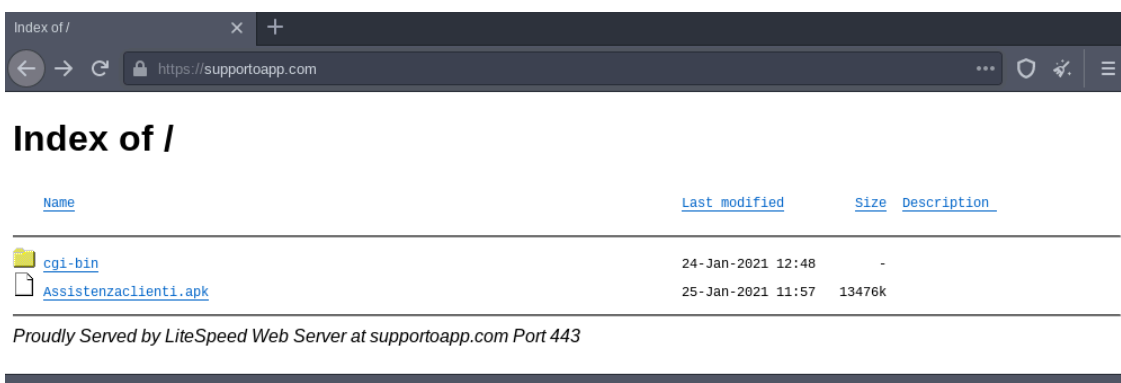


Individuato sito che veicola in Italia un APK malevolo

Archived: 2026-04-05 16:03:33 UTC

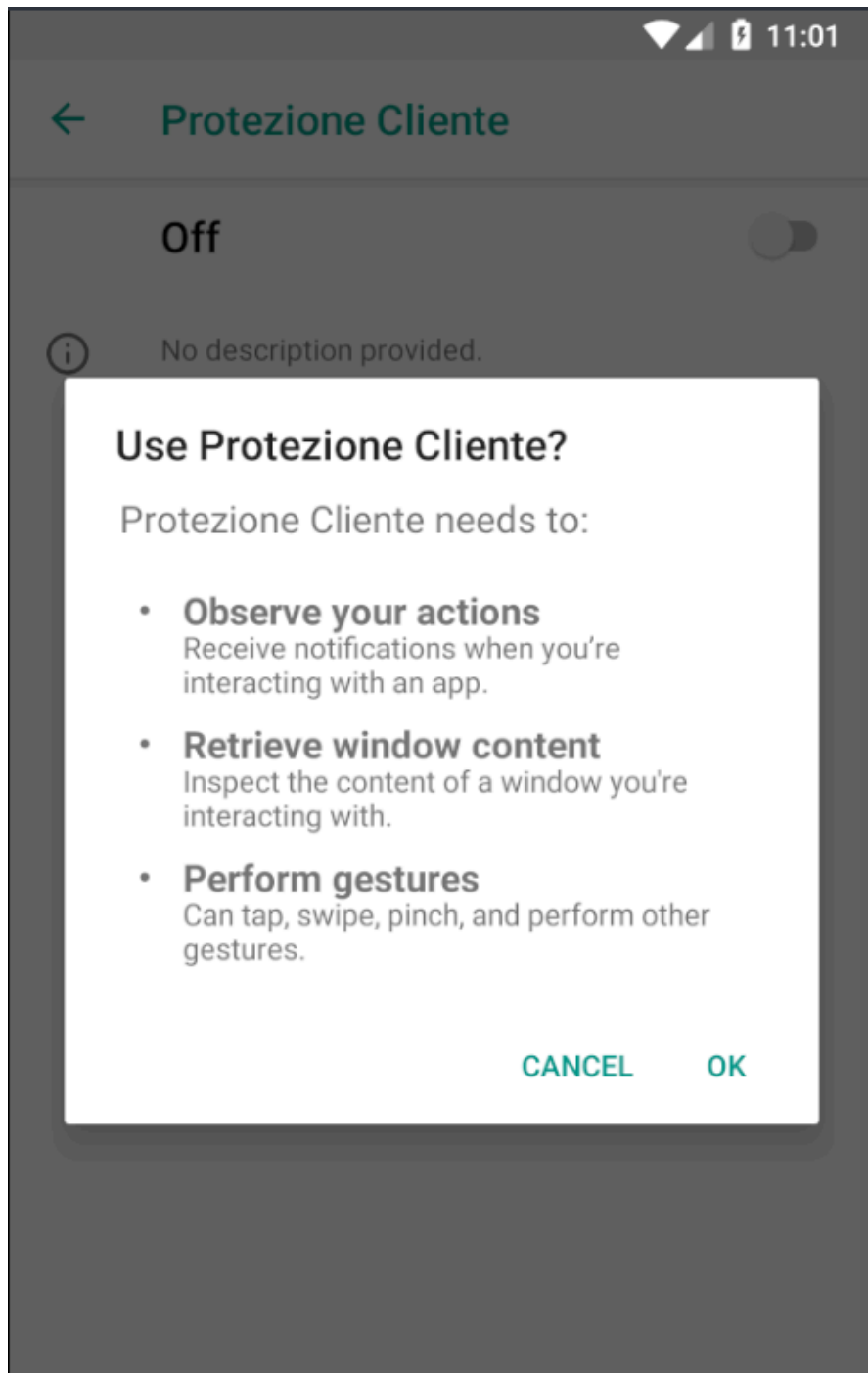
25/01/2021

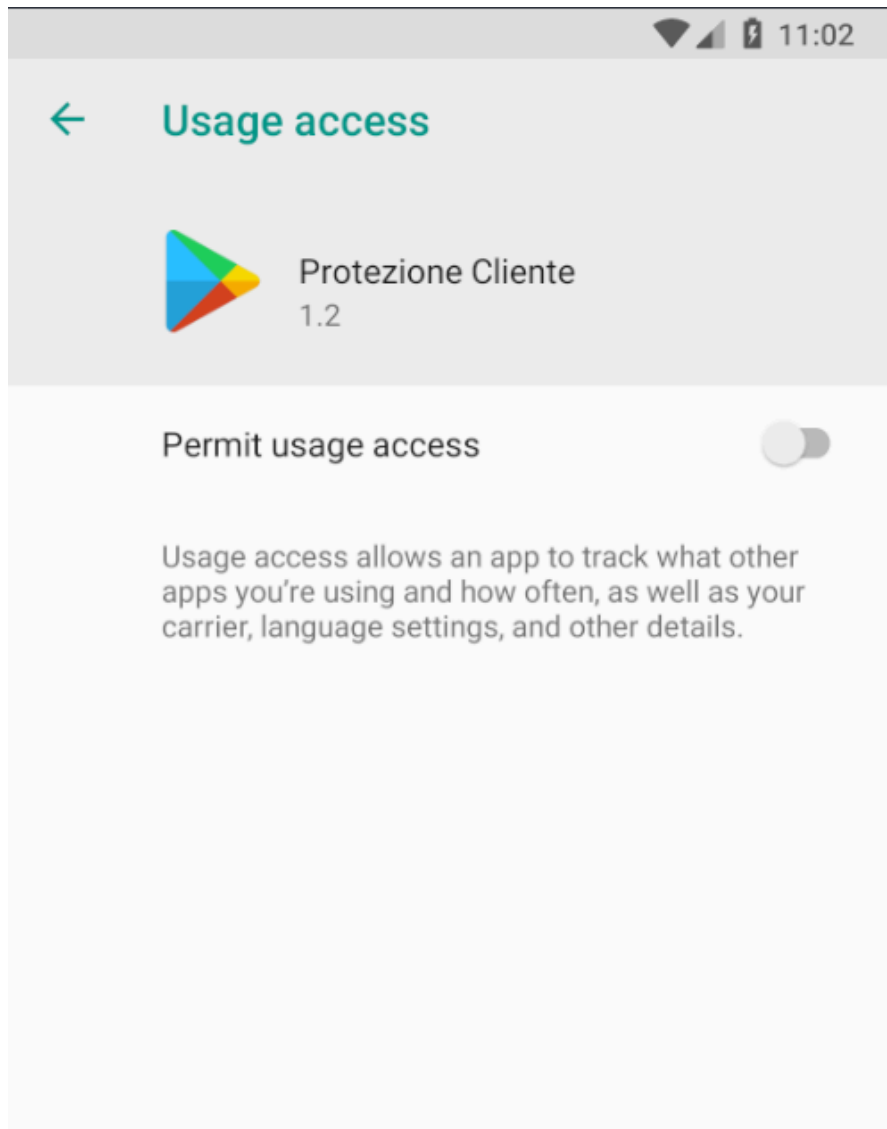
[apk](#)



In data odierna è stato individuato da [AddressIntel](#) un dominio denominato “supportoapp[.]com” dal quale è possibile scaricare il file “Assistenzaclienti.apk” caricato sul server remoto in data odierna.

Una volta installata l’app, che si presenta con il nome “Protezione Cliente“, viene richiesto all’utente di abilitare il servizio di accessibilità che servirà per attivare le funzionalità di keylogger e per accedere ad una serie di permessi.





I permessi richiesti permettono di mostrare pagine di phishing all'apertura di specifiche app. Di seguito la lista dei permessi di cui l'app necessita:

```
CALL_PHONE  
CAMERA  
DISABLE_KEYGUARD  
INTERNET  
READ_PHONE_STATE  
READ_SMS  
RECEIVE_MMS  
RECEIVE_SMS  
RECORD_AUDIO  
SEND_SMS  
SYSTEM_ALERT_WINDOW  
WRITE_EXTERNAL_STORAGE  
WRITE_SMS  
INJECT_EVENTS
```

```
PACKAGE_USAGE_STATS
READ_PRIVILEGED_PHONE_STATE
ACCESS_NETWORK_STATE
ACCESS_SUPERUSER
MODIFY_AUDIO_SETTINGS
READ_EXTERNAL_STORAGE
RECEIVE_BOOT_COMPLETED
REQUEST_DELETE_PACKAGES
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
REQUEST_INSTALL_PACKAGES
WAKE_LOCK
```

Appena concessi i permessi, viene effettuata una prima chiamata a “*checkip.amazonaws.com*” da cui ricava l’indirizzo IP del dispositivo compromesso e successivamente dialoga con il C2 a questo indirizzo: “*montanatomy[.]xyz*” sulla porta 443.

Il dominio del C2 è riportato in chiaro all’interno dell’APK ma i comandi per le successive query vengono ottenute dalla decodifica di una serie di stringhe cifrate con AES-CBC e chiave embedded.

```
ZVDq6XmPwgPwcyf+mpEchW==      prefs
rX4t/n/rHgnfD8vgAeYUtg==      botid
zEe3Vzvs4Ro7gGk/dyzSPw==      uplink
a7RxrCCIyPmL5VS5fG+ZYQ==      sgen
aWIhQJz8zaEgGmKnzUvCyA==      true
yHaqJjTy5ioS10C/XjMSzw==      false
hSUMJLYzj0bUŁZVEjsn+/w==      SCREEN TRND OFF
rpe153hSko9oUfzqsHuuag==      upsms
4A4EŁ5wEF3s0j+f1wmAVzWJVArpMVL2bgVqHytv1Wbg= uploads/injects/
0KLegoWAi55moyFK/a0ipw==      8219AM7Z12
5V4Fcp09IQDkpUe0La/wxQ==      command
R8txzKaApEN5LQeXUI6MeQ==      Android
nJhmr4steszQKVJISDRoQ5Q==      php?p=
9QGDDuTgW5oPFGWJLj fMkg==      /block.txt
AvmYjBo4IgbmaQ9vnTMvhw==      Jedi
H70wGnG6tdouqxheEiUYbQ==      /Injections.txt
TDSennm0Lo19z7fP6/w9pA==      typ
SxQ2H2zŁ+pHxY8MZF4VY3Q==      Injections.txt
AF+MX/qPdTmaDNw3NN4log==      tapp
zUTpVSlnBS9Xpa4tH+AARw==      app/device/ping
M3qwp3WnfjLJjhh159nPxw==      app/device/
EM0KB4K4hAdłSN5FN4sDjg==      app/device/sms
5WFhGNwtv2v+KSAwEzRŁ+w==      ping
```

```
public class C0526g {  
    /* renamed from: Xz */  
    public static String f1764Xz = "https://montanatomy.xyz/api/";  
    /* renamed from: Yz */  
    public static String f1765Yz = "https://montanatomy.xyz";  
    /* renamed from: Zz */  
    public static String f1766Zz = "RHBuUXFEhkrbrHaYIZ6VYH3uNIBRnwTe";  
    /* renamed from: _z */  
    public static String f1767_z = "ZVDq6XmPwgPwcyf+mpEcHw==";  
    /* renamed from: aA */  
    public static String f1768aA = "rX4t/n/rHgnfD8vgAeYUtg==";  
    /* renamed from: bA */  
    public static String f1769bA = "zEe3Vzvs4Ro7gGk/dyzSPw==";  
    /* renamed from: cA */  
    public static String f1770cA = "a7RxrCCIyPmLVSSfG+ZYQ==";  
    /* renamed from: dA */  
    public static String f1771dA = "aWIhQJz8zaEgGmKnzUvCyA==";  
    /* renamed from: eA */  
    public static String f1772eA = "yHaqJjTy5ioS10C/XjMSzw==";  
    /* renamed from: fA */  
    public static String f1773fA = "hSumJLYzj0bULZVEjsn+/w==";  
    /* renamed from: gA */  
    public static String f1774gA = "rpe153hSko9oUfzqsHuuag==";  
    /* renamed from: hA */  
    public static String f1775hA = "4A4EL5wEF3s0j+f1wmAVzWJVaRpMVL2bgVqHytv1wbg=";  
    /* renamed from: iA */  
    public static String f1776iA = "OKLegoWai55moyFK/a0ipw==";  
    /* renamed from: jA */  
    public static String f1777jA = "5V4Fcp09IQDkpUe0La/wxQ==";  
    /* renamed from: kA */  
    public static String f1778kA = "R8txzKaApENSLQeXUI6MeQ==";  
}
```

A sinistra le stringhe decifrate, a destra il codice sorgente dell'APK con il C2 in chiaro

Secondo [VirusTotal](#) il sample viene riconosciuto come un generico malware Android/Banker, quale in realtà è ma, al momento, questo malware non viene associato a nessuna famiglia e/o campagna già nota.

Source: <https://cert-agid.gov.it/news/individuato-sito-che-veicola-in-italia-un-apk-malevolo/>