wanghao

Botnet

PureCrypter is busy pumping out various malicious malware families

In our daily botnet analysis work, it is common to encounter various loaders.Compared to other types of malware, loaders are unique in that they are mainly used to "promote", i.e., download and run other malware on the infected machine. According to our observations, most loaders are

· Aug 29, 2022 · 12 min read

loader

PureCrypter Loader持续活跃，已经传播了10多个其它家族

在我们的日常botnet分析工作中，碰到各种loader是常事。跟其它种类的malware相比，loader的特殊之处在于它主要用来“推广”，即在被感染机器上下载并运行其它的恶意软件。根据我们的观察，大部分loader是专有的，它们和推广的家族之间存在绑定关系。而少数loader家族会将自己做成通用的推广平台，可以传播其它任意家

族，实现所谓的malware-as-a-service（MaaS）。跟专有loader相比，MaaS类型显然更危险，更应该成为我们的首要关注目标。 本文介绍我们前段时间看到的一个MaaS类型的loader，它名为PureCrypter，今年非常活跃，先后推广了10多个其它的家族，使用了上百个C2。因为zscaler已经做过详细的样本分析，本文主要从C2和传播链条角度介绍我们看到的PureCrypter传播活动，分析其运作过程。 本文要点如下： * PureCrypter是一款使用C#编写的loader，至少2021年3月便已出现，能传播任意的其它家族。 * PureCrypter今年持续活跃，已经传播了包括Formbook、SnakeKeylog

· Aug 29, 2022 · 14 min read

360 Netlab Blog - Network Security Research Lab at 360 © 2025 Powered by Ghost