000.123

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:	680.00 KB (696320 bytes)
Compile time:	2017-07-15 04:42:08
MD5:	29c3122a162e176d96a598260ad1502b
SHA1:	bf702ae167d7a3231b3a0b6ac7458bcc9e2d839c
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-04-25 12:24:02

URL(s) file hosting

http://i876edw4e5f6tg78hy9tg7r6ftgiy8.erlivia.ltd/000.123

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

Import library

mscoree.dll

12 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

Anomalous binary characteristics

- anomaly: Unprintable characters found in section name

Installs itself for autorun at Windows startup

- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\f6ed5w4derfyu.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\000.123:Zone.Identifier

The binary likely contains encrypted or compressed data.

- section: name: VH\x01nR2", entropy: 8.00, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE, raw_size: 0x0000fa00, virtual_size: 0x0000f860
- section: name: .text, entropy: 7.20, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0003f000, virtual_size: 0x0003ee68

Performs some HTTP requests

- url: http://89.34.237.212/000/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://89.34.237.212/000/fre.php

Network activity detected but not expressed in API logs

Reads data out of its own binary image

- self_read: process: 000.123, pid: 2448, offset: 0x00000000, length: 0x000aa000

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

- ioc: y.gl
- ioc: 5g.gb1
- ioc: ..8mvq
- ioc: f.7bX
- ioc: m.11
- ioc: d.oq
- ioc: 3.0f
- ioc: h.ou
- ioc: l.zo
- ioc: mi.yj
- ioc: x.5t
- ioc: 5.6v
- ioc: 0i.wy/
- ioc: yqq.cd
- ioc: z.lh
- ioc: q.fg
- ioc: q.yi
- ioc: u.p0
- ioc: v5.ei

- ioc: t.y4
- ioc: o.k7
- ioc: v.45wm
- ioc: q.0p
- ioc: j.lm
- ioc: ..3ojp
- ioc: g.64k
- ioc: o.bt
- ioc: v.ou
- ioc: 6.3a
- ioc: g.0l
- ioc: u.a9S
- ioc: i..f
- ioc: u.67
- ioc: 5.16

Creates RWX memory

2 HTTP Request(s) detected

http://89.34.237.212/000/fre.php
Hostname: 89.34.237.212
IP Address:
Port: 80
Count: 2

http://89.34.237.212/000/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