Cisco AMP Threat Grid

统一恶意软件分析和威胁情报

2014 年 10 月

简介

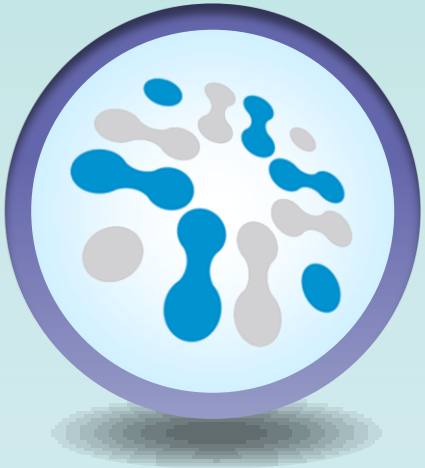
AMP Threat Grid 是第一款可扩展的统一恶意软件分析和威胁情报解决方案。

提交

- 分析人员或系统（API） 向 Threat Grid 提交可疑样本。

专有分析

- 自动化引擎使用多项技术进行观察、解构和分析。



更加丰富的内容集成

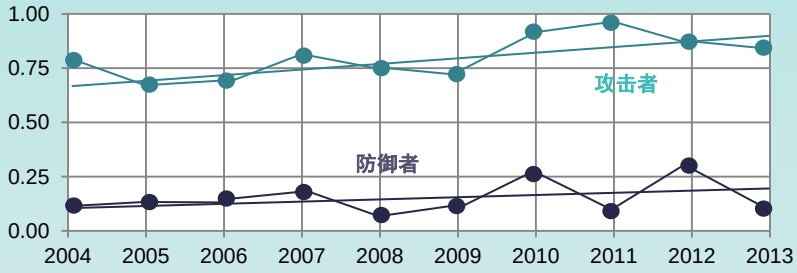
- 生成实用的威胁内容和情报，可以打包并集成到现有的各种系统或者单独使用。

实现前所未有的关联规模

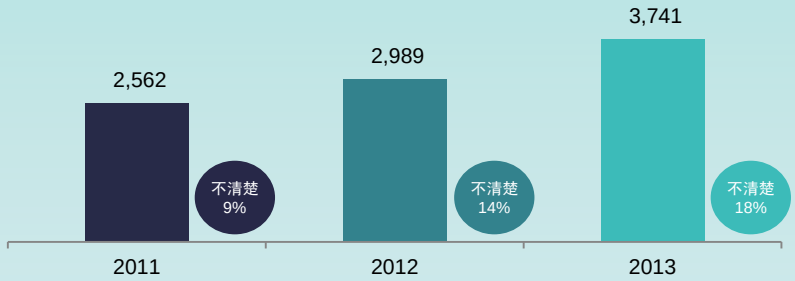
- AMP Threat Grid 平台将样本结果与上百万个其他样本/几十亿种人为因素关联起来。

快速演变的威胁形势

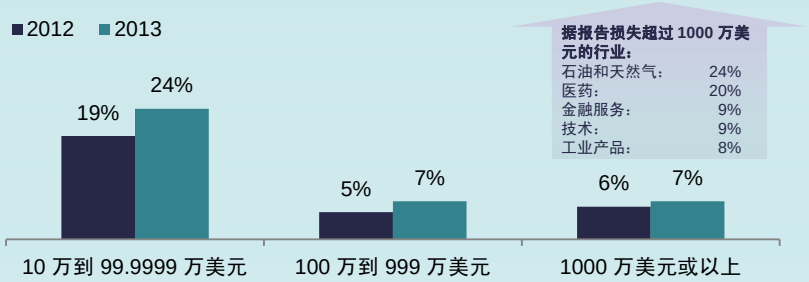
防御者跟不上变化。DBIR 2014 年



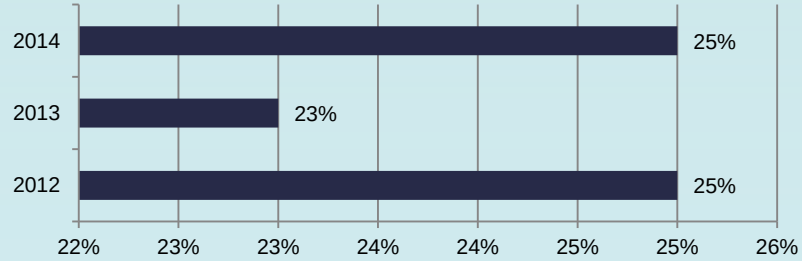
检测到的事件增加 25%。PwC 2014 年



平均损失增加 18%。PwC 2014 年



25% 到 50% 技能短缺。ESG 2014 年



http://www.verizonenterprise.com/DBIR/2014/
http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml
http://www.rsaconference.com/writable/presentations/file_upload/prof-m03a-the-security-staff-and-skills-shortage-is-worse-than-you-think.pdf

企业安全挑战

企业安全运营不堪重负，无法应对当前的挑战

有限的时间

如果需要数天、数周甚至数月时间来检测恶意软件，会给组织带来难以承受的损失

有限的知识

恶意软件分析人员成本高昂并且是稀缺资源

有限的财务资源

安全预算紧张；需要更加充分地利用现有投资

现有解决方案的局限性

现有解决方案无法跟上威胁形势的变化速度

	现有问题	说明
X	沙盒测试处于初级阶段	现有沙盒无力抵御高级威胁
X	分析质量低	准确性差，无历史回顾
X	缺乏可视性	对高级恶意软件的了解有限甚至毫无了解
X	不实用的威胁情报	给分析人员带来的价值有限
X	架构过时	无法通过扩展来处理大量数据
X	集成性差	无法充分地利用现有安全基础设施

如果您能做到以下几点，结果会怎样？

利用现有安全技术和资源抵御高级攻击

提高安全和响应团队的效率

更快地发现漏洞并更迅速地响应安全事件

Cisco AMP Threat Grid

统一恶意软件分析和威胁情报解决方案

- 积极主动。
- 更快恢复。
- 抵御高级威胁。
- 从现有投资中获取最大价值。

Cisco® AMP Threat Grid 颠覆了以往的方式，企业现在可以使用准确且情景丰富的恶意软件分析和威胁情报来抵御高级网络攻击。

改善防御并加速响应

Cisco® AMP Threat Grid 增强整个企业内部的安全职能：

SOC 团队	IR 团队	威胁情报团队	安全基础设施工程团队
获得更加准确的实用数据	使用证据确凿的信息更加快速地了解可疑行为	主动地改善安全基础设施	采用自动化方式，更加快速地利用威胁信息并采取应对措施

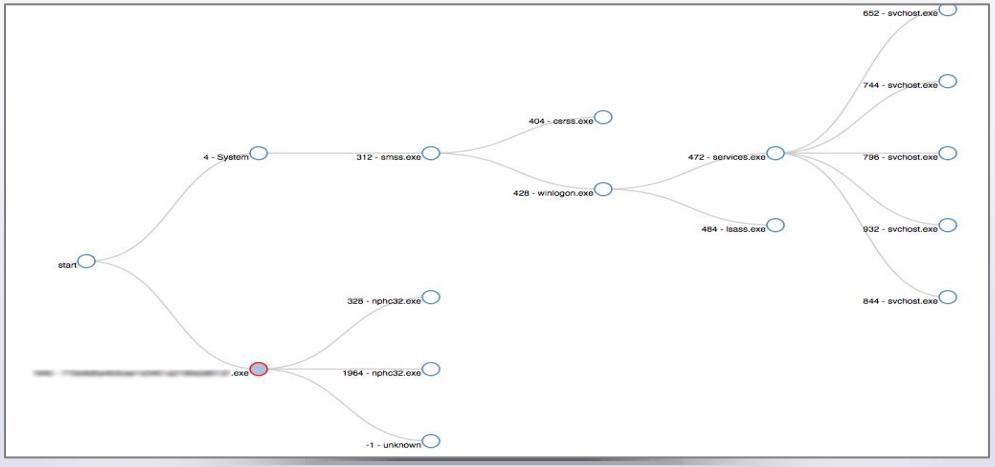
专有分析

“旁观者”方式

- 在 VM 中不出现

关于静态和动态分析的专有技术

- 观察对本地主机和网络通信的所有更改



例如，动态分析期间的流程树可视化

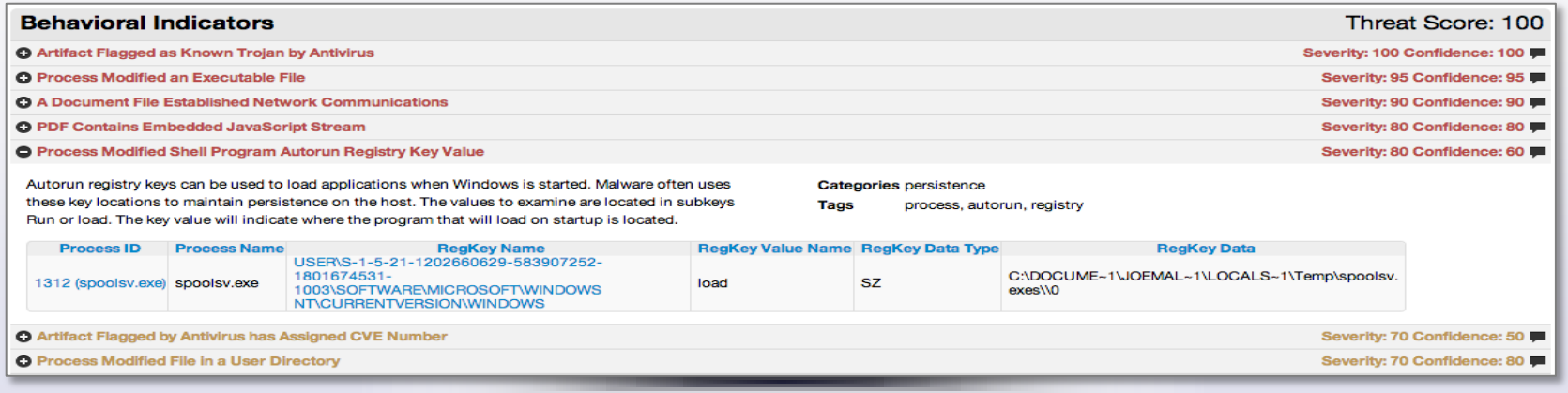
威胁指数

超过 300 个行为指标（还在不断增加）

- 恶意软件系列、恶意行为等等
- 详细的说明和实用信息

按把握程度划分威胁优先级

- 丰富 SOC 分析人员和 IR 的知识并提高效率（以及改进安全产品）



Behavioral Indicators — Threat Score: 100

- Artifact Flagged as Known Trojan by Antivirus — Severity: 100 Confidence: 100
- Process Modified an Executable File — Severity: 95 Confidence: 95
- A Document File Established Network Communications — Severity: 90 Confidence: 90
- PDF Contains Embedded JavaScript Stream — Severity: 80 Confidence: 80
- Process Modified Shell Program Autorun Registry Key Value — Severity: 80 Confidence: 60

Autorun registry keys can be used to load applications when Windows is started. Malware often uses these key locations to maintain persistence on the host. The values to examine are located in subkeys Run or load. The key value will indicate where the program that will load on startup is located.

Categories persistence
Tags process, autorun, registry

Process ID	Process Name	RegKey Name	RegKey Value Name	RegKey Data Type	RegKey Data
1312 (spoolsv.exe)	spoolsv.exe	USER\S-1-5-21-1202660629-583907252-1801674531-1003\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS	load	SZ	C:\DOCUME~1\JOEMAL~1\LOCALS~1\Temp\spoolsv.exes\\0

- Artifact Flagged by Antivirus has Assigned CVE Number — Severity: 70 Confidence: 50
- Process Modified File in a User Directory — Severity: 70 Confidence: 80

云的力量和规模

一个月 600 万到 1000 万个分析 （还在不断增加）

- 接近实时的分析

将每个样本分析与上百万个恶意软件人为因素进行关联

- 无与伦比的规模和全球威胁覆盖范围

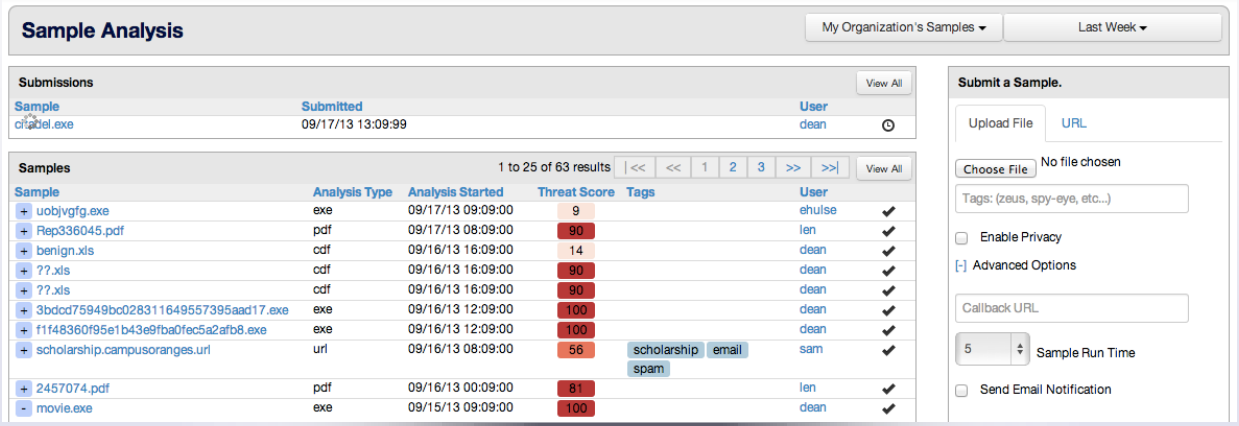
基于情景的恶意软件分析

接近实时且准确地识别攻击

- 详细的报告中明确了关键行为指标和威胁指数

能够围绕任何数据元素进行分析

- 在几分钟内即可下载分析 JSON



优质内容馈送

实用的威胁情报
- 主动拦截未来攻击，并充分利用现有安全措施

专门从针对实际攻击的专有恶意软件分析构建而成
- 带有情景的馈送（高度可靠 - 参考源样本）

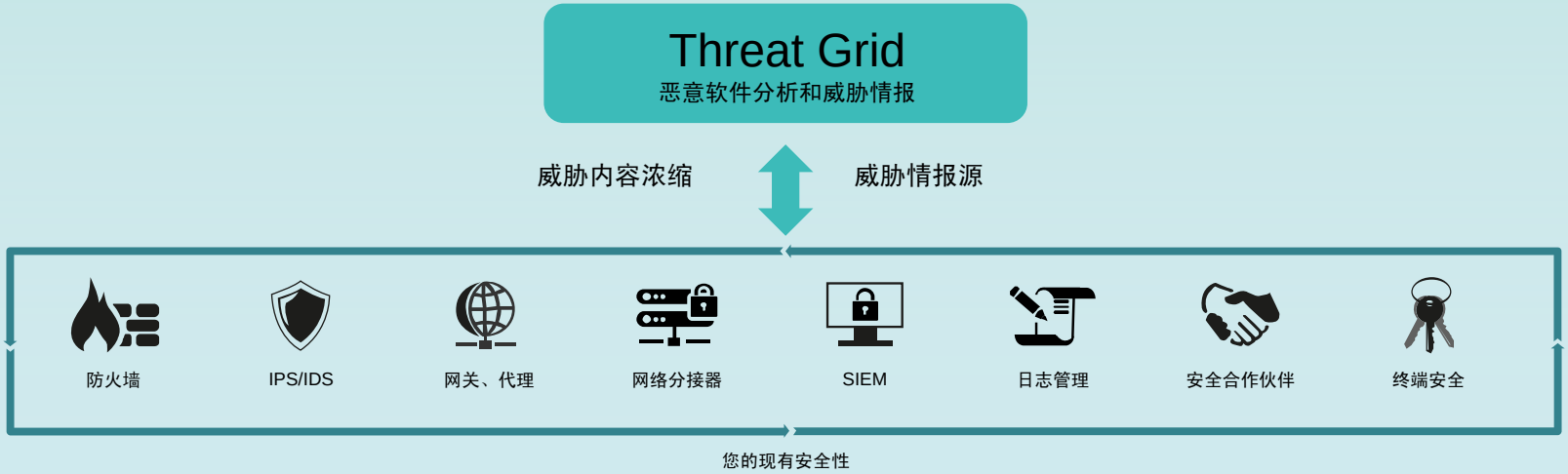
预封装或自定义的优质内容
- 各种木马病毒、RAT 等等
- 含有恶意通讯内容的 PDF 和 Microsoft Office 文档
- 威胁指数高的恶意软件
- 其他…

易于使用的标准格式
- JSON、CyBOX、STiX、CSV 和 Snort 规则
- 从 Cisco® AMP Threat Grid 云平台提供

安全集成和自动化

从现有安全投资中获取最大价值

- Cisco® AMP Threat Grid 的 REST API 可自动执行样本分析、浓缩和报告
  - 自动通过众多技术（主机或网络）进行提交
  - 将结果融入大量技术



内部设备

强大的安全性和合规性

- 利用 Cisco® AMP Threat Grid 云的完整功能进行本地恶意软件分析
- 为了满足政策法规的要求，所有数据都限制在内部
- 来自 Cisco AMP Threat Grid 的连续、单向联合数据流有助于确保情景的完整性
- 从云到设备（UI、API 等等）提供一致的用户体验

Cisco AMP Threat Grid 的独特价值

SOC | 调查和响应 | 威胁情报 | 安全基础设施工程

基于情景的恶意软件分析

云的力量和规模

威胁指数

专有分析

预封装的自定义馈送

API 集成和自动化

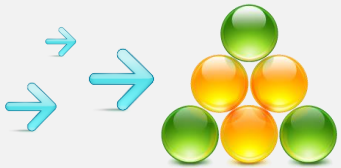
设备

Cisco® AMP Threat Grid 门户

抵御高级威胁 | 更加快速地恢复 | 积极主动 | 从现有投资中获取最大价值

客户成功案例：大型金融服务公司

挑战	解决方案	优势
▪ 大量攻击（高级攻击和常见攻击）	▪ Cisco® AMP Threat Grid 与邮件网关、SIEM 和 GRC 平台相集成	▪ 识别并消除恶意软件攻击 ▪ SOC 和 IR 团队采取更加有效和一致的行动



消费模式

Cisco® AMP Threat Grid 是一款平台解决方案，可以通过 Web 门户或 API 进行访问

- 年度订阅定价基于分析人员席位和样本

分发平台

- 云：位于美国的数据中心 （在 2015 财年扩大了地理范围）
  - 安全的逻辑访问和物理设施
  - 无外部云提供商元素：独立处理和存储（Cisco AMP Threat Grid 开发了 IP 和专用硬件）
- 设备：仅限用于本地分析
  - 适用于在提交其环境以外的恶意软件样本方面存在合规性和政策限制的企业
  - 与 Cisco AMP Threat Grid SaaS 解决方案相同的功能和用户体验
  - 客户必须订阅 SaaS，以便通过来自云的连续的联合数据流确保不会因为独立系统而失去情景关联性

致谢与后续步骤

有关 Cisco® AMP Threat Grid 的更多信息，请访问 Cisco.com

http://www.threatgrid.com

谢谢。