1. Analysis of the malicious document files

The malicious document is a .docx file, which contains a password-protected macro. After extracting the macro from this file, we analyzed the code which is responsible for downloading the malicious file from below mentioned URL.

hxxp://vas???oiblog.sp??e/up?ate/KB25421.exe

The macro also contained a code to install a backdoor with the help of putty.exe. This executable is downloaded by the malware from the below mentioned URL.

http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

The downloaded file is a malware downloader in itself. It communicates with its linked command and control (C&C) server and downloads the Cryptowall malware into the victim's system. The C&C server contains pages which stores the victim's browser's and email password.

2. Process Execution Flow

Figure 2 displays the process execution flow of the malware.

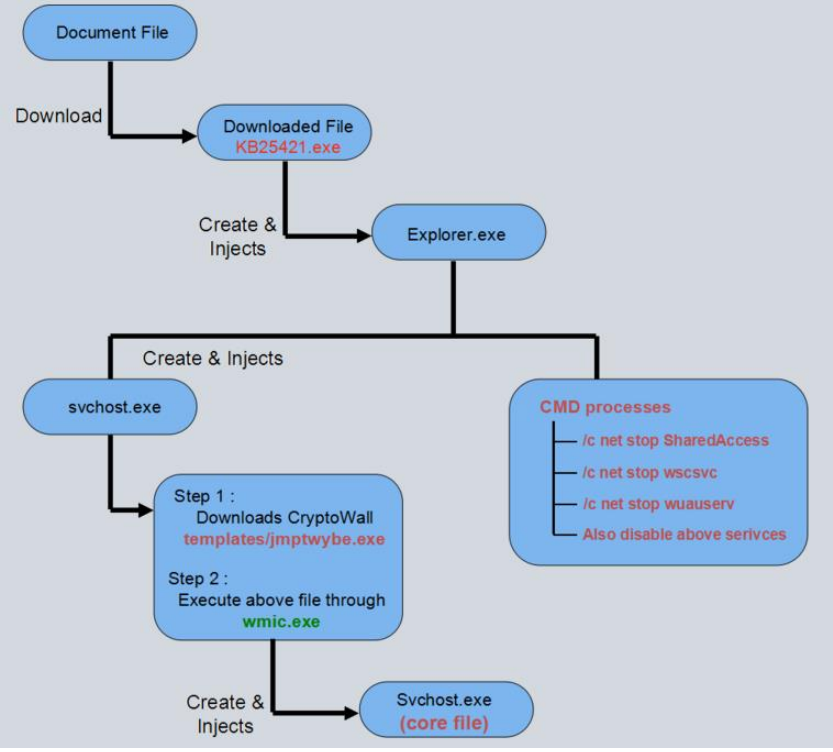


Figure 1

2.1 Explanation of the CMD Processes:

cmd.exe /c net stop wscsvc
The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include firewall (ON/ OFF), Anti-virus (ON/ OFF/ Out-of-date), antispyware (ON/ OFF/ Out-of-date), Windows Update (Automatically/ Manually Download and Install Updates), User Account Control (ON/ OFF), and Internet settings (Recommended/ Not recommended).

cmd.exe /c net stop wuauserv
Stops the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.

cmd.exe /c net stop SharedAccess
Stops network address translation, addressing, name resolution and/ or intrusion prevention services for a home or small office network. It also disables the above stopped services so that security services will not start on reboot.

cmd.exe /c sc config wscsvc start = disabled
cmd.exe /c sc config wuauserv start = disabled
cmd.exe /c sc config SharedAccess start = disabled

Use of wmic.exe

The malware uses WMI (Windows Management Instrumentation) framework commands to run the downloaded malware.

Parameters used with wmic.exe to execute process is shown below.

“wmic.exe process call create {Absolute file path to be Executed}”

3. Campaign Information

The analyzed sample belongs to **crypt5022** campaign id. Below is the information structure the malware sends to its C&C before encrypting the files.

{1|crypt5022|332A59BEE27BFE8B4A7D721CC3A0B3DB|2|1|2|}

Description	Value
Command	1
Campaign Code	crypt5022
Victim Unique MD5 Key	332A59BEE27BFE8B4A7D721CC3A0B3DB
Operating System Version	2
CPU Architecture	1
User Privileges	2

Figure 2

3.1 C&C Panel Information

After penetrating the C&C server, we extracted some interesting internal information regarding the malware and its database structure. Below are some snapshots of the extracted info from the C&C panel.

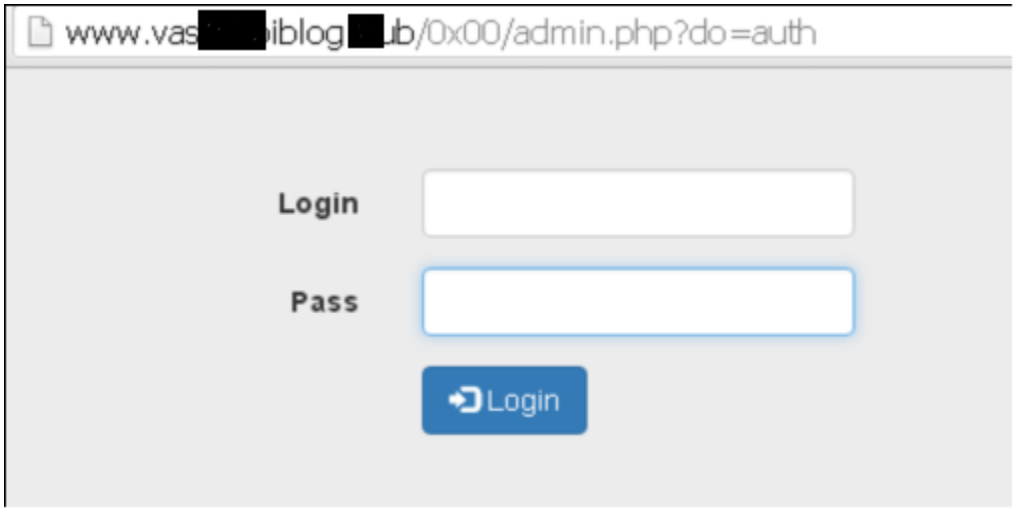


Figure 3. Admin Login Panel

The C&C server has two directory structure on its root. As one of the directory names is prefixed with 'old_', so we can assume that the malware author might have updated the panel or it might be a testing directory. The malware communicates with pages hosted in '0x00' directory.

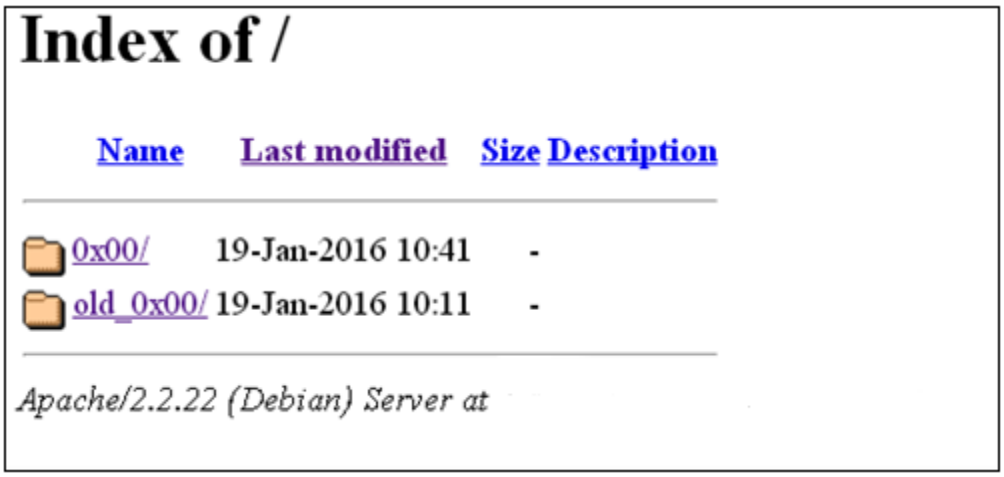


Figure 4. Directory structure at C&C Server

In the '/0x00/uploads' directory, there are some executables hosted by the server. These executables have a '.dat' extension.

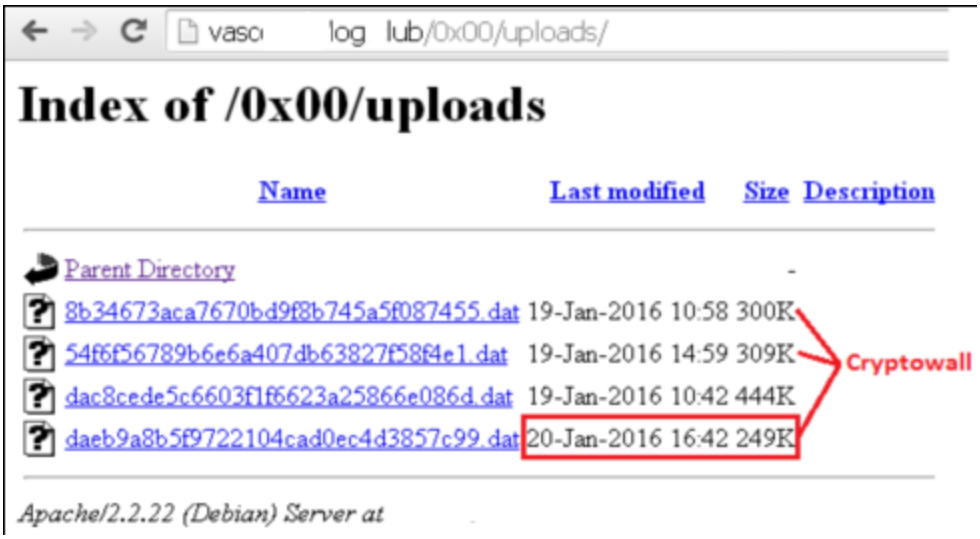


Figure 5. Uploaded malware

The below table describes the files present on the server. The malware installed a backdoor on the infected machine with the help of a Putty application.

Files Found On Server	File Description
8b34673aca7670bd9f8b745a5f087455.dat	Cryptowall Ransomware
54f6f56789b6e6a407db63827f58f4e1.dat	Cryptowall Ransomware

dac8cede5c6603f1f6623a25866e086d.dat	Putty Genuine application
daeb9a8b5f9722104cad0ec4d3857c99.dat	Cryptowall Ransomware

Figure 6. Server File Description

The C&C panel also hosts the installed page of the malware. The installation panel is used by admin to modify existing settings of database tables.

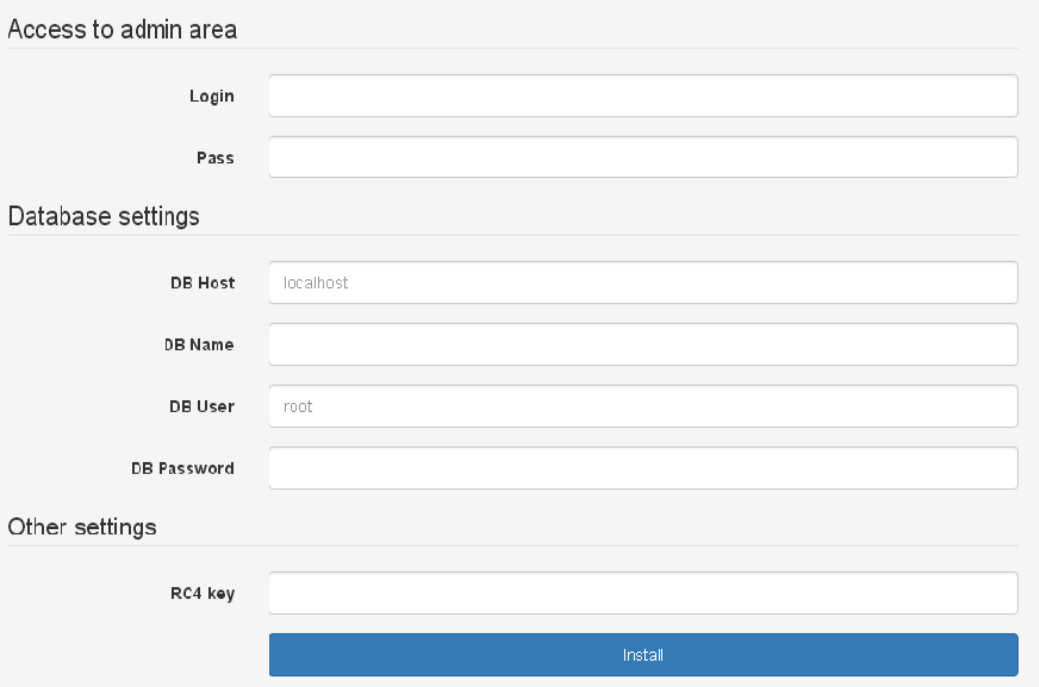
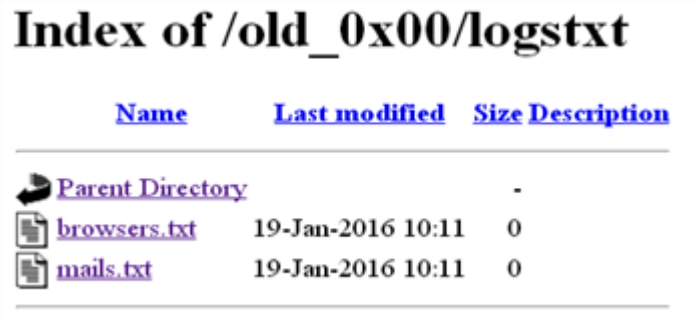


Figure 7. C&C Installation Panel

The C&C server hosts Install directory at '/0x00/install' path. It gives some interesting information about php version used, other supported extensions to mysql and installed (supported) extensions to hosted server.

'/old_0x00/logstxt/' and '/0x00/logstxt/' directory on the C&C server have two files.

1) Browsers.txt: Contains user name, passwords stored in browser on infected machine.
2) Mails.txt: Contains user name and passwords of mail accounts.



Index of /old_0x00/logstxt

Name	Last modified	Size	Description
Parent Directory		-	
browsers.txt	19-Jan-2016 10:11	0	
mails.txt	19-Jan-2016 10:11	0	

Figure 8. Log folder

We also managed to extract some dump files from the server. It contains database, table structure, and local database login information. Below are the snapshots of the dump files.

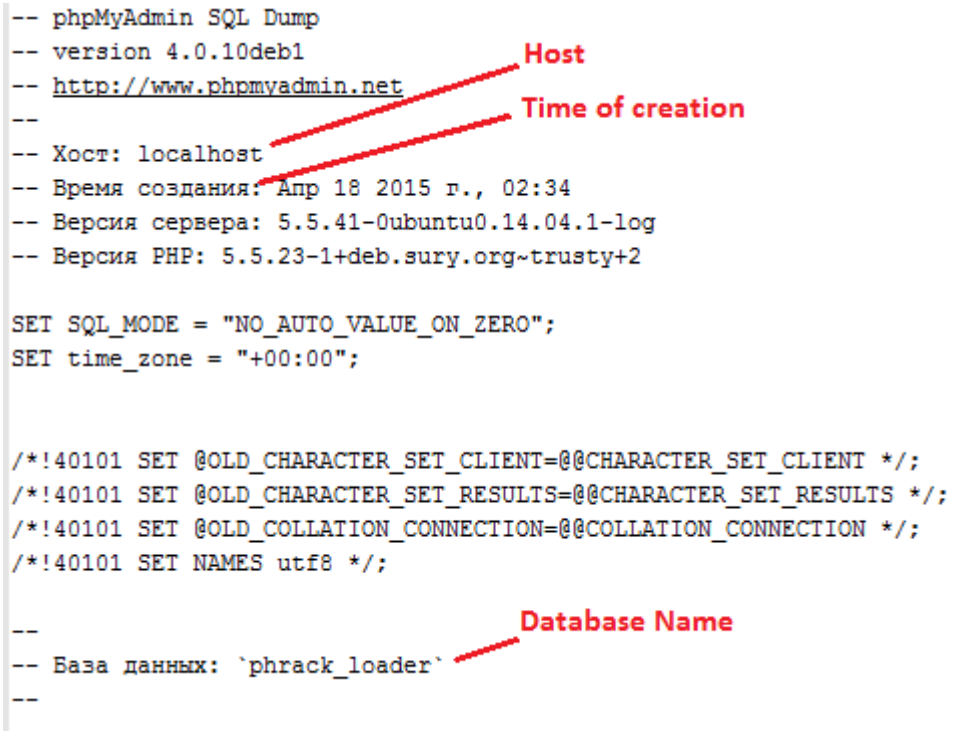


Figure 9. Dump file (Database and host info)

```
-- Структура таблицы `bots`

CREATE TABLE IF NOT EXISTS `bots` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `guid` varchar(16) NOT NULL,
  `ip` varchar(15) NOT NULL,
  `country` varchar(2) DEFAULT NULL,
  `bits` int(11) NOT NULL DEFAULT '32',
  `pl` tinyint(1) NOT NULL,
  `os` int(11) NOT NULL,
  `created_at` datetime NOT NULL,
  `last_visit_at` datetime NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `guid` (`guid`),
  KEY `country` (`country`,`bits`,`pl`,`os`),
  KEY `last_visit_at` (`last_visit_at`)
) ENGINE=InnoDB  DEFAULT CHARSET=utf8 AUTO_INCREMENT=54 ;
```

```
CREATE TABLE IF NOT EXISTS `tasks` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(15) NOT NULL,
  `type` enum('local','remote') NOT NULL DEFAULT 'local',
  `pl` tinyint(1) DEFAULT NULL,
  `countries` varchar(2048) NOT NULL,
  `countries_inverse` tinyint(1) NOT NULL,
  `local_file` varchar(255) DEFAULT NULL,
  `remote_file` varchar(512) DEFAULT NULL,
  `limit` int(11) NOT NULL,
  `load` int(11) NOT NULL,
  `exec` int(11) NOT NULL,
  `update_remote_fraq` int(11) DEFAULT NULL,
  `last_update_remote_at` datetime NOT NULL,
  `created_at` datetime NOT NULL,
  `status` tinyint(1) NOT NULL DEFAULT '1',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=utf8 AUTO_INCREMENT=6 ;
```

Figure 10. Dump file (Database tables bots, tasks)

```
--
-- Структура таблицы `tasks_bots`
--

CREATE TABLE IF NOT EXISTS `tasks_bots` (
  `task_id` int(11) NOT NULL,
  `bot_guid` varchar(16) NOT NULL,
  `exec` tinyint(1) NOT NULL DEFAULT '0',
  KEY `bot_guid` (`bot_guid`),
  KEY `task_id` (`task_id`,`exec`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------
```

```
-- Структура таблицы `task_logs`
--

CREATE TABLE IF NOT EXISTS `task_logs` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `log` varchar(512) NOT NULL,
  `task_id` int(11) NOT NULL,
  `error` tinyint(4) NOT NULL DEFAULT '0',
  `created_at` datetime NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB  DEFAULT CHARSET=utf8 AUTO_INCREMENT=12 ;
```

Figure 11. Dump file (Database tables tasks_bots, task_logs)

4) List of Compromised Websites

The malware uses RC4 and then Rtl decompression to decode server names. From those we found a list of the following compromised server names. It has 52 unique host names.

C&C Server: www.vas???oi?log.??b

IP Address: 85.??.31.1?:80
Location: Germany

C&C server is used to download CryptoWall and to send the victim's information, browser and email credentials. These sites are used to send and receive encryption-related information.

soh?lari.net/GnOLXh.php	zuiy??gou.com/Pfy2Qs.php	ecoin??.kz/LUoMqa.php
lpt??h.sk/g3lfoj.php	si???op.pl/Si0cCJ.php	tbra??le.com.br/XAT7zH.php
asia??ster.kz/vUn1wz.php	rai??china.com/NSrcQE.php	derm??ightcr.com/tHja9Z.php
euro??rtners.it/Dd6VPR.php	balust??dydrewniane.pl/Fcb7VZ.php	dor??bociort.ro/6sZTLc.php
highcl??escorts4u.com/Snuxg7.php	golcu??ehberi.com/6JQEva.php	ahtub??ishing.com/CXjq48.php
fun??ne-veza.sk/Owm50c.php	ask-??-anything.tk/PsdO76.php	ot??itka.com.ua/tjhW2B.php
all??-music.nl/yBDEMc.php	arcti??ear.net/MRGKAC.php	anily??dirim.net/zn9mur.php
maxi??rga.co/L8HU29.php	gios??sa.com/Zoe2aN.php	bud??.info/zYNKoq.php
fiyas??birlik.com/UxAK5e.php	gr??rio.com.br/4A0Hw5.php	lazy??anch.us/PtAg1I.php
inicc.yuc??an.gob.mx/UIagAy.php	oferta??lampago.com.br/4jiPBG.php	ggvidro??utomotivos.com.br/KMYz1s.php
maste??rade.tk/12fDze.php	vlado??verka.sk/6RGZgC.php	otk??tka.com.ua/MVc9hg.php
zha??n.kz/TSOXQLphp	mehme??kinci.biz/Hg3V8b.php	apa??ment.od.ua/I35pl6.php
centr??escorts4u.com/XqVFBm.php	e-mi??nat.ro/ZeNpML.php	wi??ka.com.br/SGJ_Fr.php
eco??ty.kz/7_9SR6.php	tu??y.com.tr/prkdzF.php	sowe??ness.be/fYvA5U.php
diner???perto.pe/zOesbw.php	arii??ouse.nl/iMVfC4.php	sow???ness.be/isB2Ac.php
alle???rts4u.com/dfgOwA.php	quadp??ticle.com/fZ1Y8M.php	time??dedon.com/CBRrYv.php
ron??agp.ir/U_ABoi.php	kad??7.pl/fFe_xr.php	love??z/yMZFGp.php
very???loan.com/1vR9hu.php		

Figure 12

Analyzed Files

File Name	MD5	Detected As
KB25421.exe	713D6FC7A9FA3360D990B8F8122BE59D	Trojan.Bulta.RF5
<Randomname.exe>	39D64CEC07655CD5EADC44AB4BA8AC73	Trojan.Bulta.RF5
<Randomname.exe>	068A6BC35D89EDD9FCBC4163B9800151	Trojan.Agen.r4
<Randomname.exe>	CF03E53EBCE9251E469414AB76BF5206	TrojanRansom.Crowti.r4

END