Cybereason Exposes Chinese Threat Actors Compromising Telecommunications Providers for Cyber Espionage

Issued by Cybereason

3 Aug 2021

DeadRinger Research Highlights Attack Trends Leveraging Third-Party Service Providers to Compromise Multiple Targets

Cybereason, the leader in operation-centric attack protection, today announced the discovery of several previously unidentified cyber attack campaigns infiltrating major telecommunications providers across Southeast Asia.

Similar to the recent SolarWinds and Kaseya attacks, the threat actors first compromised third-party service providers - but in this case instead of using them to deliver malware through a supply chain attack, the intent was to leverage them to conduct surveillance of their customers' confidential communications.

The report comes on the heels of the Biden administration's public rebuke of China's Ministry of State Security for the recent HAFNIUM attacks that exploited vulnerabilities in unpatched Microsoft Exchange Servers and put thousands of organisations worldwide at risk. Exploitation of these same vulnerabilities were central to the success of the attacks detailed in this research.

In the report, titled *DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos*, multiple clusters of attack activity were identified that have evaded detection since at least 2017 and are assessed to be the work of several prominent Advanced Persistent Threat (APT) groups aligned with the interests of the Chinese government.

Cybereason observed a significant overlap in tactics, techniques and procedures (TTPs) across the three operations and assessed that the attackers were likely tasked with parallel objectives under the direction of a centralised coordinating body aligned with Chinese state interests.

"The attacks are very concerning because they undermine the security of critical infrastructure providers and expose the confidential and proprietary information of both public and private organisations that depend on secure communications for conducting business," said Cybereason CEO and co-founder Lior Div.

"These state-sponsored espionage operations not only negatively impact the telcos' customers and business partners, they also have the potential to threaten the national security of countries in the region and those who have a vested interest in the region's stability," he explains.

"This is why Cybereason maintains a global team of seasoned threat intelligence investigators whose focus is to expose the tactics, techniques and procedures of advanced adversaries so we can better protect organisations from these kinds of complex attacks now and into the future."

Key Findings Include:

- **Adaptive, Persistent and Evasive:** The highly adaptive attackers worked diligently to obscure their activity and maintain persistence on the infected systems, dynamically responding to mitigation attempts after having evaded security efforts since at least 2017, an indication that the targets are of great value to the attackers.
- **Compromise of Third-Parties to Reach Specific Targets:** Similar to the recent SolarWinds and Kaseya attacks, the threat actors first compromised third-party service providers - but in this case instead of using them to deliver

malware through a supply chain attack, the intent was to leverage them to conduct surveillance of their customers' confidential communications.

- **Microsoft Exchange Vulnerabilities Exploited:** Similar to the HAFNIUM attacks, the threat actors exploited recently disclosed vulnerabilities in Microsoft Exchange Servers to gain access to the targeted networks. They then proceeded to compromise critical network assets such as Domain Controllers (DC) and billing systems which contain highly sensitive information like Call Detail Record (CDR) data, allowing them access to the sensitive communications of anyone using the affected telecoms' services.
- **High Value Espionage Targets:** Based on previous findings from the Operation Soft Cell Report Cybereason published in 2019, as well as other published analysis of operations conducted by these threat actors, it is assessed that the telecoms were compromised in order to facilitate espionage against select targets. These targets are likely to include corporations, political figures, government officials, law enforcement agencies, political activists and dissident factions of interest to the Chinese government.
- **Operating in the Interest of China:** Three distinct clusters of attacks have varying degrees of connection to APT groups Soft Cell, Naikon and Group-3390 -- all known to operate in the interest of the Chinese government. Overlaps in attacker TTPs across the clusters are evidence of a likely connection between the threat actors, supporting the assessment that each group was tasked with parallel objectives in monitoring the communications of specific high value targets under the direction of a centralised coordinating body aligned with Chinese state interests.
- **Potential for Broader Impact:** These attacks compromised telcos primarily in ASEAN countries, but the attacks could be replicated against telcos in other regions. While the prevailing assessment is that the operations were intended for espionage purposes only, the fact remains that had the attackers decided to change their objectives from espionage to interference, they would have had the ability to disrupt communications for any of the affected telecoms' customers.

The full report can be accessed here: *DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos*, and we invite you to join us for a *live webinar on Thursday, August 12th, at 19:00* where Cybereason's Head of Threat Research Assaf Dahan and VP of Security Practices Mor Levi will walk through the espionage operations uncovered in the DeadRinger report.

- **FBI warns US companies to avoid malicious USB devices** 18 Jan 2022
- **Cybereason 2022 trends and predictions** 29 Nov 2021
- **Cybereason Exposes Chinese Threat Actors Compromising Telecommunications Providers for Cyber Espionage** 3 Aug 2021
- **Cybereason acquires empow to enhance XDR offerings** 20 Jul 2021
- **Cybereason Secures $275 Million in Crossover Financing to Extend Global Leadership in XDR** 14 Jul 2021

Cybereason

Cybereason is the champion for today's cyber defenders with future-ready attack protection that extends from the endpoint, to the enterprise, to everywhere.

Profile | News | Contact | Twitter | Facebook | RSS Feed