AhnLab

安全月刊

2019.10 Vol.83

AISF 2019

AhnLab举办2019年综合安全会议“AISF”

从威胁情报到云，解析网络安全的现实

9月25日，AhnLab在首尔Grande Intercontinental大酒店举行了面向企业、金融和公共机构安全人员的综合安全会议“Anlab ISF 2019”。本次活动包括全球最大的企业增长咨询公司Frost&Sullivan弗若斯特沙利文咨询公司（以下简称“沙利文公司”）的安全分析师Kenny Yeo的主题演讲，以及有关最新安全趋势和响应策略为主题的各种会议发表。此外，还通过运营展位展示了AhnLab的最新产品和服务，以及演示和客户可以亲自参加体验的各种活动。

今年迎来 11 届的 AhnLab ISF（AhnLab Integrated Security Fair， 以下简称“AISF”）2019 的主题是“安全推动未来转型（Driving Transformation beyond the NEXT）”。在本次活动中，AhnLab 专注于最新的 IT 和安全主题，例如 5G、OT、SOAR、威胁捕获（Threat Hunting）和威胁情报（Threat Intelligence），并通过“下一代安全战略”和“最新攻击技术和响应”两个会场进行会议发表。展位还现场演示了 AhnLab 最新的安全解决方案，并通过在整个场地举行的各种活动和展示会现场回答了客户的问题。

▲ AhnLab首席执行官权治重

AhnLab 首席执行官权治重在本次活动中通过欢迎辞表示：“基于 ICT 的数字化转型的成功取决于安全。AhnLab 将对不断变化的客户环境和数字化转型需求做出敏捷的响应。”

▲ 700多名安全官员参加了上个月举行的AISF 2019活动

沙利文公司的分析师 Kenny Yeo 发表了主题演讲，题为“亚太地区网络安全格局的变化（The Changing Cyber Security Landscape in Asia Pacific）”。 他说：“随着 5G 技术的数字化转型的加速，IT、OT 和 IoT 的融合将进一步加强。” 还指出：“由于安全入侵事件（例如客户信息泄漏）造成的企业损失比公司认为的更加长、更糟。在数字化转型时代，安全将成为企业的重要业务价值和竞争优势。”

▲ 沙利文公司的分析师Kenny Yeo和AhnLab常务理事Sangkook, Lee

AhnLab 常务理事 Sangkook, Lee 以“安全响应的实体（The Reality of Security Response）”为主题，强调了采用新的安全策略以及威胁响应的范式转变的必要性。Sangkook, Lee 对比说明了攻击者和作为防御者的安全官员的观点，并说：“当前的以单点解决方案为中心的响应很难取得效果。”他强调：“当各解决方案在一个平台上有机运行时，不仅可以最大程度地减少攻击的范围，而且可以防止持续的威胁损害，并为将来的攻击做准备。”另外，关于最近作为下一代安全解决方案受到关注的端点检测和响应（EDR）解决方案，他指出：“EDR 提供可见性，可以通过获取证据数据来验证安全事件的有效性并确定响应优先级。它不是原封不动地运营建立（Set up）的解决方案，而是通过客户和安全公司之间共享和协作威胁信息而增强（Build up）的解决方案。”

AhnLab 追踪不断变化的威胁的实体

最近，国内外媒体的报道显示出对国家资助（State-sponsored）的黑客组织正在受到注目。AhnLab 持续监视和发布有关已对韩国国家机构和企业发起攻击的多个攻击组的报告，包括最近成为话题的 Andariel 组织。在本次活动中，AhnLab 分享了有关最新威胁趋势的详细信息，包括针对韩国国家机构和企业的针对性攻击。

▲ AhnLab ASEC响应小组负责人Taehwan, Park和首席研究员Minseok, Cha

AhnLab 的 ASEC 响应小组负责人 Taehwan, Park 就安全威胁的最新趋势作了演讲，重点关注韩国国内公司和机构的安全入侵事件。他说：“近年来，攻击组织之间已经结成联盟并进行合作以谋取更大的利润。这就是为什么针对国家机构和企业的高级持续性威胁（APT）数量不断增加的原因。”他强调:“虽然针对个人用户的勒索软件规模有所减少，但仅针对特定行业和特定组织的针对型勒索软件的攻击正在上升。需要持续监控威胁引入的各种路径以及对每个攻击阶段的响应。”

AhnLab 分析研究团队的首席研究员 Minseok, Cha 以“穿越韩国和日本的 Tick 组织的实体”为主题，详细介绍了有关 Tick 组织的攻击方法和最新攻击案例。Minseok, Cha 说：“Tick 组织的活动长达 10 年时间，各种各样的恶意代码已经被发现，为了避开安全分析家的分析，使用各种攻击手段。特别是，由于捕获到与其他攻击组织有相关的许多情况，因此应制定各种检测规则以快速检测恶意代码的变种和潜在威胁。”另外，他还建议：“就像 Tick 组织的事例，为了响应有组织的且持续展开的针对性攻击，要确保对进入企业内部的所有威胁的可见性，处理当前存在的威胁，还要防止将来通过同一路径进入的攻击。”

如何响应勒索软件的针对性攻击

与去年相比，今年勒索软件的数量和感染的频率总体有所下降。然而，它变成针对企业的针对性攻击，以获取更大的收入。在韩国，典型的例子是 Clop 勒索软件。据说 Clob 勒索软件的幕后黑手是俄罗斯攻击组织，该勒索软件仅在韩国就已破坏了 13,000 多个系统。

▲ AhnLab资深研究员 Myeongsu, Lee和EP咨询团队次长 Byungmoo, Ahn

AhnLab 分析研究团队资深研究员 Myeongsu, Lee 通过主题为“APT + 勒索软件”的演讲，详细解释了基于 MITRE ATT&CK 框架的 Clop 勒索软件的攻击方法，并演示了实际攻击过程。Myeongsu, Lee 说道：“90%的 Clop 勒索软件受害是通过电子邮件感染的，从攻击 Active Directory（AD）这一点可以看出是一个针对企业的针对性攻击。Clop 勒索软件体现了高度复杂技术，使用分阶段（Staging）技术（例如分阶段进行感染并运行，分散攻击源等）以避开安全解决方案或分析人员的检测和响应。”还说道：“尤其在某些情况下，勒索软件不运行或在加密文件的同时窃取用户的电子邮件帐户。要响应针对性的勒索软件，要求在检测并删除勒索软件之后也要持续监控内部系统，以识别潜在威胁和痕迹并主动响应后续攻击。”

AhnLab EP 咨询团队次长 Byungmoo, Ahn 以“$how Me the Money? Drop the Clop!”为主题，介绍了 Clop 勒索软件的受害事例和有效的响应方案。他说道：“最近针对国内外企业的针对型勒索软件增长的原因也是收入（Money）。尽管引入了各种安全解决方案，但是由于他们无法有机地工作，因此无法有效响应。”还强调：“利用已知的漏洞的持续攻击证明了企业的补丁管理存在限制。建立基本的防病毒和补丁管理、内部重要系统访问控制，同时跟踪端点上的威胁并通过网络和端点之间的链接来建立全方位的响应机制，这一点很重要。”

Time to Hunt！威胁响应也是“情报之战”

安全人员最为关心的部分仍然是“威胁响应”。这就是为什么人们经常谈论“威胁情报（Threat Intelligence）”或“威胁捕获（Threat Hunting）”的原因。

▲ AhnLab产品规划团队负责人Changhee, Kim和EP咨询团队部长Minkyoung, Baek

AhnLab 产品规划团队负责人 Changhee, Kim 以“威胁情报，专注于实效性”为主题，发表了威胁情报的定义和如何在企业使用它。Changhee, Kim 说：“威胁情报是基于证据的威胁数据知识，并用作做出响应威胁的决策的基础。虽然很多企业提供威胁情报，但他们需要检查该信息在企业环境中是否有效以及公司可以实现目标。”还说：“AhnLab 分析从端点收集的实际威胁信息，提供有效的威胁情报，反映到产品中，并以各种内容提供给顾客。”最后表示：“我们将根据客户的需求，将威胁情报作为一个服务实时共享和利用。”

AhnLab EP 咨询团队部长 Minkyoung, Baek 以“通过 EDR 解决方案的威胁响应事例“为主题介绍了利用 EDR 解决方案的主动响应方案和威胁捕获战略。Minkyoung, Baek 说：“当前攻击的主要特征是威胁在目标内部的停留时间（Dwell time）很长。因此，我们需要跟踪隐藏的威胁，并在损害发生之前识别并做出反应。”这是威胁捕获（Threat Hunting）的开始。EDR 收集并分析端点上的行为日志，以识别威胁访问的文件，尝试提升特权等隐藏的行为意图。他强调：“通过 EDR 掌握入侵原因并防止再次发生，可以将损害的范围和规模最小化。还可以将 EDR 的收集和分析结果链接到连接策略和响应，可以主动应对可能发生的威胁。”

扩大的安全领域，云和运营技术（OT）

近来，随着韩国企业基础架构的云迁移加速，对云安全的关注也在增加。

▲ AhnLab常务理事Youngjin, Rho、安全架构团队负责人Chulmin, Park和EP技术支持团队课长Byungju, Kim

AhnLab NW 开发本部常务理事 Youngjin, Rho 以“云安全威胁和 CWPP 战略”为主题，从企业安全角度解释了云工作负载保护平台（CWPP）的重要性。Youngjin, Rho 说：“随着云计算市场在全球范围内的扩展，韩国的云计算市场正在围绕 IaaS（基础设施即服务）发展。”并指出：“尽管有关云基础架构的问题正在提出，但是很难找到合适的安全解决方案。”还强调：“为了保护企业云工作负载，就最小化威胁面和零信任（Zeor Trust）而言，应用程序控制和网络通信控制至关重要。”最后说明：“AhnLab 将提供专有的应用程序控制技术和 HIPS 产品，以有效地保护云工作负载。我们计划通过单一平台管理来管理云和现有的内部部署（on-premise）环境。”

AhnLab 安全架构团队负责人 Chulmin, Park 以“企业云环境安全框架”为主题，解释了云治理、云安全技术和云运营管理领域的安全要求和技术要求，并介绍了 AhnLab 的产品组合。Chulmin, Park 说：“随着当前已正式进入云时代，任何组织都应该将其业务基础架构转变为云。 目前，云和本地混合在一起，但是在不久的将来它将变为多云环境，因此要考虑现在和未来的安全响应计划。”接着说道：“AhnLab 已经将其安全托管服务框架转换为云。在云运营和管理方面，公司通过各种云控制服务和咨询服务来支持客户的稳定、安全的云转换。”

如果向云迁移是数字化转型的开始，那么第四次工业革命的核心就是运营技术（OT）。这就是为什么最近的很多安全专家都强调 OT 安全的原因。在这方面，AhnLab EP 技术支持团队课长 Byungju, Kim 通过“最新的安全威胁和改变 OT 环境的对策”主题发表，介绍了工业控制系统（ICS）遭受黑客入侵的案例，并提出了 OT 环境安全的准则。

Byungju, Kim 说：“直到最近，诸如 IT 和工业设施等一般的工作环境和 OT 仍被明确地区分，并且 OT 被认为是相对安全的，因为它存在于封闭的网络中。但是，随着 OT 和 IT 的融合，以及 OT 环境中网络连接的增加，对 OT 安全的认识和接近必须改变。”他指出：“OT 环境安全中最重要的技术因素是基于白名单的应用程序控制。随着最近使用通用应用程序的 OT 系统的增加，很难以通用方式将超过 10,000 个

进程列入白名单。” 接着补充说明：“AhnLab 通过专有技术提供基于白名单的自动化应用程序控制，还提供多种产品阵容来保护复杂的 OT 环境。”

5G 时代的网络安全和威胁响应的自动化

随着我们进入超连接时代，企业正在担心可靠的服务，安全人员则担心网络安全威胁。在这方面，AhnLab 网络业务规划团队部长 Jaehoon, Hwang 和课长 Junhyeok, Yim 介绍了最新的网络安全威胁和响应方案。

Jaehoon, Hwang 以“网络威胁响应中的 Plus Alpha”为主题，介绍了一种实用的网络安全管理策略。他说：“随着我们迁移到 5G 环境，网络带宽已比现有带宽增加了 20 倍。此外，由利用物联网设备漏洞的 bot 引起的网络威胁也在增加。” 并强调：“到目前为止，如果关注点集中在网络的垂直边界进行‘拦截’，那么该是时候从水平的角度关注‘响应’了。还需要入站和出站流量以及内部流量的监视和检测。”

▲ AhnLab网络业务规划团队的部长Jaehoon, Hwang和课长Junhyeok, Yim，服务业务规划团队次长Yong, Kwon

Jaehoon, Hwang 说：“AhnLab 的下一代网络入侵防御解决方案 AhnLab AIPS 是针对 5G 环境进行优化的网络安全解决方案。根据其独特的威胁检测规则，可以主动响应网络上的最新安全威胁。”

关于网络安全，Junhyeok, Yim 提供了有关 DDoS 攻击的最新信息以及稳定业务运营的对策。他说：“在韩国发生的 DDoS 攻击与其他国家略有不同。韩国几乎没有 100Gbps 攻击，使用物联网设备的 DDoS 攻击也很少。反而，由于 DDoS 攻击工具已为大众所用，因此 DDoS 攻击在韩国由于政治和社会问题而频繁发生，在有关比特币或网络游戏领域也经常发生。DDoS 攻击可以通过使公司网络瘫痪来发动二次攻击。AhnLab 为每个保护目标提供了多层过滤器和详细的响应方案，并具有将服务和内部部署链接在一起的混合响应机制。”

随着企业基础架构的多样化和安全威胁的日益复杂，越来越多的公司正在考虑威胁响应自动化。在这方面，AhnLab 服务业务规划团队次长 Yong, Kwon 介绍了“有效的 SOAR 引进计划”。Yong, Kwon 表示：“随着企业引进多个安全产品，发生了更多的安全事件，这使安全管理人员难以响应。通过自动化（Automation）和安全解决方案之间的链接（Orchestration）最大程度地减少安全人员的重复任务，并识别实际威胁后响应。” 他介绍了 SOAR（Security Orchestration, Automation, and Response: 安全

协调、自动化和响应）的定义，并解释了四个关键功能以及如何在 AhnLab Sefinity AIR 中实现该功能。他表示：“SOAR 必须能够通过分析客户环境来按需执行定制工作。AhnLab 基于通过多年积累的经验和技术，为各种客户环境提供优化的 SOAR。”

现场即问即答，实时响应客户的问题

此次 ASIF 2019 活动同时运营了 AhnLab 的产品展位和产品演示，以便客户可以看到最新的安全技术和 AhnLab 解决方案并实时响应客户提出的问题以解决他们对安全的疑问。

▲ 在展示中心正在演示AhnLab解决方案

AhnLab 的认可合作伙伴 SCK、Beats Korea、Demoa、Neosian、Dinotech、Soft2000、Inside Pro、FC Information、LNS Information Technology、U&I Soft、Yukon Tech、Econet System、2CL System、Taekwang Network Information、Timegate 和 Dell Technologies 参加了本次活动，并运营展位，回答了希望引进最新安全解决方案的客户的问题。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com