УДК 32.019.5:004.493

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНОГО ВІРУСУ STUXNET

Руденко О.Я.
Національний університет «Острозька академія», студентка

Stuxnet – це новий вірус, руткіт, що заражає комп'ютери із встановленою операційною системою (ОС) Microsoft Windows [7]. Вперше шкідливе програмне забезпечення (ПЗ) виявила білоруська антивірусна програма VirusBlokAda у червні 2010 року [5]. Відповідно до висновків співробітників вірус пошкоджує не лише комп'ютери звичайних користувачів, але і промислових систем, що управляють автоматизованими виробничими процесами.

Stuxnet використовує чотири недоліки Microsoft Windows:

- вразливість «нульового дня» (zero-day);
- дуже велике навантаження на апаратну частину комп'ютера при використанні усіх зручностей цієї ОС;
- неповна багатофункціональність (одночасно можуть виконуватися лише 4-5 об'ємних за розміром додатки. Якщо некоректна робота одного із них приведе до руйнування системних файлів, то Windows працюватиме зі збоями);
- критичність часу: неможливість застосовувати ОС для обробки сигналів, що надходять ззовні, у реальному масштабі часу. У цьому випадку Windows просто «зависне».

Поширення

Слабкі сторони Windows лише сприяють особливому механізму поширення рулкіту за допомогою USB-flash накопичувачів. Використання справжніх цифрових підписів (Realtek та JMicron) дозволило уникнути захисну дію антивірусних програм. Нова вразливість дозволяє завантажувати будь-яку DLL-бібліотеку як тільки користувач відкриє вміст флеш-накопичувача. Разом із шкідливим .DLL-файлом є .LNK-файл. Який на перший погляд є звичайним ярликом. Проте його відображення у Microsoft Windows чи Total Commander автоматично виконує .DLL-файл, що знаходиться поруч. Після цього можна вважати, що Stuxnet потрапив у комп'ютер.

Встановлення

Вірус копіює файл, що його виконує, як %System%\drivers\mrxcls.sys. Для автоматичного запуску наступного старту системи вірус створює ключ реєстру служби:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls]
"Description"="MRXCLS"
"DisplayName"="MRXCLS"
"ErrorControl"=dword:00000000
"Group"="Network"
"ImagePath"="\\??\\%System%\Drivers\\mrxcls.sys"
"Start"=dword:00000001
"Type"=dword:00000001
```

Створює файл %System%\drivers\mrxnet.sys розміром 17400 байт, що визначається як Rootkit.Win32.Stuxnet.b. Крім того, вірус створює файли, які містять його код і дані у зашифрованому вигляді:

- %windir%\inf\mdmcpq3.pnf (4633 байт);
- %windir%\inf\mdmeric3.pnf (90 байт);
- %windir%\inf\oem6c.pnf (323848 байт);
- %windir%\inf\oem7a.pnf (498176 байт).

Загальний розмір вірусу – 26616 байт. Вразливість починає проявлятися тоді, коли користувач пробує переглянути вміст кореня змінного носія файловим менеджером, з опцією відображення позначень файлів. Після цього Stuxnet активується і негайно приховує власні шкідливі файли [6].

Деструктивна дія

Stuxnet призначений для внесення шкідливого коду (inject) у процеси користувацького режиму. Тому вірус завантажує динамічну бібліотеку DLL у системні процеси в (svchost.exe, services.exe, lsass.exe), а потім створює бібліотеки іменами виду (kernel32.dll.aslr., shell32.dll.aslr.).

Впроваджуваний код міститься у файлі %WinDir%\inf\oem7A.PNF у зашифрованому вигляді. Саме він і є основним функціональним елементом шкідливого програмного забезпечення, що дає можливість поширення Stuxnet на змінних носіях, а також збір різних даних про роботу системи.

Маючи список комп'ютерів у локальній мережі, вірус перевіряє, чи запущений хоча б на одному із них Microsoft SQL сервер. Якщо такий сервер виявлений, вірус постарається підключитися до бази даних, використовуючи ім'я користувача і пароль WinCCConnect/2WSXcder. Інформація збирається з файлів з такими розширеннями: *.S7P, *.MCP, *.LDF. пошук необхідних файлів здійснюється на всьому жорсткому диску комп'ютера. Зібравши потрібні дані, рулкіт відправляє їх за допомогою Інтернет на сервери зловмисників у зашифрованому вигляді. Файл цього вірусу підписаний цифровим підписом Realtek Semiconductor Corp [4].

Для того, щоб уникнути або хоча б зменшити ризик зараження вірусом, варто посилити контроль мережного доступу до комп'ютерів, підтримувати актуальну версію антивірусного програмного забезпечення, мінімізувати використання комп'ютерів неперевірених USB-носіїв.

Список використаних джерел

1. Безопасность SCADA: Stuxnet – что это такое и как с ним бороться? [Электронный ресурс] / П. Волобуев. – Режим доступа : URL. http://www.securitylab.ru/analytics/400024.php. – Название с экрана.
2. За червём Stuxnet и впрямь стояли израильские спецслужбы [Электронный ресурс] / Д. Целиков. – Режим доступа : URL. http://soft.compulenta.ru/587637/. – Название с экрана.
3. Кивино гнездо: Боевой червь Stuxnet [Электронный ресурс] / Б. Киви. – Режим доступа : URL. http://www.computerra.ru/own/kiwi/564744/. – Название с экрана
4. Официальное письмо Siemens о вирусе Stuxnet с комментариями [Электронный ресурс] / С. Михайлин. – Режим доступа : URL. http://housea.ru/index.php/pulse/16012. – Название с экрана.
5. Шпионский ярлык: история трояна Stuxnet [Электронный ресурс] / А. Синцов. – Режим доступа : URL. http://xakep.ru/post/53950/. – Название с экрана.
6. Rootkit.Win32.Stuxnet.a [Електронний ресурс]. – Режим доступу : URL. http://www.securelist.com/ru/descriptions/15071647/Rootkit.Win32.Stuxnet.a#doc1. – Назва з екрану.
7. Stuxnet и промышленная безопасность [Электронный ресурс] / А.В Фрейдман. – Режим доступа : URL. http://www.phocus-scada.com/rus/pub/Stuxnet&IndustrialSecurity.html#Toc41. – Название с экрана.