TM Follow-Up (TAG_APT35_14/10/21)

medium.com/@ThreatMiner/tm-follow-up-tag-apt35-14-10-21-72134fab9aea

ThreatMiner October 20, 2021

ThreatMiner

Oct 20, 2021

.

3 min read

The purpose of these entries is to enrich provided IOCs, provide information discovered by our analysts (in some cases this will be new information not shared in the initial report) and provide a springboard for more analysis/research possibilities.

ThreatMiner is going to be doing these more regularly going forward.

Stay Tuned…

Blog URL:

Example Analysis Report:

APK Sample:

MD5:8a847b0f466b3174741aac734989aa73
SHA-1:03eadb4ab93a1a0232cb40b7d2ef179a1cd0174d
SHA-256:5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5
File Size: 11.75 MB
Package Name: com.example.vpnner
Main Activity: com.example.vpnner.MainActivity

Possible other name (internal?) for APK: “Dragon VPN”

```
private void startMyOwnForeground() {
    NotificationChannel notificationChannel = new NotificationChannel("com.example.application", "Dragon VPN", 0);
    notificationChannel.setLightColor(-16776961);
    notificationChannel.setLockscreenVisibility(0);
    ((NotificationManager) getSystemService("notification")).createNotificationChannel(notificationChannel);
```

com.example.vpnner.MainService

Activities:

com.example.vpnner.**RepeatActivity**
com.example.vpnner.**DiallingActivity** *(Typo)*
com.example.vpnner.**SMSActivity**
com.example.vpnner.**CameraActivity**
com.example.vpnner.**AucioRecorderActivity** *(Typo)*
com.example.vpnner.**CallLogsActivity**
com.example.vpnner.**AccessStorageActivity**
com.example.vpnner.**LocationActivity**
com.example.vpnner.**READCONTACTSActivity**
com.example.vpnner.**ShotActivity**
com.example.vpnner.**MainActivity**
de.blinkt.openvpn.DisconnectVPNActivity
com.example.vpnner.**FullScreenActivity**
com.example.vpnner.**LockScreenActivity**
com.google.android.gms.common.api.GoogleApiActivity

Service(s):

de.blinkt.openvpn.core.OpenVPNService
com.example.vpnner.**MainService**
com.example.vpnner.**MyJobIntentService**

Receiver(s):

com.example.vpnner.**StartActivityOnBootReceiver**
com.example.vpnner.**NotificationReceiver**

Constant(s):

```
package com.example.vpnner;

import android.os.Environment;

public class Constants {
    public static String ApplicationName = "SaferVPN";
    public static String Base_Path = Environment.getExternalStorageDirectory().getAbsolutePath();
    public static String DCIM_Folder_Path = Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_DCIM).getAbsolutePath();
    public static String Domain = "http://cdsa.xyz";
    public static String Download_Folder_Path = Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_DOWNLOADS).getAbsolutePath();
    public static String Internal_Storage_Folder_Path = Environment.getExternalStorageDirectory().getAbsolutePath();
    public static String Movies_Folder_Path = Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_MOVIES).getAbsolutePath();
    public static String Pictures_Folder_Path = Environment.getExternalStoragePublicDirectory(Environment.DIRECTORY_PICTURES).getAbsolutePath();
    public static String Server_BigDownload = "Api/AndroidBigDownload";
    public static String Server_Download = "Api/AndroidDownload";
    public static String Server_GetPublicIp = "Api/GetPublicIp";
    public static String Server_HttpModuleData = "Api/AndroidHttpModuleData";
    public static String Server_HttpModuleDataAppend = "Api/HttpModuleDataAppend";
    public static String Server_IsRunAudioRecorder = "Api/IsRunAudioRecorder";
    public static String Server_IsRunClipboard = "Api/IsRunClipboard";
    public static String Server_IsRunGPS = "Api/IsRunGPS";
    public static String Server_Session = "Api/Session";
    public static String Server_TargetLog = "Api/AndroidTargetLog";
    public static String TargetName = "Target1";
    public static String Target_Photo_Folder_Name = "Photo";
    public static String Target_Program_Folder_Name = "AndMal";

    public static class MessageEvent {
    }
}
```

com.example.vpnner.Constants

URI:

/Api/AndroidBigDownload
/Api/AndroidDownload
/Api/GetPublicIp
/Api/AndroidHttpModuleData
/Api/HttpModuleDataAppend
/Api/IsRunAudioRecorder
/Api/IsRunClipboard
/Api/IsRunGPS
/Api/Session
/Api/AndroidTargetLog

Defined Module(s):

“RequestPermissionsModule”
“DownloadModuleStop”
“ClipboardModuleStop”
“ScreenshotModuleStop”
“DownloadModule”
“FileManagerModule”
“ContactsModule”
“CellInfoLocationModule”
“GPSModule”
“MonitorPermissionsModule”
“DiallingModule”
“ReadSMSModule”
“SendSMSModule”
“ApplicationsModule”

“CallLogsModule”
“CameraModule”
“AudioModuleStop”
“Audio”
“ClipboardModule”
“ScreenshotdModule”

Additional domain(s) discovered:

westernrefrigerator[.]xyz [VPN endpoint]

Resolve IP(s):

- 94[.]23[.]152[.]211 [OVH SAS | AS16276]
- 135[.]125[.]21[.]240 [OVH SAS | AS16276]

IP/Domain Relationship(s)*:

IP resolve history for domains listed as IOCs — “**[multiple]**” indicates the given IP has been associated with more than 1 of the listed domain IOCs (provided in TAG reporting)

94[.]23[.]152[.]211 [westernrefrigerator[.]xyz] [single]
51[.]254[.]172[.]178 [cdsa[.]xyz] [single]
151[.]106[.]5[.]167 [communication-shield[.]site] [single]
192[.]155[.]108[.]153 [communication-shield[.]site] [single]
192[.]155[.]108[.]152 [communication-shield[.]site] [single]
192[.]155[.]108[.]158 [communication-shield[.]site] [single]
151[.]106[.]5[.]166 [communication-shield[.]site] [single]
5[.]135[.]250[.]245 [identifier-service-review[.]site] **[multiple]**
5[.]135[.]250[.]245 [verify-service-activity[.]site] **[multiple]**
188[.]165[.]133[.]122 [recovery-service-activity[.]site] [single]
51[.]254[.]25[.]200 [recovery-activity-identification[.]site] **[multiple]**
51[.]254[.]25[.]200 [review-session-confirmation[.]site] **[multiple]**
178[.]32[.]138[.]103 [service-activity-session[.]online] [single]
94[.]23[.]76[.]54 [customers-verification-identifier[.]site] [single]
185[.]224[.]138[.]25 [accessverification[.]online] [single]
192[.]254[.]231[.]253 [continuetogo[.]me] [single]
192[.]185[.]0[.]218 [filetransfer[.]club] [single]
192[.]185[.]32[.]98 [filetransfer[.]club] [single]
209[.]99[.]40[.]222 [filetransfer[.]club] [single]
68[.]65[.]123[.]232 [summit-files[.]com] [single]
85[.]10[.]193[.]10 [nco2[.]live] [single]
199[.]59[.]242[.]153 [service-reset-password-moderate-digital[.]rf[.]gd] **[multiple]**

199[.]59[.]243[.]200 [service-reset-password-moderate-digital[.]rf[.]gd] **[multiple]**
199[.]59[.]242[.]153 [reset-service-identity-mail[.]42web[.]io] **[multiple]**
199[.]59[.]243[.]200 [reset-service-identity-mail[.]42web[.]io] **[multiple]**
185[.]27[.]134[.]133 [reset-service-identity-mail[.]42web[.]io] [single]
199[.]59[.]243[.]200 [reset-service-identity-mail[.]42web[.]io] **[multiple]**
199[.]59[.]242[.]153 [digital-email-software[.]great-site[.]net] **[multiple]**

++

Unique IPs with overlap*:

199[.]59[.]243[.]200 [Bodis, LLC]
199[.]59[.]242[.]153 [Bodis, LLC]
51[.]254[.]25[.]200 [OVH SAS]
5[.]135[.]250[.]245 [OVH SAS]

++

Unique IPs*:

51[.]106[.]5[.]166
151[.]106[.]5[.]167
178[.]32[.]138[.]103
185[.]224[.]138[.]25
185[.]27[.]134[.]133
188[.]165[.]133[.]122
192[.]155[.]108[.]152
192[.]155[.]108[.]153
192[.]155[.]108[.]158
192[.]185[.]0[.]218
192[.]185[.]32[.]98
192[.]254[.]231[.]253
199[.]59[.]242[.]153
199[.]59[.]243[.]200
209[.]99[.]40[.]222
51[.]254[.]172[.]178
51[.]254[.]25[.]200
5[.]135[.]250[.]245
68[.]65[.]123[.]232
85[.]10[.]193[.]10
94[.]23[.]152[.]211
94[.]23[.]76[.]54

*IPs are low fidelity IOCs — but are being listed as base pivots for additional research