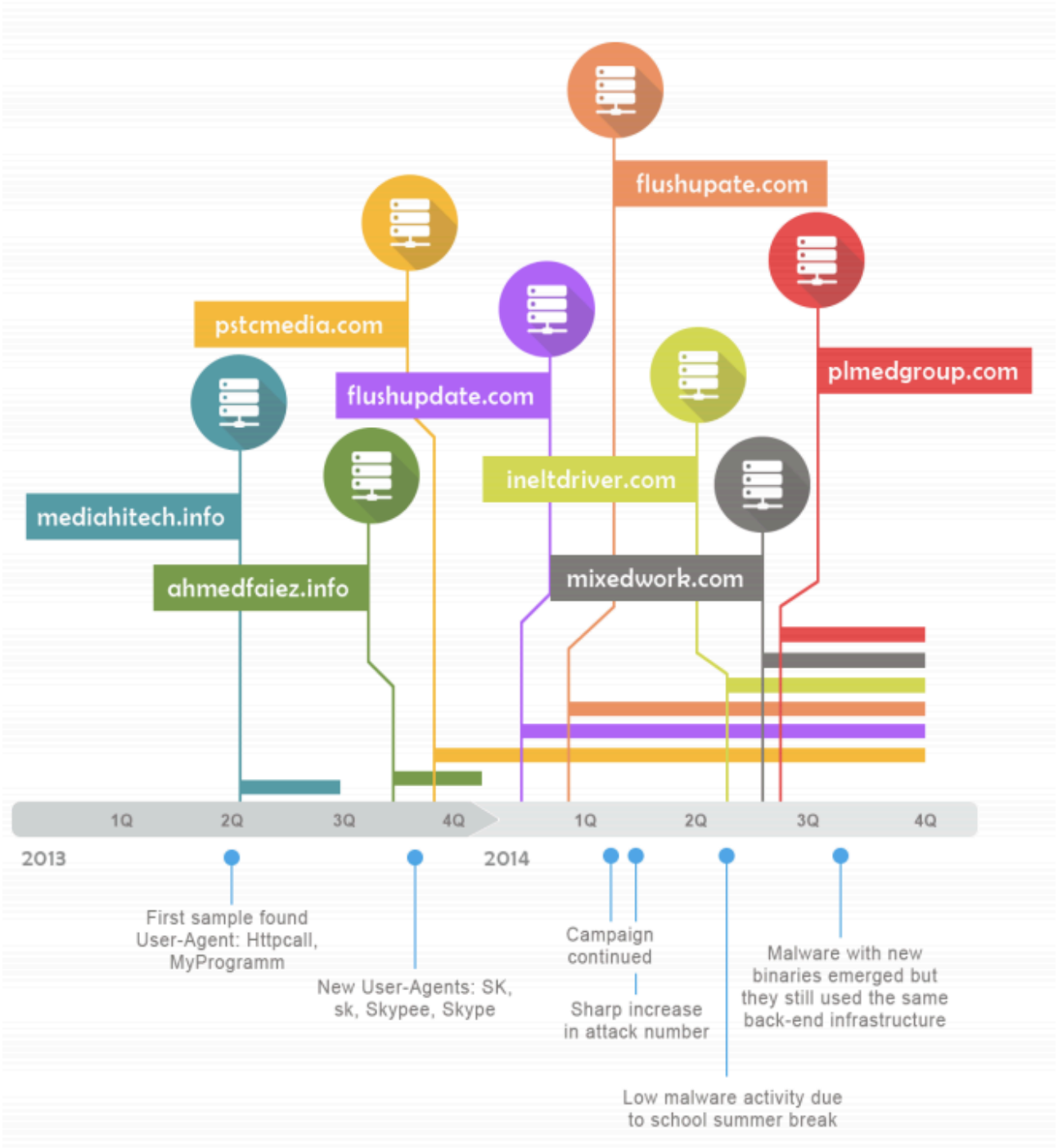
Arid Viper - Israel entities targeted by malware packaged with sex video

By Pierluigi Paganini

Published: 2015-02-19 · Archived: 2026-04-05 14:02:59 UTC

Pierluigi Paganini February 19, 2015



Attackers behind the Arid Viper and the Yanbian Gang exploited sex content for their campaigns against victims in Israel and Kuwait, and South Korea.

Security experts at Trend Micro have uncovered a cyber espionage campaign, dubbed Operation Arid Viper, that targeted Israeli institutions. The Operation Arid Viper is run by Arab-speaking hackers that sought to extract sensitive documents by sending phishing emails. The phishing campaigns targeted government office, infrastructure providers, a military organization and academic institutions in Israel and Kuwait

The particularity of the Operation Arid Viper is represented by the tactic adopted by the attackers to lure victims. The malicious emails sent by hackers include a malware packaged with a short pornographic video.

"This month, actors of Operation Arid Viper and members of the Yanbian Gang jumped on the sexually explicit content bandwagon, using them in separate attacks that target respective victims in Israel and Kuwait, and South Korea. Operation Arid Viper attacked five Israeli-based organizations in the government, transport, infrastructure, military, and academic industries, and one organization in Kuwait using spear-phishing emails that dropped a pornographic video on a victim's computer." reported Trend Micro in a blog post.

The attackers exploit the fact that targeted individuals who might be receiving pornographic video at work and so would hesitate to report the incident, this circumstance allow the malware to remain undetected.

"These victims' failure to act on the threat could have then allowed the main malware to remain undiscovered*." states Trend Micro. "It targeted professionals who might be receiving very inappropriate content at work and so would hesitate to report the* incident*."*

The malware used by Arid Viper once infected the victims' PC searched for Microsoft Office files and text files. It reported the located files to the command and control server, which then decided which files to exfiltrate from the machine.

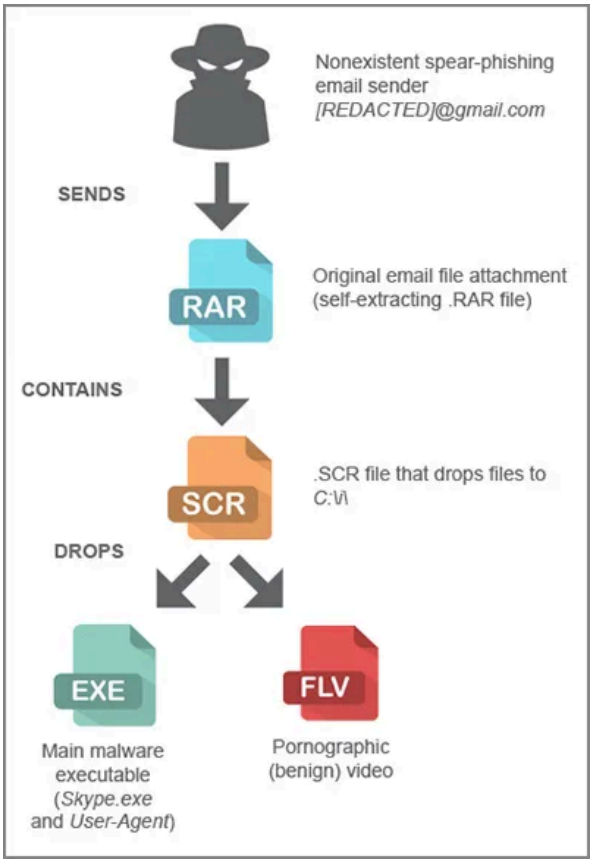
Unfortunately, researchers at Trend Micro reported that the command and control servers used by Arid Viper were "closely locked down, providing a very little hint that could aid our investigation."

The researchers have found a few similarities between the Arid Viper campaign and the Advtravel, including the control infrastructure and the attack kill chain.

The infection Chains for both Operation Arid Viper and Advtravel started with spear-phishing emails that came with a .RAR file attachment that automatically extracts an .SCR file that drops two files when executed.

The Advtravel campaign infected more than 500 systems, the majority of them located in Egypt. The hackers were focused on grabbing screen images from victims' computers, in an attempt to identify victims. Anyway, the experts at Trend Micro consider the operators behind the Advtravel campaign much less skilled than Arid Viper.

"This could be a sign that they are looking for incriminating or compromising images for blackmail purposes," Trend Micro reports. "As such, the attackers may be less-skilled hackers who are not after financial gain nor hacking for espionage purposes."



"The first file is a pornographic video clip, which serves as a social engineering bait while the second file is the actual malware connecting to the C&C servers. Once the second-stage malware is in the system, it sets itself to autorun each time the systems reboot, even posing as an Internet communication software. "

The researchers are spending a great effort in the investigation of the Arid Viper gang, in particular on the way they organized the command and control infrastructure, they suspect a link with possible threat actors to the Gaza Strip. They suggest the existence of a supra-organization behind both campaigns despite they presented different complexity of TTPs.

"Although the malware involved in operation Advtravel *is different from that of Operation Arid Viper, both operations still have a few similarities, such as sharing the same server and having the domains used in* Advtravel *registered with the same emails as the Operation Arid Viper. Notably, the same server and site registration details suggest the existence of a supra-organization, a forum or an influential sponsor could be providing various hacking groups with the means to pursue their ends."*

Let me suggest you to read the report from Trend Micro titled "*OPERATION ARID VIPER – Bypassing the Iron Dome*"

[adrotate banner="9"]	**[adrotate banner="12"]**

Pierluigi Paganini

(Security Affairs – *Arid Viper*, Advtravel)

[adrotate banner=”5″]

[adrotate banner=”13″]

Source: http://securityaffairs.co/wordpress/33785/cyber-crime/arid-viper-israel-sex-video.html