Iranian hackers behind the Magic Hound campaign linked to Shamoon

securityaffairs.co/wordpress/56348/intelligence/magic-hound-campaign.html

February 16, 2017

February 16, 2017 By Pierluigi Paganini

Security researchers discovered cyber espionage operation dubbed Magic Hound campaign that is linked to Iran and the recent Shamoon 2 attacks.

Security experts at Palo Alto Networks have discovered a new cyber espionage campaign linked to Iran that targeted several organizations in the Middle East.

The espionage campaign dubbed Magic Hound, dates back at least mid-2016. Hackers targeted organizations in the energy, government, and technology industries, all the targets are located or have an interest in Saudi Arabia.

The attackers leverage a wide range of custom tools and an open-source cross-platform remote access tool (RAT) dubbed Pupyfor the Magic Hound campaign.

“According to the developer, PupyRAT is a “multi-platform (Windows, Linux, OSX, Android), multi-function RAT and post-exploitation tool mainly written in Python.” CTU™ analysis confirms that PupyRAT can give the threat actor full access to the victim’s system.” reads the analysis published by SecureWorks.

The arsenal of the threat actor includes different types of custom tools such as droppers, downloaders, executable loaders, document loaders and IRC bots.

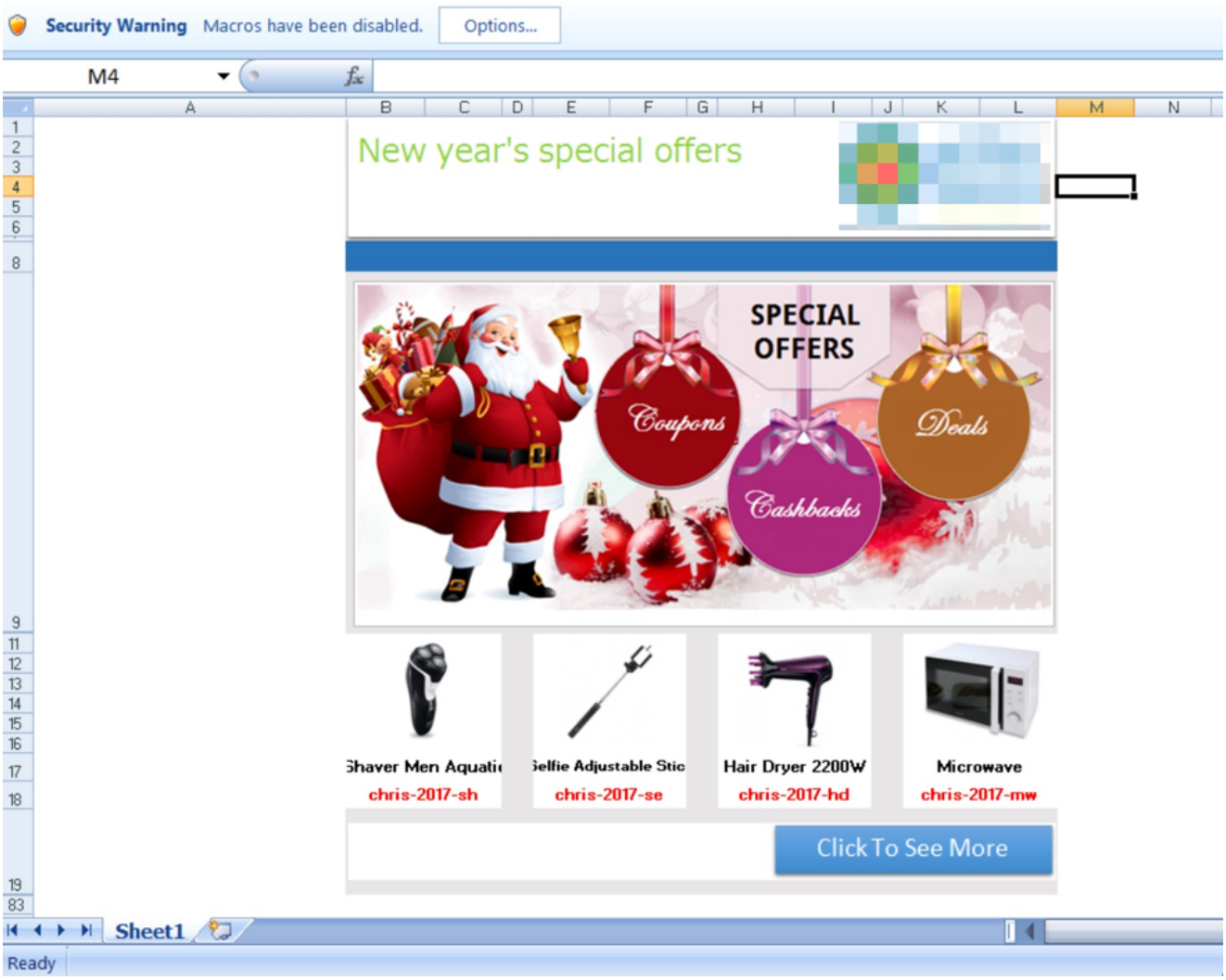
"Unit 42 has discovered a persistent attack campaign operating primarily in the Middle East dating back to at least mid-2016 which we have named Magic Hound. This appears to be an attack campaign focused on espionage. Based upon our visibility it has primarily targeted organizations in the energy, government, and technology sectors that are either in in *or business interests in Saudi Arabia." reads the analysis published by PaloAlto Networks.*

"Link analysis of infrastructure and tools also revealed a potential relationship between Magic Hound and the adversary group called "Rocket Kitten" (AKA Operation Saffron Rose, Ajax Security Team, Operation Woolen-Goldfish) as well as an older attack campaign called Newscasters."

The same campaign was also monitored by experts at SecureWorks that attributed it to a threat actor tracked as COBALT GYPSY that is associated with the Iranian government.

The attackers behind the Magic Hound used Word and Excel documents embedding malicious macros that were able to download and execute additional tools using PowerShell.

The bait files appear to be holiday greeting cards, job offers, and official government documents from the Ministry of Health and the Ministry of Commerce in Saudi Arabia.



An interesting discovery made by the experts is that some of the domains used in the Magic Hound campaign were also uncovered by IBM X-Force researchers in the analysis of the Shamoon 2 attack chain.

According to the experts at Palo Alto Networks an IRC bot used in the Magic Hound campaign is very similar to a piece of malware used by Newscaster, aka Charming Kitten and NewsBeef, an Iranian actor that targeted individuals in the U.S., Israel and other countries using fake social media profiles.

Iranian hackers appear very active in this period, both Charming Kitten and Rocket Kitten actors were mentioned in an analysis of MacDownloader used by to exfiltrate data from Mac computers.

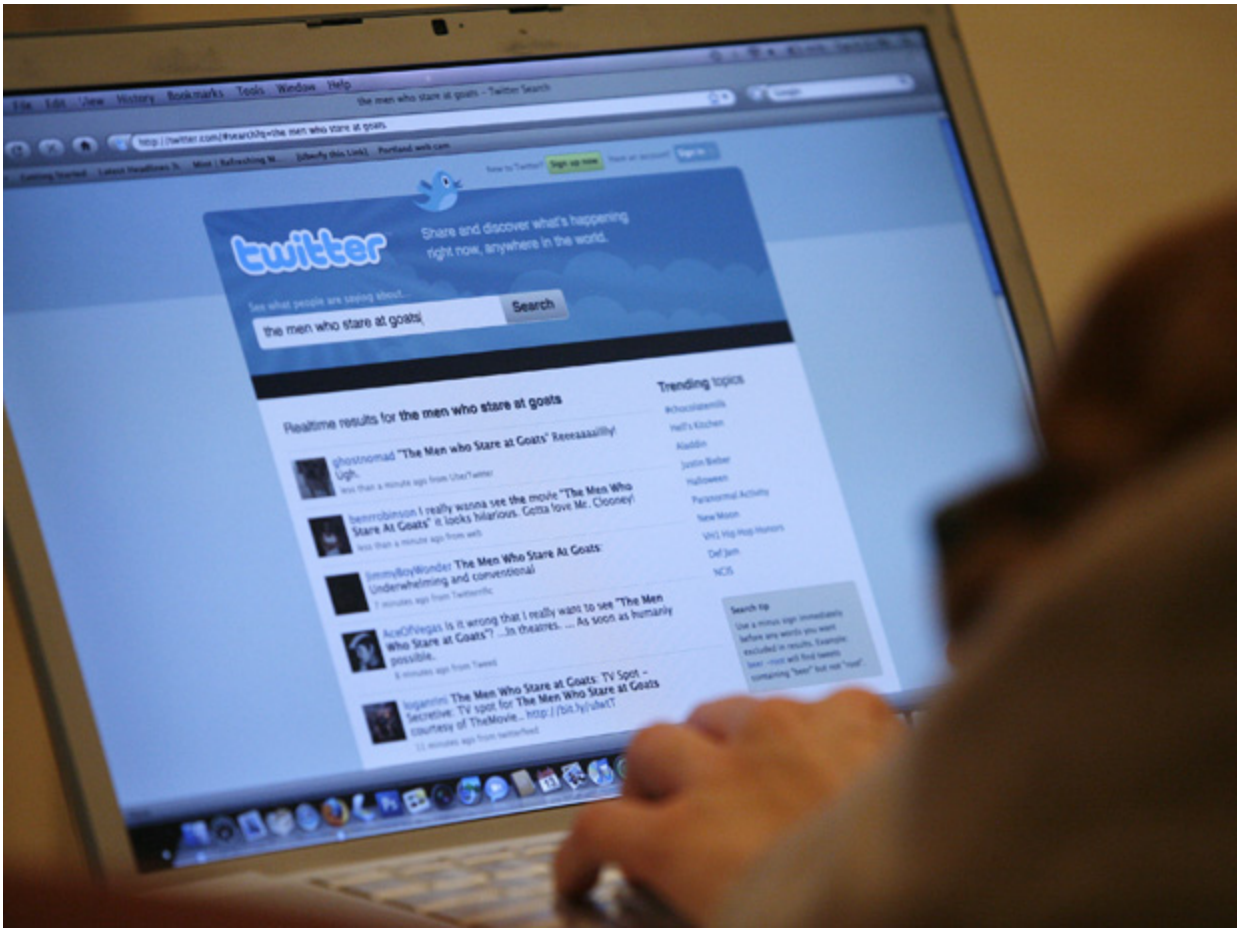
Pierluigi Paganini

(Security Affairs – Magic Hound camapign, Iranian hackers)

Ajax Security Teamcyber espionageIranian hackersMagic HoundOperation Saffron RoseOperation Woolen-GoldfisRocket KittenSaudi Arabia

Share On

You might also like



Ex Twitter employee found guilty of spying for Saudi Arabian government

August 11, 2022 By Pierluigi Paganini

China-linked threat actors have breached telcos and network service providers

June 8, 2022 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations

- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me