Redosdru.V Malware that hides in encrypted DLL files to avoid detection by Firewalls

securitynews.sonicwall.com/xmlpost/redosdru-v-malware-that-hides-in-encrypted-dll-files-to-avoid-detection-by-firewalls-may-112016/

May 11, 2016

The Dell Sonicwall Threats Research team observed reports of a New Malware family named **GAV: Redosdru.V** actively spreading in the wild. This time attackers used a dropper to download the original Malware that hides in encrypted DLL files to avoid detection by Firewalls.

```
.data:004040B0 aA6say2ya6srpmp db 'A6say2yA6SRpMPhldVejrlYY0vdWmPsu4GcI1XpBUThrPH2jOqWSzpRn8s6Nk/4Qm'
.data:004040B0                                         ; DATA XREF: sub_401D80+163To
.data:004040B0                 db 'xqAJdw9GDILp1Q2w/3A9yF1fDHx6VZ6+7NJ49r+0+DrXSBA7bydgMALqA9Y3jghCN'
.data:004040B0                 db 'N6FAwEZx1MY0cJrsPGIz/26MY7tXD2p73Jq2UfTtbEMHHOh75N3B0/PE0HHry61XY'
.data:004040B0                 db 'ijRQOnDa5H2CcBOhHXkCx05X4Xebs8Bs54R7N26EwS2wNeAVpTUfesAPHjjNEGypo'
.data:004040B0                 db 'U9Spv7a4EOZYNcntY+cnhOFFD0vRCWP1Xg9YV9dha33maQ1YiXYal9+kQdF/Eg4KM'
.data:004040B0                 db 's68KK/aqDdMqLD2BpFbCNAtXbDi07KaB1rYCGHMIeNtDb0fq5wESiuwofaS+wEdax'
.data:004040B0                 db 'rh7+p6k1e9ExyGs6Fx/LbKnvzbM9S5dNDFWPYyfGQbuw6KFJNRti98X26ruKAgoBF'
.data:004040B0                 db 'L9u4fO3PwMYCEfuq9eCTae0KK7noAmg==',0
```

Infection Cycle:

Md5:

807db66fd414f3eb5e74e10fc4309ae3

The Malware adds the following files to the system:

Malware.exe

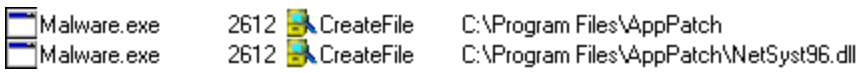
- C:Program FilesAppPatchNetsyst96.dll
- C:Program FilesMicrosoft FduoodFduzjyw.exe

The Trojan adds the following keys to the Windows registry to ensure persistence upon reboot:

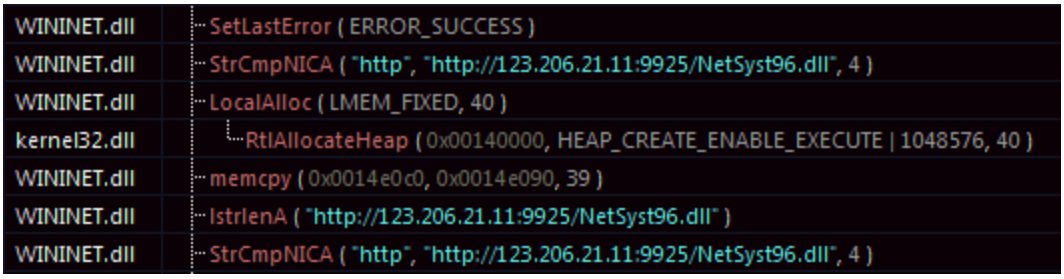
HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun

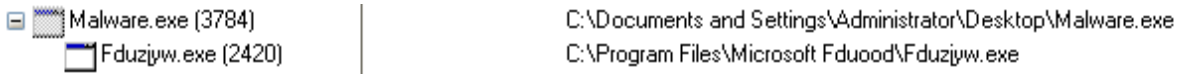
Wsejti gzuaqwud=C:Program FilesMicrosoft FduoodFduzjyw.exe

Once the computer is compromised, the malware copies its own files to **AppPatch** folder.



The Malware tries to download encrypted DLL file from its own C&C server from following domain:





Here is an example of encrypted DLL file:

Command and Control (C&C) Traffic

Redosdru.V performs communication over 9925 and 60321 ports. The malware sends your system information to its own C&C server via following format, here is an example:

PID	Port Number	Port Type	Processes	Host Address	Remote Port
2612	1114	TCP	Malware.exe	123.206.21.11	9925
4	445	TCP	System	0.0.0.0	
960	135	TCP	svchost.exe	0.0.0.0	
4	139	TCP	System	0.0.0.0	
1008	123	UDP	svchost.exe		

PID	Port Number	Port Type	Processes	Host Address	Remote Port
1804	1037	TCP	Fduzjyw.exe	198.70.67.16	80
1804	1038	TCP	Fduzjyw.exe	69.12.77.204	60321
4	445	TCP	System	0.0.0.0	
960	135	TCP	svchost.exe	0.0.0.0	
1796	1029	TCP	alg.exe	0.0.0.0	
4	139	TCP	System	0.0.0.0	
1056	123	UDP	svchost.exe		
704	500	UDP	lsass.exe		

Stream Content

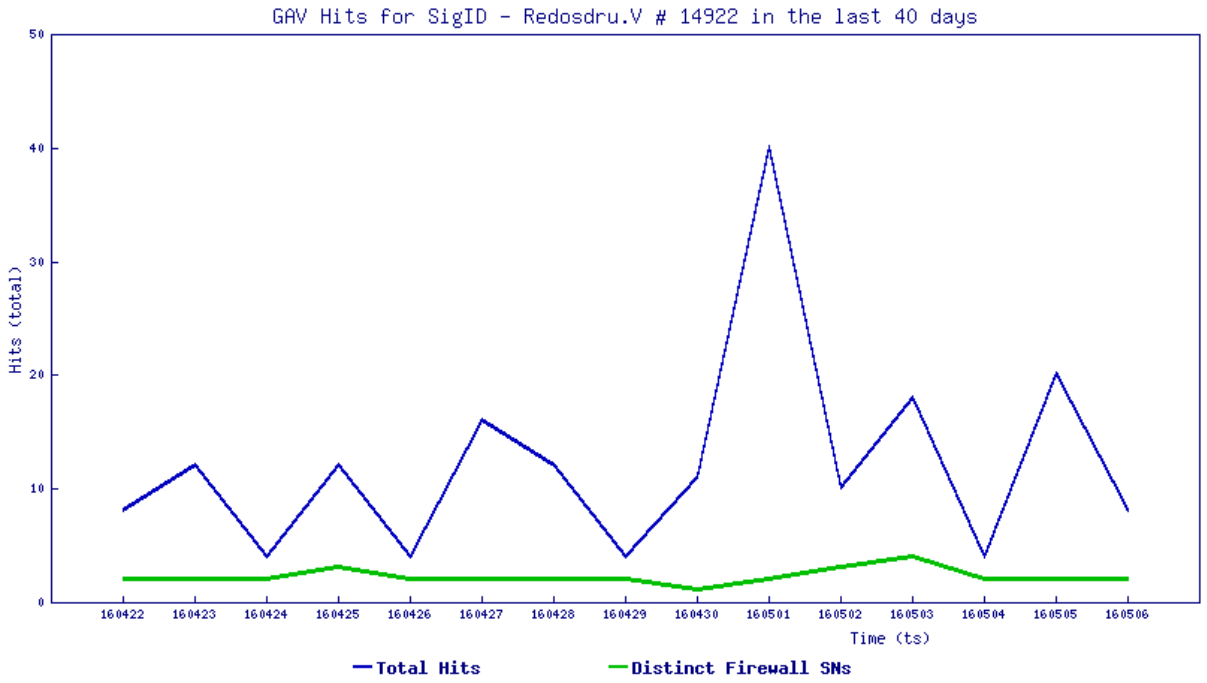
```
s..O;.-......!%W.x...d..eF 1..Y.....b``....Ee...
....
..t.. ..."........@...O.. .r.X...i.....&i.f.&.&.......{T1..ycxj....k.6a.z.fv
!.f...F.F..f.....f
.&V&..G..8........l_t.....[P'.
```

```
GET /fcg-bin/cgi_get_portrait.fcg?uins=12345678 HTTP/1.1
Host: users.qzone.qq.com

HTTP/1.1 200 OK
Server: QZHTTP-2.37.1
Cache-Control: max-age=86400
Content-Type: text/html
Content-Length: 109
Connection: keep-alive

portraitCallBack({"12345678":["http://qlogo3.store.qq.com/qzone/12345678/12345678/100",79940,-1,4,0,1,"",0]})
```

We have been monitoring varying hits over the past few days for the signature that blocks this threat:



Total hits for signature: 183

SonicWALL Gateway AntiVirus provides protection against this threat via the following signature:

GAV: Redosdru.V (Trojan)