# 安天发布《Nemty 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Nemty 的勒索软件。Nemty 勒索软件最早在 2019 年 8 月被发现，其传播方式主要为 RDP 暴力破解。与目前最普遍的钓鱼邮件传播相比，RDP 连接对攻击者来说更加方便，他们不需要等待受害者“主动上钩”，就能进行后续操作。

勒索软件 Nemty 执行后，首先会加密计算机上的文件，创建加密文件的加密副本，并追加名为“.nemty”的后缀。创建两封相同的名为“NEMTY-DECRYPT.txt”的勒索信，勒索信中包含下载并安装 TOR 浏览器、联系网站地址和勒索说明等。调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。勒索软件 Nemty 会避开以下国家和地区进行文件加密：俄罗斯、白俄罗斯、哈萨克斯坦、塔吉克斯坦共和国和乌克兰。目前被加密的文件在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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

## 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、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆概要信息

| | |
|---|---|
| 文件名 | 267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 183 KB |
| MD5 | 0E0B7B238A06A2A37A4DE06A5AB5E615 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan/Win32.Generic |
| 判定依据 | BD 静态分析 |

完整报告地址：https://1.119.163.6/vue/details?hash=0E0B7B238A06A2A37A4DE06A5AB5E615

◆运行环境

| 操作系统 | 内置软件 |
|---|---|
| WinXP 5.1.2600 Service Pack 3 Build 2600 | 默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader |

◆险危行为

| 行为描述 | 危险等级 |
|---|---|
| 访问下载站点 | ★★★ |
| 堆喷射 | ★★★★★ |
| 释放后缀为图片的 PE 文件 | ★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 加载运行时 DLL | ★ |
| 壳行为填充导入表 | ★★ |
| 获取驱动器类型 | ★ |
| 获取计算机名 | ★ |
| 独占模式打开，防止复制读取，防止杀毒软件扫描上报 | ★ |
| 文档篡改 | ★★ |
| 释放 PE 文件 | ★ |
| 设置自启动项 | ★★ |

◆UDP 信息

| 源 IP | 源端口 | 目的 IP | 目的端口 |
|---|---|---|---|
| 192.168.122.111 | 1032 | 192.168.122.1 | 53 |
| 192.168.122.1 | 53 | 192.168.122.111 | 1032 |
| 0.0.0.0 | 68 | 255.255.255.255 | 67 |
| 192.168.122.1 | 67 | 192.168.122.111 | 68 |
| ..... | ..... | ..... | ..... |



安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 09 月 02 日 ( 总第 198 期 ) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

# “优势互补、资源共享、共同发展”2019 哈尔滨工程大学实训精彩回顾

为进一步提升网络空间安全人才培养质量，为东北老工业基地改造提供人力支持和智力保障，为国家、行业和自身培养输送合格网络安全人才，安天集团与哈尔滨工程大学本着“优势互补、资源共享、共同发展”原则共同建设教学实践基地，在培养网络空间安全实用型人才领域展开深度校企合作。

8 月 23 日，为期 1 个月的哈尔滨工程大学信息安全专业实训活动圆满结束，安天集团副总工 设计课程并授课、CERT 高级网络安全分析工程师指导答疑、人力资源中心实施教务管理，引领 50 名来自哈尔滨工程大学的同学征战网络安全的星辰大海。

实训第一天同学们在安天的合影

### 场景教学实战实训

本次实训针对学生所学专业，围绕逆向工程实践、企业与行业认知、网络安全威胁基础、职业生涯规划等方面展开课程。安天网络安全工程师基于多年一线实战经验，结合大量鲜活的真实案例，兼顾学生网络安全知识掌握程度，在培养兴趣、扩展视野、网络安全研究、应急响应等方面与参训同学进行了互动交流。课程实践环节，模拟安天的实际安全研究与应急处理工作，将学生分成 3-4 人的项目小组，每组以承接项目任务，并按照事先规定的项目周期和计划进行。在此过程中，按照项目管理规定要求对项目小组和每个项目组成员进行考核，让学生在学习技术的同时，


实训现场

真实感受企业的管理要求和项目压力。

### 学有所得学有所获

学习的目的全在于运用。“初来乍到，面对汇编语言和新工具的使用有些手足无措，入门比较困难，在老师的精心指导与耐心解答下，我们学习到了丰富的知识和技巧。”；“这次实训我了解了众多恶意代码，并认识到：无论恶意代码的设计手段多么高深，总有人会站出来与之对抗，维护网络安全，哪怕这份工作很难被大众认知和理解，这场与恶意代码对抗的斗争也不会停止。”；“我们学习了 10 余种工具，选择对的工具才能有效和恶意代码对抗，在这个过程中我们掌握了逆向基本功，接触到了信息安全的一线工作，获得了解决问题的能力，提高了团队合作能力和自

摘自学生实训汇报内容

我表达能力。”参训的同学们深有感触的说。

本次实训安天直面国家网信事业发展需要和自身成长需求，强调以爱国主义和安全工作者的职业操守为前提，以安全架构、安全开发、安全分析、安全运维工程师的培养为重点。

网络安全教育不仅仅是经验、技能教育，更要包括原则立场、科学方法和实证精神。当前网络安全是持续复杂艰巨的工作，残酷严峻的现实挑战面前，理论与实践之间会有巨大的差距，需要系统的学习、冷静的思考和扎实的行动。

安天作为引领威胁检测与防御能力发展的网络安全国家队，拥有一支经历十几年积淀，对安全事业忠诚，技术优秀的核心技术骨干队伍，是业内技术最全面、凝聚力最强、安全价值观最正的公司之一。依托自主先进核心技术与安全理念，致力为战略客户和关键基础设施提供整体安全解决方案。安天产品和服务为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等基础能力。安天为客户建设实战化的态势感知体系，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，赋能客户筑起可对抗高级威胁的网络安全防线。

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | TA505 针对多国投放 ServHelper 和 FlawedAmmyy |
| 英文标题 | TA505 At It Again: Variety is the Spice of ServHelper and FlawedAmmyy |
| 作者及单位 | Trend Micro |
| 内容概述 | 趋势科技研究人员观察到 TA505 在 7 月中旬的新攻击活动。该活动针对新增目标国家包括土耳其、塞尔维亚、罗马尼亚、韩国、加拿大、捷克共和国和匈牙利，使用 .ISO 镜像文件附件作为攻击入口点，以及 .NET 下载程序、新形式的宏交付，最终投放 ServHelper 变种和 .DLL FlawedAmmyy 下载器变种。针对土耳其和塞尔维亚银行的活动示例中，邮件附件的 .ISO 镜像为 .LNK 文件，使用命令行 msiexec 从 URL 执行 MSI 文件，然后 pm2 文件包含并运行使用 NSIS 创建的安装程序文件，安装其包含的 ServHelper。其它示例中还使用 Excel 附件包含的恶意宏，从 URL 下载 NSIS 创建文件，最终安装 ServHelper，与 C2 通信采用 XOR 加密。针对韩国企业的攻击中，在以上流程基础上使用 .NET 下载程序最终安装 FlawedAmmyy。而在 8 月第一周观察到的针对加拿大的攻击中，用户启用文档恶意宏后，将使用 IE 通信下载文本文件，宏处理文件中使用 XOR 加密和打包 .DLL FlawedAmmyy 下载器，写入磁盘，最终安装 FlawedAmmyy RAT。 |
| 链接地址 | https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/ |

## 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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

| 恶意代码类别 | | 名称与发现时间 | 威胁等级 | 简要描述 |
|---|---|---|---|---|
| 移动恶意代码 | 新出现的样本家族 | Trojan/Android.FakeFB.ad[prv,exp] 2018-08-25 | 高 | 该应用程序伪装成 Facebook，诱导用户输入账号密码，通过 firebase 联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗，建议卸载。 |
| | | Trojan/Android.SmsSpy.cb[prv,exp] 2018-08-26 | 中 | 该应用程序伪装短信相关应用，运行运行获取用户短信并私自转发至指定号码，造成用户隐私泄露和资费消耗，建议卸载。 |
| | | Trojan/Android.dialer.d[exp] 2018-08-27 | 低 | 该应用程序运行拨打指定电话，诱导用户点击色情图片，点击则发送短信，同时后台访问未知网址，造成用户资费消耗，存在未知风险，建议用户立即卸载，使用健康绿色应用。 |
| | 较为活跃样本 | G-Ware/Android.Downloader.gg[exp,rog] | 中 | 该应用程序运行后伪装成其他软件，启动要求激活设备管理器，并自动隐藏图标，之后联网获取指令私自下载安装，造成用户资费消耗，建议卸载。 |
| | | Trojan/Android.Rootnik.k[rog,sys,rtt] | 中 | 该应用程序伪装系统应用，安装无图标，下载提权文件利用漏洞提权，然后私自下载未知文件静默安装，会造成用户资费损耗，请卸载。 |
| | | RiskWare/Android.ltbocai.b[rog] | 中 | 该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载 |
| | | Trojan/Android.YunchenrjSpy.a[prv,fra] | 中 | 该应用程序伪装破解工具、外挂等应用，本身无实际功能，运行私自拍照并上传到指定网址，会造成用户隐私泄露，建议立即卸载。 |
| | | G-Ware/Android.HiddenApp.cm[exp,rog] | 低 | 该应用程序伪装为知名应用，运行隐藏图标，后台加载广告，造成用户的资费消耗，建议卸载。 |
| PC 平台恶意代码 | 活跃的格式文档漏洞、0day 漏洞 | LNK 远程代码执行漏洞（CVE-2019-1188） | 高 | 当 Windows 处理 .LNK 文件时，可能会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。攻击者可能会向用户显示包含恶意 .LNK 文件的驱动器或远程共享，当用户在 Windows 资源管理器中打开此驱动器或远程共享时，恶意二进制文件会在目标系统上执行攻击者编写的代码。 |
| | 较为活跃样本 | Trojan[Monitor]/Win32.SpectorPro | 中 | 此威胁是一种可以监视系统状态的木马家族。该家族样本运行后收集操作系统信息，连接远程服务器并回传。 |
| | | Trojan/JS.Tadtruss | 中 | 此威胁是一种可以下载恶意代码的木马家族。该家族样本一般是 JS 脚本，运行后连接远程服务器下载恶意代码并执行。 |
| | | GrayWare[AdWare]/Win32.ExtCrome | 低 | 此威胁是一种可以弹出广告的灰色软件家族。该家族样本运行后安装广告件，在用户浏览网页时弹出广告，占用系统资源，影响用户使用。 |
| | | GrayWare[AdWare]/Win32.Webalt | 低 | 此威胁是一种可以下载并安装推广应用的灰色软件家族。该家族样本运行后连接网络下载推广应用并安装，可以弹出广告，占用系统资源，影响用户使用。 |
| | | GrayWare[AdWare]/Win32.Lola | 低 | 此威胁是一种可以弹出广告的灰色软件家族。该家族样本运行后安装广告件，在用户浏览网页时弹出广告，占用系统资源，影响用户使用。 |



# 如何利用 SIEM 来增强企业威胁检测能力

Diana Kightlinger/ 文 安天技术公益翻译组 / 译

“安全信息和事件管理”（SIEM）解决方案已经存在了十多年，至今它仍在不断发展。当前仍有很多企业不知道如何有效利用 SIEM，以及 SIEM 是如何捕获和利用数据的（包括结构化和非结构化数据，内部和外部数据），或如何有效实施 SIEM 解决方案。

然而，威胁并没有停滞不前，不管是攻击类型和还是攻击数量都在不断变化；对这些企业来说，这很不幸。目前，企业不仅面临安全人才短缺的问题，而且解决单一问题的防御方案还遍布各个不同的企业。防御者需要采用 SIEM 解决方案检测企业整体环境中的威胁，采用人工智能（AI）技术识别可疑活动背后的关联，以及采用自动化流程快速阻断攻击。

### SIEM 究竟是什么？

首先，我们要了解 SIEM 是什么。SIEM 是“安全信息管理”（SIM）和“安全事件管理”（SEM）的结合，通过对本地和云活动的细粒度和实时可见性，帮助企业检测威胁。

曾经，审计和合规需求——从“支付卡行业数据安全标准”（PCI DSS）到《萨班斯法案》（SOX），再到《健康保险流通与责任法案》（HIPAA），推动了 SIEM 市场的发展。但是，随着威胁形势不断变化，网络攻击者的复杂性不断增加，我们需要重新思考“SIEM 究竟是什么”这一问题。从合规性角度来看，SIEM 扩展到威胁检测领域，且仍然是安全运营中心（SOC）的核心任务。

### 集中展示全网安全状况

复杂的 SIEM 系统能够为 SOC 赋能，帮助 SOC 检测已知和未知威胁、快速有效地响应事件。但是，随着企业采用新型技术，如物联网（IoT），攻击面不断增长，形成了新的安全盲点。

为了检测和调查威胁，企业需要全面了解本地和云（包括混合云和多重云）资产，以及网络和用户行为，以帮助分析师发现可能表示数据泄露或网络攻击的异常情况。通过这些措施，企业向合规和监管审计师证明其 SIEM 系统的有效性和准确性。

鉴于企业缺乏网络安全技能，他们需要更易于部署、管理和维护的 SIEM 解决方案。面对不断增加的数据源，企业需要付出很大的精力，才能对其进行整合和调整。如果企业想部署解决方案来改进检测、调查和决策，则需要供应商持续分享专业知识。这样一来，企业的安全团队就不用“硬着头皮”干活了。

### AI 加速调查

SIEM 解决方案可以用于很多安全用例，如检测端点威胁、内部威胁，以及网络钓鱼攻击。但是，防御者需要识别威胁以及威胁行为的症状。随着这种需求不断增长，机器学习和高级历史分析等技术开始发展。这些技术可以识别异常行为，帮助防御者更早地做出反应，以便阻止攻击者并减轻损失。

只产生大量安全告警，而不能将这些告警与一些安全工具集成，这种安全解决方案不是分析师们想要得到的。他们可以采用 AI 赋能的分析技术，调查和寻找导致现有异常的根本原因和产生这些异常的事件链条。

在检测潜在的威胁方面，AI 不会取代基于规则的算法或机器学习算法，也不会取代人类。但是，如果 SOC 缺乏调查这些威胁的人才，可以采用 AI 技术加快分析和洞察速度，以便在攻击者做出动作之前识别威胁。借助一些片段数据和威胁知识，AI 的认知能力能自动做出决策，并持续改进。

此外，AI 可以帮助分析师实施、配置和支持用例。对企业来说，跟上威胁变化并缩小差距至关重要，而 AI 可以评估威胁的优先级并实现大部分工作的自动化。

### 自动化实现增值活动

大多数网络攻击都针对关键的企业数据——一旦攻击者获得访问权限，企业就需要快速有效的事件响应流程，为分析师赋能以便阻止这些攻击造成的破坏。但是，SIEM 侧重威胁检测，其工具通常每秒处理 10,000 到 500,000 个事件。SIEM 应向事件响应系统提供处理威胁所需的数据和证据。

企业需要认识到，SIEM 并非事件响应工具。在事件响应方面，“安全编排、自动化和响应”（SOAR）解决方案更有优势。SOAR 通过自动执行不需要人工干预的枯燥和重复性任务，帮助安全团队提高生产力，使安全团队可以专注于人员、流程和技术。顶级解决方案根据客户数据、业务功能及声誉面临的风险，为威胁添加情境并确定其优先级。

为 SIEM 增加自动化功能和情报，能够为安全团队赋能，使他们专注于增值活动，例如主动威胁猎杀和威胁防御。网络攻击者在基础设施中驻留的时间越短，他们造成的伤害就越小，因此这一点至关重要。分析师可以通过洞察力和判断力识别策略变化，限制应用程序或数据库的风险使用，阻断恶意攻击者，而且不会中断客户对企业的访问。

总地来说，恰当的 SIEM 解决方案可以帮助企业全面了解各种数据和威胁，使企业不局限于单个告警，从而帮助企业识别潜在事件并确定其优先级，并通过 AI 技术加速调查流程——有助于企业采取更加积极主动的安全策略。

| 原文名称 | What Is SIEM and How Does It Enhance Threat Detection? |
|---|---|
| 作者简介 | Diana Kightlinger。Diana Kightlinger 是一位经验丰富的记者、撰稿人和博主，擅长科学、技术和医疗领域。 |
| 原文信息 | 2019 年 8 月 26 日发布于 Security Intelligence。<br>原文地址 https://securityintelligence.com/articles/what-is-siem-and-how-does-it-enhance-threat-detection/ |
| 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。 |