Technical Details of malicious attachment

File Name: SHIPMENT_ARRIVAL.doc

MD5: 4B2388DA552BDE61EBC3C634BE4B8B1E

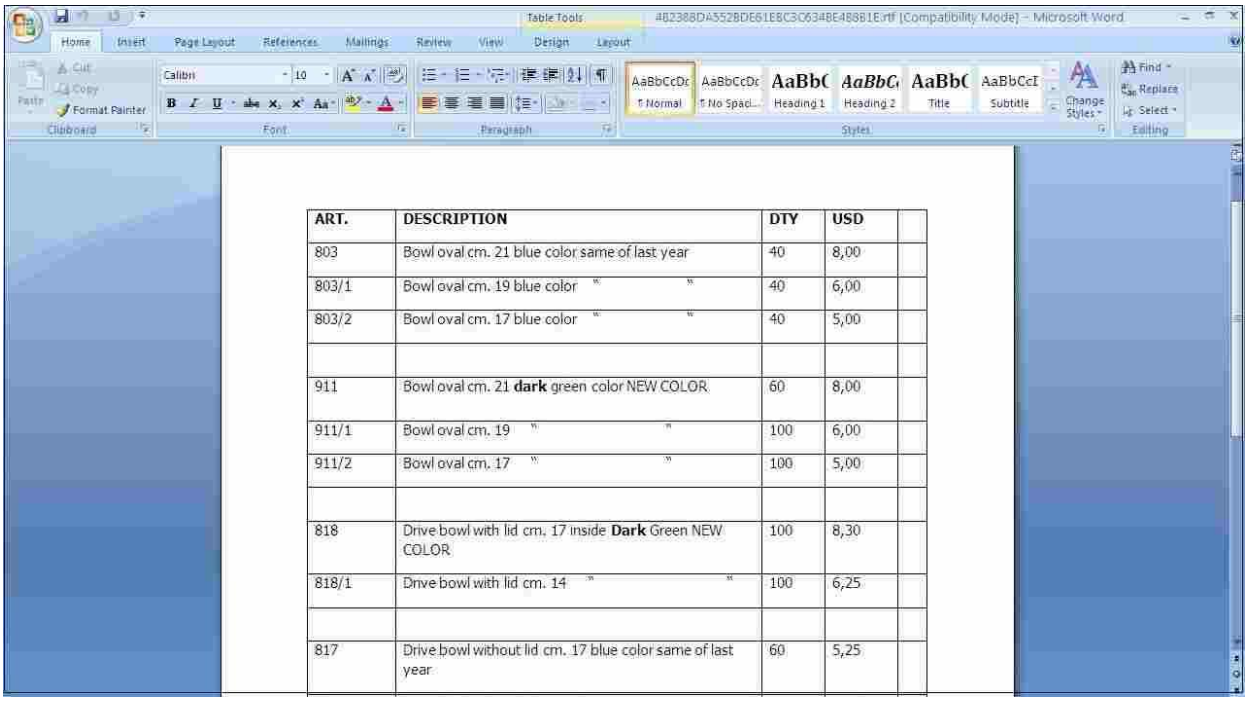
File Size: 714KB

Quick-Heal detection name: CVE-RTF-2012-0158

The RTF file drops the following executable:

C:\Documents and Settings\User\Local Settings\svchost.exe

The dropped file gets executed and displays a decoy as shown below:



ART.	DESCRIPTION	DTY	USD	
803	Bowl oval cm. 21 blue color same of last year	40	8,00	
803/1	Bowl oval cm. 19 blue color " "	40	6,00	
803/2	Bowl oval cm. 17 blue color " "	40	5,00	
911	Bowl oval cm. 21 **dark** green color NEW COLOR	60	8,00	
911/1	Bowl oval cm. 19 " "	100	6,00	
911/2	Bowl oval cm. 17 " "	100	5,00	
818	Drive bowl with lid cm. 17 inside **Dark** Green NEW COLOR	100	8,30	
818/1	Drive bowl with lid cm. 14 " "	100	6,25	
817	Drive bowl without lid cm. 17 blue color same of last year	60	5,25	

The dropped component is an infostealer made from either iSpy, Predator or Knight RAT tool.

Analysis of the infostealer component
The infostealer component can carry out the following malicious activities:

1. Keylogging
2. Capturing screenshots
3. Stealing passwords
4. Capturing video
5. Collecting system information

Further analysis shows that the malware is using AES decryption algorithm for decrypting the strings present in its binary code. It sends the stolen information to the email address kept in binary in an encrypted format.

The malware uses the following email addresses:

Kay.boy@yandex.com
Austinfred@yandex.com
Keylogger79@gmail.com

The admin panel used for the campaign, shows that the malware authors are using three different loggers.

Comparison of information stolen by each of the keylogger:

Information Type	iSpy	Predator	Knight
System Information	• Username • Windows Version • Installed Language • Installed .NET Framework • System Privileges • Default Browser • Installed Anti-Virus • Installed Firewall • Internal IP • External IP	• Local Date and Time • Installed Language • Operating System • Internal IP Address • External IP Address • Installed Anti-Virus • Installed Firewall	• Username • IP Address • Windows Version • UI Language • Installed Anti-Virus • Installed Applications • Application Publisher
Credentials of Email Clients	• Email Client's Name • Display Name • Email Address • Server • Port • Username • Password • SMTP Server • SMTP Port	• Email Client Name • Server • Server Port • Secured • Type • Username • Password • Profile • Password Strength • SMTP Server	• Application • Host • Username • Password

		• SMTP Server Port	
Web Browser Cached Credentials	• Browser Name • Website• Username • Password	• Browser Name • Website • Username • Password • Password strength	• Browser Name • Website • Username • Password
Microsoft Office Operating System AutoCAD	• Product ID • Product Name • License Key • Installation Path		

Ways of sending stolen data
The detected keyloggers use the following methods for sending the stolen information.

1. **Using SMTP**: Sends stolen data to mail by using SMTP server on port 587
2. **FTP upload**: Uploads file to FTP server.
3. **Web Request/PHP**: Sends data as web requests to web servers.

Each keylogger sends stolen information to a predetermined email in the following format

Keylogger	First Run	Data Stolen
Predator	Predator Pain v13 - Server Ran - [ComputerName]	Predator Pain v13 | Stealer Log - [ComputerName]
Knight Logger	FIRST RUN Knight Logger first run Username@ComputerName	[ACCOUNT] Knight Logger of [Username]@[ComputerName]

iSpy	iSpy Keylogger - Notification - ComputerName\UserName	iSpy Keylogger - WebCam- ComputerName\UserName iSpy Keylogger - Screenshot - ComputerName\UserName iSpy Keylogger - Password Recovery - ComputerName\UserName iSpy Keylogger - Clipboard - KeyStroke - ComputerName\UserName

Activity of iSpy logger
iSpy Logger, when executed, disables Command Prompt, Task Manager and Registry Editor by setting values of the following registry keys:
Software\\Policies\\Microsoft\\Windows\\System-
"DisableCMD" = 1
"DisableTaskMgr" = 1
"DisableRegistryTools" = 1

Preventing antivirus programs process from working
To evade detection by antivirus programs, the malware disables their processes by using debugger settings in the registry:

"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\[**ProcessName**]\Debugger"

iSpy sets this value to "rundll32.exe"

ProcessName is from the below list:

rstrui.exe	AvastSvc.exe	avconfig.exe	AvastUI.exe
instup.exe	mbam.exe	mbamgui.exe	mbampt.exe
mbamservice.exe	hijackthis.exe	spybotsd.exe	ccuac.exe
avguard.exe	avgnt.exe	avgui.exe	avgcsrvx.exe
avgrsx.exe	avgwdsvc.exe	egui.exe	zlclient.exe
keyscrambler.exe	avp.exe	wireshark.exe	ComboFix.exe
MpCmdRun.exe	msseces.exe	MsMpEng.exe	avscan.exe
mbamscheduler.exe	avcenter.exe	avgidsagent.exe	bdagent.exe

Communication via email

Screenshot Capturing

iSpy takes screenshots of the victim's desktop and uploads it to the web server hxxp://sm.uploads.im/[Filename.png]. This link is sent as an email with the following subject line:
"iSpy Keylogger - Screenshot - ComputerName\UserName"

Video Capturing

iSpy captures videos using web cam and uploads them to video hosting sites and sends path of the file via email with following subject line:
"iSpy Keylogger - WebCam- ComputerName\UserName"

Detection Reports

File Name	MD5	**Quick Heal Detection Name**
SHIPPMENT_ARRIVAL.doc	4B2388DA552BDE61EBC3C634BE4B8B1E	CVE-RTF-2012-0158
svchost.exe	867077b4a536c4bbff31c6a957f8927f	TrojanSpy.Siplog.ST3

svchost.exe	6BB1D69AC18E4E770D360AF4E2595417	TrojanSpy.Predtr.ST3
svchost.exe	f0153d96f59570d93b961db6046f03f6	TrojanSpy.Siplog.ST3
svchost.exe	97cc38c47497e0e08d83d263cf9071ce	TrojanSpy.Siplog.ST3
svchost.exe	fee794fb60fe365ddacc5d9a0427c9a9	TrojanSpy.Siplog.ST3