网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

威胁框架的新进展

安天 | 研究院

CONTENTS
目 录

01 新内容

版本	时间	内容/结构主要变化
V3	2018.10.23 2019.04.29	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术11 + 技术223 . V1 & V2 已不在MITRE网站 (github)
V4	2019.04.30 2019.07.30	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术12 + 技术244 . 增加了战术“Impact”
V5	2019.07.31 2019.10.23	分类：Enterprise (All, Linux, macOS, Windows), Pre-, Mobile 企业版战术/技术：战术12 + 技术244 . 引入了“缓解”
V6	2019.10.24 2020.03.30	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS 企业版战术/技术：战术12 + 技术266 . 增加了类型“云，工控”， 丰富了技术内容
V7 beta	2020.03.31 2020.07.07	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS . 企业版战术/技术：战术12 + 技术156 + 子技术260 . 技术 细化为“子技术”
V7	2020.07.08 2020.10.26	分类：Enterprise (Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>), Pre-, Mobile (Android, iOS), ICS . 企业版战术/技术：战术12 +技术156 + 子技术272 . 形成“子技术”正式版
V8	2020.10.27 2021.04.28	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <AWS, GCP, Azure, Office365, Azure AD, SaaS>, Network), Mobile (Android, iOS), ICS . 企业版战术/技术：战术14 +技术178 + 子技术352 统一“Pre-”与“Enterprise”，扩展了战术“侦察，资源开发”，技术内容继续丰富
V9	2021.04.29 2021.10.20	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <Office365, Azure AD, Google Workspace, SaaS, IaaS>, Network, Containers), Mobile (Android, iOS), ICS 企业版战术/技术：战术14 +技术185 + 子技术367 . 数据源描述-I，调整云，增加容器，技术内容继续丰富
V10	2021.10.21 n/a	分类：Enterprise (Pre-, Windows, macOS, Linux, Cloud <Office365, Azure AD, Google Workspace, SaaS, IaaS>, Network, Containers), Mobile (Android, iOS), ICS 企业版战术/技术：战术14 +技术188 + 子技术379 . 数据源描述-II，技术内容继续丰富

更新概要

- 总体来看，各个重要更新及其意义
  - 攻击技术分解为攻击子技术（v7，2020）
    将“技术”分解为“子技术”，构建对威胁更为精准的刻画
  - 合并 Pre- 形成企业版战术统一 （v8，2020）
    前摄以识别“潜在的威胁”，并形成对“网空杀伤链”的分析闭环
  - 面向新兴场景 （云.v6 工控.v6 Network.v8 容器.v9 云调整v.9）
    引入云、容器、工控等模型，扩展框架威胁分析的适用范围
  - 重构数据源描述 （v.9 & v.10，2021）
    优化威胁检测的关键环节，推动框架实用易用
  - **子技术 Sub-Technique，数据源/数据组件 DataSource/DataComponent**