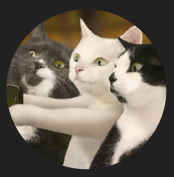

daji

Botnet

A new botnet Orchard Generates DGA Domains with Bitcoin Transaction Information

DGA is one of the classic techniques for botnets to hide their C2s, attacker only needs to selectively register a very small number of C2 domains, while for the defenders, it is difficult to determine in advance which domain names will be generated and registered. 360 netlab has long focused


· Aug 5, 2022 · 13 min read

Botnet

DGA家族Orchard持续变化，新版本用比特币交易信息生成DGA域名

DGA是一种经典的botnet对抗检测的技术，其原理是使用某种DGA算法，结合特定的种子和当前日期，定期生成大量的域名，而攻击者只是选择性的注册其中的极少数。对于防御者而言，因为难以事先确定哪些域名会被生成和注册，因而防御难度极大。 360 netlab长期专注于botnet攻防技术的研究，维护了专门的DGA算法和情

报库，并通过订阅情报的方式与业界分享研究成果。近期我们在分析未知DGA域名时发现一例不但使用日期，还会同时使用中本聪的比特币账号交易信息来生成DGA域名的例子。因为比特币交易的不确定性，该技术比使用时间生成的DGA更难预测，因而防御难度更大。 该技术发现于一个名为Orchard的botnet家族。自从2021年2月份首次检测到该家族以来，我们发现它至少经历了3个版本的变化，中间甚至切换过编程语言。结合长期的跟踪结果和其它维度的信息，我们认为Orchard会是一个长期活跃、持续发展的botnet家族，值得警惕。本文将介绍Orchard的最新DGA技术，以及它这3个版本的发展过程。本文要点如下： * Orchard是一个使用了DGA技术的botnet家族，核心功能


· Aug 5, 2022 · 18 min read