

勒索软件流行态势分析

2023 年 12 月



勒索软件传播至今，360 反勒索服务已累计接收到数万勒索软件感染求助。随着新型勒索软件的快速蔓延，企业数据泄露风险不断上升，勒索金额在数百万到近亿美元的勒索案件不断出现。勒索软件给企业和个人带来的影响范围越来越广，危害性也越来越大。360 全网安全大脑针对勒索软件进行了全方位的监测与防御，为需要帮助的用户提供 360 反勒索服务。

2023 年 12 月，全球新增的活跃勒索软件家族有 LIVE、DragonForce、Tisak 等。其中 DragonForce 家族采用多重勒索方式运营，Tisak 家族除加密 Windows 设备外还会攻击 ESXI 服务器。

以下是本月值得关注的部分热点：

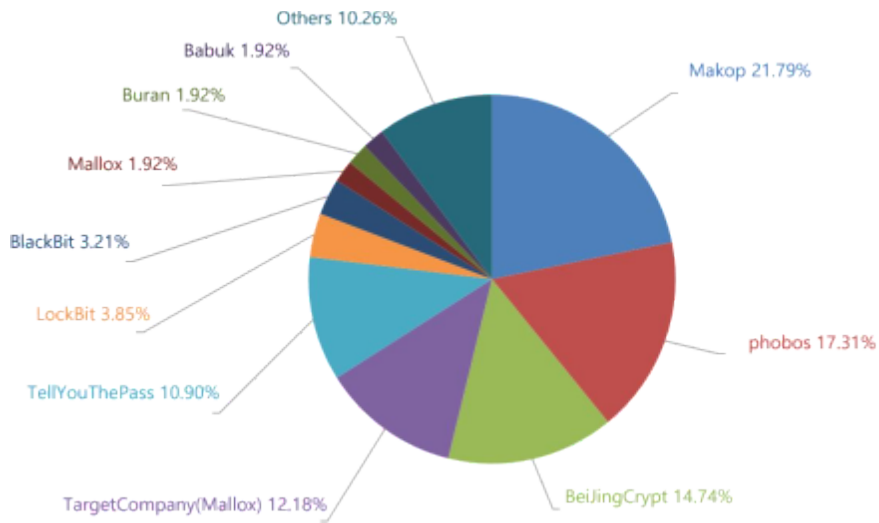
1. 美国海军承包商 Austal 在数据泄露后承认遭受网络攻击
2. Akira 勒索软件团伙声称对 Nissan 澳大利亚的网络攻击负责
3. 育碧表示正在调查有关新安全漏洞的报告

基于对 360 反勒索服务数据的分析研判，360 数字安全集团高级威胁研究分析中心(CCTGA 勒索软件防范应对工作组成员) 发布本报告。

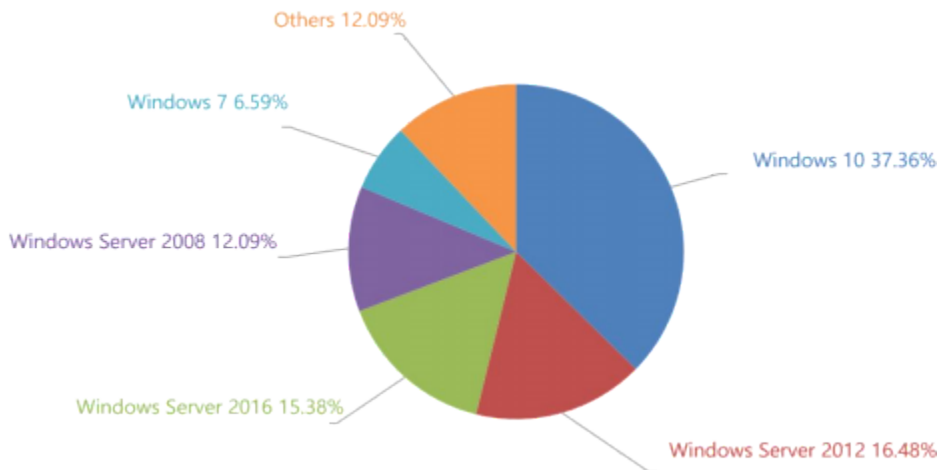
感染数据分析

针对本月勒索软件受害者设备中所中病毒家族进行统计：Makop 家族占比 21.79%居首位，第二的是占比 17.31%

的 phobos，BeiJingCrypt 家族以 14.74%位居第三。



对本月受害者所使用的操作系统进行统计，位居前三的是：Windows 10、Windows Server 2012 以及 Windows Server 2016。



2023 年 12 月被感染的系统中桌面系统和服务器系统占比显示，受攻击的系统类型服务器系统占比与桌面系统基本相当。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/687200126151006060>