# Russian Language Malspam Pushing Redaman Banking Malware

unit42.paloaltonetworks.com/russian-language-malspam-pushing-redaman-banking-malware/

Brad Duncan, Mike Harbison

January 23, 2019

By Brad Duncan and Mike Harbison

January 23, 2019 at 6:00 AM

Category: Unit 42

Tags: Banking Trojan, Malspam, redaman, Russia

This post is also available in: <u>日本語 (Japanese)</u>

Redaman is banking malware first noted in 2015 that targets recipients who conduct transactions using Russian financial institutions. First reported as the <u>RTM banking Trojan</u>, vendors like <u>Symantec</u> and <u>Microsoft</u> described an updated version of this malware as Redaman in 2017. We have found versions of Redaman in Russian language mass-distribution campaigns during the last four months of 2018. This blog tracks recent developments from an ongoing campaign of malicious spam (malspam) currently distributing this banking malware from September through December of 2018. We cover the following areas:

- Infection vector
- Email characteristics
- Targeted recipients
- Analysis of a Redaman sample
- Infection traffic

#### **Infection vector**

Since September of 2018, Redaman banking malware has been distributed through malspam. In this campaign, the Russian language malspam is addressed to Russian email recipients, often with email addresses ending in *.ru*. These emails have file attachments. These file attachments are archived Windows executable files disguised as a PDF document. In September 2018, the attachments were zip archives. In October 2018, the attachments were zip archives. In November 2018, the attachments were rar archives. And in December 2018, the attachments changed to gzip archives with file names ending in *.gz*.

## **REDAMAN MALSPAM INFECTION CHAIN**



*Figure 1: Flow chart for infections from Redaman banking malware from September through December of 2018.* 

## The emails

Subject lines, message text, and attachment names constantly change for this malspam. But the messages all have a common theme: they refer to a document or file for an alleged financial issue the recipient needs to resolve. These messages are often vague, and they contain few details on the alleged financial issue. Their only goal is to trick the recipient into opening the attached archive and double-clicking the executable contained within.

Among dozens of examples seen from September through December of 2018, here is a selection of 10 subject lines from this malspam:

- Subject: Акт сверки сентябрь-октябрь
- Subject: Весь пакет док-ов за прошлый месяц
- Subject: Все док-ты за август-сентябрь
- Subject: Деб.задолженность среда
- Subject: Документы, сверка 02.10
- Subject: Заявка на возврат за ноябрь
- Subject: Необходимо свериться среда
- Subject: Отправка на за прошлую неделю
- Subject: Пакет документов для оплаты 1е октября
- Subject: Сверка на оплату

The following are Google translations for the above subject lines:

- Subject: Act of reconciliation September-October
- Subject: All package of last month's documents

- Subject: All docs for August-September
- Subject: Debt due Wednesday
- Subject: Documents Verification for October 2018
- Subject: Application for return for November
- Subject: Check the environment
- Subject: Sending on last week
- Subject: The package of documents for payment 1st October
- Subject: Payment Verification

🜍 Сверка на проверку - Mozilla Thunderbird			_		$\times$
From Полина Логинова <bts@stresyrs.ru> 😭</bts@stresyrs.ru>	<b>5</b> Reply	" Reply All 🗸	*	Forward	More 🗸
Subject Сверка на проверку		Date Mon	n, 24 S	Sep 2018	07:17 UTC
Reply to Полина Логинова <drozdov4mari@yandex.ru></drozdov4mari@yandex.ru>	☆				
Задолженность 5662.13 рублей. Высылаю вам наши документы от сегодня Надо всё проверить и дать ответ до после	шнего чис завтра.	сла.			
🗸 🕖 1 attachment: Сверка на оплату.zip 223 КВ				t	Save 🗸
🚹 Сверка на оплату.zip 223 КВ					
		Сверка на оплату.zip			рог Рог Сверка на оплату.ехе

Figure 2: Example of Redaman malspam from September 2018.

Весь пакет док-ов за прошлый месяц - Mozilla Thun	derbird		_		×
From Елизавета Кудрявцева <rogoza@fluniv.ru> 🟠</rogoza@fluniv.ru>	<b>5</b> Reply	🏀 Reply All	~ ~	Forward	More 🗸
Subject Весь пакет док-ов за прошлый месяц		Date N	Mon, 15	Oct 2018	16:02 UTC
Reply to Елизавета Кудрявцева <sv3tlan4s@yandex.ru></sv3tlan4s@yandex.ru>					
Добрый день. Перечень документов в приложении. Все док-ты требуется заверить: подпись+п Для того чтобы не заверять каждый лист р документов. Так же надо подписать расчёт и поставить	ечать+ко аздельно печать и	пия верна. предлагаю направить	сдела в скан	ть скле е.	ейку
\vee 🔋 1 attachment: Весь пакет документов за сентябрь	<b>.7z</b> 205 KB				Save 🗸
Весь пакет документов за сентябрь.7z 205 КВ					
		Весь пакет документов за	_	Век	РОГ сь пакет ументов за

Figure 3: Example of Redaman malspam from October 2018.



Figure 4: Example of Redaman malspam from November 2018.



Figure 5: Example of Redaman malspam from December 2018.

## **Targeted recipients**

The content of these emails and data from our <u>AutoFocus</u> threat intelligence platform confirms this campaign is primarily targeting Russian recipients. We found 3,845 email sessions in AutoFocus with attachments tagged as Redaman banking malware from September through December 2018. Data on the top 10 senders and recipients of this malspam follow:

Mail servers of the top 10 senders:

- From Russia 3,456
- From Belarus 98
- From Ukraine 93
- From Estonia 29
- From Germany 30
- From United States 21
- From Netherlands 12
- From Great Britain 7
- From Switzerland 7

• From Latvia - 2

Mail servers of the top 10 recipients:

- To Russia 2,894
- To Netherlands 195
- To United States 55
- To Sweden 24
- To Japan 16
- To Kazakhstan 12
- To Spain 12
- To Finland 11
- To Germany 6
- To Austria 4



Figure 6: AutoFocus map visualization for distribution of email recipients, September through December of 2018.

## Analysis of a Redaman sample

We analyzed a sample of Redaman malware from malspam on November 13th, 2018.

SHA256 hash of rar archive from the malspam:

f6fb51809caec2be6164863b5773a7ee3ea13a449701a1f678f0655b6e8720df

SHA256 hash of Redaman executable extracted from the rar archive:

cd961e81366c8d9756799ec8df14edaac5e3ae4432c3dbf8e3dd390e90c3e22f

SHA256 hash of Redaman DLL created by the above executable:

14d33b02a497e46f470d30180a09a1057c6802c1f37b0efbf82cbdc47a8ae7ff

When the Windows executable for Redaman is first run, it checks for the following files or directories on the local host (C:\ or D:\ drives):

- C:\cuckoo
- C:\fake\_drive
- C:\perl
- C:\strawberry
- C:\targets.xls
- C:\tsl
- C:\wget.exe
- C:\\*python\*

If any of the above files or directories exist, the Windows executable throws an exception and exits. This indicates Redaman checks if it is running in a sandbox or similar type of analysis environment.

If no exceptions occur, the Windows executable drops a DLL file in the user's *AppData\Local\Temp\* directory, creates a randomly-named folder under *C:\ProgramData\* directory and moves the DLL under that folder as a random file name. This Redaman DLL is made persistent through a scheduled Windows task with the following properties:

- Name: Windows Update
- Description: Updating Windows components.
- Triggers: Executed whenever the user logs on
- Action: rundll32.exe "C:\ProgramData\%random value%\%random value.random 3character extension%",DIIGetClassObject host

After creating a scheduled task and causing the DLL to load, the initial Redaman executable file deletes itself.

📕   🛃 📕 🗕   abgl	knpaf						×	
File Home	Share View						~ ?	
← → • ↑ ▲ >	This PC > Local Disk	: (C:) > Pro	ogramData > ab	gknpaf	v ت	Search ab	g 🔎	
Name	^	Туре	9	Size				
doldfbkb.cjb		CJB	File	208 KB				
Task Scheduler						_		×
File Action View Hel	р							
🗢 🔿 🖄 📅 🛛 🖬								
	1							
Task Scheduler (Local)	Name	Status	Triggers			Author	_	
<ul> <li>Task Scheduler (Local)</li> <li>Task Scheduler Lib</li> </ul>	Name Windows Update	Status Running	Triggers At log on of			Author Microsoft	t Corporat	ion
<ul> <li>Task Scheduler (Local)</li> <li>Task Scheduler Lib</li> </ul>	Name () Windows Update	Status Running	Triggers At log on of			Author Microsoft	t Corporat	ion
<ul> <li>Task Scheduler (Local)</li> <li>Task Scheduler Lib</li> </ul>	Name Windows Update General Triggers A	Status Running Actions Co	Triggers At log on of onditions Settin	igs History (dis	abled)	Author Microsoft	t Corporat	ion
<ul> <li>Task Scheduler (Local)</li> <li>Task Scheduler Lib</li> </ul>	Name Windows Update General Triggers A Action	Status Running actions Ca Details	Triggers At log on of onditions Settin	igs History (dis	abled)	Author Microsoft	t Corporat	ion
Task Scheduler (Local)	Name Windows Update General Triggers A Action Start a program	Status Running Actions Ca Details rundll32.es	Triggers At log on of onditions Settin xe "C:\ProgramDat	igs History (dis a\abgknpaf\dol	abled) dfbkb.cjb",D	Author Microsoft	t Corporat	ion ^
Task Scheduler (Local) Task Scheduler Lib	Name Mindows Update General Triggers A Action Start a program	Status Running Actions Co Details rundll32.ex	Triggers At log on of onditions Settin xe "C:\ProgramDat	ngs History (dis a\abgknpaf\dol	abled) dfbkb.cjb",D	Author Microsoft	t Corporat	ion t v

Figure 7: Example of a Redaman DLL persistent through a scheduled task.

Process Hacker [		]					_			$\times$
Hacker View Tools Users He	р									
🔁 Refresh 💮 Options 🛛 👪 Fin	d hand	lles or DLLs 💈	System	information		Search	Processe	es (Ctrl+K	()	Q
Processes Services Network Disl	ĸ	_		1					,	
Name	PIC	rundll32.	exe (3888)	Properties			_		$\times$	~
> 💽 System Idle Process	C		-	•		0.01		-		
Registry	88	Memory	Env	ironment	Handles	GPU	J	Comme	nt	-
Csrss.exe	408	General	Statistics	s Perform	ance I	nreads	Token	Mout	lles	
✓ ■ wininit.exe	484	Name		Base address	Size	Description			~	
✓ ■ services.exe	584	IPHLPAPI.	DLL	0x73a20000	192 kB	IP Helper	API			
	731	kernel.app	core.dll	0x76fd0000	60 kB	AppModel	API Host			
	011	kernel32.d	II	0x77080000	896 kB	Windows N	NT BASE A	API Client.		
Svchost.exe	012	kernel32.d	ll.mui	0x6220000	952 kB	Windows N	NT BASE A	API Client.		
svchost.exe	864	KernelBase	.dll	0x773f0000	1.89 MB	Windows N	NT BASE A	API Client.		
svchost.exe	904	kkbhicmp.	dmj	0x400000	416 kB					
svchost.exe	364			0x2f20000	788 KB	Multiple Dr	outdor Do	uter DU		
🔳 svchost.exe	656	msasn1 dll		0x756460000	90 KD 56 kB	ASN 1 Run	ovider Ro			
svchost.exe	85.6	msctf.dll		0x740f0000	1.26 MB	MSCTE Ser	ver DLL	•		
✓ ■ svchost.exe	476	mskeyprot	ect.dll	0x73400000	64 kB	Microsoft k	Key Protec	tion Provi		
■ taskhostw.exe	2716	msvcp_wir	n.dll	0x74070000	500 kB	Microsoft®	) C Runtin	ne Library		
✓ 🗋 rundll32 exe	5224	msvcrt.dll		0x75f10000	764 kB	Windows N	NT CRT D	LL		
	3880	mswsock.c	111	0x73580000	344 kB	Microsoft V	Vindows S	Sockets 2.		
	1100	mswsock.c	lll.mui	0x5330000	12 kB	Microsoft V	Vindows S	Sockets 2.		
svcnost.exe	1100	NapiNSP.d	II	0x73190000	68 kB	E-mail Nan	ning Shim	Provider		
svchost.exe	1112	ncrypt.dll		0x733e0000	124 kB	Windows N	Crypt Ro	uter		
Image: Svchost.exe	1184	ncryptsslp.		0x73390000	108 kB	Microsoft S		Provider	5	1
svchost.exe	<	netutils dll		000000000000000000000000000000000000000	70 KB	wet win32	API DLL		Ŧ	
CPU Usage: 27.97% Physical me	mory:	netutis.uli						/		
	_							Clos	se .	

Figure 8: Process Hacker showing the Redaman DLL active using rundll32.exe.

Redaman uses an application-defined hook procedure to monitor browser activity, specifically Chrome, Firefox, and Internet Explorer. It then searches the local host for information related to the financial sector. Other capabilities of Redaman include:

- Downloading files to the infected host
- Keylogging activity
- Capture screen shots and record video of the Windows desktop
- Collecting and exfiltrating financial data, specifically targeting Russian banks
- Smart card monitoring
- Shutting down the infected host
- Altering DNS configuration through the Windows host file
- Retrieving clipboard data
- Terminating running processes
- Adding certificates to the Windows store

## Infection traffic

We generated the following infection traffic using the executable with SHA256 hash cd961e81366c8d9756799ec8df14edaac5e3ae4432c3dbf8e3dd390e90c3e22f on November 14th, 2018:

- 104.28.16[.]33 port 443 namecha[.]in GET /name/d/stat-counter-3-1
- 185.141.61[.]246 port 80 185.141.61[.]246 POST /index.php
- 193.37.213[.]28 port 80 193.37.213[.]28 POST /p/g\_3453456jawd346.php

	🎗 🙆 🍳 👄 🔿	😫 T	§ 🕭 📃 🗏 🔍	ର୍ ବ୍ 🏢	
http.request or ssl.handsh	ake.type == 1				Expression +
Time	Dst	port	Host	Server Name	Info
2018-11-14 18:39	104.28.16.33	443		namecha.in	Client Hello
2018-11-14 18:39	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:39	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:40	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:40	193.37.213.28	80	193.37.213.28		POST /p/g_3453456jawd346.php HTTP/1.0
2018-11-14 18:40	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:40	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:44	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:49	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:50	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:54	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 18:59	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 19:04	185.141.61.246	80	185.141.61.246		POST /index.php HTTP/1.1 (application
2018-11-14 19.09	185 141 61 246	80	185 141 61 246		POST /index nhn HTTP/1 1 (annlication >

Figure 9: Redaman infection traffic filtered in Wireshark.

Network activity started with an HTTPS URL to *namecha[.]in*, which is an alternative namecoin block explorer. <u>Namecoin</u> is a cryptocurrency system that can be used for decentralized DNS. That proves to be the case here, since the URL returned an IP address used for subsequent post-infection traffic as shown in Figure 10.

- → C ☆ 🔒 https://na	mecha.in/nam	e/d/stat-counter-3-1	l				@ ☆
Namecoin Block Ex	plorer				Contact	Search	Go
Name d/sta	it-coui	nter-3-1	(stat-co	unter-3	3-1.bit)	IP address used for	of server Redaman
Summary				Current v	alue		C2 traffic
Status	Active			{			
Expires after block	456955 (23	683 blocks to go)		"ip"	185.141.61.246	5"	
Last update	2018-10-10	22:47:39 (block 4	<u>20955</u> )	1			
Registered since	2018-09-22	01:25:11 (block 4	<u>18190</u> )	}			
Operations							
Date/time	Block	Transaction	Operation		Value		
2018-10-10 22:47:39	<u>420955</u>	11bef57297	OP_NAME_UP	DATE	{"ip":["185.141.6	1.246"]}	
2018-09-22 01:25:11	<u>418190</u>	e206cc4573	OP_NAME_FIR	STUPDATE	{"ip":["94.156.18	9.28"]}	
2018-09-21 21:05:06	<u>418165</u>	<u>51a4f3c2a1</u>	OP_NAME_NE	N	c268672c99a11	7056b5953715e1aef39c	b65f532

Figure 10: Data returned from **namecha[.]in** used for subsequent infection traffic.

During the infection, callback traffic was periodically sent to a command and control (C2) sever at 185.141.61[.]246. Shortly after the infection, return traffic from the C2 server sent a Pony variant DLL to the infected Windows client.

POST /index.php HTTP/1.1 Cache-Control: no-cache Connection: Close Pragma: no-cache Content-Type: application/x-www-form Accept: text/html, application/xhtml	n-urlen l+xml,	coded */*	^	58 k re	B of encode turned from server is a varia	ed data the C2 a Pony nt DLL
Accept-Language: en-US Content-Length: 79	Wires	hark · Export · HT	TP object list			x c
Host: 185.141.61.246	Packet	Hostname	Content Type	Size	Filmame	^
4.E{.W.HfJ%.4=Ia.	37	185.141.61.246	application/x-www-form-urlencoded	39 bytes	i dex.php	
RD/Du(PK6H.9.oKTQHTTP/1.1 Server: nginx	40	185.141.61.246	application/octet-stream	9 bytes	ndex.php	
Date: Wed, 14 Nov 2018 18:40:22 GMT	49 52	185.141.61.246	application/x-www-form-urlencoded application/octet-stream	125 byte 9 bytes	index.php index.php	
Content-Type: application/octet-stn Transfer-Encoding: chunked	63	185.141.61.246	application/x-www-form-urlencoded	79 by	index.php	
Connection: close	189	185.141.61.246	application/octet-stream	58 kB	index.php	
X-Powered-By: PHP/5.5.38-1~dotdeb+	200	193.37.213.28	text/html	20 bytes	g_3453456jawd346	i.php
Content-Transfer-Encoding: binary	210	185.141.61.246	application/x-www-form-urlencoded	43 bytes	index.php	
Last-Modified: Fri, 01 Jan 1990 0:	216	185.141.61.246	application/x-www-form-urlencoded	125 bytes	index.php	
Expires: Fri, 01 Jan 1990 00:07:00	219	185.141.61.246	application/octet-stream	9 bytes	index.php	
Cache-control: must-revalidate, no-	223	185.141.61.246	application/octet-stream	9 bytes	index.php	
Pragma: no-cache	233	185.141.61.246	application/x-www-form-urlencoded	39 bytes	index.php	
i ruginar no cache	236	185.141.61.246	application/octet-stream	9 bytes	index.php	
.c.e}.e!.3%r."h@~f>%	245	185.141.61.246	application/x-www-form-urlencoded	89 bytes	index.php	
.f,.Y.y&.RiTz.B	248	185.141.61.246	application/octet-stream	9 bytes	index.php	
1 client pkt(s), 1 server pkt(s), 1 turn(s).	257	185.141.61.246	application/x-www-form-urlencoded	355 bytes	index.php	
Entire conversation (59 kB)	260	185 1/1 61 2/6	application/octot-stream	Q butoc Save All	Close	Help
Find:			Jave	Save All	CIOSE	help

Figure 11: Using Wireshark to find 58 kB of encoded data returned from the C2 server at 185.141.61[.]246.

Data for the Pony variant DLL was XOR encoded with multiple XOR keys and <u>RTLcompressed</u>. The SHA256 of this Pony variant DLL is b4701d95219d465e978c4a815fcce89787916da33ae2a49d0e76d4445fd39ada, and it generated traffic to **193.37.213[.]28/p/g\_3453456jawd346.php** during the infection.

## Conclusion

Since it was first noted in 2015, this family of banking malware continues targeting recipients who conduct transactions with Russian financial institutions. We found over 100 examples of malspam during the last four months of 2018, and this blog provides a closer look at Redaman during that timeframe. We covered the following areas:

- Infection vector
- Email characteristics
- Targeted recipients
- Analysis of a Redaman sample
- Infection traffic

We expect to discover new Redaman samples as 2019 progresses.

Palo Alto Networks customers are protected from this threat. Traps identifies these files through Local Analysis and Wildfire has classified them as malicious. Our threat prevention platform detects this malware, and see the below appendices below for details on Redaman malware we discovered from September through December of 2018.

## Appendix A

SHA256 file hashes for 119 malspam attachments, 30 extracted Redaman executable files, and 30 dropped Redaman DLL files found from September through December 2018. Information is available at: <u>https://github.com/pan-</u>

unit42/iocs/blob/master/Redaman\_banking\_malware/2018-09-thru-2018-12-file-hashes-for-Redaman-banking-malware.txt

## Appendix B

SHA256 file hashes, archive file names, and extracted file names for Redaman banking malware found in September 2018. Information is available at: <u>https://github.com/pan-unit42/iocs/blob/master/Redaman\_banking\_malware/2018-09-file-hashes-for-Redaman\_banking-malware.txt</u>

## Appendix C

SHA256 file hashes, archive file names, and extracted file names for Redaman banking malware found in October 2018. Information is available at: <u>https://github.com/pan-unit42/iocs/blob/master/Redaman\_banking\_malware/2018-10-file-hashes-for-Redaman\_banking-malware.txt</u>

#### Appendix D

SHA256 file hashes, archive file names, and extracted file names for Redaman banking malware found in November 2018. Information is available at: <u>https://github.com/pan-unit42/iocs/blob/master/Redaman\_banking\_malware/2018-11-file-hashes-for-Redaman\_banking-malware.txt</u>

#### Appendix E

SHA256 file hashes, archive file names, and extracted file names for Redaman banking malware found in December 2018. Information is available at: <u>https://github.com/pan-unit42/iocs/blob/master/Redaman\_banking\_malware/2018-12-file-hashes-for-Redaman\_banking-malware.txt</u>

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our <u>Terms of Use</u> and acknowledge our <u>Privacy</u> <u>Statement</u>.