boby.exe

Is DLL | Packer | Anti Debug | Anti VM | Signed | XOR

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	983.50 KB (1007104 bytes)
Compile time:	2017-07-10 03:36:02
MD5:	d9dd495f577d243c3f493f63d96ae656
SHA1:	0aa4d90c6f3ba8f6fc9c9263b1ebf3d26b7b82d2
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-19 12:57:04

URL(s) file hosting

http://lalecitinadesoja.com/imagenesdeunasdisenos.com/files/boby.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-19 04:59:24	25/69	

Import library

mscoree.dll

7 Behaviors detected by system signatures

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\boby.exe:Zone.Identifier

Crashed cuckoomon during analysis. Report this error to the Github repo.

 - pid: 2380
 - message: Exception reported at offset 0x12410 in cuckoomon itself while accessing 0x40 from hook RtlDispatchException

Exhibits behavior characteristic of iSpy Keylogger

Creates RWX memory

At least one IP Address, Domain, or File Name was found in a crypto call

 - ioc: u.6uF
 - ioc: 2.22
 - ioc: 8.h8
 - ioc: g.jn
 - ioc: 4.b3
 - ioc: k.nu
 - ioc: n.a4
 - ioc: .l.n8
 - ioc: r.vs
 - ioc: w.is
 - ioc: d0.qpe
 - ioc: y.es
 - ioc: 0.mj_
 - ioc: 5.lm
 - ioc: p.s4
 - ioc: j.v6u
 - ioc: s.47
 - ioc: 5p.01
 - ioc: d.owl
 - ioc: d.aiw
 - ioc: 8.xl
 - ioc: b.fr
 - ioc: 7.peW
 - ioc: m.uh
 - ioc: ft.3x
 - ioc: e.sw
 - ioc: m.6u
 - ioc: w.sf
 - ioc: 7.sxC
 - ioc: 4.57

A process created a hidden window

 - Process: boby.exe -> C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe

The binary likely contains encrypted or compressed data.

 - section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x000f5400, virtual_size: 0x000f5394