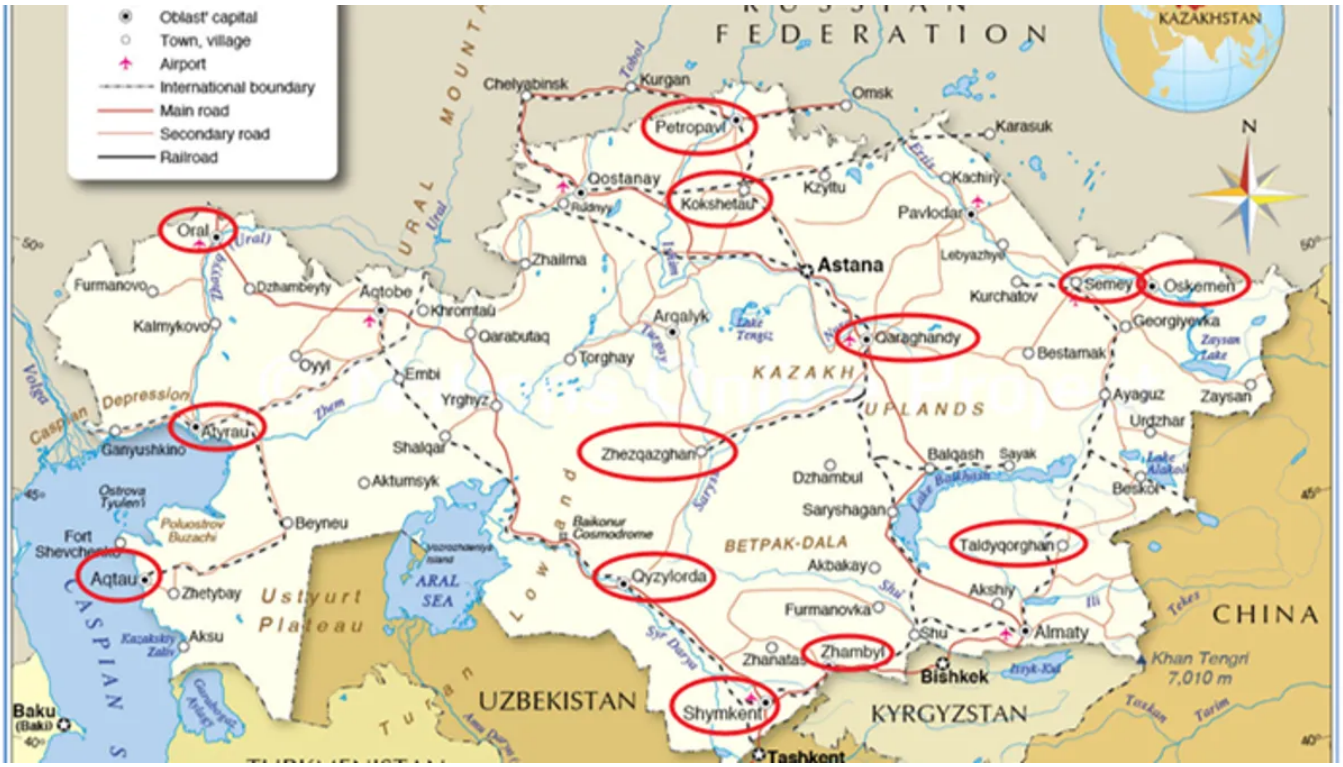
Extensive hacking operation discovered in Kazakhstan

zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/



Home Innovation Security

Researchers say an advanced hacking group has been using custom-developed hacking tools, expensive surveillance kits, mobile malware, and radio communications interception hardware to spy on Kazakhstan targets.

Written by Catalin Cimpanu, Contributor on Nov. 23, 2019

-
-
-
-
-

Chinese cyber-security vendor Qihoo 360 published a report on Friday exposing an extensive hacking operation targeting the country of Kazakhstan.

Targets included individuals and organizations involving all walks of life, such as government agencies, military personnel, researchers, journalists, private companies, the educational sector, religious figures, government dissidents, and foreign diplomats alike.

The campaign, Qihoo 360 said, was broad, and appears to have been carried by a threat actor with considerable resources, and one who had the ability to develop their private hacking tools, buy expensive spyware off the surveillance market, and even invest in radio communications interception hardware.

Signs point that some attacks relied on sending targets carefully crafted emails carrying malicious attachments (spear-phishing), while others relied on getting physical access to devices, suggesting the use of on-the-ground operatives deployed in Kazakhstan.

Meet Golden Falcon

Qihoo researchers named the group behind this extensive campaign Golden Falcon (or APT-C-34). The Chinese security vendor claimed the group was new, but when ZDNet reached out to Kaspersky, we were told Golden Falcon appears to be another name for DustSquad, a cyber-espionage entity that has been active since 2017.

The only report detailing its previous hacking operations dates back to 2018 when it was seen using spear-phishing emails that lead users to a malware-laced version of Telegram.

Just like the attacks documented by Qihoo this week, the 2018 attacks also focused on Kazakhstan but had used a different malware strain.

Qihoo's new report is primarily based on data the Chinese company obtained after it gained access to one of Golden Falcon's command and control (C&C) server, from where they retrieved operational data about the group's activities.

Here, the Chinese firm said it found data retrieved from infected victims. Collected data involved primarily office documents, taken from hacked computers.

All the stolen information was arranged in per-city folders, with each city folder containing data on each infected host. Researchers said they found data from victims located in Kazakhstan 13 largest cities, and more.

Image: Qihoo 360

The data was encrypted, but researchers said they were able to decrypt it. Inside, they also found evidence that Golden Falcon was also spying on foreign nationals in the country -- with Qihoo naming Chinese international students and Chinese diplomats as targets.

Expensive hacking tools

Files on the C&C server revealed what types of hacking tools this group was using. Two tools stood out. The first was a version of RCS (Remote Control System), a surveillance kit sold by Italian vendor HackingTeam. The second was a backdoor trojan named Harpoon (Garpun in the Russian language) that appears to have been developed by the group itself.

In regards to its use of RCS, what stood out was that Golden Falcon was using a new version of RCS. The RCS version number is important because, in 2015, a hacker breached and then leaked all the HackingTeam's internal files, including the source code for RCS.

At the time, the RCS version number was 9.6. According to Qihoo, the version number for the RCS instances they found in Golden Falcon's possession was 10.3, a newer version, meaning the group most likely bought a newer version from its distributor.

But Golden Falcon was also in the possession of another potent tool. Qihoo says the group was using a unique backdoor that hasn't been seen outside the group's operations and was most likely their own creation.

The Chinese vendor said it obtained a copy of this tool's manual. It is unclear if they found the manual on the group's C&C server, or if they obtained it from another source. The manual, however, shows a well-developed tool with a large feature-set, on par with many of today's top existing backdoor trojans.

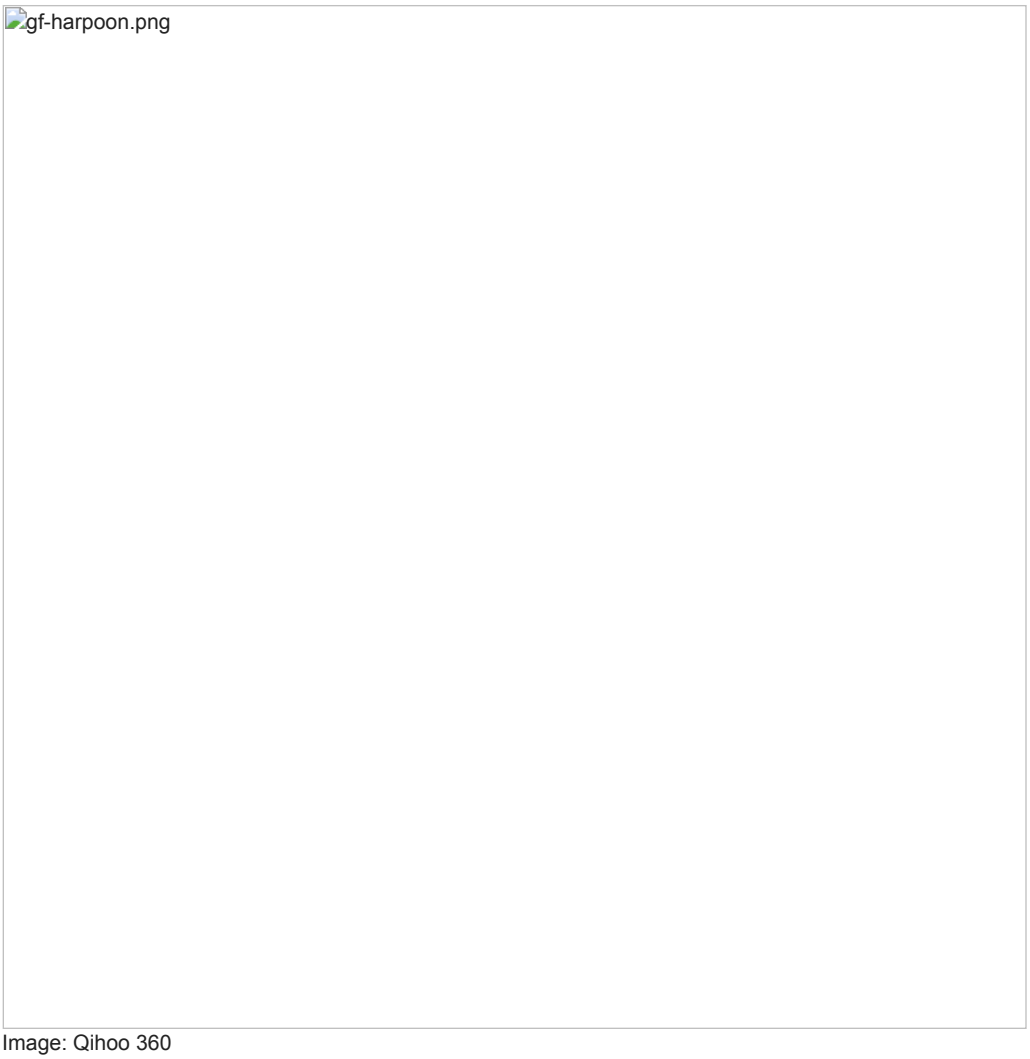


Image: Qihoo 360

Features include:

- Keylogging
- Steal clipboard data
- Take screenshot of the active window at predetermined intervals
- List the contents of a given directory
- Get Skype login name, contact list, and chat message history
- Get Skype and Google Hangouts contacts and voice recordings

- Record sound via the microphone, eavesdropping
- Copy a specified file from the target computer
- Automatically copy files from removable media
- Store all intercepted data in an encrypted data file, inside a specified directory
- Send stolen data to a specified FTP server
- Run a program or operating system command
- Download files from a given FTP into a specific directory
- Remotely reconfigure and update components
- Receive data files from a given FTP and automatically extract the files to a specified directory
- Self-destruct

Most of the features listed above are the norm for most high-level backdoor trojans, usually encountered in nation-state level cyber-espionage.

Mobile malware

But Qihoo researchers also found additional files, such as contracts, supposedly signed by the group.

It is important to point out that cyber-espionage groups don't leave contracts sitting around on C&C servers. It is unclear if these contracts were found on Golden Falcon's C&C server, or were retrieved from other sources. Qihoo didn't say.

One of these contracts appears to be for the procurement of a mobile surveillance toolkit known as Pegasus. This is a powerful mobile hacking tool, with Android and iOS versions, sold by NSO Group.

The contract suggests that Golden Eagle had, at least, shown interest in acquiring NSO's Android and iOS surveillance tools. It is unclear if the contract was ever completed with a sale, as Qihoo didn't find any evidence of NSO's Pegasus beyond the contract.

Image: Qihoo 360

Either way, Golden Eagle did have mobile hacking capabilities. This capability was provided via Android malware supplied by the HackingTeam.

Qihoo said the malware they analyzed included 17 modules with features ranging from audio eavesdropping to browser history tracking, and from stealing IM chat logs to tracking a victim's geo-location.

Radio interception hardware

A second set of contracts showed that Golden Falcon had also acquired equipment from Yurion, a Moscow-based defense contractor that's specialized in radio monitoring, eavesdropping, and other communications equipment.

Again, Qihoo only shared details about the contract's existence, but could not say if the equipment was bought or used -- as such capabilities go beyond the tools at the disposal of a regular security software company.

Image: Qihoo 360

Tracking down members?

The Chinese cyber-security firm also said it tracked down several Golden Falcon members through details left in legal digital signatures, supposedly found inside the contracts they discovered.

Researchers said they tracked four Golden Falcon members and one organization.

Using data that was left uncensored in a screenshot shared by Qihoo, we were able to track one of the group's members to a LinkedIn profile belonging to a Moscow area-based programmer that the Chinese firm described as "a technical engineer" for Golden Falcon.

No official attribution -- but plenty of theories

Neither Qihoo nor Kaspersky, in its 2018 report, make any formal attribution for this group. The only detail the two shared was that this was a Russian-speaking APT (advanced persistent threat -- a technical term used to describe advanced, nation-state backed hacking units).

During research for this article, ZDNet asked a few analysts for their opinions. The most common theories we heard were that this "looks" to be (1) a Russian APT, (2) a Kazakh intelligence agency spying on its citizens, (3) a Russian mercenary group doing on-demand spying for the Kazakh government -- with the last two being the most common answer.

However, it should be noted that these arguments are subjective and not based on any actual substantial proof.

The use of HackingTeam surveillance software, and the inquiry into buying NSO Group mobile hacking capabilities does show that this could be, indeed, an authorized law enforcement agency. However, Qihoo also pointed out that some of the targets/victims of this hacking campaign were also Chinese government officials in north-west China -- meaning that if this was a Kazakh law enforcement agency, then they seriously overstepped their jurisdiction.

The Qihoo Golden Falcon report is available here, in Chinese, and here, translated with Google Translate. The report contains additional technical information about the malware used in these attacks, information that we didn't include in our coverage because it was too technical.

The world's most famous and dangerous APT (state-developed) malware

---