Operation Shady RAT - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation Shady RAT

Names	Operation Shady RAT *(McAfee)*
Country	China
Sponsor	State-sponsored, PLA Unit 61398
Motivation	Information theft and espionage
First seen	2006
Description	(McAfee) With the goal of raising the level of public awareness today we are publishing the most comprehensive analysis ever revealed of victim profiles from a five year targeted operation by one specific actor—Operation Shady RAT, as I have named it at McAfee (RAT is a common acronym in the industry which stands for Remote Access Tool). This is not a new attack, and the vast majority of the victims have long since remediated these specific infections (although whether most realized the seriousness of the intrusion or simply cleaned up the infected machine without further analysis into the data loss is an open question). McAfee has detected the malware variants and other relevant indicators for years with Generic Downloader.x and Generic BackDoor.t heuristic signatures (those who have had prior experience with this specific adversary may recognize it by the use of encrypted HTML comments in web pages that serve as a command channel to the infected machine). McAfee has gained access to one specific Command & Control server used by the intruders. We have collected logs that reveal the full extent of the victim population since mid-2006 when the log collection began. Note that the actual intrusion activity may have begun well before that time but that is the earliest evidence we have for the start of the compromises. The compromises themselves were standard procedure for these types of targeted intrusions: a spear-phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit when opened on an unpatched system will trigger a download of the implant malware. That malware will execute and initiate a backdoor communication channel to the Command & Control web server and interpret the instructions encoded in the hidden comments embedded in the webpage code. This will be quickly followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and

	move laterally within the organization to establish new persistent footholds via additional compromised machines running implant malware, as well as targeting for quick exfiltration the key data they came for.
Observed	Sectors: Energy, Government, Industrial, IT, Media, Telecommunications, Think Tanks, Non-profit organizations. Countries: Canada, Denmark, Germany, Hong Kong, India, Indonesia, Japan, Singapore, South Korea, Switzerland, Taiwan, UK, USA, Vietnam.
Tools used	
Information	<https://web.archive.org/web/20110804083836/http:/www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> <https://www.vanityfair.com/news/2011/09/chinese-hacking-201109> <https://en.wikipedia.org/wiki/Operation_Shady_RAT>

Last change to this card: 21 May 2021

Download this actor card in PDF or JSON format
