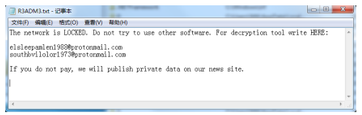
# 安天智甲有效防护 ILMWL 勒索软件


▲ILMWL 勒索信

近日，安天 CERT 在梳理网络安全事件时发现一个名为 ILMWL 的勒索软件。该勒索软件最早发现于 2020 年 9 月，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。该勒索软件运行后，将在短时间内完成对计算机文件的加密操作。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 ILMWL 勒索软件的加密行为。

ILMWL 勒索软件样本运行后，创建多个线程，实现在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.ILMWL”命名的后缀。在桌面文件夹和所有含有被加密文件的路径下创建名为“R3ADM3”的勒索信，加密完成后并不自动弹出勒索信息。该勒索信内容包含勒索说明和联系邮箱，并在其中强调若不支付赎金，将公开用户数据。

ILMWL 勒索软件采用“AES+RSA”加密算法，目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

## 木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、信标检测鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

| | |
|---|---|
| 文件名 | ILMWL.exe |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 240 KB |
| MD5 | DC71636C29E5D3901E3571C86B94 63AF |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan/Win32.Kryptik |
| 判定依据 | 反病毒引擎 |

◆ 操作系统

| 操作系统 | 内置软件 |
|---|---|
| Win7 x86 6.1.7600 Build 7600 | 默认、IE9、Google Chrome、Firefox、Office 2007、 Flash、WPS、FoxitReader、Adobe Reader |

◆危险行为

| 行为描述 | 危险等级 |
|---|---|
| 检测虚拟机 | ★★★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 加载运行时 DLL | ★ |
| 疑似桌面控制 | ★ |
| 壳行为填充导入表 | ★★ |
| 访问文件尾部 | ★ |
| 获取计算机名 | ★ |
| 检索系统内存信息 | ★ |
| 获取系统信息（处理器版本、处理器类型等） | ★ |
| 获取系统版本 | ★ |
| 获取驱动器类型 | ★ |
| 枚举窗口 | ★ |

◆扫描二维码查看完整报告



安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 9 月 21 日 ( 总第 248 期 ) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

# 苦象组织近期网络攻击活动及泄露武器分析

2012 年以来，安天针对印度方向的网络攻击进行了持续的跟踪与分析，追踪其攻击行动、溯源其幕后团伙，多年以来持续曝光相关攻击活动，震慑印方攻击组织。安天于 2016 年 7 月发布报告“白象的舞步——来自南亚次大陆的网络攻击”；2017 年 12 月发布报告“潜伏的象群—来自印方的系列网络攻击组织和行动”；2019 年 5 月发布报告“响尾蛇 (SideWinder) APT 组织针对南亚国家的定向攻击事件”；2020 年 1 月发布报告“折纸行动：针对南亚多国军政机构的网络攻击”。

本次报告涉及的攻击组织，安天在 2017 年“潜伏的象群”报告中曾披露过其苦酒行动，其他厂商也称为：BITTER、蔓灵花、APT-C-17、T-APT-04 等，根据安天的“攻击组织中文命名规范”，结合其网络攻击活动和地缘政治特点，安天正式将该组织命名为“苦象”。经过长时间的观测发现，该组织近期十分活跃，目前发现多批次涉及钓鱼网站和投递载荷两类攻击活动：

1. 攻击者注册多个域名，架设钓鱼网站，对国内重要的机构单位进行邮箱钓鱼攻击。相关钓鱼网站地址构造特点和攻击目标符合 2019 年曝光过的苦象组织对国内钓鱼攻击的特点。

2. 攻击者将载荷存放于攻陷网站，通过投递快捷方式格式的攻击诱饵向目标的机器植入载荷（组织特有的 .NET 远控木马）。通过此前对苦象组织泄露的控制后台源码和载荷分析，我们大致还原了该组织其中一常用木马的后台控制细节。经分析比对，我们认为该攻击活动来自苦象组织。

综上所述，安天 CERT 认为这一系列攻击应是苦象组织的近期攻击活动。本次系列相关攻击活动特征总结如下：

| 事件要点 | 内容 |
|---|---|
| 事件概述 | 苦象组织近期网络攻击活动 |
| 攻击目标 | 中国、巴基斯坦等 |
| 攻击手法 | 邮箱钓鱼、投递木马、利用攻陷网站 |
| 攻击意图 | 窃密 |
| 攻击时间 | 2020年中 |

**安天全线产品可以有效对抗上述威胁**

因篇幅限制，完整分析报告（公开版）请扫描下方二维码（左）获取。

2012 年以来，安天持续跟踪和分析来自印度方向的网络攻击，曝光相关攻击活动并对其进行追踪溯源，震慑印方攻击组织。扫描上方二维码（右）获取相关分析报告（公开版）合辑。

# 《金融科技时代》刊登安天创始人署名文章《金融行业要立足应对高级威胁构建综合防御体系》

金融安全是国家安全的重要组成部分，为保障金融安全，9 月出版的《金融科技时代》杂志刊登了全国政协委员、中国网络安全产业联盟理事长、安天集团创始人、董事长肖新光题为《金融行业构建综合防御体系应对高级威胁》的署名文章。文章对金融关键信息基础设施的安全状况进行了阐述，复盘了一起针对金融行业的 $A^2PT$ 攻击活动，建议金融机构了解高度复杂的攻击活动，提升金融行业的网络安全综合防御体系的和防御能力。

扫描下方二维码
获取文章完整内容

# 2020 国家网络安全宣传周——安天在产业创新发展论坛上分享专题报告

2020 年 9 月 15 日，由郑州市人民政府主办，中国网络安全产业联盟（CCIA）承办的“2020 年国家网络安全宣传周——网络安全产业创新发展主题论坛”成功举办。中央网信办网络安全协调局处长刘博出席论坛并致辞，中国网络安全产业联盟秘书长、中国电子技术标准化研究院副院长程多福发布《2020 年中国网络安全产业分析报告》。本次论坛由中国网络安全产业联盟副秘书长许玉娜主持。

刘博处长在致辞中强调，习近平总书记对网络安全工作的重要指示精神，为新形势下做好网络安全工作指明了前进方向，提供了根本遵循。特别是今年受疫情影响，网络的影响力日益壮大，但同时面对的问题也日趋复杂，网络安全企业要积极防范新技术新应用带来的新的网络安全风险，研究新课题、解决新风险，让网络安全产业为各行各业提供有力的保障。

本次论坛特别邀请了全国政协委员、CCIA 理事长、安天首席架构师肖新光做《以威胁框架为参照系的产品能力演进》专题报告。

本次论坛还举行了“2020 年优秀网络安全解决方案和网络安全创新产品评选活动”颁奖典礼，安天资产安全运维平台凭借自身优秀的设计理念、成熟的产品能力和技术创新能力，获颁“2020 年网络安全创新产品优秀奖”，相关负责人上台领奖。

扫描上方二维码获取
《以威胁框架为参照系的产品能力演进》
报告完整内容

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | Adobe 发布 Adobe Media Encoder 带外更新 |
| 英文标题 | Adobe releases out-of-band security update for Adobe Media Encoder |
| 作者及单位 | Lawrence Abrams |
| 内容概述 | Adobe 已发布 Adobe Media Encoder 的带外安全更新，该更新修复了三个“重要”安全漏洞。这三个漏洞被归类为“信息泄露”，这可能会使敏感信息在活跃用户的安全情况下被泄露。该更新修复了可能导致信息泄露的越界读取漏洞，这些漏洞的优先级为“3”，这意味着它们不是攻击者的目标，也没有使用它们的主动攻击。用户应安装 Adobe Media Encoder 14.4 来修复这三个漏洞。 |
| 链接地址 | https://www.bleepingcomputer.com/news/security/adobe-releases-out-of-band-security-update-for-adobe-media-encoder/ |

## 每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

| 恶意代码类别 | 名称 | 威胁等级 | 简要描述 |
|---|---|---|---|
| 活跃漏洞 | Microsoft Exchange server 安全漏洞（CVE-2020-16875） | 高 | Microsoft Exchange server 中存在远程代码执行漏洞，该漏洞源于 cmdlet 参数的验证不当，攻击者可利用该漏洞在系统用户上下文中运行任意代码。 |
| | Microsoft SharePoint 安全漏洞（CVE-2020-1452） | 高 | Microsoft SharePoint 中存在安全漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。攻击者可以利用该漏洞获得与当前用户相同的用户权限。 |
| | Microsoft Word 安全漏洞（CVE-2020-1218） | 高 | Microsoft Word 中存在资源管理漏洞。该漏洞源于软件无法正确处理内存中的对象。 |
| 较为活跃样本家族 | Trojan/Win32.Vobfus | 中 | 此威胁是一种木马类家族。该家族木马运行后会修改注册表，阻止用户显示隐藏文件夹，连接网络下载其它恶意程序。该家族木马通常通过网络及可移动设备进行传播。 |
| | Worm[Email]/Win32.Fearso | 中 | 此威胁是一种可以复制自身并传播的蠕虫家族。该蠕虫家族通过 Microsoft Outlook 发送大量的带毒邮件以及通过文件共享服务传播。该病毒程序文件的图标跟著名的压缩 / 解压缩软件 WinRAR 的图标一样，以此来诱导用户点击运行。 |
| | Trojan/Win32.Mansabo | 中 | 此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。 |
| | Trojan[Backdoor]/Win32.DarkKomet | 中 | 此威胁是一种后门类木马价值。该家族木马通常通过垃圾邮件附件、恶意链接及网上的免费应用下载等方式传播。该木马运行后会监控用户的行为，并为黑客打开系统后门，这会导致用户的信息被窃取并将窃取到的信息发送给黑客，同时该木马还可以下载其他恶意软件。 |
| | Trojan[Backdoor]/Linux.Mirai | 中 | 此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。 |
| | Trojan/Android.Hiddapp | 中 | 此威胁是安卓平台上一种具有隐藏功能的木马类家族。该家族样本运行后，会隐藏图标，使用不同的方法向用户显示尽可能多的广告，包括安装新的隐藏广告软件。通过利用超级用户权限，该家族样本可以隐藏在系统文件夹中，清除难度较大。 |
| | Trojan[Spy]/Android.SmForw | 中 | 此威胁是安卓平台上一种间谍类木马家族。该家族样本运行后，长久驻留系统，持续监控用户，收集用户系统信息，造成用户隐私泄露。 |



# 网络流量分析为安全团队带来四大优势

纳迪姆·扎希德 / 文 安天技术公益翻译组 / 译

网络流量分析和安全性

无论公司规模如何，都有可能遭受攻击。为了在这种新的混合网络环境中改善安全状况，企业开始将安全运营（SecOps）和网络运营（NetOps）团队结合起来。实际上，为了反映企业对网络分析解决方案（更注重安全性）的需求变化，Gartner 最近已将其细分市场“网络流量分析”更名为“网络检测和响应”（NDR）。总体而言，通过网络数据分析（尤其是网络流量分析），安全运营团队可以获得以下四个优势。

### 基于行为的威胁检测

在大多数反病毒和防火墙解决方案中，基于特征的威胁检测都是反应性的。发现恶意软件后，供应商会为其创建特征；或者从第三方来源（例如谷歌 VirusTotal）获得它们的信息，然后更新其产品以进行识别和防御。

虽说该方法能够快速筛选已知危险文件，防止其进入企业网络，但是有局限性。最明显的一点是：无法捕获未知威胁（因为其特征未知）。更重要的是，越来越多的恶意软件采用模糊技术来规避基于特征的检测。网络安全公司 WatchGuard Technologies 研究发现：在 2019 年的所有恶意软件中，有三分之一可以规避基于特征的检测；而到了 2019 年第四季度，这一数字飙升至三分之二。为了应对此类威胁，企业需要采用不同的检测方法。

网络流量分析（也称为 NDR）将高级分析、机器学习（ML）和基于规则的检测相结合，来识别整个网络中的可疑活动。NDR 工具分析原始流量，构建反映正常网络行为的模型，并在检测到异常模式时发出告警。

基于特征的解决方案旨在阻止恶意软件进入网络，而大多数 NDR 解决方案可以监控纵向流量，还能监控横向流量以及云本地流量。随着企业转向虚拟和云优先解决方案，这些功能越来越重要了。即使恶意软件能够规避基于特征的检测，通过 NDR 解决方案，安全运营团队也可以检测并阻止它们。要运行这些 NDR 解决方案，需要获取高质量的网络数据。

### 提供用于安全分析、合规性和取证的数据

安全运营团队通常需要网络和行为数据，来进行安全性分析或合规性审查。这通常需要来自网络（这些网络跨数据中心、分支机构和多重云环境部署）的物理、虚拟和云原生元素的元数据和数据包。

数据越容易访问、索引和理解（最好采用“单一面板”解决方案），就越有价值。要想获取此类信息，企业需要混合使用物理和虚拟网络探针以及数据包代理，以便从网络的各个角落收集和整合数据，进而处理数据并将其交付给安全工具堆栈。

通过 NDR 解决方案，安全运营团队可以捕获和保存与感染信标（IOC）相关的网络数据，以便在事件发生时进行快速的取证搜索和分析。这种捕获、保存、分类和关联元数据和数据包的能力，使安全运营团队能够在事件发生后进行调查，确定出了什么问题以及如何在将来更好地识别和预防攻击。

### 提供更好的网络可见性，实现更好的安全自动化

技能娴熟的安全专家很少，他们的时间非常宝贵。实现安全任务的自动化，有助于企业更快地解决事件，并为安全运营团队腾出时间，使其专注于更重要的任务。不幸的是，可见性和自动化取决于数据的质量和粒度——数据太少和太多都可能带来问题。

如果数据太少，自动化解决方案就缺乏依据。如果数据过多，威胁检测系统会发出过多告警，自动响应功能就会关闭相关账户或工作负载，这弊大于利。

数据缺失、太多告警或固有盲点意味着，NDR 所依赖的机器学习和分析模型将无法正常工作，这会产生大量误报，导致安全团队无暇应对实际威胁。从长远来看，这意味着 SOC 团队需要做更多的工作。

成功实现自动化的关键是：拥有高质量的网络数据，产生正确的安全告警。这样一来，企业可以实现响应的自动化。

### 减少恶意软件的驻留时间

NDR 解决方案通常不会以内联方式部署（这取决于 IT 团队），因此难以阻止威胁。即使如此，NDR 解决方案仍然可以通过快速识别可疑行为或流量，缩短事件响应窗口并减少恶意软件的驻留时间。NDR 工具生成的结果可以输入到下游安全工具中，帮助这些工具验证和修复威胁。

在整个安全行业中，恶意软件的驻留时间一直在减少。2019 年 Verizon《数据泄露调查报告》（DBIR）发现，56％的数据泄露需要几个月或更长时间才能检测到。但 2020 DBIR 发现，81％的数据泄露在几天或更短时间内就能被遏制。这一结果非常鼓舞人心。企业应继续让安全运营团队与网络运营团队合作，以进一步减少恶意软件驻留时间。

NDR（或网络流量分析）的优势远远超出了传统的网络运营。通过合作，网络运营和安全运营团队可以创建可靠的可见性体系结构和实践，以增强企业安全状况，在发生攻击时妥善应对。

具备了全面的网络可见性，安全团队就可以通过安全交付层查看所有相关信息，使用基于行为的或自动化的威胁检测方法，捕获和存储相关数据以进行深入的取证调查和事件响应。

| 原文名称 | Four ways network traffic analysis benefits security teams |
|---|---|
| 作者简介 | 纳迪姆 · 扎希德（Nadeem Zahid）。纳迪姆 · 扎希德是 cPacket Networks 产品管理和营销副总裁。 |
| 原文信息 | 2020 年 9 月 11 日发布于 Help Net Security<br>原文地址 https://www.helpnetsecurity.com/2020/09/11/four-ways-network-traffic-analysis-benefits-security-teams/ |
| 免责声明 | 本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。<br>本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 |