Лабораторія комп'ютерної криміналістики
info@cyberlab.com.ua www.cyberlab.com.ua

ІнфоОберіг
welcome@infooberig.com www.infooberig.com

Загальний огляд

10-11 грудня 2018 року зафіксовано чергову розсилку шкідливого програмного забезпечення на електронні адреси приватних нотаріусів Нотаріальної палати України. Мета атаки - внесення несанкціонованих дій в державні реєстри від імені заражених нотаріусів.

За попередніми даними розсилка направлена на нотаріусів м.Києва та Сумської області.

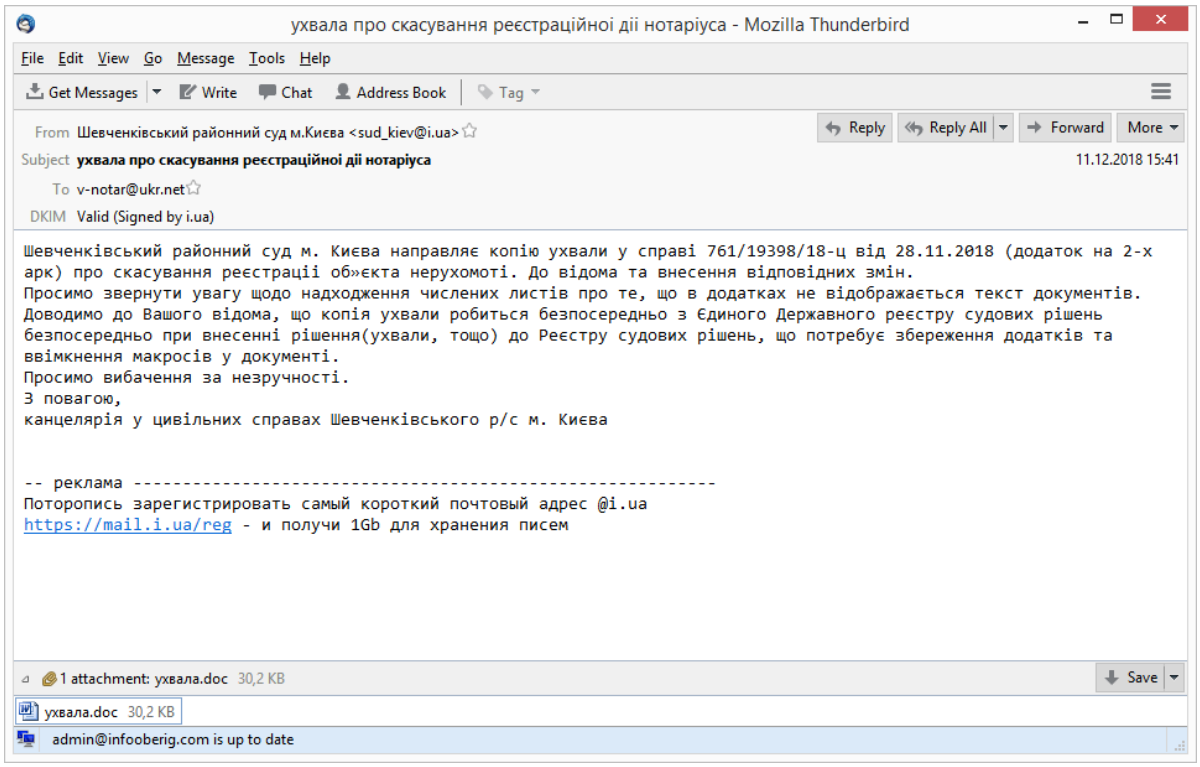
Атака виконувалась з використанням соціальної інженерії - листи надходили від імені нібито Шевченківського районного суду м.Києва. На відміну від попередніх розсилок, в цей раз розсилались заражені файли документів Word (в форматі docx), які містили два варіанти поширення шкідливої програми:

- документ Word з макросом
- документ Word з вбудованим шкідливим файлом.

Після відкриття заражених документів на комп'ютері нотаріуса відбувається прихована від користувача установка модифікованої версії програми для віддаленого доступу **RMS TektonIT**. В подальшому вказана програма використовується зловмисниками для віддаленого підключення до комп'ютера нотаріуса та встановлення низки інших програм, які дозволяють викрасти паролі доступу та створити віртуальну копію апаратного ключа доступу до державних реєстрів. В результаті успішних атак в Єдині та Державні реєстри від імені заражених нотаріусів вчиняються незаконні нотаріальні дії.

Слід звернути увагу, що на момент розсилки і впродовж 4 годин після неї **шкідливі файли не виявлялися жодним антивірусом** (за даними сервісу VirusTotal).

Зафіксовано декілька варіантів шкідливих листів, зразок наведено на рисунку.



Лабораторія комп'ютерної криміналістики
info@cyberlab.com.ua www.cyberlab.com.ua

ІнфоОберіг
welcome@infooberig.com www.infooberig.com

Розсилки здійснювалися з електронних адрес **sud_kiev@i.ua, shev_sud@ukr.net, shevchenk_sud@ukr.net**, від в якості відправника зазначено «**Шевченківський районний суд м.Києва**», тема повідомлень «**ухвала про скасування реєстраційної дії нотаріуса**».

Індикатори компрометації

Файли

Ім'я файлу	Розмір, байт	MD5
ухвала.doc	30 948	787b61b8cf8bcbf84b143372c58e3d8b
Ухвала1.docx	3 203 028	36d691c4f47a921c8a2bda9a601bd847
Ухвала2.docx	3 207 365	1848593e91f3f754f4b7169ea96c551a
system32.exe	3 356 659	cb983da73e4fe2e412b2cb15400f8146
i.cmd	243	a09b1fae1a7f4daf463cafea31884641
syst.dll	2 955 002	33c7e9f9ec79de9cbb6803c240ed29af
exit.exe	46 064	1ef6de479454047ce01a8a0fb71b0167
winserv.exe	2 786 296	cf2ab077a46219b6ce4a53517dd489ea
i.cmd	264	cf96a6e7699ea815789970bf56b12c7d
settings.dat	2 915	22a63eb40b804dbafd59fa7f554dd23b
Ошибка.exe	3 350 192	67f4847cfffa7c27d42b1b5673fb43dd
i.cmd	243	a09b1fae1a7f4daf463cafea31884641
syst.dll	2 951 770	6a4c03834addf5f747df4a6f92084f7c
exit.exe	42 443	54c67201a45190c0642854c875ead753
settings.dat	2 916	2dea8b4a9a8c549f460057653732666b

Директорії

C:\ProgramData\Microtik\

Ключі реєстру RMS

Ключ	Параметр	Значення
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\	Microtik	c:\ProgramData\Microtik\winserv.exe
HKCU\SOFTWARE\tektonit\Remote MANIPULATOR System\		

Сервери

gogiloudg2.temp.swtest.ru
109.196.164.98
104.128.230.148