网络安全现状分析及趋势

陈羽兴
卡巴斯基实验室

KASPERSKY lab

卡巴斯基安全分析及预测

这份预测基于一整年的数据与调查结果

- Global Research and Analysis Team (GReAT)
- 2008起建立
- 40+位安全专家，遍布全球
- 对100+APT组织进行追踪

KASPERSKY lab

卡巴斯基实验室历年发现的高级威胁

KASPERSKY lab

APT报告样例

维基解密“Vault7”工具技术分析

版本：1.0（2017年3月16日）

执行概要

2017年3月7日星期二，维基解密[1]发布了一个包含所谓的CIA 内部数据库（以维基百科模式）的泄密系列（“Vault7”）的第一部分。此数据库包括 CIA 网络分析师、开发人员和合作伙伴使用的文档、报告、讨论、工具和其他文件,大小约1GB。虽然数据的来源仍然未知，但内容确实是合法的，我们有理由相信此次泄漏是真实的。

2017年3月8日，我们发布了对转储文件的初步分析，包括公开论文中引用以及残留的恶意软件植入的部分简要概述。显然，许多目光都在关注此次泄漏，我们不是唯一注意到文本[3]中的恶意软件样本的人。本文包含其中一个恶意软件植入的技术细节。本文概况如下：

- 2017年3月7日，维基解密发布了一个转储，其中包括多个疑似来自美国情报机构的工具
- 虽然被高度编译，但转储包含的数据足够我们重建一个恶意软件样本
- 恶意软件使用.NET 2.0 编写，并使用 SmartAssembly 进行模糊处理
- 持续依赖 Windows 调度任务，PowerShell 和注册表项，使其彻底实现无文件感染
- 看似合法的命令和控制手段，以及类 Pastebin 网站
- 分析还包括之前未曾发现的同一作者的一些恶意软件组件，我们在泄漏发生后设法找到了它们

KASPERSKY lab

GREAT团队

KASPERSKY Global Research & Analysis Team

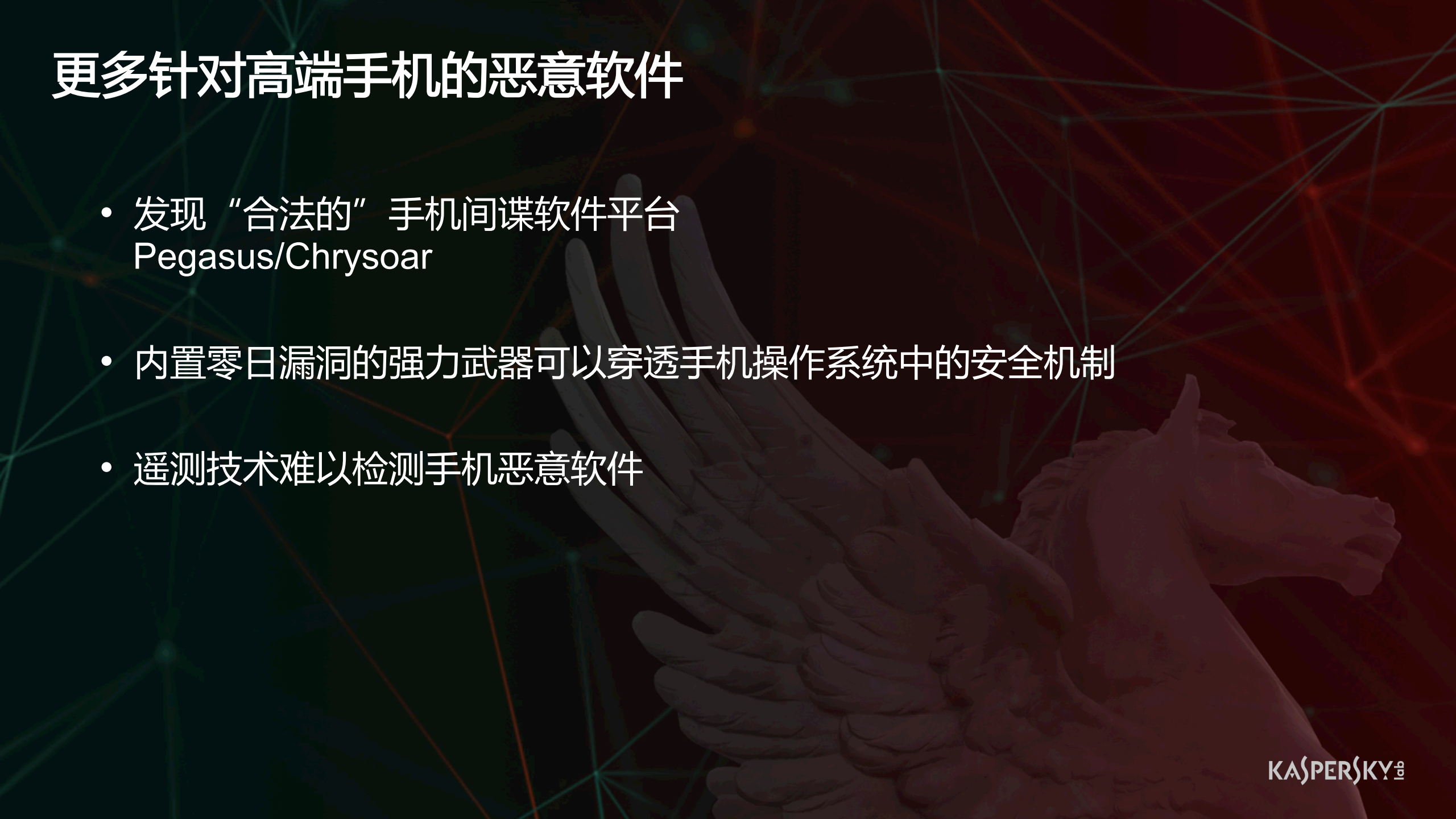
- APT发现
- APT调查
- Threat Intelligence Service（威胁情报服务）

针对供应链的攻击愈演愈烈

- ShadowPad, ExPetr, CCleaner
- 木马型软件的更新
- 第三方软件的广泛使用 – 更易进行攻击
- 专用软件更易被瞄准
- 更难被识别

更多针对高端手机的恶意软件

- 发现“合法的”手机间谍软件平台 Pegasus/Chrysoar
- 内置零日漏洞的强力武器可以穿透手机操作系统中的安全机制
- 遥测技术难以检测手机恶意软件



KASPERSKY lab

更多类似BeEF的web框架分析工具

- 零日漏洞价格昂贵
- 要保护珍贵的漏洞信息不在调查中被发现
- 在发送攻击组件前进行更多的侦查工作
- 通过学习来确认是否有更小的漏洞可以利用

复杂的 UEFI 攻击

- Unified Extensible Firmware Interface (UEFI)
  是一种详细描述全新类型接口的标准，是适用于电脑的标准固件接口，传统BIOS技术正在逐步被UEFI取而代之，在最近新出厂的电脑中，很多已经使用UEFI，使用UEFI模式安装操作系统是趋势所在。
- 恶意代码直接通过UEFI运行启动，绕过所有的反病毒软件甚至操作系统
- UEFI 恶意代码最早出现在2015年
- 更多先进的功能, 越来越多的APT将使用到UEFI恶意代码

破坏性攻击持续增长

- Shamoon 破坏性恶意代码在4年后再次出现
- Shamoon 2.0 瞄准沙特阿拉伯的经济部门
- 大量的系统遭到破坏
- 新的磁盘擦除器StoneDrill攻击欧洲石油公司，Newsbeef APT
- ExPetr ‘磁盘擦除器即勒索软件’
- 在网络战中占据一席之地

越来越多的加密系统将被颠覆

- 政府机构提出物联网加密策略
- 公司要求具备特定的加密算法
- 密码安全产品被发现存在缺陷
- 更严重的加密漏洞将被发现并（希望）获得修补

KASPERSKY lab

电子商务领域的身份认证危机

- 2017 -个人可识别信息（PII）的大规模泄漏 例如：Equifax艾可飞
- 就目前的保护水平而言，各类组织和政府对互联网的使用是很难持续的
- 企业和政府将会面临选择：多因素安全 还是 减少数字化服务
- 减少因特网在政务流程中的使用并且减少运营成本

更多的路由器和调制解调器攻击

- 路由器和调制解调器是被低估的攻击工具
- 必备的设备，直面互联网，几乎从不打补丁
- 位于网络的关键节点
- APTs攻击者开始对这种设备产生重大的兴趣
- 利于持久、隐蔽的访问网络
- 可以方便攻击者冒充不同的互联网用户
- 通过指向不同的地址来隐藏踪迹

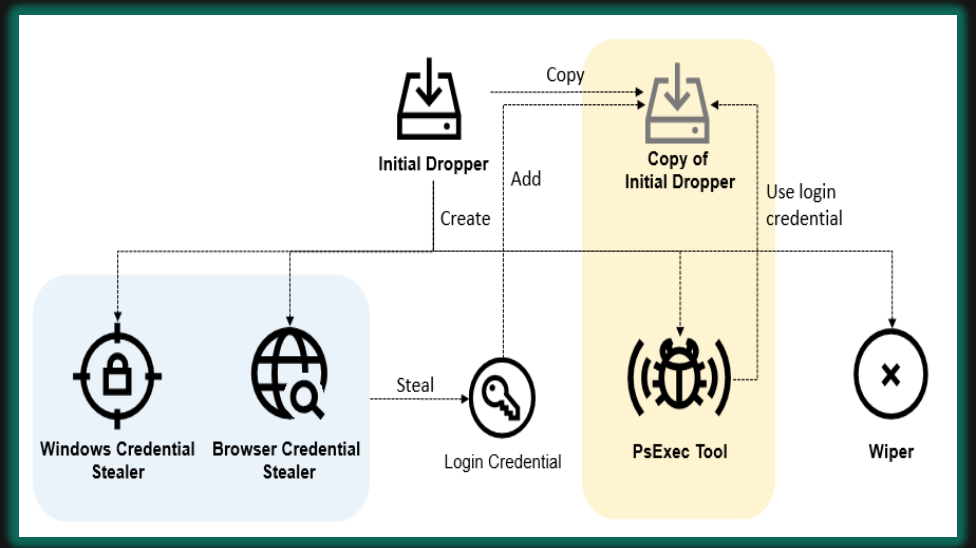
社交媒体的政治化作用凸显

- 社交媒体开始扮演了一个重要的政治化角色
- 全球需要对虚假用户和僵尸用户作真实性检查及鉴别
- 日益增长的巨型僵尸网络将被APT发起者所利用
- 用户对主要社交媒体网络的不信任和反感

反溯源

Olympic Destroyer

- 自我复制的网络蠕虫
- 收集用户账号信息
- Wiper（摧毁数据）
- 系统无法重启



反溯源

NotPetya?

Eternal Romance?

Chinese Hackers?

Lazarus?

卡巴斯基建议

- 把安全植入系统（Security by-design）
- 分层深度防御（Protection in-depth）
- 提升检测和响应能力（machine learning & intelligence services)

KASPERSKY lab

卡巴斯基威胁管理和防御平台

KASPERSKY
ANTI TARGETED
ATTACK:防御复杂的威胁

KASPERSKY
CYBERSECURITY
SERVICES: 安全服务

KASPERSKY
ENDPOINT
DETECTION AND
RESPONSE: 端点检测和响应


谢谢！
KASPERSKY lab