eRY

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

MalFamily: Emotet **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
File size:	427.00 KB (437248 bytes)
Compile time:	2020-09-18 21:25:24
MD5:	b6fff8ead8a2a1e464bb042ed1eb3f79
SHA1:	200a1243d3e54d64017fdc5b066ce673b949d9bf
Import hash:	39948763cc1873dc50981ea479aab099
Submitted:	2021-08-14 15:03:07

URL(s) file hosting

http://mbsolutions.ge/wp-admin/eRY/

Antivirus Report

Report date	Detection Ratio	Permalink
No report available		

Import library

VERSION.dll
KERNEL32.dll
ADVAPI32.dll
PSAPI.DLL

USER32.dll
comctl32.dll

10 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN Win32/Emotet CnC Activity (POST) M10

Anomalous binary characteristics

- anomaly: Actual checksum does not match that reported in PE header

Performs some HTTP requests

- url: http://91.105.94.200/DMVSbT7xomE7n8hn0x/rP2WWqwX4TS/ExOMNHIt6/OiJ3zQwp0E/bkrrbu3igWcIQzC/
- url: http://51.38.124.206/ZT75iBjhpbwktxfbR86/d9VcfV5/CCb7WpM2kh/uYdL6ccVNN/
- url: http://189.2.177.210:443/XY54k4DiHMKwc6V/r6ZkyvoZ6E/
- url: http://181.30.61.163:443/1Bvcry0p/qPoOYcVRFJoAv/DOTbB/KTTSrG93AV69/TUneh/
- url: http://185.178.10.77/RDg66RusYe/49VH7oV23CcG5fuMv/dpMBZPfGppsQUYA/KorYJerEiaohe/7sA4bpk92K/
- url: http://199.203.62.165/CE1ZEkhpQ/pndb1CoKx/tkjKoGhHrKKSYRSZ3/o16V0UW/
- url: http://177.73.0.98:443/DWpvRYh4qc5/TX1KMfrZhntpksxBZU/Xq5cT3qjf5PAEw/whoFGqhw47/
- url: http://185.183.16.47/hYUGSs41b6huY/urqn/9OFhhG/ngGrGYAqeFegLnp/
- url: http://78.249.119.122/5z1TecxAjvnJGrjO/QcOSqNR3/jixX/OBifrEnLWPN/MAb5XTageKMPicf31lN/
- url: http://191.182.6.118/lYjUbcguD5n2w/bk6lsg7BJuxZ4g4/4PQko0N/97BZ0RghG/
- url: http://96.227.52.8:443/6Zg0/
- url: http://186.103.141.250:443/ZcE6Y11G4w1UjX/oAYIk59/Fsg1xIo1P97N/
- url: http://50.121.220.50/JFY0cIDYy/rSKZz1gM1tMFUB/7LlZrhjVqMD9R4IDCX/XeuunBCn/Na3aQ3gY/ZBwKZhZuyUMgBb/
- url: http://61.197.92.216/HOweGhIUB/RFQaRdb7h/g40SWH/cbd07UUcUscDiWy/DiGEdzsUsF4kTv/H7go3k/
- url: http://82.76.111.249:443/gKurel9gK2Ue2g/qcHS8XcSd/MIUl/TMMlsd6wMg/YxXTVldU3DmBp7Thz/
- url: http://110.142.219.51/Nk4g/
- url: http://92.24.50.153/kUVjVQp/zCbLTVqkXc4NH7/m622ypTplLm1/PkSJ2/1UfDgKDu1RHcUW9/IYwes/
- url: http://190.24.243.186/pq2Vrnv28/vwdoDuK8aTWDrCNm4/
- url: http://190.2.31.172/nCUzcDVbtlZc4l/
- url: http://82.230.1.24/FJJn01dDjVPHvlLEJ/FyjJ9tq4tJNQ/
- url: http://188.135.15.49/bGu27fNJVhPrZN5H/P9RjYjqoeFiL/mSRIqJW3FYH/
- url: http://216.47.196.104/PBPdFVvqWqng2yZb/
- url: http://35.143.99.174/YiW82gY/RmXhz2b/hGXJn2eN2xJcHbhMO9Y/jU9Bzu/
- url: http://220.109.145.69/Wvi5HlYglttJwEgL/
- url: http://170.81.48.2/riNNYbC6hBZE22ET/

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

- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://91.105.94.200/DMVSbT7xomE7n8hn0x/rP2WWqwX4TS/ExOMNHIt6/OiJ3zQwp0E/bkrrbu3igWcIQzC/
- suspicious_request:

http://51.38.124.206/ZT75iBjhpbwktxfbR86/d9VcfV5/CCb7WpM2kh/uYdL6ccVNN/
- suspicious_request: http://189.2.177.210:443/XY54k4DiHMKwc6V/r6ZkyvoZ6E/
- suspicious_request: http://181.30.61.163:443/1Bvcry0p/qPoOYcVRFJoAv/DOTbB/KTTSrG93AV69/TUneh/
- suspicious_request: http://185.178.10.77/RDg66RusYe/49VH7oV23CcG5fuMv/dpMBZPfGppsQUYA/KorYJerEiaohe/7sA4bpk92K/
- suspicious_request: http://199.203.62.165/CE1ZEkhpQ/pndb1CoKx/tkjKoGhHrKKSYRSZ3/o16V0UW/
- suspicious_request: http://177.73.0.98:443/DWpvRYh4qc5/TX1KMfrZhntpksxBZU/Xq5cT3qjf5PAEw/whoFGqhw47/
- suspicious_request: http://185.183.16.47/hYUGSs41b6huY/urqn/9OFhhG/ngGrGYAqeFegLnp/
- suspicious_request: http://78.249.119.122/5z1TecxAjvnJGrjO/QcOSqNR3/jixX/OBifrEnLWPN/MAb5XTageKMPicf31lN/
- suspicious_request: http://191.182.6.118/lYjUbcguD5n2w/bk6lsg7BJuxZ4g4/4PQko0N/97BZ0RghG/
- suspicious_request: http://96.227.52.8:443/6Zg0/
- suspicious_request: http://186.103.141.250:443/ZcE6Y11G4w1UjX/oAYIk59/Fsg1xIo1P97N/
- suspicious_request: http://50.121.220.50/JFY0cIDYy/rSKZz1gM1tMFUB/7LlZrhjVqMD9R4IDCX/XeuunBCn/Na3aQ3gY/ZBwKZhZuyUMgBb/
- suspicious_request: http://61.197.92.216/HOweGhIUB/RFQaRdb7h/g40SWH/cbd07UUcUscDiWy/DiGEdzsUsF4kTv/H7go3k/
- suspicious_request: http://82.76.111.249:443/gKurel9gK2Ue2g/qcHS8XcSd/MIUl/TMMlsd6wMg/YxXTVldU3DmBp7Thz/
- suspicious_request: http://110.142.219.51/Nk4g/
- suspicious_request: http://92.24.50.153/kUVjVQp/zCbLTVqkXc4NH7/m622ypTplLm1/PkSJ2/1UfDgKDu1RHcUW9/IYwes/
- suspicious_request: http://190.24.243.186/pq2Vrnv28/vwdoDuK8aTWDrCNm4/
- suspicious_request: http://190.2.31.172/nCUzcDVbtlZc4l/
- suspicious_request: http://82.230.1.24/FJJn01dDjVPHvlLEJ/FyjJ9tq4tJNQ/
- suspicious_request: http://188.135.15.49/bGu27fNJVhPrZN5H/P9RjYjqoeFiL/mSRIqJW3FYH/
- suspicious_request: http://216.47.196.104/PBPdFVvqWqng2yZb/
- suspicious_request: http://35.143.99.174/YiW82gY/RmXhz2b/hGXJn2eN2xJcHbhMO9Y/jU9Bzu/
- suspicious_request: http://220.109.145.69/Wvi5HlYglttJwEgL/
- suspicious_request: http://170.81.48.2/riNNYbC6hBZE22ET/

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

Expresses interest in specific running processes

- process: eRY.exe

Dynamic (imported) function loading detected

- DynamicLoader: ntdll.dll/qsort
- DynamicLoader: ntdll.dll/bsearch
- DynamicLoader: ntdll.dll/wcslen
- DynamicLoader: kernel32.dll/VirtualFree
- DynamicLoader: kernel32.dll/Process32Next
- DynamicLoader: kernel32.dll/Process32First
- DynamicLoader: kernel32.dll/CreateToolhelp32Snapshot
- DynamicLoader: kernel32.dll/CloseHandle
- DynamicLoader: kernel32.dll/SetLastError
- DynamicLoader: kernel32.dll/HeapAlloc
- DynamicLoader: kernel32.dll/HeapFree
- DynamicLoader: kernel32.dll/GetProcessHeap
- DynamicLoader: kernel32.dll/ExitProcess
- DynamicLoader: kernel32.dll/VirtualAlloc
- DynamicLoader: kernel32.dll/VirtualProtect
- DynamicLoader: kernel32.dll/VirtualQuery
- DynamicLoader: kernel32.dll/FreeLibrary

- DynamicLoader: kernel32.dll/GetProcAddress
- DynamicLoader: kernel32.dll/LoadLibraryA
- DynamicLoader: kernel32.dll/LoadLibraryW
- DynamicLoader: kernel32.dll/IsBadReadPtr
- DynamicLoader: kernel32.dll/GetNativeSystemInfo
- DynamicLoader: kernel32.dll/SortGetHandle
- DynamicLoader: kernel32.dll/SortCloseHandle
- DynamicLoader: CRYPTSP.dll/CryptAcquireContextW
- DynamicLoader: CRYPTSP.dll/CryptImportKey
- DynamicLoader: CRYPTSP.dll/CryptGenKey
- DynamicLoader: CRYPTSP.dll/CryptCreateHash
- DynamicLoader: CRYPTSP.dll/CryptDuplicateHash
- DynamicLoader: CRYPTSP.dll/CryptEncrypt
- DynamicLoader: CRYPTSP.dll/CryptExportKey
- DynamicLoader: CRYPTSP.dll/CryptGetHashParam
- DynamicLoader: CRYPTSP.dll/CryptDestroyHash
- DynamicLoader: RASAPI32.dll/RasConnectionNotificationW
- DynamicLoader: sechost.dll/NotifyServiceStatusChangeA
- DynamicLoader: CRYPTBASE.dll/SystemFunction036
- DynamicLoader: CRYPTSP.dll/CryptDecrypt

Mimics the system's user agent string for its own requests

Creates RWX memory

SetUnhandledExceptionFilter detected (possible anti-debug)

25 HTTP Request(s) detected

http://91.105.94.200/DMVSbT7xomE7n8hn0x/rP2WWqwX4TS/ExOMNHlt6/OiJ3zQwp0E/bkrrbu3igWcIQzC/
Hostname: 91.105.94.200
IP Address:
Port: 80
Count: 1

http://51.38.124.206/ZT75iBjhpbwktxfbR86/d9VcfV5/CCb7WpM2kh/uYdL6ccVNN/
Hostname: 51.38.124.206
IP Address:
Port: 80
Count: 1

http://189.2.177.210:443/XY54k4DiHMKwc6V/r6ZkyvoZ6E/
Hostname: 189.2.177.210:443
IP Address:
Port: 443
Count: 1

http://181.30.61.163:443/1Bvcry0p/qPoOYcVRFJoAv/DOTbB/KTTSrG93AV69/TUneh/
Hostname: 181.30.61.163:443
IP Address:
Port: 443
Count: 1

http://185.178.10.77/RDg66RusYe/49VH7oV23CcG5fuMv/dpMBZPfGppsQUYA/KorYJerEiaohe/7sA4bpk92K/
Hostname: 185.178.10.77
IP Address:
Port: 80
Count: 1

http://199.203.62.165/CE1ZEkhpQ/pndb1CoKx/tkjKoGhHrKKSYRSZ3/o16V0UW/
Hostname: 199.203.62.165
IP Address:
Port: 80
Count: 1

http://177.73.0.98:443/DWpvRYh4qc5/TX1KMfrZhntpksxBZU/Xq5cT3qjf5PAEw/whoFGqhw47/
Hostname: 177.73.0.98:443
IP Address:
Port: 443
Count: 1

http://185.183.16.47/hYUGSs41b6huY/urqn/9OFhhG/ngGrGYAqeFegLnp/
Hostname: 185.183.16.47
IP Address:
Port: 80
Count: 1

http://78.249.119.122/5z1TecxAjvnJGrjO/QcOSqNR3/jixX/OBifrEnLWPN/MAb5XTageKMPicf31lN/
Hostname: 78.249.119.122
IP Address:
Port: 80
Count: 1

http://191.182.6.118/lYjUbcguD5n2w/bk6lsg7BJuxZ4g4/4PQko0N/97BZ0RghG/
Hostname: 191.182.6.118
IP Address:
Port: 80
Count: 1

http://96.227.52.8:443/6Zg0/
Hostname: 96.227.52.8:443
IP Address:
Port: 443
Count: 1

http://186.103.141.250:443/ZcE6Y11G4w1UjX/oAYIk59/Fsg1xIo1P97N/
Hostname: 186.103.141.250:443
IP Address:
Port: 443
Count: 1

http://50.121.220.50/JFY0cIDYy/rSKZz1gM1tMFUB/7LlZrhjVqMD9R4IDCX/XeuunBCn/Na3aQ3gY/ZBwKZhZuyUMgBb/
Hostname: 50.121.220.50
IP Address:
Port: 80
Count: 1

http://61.197.92.216/HOweGhIUB/RFQaRdb7h/g40SWH/cbd07UUcUscDiWy/DiGEdzsUsF4kTv/H7go3k/
Hostname: 61.197.92.216
IP Address:
Port: 80
Count: 1

http://82.76.111.249:443/gKurel9gK2Ue2g/qcHS8XcSd/MIUl/TMMlsd6wMg/YxXTVldU3DmBp7Thz/
Hostname: 82.76.111.249:443
IP Address:

Port: 443
Count: 1

http://110.142.219.51/Nk4g/
Hostname: 110.142.219.51
IP Address:
Port: 80
Count: 1

http://92.24.50.153/kUVjVQp/zCbLTVqkXc4NH7/m622ypTplLm1/PkSJ2/1UfDgKDu1RHcUW9/IYwes/
Hostname: 92.24.50.153
IP Address:
Port: 80
Count: 1

http://190.24.243.186/pq2Vrnv28/vwdoDuK8aTWDrCNm4/
Hostname: 190.24.243.186
IP Address:
Port: 80
Count: 1

http://190.2.31.172/nCUzcDVbtlZc4l/
Hostname: 190.2.31.172
IP Address:
Port: 80
Count: 1

http://82.230.1.24/FJJn01dDjVPHvlLEJ/FyjJ9tq4tJNQ/
Hostname: 82.230.1.24
IP Address:
Port: 80
Count: 1

http://188.135.15.49/bGu27fNJVhPrZN5H/P9RjYjqoeFiL/mSRIqJW3FYH/
Hostname: 188.135.15.49
IP Address:

Port: 80
Count: 1

http://216.47.196.104/PBPdFVvqWqng2yZb/
Hostname: 216.47.196.104
IP Address:
Port: 80
Count: 1

http://35.143.99.174/YiW82gY/RmXhz2b/hGXJn2eN2xJcHbhMO9Y/jU9Bzu/
Hostname: 35.143.99.174
IP Address:
Port: 80
Count: 1

http://220.109.145.69/Wvi5HlYglttJwEgL/
Hostname: 220.109.145.69
IP Address:
Port: 80
Count: 1

http://170.81.48.2/riNNYbC6hBZE22ET/
Hostname: 170.81.48.2
IP Address:
Port: 80
Count: 1

41 Host(s) detected

IP Address	Hostname	Reverse DNS
96.227.52.8		static-96-227-52-8.phlapa.fios.verizon.net.
92.24.50.153		host-92-24-50-153.as13285.net.
91.105.94.200		
87.106.46.107		s20305366.onlinehome-server.info.

82.76.111.249		82-76-111-249.rdsnet.ro.
82.230.1.24		bas33-2_migr-82-230-1-24.fbx.proxad.net.
78.249.119.122		ang85-1-78-249-119-122.fbx.proxad.net.
77.90.136.129		reserved-77-90-136-129.insec.gmbh.
72.47.248.48		
68.183.170.114		68.183.170.114-e1-8080-keep-up.
61.197.92.216		pl2008.ag1313.nttpc.ne.jp.
54.37.42.48		
51.38.124.206		206.ip-51-38-124.eu.
51.255.165.160		160.ip-51-255-165.eu.
50.28.51.143		
50.121.220.50		static-50-121-220-50.clbg.wv.frontiernet.net.
5.196.35.138		vps10.open-techno.net.
5.189.178.202		mail.erotikversand.de.
38.88.126.202		
35.143.99.174		035-143-099-174.biz.spectrum.com.
220.109.145.69		i220-109-145-69.s41.a007.ap.plala.or.jp.
216.47.196.104		196-104.graceba.net.
213.197.182.158		
212.71.237.140		li666-140.members.linode.com.
199.203.62.165		odap-199-203-62-165.bb.netvision.net.il.
192.241.146.84		
191.182.6.118		bfb60676.virtua.com.br.
190.24.243.186		static-190-24-243-186.static.etb.net.co.
190.2.31.172		customer-static-2-31-172.iplannetworks.net.

189.2.177.210		
188.135.15.49		
186.70.127.199		199.cpe-186-70-127.gye.satnet.net.
186.103.141.250		186-103-141-250.static.tie.cl.
185.183.16.47		47.16.183.185.dyn.akiwifi.com.
185.178.10.77		host-185-178-10-77.as206732.net.
181.30.61.163		163-61-30-181.fibertel.com.ar.
177.73.0.98		177-73-0-98.inbnet.com.br.
172.104.169.32		li1760-32.members.linode.com.
170.81.48.2		170.81.48.2.tacnettelecom.com.br.
111.67.12.221		vmh17370.hosting24.com.au.
110.142.219.51		anth992200.lnk.telstra.net.

19 Countr(y|ies) detected

Hosts	Country
9	United States
5	France
4	Brazil
3	Germany
2	Argentina
2	Italy
2	Japan
2	Australia
2	United Kingdom
1	Chile

1	Singapore	
1	Spain	
1	Ecuador	
1	Israel	
1	Latvia	
1	Romania	
1	Lithuania	
1	Colombia	
1	Oman