The DarkHotel threat actors have been known to operate for a decade now, targeting thousands of businesses across the world via Wi-Fi infrastructure in hotels. Blending whaling (high-level spear phishing) techniques with advanced malware and other complex attack avenues (such as digital certificate factoring), the threat actors have been able to run their business undisturbed for years, except for the few times when samples of DarkHotel malware got documented in blog posts by threat researchers.

Our threat researchers have come across a very particular DarkHotel attack known as Inexsmar, which appears to mark a significant departure from the APT group's traditional modus operandi. This sample dates back to September 2016 and seems to be used in a campaign that targets political figures rather than the usual corporate research and development personnel, CEOs and other senior corporate officials.

This attack uses a new payload delivery mechanism rather than the consacrated zero-day exploitation techniques, blending social engineering with a relatively complex Trojan to infect its selected pool of victims.

An in-depth analysis of this Inexsmar campaign can be downloaded here: Inexsmar: An unusual DarkHotel campaign (2268 downloads)

Tags DarkHotel Inexsmar targeted attack whitepaper

About the author

Bogdan BOTEZATU

Bogdan Botezatu is living his second childhood at Bitdefender as senior e-threat analyst. When believes that most things in life can be beat with strong heuristics and that antimalware research is like working for a secret agency: you need to stay focused at all times, but you get all the glory when you catch the bad guys.

Scavo Iceni

July 23, 2017 at 8:50 pm

Guys,

Can you please do the industry a favour and redeem some credibility?

When you put IoCs into a report, don't make is to that you cannot cut-and-paste the checksums and alike. Doing this is just plain sh*tty. Why make people type IoCs in by hand? Unless of course you intention it to sell them as a premium service. In which case, don't put them in the report at all. Sadly, this isn't the first time I've flagged this up. #notimpressed

Bogdan BOTEZATU

July 24, 2017 at 4:14 pm

Hey there,

Let me rephrase your previous message a little.

"Hey guys! I was looking into your research and I noticed that one can't copy and paste the indicators of compromise at the end of the paper and I thought I'd let you know. Maybe your PDF file is not compatible with other clients or maybe your guy who laid this out forgot to check a box somewhere to export it as text, not as images. Anyway, can you do me a solid and export this in a copy-pasta-friendly manner, cause it's really painful to spell a SHA1 out".

And I'd be like, "Yeah, sure buddy, thanks for letting us know. By the way, here are the IoCs, enjoy!"

RAR archive SHA1: a6c7a7bcaabc3584b1fb4d6aeb66ec158b65d444
Filename: Pyongyang Directory Group email SEPTEMBER 2016 RC_Office_Coordination_Associatewxcod.scr

ZIP archive SHA1: fd99a19b39eb6f1cbf915ee1f73e9e8d62c18b44

7-Zip archive SHA1: 92cc0e7348aa3ee9386b25076868dee72e5193e4

Filename: f_cod.exe