pputty.exe

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

MalFamily: Passwordstealera **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	348.00 KB (356352 bytes)
Compile time:	2017-10-09 17:06:41
MD5:	256d4639b4514c420f482cc9e795cac3
SHA1:	103667324e0c5cc4e670176a3c4bcfcbad06abba
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-10-26 13:54:05

URL(s) file hosting

http://win.budgetshowdown.com:8080/web/pputty.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-10-11 00:30:13	48/65	

Import library

mscoree.dll

5 Behaviors detected by system signatures

Retrieves Windows ProductID, probably to fingerprint the sandbox

Collects information to fingerprint the system

Network activity detected but not expressed in API logs

Performs some HTTP requests

- url: http://ip-api.com/json/
- url: http://freegeoip.net/xml/
- url: http://api.ipify.org/

Looks up the external IP address

- domain: api.ipify.org

3 HTTP Request(s) detected

http://ip-api.com/json/
Hostname: ip-api.com
IP Address: 185.194.141.58
Port: 80
Count: 1

http://freegeoip.net/xml/
Hostname: freegeoip.net
IP Address: 104.31.11.172
Port: 80
Count: 1

http://api.ipify.org/
Hostname: api.ipify.org
IP Address: 174.129.241.106
Port: 80
Count: 1