surecrew.exe

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

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	745.50 KB (763392 bytes)
Compile time:	2018-04-13 07:03:46
MD5:	bb53429c934474eb4ae15362b0b0fed9
SHA1:	88339aea119d80c639e1e98483936a8ca92e7fce
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-15 01:27:02

URL(s) file hosting

http://www.mcvillars.com/Sirjaypompe/surecrew.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-10 23:33:35	53/67	

Import library

mscoree.dll

10 Behaviors detected by system signatures

Creates a copy of itself

- copy: C:\Users\Seven01\Desktop\bbbbbt.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\bbbbbt
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\bbbbbt.txt | cmd

Executed a process and injected code into it, probably while unpacking

- Injection: bbbbbt.exe(2752) -> bbbbbt.exe(3000)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0004a400, virtual_size: 0x0004a344
- section: name: .rsrc, entropy: 7.99, characteristics: IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ, raw_size: 0x0006fc00, virtual_size: 0x0006fb5c

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
- url: http://www.wwwjinsha441.com/hx251/?v6=z9dM7K4hkPT3SdIiafSL5treIp8aRXYBQmftBM7EyXtHLKb7a56oL10qMrwPRRoqP/ovNXQY&-Zi=V6ALsRj0n
- url: http://www.17mobile.loan/hx251/?v6=O0A0p3PxsvMxODXa/DRDsKns5Y91c+jh3wm0q6A45O5Iz/eiEM1yx4WqLYi9g0QLQXwCzbCb&-Zi=V6ALsRj0n
- url: http://www.17mobile.loan/hx251/
- url: http://www.hemalipaterl.com/hx251/?v6=pcbhwblwWCwYoF4aDva0Y4R6u1QpH7UtlACxSbhAuZvIiwPMFRBhQIMYmb7jryjJW73+oayH&-Zi=V6ALsRj0n
- url: http://www.hemalipaterl.com/hx251/
- url: http://www.alplp.link/hx251/?v6=qd0+Lg6BfVzDx2IHVHj51hHqGNsADaywABgYQaTM+JMWh+JnC6AOL3xKROowfymh5ACbRCAp&-Zi=V6ALsRj0n
- url: http://www.alplp.link/hx251/
- url: http://www.zafsdyg.com/hx251/?v6=wVe094DaKVEtz+/vB9TkbZlc/SFEifjlugzZwuALPbrZGECwVUfUXO8lnXaIJvlZ+DygeVrv&-Zi=V6ALsRj0n
- url: http://www.zafsdyg.com/hx251/
- url: http://www.virtudessarmientocoach.com/hx251/?v6=79UmuHsPLanZ38eBpQ1VbXXBrGQSqMveenUOjxymv1NHu31LemkHmTBqjsfKU/YYikldA5Ci&-Zi=V6ALsRj0n
- url: http://www.virtudessarmientocoach.com/hx251/

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

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://www.wwwjinsha441.com/hx251/?v6=z9dM7K4hkPT3SdIiafSL5treIp8aRXYBQmftBM7EyXtHLKb7a56oL10qMrwPRRoqP/ovNXQY&-Zi=V6ALsRj0n
- suspicious_request: http://www.17mobile.loan/hx251/?v6=O0A0p3PxsvMxODXa/DRDsKns5Y91c+jh3wm0q6A45O5Iz/eiEM1yx4WqLYi9g0QLQXwCzbCb&-Zi=V6ALsRj0n
- suspicious_request: http://www.17mobile.loan/hx251/
- suspicious_request: http://www.hemalipaterl.com/hx251/?v6=pcbhwblwWCwYoF4aDva0Y4R6u1QpH7UtlACxSbhAuZvIiwPMFRBhQIMYmb7jryjJW73+oayH&-Zi=V6ALsRj0n
- suspicious_request: http://www.hemalipaterl.com/hx251/
- suspicious_request: http://www.alplp.link/hx251/?v6=qd0+Lg6BfVzDx2IHVHj51hHqGNsADaywABgYQaTM+JMWh+JnC6AOL3xKROowfymh5ACbRCAp&-Zi=V6ALsRj0n
- suspicious_request: http://www.alplp.link/hx251/
- suspicious_request:

http://www.zafsdyg.com/hx251/?v6=wVe094DaKVEtz+/vB9TkbZlc/SFEifjlugzZwuALPbrZGECwVUfUXO8lnXaIJvlZ+DygeVrv&-Zi=V6ALsRj0n
- suspicious_request: http://www.zafsdyg.com/hx251/
- suspicious_request: http://www.virtudessarmientocoach.com/hx251/?v6=79UmuHsPLanZ38eBpQ1VbXXBrGQSqMveenUOjxymv1NHu31LemkHmTBqjsfKU/YYikldA5Ci&-Zi=V6ALsRj0n
- suspicious_request: http://www.virtudessarmientocoach.com/hx251/

Drops a binary and executes it

- binary: C:\Users\Seven01\Desktop\bbbbbt.exe

A process created a hidden window

- Process: surecrew.exe -> "cmd"
- Process: bbbbbt.exe -> "cmd"

Network activity detected but not expressed in API logs

Creates RWX memory

17 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

Hostname: www.download.windowsupdate.com

IP Address: 95.101.34.89

Port: 80

Count: 1

http://www.wwwjinsha441.com/hx251/?v6=z9dM7K4hkPT3SdIiafSL5treIp8aRXYBQmftBM7EyXtHLKb7a56oL10qMrwPRRoqP/ovNXQY&-Zi=V6ALsRj0n

Hostname: www.wwwjinsha441.com

IP Address: 174.139.98.78

Port: 80

Count: 1

http://www.17mobile.loan/hx251/?v6=O0A0p3PxsvMxODXa/DRDsKns5Y91c+jh3wm0q6A45O5Iz/eiEM1yx4WqLYi9g0QLQXwCzbCb&-Zi=V6ALsRj0n

Hostname: www.17mobile.loan

IP Address: 104.27.149.94

Port: 80

Count: 1

http://www.17mobile.loan/hx251/

Hostname: www.17mobile.loan

IP Address: 104.27.149.94
Port: 80
Count: 1

http://www.17mobile.loan/hx251/
Hostname: www.17mobile.loan
IP Address: 104.27.149.94
Port: 80
Count: 1

http://www.hemalipaterl.com/hx251/?v6=pcbhwblwWCwYoF4aDva0Y4R6u1QpH7UtlACxSbhAuZvIiwPMFRBhQIMYmb7jryjJW73+oayH&-Zi=V6ALsRj0n
Hostname: www.hemalipaterl.com
IP Address: 199.188.206.251
Port: 80
Count: 1

http://www.hemalipaterl.com/hx251/
Hostname: www.hemalipaterl.com
IP Address: 199.188.206.251
Port: 80
Count: 1

http://www.hemalipaterl.com/hx251/
Hostname: www.hemalipaterl.com
IP Address: 199.188.206.251
Port: 80
Count: 1

http://www.alplp.link/hx251/?v6=qd0+Lg6BfVzDx2IHVHj51hHqGNsADaywABgYQaTM+JMWh+JnC6AOL3xKROowfymh5ACbRCAp&-Zi=V6ALsRj0n
Hostname: www.alplp.link
IP Address:
Port: 80
Count: 1

http://www.alplp.link/hx251/

Hostname: www.alplp.link
IP Address:
Port: 80
Count: 1

http://www.alplp.link/hx251/
Hostname: www.alplp.link
IP Address:
Port: 80
Count: 1

http://www.zafsdyg.com/hx251/?v6=wVe094DaKVEtz+/vB9TkbZlc/SFEifjlugzZwuALPbrZGECwVUfUXO8lnXaIJvlZ+DygeVrv&-Zi=V6ALsRj0n
Hostname: www.zafsdyg.com
IP Address: 104.149.211.18
Port: 80
Count: 1

http://www.zafsdyg.com/hx251/
Hostname: www.zafsdyg.com
IP Address: 104.149.211.18
Port: 80
Count: 1

http://www.zafsdyg.com/hx251/
Hostname: www.zafsdyg.com
IP Address: 104.149.211.18
Port: 80
Count: 1

http://www.virtudessarmientocoach.com/hx251/?v6=79UmuHsPLanZ38eBpQ1VbXXBrGQSqMveenUOjxymv1NHu31LemkHmTBqjsfKU/YYikldA5Ci&-Zi=V6ALsRj0n
Hostname: www.virtudessarmientocoach.com
IP Address: 217.160.230.167
Port: 80
Count: 1

http://www.virtudessarmientocoach.com/hx251/
Hostname: www.virtudessarmientocoach.com
IP Address: 217.160.230.167
Port: 80
Count: 1

http://www.virtudessarmientocoach.com/hx251/
Hostname: www.virtudessarmientocoach.com
IP Address: 217.160.230.167
Port: 80
Count: 1