Nomadic Octopus: cyber espionage in Central Asia

virusbulletin.com/conference/vb2018/abstracts/nomadic-octopus-cyber-espionage-central-asia/

Thursday 4 October 11:00 - 11:30, Green room

Anton Cherepanov (ESET)

ESET researchers recently discovered an interesting cyber espionage campaign active in several countries of Central Asia. We attribute these attacks to a previously undocumented APT group that we have named Nomadic Octopus. Our findings suggest that this APT group has been active since at least 2015. The main goal of Nomadic Octopus appears to be cyber espionage against high-value targets, including diplomatic missions in the region. However, besides these high-value targets, we have seen a campaign targeting a local political blogger, which may suggest that Nomadic Octopus also conducts cyber surveillance operations. Nomadic Octopus performs its activity using unique, custom-made malware. In our talk, we will uncover details about this new APT group and provide a technical analysis of the malicious toolkit used in the attacks.

Anton Cherepanov

Anton Cherepanov is a senior malware researcher at *ESET*, where his responsibilities include the analysis of complex threats. He has performed extensive research on cyberattacks in Ukraine and on BlackEnergy APT group malware. His research has been presented at numerous conferences, including Black Hat USA, Virus Bulletin, CARO Workshop, PHDays and ZeroNights. He won a Pwnie Award in 2017 for his discovery and analysis of the M.E.Doc backdoor – the origin of the NotPetya ransomware outbreak. His interests focus on IT security, reverse engineering and the automation of malware analysis

@cherepanov74