Domestic Kitten: an Iranian surveillance program

Wednesday 2 October 14:00 - 14:30, Green room

Aseel Kayal (Check Point)
Lotem Finkelstein (Check Point)

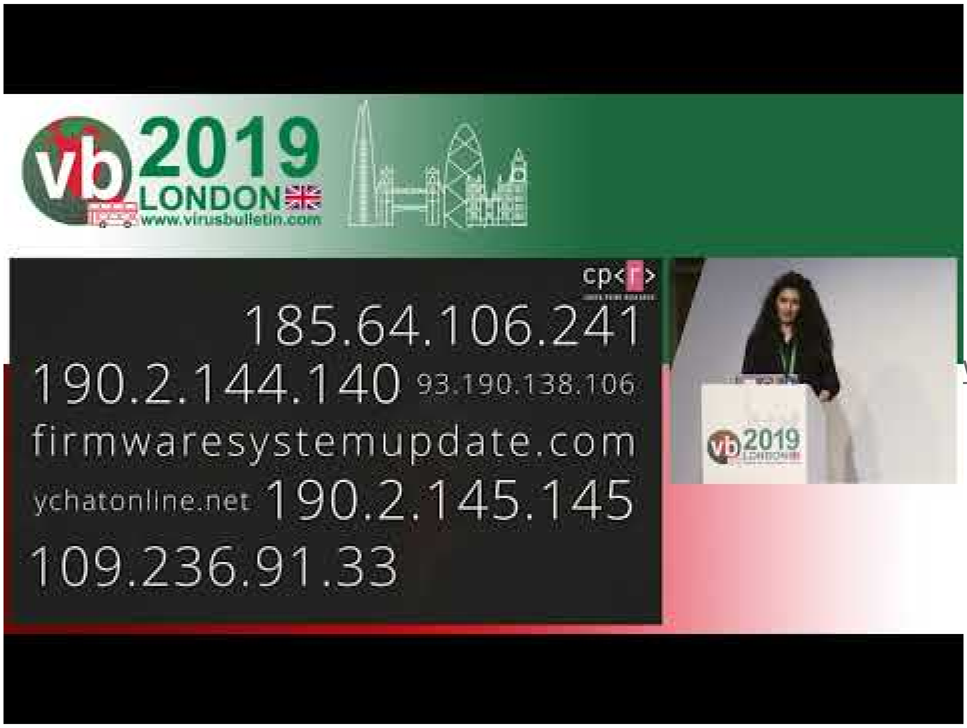
In a fundamental regime that is constantly wary of anything that might jeopardize its stability, and a region that is a hotbed of political conflicts and dissensions, it is not surprising to discover a large-scale surveillance campaign that keeps an eye out not only for external threats, but also for internal ones.

Lately we uncovered an operation dubbed "Domestic Kitten", which uses malicious *Android* applications to steal sensitive personal information from its victims: screenshots, messages, call logs, surrounding voice recordings, and more. This operation managed to remain under the radar for a long time, as the associated files were not attributed to a known malware family and were only detected by a handful of security vendors.

Whether it is an application that changes the device's background into ISIS-related images, or one that impersonates a legitimate Kurdish news agency, the malicious APKs used by this actor were tailored for the use of specific ethnic groups. Those ethnic groups and minorities can be considered a natural enemy to the Islamic Republic of Iran: Kurds, ISIS supporters, Sunni Muslims, and even Iranian citizens.

Our suspicions of the attack's origin were confirmed when we were able to gain access to logs that were uploaded from the victims' infected devices to the C2 servers. The information we gathered from those findings also revealed the true dimensions of the attack as well as its lifespan, with the earliest malicious instances dating back to 2016.

In our presentation, we will discuss the evolution of the mobile spyware, the Iranian fingerprints it carries, and the political motives behind the launch of such an attack. In addition, we will share never-before-seen insights into the data stolen from hundreds of victims.



185.64.106.241
190.2.144.140 93.190.138.106
firmwaresystemupdate.com
ychatonline.net 190.2.145.145
109.236.91.33

Watch Video At:

https://youtu.be/pW4pfIyfO_4

Related links

- Domestic Kitten: An Iranian Surveillance Operation (*Check Point*)
- Zooming In On "Domestic Kitten" (*Check Point*)
- Mobile Cyberespionage Campaign ‘Bouncing Golf’ Affects Middle East (*Trend Micro*)

Aseel Kayal

Aseel is a malware analyst at *Check Point Research*. She joined *Check Point* as a security analyst in 2016. She received her Bachelor's degree in computer science and English literature, and speaks Arabic, Hebrew and English. Aseel's research mainly focuses on threat groups and cyber attacks in the Middle East. Some of her work has been presented at security conferences such as Virus Bulletin and Botconf.

@CurlyCyber

Lotem Finkelstein

Equipped with years of experience in the field of threat intelligence from his former role as a Major Officer in the Intelligence Forces of Israel, Lotem joined *Check Point*'s Threat Intelligence and Research organization four years ago. While he was completing his B.Sc. degree in communication system engineering at Ben-Gurion University, Lotem took on several roles as malware analyst and a team leader at *Check Point*. During 2018 Lotem took over the threat intelligence department at *Check Point*, focusing his efforts on pinpointing attacks and uncovering large-scale operations.

@Lotemfi