adobe.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:	817.50 KB (837120 bytes)
Compile time:	2017-07-07 12:37:53
MD5:	73955155eea1ff12f7edd3159abd2512
SHA1:	b664d86eab79bc1512b84ae5498b53191b3f1d67
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-16 20:48:03

URL(s) file hosting

http://erlivia.ltd/adobe.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-04-16 12:01:46	19/66	

Import library

mscoree.dll

11 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN LokiBot User-Agent (Charon/Inferno)

- signature: ET TROJAN LokiBot Checkin
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M2
- signature: ET TROJAN LokiBot Request for C2 Commands Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1
- signature: ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\dfgetyhyujik78u6yt4fw3.exe

Exhibits behavior characteristic of iSpy Keylogger

Attempts to remove evidence of file being downloaded from the Internet

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

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: 0x000cba00, virtual_size: 0x000cb9d4

Performs some HTTP requests

- url: http://89.34.237.212/annonymous/fre.php

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- post_no_referer: HTTP traffic contains a POST request with no referer header
- http_version_old: HTTP traffic uses version 1.0
- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://89.34.237.212/annonymous/fre.php

Network activity detected but not expressed in API logs

Reads data out of its own binary image

- self_read: process: adobe.exe, pid: 2292, offset: 0x00000000, length: 0x000cc600

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: yd.ox
- ioc: z.bl
- ioc: k.nu
- ioc: n.a4
- ioc: .l.n8
- ioc: r.vs
- ioc: w.is
- ioc: d0.qpe
- ioc: 0.mj_
- ioc: d.qg
- ioc: v.5z

Creates RWX memory

2 HTTP Request(s) detected

http://89.34.237.212/annonymous/fre.php

Hostname: 89.34.237.212
IP Address:
Port: 80
Count: 2

http://89.34.237.212/annonymous/fre.php
Hostname: 89.34.237.212
IP Address:
Port: 80
Count: 2

1 Host(s) detected

IP Address	Hostname	Reverse DNS
89.34.237.212		

1 Countr(y|ies) detected

Hosts	Country
1	Romania