Global espionage campaign targeting the telecommunications sector

Reference: Memo [190626-1] Date: 26/06/2019 - Version: 1.1
Keywords: telecoms, espionage, China
Sources: publicly available information

Key Points

- A global cyber-espionage campaign has targeted telecommunications providers from Africa, the Middle East, and Europe.
- Attackers were looking after call detail records, along with other personal data, credentials and geo-location of specific individuals.
- The interest and resources shown by the attackers denote a highly likely state-sponsored espionage origin.

Summary

On June 25, cyber security firm Cybereason uncovered a cyber-espionage campaign targeting at least 10 cellular providers around the world. Providers are from Africa, the Middle East, and Europe. North American was not impacted according to Cybereason. The campaign has been active since at least 2017. The attackers were looking after call detail records (CDR), along with other personal data, billing data, credentials, email servers, geo-location of users, and more. Attackers did not exfiltrate the entire archives of the telcommunications companies. Instead, they accessed the data by querying the systems from within the target network.

Initial compromise: The attackers deployed a malicious web shell on vulnerable IIS servers. The attackers were then able to leverage the web shell to run reconnaissance commands, steal credentials, and deploy other tools. The web shell was a modified version of China Chopper, a tool which has been used by several groups including Leviathan (aka APT40) and APT27 (aka Emissary Panda).

Reconnaissance: The attackers launched a series of reconnaissance commands to try to obtain and enumerate information about the compromised machines, network architecture, users, and active directory enumeration. One of the reconnaissance commands was to run a modified nbtscan tool ("NetBIOS nameserver scanner") to identify available NetBIOS name servers locally or over the network. This tool has been used in the past by APT10. The tool allows to search services of interest across the IT estate and footprint endpoints of interest. It is also capable of identifying system information.

Credential stealing: The attackers attempted to dump credentials stored on compromised machines, using a modified version of Mimikatz tool that dumps NTLM hashes. This version of Mimikatz did not require any command line arguments, most likely in an attempt to avoid detection based on command-line auditing.

Lateral movement: Once the attackers mapped the network and obtained credentials, they began to move laterally. They were presumably able to compromise critical assets including production servers and database servers, and they apparently managed to gain full control of the Domain Controller. The threat actor relied on WMI and PsExec and install their tools across multiple assets.

Maintaining a long-term foothold: The attackers abused the stolen credentials to create rogue, high-privileged domain user accounts which they then used to act on their objectives. By creating these accounts, they ensured they would maintain access between different attack waves. Once the attackers regain their foothold, they already have access to a high-privileged domain user account. This significantly reduces the "noise" of having to use credential dumpers repeatedly, which helped them evade detection. To maintain access across the compromised assets, the attackers also deployed a remote access trojan (RAT) dubbed PoisonIvy. This malware is publicly available and has been used by many groups including APT1, Temper Panda (aka admin@338), DragonOK and others.

Secondary web shells: In later stages, the attackers deployed two other custom-built web shells. From these web shells, they launched reconnaissance commands, stole data, and dropped additional tools including portqry.exe, renamed cmd.exe, WinRAR, and the notorious HTRAN. HTRAN is a tool that proxies connections through intermediate hops and aids users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks.

Data exfiltration: The attackers exfiltrated stolen data using multiple different channels including web shells, PoisonIvy, and HTRAN. In an attempt to hide the contents of the stolen data, the attackers used WinRAR to compress and password-protect it. The WinRAR binaries and compressed data were found mostly in the Recycle Bin folder. In order to exfiltrate data from a network segment not connected to the internet, the attackers deployed a modified version of HTRAN. This 'connection bouncer' tool lets the threat actor redirect ports and connections between different networks and obfuscate command and control (C2) server traffic.

Comments

The interest shown by attackers in the collection of metadata, also named call detail records (source, destination, duration, location of calls) denotes an espionage rather than a cyber-criminal motive. Metadata are sometimes more important than the contents of the calls. It allows an intelligence service to build a whole picture of their targets: who they're talking to, who are their peers and co-workers, when do they wake up and go to bed, where they work, what they route to work looks like.

Cybereason has attributed the campaign to APT10, based on their analysis of techniques, tactics and procedures (TTPs) used by the attackers. As pointed out by cyber security researcher Timo Steffens, in other campaigns the APT10 group worked for the Chinese Ministry of State Security. Stealing location data would be consistent with MSS's mission, again. However, Timo Steffens and several researchers noted that these TTPs are rather generic and could fit several other Chinese groups.

Notwithstanding the exact attribution, the global reach of the campaign and the vulnerabilities of telecommunications providers remain highly worrying. The Regin attack against Belgacom which was publicly revealed in 2014 by Kaspersky Lab and Symantec is a noteworthy example of a highly likely state sponsored attack against a telecom provider. Some sources has attributed this attack to US and British (GCHQ) intelligence agencies.