверу single-office.ddns[.]net (на момент аналізу IP-адреса домену була 95.142.45[.]58).



Компоненти вірусу маскуються під програмне забезпечення корпорацій Apple та Adobe. Крім того, шкідливе програмне забезпечення може видаляти системні файли та власні файли для приховування слідів діяльності, що може спричинити не можливість запуску операційної системи.

Під час активної дії виконуваної компоненти spisok_24.08.2018.com (або "забезпечте моніторинг мережевого обладнання на факт звертання до підозрілих адрес.com") створюється процес Icloud.exe який в свою чергу запускає cmd.exe у прихованому режимі та процес timeout.exe, мета якого періодично поновлювати зв'язок з командним сервером для передачі та отримання інформації. Не виключено отримання вказівок з командного сервера.

Зловмисники за допомогою даного шпигунського програмного забезпечення легко підключаються до системи, стежать за діями жертви і крадуть її конфіденційну інформацію.

Індикатори компрометації (IOC):

Шкідливі домени та IP (C2):

single-office.ddns[.]net

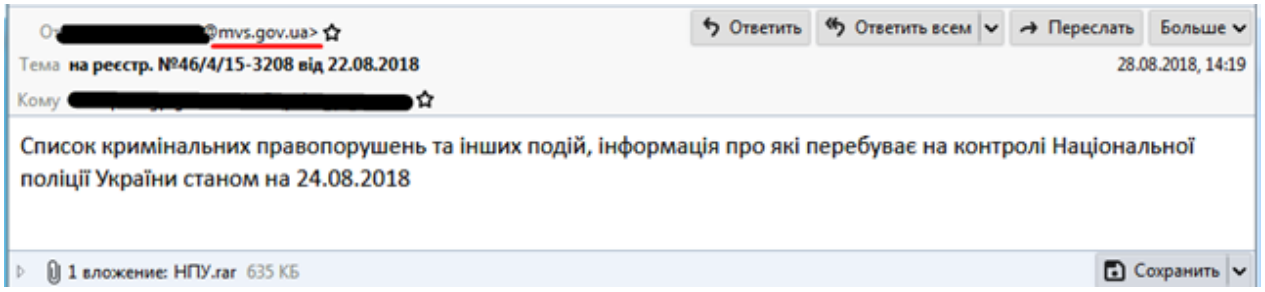
95.142.45[.]58

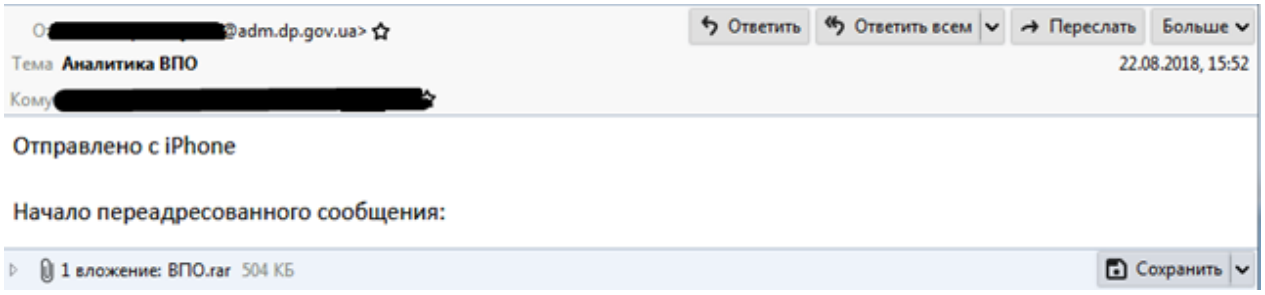
Email:

porohman@i.ua

porohwoman@i.ua

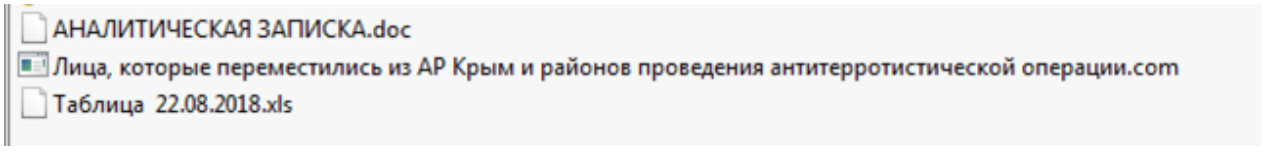
Приклад повідомлень :





Вміст вкладень може відрізнятися, але спільним є те, що в архіві міститься файл (або файли) з схожою на достовірну інформацію та виконуваний файл з розширенням .com, який і є вірусом.

Приклади вкладень:



Шкідливі файли:

"Лица, которые переместились из АР Крым и районов проведения антитерротистической операции.com"

MD5: 76741F7B1FF4860475B34BAD2606DD16

https://www.virustotal.com/#/file/97fe980403bebf0bd2b1dda6c0c674787fb945827fedabb0656ee40eb92a6efa/detection

spisok_24.08.2018.com

MD5: 8717F3723C2BB557B548EF8483BEA91C

https://www.virustotal.com/#/file/50181154303284c8dbd64287efa16bca82a350f565b32b0d9f2d9a8aedc889b4/detection

./ipad.system

MD5: e5d73afdbd5b440cc45e59e6db509d71

https://www.virustotal.com/#/file/b024234d583b3adb5ae4ec3809d316b4f2f48839b3d9baec615750f35ce231cc/detection

./IcloudSecurity.lnk

MD5: 355b8b3170f01c5db98461b7451008d6

https://www.virustotal.com/#/file/cce68c4b705595610289293922b96513d71d8b376f6e9fe0b32513ccf1274178/detection

./НПУ.docx

MD5: 23577b4223db2762bc4521dcc8c9e5c5

/Iclouding.exe

MD5: 834c709455bfefb9b0e8976bad13a8f4

.

./icloud.cmd

MD5: 9d03d5fb154b1cb54da8a6ab71999251

./iclouds.cmd

MD5: 1d4874db97fcce7c3537f49ec8aa0672

Рекомендації CERT-UA:

- рекомендуємо адміністраторам слідкувати за спробами підключення до зазначеного C2 домену та IP, для виявлення потенційно заражених систем.

- уникайте повідомлень вказаного та схожого змісту та застережіть персонал від запуску вкладень у підозрілих повідомленнях та файлів з виконуваними форматами ;

- адміністраторам поштових серверів, зверніть увагу на фільтрування вхідних/вихідних інформаційних потоків, зокрема поштового веб-трафіку, налаштуйте захист від спаму та підробки адреси відправника за допомогою технологій DKIM, SPF, DMARC;

- перевірте журнальні файли на предмет наявності записів з зазначеними вище індикаторами;

- обмежіть можливість запуску виконуваних файлів (*.exe) на комп’ютерах користувачів з директорій %TEMP%, %APPDATA%.

- регулярно оновлюйте антивірусну базу та сканувати потенційно заражені системи;

- регулярно робіть резервні копії важливого програмного забезпечення та данних;

- періодично робіть повну перевірку "чутливих" комп'ютерів на предмет наявності шкідливого програмного забезпечення;

- регулярно оновлюйте програмне забезпечення;
