MONSOON - Analysis Of An APT Campaign

X-Labs

August 8, 2016

Nicholas Griffin Security Researcher

APT

MONSOON is the name given to the Forcepoint Security Labs investigation into an ongoing espionage campaign that the Special Investigations team have been tracking and analysing since May 2016. We have released our technical analysis in the form of a whitepaper.

Monsoon Targets Specific Victims

The overarching campaign appears to target both Chinese nationals within different industries and government agencies in Southern Asia. It appears to have started in December 2015 and is still ongoing as of July 2016. The malware components used in MONSOON are typically distributed through weaponised documents sent through e-mail to specifically chosen targets. Themes of these documents are usually political in nature and taken from recent publications on topical current affairs.

Several Sophisticated Malware Components

MONSOON includes the use of multiple malware families, including Unknown Logger Public, TINYTYPHON, BADNEWS, and an AutoIt backdoor. BADNEWS is particularly interesting, containing resilient command-and-control (C&C) capability using RSS feeds, Github, forums, blogs and Dynamic DNS hosts. Malware used in MONSOON contains the ability to bypass Windows User Account Control and evade modern anti-malware solutions.

Who Is Behind MONSOON?

Amongst the evidence gathered during the MONSOON investigation were a number of indicators which make it highly probable that this adversary and the Operation Hangover adversary are one and the same and are operating out of the Indian Sub Continent.

How And When Did We Do The Research?

Our investigation into MONSOON began in May 2016. Over the course of our investigation we discovered over 170 malicious documents and 4 distinct malware families.

Download Links

Our deep-dive technical analysis is available for download now from https://www.forcepoint.com/resources/datasheets/monsoon-analysis-apt-campaign

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Learn more about Forcepoint