rRS

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 21:21:39
MD5:	1d94974d27fc9127c69992d325afbc89
SHA1:	f238ed9987b52b8368c872804e64fea64360f0be
Import hash:	39948763cc1873dc50981ea479aab099
Submitted:	2021-08-30 06:57:07

URL(s) file hosting

http://justinscott.com.au/sites/rRS/

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://71.72.196.159/UObQ/Sf3PRIwYeFEu5y/476ZJiIAGac8QXVLV/Zh3Pj7sEsu9o5y/laYSDQggB241WhDC/
- url: http://94.23.216.33/ow7XVOh/IPUBkFDflCUxz/sfhzKTj9XwKH/DXAeEAOy8NEO/
- url: http://94.23.237.171:443/5WZNmOL4PVikWS5eHb2/PRKTRDmt8UKJ/
- url: http://61.19.246.238:443/zr1N5HGb3Sicdf/ziH9YEjXOg/BUEGc/
- url: http://156.155.166.221/m07j/vDEfXbYL9oexTDXh/RDhLMBmkX6TbimvROY/LUw7m28XeTx5/OmWCYj79WERvBQi/
- url: http://50.35.17.13/3BIMiYFiT2flGT76/Om3nHU0e7Sfkv/UnZJhEn7PmuyEIa/
- url: http://153.137.36.142/pwKp0Xw/i7MYdq467wjX2PiknJ/
- url: http://185.94.252.104:443/BR0f2Os0yRWkFO5p/
- url: http://174.45.13.118/AFo4GL/
- url: http://62.75.141.82/FbZC/dYaHYStoY66dr3kpY9/JhoMsxI/
- url: http://213.196.135.145/I30F8OMY8LTMu6/
- url: http://188.219.31.12/RTT0Tu83DfRRqVitM4O/IosUZs/K5S6ESG08Mkz/dGaaAcUDOUOscqoO/
- url: http://82.80.155.43/alOAASEoc66JSo64/
- url: http://187.161.206.24/kOGtFLMWs/utuhMSDWpip3QO/xbYWv2/lPROQt7pa/
- url: http://172.91.208.86/0eWn073K6/BRKdD4gL/sSVh0Xfglg3vxw0Yn/CAUU/
- url: http://124.41.215.226/d9l4vyIdVu3/O4qn/k9DCR0gLoZ/00FPaqZ0BzGZEG6Z/
- url: http://107.5.122.110/n81pRwVGKh0/2Y6NCA0Okj7kpZ1JL/5cblB2E55h4P69D/c7Hxk6SMCcB8Yc/
- url: http://200.123.150.89:443/hfUvzHy29u/
- url: http://1.221.254.82/UgLERjI/U8BLm7yn7lMfcB/V6nm2E/Sr5IRcGm/
- url: http://181.169.34.190/p2UtL2m/HWj9GMXjRe0mZpLXw/Z49LFJmO/Omgv848SVvI/
- url: http://47.144.21.12:443/45fYp4bQkbREsJxuMYH/Q7d813Nw/
- url: http://89.216.122.92/FcR9Npv4K/idoKEHthMLuL6JmNcAi/8pdE58G/grfbj8jJx4zx/qHPPcRswcejQs5dUN/wc1QQw/
- url: http://84.39.182.7/hEJ3LjEhK/lsqJedctAMp0P/SjVbhJRrjzdAsGdXvX9/dz8WViVLdn/
- url: http://94.200.114.161/VZV5Jd3MI23/CxuKUUt6vB7jg/
- url: http://139.99.158.11:443/bvody2/
- url: http://220.245.198.194/VmL1vd7ycXcP7eIrpF/heV6/o1j3GTfi/
- url: http://62.30.7.67:443/Lb9x7OC0ZqL6ogn/Usi7tdfM/

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://71.72.196.159/UObQ/Sf3PRIwYeFEu5y/476ZJiIAGac8QXVLV/Zh3Pj7sEsu9o5y/laYSDQggB241WhDC/
- suspicious_request: http://94.23.216.33/ow7XVOh/IPUBkFDflCUxz/sfhzKTj9XwKH/DXAeEAOy8NEO/
- suspicious_request: http://94.23.237.171:443/5WZNmOL4PVikWS5eHb2/PRKTRDmt8UKJ/

- suspicious_request: http://61.19.246.238:443/zr1N5HGb3Sicdf/ziH9YEjXOg/BUEGc/
- suspicious_request: http://156.155.166.221/m07j/vDEfXbYL9oexTDXh/RDhLMBmkX6TbimvROY/LUw7m28XeTx5/OmWCYj79WERvBQi/
- suspicious_request: http://50.35.17.13/3BIMiYFiT2flGT76/Om3nHU0e7Sfkv/UnZJhEn7PmuyEIa/
- suspicious_request: http://153.137.36.142/pwKp0Xw/i7MYdq467wjX2PiknJ/
- suspicious_request: http://185.94.252.104:443/BR0f2Os0yRWkFO5p/
- suspicious_request: http://174.45.13.118/AFo4GL/
- suspicious_request: http://62.75.141.82/FbZC/dYaHYStoY66dr3kpY9/JhoMsxI/
- suspicious_request: http://213.196.135.145/I30F8OMY8LTMu6/
- suspicious_request: http://188.219.31.12/RTT0Tu83DfRRqVitM4O/IosUZs/K5S6ESG08Mkz/dGaaAcUDOUOscqoO/
- suspicious_request: http://82.80.155.43/alOAASEoc66JSo64/
- suspicious_request: http://187.161.206.24/kOGtFLMWs/utuhMSDWpip3QO/xbYWv2/lPROQt7pa/
- suspicious_request: http://172.91.208.86/0eWn073K6/BRKdD4gL/sSVh0Xfglg3vxw0Yn/CAUU/
- suspicious_request: http://124.41.215.226/d9l4vyIdVu3/O4qn/k9DCR0gLoZ/00FPaqZ0BzGZEG6Z/
- suspicious_request: http://107.5.122.110/n81pRwVGKh0/2Y6NCA0Okj7kpZ1JL/5cblB2E55h4P69D/c7Hxk6SMCcB8Yc/
- suspicious_request: http://200.123.150.89:443/hfUvzHy29u/
- suspicious_request: http://1.221.254.82/UgLERjI/U8BLm7yn7lMfcB/V6nm2E/Sr5IRcGm/
- suspicious_request: http://181.169.34.190/p2UtL2m/HWj9GMXjRe0mZpLXw/Z49LFJmO/Omgv848SVvI/
- suspicious_request: http://47.144.21.12:443/45fYp4bQkbREsJxuMYH/Q7d813Nw/
- suspicious_request: http://89.216.122.92/FcR9Npv4K/idoKEHthMLuL6JmNcAi/8pdE58G/grfbj8jJx4zx/qHPPcRswcejQs5dUN/wc1QQw/
- suspicious_request: http://84.39.182.7/hEJ3LjEhK/lsqJedctAMp0P/SjVbhJRrjzdAsGdXvX9/dz8WViVLdn/
- suspicious_request: http://94.200.114.161/VZV5Jd3MI23/CxuKUUt6vB7jg/
- suspicious_request: http://139.99.158.11:443/bvody2/
- suspicious_request: http://220.245.198.194/VmL1vd7ycXcP7eIrpF/heV6/o1j3GTfi/
- suspicious_request: http://62.30.7.67:443/Lb9x7OC0ZqL6ogn/Usi7tdfM/

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

Expresses interest in specific running processes

- process: rRS.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)

27 HTTP Request(s) detected

http://71.72.196.159/UObQ/Sf3PRIwYeFEu5y/476ZJiIAGac8QXVLV/Zh3Pj7sEsu9o5y/laYSDQggB241WhDC/
Hostname: 71.72.196.159
IP Address:
Port: 80
Count: 1

http://94.23.216.33/ow7XVOh/IPUBkFDfICUxz/sfhzKTj9XwKH/DXAeEAOy8NEO/
Hostname: 94.23.216.33
IP Address:
Port: 80
Count: 1

http://94.23.237.171:443/5WZNmOL4PVikWS5eHb2/PRKTRDmt8UKJ/
Hostname: 94.23.237.171:443
IP Address:
Port: 443
Count: 1

http://61.19.246.238:443/zr1N5HGb3Sicdf/ziH9YEjXOg/BUEGc/
Hostname: 61.19.246.238:443
IP Address:
Port: 443

Count: 1

http://156.155.166.221/m07j/vDEfXbYL9oexTDXh/RDhLMBmkX6TbimvROY/LUw7m28XeTx5/OmWCYj79WERvBQi/
Hostname: 156.155.166.221
IP Address:
Port: 80
Count: 1

http://50.35.17.13/3BIMiYFiT2flGT76/Om3nHU0e7Sfkv/UnZJhEn7PmuyEla/
Hostname: 50.35.17.13
IP Address:
Port: 80
Count: 1

http://153.137.36.142/pwKp0Xw/i7MYdq467wjX2PiknJ/
Hostname: 153.137.36.142
IP Address:
Port: 80
Count: 1

http://185.94.252.104:443/BR0f2Os0yRWkFO5p/
Hostname: 185.94.252.104:443
IP Address:
Port: 443
Count: 1

http://174.45.13.118/AFo4GL/
Hostname: 174.45.13.118
IP Address:
Port: 80
Count: 1

http://62.75.141.82/FbZC/dYaHYStoY66dr3kpY9/JhoMsxI/
Hostname: 62.75.141.82
IP Address:
Port: 80

Count: 1

http://213.196.135.145/I30F8OMY8LTMu6/
Hostname: 213.196.135.145
IP Address:
Port: 80
Count: 1

http://188.219.31.12/RTT0Tu83DfRRqVitM4O/losUZs/K5S6ESG08Mkz/dGaaAcUDOUOscqoO/
Hostname: 188.219.31.12
IP Address:
Port: 80
Count: 1

http://82.80.155.43/alOAASEoc66JSo64/
Hostname: 82.80.155.43
IP Address:
Port: 80
Count: 1

http://187.161.206.24/kOGtFLMWs/utuhMSDWpip3QO/xbYWv2/lPROQt7pa/
Hostname: 187.161.206.24
IP Address:
Port: 80
Count: 1

http://172.91.208.86/0eWn073K6/BRKdD4gL/sSVh0Xfglg3vxw0Yn/CAUU/
Hostname: 172.91.208.86
IP Address:
Port: 80
Count: 1

http://124.41.215.226/d9l4vyIdVu3/O4qn/k9DCR0gLoZ/00FPaqZ0BzGZEG6Z/
Hostname: 124.41.215.226
IP Address:
Port: 80
Count: 1

http://107.5.122.110/n81pRwVGKh0/2Y6NCA0Okj7kpZ1JL/5cblB2E55h4P69D/c7Hxk6SMCcB8Yc/
Hostname: 107.5.122.110
IP Address:
Port: 80
Count: 1

http://200.123.150.89:443/hfUvzHy29u/
Hostname: 200.123.150.89:443
IP Address:
Port: 443
Count: 1

http://1.221.254.82/UgLERjl/U8BLm7yn7lMfcB/V6nm2E/Sr5lRcGm/
Hostname: 1.221.254.82
IP Address:
Port: 80
Count: 1

http://181.169.34.190/p2UtL2m/HWj9GMXjRe0mZpLXw/Z49LFJmO/Omgv848SVvl/
Hostname: 181.169.34.190
IP Address:
Port: 80
Count: 1

http://47.144.21.12:443/45fYp4bQkbREsJxuMYH/Q7d813Nw/
Hostname: 47.144.21.12:443
IP Address:
Port: 443
Count: 1

http://89.216.122.92/FcR9Npv4K/idoKEHthMLuL6JmNcAi/8pdE58G/grfbj8jJx4zx/qHPPcRswcejQs5dUN/wc1QQw/
Hostname: 89.216.122.92
IP Address:
Port: 80
Count: 1

http://84.39.182.7/hEJ3LjEhK/lsqJedctAMp0P/SjVbhJRrjzdAsGdXvX9/dz8WViVLdn/
Hostname: 84.39.182.7
IP Address:
Port: 80
Count: 1

http://94.200.114.161/VZV5Jd3MI23/CxuKUUt6vB7jg/
Hostname: 94.200.114.161
IP Address:
Port: 80
Count: 1

http://139.99.158.11:443/bvody2/
Hostname: 139.99.158.11:443
IP Address:
Port: 443
Count: 1

http://220.245.198.194/VmL1vd7ycXcP7eIrpF/heV6/o1j3GTfi/
Hostname: 220.245.198.194
IP Address:
Port: 80
Count: 1

http://62.30.7.67:443/Lb9x7OC0ZqL6ogn/Usi7tdfM/
Hostname: 62.30.7.67:443
IP Address:
Port: 443
Count: 1

42 Host(s) detected

IP Address	Hostname	Reverse DNS
95.213.236.64		festihouse.com.
95.179.229.244		95.179.229.244.vultr.com.

94.23.237.171		ns308512.ip-94-23-237.eu.
94.23.216.33		ns305011.ip-94-23-216.eu.
94.200.114.161		
91.211.88.52		
89.216.122.92		cable-89-216-122-92.static.sbb.rs.
87.106.136.232		s16222592.onlinehome-server.info.
84.39.182.7		static.masmovil.com.
83.169.36.251		lvps83-169-36-251.dedicated.hosteurope.de.
82.80.155.43		bzq-82-80-155-43.red.bezeqint.net.
78.24.219.147		smitbakin.ru.
71.72.196.159		cpe-71-72-196-159.cinci.res.rr.com.
62.75.141.82		static-ip-62-75-141-82.inaddr.ip-pool.com.
62.30.7.67		67.7-30-62.static.virginmediabusiness.co.uk.
61.19.246.238		
50.35.17.13		
47.144.21.12		47-144-21-12.lsan.ca.frontiernet.net.
220.245.198.194		220-245-198-194.static.tpgi.com.au.
213.196.135.145		catv-135-145.tbwil.ch.
209.141.54.221		
203.153.216.189		server.discovery.co.id.
200.123.150.89		customer-static-123-150-89.iplannetworks.net.
188.219.31.12		net-188-219-31-12.cust.vodafonedsl.it.
187.161.206.24		187.161.206.24-clientes-izzi.mx.
185.94.252.104		gateway.wlan.ffm.megaservers.de.
181.169.34.190		190-34-169-181.fibertel.com.ar.

176.111.60.55		55.60.111.176.united.net.ua.
174.45.13.118		174-045-013-118.res.spectrum.com.
172.91.208.86		cpe-172-91-208-86.socal.res.rr.com.
157.245.99.39		157.245.99.39-e2-8080.
156.155.166.221		156-155-166-221.ip.internet.co.za.
153.137.36.142		p3460142-ipngn824hodogaya.kanagawa.ocn.ne.jp.
139.99.158.11		11.ip-139-99-158.net.
139.162.108.71		li1592-71.members.linode.com.
137.59.187.107		
134.209.36.254		
124.41.215.226		
120.138.30.150		
107.5.122.110		c-107-5-122-110.hsd1.mi.comcast.net.
104.236.246.93		
1.221.254.82		

25 Countr(y|ies) detected

Hosts	Country
10	United States
3	Germany
3	France
2	Japan
2	Russian Federation
2	Argentina
2	Australia

1	South Africa	
1	Ukraine	
1	Mexico	
1	Greece	
1	Singapore	
1	Korea, Republic of	
1	New Zealand	
1	Nepal	
1	Italy	
1	United Arab Emirates	
1	United Kingdom	
1	Serbia	
1	Israel	
1	Thailand	
1	unknown	
1	Indonesia	
1	Switzerland	
1	Iran, Islamic Republic of