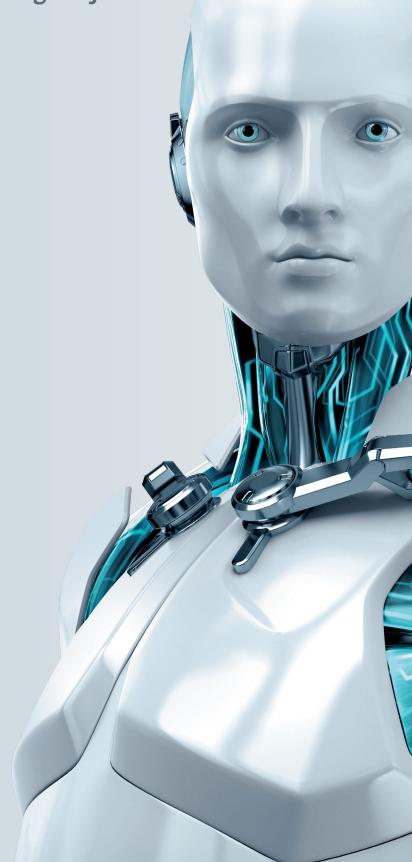
A Guide to the RTM Banking Trojan

Matthieu Faou & Jean-Ian Boutin

February 2017





A Guide to the RTM Banking Trojan

Matthieu Faou & Jean-Ian Boutin

February 2017



TABLE OF CONTENT

1. Targets	5
2. Infection vectors	8
2.1. Is the malware related to Buhtrap?	9
3. Evolution	10
3.1. Versioning	10
3.2. Timeline	11
4. Technical analysis	11
4.1. Installation and persistence	12
4.3. Network	14
4.4. Fingerprint	17
4.5 Monitoring	19
4.6. Uninstall	20
4.7. Config	21
4.8. Other functions	21
5. Conclusion	24
6. Indicators of Compromise	25
6.1. ESET detection names	25
6.2. File names	25
6.3. Registry indicators	25
6.4. Hashes	25
6.5. C&C server domain names	27
6.6. C&C server IP addresses	27
6.7. PDB paths	27
6.8. Strings	28
7. Bibliography	30

LIST OF TABLES

Table 1	Code-signing certificates used by RTM	10
Table 2	List of botnet prefixes	10
Table 3	Possible values of the action field	16
Table 4	Targeted software	18
Table 5	Targeted URLs	18
Table 6	Identifier for a banking related machine	19
Table 7	Banking windows targeted	19
Table 8	Configuration keys	21
LISTO	FIGURES	
LIST OF	FIGURES	
Figure 1	RTM telemetry	5
Figure 2	Decoy document used in recent RTM campaigns	6
Figure 3	"1C: Enterprise 8" software export window	7
Figure 4	1c_to_kl.txt example	7
Figure 5	Infection vectors timeline	8
igure 6	Code-signing certificate used by both RTM and Buhtrap	9
Figure 7	Timeline of the RTM malware	11
Figure 8	DLL name for sample F4C746696B0F5BB565D445EC49DD912993DE6361	12
Figure 9	Additional step in the RC4 algorithm	13
Figure 10	Encrypted strings structure	14
Figure 11	C&C feed hosted on livejournal	14
Figure 12	C&C requests protocol	15
Figure 13	C&C replies protocol	16
Figure 14	Login page for the RTM panel	17
Figure 15	Cleaning DLL name	20
Figure 16	Configuration values xor key	21
Figure 17	Bogus registry check dialog	22
Figure 18	Fake registry error	23
Figure 19	Actual UAC prompt from Windows	23



There are several groups actively and profitably targeting businesses in Russia. A trend that we have seen unfold before our eyes lately is these cybercriminals' use of simple backdoors to gain a foothold in their targets' networks. Once they have this access, a lot of the work is done manually, slowly getting to understand the network layout and deploying custom tools the criminals can use to steal funds from these entities. Some of the groups that best exemplify these trends are Buhtrap, Cobalt and Corkow.

The group discussed in this white paper is part of this new trend. We call this new group RTM [1]; it uses custom malware, written in Delphi, that we cover in detail in later sections. The first trace of this tool in our telemetry data dates back to late 2015. The group also makes use of several different modules that they deploy where appropriate to their targets. They are interested in users of remote banking systems (RBS), mainly in Russia and neighboring countries.

In this paper, we cover the details of their tools, whom they target, and offer a rare glimpse into the type of operation they are carrying out.

1. TARGETS

That this group is mostly targeting businesses is apparent from the processes they are looking for on a compromised system. They look for software that is usually only installed on accountants' computers, such as remote banking software or tools to help with accounts payable. The full list of the processes they target is detailed in Section 4.4.2.

While both RTM and Buhtrap [2] are looking for a quite similar process list, the infection vectors are quite different. While the latter mostly used spear phishing campaigns, this group uses typical crimeware distribution channels such as drive-by downloads and spam. From our telemetry data, we see this threat actor focusing mostly on Russia and neighboring countries, with a few hits elsewhere. However, due to the mass spreading mechanism used, seeing detections outside the presumed primary region of interest is not surprising.

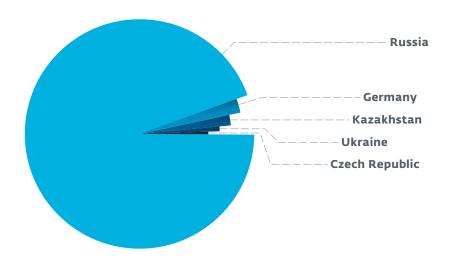


Figure 1 RTM telemetry

A Guide to the RTM Banking Trojan



The total number of detections we have for this threat is low and the complexity of the malware is high, indicating that this group is targeting specific, high-value targets in the Russian region.

In fact, the latest campaigns we have seen using the RTM malware contained interesting decoy documents as depicted in **Figure 2**.



Figure 2 Decoy document used in recent RTM campaigns

We found several types of decoy documents used by this group, such as contracts, invoices or tax-related forms. The nature of these decoy documents combined with the type of software targeted by this group lead us to believe they are going after accounting departments in Russian firms. These targets were also attacked by the Buhtrap group in 2014-2015.

While researching this group, we were able to interact with a few command and control (C&C) servers. The full list of commands that can be received from a C&C server will be covered in the following sections, but for now we can say that the client sends keylogger logs directly to the C&C, which then may respond with additional commands.

However, the days where you could just connect to the C&C and gather all the interesting interactions you wanted are mostly gone. To receive commands from the server, we had to provide realistic logs. We were rewarded for our efforts by seeing several relevant commands.

The first one was a request for the bot to hand over a specific file: 1c_to_k1.txt. This file is an export from popular accounting software called "1C: Enterprise 8" which, conveniently enough, is present in the process list that the bot is actively seeking. This software can work in tandem with different Remote Banking Systems (RBS) by exporting transfer data to a text file. This text file can then be imported into an RBS to automate the payment order as seen in **Figure 3**.



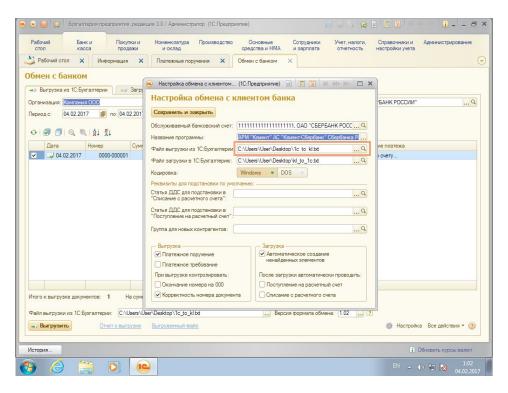


Figure 3 "1C: Enterprise 8" software export window

As the data in this file contain information about the transfer, it is possible for the fraudsters to modify the information in the file in order to steal money from the victim.

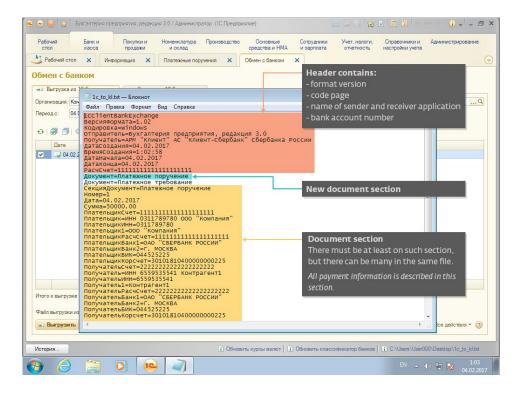


Figure 4 1c_to_kl.txt example



About a month after these files were requested from the C&C server, we saw the apparition of a new module: 1c_2_kl.dll. This module was pushed as a plugin to compromised systems and has the capacity to parse the export file automatically by injecting itself in the accounting software process. This module will be detailed in a later section.

Interestingly, FinCERT, a Russian CERT responsible for fighting cybercrime targeting Russian financial institutions, issued a statement warning potential victims against criminals going after 1c_to_kl.txt export files in late 2016. Also, the developers of "1C: Enterprise 8" are already aware of this scheme and issued a statement [3] acknowledging the problem and enumerating the possible protective measures the user can take to prevent this attack.

We also saw additional modules being downloaded once the bots reported to the C&C, such as a VNC module. This VNC module has both a 32 and 64-bits variants and is similar to a VNC module already seen in used in Dridex campaigns. We hypothesize that once the bot installs this VNC module, the criminals will use it to connect to the computer remotely and look around to see what they could do to take full advantage of the system. Organized groups like these usually then try to move laterally in the network, recovering account passwords through tools such as mimikatz and using other offensive tactics to learn more about the network and make the malware's presence as persistent as possible.

2. INFECTION VECTORS

The following figure shows the different infection vectors' first-seen date gathered throughout our tracking.



Figure 5 Infection vectors timeline



This group has used a large array of infection vectors, mostly revolving around drive-by downloads and spam. These channels are well suited for targeted attacks, since for the former, cybercriminals can pick websites likely to be visited by their targets, and for the latter, send emails with attachments directly to businesses or individuals the cybercriminals are attacking.

The fact that their malware is distributed through several different channels – such as the RIG [4] and Sundown exploit kits or spam runs – also shows that this group has strong ties with criminals in the underground market who are selling these services.

2.1. Is the malware related to Buhtrap?

As RTM exhibits some operational similarities to what we have seen with Buhtrap, one might legitimately wonder whether they are related.

In September 2016, we saw an RTM sample being distributed by a Buhtrap downloader. We also saw two code-signing certificates used to sign samples of both Buhtrap and RTM. The first one, issued to a company allegedly called TOV DNISTER-M, was used to sign a Delphi second stage (SHA-1: 025C718BA31E43DB1B87DC13F94A61A9338C11CE) as well as a Buhtrap DLL (SHA-1: 1E2642B454A2C889B6D41116CCDBA83F6F2D4890).

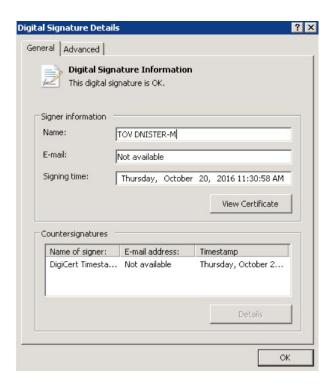


Figure 6 Code-signing certificate used by both RTM and Buhtrap

The second one, issued to a company allegedly called Bit-Tredj, was used to sign Buhtrap downloaders (SHA-1: 7C1B6B1713BD923FC243DFEC80002FE9B93EB292 and B74F71560E48488D2153AE2FB51207A0AC206E2B) fetching and installing an RTM payload. **Table 1** highlights key characteristics of these certificates.

Although they shared the code-signing certificate with other malware families, they also used one that, according to our telemetry, was used only by them. It was issued to a company allegedly called Kit-SD and was used to sign some RTM malware (e.g. SHA-1: 42A4B04446A20993DDAE98B2BE6D5A797376D4B6).



Table 1 Code-signing certificates used by RTM			
Company Name	Validity Period	Thumbprint & Serial	
Bit-Tredj	29/05/2016 – 30/05/2017	Thumbprint 2c14b428c4f5e260db13cff1b6b28d22beb59d7f Serial 54460e1fcd612cd3377ac2cd76e4240f	
TOV DNISTER-M	19/04/2016 - 20/04/2017	Thumbprint 457880da8899679870ad5b87312d882c006c9559 Serial 2567a463a84bb9d4207a11ec979205ac	
Kit-SD, OOO	21/06/2016 – 22/06/2017	Thumbprint b79d75191b3c0e3742b42c82e0a40dff9976708a Serial 1e21a4adcda618adc7b53193ef4aaf62	

Because they used the same Buhtrap downloader, they also shared some network indicators, since an RTM payload was downloaded from Buhtrap infrastructure. That said, as RTM has been using several different ways to distribute their malware besides the Buhtrap downloader, we believe that the groups using these two malware families are not the same. However, they are using a similar modus operandi. They are both targeting businesses using accounting software, are fingerprinting systems of interest similarly, are looking for smart card readers, and finally, they deploy an array of malicious tools to spy on their victims.

3. EVOLUTION

In this section, we will cover the different versions of the malware we have seen during our tracking, but first we need to define a way to follow its evolution.

3.1. Versioning

RTM stores configuration data in registry keys and a particularly interesting piece of information is called *botnet-prefix*. A list of all the values we have seen in the samples we analyzed is presented in **Table 2**.

Table 2	List of botnet prefixes			
0.1.6.4	0.1.6.6	0.1.7.6	0.1.9.0	
bit	bit2	bit3	hit3	
mtr	KL2	kosmos	main	

We are not sure of the purpose of this value. It may be used to record a version of the malware. However, we observed very few changes between consecutive versions such as bit2 and bit3 or 0.1.6.4 and 0.1.6.6. Moreover, one of the prefixes, main, has existed since the beginning and even evolved from typical C&C domains to .bit domains, as we will explain in Section 4.3.



3.2. Timeline

Using telemetry data, we created a timeline of the first appearance of the samples we have seen. This is presented in **Figure 7**.

	2015 October	2016 March	2016 April
	 First konwn appearance of the RTM malware. Main prefix. 	Appearance of the KL2 prefix.	 Switch to .bit C&C domains for all the prefixes. Appearance of the bit2 and bit3 prefixes.
			2016 July
			First known appearance of the hit3 prefix. Does not use .bit C&C domains
	2016	2016	2016
	December	October	September
		October First known appearance of the 0.1.6.6 prefix.	First known appearance of the kosmos and 0.1.6.4 prefixes.
_	December First known appearance	First known appearance	First known appearance of the kosmos

Figure 7 Timeline of the RTM malware

4. TECHNICAL ANALYSIS

In this section, we describe the main functions of the RTM banker. These include the persistence mechanism, their custom version of the RC4 algorithm, the network protocol, the spying abilities and some other miscellaneous functions. In particular, we will focus on the samples SHA-1 AA0FA4584768CE9E16D67D8C529233E99FF1BBF0 and 48BC113EC8BA20B8B80CD5D4DA92051A19D1032B.



4.1. Installation and persistence

4.1.1. Executable

The core of the RTM malware is a DLL but it is dropped onto the disk by a .EXE. That executable file is generally packed and contains the DLL code. When it is launched it only extracts the DLL and runs it using the following command:

rundll32.exe "%PROGRAMDATA%\Winlogon\winlogon.lnk",DllGetClassObject host

4.1.2. DLL

The main DLL is always dropped on the disk as winlogon.lnk in the %PROGRAMDATA%\Winlogon folder. This file extension usually refers to a shortcut [5] but this file is actually a DLL written in Delphi, which was called core.dll by its developers as shown in **Figure 8**.

core.dll DllGetClassObject

Figure 8 DLL name for sample F4C746696B0F5BB565D445EC49DD912993DE6361

Just after being launched, the malware sets up its persistence mechanism. It can do this in two different ways, depending on the victim's level of user privileges. That is, if running as admin, it can add an entry in the https://linklows.currentversion.kun registry under the name "Windows Update". The commands that are in the data of the "Windows Update" value will be executed at the start of the user session.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows Update [REG_SZ]
= rundll32.exe "%PROGRAMDATA%\winlogon.lnk",DllGetClassObject host

It will also try to add a task in the Windows Task Scheduler. This task will launch the winlogon.lnk DLL with the same export and parameter as explained before.

If running as an ordinary user, it will add a value in the HKCU\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run\ registry under the same name, "Windows Update" and with the same data:

rundll32.exe "%PROGRAMDATA%\winlogon.lnk",DllGetClassObject host

4.2. Modified RC4 algorithm

Despite its known weaknesses, the RC4 algorithm is regularly used by malware authors. However, RTM's programmers have decided to modify it slightly, possibly to slow down analysis by security researchers. This variant of RC4 is widely used in RTM in its malware to encrypt strings, network data, configuration and modules.



4.2.1. Differences

The original RC4 algorithm is divided into two main parts: the Key-Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA) [6]. The KSA part consists of the initialization of the *s table* using the key. In the PRGA part, the plain text is processed, using the *s table*, to obtain the ciphertext.

In the RTM malware, the authors added an intermediate step between the initialization of the *stable* and the encryption of the plaintext, meaning that it comes between the KSA and the PRGA. Before encrypting data, the *stable* is XORed with a four-byte number. This additional key is variable and is given at the same time as the data to encrypt or decrypt. The function that performs this additional step is given in **Figure 9**.

```
__fastcall TCrypt_RC4_variant_xor_stable(int a1, char *s_table, char
unsigned int
*xored_s_table, int iv)
   unsigned int i; // eax@1
   unsigned int v5; // eax@2
   i = 0:
   do
      *&xored_s_table[i] = iv ^ *&s_table[i];
      v5 = i + 4:
      *&xored_s_table[v5] = iv ^ *&s_table[v5];
      v5 += 4;
      *&xored_s_table[v5] = iv ^ *&s_table[v5];
      v_5 += 4:
      *&xored s table[v5] = iv ^ *&s table[v5];
      *&xored s table[v5] = iv ^ *&s table[v5];
      v5 += 4;
      *&xored_s_table[v5] = iv ^ *&s_table[v5];
      v5 += 4;
      *&xored_s_table[v5] = iv ^ *&s_table[v5];
      v5 += 4;
      *&xored_s_table[v5] = iv ^ *&s_table[v5];
      i = v5 + 4;
   while ( i < 255 );</pre>
   return i;
}
```

Figure 9 Additional step in the RC4 algorithm

4.2.2. String encryption

At first glance, there are few strings readable in the main DLL. The others are encrypted with the previous algorithm using the structure described in **Figure 10**. We found more than 25 different RC4 keys used for string encryption in the samples we analyzed while the XOR key is different for each string. The value of the integer field separating each string structure is always oxFFFFFFFF.

At the beginning of its execution, the malware decrypts the strings into a global variable. Then, when it needs to access a string, it dynamically computes the address of the decrypted strings based on a base address and an offset.



The strings contain interesting information about the functions of the malware. Some examples of these strings are found in Section 6.8.

```
struct struct_encrypted_string
{
    int separator; //constant - OxFFFFFFFF
    int size;
    int xor_key[4];
    char encrypted_data[size];
};
```

Figure 10 Encrypted strings structure

4.3. Network

The way the malware contacts the C&C has changed over the different versions. The first few samples, from October 2015 to April 2016, used traditional domain names along with an RSS feed hosted on livejournal.com to update the C&C list. Starting in April 2016, we observed in our telemetry data a move toward the use of .bit domains, which provides, as explained in Section 4.3.2, more resilience against domain takedown. The move is confirmed by the registration date of the C&C domains: the first RTM C&C .bit domain, fde05d0573da.bit, was registered on March 13th, 2016.

All C&C URLs we saw during our tracking shared a common path: /r/z.php. As this path is uncommon, it helps to identify RTM requests in network flows.

4.3.1. C&C feed

Older samples used a feed to update their list of C&C servers. This is hosted on livejournal.com and at the time of writing it is still up at the URL hxxp://f72bba81c921(.)livejournal(.)com/data/rss. Livejournal [7] is a US/Russian company providing social network services such as a blog-hosting platform. The RTM operators simply created a blog on livejournal and posted an article containing the feed of encrypted C&Cs. A screenshot of this blog is presented in **Figure 11**.

Figure 11 **C&C feed hosted on livejournal**

A Guide to the RTM Banking Trojan



The C&C strings are encrypted with the RC4 algorithm variant presented in Section 4.2. The actual version (November 2016) of the feed contains the following C&C addresses:

- hxxp://cainmoon(.)net/r/z.php
- hxxp://rtm(.)dev/o-3/z.php
- hxxp://vpntap(.)top/r/z.php

4.3.2 .bit domains

In the most recent versions of the RTM malware, the authors switched to C&C domains that use the .bit Top-Level Domain (TLD) [8]. This is not in the Internet Corporation for Assigned Names and Numbers (ICANN) list of TLDs [9]. Instead, it relies on the Namecoin cryptocurrency, a fork of the well-known Bitcoin. Malware authors do not frequently use the .bit TLD for their C&C domains, though an example of such use was previously seen in a version of the Necurs botnet [10].

Unlike Bitcoin, Namecoin blockchain users are able to store data. One of the main uses for this feature is the top level domain .bit. It is possible to register domains that will be stored in the blockchain. The associated record in the blockchain also includes the IP addresses the domain is resolving to. Thus, this TLD is said to be "censorship-resistant" because only the registrant can change the resolution of a .bit domain. That means it is much more difficult to disrupt a malicious domain using this kind of TLD.

However, the RTM malware does not embed any of the software needed to read the Namecoin blockchain. It relies on DNS tier servers like dns.dot-bit.org or OpenNic servers to resolve the .bit domains. Hence, it has the same resilience as the DNS servers it uses. We observed that some C&C domains stopped being resolved after they were mentioned in a blogpost.

Another advantage to the attackers of the .bit TLD is the cost. To register a domain, the operators only need to pay 0.01NC which corresponds to 0.00185 USD (as of December 5th, 2016). By comparison, a .com domain costs at least 10 USD.

4.3.3. Protocol

To contact its C&C, the malware uses HTTP POST requests with data formatted using a custom protocol. The path is always /r/z.php and User-Agent set to Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0).

In the requests to the C&C server, the data are formatted as follows, where the offset values are in bytes:

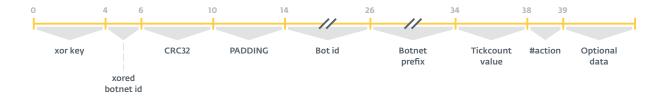


Figure 12 **C&C requests protocol**

The bytes o to 6 are not encrypted while the bytes starting at 6 are encrypted with the RC4 algorithm variant.

Read The ManualA Guide to the RTM Banking Trojan



The packet structure of the C&C's replies is simpler. The bytes from 4 to packet size are encrypted.



Figure 13 **C&C replies protocol**

A list of the possible values of the action byte is provided in **Table 3**.

Table 3	Possible v	alues of t	he action	field
Iables	PUSSIDIE 1	vaiues oi t	ne action	IICIU

Value	Action
0	OK (ACK)
1	Core. Optional: a string that contains a command.
3	Unrecognized request type
4	Unexpected request type
5	Install module
6	Execute downloaded executable
7	Execute downloaded executable. If the process does not have administrative rights, it will try to elevate its privileges using the method presented in Section 4.8.2.
8	Load downloaded DLL
9	Load and execute an MZ executable in memory without using a file.
10	Add a certificate to the windows store
11	Self-Update
12	Write a file into the common app data folder. (Usually C:\ProgramData)

The malware always computes the CRC₃₂ of the decrypted data and compares it with the one provided in the packet. If they differ, it will simply drop the packet.

A Guide to the RTM Banking Trojan



The optional data can contain different objects such as a PE file, a file to search in the file system or a new C&C URL.

4.3.4. Panel

Interestingly, we note that a panel is available on the C&C servers used by RTM. A screenshot of the login page is shown in **Figure 14**.

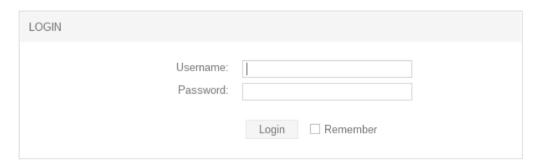


Figure 14 Login page for the RTM panel

4.4. Fingerprint

The RTM malware is a banking Trojan so it is not surprising that its operators need information about the victim's machine. The information gathered by the bot can be divided into two parts. On one hand, we find common information about the OS attributes. On the other hand, the malware checks whether the compromised machine contains artefacts related to Russian remote banking systems.

4.4.1. Common information

After the malware is installed or launched after a reboot, a report containing common information is sent to the C&C server. It contains:

- The time zone
- The default language identifier
- · The privileges of the logged-in user
- The process integrity level
- The username
- The computer name
- The OS version
- The additional modules installed
- · The security software installed
- The list of smart card readers



4.4.2. Remote banking system

A typical target for banking Trojans is the remote banking system [11] [2]. RTM is not an exception, as one of its classes is called TBdo. Bdo is the Russian translation for RBS (Remote Banking System) so it is clear that RBS is a target for this malware. This class is able to perform several tasks including the scanning of drives and of browsing history.

When the malware scans the drive, its sole aim is to determine whether banking software is installed on the machine. A full list of targeted software is available in Table 4. If it finds an interesting file, it reports the information to the C&C server. The next actions performed by the malware depend on the logic, which is on the C&C server-side.

Table 4	Targeted software				
_ftcgpk.exe	lcv8s.exe	CLBANK.EXE	iscc.exe	sbis.dll	wcInt.exe
lcv7.exe	bicrypt	client.jks	ISClient.exe	sbis.exe	webmoney.exe
1cv7l.exe	bssax.ocx	faktura	maratl.exe	SGBClient.exe	winpost.exe
1cv7s.exe	cbmain.ex	ifobsclient.exe	npbssplugin.dll	SGBClient.exe	
1cv8.exe	cbsmain.dll	internetbanktools.exe	qiwicashier.exe	transaq.exe	
lcv8c.exe	cft - bank client	intpro.exe	rclient.exe	wallet.dat	

The RTM malware also looks for banking URL patterns in IE's browsing history and in the opened tabs. For the history, it browses using the functions FindNextUrlCacheEntryA and FindFirstUrlCacheEntryA and for each entry, it checks to see if the URL matches one of the patterns shown in **Table 5**.

For opened tabs, it connects to Internet Explorer and Firefox through the Dynamic Data Exchange (DDE) [12] mechanism to access the current URL of tabs opened. For each tab, it also checks if that matches a pattern shown in **Table 5**.

The browsing history and the opened tabs check is executed in a WHILE loop with a sleep of 1 second between the checks. The other data monitored in real time will be detailed in Section 4.5.

Table 5	Targeted URLs		
	bsi.dll?	faktura.ru	elba.raiffeisen
	online.payment.ru	/iclient/	handybank.
	bankline.ru	ibank2	wupos.westernunion
	/ic/login.zhtml	bco.vtb24.ru	online.sberbank
	/servlets/ibc	elbrus.raiffeisen	

If a pattern is found, it is reported to the C&C using the list of strings presented in **Table 6**.



Table 6	Identifier for a banking related machine					
BSS		RosBank	BiCrypt	SberBank_Fiz	ISCC	
BSS_PC		SberBank_BO	VTB24	CFT	WebMoney	
iBank2_PC		INIST	SGB	WinPost	XTC	
Faktura		Inversion	Raiffeisen	SBIS	iFOBS	
РСВ		Interbank	HandyBank	ClBank	TRANSAQ	
InterPro		iBank2	WU	QiwiCashier	OSMP	

4.5 Monitoring

When the malware starts, various fingerprint information is sent to the C&C server, including the presence of banking software. This fingerprinting occurs only when the malware first starts monitoring the system, just after the initial scan is finished.

4.5.1. Remote banking system

The previously discussed class **TBdo** is also responsible for monitoring banking-related events. As in the initial scan, it uses DDE to check tabs in Firefox and Internet Explorer; another class, **TShell**, is also used to monitor shell windows (Internet Explorer and Explorer windows).

This class uses the COM interfaces IShellWindows, iWebBrowser, DWebBrowserEvents2 and IConnectionPointContainer to monitor the windows. When the user navigates to a new webpage, the malware is notified. It then checks the URL against the patterns provided in **Table 5**. If a match is found, it will take six consecutive screenshots, waiting 5 seconds between each one. Finally, it sends the screenshots to the C&C server.

It also checks for some window titles, related to banking software. A full list of these titles is available in **Table 7**.

Table 7	Banking windows targeted		
	Window name	Class name	
	ClBank	SunAwtFrame	
	ClBank	SunAwtDialog	
	Логин (Login)	TLoginWindow	
	Null	TfmISClient	
	Ключ электронной подписи (Key Electronic Signature)	TInitialForm	

A Guide to the RTM Banking Trojan



4.5.2. Smart card

The RTM malware has the ability to monitor smart card readers connected to the infected computers. These devices are used in some countries to validate banking related orders. So, if this kind of device is attached to the computer, it may indicate that these machines are used to perform banking transactions.

However, unlike other banking Trojans [13], it is not able to interact with these smartcards. Such features may be included in an additional module we have not yet seen.

4.5.3. Keylogger

An important part of the monitoring of the victim's computer is to record the keystrokes. Moreover, it seems that the RTM developers did not want to miss any information, as they monitor not only the keyboard but also the virtual keyboard and the clipboard.

To do so, they use the SetWindowsHookExA function to hook the keyboard and the mouse. When an event occurs, they log the key pressed, or the key corresponding to the click on the virtual keyboard, along with the software name and the date. Then, the buffer is sent to the C&C.

For the clipboard, they use the SetClipboardViewer function. They only log the clipboard content when the data is text. As for the keyboard, they also log the software name and the date before sending the buffer to the C&C.

4.5.4. Screenshots

The last monitoring feature is the ability to make screenshots. This is used when the shell monitoring class detects an interesting website or when a banking software window is detected. The screenshot is taken using the GDI library before being sent to the C&C.

4.6. Uninstall

The C&C can send a command to stop all the malware activities and clean the computer. It will clean all the files and the registry entries created during the execution of RTM on the victim's machine. Then, using an additional DLL encrypted in the malware, it will kill the malware and delete the winlogon file. Finally, it shuts down the computer. As shown in Figure 15, this DLL was called erase.dll by its developers.

erase.dll DllGetClassObject

Figure 15 Cleaning DLL name

A more destructive command can be sent to the malware, called *uninstall-lock*. If the malware has administrative rights it will try to erase the MBR. If it fails, it tries to move the MBR to a random path. If it succeeds, the computer will no longer boot after the shutdown. In this event, it would probably lead to a full reinstallation of the machine, erasing all possible forensic evidence. If the program has low privileges, the malware writes a .EXE that is encrypted in the main RTM DLL. This .EXE is really small and only implements the code needed to shut down the computer. It will also register this executable in the HKCU\CurrentVersion\Run registry key. Thus, each time the user starts a session, the computer will immediately shut down.



4.7. Config

By default, the RTM malware doesn't really have a config file. However, the C&C can push config values that will be stored in the registry and used by the malware. A list of configuration keys is presented in **Table 8**.

Table 8 Configuration keys				
keylogger.last-data	botnet-id	cc.url.1		
keylogger.last-wnd-caption	cc.connect-interval	cc.url.2		
keylogger.last-exe-path	scan-files	scards.monitoring-interval		
botnet-prefix	post-install-report	dbo.detected		
scan-files	multiinstance-off	post-install-report-url		
modules-data.%modulename%	keylogger-off	dbo-detector-off		
scard-off	modules-off	modules.%modulename%		

The configuration is stored in the registry Software\[Pseudo-random string] key. In this registry key, each value corresponds to one of the strings presented in the previous table. However, the values and the associated data are encrypted using RTM's custom RC4 algorithm.

The data has the same structure as the network or the strings. The four-byte XOR key is added at the beginning of the encrypted data.

For the configuration values, the XOR key is different and depends on the size of the value. It can be computed as follows:

```
xor_key = (len(config_value) << 24) | (len(config_value) << 16) | len(config_value) << 8)</pre>
```

Figure 16 Configuration values xor key

4.8. Other functions

This malware has many other functions that we present here.

4.8.1. Additional modules

It can run additional modules that are DLL files. They are sent over the network by the C&C server and could be run as external programs. They can also be mapped in memory and launched in new threads.

For storage, they are saved in .dtt files and encrypted using the custom RC4 algorithm with the same key used for the network communications.

At this time, we have seen only the VNC module (8966319882494077C21F66A8354E2CBCA0370464), the browser data exfiltration module (03DE8622BE6B2F75A364A275995C3411626C4D9F) and the 1c_2_kl module (B1EE562E1F69EFC6FBA58B88753BE7D0B3E4CFAB) being installed on an infected machine.

A Guide to the RTM Banking Trojan



For the VNC module, the C&C server later sent a command, asking to connect to a VNC server at a specific IP address on port 44443.

The browser data exfiltration plugin implements the class **TBrowserDataCollector**, which is able to read the IE's browsing history. It then sends the full list of visited URLs to the C&C server.

The last discovered module is called 1c_2_kl and is able to interact with the 1C software suite, which was described in Section 1. This module is divided in two parts: a main DLL and two agents (32 and 64 bits) that will be injected in every process by registering a hook to the WH_CBT event. If the agent is injected in a process of the 1C suite, it hooks the CreateFile and WriteFile functions.

Whenever the hooked <code>CreateFile</code> function is called, it keeps in memory the file path should its filename be <code>lc_to_kl.txt</code>. Then, when a call to <code>WriteFile</code> is intercepted, it calls the genuine <code>WriteFile</code> function and sends the <code>lc_to_kl.txt</code> file's path to the main module DLL by sending it a crafted <code>WM_COPYDATA</code> Windows message.

Finally, the main module DLL opens and parses the file to identify payment orders. It extracts both the total amount and number of transactions contained in the file. Ultimately, it sends this information to the C&C server. At this time, we believe this module is still in development as it contains debug messages and it cannot modify automatically the 1c_to_kl.txt file.

4.8.2. Privilege elevation

This malware can try to elevate its privileges by showing fake error messages. First, it mimics a registry check by using a similar design to typical Windows progress bars, as shown in **Figure 17**. It also uses the real *regedit* icon. We could also note the spelling mistake in "whait". After a few seconds, the scan is finished and a fake error message is displayed.

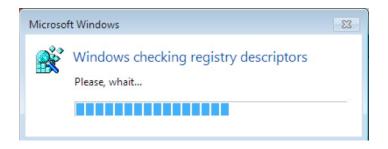


Figure 17 Bogus registry check dialog

This fake error message, shown in **Figure 18**, would easily fool a typical end user. Once again, the design is similar to that of a regular Windows error message, but again there are telltale grammatical errors not found in real Windows error dialogs. If the user clicks on one of the two choices, it will try to elevate the malware's privileges.

Immediately after the user clicks on one of the restore choices, the malware launches the DLL using the runas option in the ShellExecute function. This will run the program with administrative privileges. However, the user will be prompted with a real UAC prompt coming from the Windows system, shown in Figure 19, asking the user to allow the privilege elevation. If thus allowed, the malware will run with administrative privileges.



Thus, rather than depending on a vulnerability, it tries to confuse the user. Moreover, depending on the machine's default language, error messages will be displayed in English or in Russian.



Figure 18 Fake registry error



Figure 19 Actual UAC prompt from Windows

4.8.3. Certificates

The malware can also add certificates to the Windows store and it is able to validate the addition by automatically clicking "Yes" on the csrss.exe dialog box. This behavior is not new, as the Retefe banking Trojan is also able to self-validate a new certificate installation [14].

4.8.4. Backconnect

The malware authors also implemented a Backconnect TCP tunnel. We have not seen any usage of this functionality but it may be used to control the infected machines remotely.

4.8.5. Host file management

The C&C can send a command to the malware to modify Windows' etc/hosts file. The hosts file is used on Windows systems to make custom DNS resolutions.

A Guide to the RTM Banking Trojan



4.8.6. Find and send a file

The C&C can ask the malware to find a file on the file system and to upload it to the server. For instance, during our investigation, we received a command from the C&C server asking for the file 1c_to_kl.txt. As explained before, this file can be generated by the accounting software 1C: Enterprise 8.

4.8.7. Update

Finally, the authors can update the malware by sending a new DLL that will replace the current version.

5. CONCLUSION

Our research on the RTM malware shows that the Russian banking system is still a target of choice for criminals. Other groups, such as Buhtrap, Corkow and Carbanak, were already known to target and successfully steal money from financial institutions and their customers in Russia. Thus, RTM is another player in this profitable game.

According to our telemetry, this piece of malware has been used since the end of 2015 or earlier. Even though it does not use previously unknown techniques, it implements a full range of spying capabilities including smart card reading, keylogging and real-time monitoring of banking-related activities. It can also search for export files created by accounting software such as 1C: Enterprise 8. Finally, its command and control infrastructure is highly resilient, since it uses the decentralized and non-censurable .bit top-level domain.

The Indicators of Compromise (IOCs) are detailed in Section 6 and on GitHub. If you have any questions related to this investigation, please contact us at threatintel@eset.com.

Acknowledgements

Special thanks to our colleagues Anton Cherepanov and Jan Matušík for their help in this research.



6. INDICATORS OF COMPROMISE

6.1. ESET detection names

Win32/Spy.RTM.A
Win32/Spy.RTM.B
Win32/Spy.RTM.C
Win32/Spy.RTM.D
Win32/Spy.RTM.E
Win32/Spy.RTM.F
Win32/Spy.RTM.G
Win32/Spy.RTM.H
Win32/Hvnc.AD
Win64/Spy.RTM.A

6.2. File names

C:\ProgramData\Winlogon\winlogon.lnk

6.3. Registry indicators

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run :
 Windows Update = rundll32.exe "%PROGRAMDATA%\Winlogon\winlogon.lnk",DllGetClassObject
host

HKLU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run :
 Windows Update = rundll32.exe "%PROGRAMDATA%\Winlogon\winlogon.lnk",DllGetClassObject
host

6.4. Hashes

6.4.1. DLLs

30c8b60ccd66eafb4c861584f45fe80dab71ee22 471a8fd0aa32ce61cf5e4ebece95527d1b234de6 42h990344d77h22578h0a35adda62c0hc02a09a5 be06b838e8b4b2e6bf59ceaafa3fbbb4cebdc522 f9183b6e29fee2c3467fc591bae9bb5fe9975027 c8f0c4a88397c16695e1352a48c538fb02f1cb16 e942145c0f3549bf7be79cbf5a4031cf6614af19 0705bda19096b05130e5768ea8efdaa864ddaff0 c75273cd886c3ea18a5be7e99b11044f88abd3ef e0f377551d5b6553eedf9a0c3ef23eabfc7a937e e7777db52fc9d34d57253db242f9c195d24836d8 ef7de8d746c413a8925aa6a01f7130cfc7eac2df 00fe6cf9c85821a2a2479083acb538ee49c8c141 5d6a96466e60f15b296d9b0d4cb3e095957d0aa4 9172dd756893fe9e68b2dcc85613e7346d1a25ef 5f357fbb6ae832f7a0fcfa824fa4026db4000a0a ebdd585edfe6ff9359a38cb7fb65871f418c6c33 c3ba475f4e160a153c3baada8042b6aca5d06618 f6755195445ce89f61df8ad6aaf2bf491804224a 4a670cc34e59ea94e88c19eef6a4106cf5411624 5153886fec6cfed815601e68678286633bc564ec 4d83f2f601036bc770857f96ab16017b0afb6927 be83dd98b269bb2faf9e28e35734d3bfcf635166 f4c746696b0f5bb565d445ec49dd912993de6361 d8f3c6a1bb43d014fa34eaaae41a8d9eefd7c3b6 31b7215c892a0064a6f59c16d68a1decf39012a9 5521cce3e5e68eb6b8f7fa129daf143151436b2d da0c6236909ea861b2d24794e88ff44c051ade64 822e05f998f5d727d5a663d06273da507ef5f135

A Guide to the RTM Banking Trojan



5b7355ea8152b95a7ab9bb91e5836bf7acc39993 1f100e41213be79deacc86a9246e1d0b8a76d64b fd4b98893de80ef3fe83b58017df9718993d8bcb 6f036c802384826b630aec70d9833b5b0ed735eb 1e4b84be1e4287c9787cd56009e1e2adb3348db8 6cf45111b2d71862803cf91f2a79780149c46a27 af862050a01972db36589653dc8b155e2b3e2f8c b31a565e7c29b861b182c9880b5d38cb4211ab8f dde57ff3b630a1b4052c3ef290bb361de96eab06 bdf77429c785514bf308f7c1d1e9ddca63a33ac8 2f6fd3b5a7611d72f9f9eb60b04471f9bebc738f 0b40873f86c2e6c676dfc003c232aa3167654172 d6004423e7b80d47b6215c9d1875122e128899ed c4834a4e548b82ffe5d90042c78311b537564fe6 5cclac4f0cc6df3f0dbe2b53864a0f47899939c8 4733cf689dcc588b94fd0fba7ad4d93973486752 7175b734aa1273710008a2af6398f8bfc55f7f6b cab9247484a6c7a10672b7ca8849dd7b4577be02 daa0673cb1d3eb7dbe8aa435997ecd9e1da228fd f04300e901870efa9c9e49c440baaac23b0ce96c 9a131fc27f5397e32596e81df22260885b53cdfd 094ac3c414a9e6028afa5cdc0d4b4f3aa98b92ca 9a3e89d62795a1cb0747d279a6fdf65bfc8d5c8d df1a4c99791570a2d203075581a6aeef59ece02b 94e21bac5c0fc0d8d583a0b9b1daf5d18528cc9f aa0fa4584768ce9e16d67d8c529233e99ff1bbf0

6.4.2. Droppers/Downloaders

0961119783365e8b4dff12df7c7ae9f7388a410c 662b4daea4b07e7c95f4a58cf0be0f0281c81c67 859f66a7057304e72eaff58ded1a2aeae29a41dc 42a4b04446a20993ddae98b2be6d5a797376d4b6 48bc113ec8ba20b8b80cd5d4da92051a19d1032b 025c718ba31e43db1b87dc13f94a61a9338c11ce 059a114c2ec56434251cec7db4828418335cf29a 4a084e70fa2e6425c68c692b560acae68f89e69f 77a7735d0f83610e4d581850dd89ea15b6c5f699 83db465d10e6f403cf28ed714fbdf5e218b8fb41 8b77419e6c006303f078e77e6c1ca21547b8bdd1 9ac461ef9848367f46bf64649d46de955c4afc66 a1c7b51747ad13c5a1df470098a4585e1f24a5c4 a6d3e97d832d17d589c1a0aa24baaeccd73a2b39 e9fe3259bceb852ec1b8e5a01ff19eb7e3b08fbc f539f5f3847d60ef6b6bfe32be76fe190b9298b0 e36f88d67cd50a9bc2e5d30cbf26577ffadd4a90 d125a868c393c3490d2d24016edb159a2a5ad0a9 92a1c9fc9069744653d4d3733ebf8669a84351b9 9d2fd31c086f0e982f6b973ee5951173ab69d0b2 cca9ade798a61450adbbcac5e433dadde11867ba fca3d02a53e66d8975997ff2b03c8008a254a508 312a487b2830c62845f6feaf11d4af7c25783f1a c4844acd88eeb104a05a775e475bc48e05a238e7 c824ee17138d2002a712744c3012fc51355fb044 85a6d6938680b30bac2c755a502f6b4f104643a3 d0390f4bcd5c0a952c012fbd034e78dbe88ed184 43a4c65da2c112c42e910f4e6ea359c759064d52 5b38be812c5e21fb9efb01eea845704cf9978a6d c6e3aa123a52762bf2690b97cc79148eedd0e1e0 136185555755c537522e5ccc8a0d7487dc9dcffa 7c48114467776541032206fd9ae22be8490c45ba f89e56dd9ca78cec02d0a2b95803843c59234082 1e3061c49cf62821ca17b835b7ff8d9d8a3bb6c2 f667d946acbc69d70ea0978b9b6878d232665cad 49994863baffba440212bd24232df21fbf93d812 7c1b6b1713bd923fc243dfec80002fe9b93eb292 b74f71560e48488d2153ae2fb51207a0ac206e2b

A Guide to the RTM Banking Trojan



6.4.3. Modules

03DE8622BE6B2F75A364A275995C3411626C4D9F 8966319882494077C21F66A8354E2CBCA0370464 B1EE562E1F69EFC6FBA58B88753BE7D0B3E4CFAB

6.5. C&C server domain names

```
f72bba81c921(.)livejournal(.)com/data/rss
webstatisticaonline(.)tech
vpntap(.)top
rtm(.)dev
cainmoon(.)net
micro4n(.)top
ssdcool(.)top
cash-money-analitica(.)bit
money-cash-analitica(.)bit
vpnomnet(.)bit
vpnkeep(.)bit
fde05d0573da(.)bit
d47ea26b7faa(.)bit
feb96eb2aa59(.)bit
```

6.6. C&C server IP addresses

```
5.154.190(.)167
5.154.190(.)168
5.154.190(.)189
5.154.191(.)57
5.154.191(.)154
5.154.191(.)174
5.154.191(.)225
37.1.206(.)78
88.208.28(.)147
91.207.7(.)69
91.215.153(.)31
93.170.168(.)218
93.190.139(.)66
95.183.52(.)182
109.236.82(.)150
109.248.32(.)152
131.72.138(.)169
138.201.104(.)161
154.70.153(.)125
158.255.6(.)150
158.255.208(.)197
185.61.149(.)70
185.61.149(.)78
185.82.201(.)45
185.82.216(.)14
185.128.42(.)237
185.141.27(.)249
185.169.229(.)42
188.138.71(.)117
200.74.240(.)80
200.74.240(.)134
212.48.90(.)155
213.184.127(.)137
217.23.6(.)29
```

6.7. PDB paths

getapulab.pdb

A Guide to the RTM Banking Trojan



6.8. Strings

ZKRT, winhttp.dll, WinHttpOpen, WinHttpCloseHandle, WinHttpConnect, WinHttpOpenRequest, WinHttpReadData, WinHttpCrackUrl, WinHttpSendRequest, WinHttpReceiveResponse, WinHttpSetOption, Software\\, keylogger.last-data, keylogger.last-wnd-caption, keylogger.last-exe-path, FRTnBm6glKEZf60, kosmos, botnet-prefix, botnet-id, cc.connect-interval, GetSystemDefaultUILanguage, RTM_ModuleEP, scan-files, crypt32. dll, CryptUnprotectData, post-install-report, cc.url.1, cc.url.2, __, x32, x64, , , modules., modules-data., core, msg, del-module, unload, uninstall, uninstall-lock, find-files, shutdown, reboot, cfg-set-str-a, cfg-set-str-w, cfg-set-dw, cfg-get-str-a, cfg-get-str-w, cfg-get-dw, cfg-del-param, screenshot, dns, lpe-runas-flags, SOFTWARE\\ Microsoft\\Windows NT\\CurrentVersion, EditionID, Service Pack , SP, CSDVersion, CurrentVersion, CurrentBuildNumber, scards.monitoring-interval, files found, image/ png, .png, ROOT, csrss.exe, OldFile, Updated, dbo.detected, bsi.dll?, online.payment. ru, bankline.ru, /ic/login.zhtml, /servlets/ibc, faktura.ru, /iclient/, ibank2, bco.vtb24.ru, elbrus.raiffeisen, elba.raiffeisen, handybank., wupos.westernunion, online.sberbank., Unk, SberBank_PC, BSS, BSS_PC, iBank2_PC, Faktura, PCB, InterPro, RosBank, SberBank_BO, INIST, Inversion, Interbank, iBank2, BiCrypt, VTB24, 1C, SGB, Raiffeisen, HandyBank, WU, SberBank Fiz, CFT, WinPost, SBIS, ClBank, QiwiCashier, ISCC, WebMoney, XTC, iFOBS, TRANSAQ, OSMP, IExplore, Firefox, 0xFFFFFFFF, WWW_GetWindowInfo, \",\", gdiplus.dll, GdipGetImageEncodersSize, GdipGetImageEncoders, GdiplusStartup, GdiplusShutdown, GdipCreateBitmapFromHBITMAP, GdipDisposeImage, GdipSaveImageToStream, ole32.dll, GetHGlobalFromStream, CreateStreamOnHGlobal, kernel32.dll, CloseHandle, user32.dll, ToUnicode, CloseClipboard, WinSCard.dll, SCardFreeMemory, SCardListReadersW, SCardEstablishContext, SCardReleaseContext, SCardGetStatusChangeW, SeShutdownPrivilege, auto-elevate, Elevating success, Elevating failed, reload, Reloaded, ntdll.dll, RtlAdjustPrivilege, ZwShutdownSystem, new-cc, hosts-add, hosts-clear, dbo-scan, scard-off, modules-off, dbo-detector-off, multiinstance-off, keylogger-off, dnsapi. dll, DnsQuery_A, DnsRecordListFree, dns.dot-bit.org, 193.183.98.154, 106.186.17.181, 50.116.23.211, 130.255.73.90, 109.69.8.34, File already updated, post-install-reporturl, 527D67BF-0D37-46D8-895F-D662E8A12190, 3998A1EC-1726-42CA-830C-D6E966D21411, 5B42B658-6029-44FD-9561-1ED64E89A0AA, 692B2F88-60F4-45A4-88E2-946F98E12773, A69D400E-70E8-45F4-9438-80734E1FEA72, SYSTEM\\CurrentControlSet\\services\\Disk\\Enum, sdtf, D2, GET, POST, HTTP/1.1, Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0), Close, Accept: t, http://vpnomnet.bit/r/z.php, http://vpnkeep.bit/r/z.php, non, ?a=started&fid=, *.*, *.dtt, .dtt, rundll32.exe, open, regedit.exe, BUTTON, STATIC, msctls_progress32, DISPLAY, Windows Registry Error, Windows >\u00044\u0004=\u00040\ $\verb"u0004@ \verb"u00046 \verb"u00048 \verb"u00044" \verb| "u00042 \verb| u00044 \verb| u00045 \verb| u00045 \verb| u00045 \verb| u00045 \verb| u00045 \verb| u00045 \verb| u00046 \verb| u00045 \verb| u00046 | u00046 | u00046 | u00046 | u00046$ $\verb"u00044| \verb"u00045| \verb"u0004=| \verb"u0004=| \verb"u00045| \verb"u00040| \verb"u00049| \verb"u00048| "u00048| "u0048| "$ u0004 @\u00045\u00045\u0004A\u0004B\u0004@\u00040\u0004, Windows has encountered a corrupted registry records, \u0018\u0004A\u0004?\u0004@\u00040\u00042\u00048\u0004B\ u0004L\u0004 7\u00040\u0004?\u00048\u0004A\u00048\u0004, Restore records, \u0018\ $\verb"u0004A| \verb"u0004@| \verb"u00040| \verb"u00042| \verb"u00048| \verb"u0004E| \verb"u0004E| \verb"u00040| \verb"u00049| \verb"u00048| "u00048| "u0048| "u0$ u0004A\u00048\u0004 8\u0004 ?\u0004@\u0004>\u00042\u00045\u0004@\u00048\u0004B\u0004L\ u0004 =\u00040\u0004 >\u0004H\u00048\u00041\u0004:\u00048\u0004, Restore records and check for errors, \u0001f\u0004>\u00044\u0004@\u0004>\u00041\u0004=\u00045\u00045\u0004 \u00041\u0004 M\u0004B\u0004>\u00049\u0004 >\u0004H\u00048\u00041\u0004:\u00045\u0004, More details about this error, \u0001e\u000041\u00004=\u000040\u00004@\u00004C\u000046\u000045\ $u0004 = \\ u0004 \\ \\ u0004 \\ \\ u0004 \\ \\ u00042 \\ \\ u00044 \\ \\ u00045 \\ \\ u00044 \\ \\ u00044 \\ \\ u00045 \\ \\ u00044 \\ \\ u00045 \\ \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u00044 \\ u0004 \\ \\ u00044 \\$ u0004K\u00045\u0004 7\u00040\u0004?\u00048\u0004A\u00048\u0004 2\u0004 @\u00045\u00045 u0004A\u0004B\u0004@\u00045\u0004 Windows., Multiple corrupted records has been found in Windows registry., \u0014\u0004;\u00040\u0004 C\u0004A\u0004B\u0004@\u00040\u0004=\ u00045\u0004=\u00048\u00040\u0004 >\u0004H\u00041\u0004:\u00048\u0004, Windows 8\u0004A\u0004?\u0004@\u00040\u00042\u00048\u0004B\u0004 ?\u0004>\u00042\u0004@\u00045\ $u00046 \setminus u00044 \setminus u00045 \setminus u0004 = \setminus u0004 = \setminus u0004K \setminus u00045 \setminus u00040 \setminus u0004? \setminus u00048 \setminus u0004A \setminus u00046 \setminus u00048 \setminus u00048$ u00048\u0004., To resolve this problem, Windows restore these records., \u0014\u00045\ $u0004B \\ u00040 \\ u0004; \\ u00048 \\ u0004 \\ > \\ u0004H \\ u00048 \\ u00041 \\ \\ u00044; \\ u00044: \\ \\ u0004: \\ \\ u0004$ $u00045 \setminus u00042 \setminus u00045 \setminus u0004e \setminus u0004e \setminus u00044 \setminus u00044 \setminus u00045 \setminus u00044 \setminus u00044 \setminus u0004e \setminus u00046 \setminus u$ u00048\u0004?\u0004B\u0004>\u0004@\u0004, Error details: Incorrect descriptor, \u001f\ $u0004 > \\ u00042 \\ u00046 \\ u00045 \\ u00044 \\ u00045 \\ u0004 \\ = \\ u0004 \\ = \\ u0004K \\ u00045 \\ u00046 \\ = \\ v0004K \\ u00046 \\ = \\ v0004K \\ v00046 \\ = \\ v0004K \\ = \\ v0004$ u00040\u0004?\u00048\u0004A\u00048\u0004:, Corrupted records: , \u001a\u0004>\u0004;\ u00045\u00049\u0004: 3, Corrupted records count: 3, \u001e\u0004B\u0004<\u00045\u0004=\ u00040\u0004, Cancel, \u001e\u0004H\u00048\u00041\u0004:\u00040\u0004: \u0001d\u00045\ $\verb"u00042\u00045\u0004e\u0004+\u00044\u00044\u00045\u00044\u00044\cdot\u00048\u00048\u00046\u00040\u0004\u00046\u00040\u0004\u$





 $u0004? \\ u00048 \\ u0004> \\ u00044 \\ r \\ n \\ u0001a \\ u0004> \\ u00044 \\ u0004 \\ > \\ u0004H \\ u00048 \\ u00041 \\ > \\ u0004H \\ u00048 \\ = \\ u0004H \\ u00048 \\ = \\ u0004H \\ = \\$ u0004:\u00048\u0004: 0xc0005071, Error: Incorrect descriptor\r\nError code: 0xc0005071, Microsoft Windows, \u0001f\u0004@\u0004>\u00042\u00045\u0004@\u0004:\u00040\u0004 4\ $u00045 \setminus u0004A \setminus u0004: \setminus u00048 \setminus u00048 \setminus u0004B \setminus u0004 + \setminus u00048 \setminus u0004 + \setminus u00042 \setminus u0004 = \setminus u00048 \setminus u00048 \setminus u0004 + \setminus u00048 \setminus u0004$ u00045\u00045\u0004A\u0004B\u0004@\u00040\u0004 Windows, Windows checking registry descriptors, \u001f\u0004>\u00046\u00040\u0004;\u0004C\u00049\u0004A\u0004B\u00040\ u0004, ?\u0004>\u00044\u0004>\u00046\u00044\u00048\u0004B\u00045\u0004..., Please, whait..., runas, \",DllGetClassObject host, .1, #32770, SysCredential, ComboBoxEx32, ComboBox, Edit, CLIPBOARD, .exe, WbemScripting.SWbemLocator, localhost, root\\CIMV2, SELECT * FROM Win32_NetworkAdapterConfiguration Where IPEnabled = True, WQL, root\\ SecurityCenter, SELECT * FROM AntiVirusProduct, \\VarFileInfo\\Translation, \\ StringFileInfo\\, ProductVersion, wclnt.exe, cbmain.ex, ibank.odb, internetbanktools. exe, LegalCopyright, ProductName, bicrypt, faktura, client.jks, intpro.exe, npbssplugin. dll, bssax.ocx, cbsmain.dll, isclient.exe, 1cv8.exe, 1cv8c.exe, 1cv8s.exe, 1cv7.exe, 1cv7l.exe, 1cv7s.exe, sgbclient.exe, rclient.exe, cft - bank client, winpost.exe, sbis.exe, sbis.dll, clbank.exe, qiwicashier.exe, iscc.exe, webmoney.exe, ftcqpk.exe, wallet.dat, ifobsclient.exe, transaq.exe, maratl.exe, 1\u00040\u0004=\u0004:\u0004, bank, SunAwtFrame, SunAwtDialog, \u0012\u0004E\u0004>\u00044\u0004 2\u0004 A\u00048\ u00043\u00048\u0004=\u0004, TLoginWindow, TfmISClient, TInitialForm, \u0001a\u0004;\ $u0004N \\ u0004G \\ u0004 \\ M \\ u0004; \\ u00045 \\ u00048 \\ u0004@ \\ u0004 \\ \times \\ u0004 \\ \times$ u00049\u0004 ?\u00044\u00044\u00048\u0004A\u0004A\u0004A\u0004, obj_button, obj_static, tpanel, tbsvkcontrolscroller, Tahoma, *.pif, pif, .job, Software\\Microsoft\\Windows\\ CurrentVersion\\Run, Windows Update, Tasks\\, Microsoft Corporation, Updating Windows components., Author, PTOS, schedule, Winlogon, \\winlogon.lnk, \",DllGetClassObject , SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon, Shell, \\\\.\\PhysicalDrive, bootmgr, ntldr, Global\\, drivers\\etc\\hosts, ipconfig /flushdns, iexplore.exe, firefox.exe, xb

A Guide to the RTM Banking Trojan



7. BIBLIOGRAPHY

- 1. Kafeine, 20 10 2016. [Online]. Available: https://twitter.com/kafeine/status/789063680507912192.
- 2. J.-l. Boutin, «Operation Buhtrap, the trap for Russian accountants,» ESET, og o4 2015. [Online]. Available: http://www.welivesecurity.com/2015/04/09/operation-buhtrap/.
- 3. «Информация для пользователей и партнеров №22531 от 20.01.2017,» [Online]. Available: https://lc.ru/news/info.jsp?id=22531. [Accessed o5 o2 2017].
- 4. «Rig Exploit Kit via EiTest delivers malicious payloads,» 19 10 2016. [Online]. Available: http://www.broadanalysis.com/2016/10/19/rig-exploit-kit-via-eitest-delivers-malicious-payloads/.
- 5. «Shortcut (computing),» o7 12 2016. [Online]. Available: https://en.wikipedia.org/wiki/Shortcut_(computing)#Microsoft_Windows.
- 6. «RC4,» [Online]. Available: https://en.wikipedia.org/wiki/RC4#Key-scheduling_algorithm_.28KSA.29.
- 7. «Livejournal,» [Online]. Available: http://www.livejournal.com.
- 8. McArdle, Robert; Sancho, David;, «Bitcoin Domains,» 2013. [Online]. Available: http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-bitcoin-domains.pdf.
- «List of Top-Level Domains,» ICANN, 14 12 2016. [Online].
 Available: http://data.iana.org/TLD/tlds-alpha-by-domain.txt.
- 10. «Necurs C&C domains non-censorable,» Bluecoat, og og 2013. [Online]. Available: https://www.bluecoat.com/security-blog/2013-09-10/necurs-%E2%80%93-cc-domains-non-censorable.
- 11. A. Matrosov, E. Rodionov, D. Volkov and D. Harley, «Win32/Carberp: When You're in a Black Hole, Stop Digging,» 2012. [Online]. Available: http://www.welivesecurity.com/media_files/white-papers/carberp.pdf.
- 12. "About Dynamic Data Exchange," Microsoft, [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms648774(v=vs.85).aspx.
- 13. A. Matrosov, «Smartcard vulnerabilities in modern banking malware,» ESET, o5 o6 2012. [Online]. Available: http://www.welivesecurity.com/2012/06/05/smartcard-vulnerabilities-in-modern-banking-malware/.
- 14. J. Hořejší, «Retefe banking Trojan targets UK banking customers,» AVAST, 22 o6 2016. [Online]. Available: https://blog.avast.com/retefe-banking-trojan-targets-uk-banking-customers.