Operation Buhtrap, the trap for Russian accountants

By Jean-Ian Boutin

Archived: 2026-04-05 13:29:25 UTC

Late in 2014, we noticed and started to track an undocumented malicious campaign targeting Russian businesses, and that has been active for well over a year. The malware used in this campaign is a mix of off-the-shelf tools, NSIS-packed malware and bespoke spyware that abuses Yandex's Punto software, a program for Russian users which silently and automatically changes the keyboard language depending on what the user is typing. Once the cybercriminals have compromised a computer, they use custom tools to analyze its content, install a backdoor and finally deploy a malicious module that spies on the system and can enumerate smart cards.

The campaign targets a wide range of Russian banks, uses several different code signing certificates and implements evasive methods to avoid detection. As explained later, we believe this campaign is financially-motivated and that it targets accounting departments in Russian businesses. Operation Buhtrap is a mix of two words: "Buhgalter" and "trap". "Buhgalter" means "accountant" in Russian.

This campaign is of particular interest as the techniques used by these cybercriminals are often associated with targeted attacks and not generally used by financially-motivated cybercriminals. Although we believe it to be a different campaign, it shares some similarities with Anunak/Carbanak in terms of techniques, tactics and procedures it uses. In this blog post, we will cover this campaign, its targets, and the tools used by these criminals.

Targets

The cybercriminals behind this campaign are installing their software only on computers that have Russia as their default Windows locale. The infection vector we have seen consists of Microsoft Word documents sent as email attachments that exploit CVE-2012-0158, a vulnerability in Microsoft Word that was patched three years ago. The images below show two of the decoy documents used in this campaign. The first document, titled "Счет № 522375-ФЛЮРЛ-14-115.doc" mimics an invoice. The second, aptly titled "kontrakt87.doc", copies a generic telecommunications service contract from MegaFon, a large Russian mobile phone operator.

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:

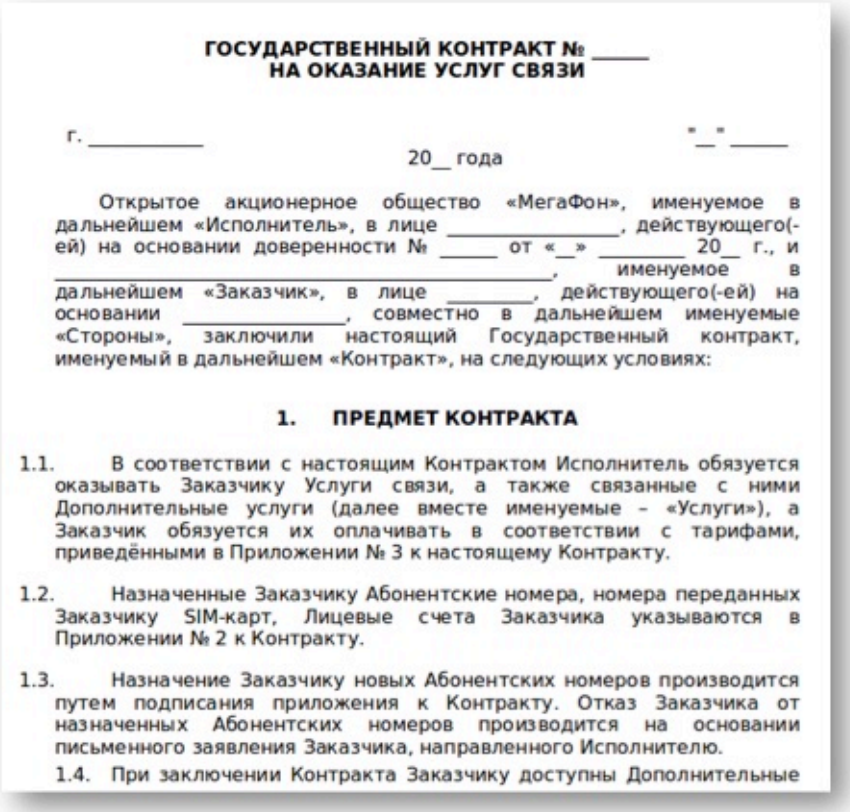
Получатель: ИНН/КПП:	ООО НПП "Стройинжиниринг" 8904043570/890401001	Р/сч	40702810600000001323
Банк получателя:	ф-л ПТБ (ОАО) в г.Новый Уренгой,Тюменская обл. г.Новый Уренгой	БИК К/сч	047195753 30101810700000000753

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



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.

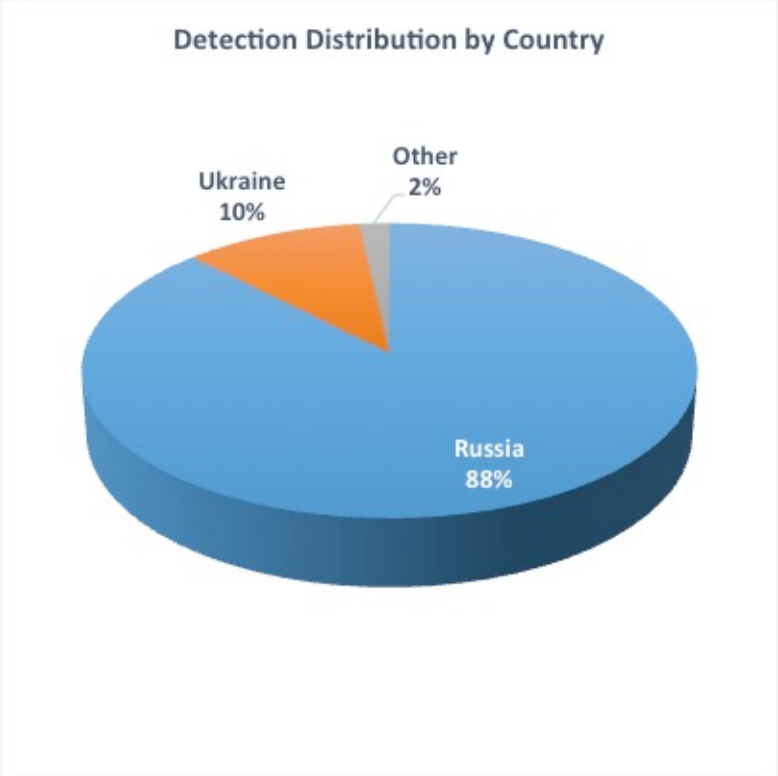
1.4. При заключении Контракта Заказчику доступны Дополнительные

The content of the decoy documents we've examined, the tactics and tools used, the references to business applications contained in some modules, as well as some of the malicious domain names that were used in this campaign, all lead us to believe that Russian businesses are their primary target.

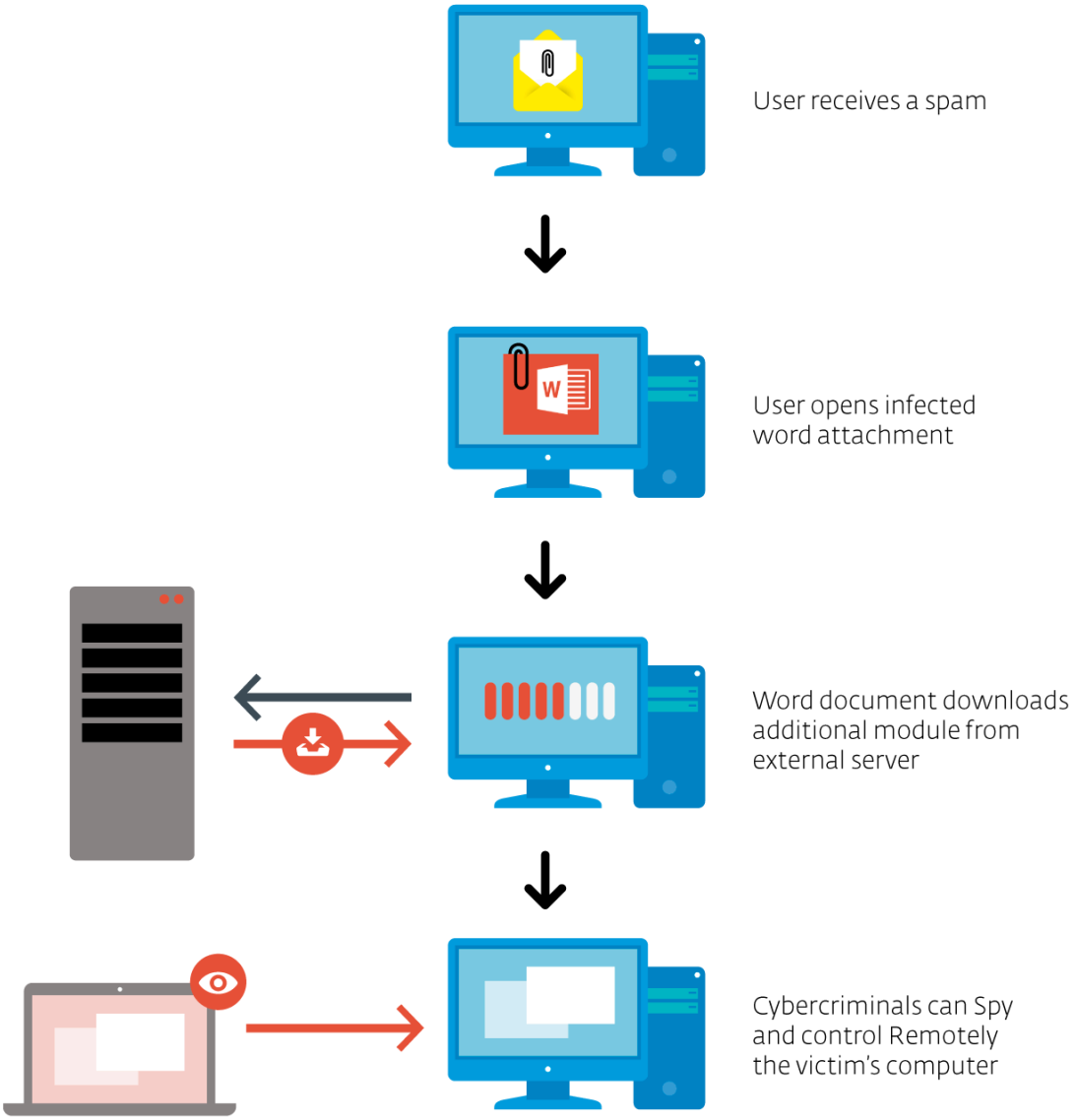
If we take it into consideration that some of the Command and Control (C&C) domain names are very similar to some accounting forums or specialized websites, and that the malware contains references to software tools and banking applications commonly used in accounting departments, we can infer that workers belonging to this department are the most likely primary targets.

The tools deployed on the victim's computer allow them to control it remotely and to record the user's actions. The malware allows the criminals to install a backdoor, attempt to obtain the account password, and even create a new account. They also install a keylogger, a clipboard stealer, a smart card module, and have the capability to download and execute additional malware.

Our telemetry for the malware families linked to this campaign is shown below. Most detections we have for these threats are located in Russia. Our telemetry also shows that the tools used by this campaign are not widespread. This reinforces our assumption that these attackers are likely focusing primarily on businesses.



Installation Overview



If the user opens the malicious attachments on a vulnerable system, an NSIS-packed trojan downloader will be dropped and executed. It will make several checks on the machine, first looking for malware researcher tools or evidence that the malware is run in a virtual machine, exiting if it finds any. It will also check whether the Windows locale is Russian (1049) and uses “FindFirst/NextUrlCacheEntry” and registry key “Software\Microsoft\Internet Explorer\TypedURLs” to know whether URLs matching the following patterns were visited on the computer:

***ICPortalSSL**	***ibank**	***i-elba**
*sib.taatta.net	*ibrs	*clbank.minbank.ru
*isfront.priovtb.com	*iclient	*chelindbank.ru/online/

***ICPortalSSL**	***ibank**	***i-elba**
*ISAPIgate.dll	*e-plat.mdmbank.com	*uwagb
*bsi.dll	*sberweb.zubsb.ru	*wwwbank
*PortalSSL	*ibc	*dbo
*IIS-Gate.dll	*elbrus	*ib
*beta.mcb.ru		

It will also check to see if any of the applications below is running on the machine:

ip-client.exe	**pkimonitor.exe**	**BC_Loader.exe**	**CbShell.exe**	**Bankline.EXE**
prclient.exe	pmodule.exe	Client2008.exe	clb.exe	GeminiClientStation.exe
rclient.exe	pn.exe	IbcRemote31.exe	CliBank.exe	_ClientBank.exe
saclient.exe	postmove.exe	_ftcgpk.exe	CliBankOnlineEn.exe	ISClient.exe
SRCLBClient.exe	productprototype.exe	scardsvr.exe	CliBankOnlineRu.exe	cws.exe
twawebclient.exe	quickpay.exe	CL_1070002.exe	CliBankOnlineUa.exe	CLBANK.EXE
vegaClient.exe	rclaunch.exe	intpro.exe	client2.exe	IMBLink32.exe
dsstart.exe	retail.exe	UpMaster.exe	client6.exe	cbsmain.dll
dtpaydesk.exe	retail32.exe	SGBClient.exe	clientbk.exe	GpbClientSftcws.exe
eelclnt.exe	translink.exe	el_cli.exe	clntstr.exe	Run.exe
elbank.exe	unistream.exe	MWClient32.exe	clntw32.exe	SGBClient.exe
etprops.exe	uralprom.exe	Adirect.exe	contactng.exe	sx_Doc_ni.exe
eTSrv.exe	w32mkde.exe	Bclient.exe	Core.exe	icb_c.exe
ibconsole.exe	wclnt.exe	bc.exe	cshell.exe	Client32.exe
kb_cli.exe	wfinist.exe	ant.exe	cyberterm.exe	BankCl.exe
KLBS.exe	winpost.exe	arm.exe	client.exe	ICLTransportSystem.exe
KlientBnk.exe	wupostagent.exe	arm_mt.exe	cncclient.exe	GPBClient.exe
lfcpaymentais.exe	Zvit1DF.exe	ARMSH95.EXE	bbclient.exe	CLMAIN.exe
loadmain.exe	budget.exe	asbank_lite.exe	EximClient.exe	ONCBCLI.exe
lpbos.exe	CB.exe	bank.exe	fcclient.exe	CLBank3.exe

ip-client.exe	pkimonitor.exe	BC_Loader.exe	CbShell.exe	Bankline.EXE
mebiusbankxp.exe	cb193w.exe	bank32.exe	iscc.exe	rmclient.exe
mmbank.exe	cbank.exe	bbms.exe	kabinet.exe	FcolseOW.exe
pcbank.exe	cbmain.ex	bk.exe	SrCLBStart.exe	RkcLoader.exe
pinpayr.exe	CBSMAIN.exe	BK_KW32.EXE	srcbclient.exe	uarm.exe
Pionner.exe		bnk.exe	Upp_4.exe	nlnotes.exe

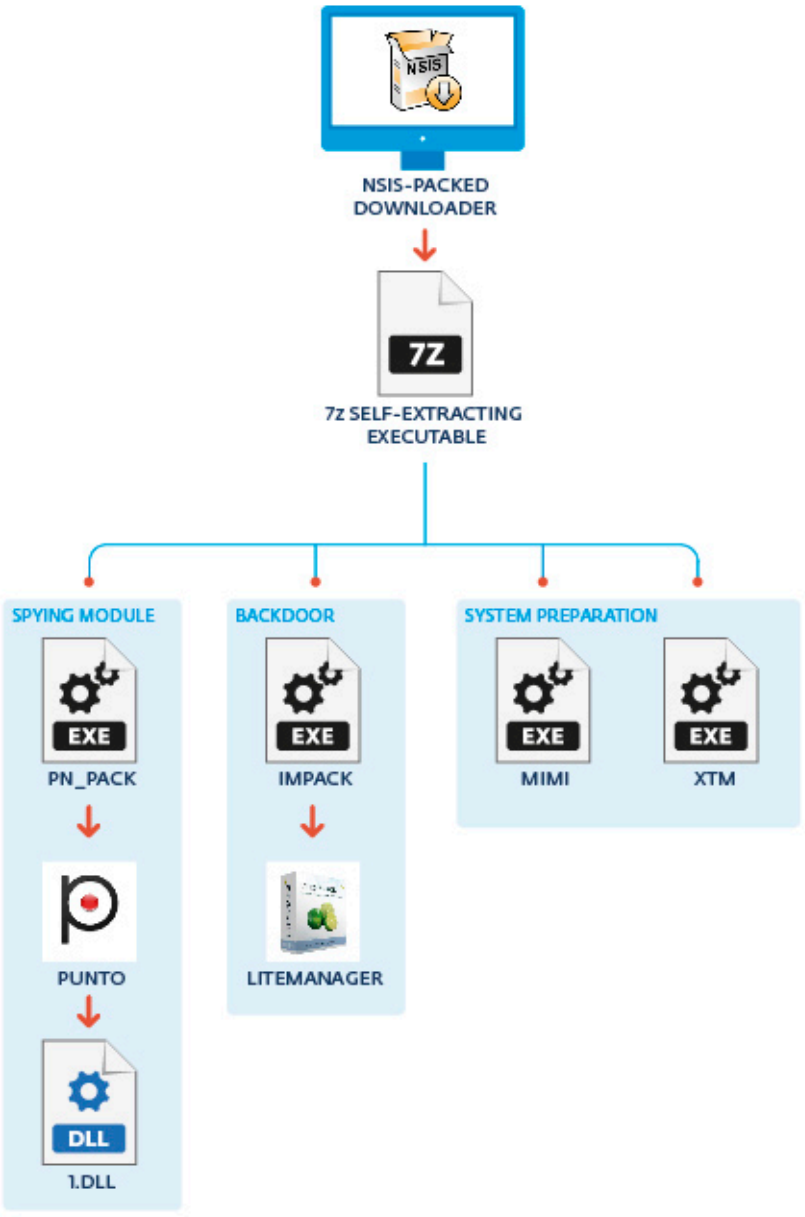
The list of processes is quite exhaustive and does not contain only banking applications. It includes, for example, “scardsvr.exe” which is Microsoft’s SmartCard reader. This makes sense knowing that this malware has smartcard reader capabilities. On the other hand, some processes are hard to identify and might be there for opportunistic reasons.

If all the requirements are met, the final stage is to download an additional file that contains all the modules used by the cybercriminal to spy on the victim.

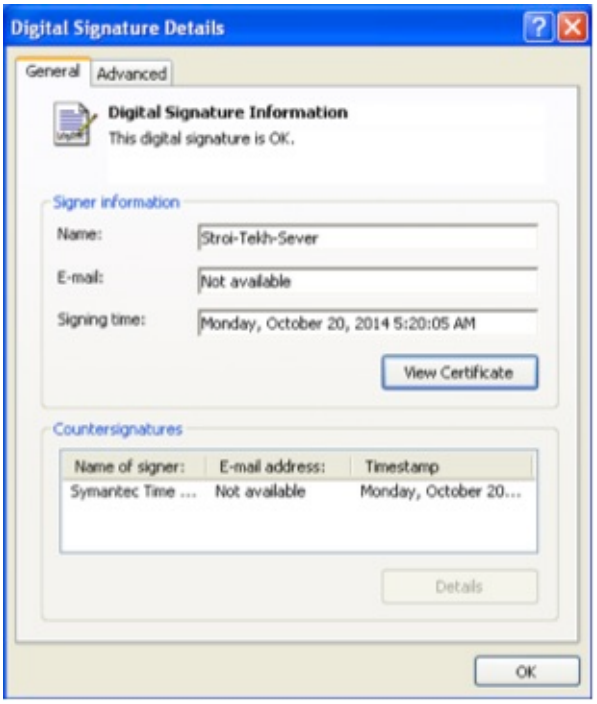
Interestingly, the downloaded archive may differ depending on the results of the checks above. In one of the earlier version of the NSIS-packed downloader we analyzed, there exist two different archives that can be downloaded from the C&C: one malicious and one benign.

One of the benign archives we downloaded ultimately installed the Windows Live Toolbar. Although the means to install the software was malicious, the final payload wasn't. These tactics were probably put in place to fool automatic processing systems: since a payload was downloaded, the system could be fooled into thinking that this is the end of the story.

The archive downloaded by the NSIS-packed dropper is a 7z self-extracting executable and contains different modules, all distributed as 7z password-protected archives. This downloaded archive contains the different modules used by this campaign. The picture below better describes the overall installation process and shows the different modules.



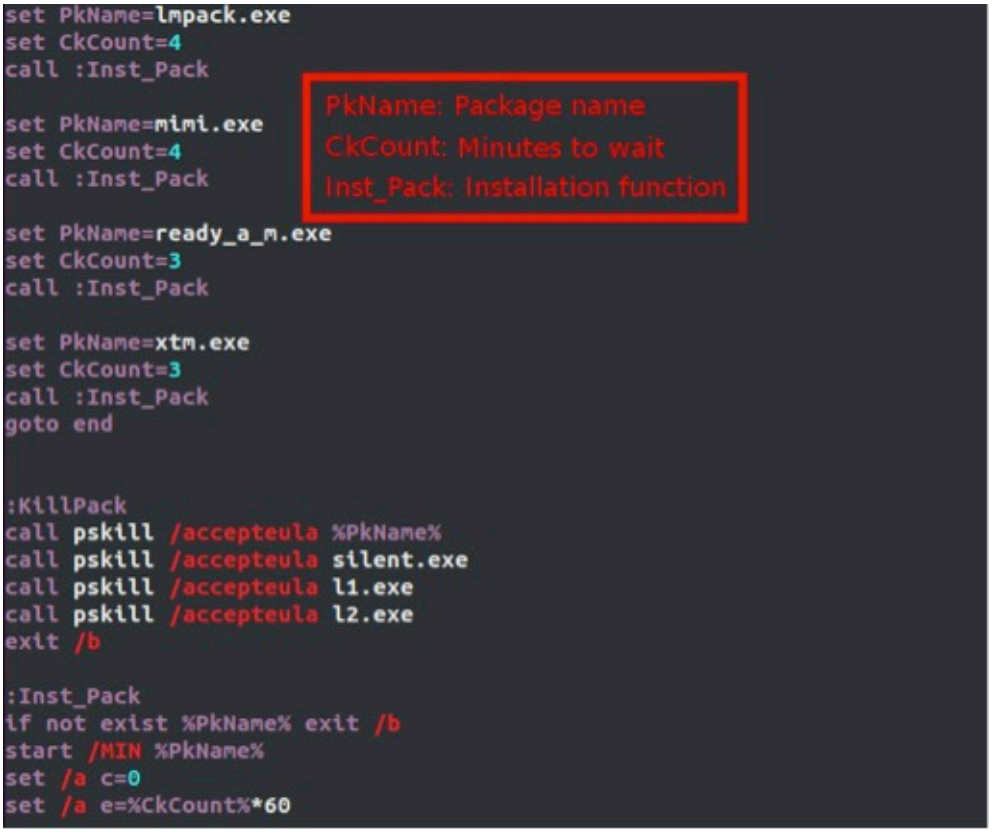
While the different modules have very different purposes, they are all similarly packaged and a lot of them are signed with a valid code-signing certificate. We found four different certificates used since the campaign started, all registered to companies in Moscow. We of course notified the certificate issuer to have them revoked.



The table below lists the different certificates that were found linked to this campaign. We believe they were all fraudulently obtained.

Company name	Validity	Serial and Thumbprint
Stroi-Tekh-Sever	09/25/2014 to 09/26/2015	Serial: 07 ac 7c a0 d1 69 d7 d3 86 ee 08 01 19 95 99 f2 Thumbprint: cf5a43d14c6ad0c7fdbcbe632ab7c789e39443ee
Flash	12/18/2014 to 12/19/2015	Serial: 57 a8 f7 1c 7e 2b 97 8c 71 60 ba 07 5e ca b4 6c Thumbprint: e9af1f9af597a9330c52a7686bf70b0094ad7616
OOO "Techcom"	12/22/2014 to 12/23/2015	Serial: 00 e9 fb cb 1b c3 8b 66 8d 9e ba a4 73 11 76 01 41 Thumbprint: 3e1a6e52a1756017dd8f03ff85ec353273b20c66
Torg-Group	10/30/2014 to 10/31/2015	Serial: 13 01 47 51 84 46 19 e6 b5 7f de ca 34 e6 04 aa Thumbprint: efad94fc87b2b3a652f1a98901204ea8fbeef474

All the modules that make up this threat share a common install procedure. They are all 7z self-extracting executables that first decompress a password-protected archive and then execute an **install.cmd** file. The following is the first install.cmd file that gets invoked after the first module has been downloaded and executed:



The install.cmd file will then install the malware or run the various tools, but will first learn more about the machine it is about to compromise, especially about the account privileges it currently has and which version of Windows is installed.
If administrator privileges are required and malware is run on a limited account, it uses two different techniques to attempt privilege escalation.

The first approach uses two files, l1.exe and cc1.exe, which implement a variant of the trick used in the leaked Carberp source code. It copies cryptbase.dll to %USERPROFILE%, patches it so that it launches the malware on execution and packs it as a MSU file. Finally, it uses wusa.exe to copy it to the system directory before launching it. The other technique exploits CVE-2013-3660. Each module that requires privilege escalation has a 32- and 64-bit version of this exploit. If gaining administrator privileges is required, the install.cmd file will try to use either of these techniques to escalate privileges locally in order to install the different modules.

While tracking this campaign, we downloaded different overall packages. Interestingly, the modules they contained were not the same. This leads us to believe that different targets might receive different modules.

System Preparation – mimi.exe and xtm.exe

This module will try to:

- Recover account passwords
- Enable remote desktop service
- Create a new account on the compromised computer

mimi.exe includes a modified version of Mimikatz, a well-known open source tool allowing password recovery for users logged in a Windows system. Both the 32- and 64-bit versions of the tools are included in the executable

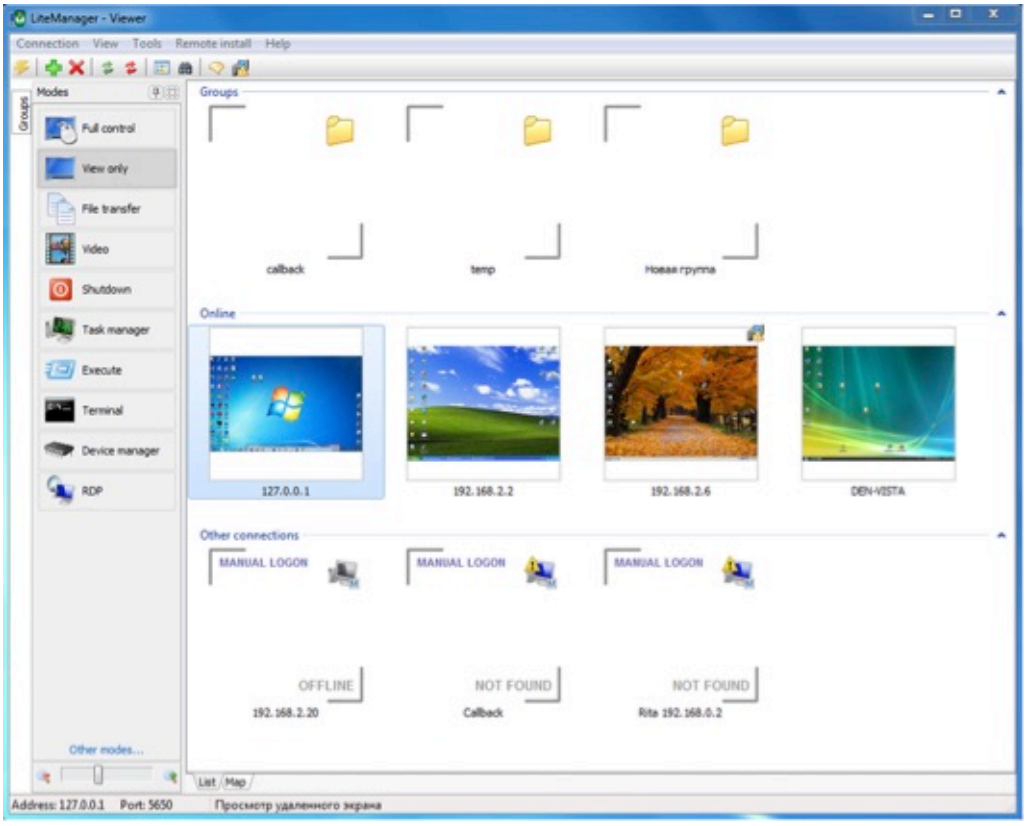
resources. While the account password recovery functionality is still there, the executable was modified to remove the user interaction part of the tool. The executable is also modified so that when run, it will invoke in succession the "privilege::debug" and "sekurlsa:logonPasswords" commands, effectively compromising the current local account password.

xtm.exe has different behavior to reach its goals depending on which Windows version it is run. In WinXP, it has scripts that will enable remote desktop services and try to create a new account. These steps are required to give the malware authors full control over the compromised system. **xtm.exe** will also change system settings, to allow multiple users to be logged on to the computer at the same time. The screenshot below shows an example of the type of commands run on a WinXP machine.

```
""sc.exe" failure dcomlaunch reset= 60 actions= """
""taskkill.exe" /f /fi "modules eq termsrv.dll""
""sc.exe" config TermService start= auto"
""net.exe" start TermService /y"
""sc.exe" config DcomLauch start= auto"
""sc.exe" config fastuserswitchingcompatibility start= auto"
""net.exe" start fastuserswitchingcompatibility /y"
""gpupdate.exe" /force"
""net.exe" user Hide 123qwe!@# /add"
```

Backdoor – lmpack.exe

This module's sole purpose is to install a backdoor onto the system. It will try to install LiteManager, a third-party tool that allows remote control of a system.



Once this software is installed, it allows the cybercriminals to connect directly to the victim's computer and control it remotely. This software even has a command line option to install the application silently, to create firewall rules, and finally to start LiteManager silently. Of course all these options are abused by the cybercriminals.

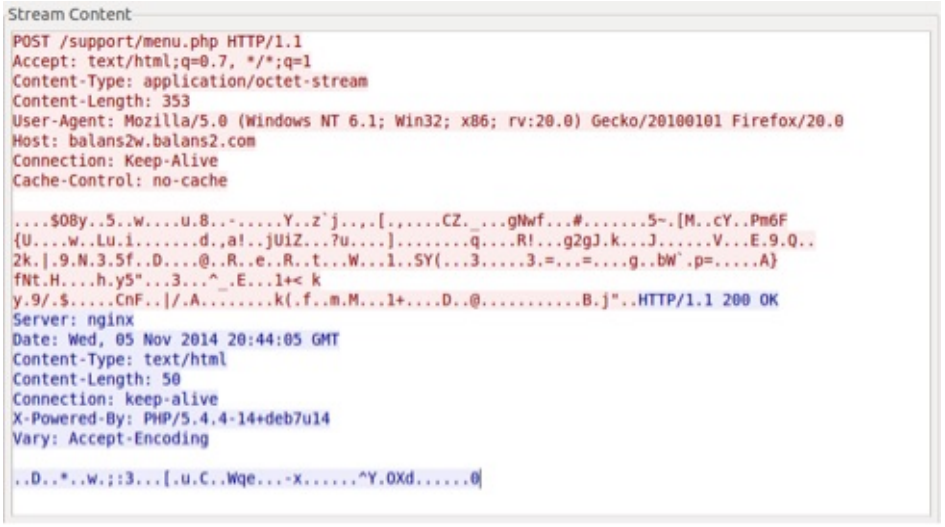
Spying module – pn_pack.exe

This module is responsible for spying on the user and communicating with the C&C. It will first install Punto, software made by Yandex that can automatically change keyboard language as the user types. The cybercriminals are then misusing this software to run the spying module through DLL side loading and are using it to

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

The module that is ultimately responsible for these tasks is an encrypted DLL that is decrypted and loaded into memory at runtime by the Punto process. It launches three threads that will ultimately perform the work outlined above. The fact that Punto is misused by this malware for keylogging purposes is not surprising: several Russian forums detail explicitly how to misuse this application for this purpose.

This module uses RC4 to encrypt its strings as well as its network communication. It will reach out to the C&C every two minutes, transmitting any data that have been stolen from the compromised system. A screenshot of a network communication as well as the different commands that can be received from the server are shown below.



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.

As the server commands are sent as a response to a status update from the user, it is not unimaginable that special code will be sent for specific events, such as when a smart card is detected on the system.

Interestingly, in all the banker modules we analyzed (the latest one having a compilation time of January 18th), there is a string “TEST_BOTNET” that is sent in every communication with the C&C. At this point, it is unclear what this means as people and organizations have already been compromised by this malware. As we believe this operation has been ongoing for more than a year, this is intriguing. Perhaps the future holds the answer.

Conclusion

We can imagine the fraudsters operating in this way: they first compromise a single computer in a business by sending a spam and luring the person into opening the attachment.

Once the malware is installed on the victim's computer, the cybercriminals have access to several tools that will help them to first compromise other computers in the company and second, spy on the user and see whether some fraudulent banking transactions can be performed.

While the tools and software used in this campaign are far from being novel, the overall campaign is quite interesting and intriguing: it diverges quite a bit from the traditional banking malware with which we are familiar.

This campaign is using specific tools to reach its goal, akin to what we are accustomed to see in targeted attacks. Seeing a campaign like this, inevitably the Anunak/Carbanak documented by Fox-IT and Kaspersky comes to mind. Although we believe that this campaign is different, some similarities were observed. The infection vector is similar, it uses a similar modified mimikatz application, and it uses a third-party remote access tool, changes system settings to allow concurrent RDP sessions, and so on.

It will be interesting to see whether this kind of operation will become the norm and if the popularity of traditional banking trojan families will diminish in return.

Special thanks to Anton Cherepanov and Joan Calvet for their help in this analysis

Hashes

Indicators of Compromise

Indicator	Value
C&C Domains	store.kontur-expres.com balans2w.balans2.com forum.buhonline.info rss.mercurynews.biz topic.buhgalter-info.com help.b-kontur.org
C&C Hardcoded IP	91.218.231.79
7z self-extracting executable URLs	hXXp://playback.savefrom.biz/video/video1.cab hXXp://playback.savefrom.biz/video/video_1.cab hXXp://download.sendspace.biz/file/install.cab hXXp://download.sendspace.biz/file/l.cab

Indicator	Value
	hXXp://library.source-forge.info/cab/cabinstal.cab hXXp://library.source-forge.info/cab/cabinstal3.cab hXXp://new.pikabu-story.com/file/file1.cab hXXp://getdownloadsfile.com/file/new1.cab hXXp://new.pikabu-story.com/file/mega.cab
Decoy document name	Счет № 522375-ФЛЮРЛ-14-115.doc kontrakt87.doc

---

Source: https://www.welivesecurity.com/2015/04/09/operation-buhtrap/