基于人工智能后发制人的网络安全新对策

邵江宁
(jnshao@microsoft.com)

AI Based Post Breach Cyber Security Strategy

Shao Jiangning

科技是国家强盛之基 . “云（计算）– 物（联网）– 大（数据）– 智（人工智能）”新信息技术创新点燃的第4次工业革命影响深远，蓬勃发展 . 全球产业变革加速演进，正在重塑世界竞争格局、改变国家力量对比 . 创新是民族进步之魂 . 中国经济发展进入新常态，必须依靠创新驱动打造发展新引擎，持续提升中国经济发展的质量和效益 . 全球的互联网用户、设备数量将以前所未有的速度增长，在线和移动应用的普及渗透正带动多元异构大数据流量实现爆炸性增长 . 在信息流的引领和带动下，物流、资金流在虚拟网络时空维度上高速交易流通，促进全球贸易的发展和经济融合，各个国家在发展进程你中有我，我中有你，更加紧密地联系在一起 .

在新形势下，新信息技术在多个维度上承载并被赋予了促进社会生产力要素相互连接、发掘潜能、实现希望，成就每一个组织和个人实现变革的“力量”. 面向未来，微软提出了三大有机统一的愿景：重塑生产力和业务流程、构建智能云平台、创造更个性化的计算 . 微软的使命是“予力全球每一人、每一组织成就不凡 . ”许多个人或者组织给微软的反馈是他们期待自身能力的提升，让他们有机会去实现更大的价值，这对微软来说是一个极大的鼓励，当社会对于通过技术创新变革的渴望超出微软的预期时，微软便深感责任重大 .

今天微软有机会服务全球的数以十亿计的网络信息系统用户，已经不能只思考技术如何让微软的收入最大化了，微软必须考虑自身的社会责任和企业使命，积极主动、务实的理解、关照、响应用户重要的利益诉求或困扰 . 保障网络信息安全是微软责无旁贷的责任和使命之一 .

安全和发展是一体之两翼、驱动之双轮 . 安全是发展的保障，发展是安全的目的 . 从黑客猎奇到网络犯罪，从个人隐私到国家机密，从网络病毒到网络攻击，我们在网络空间中面临着相同的问题 . 网络安全是全球性挑战，没有任何人能够置身事外、独善其身，维护安全是网络空间所有利益相关方的共同责任 . 个人、商业组织、政府和公共机构在分享技术创新带来的巨大红利的同时，也面对日益复杂的网络与信息安全、个人隐私和商业信息安全、公共健康和安全、经济安全、国家安全等领域的挑战，这也是数字经济转型和现代政府治理的关键 . 正如习主席在西雅图会见中美互联网论坛主要与会代表时所指出的，在社会信息化迅速发展的今天，互联网无处不在，一个安全、稳定、繁荣的网络空间对一国乃至世界和平与发展越来越具有重大意义 .

安全是今后10年万物互联环境的基础 . 只有通过广泛、密切和深度的安全协作和遵循业界久经检验的最佳安全实践做法，才能更好地保护公共健康和安全，提高经济创新，巩固国防以及实现我们对未来共同的承诺 . 因此我们要重视安全产品开发、供应链安全和运维操作安全，重视制定更有效的网络安全政策 .

网络安全威胁影响巨大

今天的匿名攻击者可以以光速（150 ms 的击键时间即可绕地球一周）进行远程攻击．移动设备（可能在安全性方面落后于传统个人计算机和便携性较低的设备）激增以及全球互联网用户数量的增长为匿名攻击者的恶意攻击创造了新的条件，如图1所示，万物互联时代最大的安全挑战是绝大多数的互联网用户在购物、社交、工作等方方面都将自己的身份信息“袒露”给了互联网，网络安全威胁和恶意网络攻击的特性正在改变，发动网络攻击所需要的技术门槛越来越低，攻击的频率和复杂性越来越高：

- 网络攻击造成巨额财物损失，2014年网络犯罪对全球经济造成的潜在损失 (Source: CSIS–McAfee Report) 估值为5 000亿美金，约占互联网经济创造价值的1/4;
- 影响品牌声誉，丢失敏感数据，公司高管被离职，商业公司由于数据破坏造成的平均损失约为350万美金 (Source: Ponemon Institute Releases 2014 Cost of Data Breach)；
- 发动大规模攻击，目标瞄准侵害用户的身份，75% 以上的网络入侵归因于用户身份的失窃 (Source: Verizon 2013 Data Breach Investigation Report)；
- 直到被发现前，攻击者在被侵入的网络中平均隐身8个月；
- 被发现的恶意软件大多是那些运行出错的；
- 攻击者使用合法的 IT 工具而不是恶意软件，因而难以被探测．

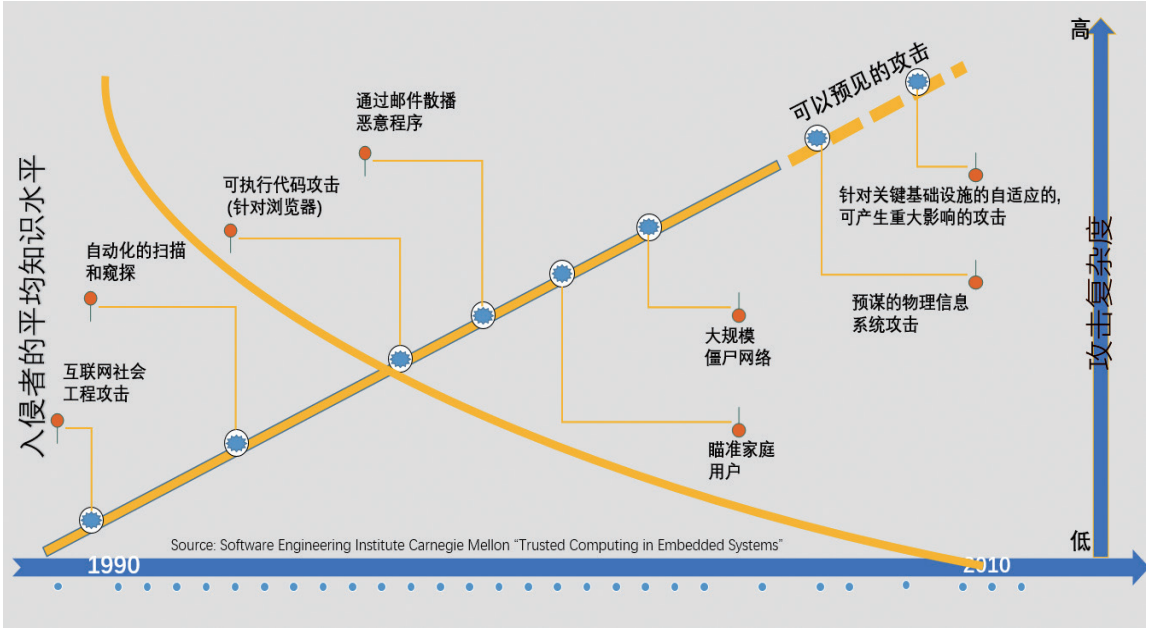


图 1 攻击的复杂度与入侵者所需要的技术

传统的网络安全策略快速失效

与恶意软件的对抗是互联网用户最关心的网络安全典型挑战之一．今天，通过购买、使用反恶意软件产品和服务来阻止大规模复制恶意软件的战斗还在进行，但是一种新型、更复杂、有针对性、强烈动态对抗性的高级持续威胁 APT(advanced persistent threat) 正在成为网络安全的主战场．

由于现有反恶意软件产品自身能力的限制，以及在实施漏洞补丁及时阻止网络攻击方面遇到的困难（如0天级漏洞），攻击者可以轻而易举地绕过恶意软件防御．

一项调查显示压倒性的（81%）被访用户认为现有反恶意软件解决方案并不是他们未来防御高级攻击的策略的一部分．

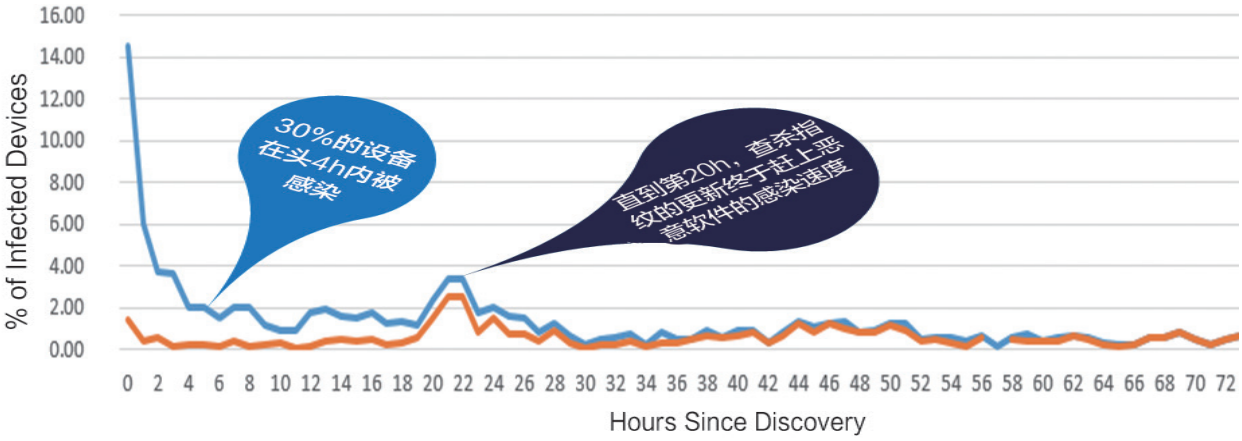


图 2 被恶意软件攻击的设备占比

通常传统的 IT 安全方案，具备如下特点：

- 非常复杂，初始设置、调优、定义规则、配置阈值 / 安全基准线，需要较长时间，反应迟缓；
- 容易误报，每天接收海量的报告，其中夹杂误报，要求用户投入其无法负担的宝贵时间去调查，效率低下；
- 设计用于边界防御，当用户身份被窃取而攻击者藏身于内网，现时的防御提供的保护及其有限 .

今天的恶意软件迭代进化周期比基于传统反恶意软件的查杀指纹更新的保护机制要快得多，如图2和图3所示 .

- 大多数恶意软件7h 内实现恶意的或者经济的目标；
- 85% 的恶意软件使用“一次性可见”文件包装，通过频繁变更文件名称和特征来对抗反恶意软件的查杀；
- 99% 恶意软件具有对抗杀毒引擎的逃逸机制；
- 恶意软件释放的恶意负载及其投递更加多变和灵活 .

美国联邦调查局局长 James Comey 2014年10月的一次演讲中提到“只有2类公司：那些已经被黑客入侵的、和那些还不知道他们已经被黑客入侵的”. 70% 的高管对自己公司在网络安全策略和防御措施上是否到位不再具有信心 . 必须采用新网络安全策略和方法 .

安全创新永不停歇

多年来，微软在应对网络威胁、保障信息安全方面被视为行业典范和标杆 . 微软长期高强度

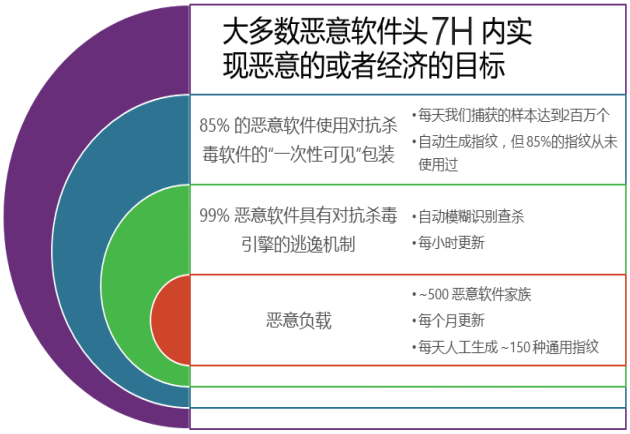


图 3 大多数恶意软件头 7H 内实现恶意的或者经济的目标

地投入巨量的人力物力保障网络安全，在理念和技术上不断创新．同时，微软积累了数10亿客户管理网络安全风险的经验，这些经验使微软可以深入了解并预估当前和未来的种种挑战．微软在产品和技术发展的重大战略规划过程中始终关注网络与信息安全，特别致力于开发和提供安全优质的产品和服务．

安全能力的持续创新是微软保持行业和市场竞争优势的重要基础．早在2002年，微软创始人比尔·盖茨宣布“在增加新功能特性和解决安全问题之间进行选择时，微软选择解决安全问题”，为微软之后的战略发展指明了方向．在微软10多

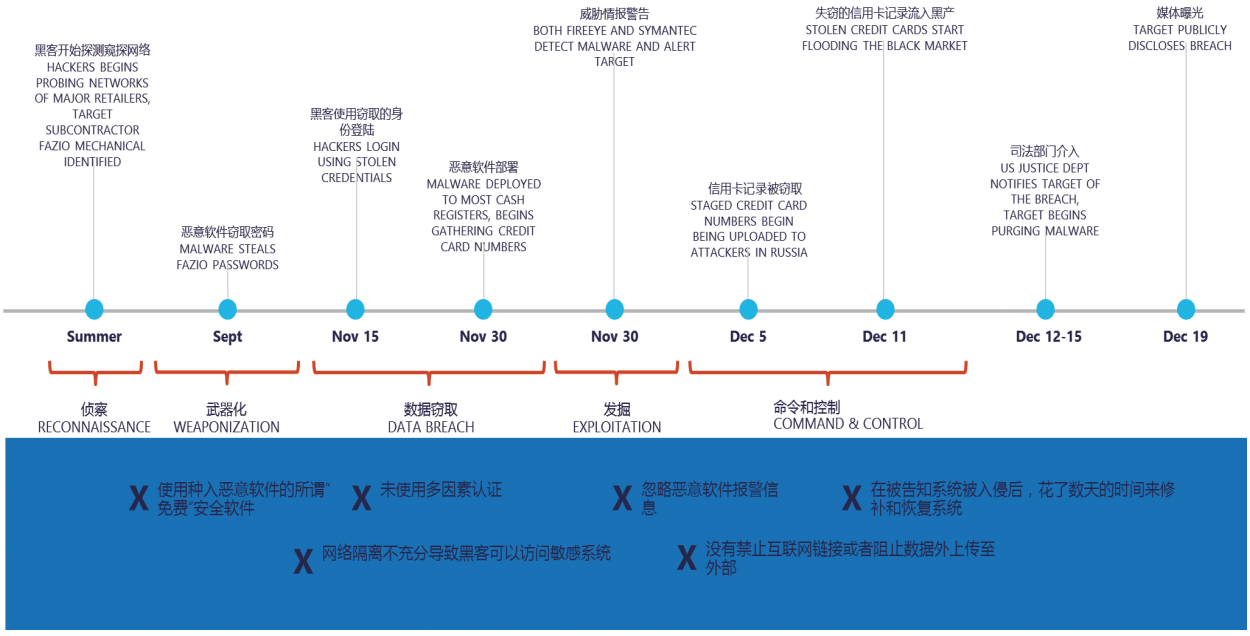


图 4 后发制人策略（The Post-breach Approach）

年来践行网络安全承诺的历程中，提高产品的安全和隐私性、服务的透明和可靠性正变得前所未有的重要．

微软拥有丰富的管理网络安全风险的经验，能够深入了解用户在应对与网络安全相关的计划和法规时所面临的问题．

1）后发制人（The Post-Breach approach）

网络安全的本质是正反双方的动态攻防对抗．当今主流的反恶意软件终端安全解决方案，大多专注于先发制人的方法（pre-breach approach）：守好网络边界，御敌于国门之外，通常会检查网络流入的文件和内存中可能隐藏的恶意内容，并实时阻止传输．但是，尽管抱有美好的期望，这种方法并不保险，也并不能防止有决心、有雄厚资金、掌握复杂的技术手段的攻击者使用诸如零天攻击、社会工程和非恶意工具来获取访问、权限和控制．一个新的后发制人的安全策略是对先发制人策略的必要的补充．

与先发制人的策略不同，后发制人的策略假定网络入侵已经发生．作为一个飞行记录器和犯罪现场调查员（CSI），监控网络终端节点上发生的安全事件，利用大规模的相关性分析和异常检测算法发现事实和证据，对正在发生的攻击活动进行报警．后发制人的策略利用攻击者在初始入侵行动后需要执行多个行动，如：侦察、隐藏和移动、在网络上寻找高价值的资产、信息提取．如图4所示，后发制人策略提供安全团队所需要识别的信息和工具，调查和响应传统监控方案通常会忽略的攻击．

这种后发制人的新策略获得了全球安全研究人员的广泛认可，并由此诞生了一个新的安全细分市场，EDR（Endpoint Detection and Response）by Gartner 或者 STAP（Specialized Threat Analysis and Protection）by IDC. 企业应当采用更多的基于探测和响应技术，关注于无查杀指纹的威胁、具

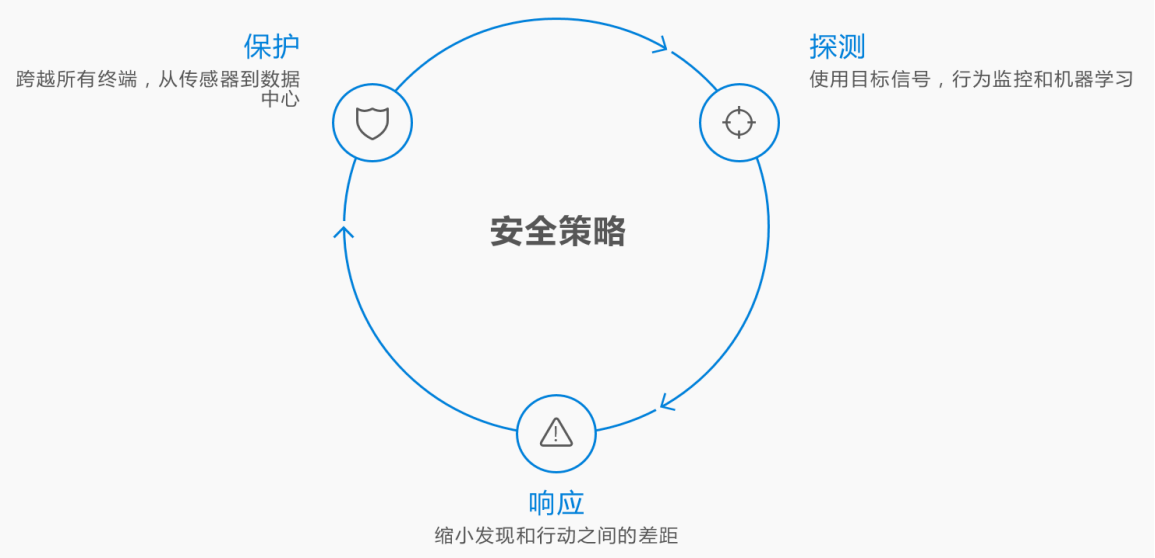


图 5 安全策略

有能够分析逃避主流安全技术检测的安全威胁能力的方案，来补充自身的终端威胁安全保护产品 .

2）360 度网络安全保障

需要强调的是，网络攻防对抗的本质是正反双方能力的较量，后发制人与先发制人安全策略两者是互补关系 . 为了应对以高级网络安全威胁为代表的攻击杀伤链条，“后发制人”策略为反恶意软件和其他“先发制人”安全防御能力提供反馈，特别是可能错过或遗漏的信号和文件样本，最后形成保护（protect）– 探测 (detect) – 响应 (respond) 360度的、完整闭环回路，如图5所示 .

图 6 安全方法

在分析当代、预判未来高级网络安全威胁的基础上，微软为企业和用户提供全球格局层面360度的网络安全保障服务，更好响应前述网络攻击杀伤链条威胁，增强安全产品部署，提升操作安全性以及防御社会工程攻击，

微软网络安全实力来源于每年在网络安全上高达10亿美金的高强度持续研发投入，以及世界级的杰出安全人才团队辛勤的安全研究工作，如图6所示 .

- 通过全球互联网搜集、监控网络安全威胁情报，实时监控网上出现的新型攻击和威胁数据；
- 经常性地发掘安全洞察或者网络威胁情报，由专业的安全研究团队分析和处理；
- 跨微软产品和服务平台，进行威胁情报信号分享和整合；
- 专业的网络安全团队负责具体的安全专业领域，如法证和网站攻击探测，研发令人激动的经过验证和调优的新检测算法 .

人工智能助力高级威胁响应

作为后发制人安全策略的实际应用，微软高级威胁分析使用行为分析来为正常的实体行为画像 . 通过利用机器学习和人工智能来识别用户和其他实

图 7 安全策略

体在其交互关系中的正常行为 .

在分析大量的高级网络攻击实例后，我们发现，在用户行为分析中仅使用机器学习算法不足以检测高级攻击：在大多数情况下，算法将在事实之后检测异常，攻击者可能已经撤离了 . 检测高级攻击的方法是通过检测安全问题和风险、TTP 实时攻击，以及利用机器学习算法的行为分析的组合 . 因而微软高级威胁分析把用户网络行为分析与已知恶意攻击、安全问题和风险的检测结合起来，以提供全面方案，如图7所示 .

数据源是检测高级攻击的魔法的关键要素 . 仅仅分析安全日志只会告诉你一半的故事，甚至会提供假阳性误报 . 真实证据位于网络数据包中 . 因而要把深度数据包检查（DPI）、日志分析和 Active Directory 中信息的组合来检测高级攻击 .

1）360 度网络安全保障

①快速

无需创建规则、阈值或基线 . 快速检测可疑活动，利用 Active Directory 流量和 SIEM 日志 . 传统的 IT 安全工具遇到复杂的安全漏洞或用户凭据被盗时，仅仅提供有限的保护 . 安全工具的初始设置，创建规则和微调可能很繁琐，需要多年的学习和适应 . 微软的高级威胁分析技术借助内置的人工智能，部署后，可以不断学习和改进，无需创建规则、阈值或基线，然后微调 . 通过分析用户，设备和资源之间的行为以及它们之间的关系，快速检测可疑活动和已知攻击 .

②学习和自适应

利用人工智能算法进行自主学习行为分析，识别异常行为 . 在不断变化的网络战术的世界里，你必须像攻击者一样快速适应 . 一旦部署将不断分析和学习实体行为 . 微软高级威胁分析能够适应变化，使用其专有算法识别异常行为并报告异常 . 微软高级威胁分析是当今唯一的基于用户行为分析的安全解决方案，将动态提示用户并自动调整其学习和检测功能 .

③提供清晰可行动信息

功能化、清晰、可操作的攻击时间线，近实时展现：谁、什么、何时和如何攻击等细节，安全管理人员的工作已经具有挑战性，即使没有关注多个安全报告和接收误报 . 攻击时间轴线是为了简化而创建的，用方便的方式实时表示重要的相关事件 . 虽然该技术非常复杂，但报告清晰，功能性强，并且可以提供可行动的建议和后续步骤 .

④警报适时

将实体的行为与其画像进行比对，但也与其他用户进行比较，因此只有在经过确认时才会引出警报 . 微软高级威胁分析穿透混乱，显示最相关的攻击数据，而不是误报 . 并且在发出安全警报前根据情况聚合归并所有的相关可疑活动 . 为了进一步提高准确性并节省时间和资源，微软高级威胁分析不仅将实体的行为与其自身的行为进行比较，还与其他实体在其交互路径中的行为进行比较 . 这意味着错误报警信息的数量大大减少，安全管理人员可以专注于真正的威胁 . 报告在所提供的信息中是清晰、功能性和可操作性的 . 简单的攻击时间轴线类似于网络界面上的社交媒体馈送，并以易于理解的方式描述安全威胁事件 .

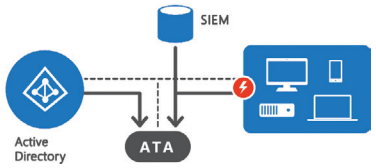
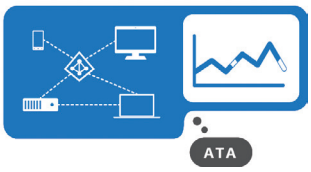
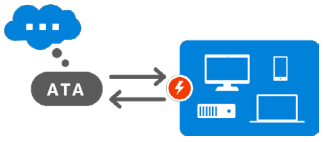
1	分析	Analyze 	• 非侵入式、监测可疑流量和网络日志 • 对攻击方隐身 • 分析认证日志 • 从 SIEM 和活动目录认证信息，收集安全相关事件
2	学习	Detect 	• 自动学习和对实体行为建立网络行为画像 • 识别实体的正常行为 • 连续学习并更新用户、设备和资源的活动
3	探测	Learn 	• 寻找异常行为，识别可疑活动 • 当且仅当异常行为是与背景聚合关联时报警 • 基于攻击者的攻击战术、技术和程序（TTP），利用世界级的安全研究来近乎实时检测安全风险和发现攻击行为 • 高级威胁分析不仅将实体的行为与其自身进行比较，而且还与实体在其交互路径中的行为进行比较
4	警报		• 在一个简单、功能化、可操作的攻击时间线上报告所有可疑活动 • 识别谁？什么？何时？怎样？ • 对于每个可疑活动，ATA 提供调查和补救的建议

图 8 高级威胁分析工作原理

安全问题和风险

- 断裂的信任
- 脆弱协议
- 已知的协议漏洞

异常行为

- 异常登录
- 远程执行
- 可疑活动

恶意攻击

- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Skeleton key malware
- 网络侦察
- 暴力破解
- 未知的威胁
- 密码共享
- 横向移动

图 9 高级威胁分析可以识别的安全威胁类别

2）高级威胁分析的效果

①通过行为分析快速探测威胁

无需创建规则或策略，部署代理或监测海量的安全报告，人工智能可以分析和不断学习.

②永远比敌人领先

高级威胁分析不断从组织实体（用户、设备和资源）的行为中自动学习，并不断自适应地调整自身以反映用户网络快速的变化.随着网络攻击者战术变得越来越复杂，高级威胁分析可通过持续学习行为分析来适应网络安全攻击的不断变化的性质.

③使用攻击时间线快速找出并关注于重点

提供后续安全响应行动步骤的建议.传统安

全工具不断产生海量的报告，然后企业安全团队通过细致的筛选找到重要和相关攻击，许多安全告警信息淹没在噪音中都没有被关注．攻击时间轴线是一个清晰、高效、方便的摘要，在时间线上展现准确的情报，了解组织内部“谁－什么－何时－如何”，提供用户强大的安全态势感知能力．

④降低误报．

坚持开放、发展的网络安全观

微软植根中国20余年，始终致力于建设一个包容本土安全生态圈在内的完善的生态系统．生在本地，长在本地，留在本地，微软通过与各方的深入合作，积极发挥自身技术优势，以技术创新和发展模式创新相结合的方式推动经济发展和产业升级，从而达到加速中国发展，努力实现多方共赢的目的．在开放的环境下，端到端的网络高度关联、相互依赖，网络安全问题也呈现出开放而非静止、封闭的状态．微软认为，业界各方只有立足开放的大环境，开展日益密切的交流、合作与互动，才能真正实现动态、综合的网络防护．

2015年在美国西雅图举行的中美互联网论坛上，中美双方表明了“发展互利共赢的中美互联网合作”以及“共同维护网络安全”的立场，这与微软一如既往所坚守的理念不谋而合．微软自始至终倡导合规、透明的网络安全技术，秉持开放、合作、互利、共赢的理念，愿与全球范围内特别是中国合作伙伴合力研究解决网络安全相关问题，维护两国人民的根本利益，让互联网更好地造福全人类．

1）倡导

在信息产业领域，微软与业界始终倡导并执行全球网络安全的最佳保护实践．通过与业界和政府合作，微软在应对新的网络威胁和打击全球网络犯罪中屡屡扮演关键角色．

2）协作

微软高度重视与中国政府相关安全部门的紧密协作．微软通过分享先进技术和经验，在公开透明的基础上加强协作，助力相关安全部门提高信息产品供应链安全性，预防和打击网络攻击．

自2003年起，在中央政府的授权和批准下，微软与国家有关安全部门深度合作，签署了政府安全项目协议（government security program，GSP），对中国政府指定的安全部门持续开放微软在国内销售的关键软件产品的源代码，确保政府安全部门能够在线访问审查产品的安全．同时，微软产品部门对政府安全部门开放共享主要产品设计开发的重要技术文档、产品测试文档、产品安全漏洞通告以及全球网络威胁预警信息．中国也是全球首批与微软签署此计划的国家之一．并在国内建立了“微软技术透明中心”．政府及其授权的政府机构将可以在该中心内运用测评工具，静态和动态测试，深度分析、评估、微软产品和服务的源代码．

3）合作

微软深刻践行安全应用即服务的理念．为了方便本土用户择优自主在应用程序商店获取、使用更具针对性的网络信息安全产品和服务，微软通过将众多可信安全伙伴解决方案无缝集成在产品服务开放平台上的方式，与本地合作伙伴共同捍卫网络安全．

Windows 操作系统在全球范围内之所以能获得成功，与全球范围内合作伙伴尤其是 Windows 在本地的 ISV 独立的安全伙伴的大力支持密不可分．目前，微软已与中国的 BAT、奇虎360等本土合作伙伴携手，向独立软件开发商开放安全平台，为中国用户提供更为安全的产品与服务，以建立更完善的网络安全生态．随着更强、更安全的 Windows 10的问世，全球范围内迎来了新一波 Windows 升级潮．在中国，联想、百度、腾讯、奇虎360等合作伙伴共同参与并推动了中国用户 Windows 10 的升级服务．

微软积极与国内领袖企业如华为、阿里巴巴开展合作，提供产品安全开发的培训支持，助力国内企业提升自主开发安全可控产品的能力．

结　语

人类只有一个地球，各国共处一个世界．今

天中国已经拥有全球最大的互联网用户群体，在“中国制造2025”、“互联网+”、“大数据发展纲要”等创新发展战略政策的指导和推动下，新一代信息科技正在快速融合、渗透到社会和行业各个领域.互联网是人类现实空间在虚拟空间的延伸，信息网络作为现代社会的“神经中枢”，虚拟网络与现实社会相互交织.因此，共建网络空间命运共同体是共建人类命运共同体的重要组成部分.

微软将秉承自己的未来使命，继续开拓创新之路.微软愿意同政府、企业和用户携手奋斗，创建更安全、更值得信赖的计算体验，遏制信息技术滥用，打击网络犯罪等现象，共同构建与维护和平、安全、开放、合作的网络空间.

邵江宁

现任微软中国首席安全官，负责微软在中国市场的网络信息安全政策和隐私保护战略的支持、执行，以及基础系统软件、大数据、云计算、人工智能平台等产品的安全技术市场布道，推动国际领先的安全技术、安全运营最佳实践经验落地于中国市场，与政府、安全机构、产业界紧密合作打造网络安全命运共同体.同时，作为政府与公共事业部的首席架构师，邵江宁先生还负责微软中国政府与公共事业部的垂直行业业务解决方案在市场推广，如智慧城市、智慧医疗、智能制造、公共安全等.邵江宁先生曾在全球大型跨国公司包括摩托罗拉，谷歌旗下移动业务子公司担任中国/亚太区首席信息安全官，具有15年以上的网络安全专业经验.

jnshao@microsoft.com