Goblin Panda targets Cambodia sharing capacities with another Chinese group hackers Temp Periscope

medium.com/@Sebdraven/goblin-panda-targets-cambodia-sharing-capacities-with-another-chinese-group-hackers-temp-periscope-7871382ffcc0

Sebdraven September 7, 2018

I keep on my hunting of Goblin Panda and I've just found two new country targeted by them: Cambodia and South Korea.

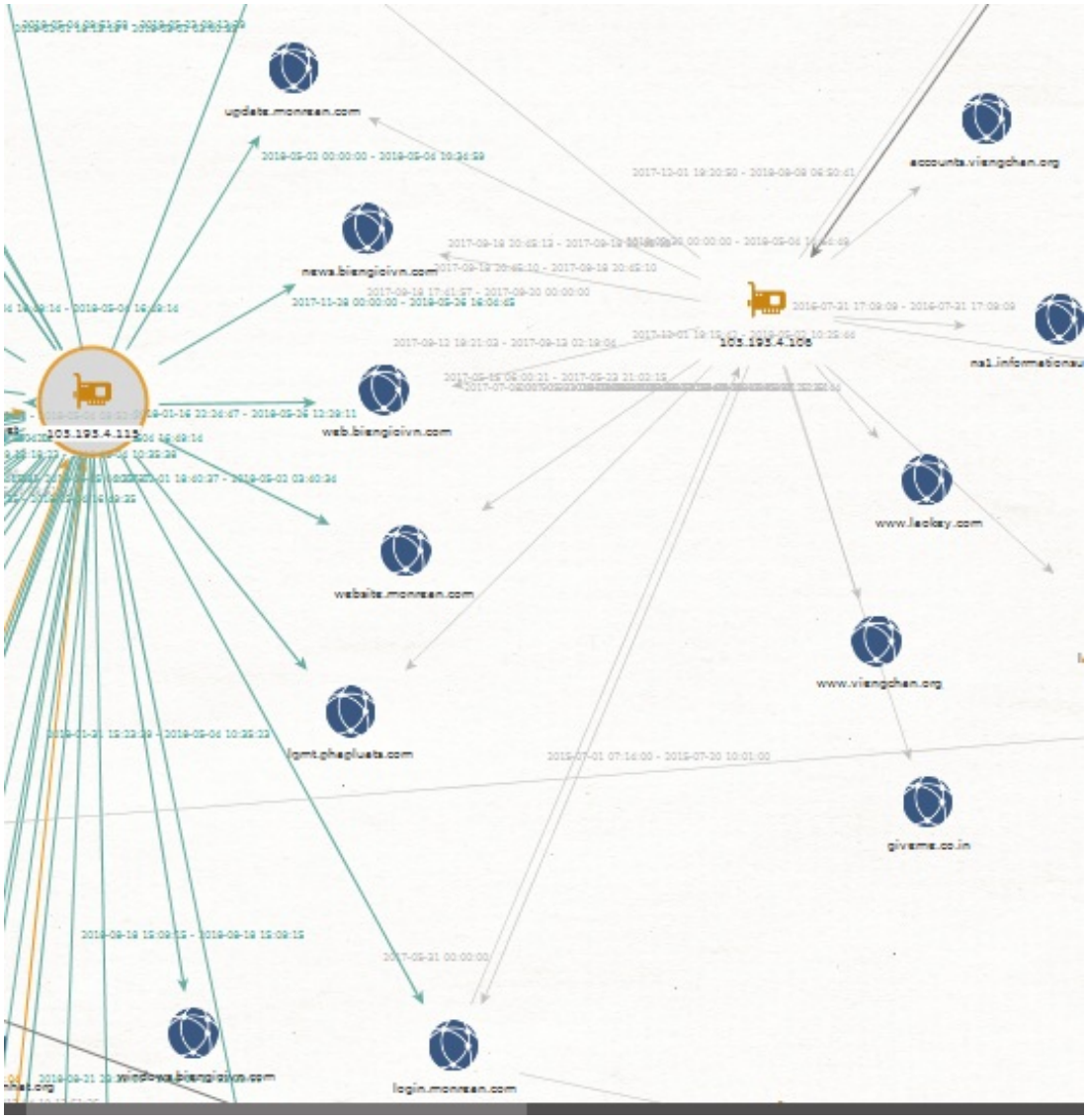
This post deals with only the Cambodia

The first document 9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e is a rtf and uses the same technics to drop on disk a legit file 77361b1ca09d6857d68cea052a0bb857e03d776d3e1943897315a80a19f20fc2 and a new core RAT. 4a5bf0df9ee222dac87e2f1b38b18660ebb92de8ba3f1cbc845f945a766dd6a6.

This file is a dll. You found a complete analysis by Fortinet.

https://www.fortinet.com/blog/threat-research/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations.html

The c2 that is contacted by the dll is weather.gbaycruise.com has the same IP used during the Vietnamese campaign 103.193.4.106. This IP has many overlaps with domains using another IP 103.193.4.115 used by the Vietnamese campaign.



And like Vietnamese, it’s the exploit toolset and drops the same rat.

Another things very interesting,all domains are provided by NAMECHEAP INC. and used the same NS server.

the dns name baoin.baotintu.com is contacted by 0e32ce9e0c309859fd0d1193f54cad0dde7928053795892a0f6c8c96cbf6753d a dll newcore rat. The RTF document writen in Cambodian is 9d0c4ec62abe79e754eaa2fd7696f98441bc783781d8656065cddfae3dbf503e

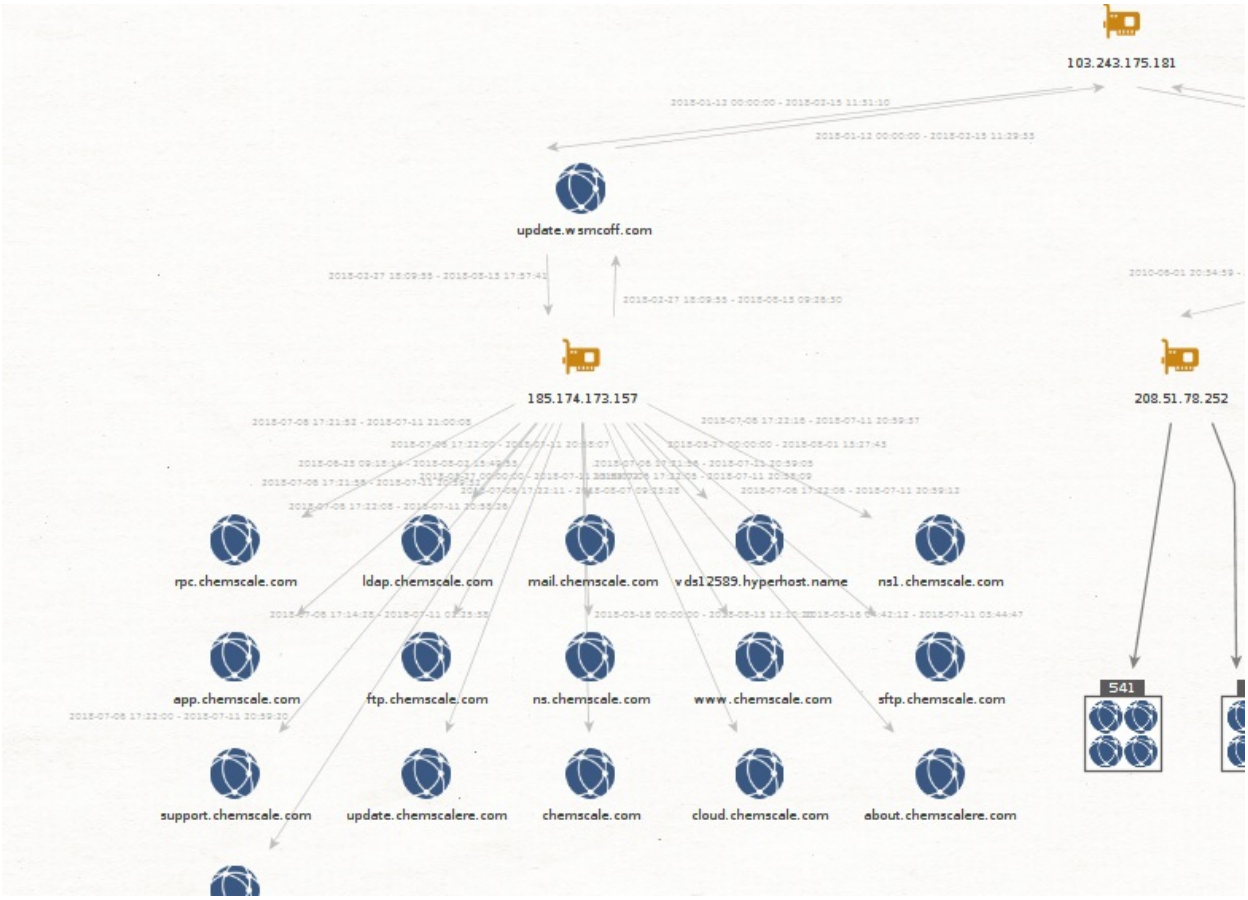
So Goblin Panda targets also the Cambodia

FireEye has published a report about Chinese Hackers group has targeted the election in Cambodia

Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals…

*Introduction FireEye has examined a range of TEMP.Periscope activity revealing extensive interest in Cambodia's…*www.fireeye.com

I found an RTF document c0b8d15cd0f3f3c5a40ba2e9780f0dd1db526233b40a449826b6a7c92d31f8d9 contacts directly 103.243.175.181.



The interesting pivot is the domain name update.wsmcoff.com.

update.wsmcoff.com has 185.174.172.157.

This IP had chemscalere.com the domain used during the campaign against Cambodia elections.

This domain update.wsmcoff.com is used by also Temp Periscope.

Goblin Panda against the Bears

*During my last investigation (here), I've found two RTFs malware documents with the same techniques of exploitation of…*medium.com

The rtfs documents for dropping the backdoor has build by the same exploit rtf kits used by Goblin Panda and all domains are registered in NAMECHEAP INC.