Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:58:31 UTC

Other threat group: Boson Spider

Names	Boson Spider *(CrowdStrike)*
Country	[Unknown]
Motivation	Financial crime
First seen	2015
Description	(IBM) When it comes to discovering new malware, it is much more common for researchers to run across information stealers, ransomware and remote-access tools (RATs) than it is to encounter brand new complex codes like banking Trojans or targeted attack tools such as Duqu. Nonetheless, it is the lesser breeds, like information stealers and RATs, that are a lot more prolific in the wild. And while banking Trojans or targeted attacks are quite specific in what they do, information stealers are by far less discriminatory and thus end up affecting a greater number of people and organizations. That brings us to CoreBot, a new information stealer discovered and analyzed by IBM Security X-Force researchers, who indicate this is one malware piece to watch out for. CoreBot appears to be quite modular, which means that its structure and internal makeup were programmed in a way that allows for the easy adding of new data theft and endpoint control mechanisms. CoreBot was discovered while the researchers were studying the activity of malware on Trusteer-protected enterprise endpoints. The malware's compiled file was named "core" by its developer. Antivirus engines do not specify this malware's name yet and detect it under generic names such as Dynamer!ac or Eldorado. But while CoreBot may appear artless at first glance, without real-time theft capabilities, it is more interesting on the inside. CoreBot has been observed to be distributed by DinaBot (operated by Scully Spider, TA547).
Observed	Sectors: Financial. Countries: Australia, Canada, Japan, UK, USA and Europe.

Tools used	CoreBot.	
Operations performed	Nov 2017	Spotted by researchers at Deep Instinct, a new version of CoreBot is being distributed in spam email campaigns with the intention of stealing information from customers of Canadian banking websites. Customers of TD, Des-Jardins, RBC, Scotia Bank, Banque National are all targeted by those behind the campaign, with successful execution of the malware allowing the attackers to steal the credentials of infected users as they login into these sites. <https://www.zdnet.com/article/corebot-banking-trojan-malware-returns-after-two-year-break/>
Information	<https://go.crowdstrike.com/rs/281-OBQ-266/images/Report_BosonSpider.pdf> <https://securityintelligence.com/watch-out-for-corebot-new-stealer-in-the-wild/>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
