dosemu.exe

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

MalFamily: Fareit **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	16.00 KB (16384 bytes)
Compile time:	2017-10-24 00:12:14
MD5:	c1e8dfad2f325fd08778ca47118e6b40
SHA1:	a3e2dcba398e7100540ff1e3bd61d58e4ae95365
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-10-28 17:09:03

URL(s) file hosting

http://95.215.1.100/dosemu.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-10-27 13:56:54	26/68	

Import library

mscoree.dll

5 Behaviors detected by system signatures

Attempts to execute a powershell command with suspicious parameter/s

- execution_policy: Attempts to bypass execution policy

Creates RWX memory

A process created a hidden window

- Process: dosemu.exe -> powershell.exe

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
- ip_hostname: HTTP connection was made to an IP address rather than domain name
- suspicious_request: http://95.215.1.100/zoo_mage.ocx

Performs some HTTP requests

- url: http://95.215.1.100/zoo_mage.ocx

1 HTTP Request(s) detected

http://95.215.1.100/zoo_mage.ocx
Hostname: 95.215.1.100
IP Address:
Port: 80
Count: 1

1 Host(s) detected

IP Address	Hostname	Reverse DNS
95.215.1.100		

1 Countr(y|ies) detected

Hosts	Country
1	Russian Federation