FIT 2017 | FREEBUF

终端安全与威胁情报的双重变奏

周　军

火绒安全联合创始人

FIT 2017 | FreeBuf Live

终端安全的重要性

- Endpoint Detection and Response
  - 终端检测（Detection）
    - 在终端安置“探针”，感知威胁信息
    - 在云端或企业内网搭建威胁信息处理平台，聚合终端感知到的威胁信息
  - 终端响应（Response）
    - 厂商下发针对不同威胁的响应策略
    - 终端用户可自主定制针对特定威胁的响应策略
- 由宏观视角聚焦高价值威胁，优化传统威胁分析模式

- 安全威胁的源头和“着陆点”
  - 只有在终端才能感知/检测基于上下文（Context）的威胁信息
  - 针对安全威胁的响应最终会“着陆”到终端
- 恶意代码模块化、协同工作、依赖终端环境，类APT攻击手段
- 随着加密通讯协议（如HTTPS）的普及，单纯基于数据流量的检测愈发困难

> “You want to get to the endpoint because it's the ultimate source of the truth”
>
> — Kevin Mandia, founder of Mandiant and president of FireEye

威胁情报的本质

检测与响应的”中间产物”——威胁情报

- 威胁情报产生于技术（检测）
  - 终端感知与后台聚合的“副产品”
  - 终端安全核心技术直接决定威胁情报的质量（粒度、深度）和形态
- 威胁情报服务于产品（响应）
  - 威胁情报直接转为对安全威胁的响应（与安全产品本身高度耦合）
  - 威胁情报指导安全技术发展、防御模型改进等

- 技术支撑策略
  - 基于终端威胁上下文的多维度威胁信息感知
  - 后台对威胁信息进行聚合、关联分析
  - 产生与终端安全技术高度耦合的威胁情报（数据特征、行为模型、……）
- 策略放大技术
  - 将威胁情报直接转化为终端安全技术“理解”的形态对终端威胁作出响应
  - 通过对威胁信息的深入分析指导检测特征、防御规则、行为模型等优化，指导安全技术发展方向

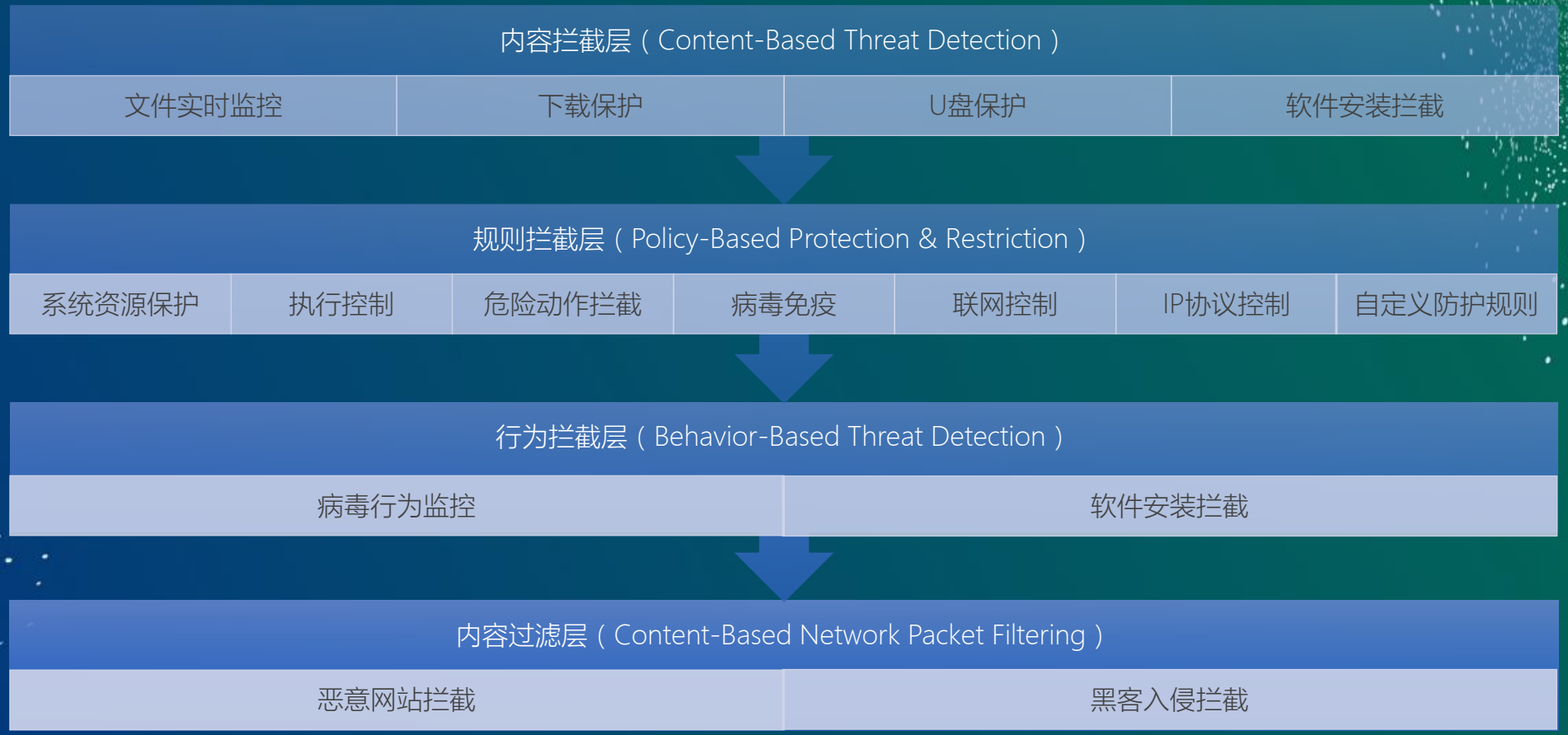
FIT 2017 | FreeBuf Live

情报驱动安全

火绒终端检测与响应体系

检测与响应（D&R）体系

强大的终端防御架构——全面的D&R体系



强大的终端技术——强大的D&R能力（内容检测）

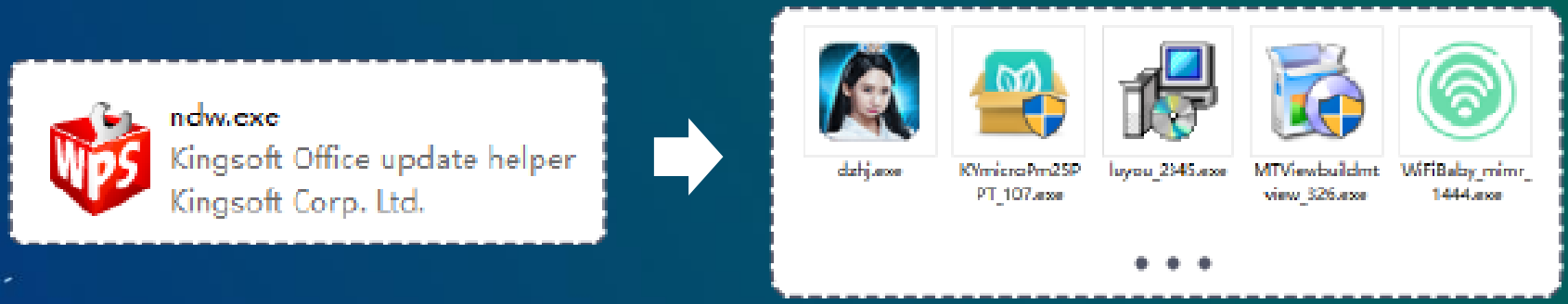
- 新一代反病毒引擎
  - 基于恶意代码DNA的通用查杀技术（Generic Detection）
  - 通过通用脱壳技术（Generic Unpacking）解决代码高级混淆/变形代码
  - 支持对超过百种文件格式的细粒度解码分析
  - 基于内容的静态启发式分析
- 虚拟行为沙盒
  - 基于虚拟化技术的行为沙盒，虚拟执行效率接近本地代码
  - 虚拟操作系统环境仿真程度高，使恶意代码在与真实主机完全隔离的虚拟环境中充分还原恶意行为
  - 基于行为的动态启发式分析

强大的终端技术——强大的D&R能力（动态防御）

- 主机入侵防御（HIPS）
  - 支持文件、注册表、应用程序、网络多维度防御规则
  - 近百个系统拦截点，针对系统脆弱点设置了超过五百个防御规则
  - 开放式的自定义防御规则，为终端用户提供有效的威胁响应手段
- 矩阵行为分析（多步防御）
  - 根据一个或多个程序的连续动作所产生的行为，评估一组相关程序的恶意性
  - 组合程序行为以及程序间的关联性进行矩阵分析
  - 以非一致性视角（Non-Canonical View）划分不同的分析矩阵，细粒度评估关联程序的行为
  - 支持威胁回滚

典型案例

- 2016年4月，火绒终端威胁情报系统检测到很多软件推广行为产生于某知名厂商升级程序（ndw.exe）
- 通过分析发现ndw.exe系被利用，目的是利用部分安全软件的“信任漏洞”进行推广

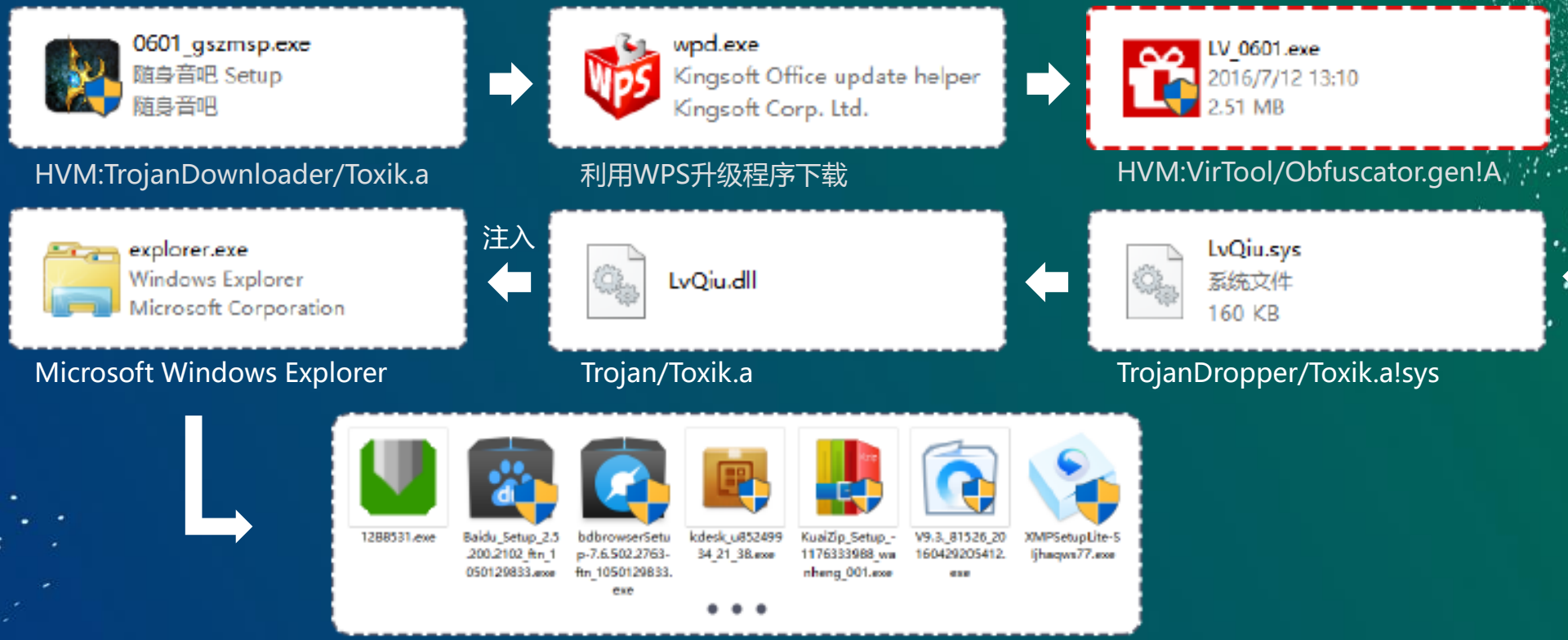


情报驱动安全—典型案例 之 “Toxik”病毒

- 通过火绒终端威胁情报系统对此类推广行为进行追溯
- 多数发起者均形如????_gszmsp.exe，随即对其展开跟踪监控

- 同年6月，发现????_gszmsp.exe下载的某些程序在火绒行为沙盒中识别到恶意行为（HVM:VirTool/Obfuscator.gen!A）
- 通过深入分析，发现病毒会释放并加载驱动进而注入恶意动态库到系统进程进行恶意推广
- 火绒将????_gszmsp.exe系列病毒命名为“Toxik”病毒

情报驱动安全—典型案例 之 “Toxik”病毒



- 通过火绒终端威胁情报系统，围绕“Toxik”病毒进行追溯分析，进而揭露病毒代码的源头直至病毒制造者

详细内容参考：《知名商业软件“喂养”病毒产业链：“Toxik”病毒追踪》（链接）

- 通过火绒终端威胁情报系统，我们还发现并曝光了包括“小马激活”病毒、“Bloom”病毒以及近期的“净广大师”病毒等多起隐秘的恶意代码事件
  - 《“小马激活”病毒新变种分析报告》（链接）
  - 《盗版用户面临的“APT攻击”风险——“Bloom”病毒分析报告》（链接）
  - 《“净广大师”病毒HTTPS劫持技术深度分析》（链接）
- 在曝光前，这些恶意程序就一直堂而皇之地“游走”于各大安全软件的“多重防御”之下

关于火绒

- 纯粹的安全公司，专注于终端安全
- 全套自主产权的新一代终端安全核心技术
  - 反病毒引擎、虚拟行为沙盒、行为防御等
- “火绒终端威胁情报系统”为基础的“终端检测与响应”运营体系
- 积累了百万忠实用户，“电脑高手”人群中享有盛誉
- 未来：企业级产品、移动端产品、威胁情报产品

Thanks