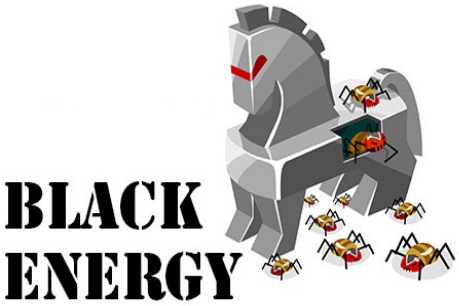
Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины



Благодаря бдящему международному InfoSec сообществу, вопреки упрямой индифферентности самих атакованных украинских организаций, видимо, яро пекущихся о репутации, история с BlackEnergy2/3 набирает обороты. Не испугавшись анонсированных украинским правительством устрашающих намерений создать перечень объектов критической информационной инфраструктуры, да что там перечень – **правила** отнесения организаций к перечню объектов критической информационной инфраструктуры, а также – вот уже почти-почти (уже как лет 5) изданного Закона Украины «Об обеспечении кибербезопасности Украины», дерзкие злоумышленники таки покусились на энергетические предприятия нашей страны и, не много не мало, доказали возможность выведения из строя автоматизированных систем управления технологическими процессами, в нашем случае – электрических подстанций. Эта атака, если не брать во внимание скептицизм в отношении возможности взлома отечественных SCADA-систем («что там ломать?»), привела к реальным последствиям, сказавшимся непосредственно на гражданах Украины.

Если бы не приданные публичности исследования компании ESET [1][2][3], а также заметки иностранных новостных СМИ [4][5][6], самая выдающаяся отечественная «кибер-история» конца 2015 года так бы и канула в лету.

Учитывая недостаток пригодного для восприятия среднестатистическим украинцем новостного материала, мы также решили внести лепту в правое дело и опубликовать результаты исследования украинской компании CyS Centrum в отношении направленных на Украину кибер-атак.

Не вдаваясь в технические подробности и, прекрасно осознавая наличие множества материалов в иностранных СМИ, мы сделаем краткий обзор атак, ассоциированных с вредоносной программой BlackEnergy2/3. К слову говоря, хоть и шутя, отметим, что атаки на энергетический сектор наконец-то оправдали название вредоносной программы, содержащей слово «Energy».

Итак, по порядку.

12 мая 2014 года (понедельник) выявлены подозрительные, хотя и весьма грубые, попытки доставить посредством электронной почты ряду украинских предприятий, относящихся к сфере железнодорожных перевозок, вредоносной программы. Хоть упомянутый файл и детектировался

изначально порядка 16-тью из 52 антивирусных продуктов, хоть он и был исполняемым PE-файлом с измененной по подобию MS Office Word иконкой, всё же заражения избежать не удалось. По всей вероятности на то время злоумышленнику было достаточно подделать адрес отправителя, сделать тему и тело письма поправдоподобнее, а также добавить в структуру исполняемого файла документ-приманку. Примеры таргетированного письма и документа-приманки отображены на рис. 1-2. Не смотря на то, что эта первая кибер-кампания была направлена на все шесть железных дорог, относящихся к сфере управления «Укрзалізниці» (Государственной администрации железнодорожного транспорта Украины), среди «счастливых» получателей письма с вредоносным вложением было, к примеру, Прикарпатьеоблэнерго, которое 23 декабря 2015 года (!) абсолютно честно известило общественность о проведенной на предприятие атаке [7]. Это позволяет сделать предположение, что уже в мае 2014 года, больше чем за полтора года до «декабрьских событий» с украинскими облэнерго, вредоносную программу BlackEnergy2/3 доставляли (пытались доставить) на атакуемый энергетический объект.

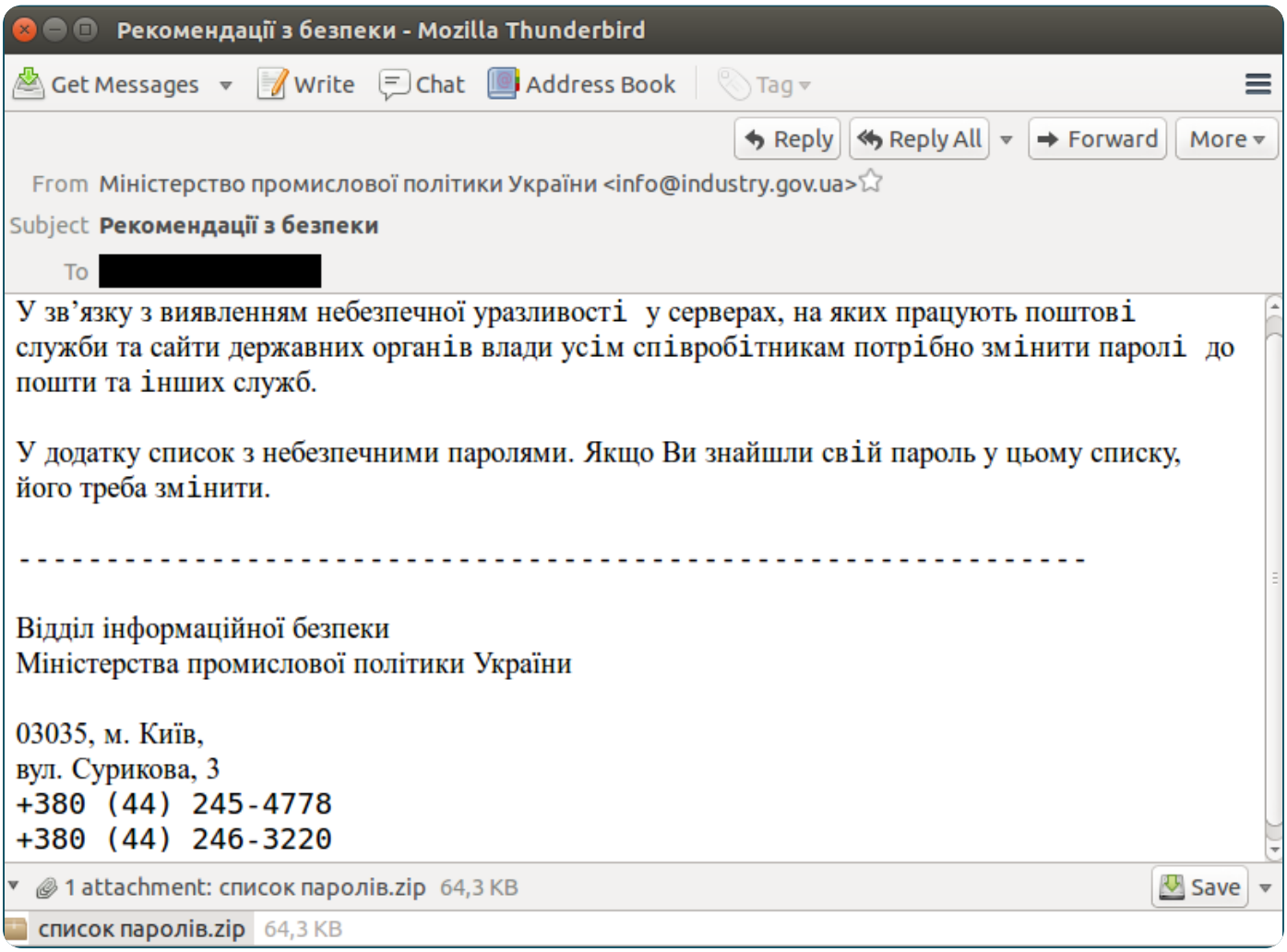


Рис. 1

1	123456
2	admin
3	password
4	test
5	123
6	123456789
7	12345678
8	1234
9	qwerty
10	asdf
11	111111
12	1234567
13	123123
14	windows
15	123qwe
16	1234567890
17	password123
18	123321
19	asdf123
20	zxcv
21	zxcv123
22	666666
23	654321

Рис. 2

Следует также отметить, что незамысловатый вредоносный файл, которым начали атаки в мае 2014 года, после его запуска устанавливал в атакуемой системе вредоносную программу BlackEnergy3 – облегченную «Lite» версию BlackEnergy способную, среди прочего, собрать информацию об атакуемом объекте для последующего развития атаки. Забегая наперед, отметим, что такой разведывательно-поступательный подход как раз и может объяснять тот факт, что BlackEnergy2, тот, что kernel-mode, то бишь исполняемый в виде вредоносного драйвера, заранее (!) содержал в своем конфигурационном файле перечень прокси-серверов, локально используемых в корпоративных вычислительных сетях атакуемых объектов.

Особенно обеспокоенным и ответственным системным администраторам, счастливым обладателям прокси-серверов в своих компьютерных сетях, рекомендуем проверить файлы регистрации событий на предмет содержания в них HTTP-запросов, содержащих следующие индикаторы компрометации (по IP-адресу или URI):

hxxp://95.211.122.36/update/cache.php

Кроме того, мы также рекомендуем проверить логи серверов электронной почты. В качестве индикатора можно использовать данные следующей строки из заголовоков электронного сообщения:

```
Received: from geodac.di.ubi.pt (geodac.di.ubi.pt [193.136.66.3])
```

По всей видимости, для организации рассылок вредоносных писем злоумышленники решили

"подломать" один из серверов Португальского университета "University of Beira Interior"

К слову говоря, мы оказывали помощь двум пострадавшим на то время организациям. Отметим, что в результате проникновения, группировка злоумышленников, как правило, получает доступ ко всему серверному и активному сетевому оборудованию, в последствии выводя его из строя. В одной из организаций, потерпевшей «крушение», как раз и были обнаружены скрипты, в коде которых атакующие оставили послания Лаборатории Касперского и компании Cisco (указанный рисунок (Рис. 9) доступен здесь). Правда, одному из атакованных предприятий посчастливилось иметь очень опытного и ответственного сотрудника, усилия которого позволили побороть угрозу и не допустить разрушений.

Так закончилась (или началась) история с «майским» (2014 года) BlackEnergy2/3.

Уже летом, примерно 13 августа 2014 года волна атак с применением BlackEnergy2/3 обрушилась снова. В этот раз они удивили всех, так как присылаемый по электронной почте вредоносный файл MS Office Power Point содержал 0-day эксплойт. На момент атаки, а также целых два месяца после нее, вредоносный файл с эксплойтом не детектировался ни одни из представленных на VirusTotal антивирусов. Позднее, после «responsible disclosure» 0-day уязвимости был присвоен идентификатор – CVE-2014-4114.

Вредоносное электронное письмо как всегда содержало очень релевантный, внушающий доверие текст и документ приманку. Примеры (хоть и не впервой) отображены на рис. 3-5.

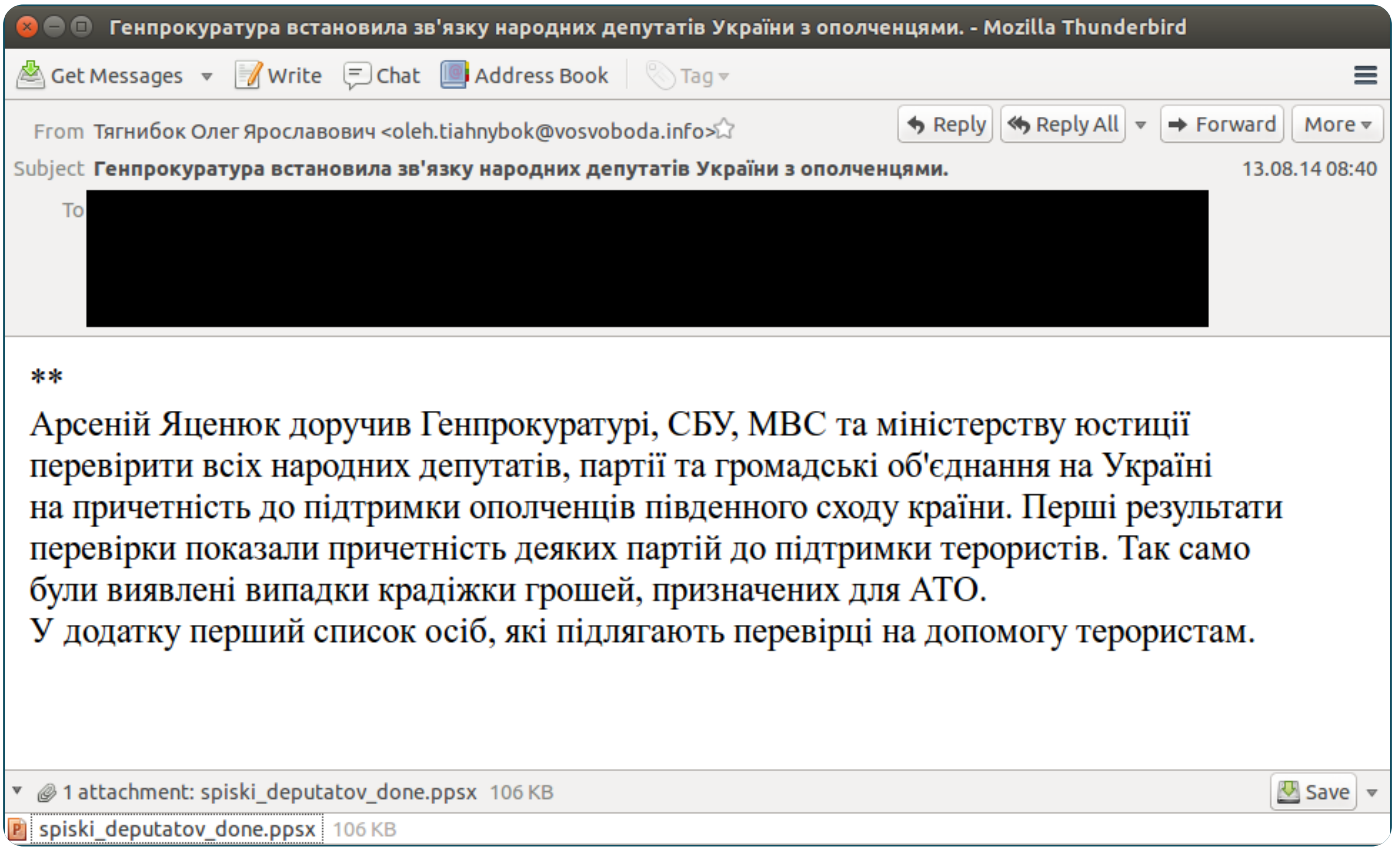


Рис. 3

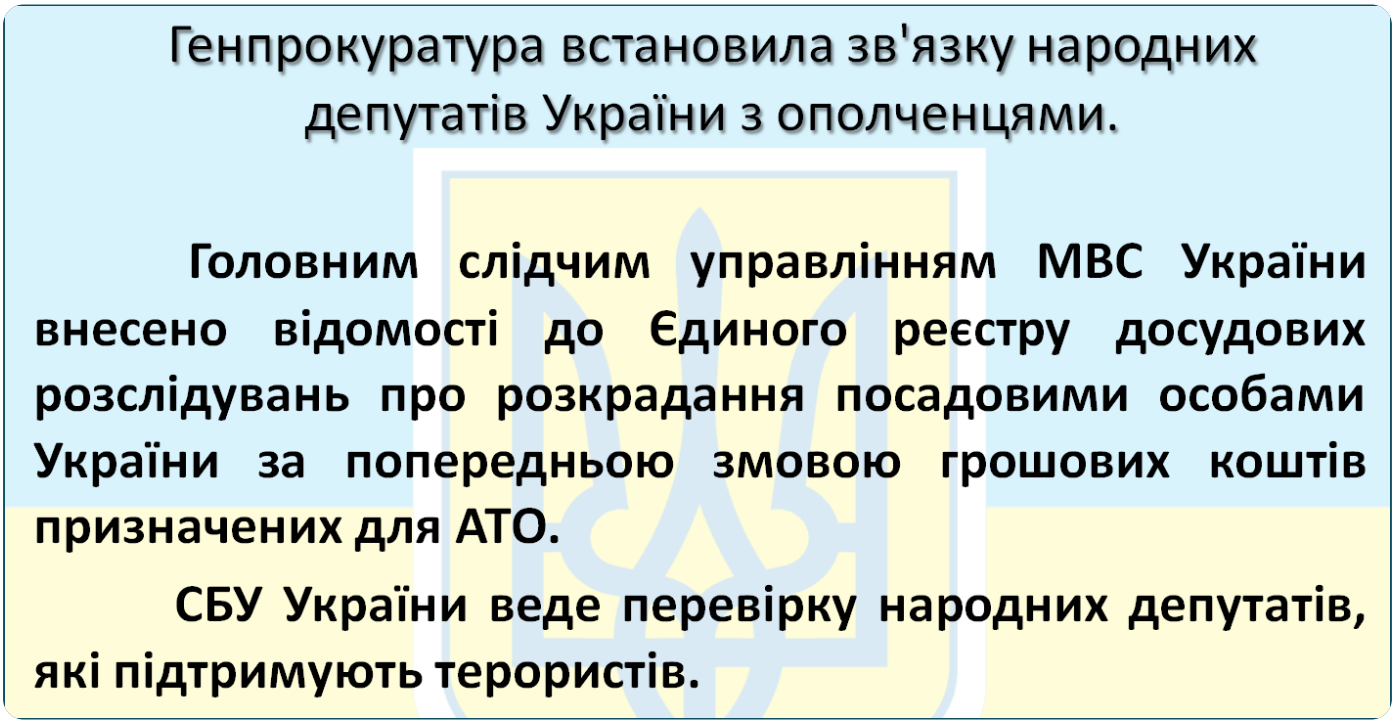


Рис.4

Рис. 5

Как и прежде, в результате эксплуатации уязвимости вредоносная программа BlackEnergy3 устанавливалась на компьютер, что, в последствии, влекло за собой установку вредоносных драйверов BlackEnergy2. В данном случае вредоносная нагрузка, после эксплуатации уязвимости, скачивалась с SMB-ресурса (Рис. 6). Более детальный анализ можно найти, например, здесь [8][9].

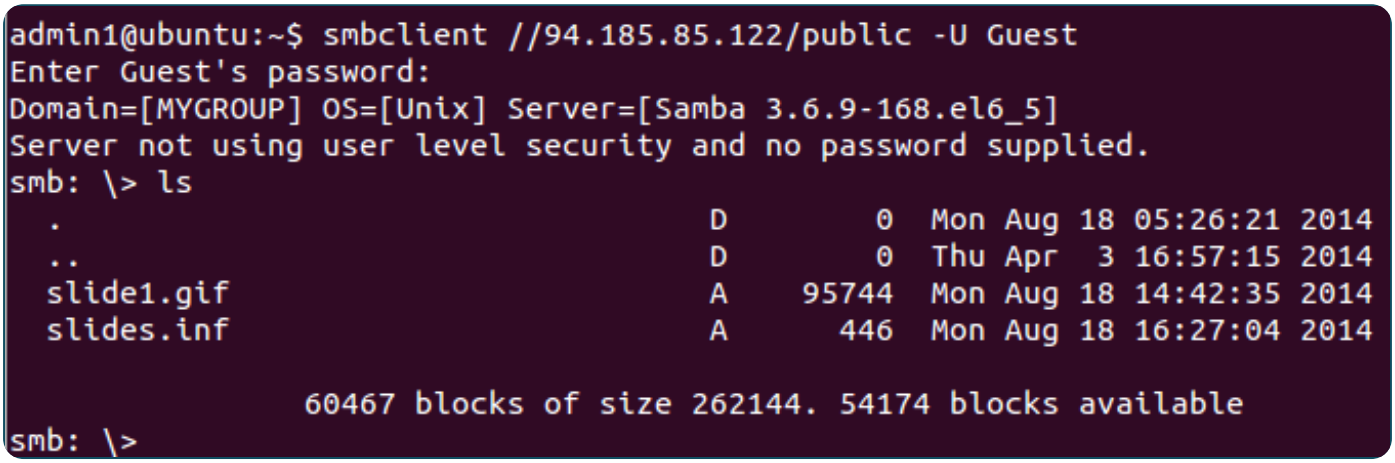


Рис. 6

При анализе одного из таких таргетированных писем в замешательство приводит тот факт, что жертвами рассылки, среди прочих, были несколько областных государственных администрации Украины и архивно-исторические организации. Известный нам перечень атакованных во время второй кибер-кампании объектов отображен ниже:

- Electronic Resource Preservation and Access Network
- Department of History, Michigan State University
- Digital Preservation Europe
- Germans from Russia Heritage Collection

- Тернопільська облдержадміністрація
- Закарпатська облдержадміністрація
- Дніпропетровська облдержадміністрація
- Миколаївська облдержадміністрація
- Державний архів Чернівецької області
- Центральний державний кінофотофоноархів України імені Г. С. Пшеничного

- Центр по проблемам информатизации сферы культуры Министерства культуры Российской Федерации
- Генеалогическое агентство Литера ру

На данном этапе описание атаки, проводимой в августе 2014 года, окончим. Все, относящиеся к делу индикаторы компрометации буду приведены ниже.

В начале марта 2015 года были получены сведения о проведении атаки с применением вредоносной программы BlackEnergy2/3 в отношении радиовещательных компаний Украины. Отличительной особенность являлось то, что присылаемые по электронной почте вредоносные документы (.xls и .pps) содержали макрос и JAR-файл, соответственно, который в свою очередь запускал PE-файл. Тематика документов-приманок была посвящена, в т.ч., революционным событиям и мобилизации. Пример одного из таких писем и документов отображен на рис. 7-9.

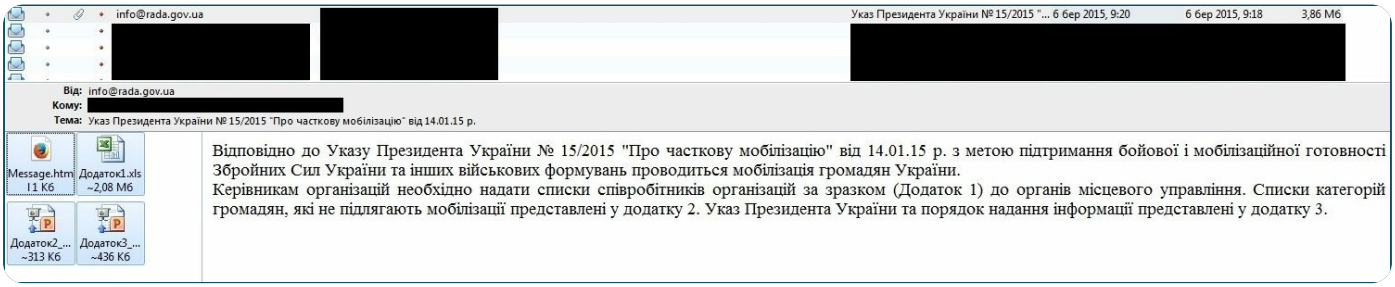

info@rada.gov.ua
Указ Президента України № 15/2015 "... 6 бер 2015, 9:20
6 бер 2015, 9:18
3,86 Мб
Від: info@rada.gov.ua
Кому:
Тема: Указ Президента України № 15/2015 "Про часткову мобілізацію" від 14.01.15 р.
Message.htm
11 Кб
Додаток1.xls
~2,08 Мб
Додаток2_...
~313 Кб
Додаток3_...
~436 Кб
Відповідно до Указу Президента України № 15/2015 "Про часткову мобілізацію" від 14.01.15 р. з метою підтримання бойової і мобілізаційної готовності Збройних Сил України та інших військових формувань проводиться мобілізація громадян України.
Керівникам організацій необхідно надати списки співробітників організацій за зразком (Додаток 1) до органів місцевого управління. Списки категорій громадян, які не підлягають мобілізації представлені у додатку 2. Указ Президента України та порядок надання інформації представлені у додатку 3.

Рис. 7

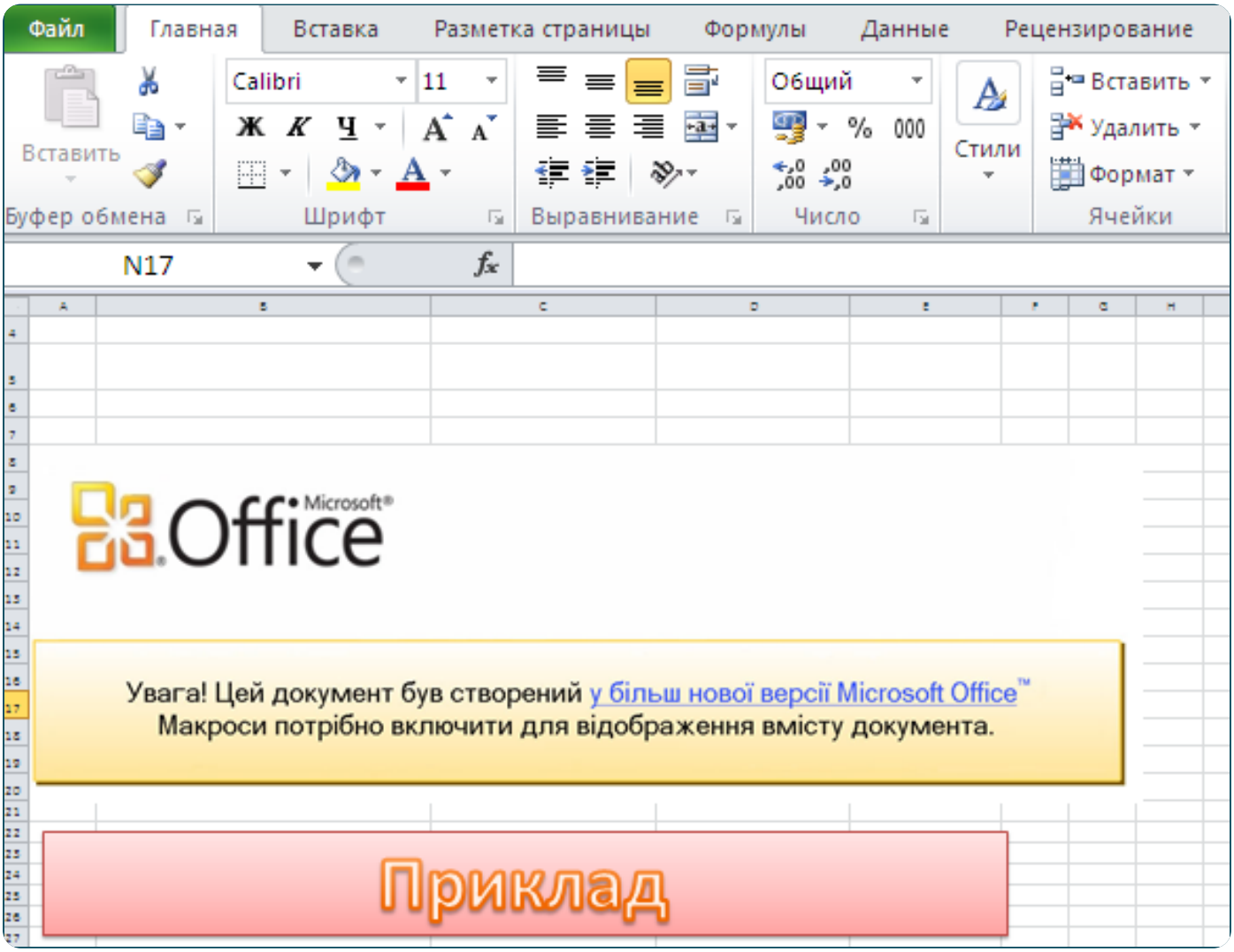

Файл
Главная
Вставка
Разметка страницы
Формулы
Данные
Рецензирование
Calibri
11
Общий
Вставить
Удалить
Формат
Стили
Буфер обмена
Шрифт
Выравнивание
Число
Ячейки
N17
Office
Microsoft
Увага! Цей документ був створений у більш нової версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документа.
Приклад

Рис. 8

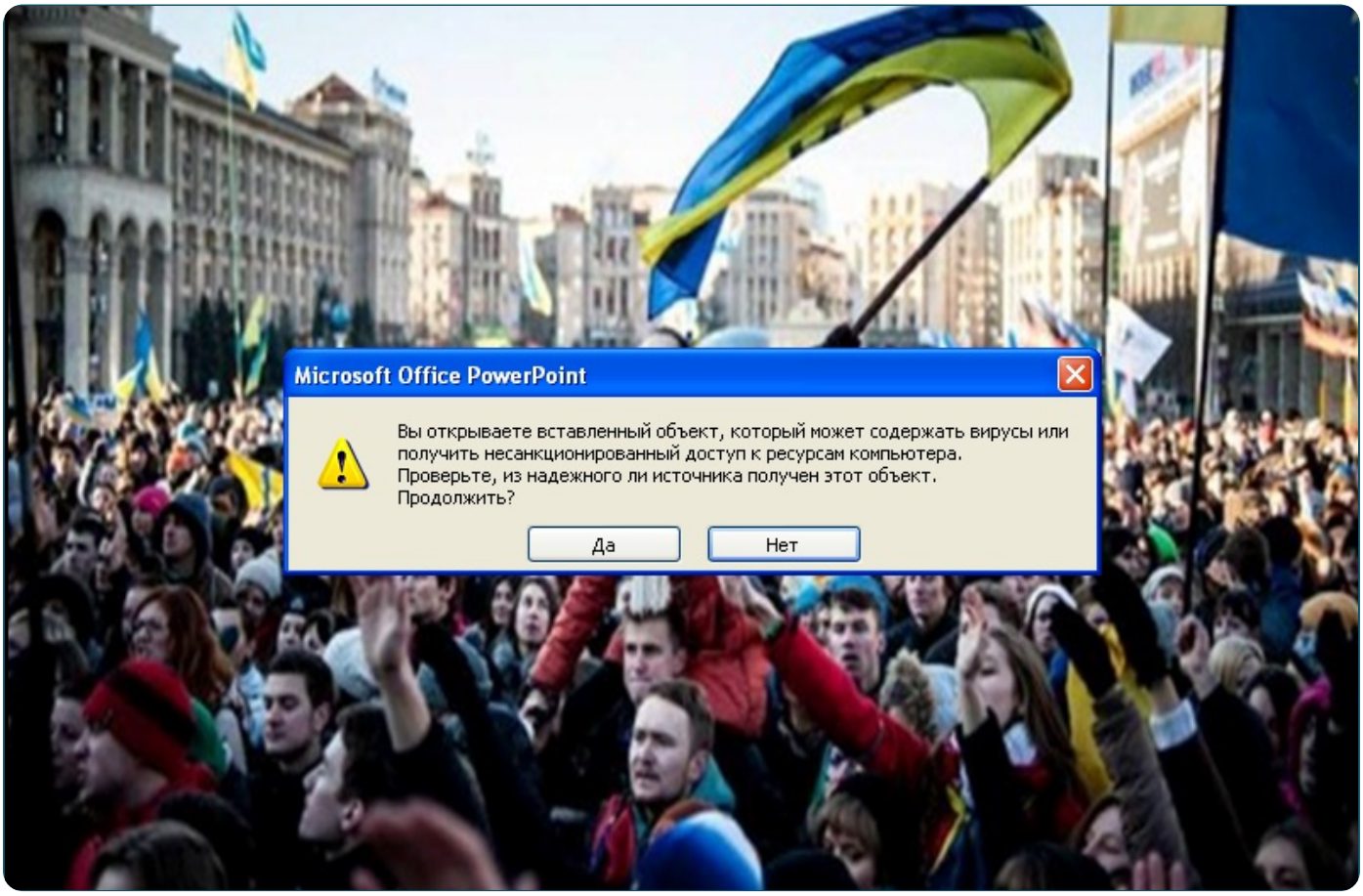


Рис. 9

Помимо индикаторов, которые характеризуют инфраструктуру бот-сети (о них написано в конце статьи), доступны также данные из заголовков электронного письма, которым атаковали радиовещательные компании:

```
Received: from Unknown (mx01.24x7h.com [213.152.168.4])
 by mx01.24x7h.com (Postfix) with SMTP id 2445F6D7BEB;
 Wed, 13 Aug 2014 07:40:38 +0200 (CEST)
Received: from svoboda.org.ua (port=80 helo=svoboda.org.ua)
 by svoboda.org.ua [193.136.66.3] with esmtp (envelope-from )
```

Очень интересно, что в этих заголовках также фигурирует "португальский" IP-адрес 193.136.66.3. Что бы не приходило на ум глядя на эти заголовки, данные Passive DNS свидетельствуют о том, что домены svoboda.org.ua и vosvoboda.info в обозримом прошлом не ассоциировались с указанным IP-адресом.

Уже в конце марта 2015 года были зафиксированы две вредоносные рассылки (с одинаковым вредоносным файлом, рис. 10).

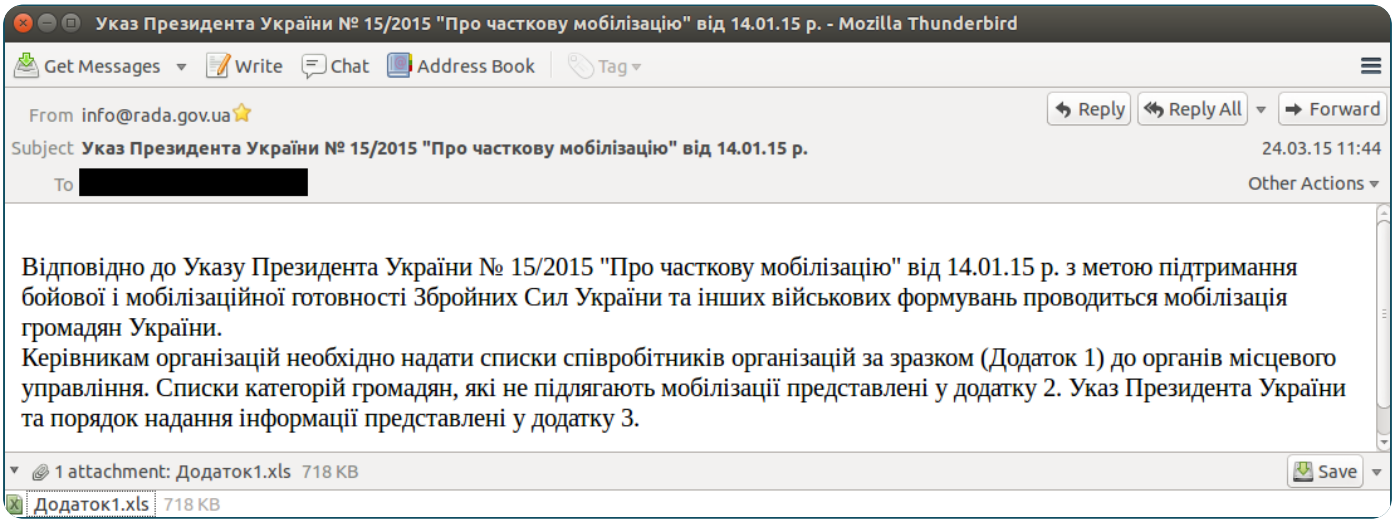


Рис. 10

Одна рассылка – в адрес государственного учреждения Украины, занимающегося архивно-библиотечной деятельностью (объект атаки очень похож на те, что были атакованы в августе 2014 года с применением 0day эксплойта). Вторым объектом атаки стало одно из облэнерго, находящееся в западной части Украины. Характер и масштабы поражений, а также образцы выявленных вредоносных программ, позволили с уверенность сказать, что данная кибер-атака была реализована с применением вредоносной программы BlackEnergy2/3.

> *Электронные письма конца марта 2015 года содержали несколько иные сетевые идентификаторы в заголовках. Для полноты картины приводим соответствующую строчку из письма про мобилизацию с одним вредоносным вложением "Додаток1.xls"*
>
> ```
> Received: from mx1-mail.com (mx1-mail.com [5.149.248.67])
> ```

Вместе с тем, следует отметить и такой немаловажный факт. В результате совместных мероприятий, проведенных с ответственным сотрудником атакованного облэнерго, было установлено, что параллельным вектором атаки на ИТ-инфраструктуру предприятия был непосредственный взлом компьютерной сети, а именно – веб-сервера, имеющего как доступ в Интернет, так и доступ к определенному сегменту внутренней сети организации. Он (веб-сервер) как раз и был «мостиком», с помощью которого атакующие проникали извне в корпоративную сеть. На этом этапе, в результате проведения компьютерно-технических исследований, также был выявлен некоторый инструментарий, применяемый злоумышленниками в процессе осуществления атаки, а именно:

reDuh – для туннелирования TCP через HTTP-запросы, бэкдор; позволяет получать доступ ко внутренним объектам сети извне [10].
weevely3 – веб-шелл для командной строки, бэкдор; позволяет получать доступ ко внутренним объектам сети извне [11].
dropbear – специальная версия SSH-сервера; открывает сокет и позволяет подключаться удаленно с использованием «вшитого» пароля или ключа, бэкдор [12].

DSEFix – для загрузки неподписанных драйверов в обход существующих механизмов защиты ОС [12].

Благодаря еще одному ответственному Сотруднику обсуждаемого облэнерго в этой области население было спасено от отключения электричества и связанных с этим отрицательных последствий. Скажем все спасибо Герою.

Следующая по списку атака была приурочена очередным украинским выборам – 25 октября 2015 года. Точнее говоря – это был апогей атаки. По имеющимся данным мы с большой долей вероятности можем сказать, что на компьютерах и серверах ряда телевизионных каналов Украины вредоносное программное обеспечение BlackEnergy2/3 было уже в конце мая 2015 года. К сожалению, на данный момент мы не располагаем соответствующим таргетированным письмом, направленным на телевизионные СМИ Украины, поэтому не можем подсказать атакованным объектам, к поиску какого вредоносного письма им обратиться. Может даже быть так, что телевизионные СМИ «зацепила» рассылка от конца марта 2015 года с применением писем такой же тематики. Учитывая данные, изложенные в статье [14], а также новость [15] и исследование компании ESET [1], можем предположить, что атаке злоумышленников в канун украинских выборов 25.10.2015 могли быть подвержены:

- ТРК Україна (11131526trk)
- СТБ (2015stb)

Как правило, в результате атаки злоумышленники уничтожали видеоматериалы, серверное оборудование и, в конечном счете, с помощью «программ-разрушителей» выводили из строя функционально значимые компьютеры (например, рабочие места операторов).

Ставя жирную точку в атаках на информационные системы Украины в 2015 году, 23 декабря 2015 года впервые в истории Украины в результате предшествующей компьютерной атаки были выведены из строя автоматизированные системы управления технологическими процессам – электрическими подстанциями, что привело к обесточивания на 3-8 часов десятков тысяч украинских граждан. Официально о произошедшем сообщили аж два предприятия – Киевоблэнерго [16] и Прикарпатьеоблэнерго [7]. Другие предприятия энергетической отрасли, среди которых могут быть соответствующие компании в Черновцах, Львове, Житомире, Харькове и других городах Украины, никаких заявлений не делали. Как и при проведении других атак, помимо самой вредоносной программы BlackEnergy2/3, в данном случае также злоумышленники применили «программу-разрушитель» для сокрытия следов противоправной деятельности путем уничтожения информации на средствах вычислительной техники. Данная программа отличалась от той, которую применяли против телевизионных СМИ, так как имела, среди прочего, функционал «таймера» и завершала работу двух конкретных процессов «sec_service.exe» и «komut.exe». До сих пор исследователи путаются в догадках того, были ли подстанции отключены автоматически специальной программой или это было сделано удаленно. Вместе с тем, факт наличия доступа к тому сегменту сети (компьютеру), с которого возможен доступ к интерфейсу управления SCADA-системами, будь-то посредством RDP/VNC/SSH и т.п., сам по себе является устрашающим.

Хотелось бы отметить, что есть основания полагать, что атаке также были подвержены:

- Аэропорт «Борисполь» (11131526kbp)
- «Международные авиалинии Украины» (обнаружен драйвер BlackEnergy2)

Некоторые из идентификаторов «билдов» вредоносных программ, указанных в статье ESET, могут быть трактованы следующим образом:

2015en – компании энергетической сферы
2015ts – компании транспортной сферы
khm10 – областная энергетическая компания
khelm – областная энергетическая компания
brd2015 – Бердянська міська рада
kiev_o – Киевоблэнерго

Небольшой перечень сетевых индикаторов компрометации приведен ниже. Рекомендуем, в первую очередь всем упомянутым в статье объектам атаки, а во-вторую – всем остальным, не пренебречь возможностью и проверить лог-файлы и информационные потоки на предмет наличия/отсутствия в них свидетельств сетевого взаимодействия с использованием указанных индикаторов:

hxxps://5.9.32.230/Microsoft/Update/KS1945777.php
hxxps://31.210.111.154/Microsoft/Update/KS081274.php
hxxps://88.198.25.92/fHKfvEhleQ/maincraft/derstatus.php
hxxps://146.0.74.7/l7vogLG/BVZ99/rt170v/solocVl/eegL7p.php
hxxps://188.40.8.72/l7vogLG/BVZ99/rt170v/solocVl/eegL7p.php
hxxps://5.149.254.114/Microsoft/Update/KC074913.php
hxxps://148.251.82.21/Microsoft/Update/KS4567890.php
hxxp://41.77.136.250/Microsoft/Update/KS081274.php

Будет не лишним проверить наличие определенных файлов, содержащих в зашифрованном виде плагины BlackEnergy2:

%WINDIR%\system32\ieapflrt.dat

Больше индикаторов вы можете почерпнуть тут [17] и тут [18].

Заключение.
По большому счету не важно, кто стоит за этими атаками, поэтому мы не прибегаем к их атрибуции кому-либо. Противостояния в мире не избежать никак и, уж тем более, всех причинно-следственных связей не установить. Более того, продемонстрированные в последние полтора года методы констатации фактов, «висловлення занепокоєнь», «різких засуджень», «обурень», «публичных порицаний», атрибуций, обличений и т.п. – вряд ли помогли бы предотвратить отключение электричества или срабатывание 0day эксплойта. Гораздо важнее вынести из всего этого уроки, как атакованным объектам, которым следовало больше переживать о благосостоянии граждан, нежели о репутации, так и правительству с их «долгостроями» в виде профильных законов, перечнями критических объектов и т.п. Пора бы начать обмениваться информацией, прислушиваться к рекомендациям (которые были и в этот раз, задолго до 23 декабря!) и начать, хотя бы, учиться на своих ошибках, покончив с ролью «опытного полигона» для всего остального мира.

Отдел исследования киберугроз CyS Centrum

Использованные материалы:

[1] http://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/
[2] http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/
[3] http://habrahabr.ru/company/eset/blog/274469/
[4] http://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/
[5] http://www.theregister.co.uk/2016/01/04/blackenergy_drains_files_from_ukraine_media_energy_organisatio
[6] http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104
[7] http://www.oe.if.ua/showarticle.php?id=3413
[8] http://www.isightpartners.com/2014/10/cve-2014-4114/
[9] http://habrahabr.ru/company/eset/blog/240345/
[10] https://github.com/sensepost/reDuh
[11] https://github.com/epinna/weevely3
[12] https://matt.ucc.asn.au/dropbear/dropbear.html
[13] https://github.com/hfiref0x/DSEFix
[14] http://lb.ua/news/2016/01/05/325082_eset_hakeri_zarazili_ukrainskie.html
[15] https://golospravdy.com/xakery-vzlomali-vse-sajty-mediagruppy-inter/
[16] http://www.koe.vsei.ua/koe/index.php?page=50&novost=208
[17] https://securelist.com/blog/research/67353/be2-custom-plugins-router-abuse-and-target-profiles/
[18] https://www.youtube.com/watch?v=I77CGqQvPE4

06.01.2016

CyS Centrum LLC
ООО "САЙБЕР СЕКЬЮРИТИ ЦЕНТРУМ"
www.cys-centrum.com

ул. Никольско-Слободская, 2-Б, подъезд 5(1), этаж 15, офис 177, Киев, Украина
02002

Тел: +38 044 338 53 30
rep@cys-centrum.com