# 安天智甲有效防护 VoidCrypt 勒索软件新变种

勒索软件名：VoidCrypt 勒索软件新变种
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.[honorsafe@keemail.me][ 随机字符串 ].honor
支付与金额：需通过邮箱与勒索者联系
免费解密工具：暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个 VoidCrypt 勒索软件新变种。该勒索软件隶属于 VoidCrypt 勒索软件家族，最早于 2020 年 10 月被发现，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。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 VoidCrypt 勒索软件新变种的加密行为。

该勒索软件样本运行后，创建多个线程，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“.[honorsafe@keemail.me][ 随机字符串 ].honor”命名的后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“!INFO.HTA”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱。为了诱导受害者尽快缴纳赎金，勒索信中强调了在加密的 48 小时后仍未付款，赎金金额将会提高一倍。

▲勒索信

该勒索软件采用“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，下为其自动生成的分析报告：

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、关联分析鉴定器、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、关联分析鉴定器、信标检测鉴定器、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 | honor.exe |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 1.28 MB |
| MD5 | 0A6C572697280DDFBEC98811D512E3C1 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan[Ransom]/Win32.Odveta.gen |
| 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 |
|---|---|
| 在启动时禁用 Windows 错误恢复 | ★★★★ |
| 查询系统硬盘大小 | ★★★ |
| 文件篡改 | ★★★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 加载运行时 DLL | ★ |
| 创建挂起进程 | ★★ |
| 获取驱动器类型 | ★ |
| 获取系统版本 | ★ |
| 获取计算机名 | ★ |
| 检索系统内存信息 | ★ |
| 枚举进程 | ★ |
| 连接网络 | ★ |
| 获取指定套接字的一个本地 ip 地址 | ★ |
| ..... | ..... |

◆扫描二维码查看完整报告



安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2020年11月30日(总第256期)试行 本期4版 扫描上方二维码查询安天所有对外开放资料

# 安天与海康威视建立深度战略合作伙伴关系

近期，安天与海康威视在杭州签署战略合作协议，安天创始人、董事长肖新光，安天执行董事长、CEO 游小明，海康威视董事长陈宗年、高级副总裁蒋玉峰等双方高管共同出席并见证签约仪式。

安天与海康威视将发挥各自在市场、技术、产品、服务等方面的优势，通过战略合作在物联网恶意代码检测、产品轻融合、技术深度融合、平台与服务项目、产业链融合等方面展开深度合作，共同创建、营销、交付端到端的解决方案，为客户带来更加安全完善的、符合监管要求和用户信任的应用体系。

此次战略合作协议的签订，是双方战略合作伙伴关系的新起点。未来，安天将进一步与海康威视建立高层领导定期沟通机制、工作部门联络机制以及信息共享机制，把握新机遇、迎接新挑战，及时研究解决双方合作中出现的新问题、新情况，推动战略合作实质性落地，形成连接共生的发展模式，共同提高双方竞争力，通过共创、共享、共担构筑决胜未来的新格局，进而实现互利共赢，共同构建以视频为核心的安全智能物联网生态体系，提升安全综合实力。

# 安天与联软科技签署战略合作协议


11 月 24 日，安天与联软科技在京签署战略合作协议，双方将充分发挥各自在端点防护、网络准入控制等安全领域积累的技术和产品优势，以模块级合作模式，全面集成与联动，实现产品能力互补，提升竞争优势，把握端点安全产品一体化融合的趋势，创造有效安全价值。安天董事长肖新光，联软 CEO 祝青柳等双方团队成员出席签约仪式。

肖新光表示：端点系统是客户业务运行和数据资产的载体，是威胁对抗的主战场，也是最后一道防线。双方在端点安全领域积累了各自的产品和技术优势。安天在威胁对抗能力方面有 20 年积累，在恶意代码查杀、主防驱动、分布式防火墙等方面，有明显的能力优势。联软是安全准入、桌面管理、DLP 等方面的细分冠军，产品成熟，客户美誉度高。未来，安天可以在产品化和产品运营能力方面全面学习联软的经验；同时在恶意代码检测、威胁对抗和威胁情报方面，对联软全面开放赋能。希望安天和联软的战略合作将融合双方的积累和优势，打造最强的终端产品体系，创造业内能力协同和行业生态合作的典范。

祝青柳表示：联软自身在准入控制和端点领域有着十多年的技术与实践积累，并始终坚持自主研发，构建开放合作生态；安天在为客户构建端点防护、流量监测、威胁分析、导流捕获等纵深安全能力有着丰富的技术和行业实践经验，强大的技术和市场优势有目共睹。面对如今行业中攻防不平衡、安全与效率难以兼顾等挑战，传统网络安全方式显然需要更迭，联软和安天的战略合作将在产品及端点技术的融合、恶意代码检测、威胁情报等多方面展开，双方将致力于打造最具竞争力的准入 + 终端响应防护产品体系，让企业的网络具有安全容错、对抗能力，将安全与业务融合，助力企业级用户搭建具有全方位防护能力的网络安全体系，构筑可对抗高级、复杂化、组织化网络威胁的安全防线。相信双方可以形成合作的乘法效应，增强彼此在各自优势市场的能力，拓展产品品类和价值内涵。

## 研究人员发现廉价视频门铃存在多个安全漏洞

一项对11个相对便宜的视频门铃的分析发现，所有这些门铃都存在高风险漏洞。研究人员希望在这个假期需要购买视频门铃的消费者最好还是选择信誉良好且值得信赖的品牌。研究人员最近通过对在线市场（如亚马逊和eBay）出售的近十种廉价视频门铃的审查发现，每台设备都存在多个安全漏洞。其中最严重的是一些设备在没有明显原因的情况下将Wi-Fi名称、密码、位置信息、照片、视频、电子邮件和其他数据发送回制造商。

（原文链接：https://www.darkreading.com/iot/security-researchers-sound-alarm-on-smart-doorbells/d/d-id/1339523）

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 澳大利亚法律服务提供商遭受勒索软件攻击 |
| 英文标题 | Law In Order hit by ransomware attack |
| 作者及单位 | Ry Crozier |
| 内容概述 | 澳大利亚为律师事务所提供文件和数字服务的供应商 Law In Order 上周末遭遇勒索病毒感染，据分析是网络流氓软件 Netwalker。Law In Order 表示，在检测到这次攻击后，它停止了许多业务运营，并召集网络安全顾问协助调查和事件响应。该公司在周二晚间设法恢复了正常业务运营。 |
| 链接地址 | https://www.itnews.com.au/news/law-in-order-hit-by-ransomware-attack-558197 |

## 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 | Windows Hyper-V 验证绕过漏洞（CVE-2020-17040） | 高 | 未授权的远程攻击通过向 Hyper-V 服务器发送特制的请求包来进行漏洞利用，利用成功后便可绕过 Hyper-V 现有的部分安全特性。 |
| | Microsoft 浏览器安全漏洞（CVE-2020-0878） | 高 | Microsoft 浏览器存在安全漏洞，该漏洞允许攻击者以执行任意代码的方式损坏内存，并可以获得与当前用户相同的用户权限。 |
| | Microsoft COM 安全漏洞（CVE-2020-0922） | 高 | Microsoft COM 存在远程代码执行漏洞，该漏洞源于外部输入数据构造代码段的过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞生成非法的代码段，修改网络系统或组件的预期的执行控制流。 |
| 较为活跃样本家族 | Trojan[Backdoor]/Win32.Padodor | 中 | 此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。 |
| | Trojan[Proxy]/Win32.Qukart | 中 | 此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。 |
| | Trojan/Win32.Yakes | 中 | 此威胁是一种木马类程序。该家族可以通过白名单机制绕过系统防火墙，获取系统的最高权限。该家族具有下载恶意程序、监控用户操作等行为。该家族木马会在执行完成后将自身删除。 |
| | Trojan/Win32.Fsysna | 中 | 此威胁是一种木马家族。该家族样本运行后会在电脑的临时文件夹下释放恶意代码，同时添加注册表启动项，并发送网络请求。 |
| | Trojan/Win32.Zenpak | 中 | 此威胁是一种下载恶意代码类木马家族。该家族木马运行后，连接恶意域名，下载并执行相关恶意代码（窃密、挖矿、勒索等），同时会收集系统基本信息回传 C2 服务器。 |
| | 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[Dropper]/Android.Wroba | 中 | 此威胁是安卓平台上的一种恶意代码释放类木马家族。该家族木马运行后激活设备管理器、隐藏图标。接收短信指令，根据指令拦截指定短信，伪造新版本通知释放恶意 apk 同时卸载正常程序，上传手机用户隐私信息至远程服务器地址。 |



# XDR：统一事件检测、响应和补救

奈尔什·德兰吉 / 文 安天技术公益翻译组 / 译

根据 IBM《2020 年数据泄露成本报告》，在 2019 年，企业识别和遏制数据泄露所需的平均时间为 279 天；2018 年为 266 天，而过去五年的平均时间为 280 天。换句话说，企业识别和遏制数据泄露的情况并没有得到改善。首席信息安全官（CISO）们需要迅速采取行动。

### 在检测和补救数据泄露方面，企业面临什么障碍?

我们分析一下安全运营中心（SOC）面临的主要障碍。首先，生成的告警太多，这使得 SOC 难以优先处理那些需要立刻关注和调查的事件。

此外，大多数大型企业对其工具层生成的安全信息，没有进行统一管理。最后，企业使用混合本地和云架构以及纯云环境这一事实，使上述问题更加复杂。

SOC 面临的另一个重要障碍是：威胁猎杀和调查主要依靠人工。SOC 使用的数据源是分散的，必须从不同的控制台进行访问，这使问题更加复杂。

“身份”是威胁猎杀的重要组成部分，而 SOC 缺乏对该部分的可见性。疫情期间，很多员工开始远程办公，“身份”就更加重要了。

当前安全架构中的分析、控制和响应面板未集成。也就是说，分析与管理和线索栈是分离的，而管理和线索栈与拦截攻击者、阻止攻击的工具也是分离的。

### “扩展检测和响应”（XDR）简介

现在，出现了一种被称为 XDR 的新架构。研究公司 Gartner 将 XDR 列为 2020 年九大安全和风险趋势之一。XDR 颠覆了当前的安全模型，用自下而上的方法替代传统的自上而下的方法，能够提供更精确和更保真的结果。

XDR 的主要推动力是将分析与检测和响应相融合。它默认这些功能不应分离。通过将它们整合在一起，XDR 能够带来诸多优势。

首先是对威胁的精确响应。借助 XDR，日志能够实现更高的保真度和更深入的细节，企业可以立刻利用这些日志进行事件响应，而不必将其保存在单独的数据库中。例如，传统的 SIEM 方法基于监控网络日志数据（以识别威胁）并做出响应。

企业通常在手动调查之后再采取补救措施，除非威胁很简单（例如可以轻松清除的商品恶意软件）。而 XDR 能够为 SOC 提供可见性，以及响应和补救能力。SOC 人员不仅可以跨网络，而且可以在端点和其他区域采取精确而非“广撒网的”行动。

XDR 试图融合分析、控制和响应面板，能够提供统一威胁视图。通过将事件数据和分析相结合，XDR 能够提供精确响应所需的完整情境信息。SOC 无需再使用多个接口来进行威胁猎杀和调查。

XDR 不同于 SIEM 模型。SIEM 模型首先将日志集中起来，提供给 SOC 找出重要内容；而 XDR 则是先找出重要内容，然后再提供给 SOC，帮助其进行响应和补救。这是 XDR 颠覆传统 SIEM 和 SOC 工作流的基础。

XDR 的另一个重要优势是，它使 SOC 能够从同一安全技术平台调查和响应事件。例如，端点生成告警或分析信标，SOC 启动调查流程，使用网络日志或其他系统日志（XDR 平台的一部分）来获取更深入的情境信息。

所有数据源都放在一个位置，而非在不同控制台之间移动。通过 XDR，SOC 人员能够在启动工作流的同一技术平台上解析和关闭工作流。

当前，大多数企业都具备可以启动工作流的工具，部分企业具备扩展工作流的工具，但是只有很少的企业具备解析工作流的工具。XDR 的目标是提供一个可以启动、调查和补救事件的单一环境。

最后，通过融合分析、网络和端点，SOC 可以响应各种控制面板上的事件，并基于事件、系统关键性和攻击活动等自定义操作。

### XDR 使什么成为可能

借助 XDR，SOC 可以与 IAM 工具集成，以强制用户重新登录或注销。如果主机直接连接到端点，SOC 可对其进行遏制。通过网络分析和深入可见性，XDR 可以提供对威胁的更深入了解和情境信息，包括威胁是否横向移动、是否泄露了数据等。

此外，XDR 使 SOC 能够以过去无法实现的方式对事件做出响应，例如采取更多网络补救措施。

要想使 XDR 成为现实，企业需要一个将所有现有安全孤岛连接起来的面板，以实现统一分析、控制和响应。这不会在一夜之间发生；但是，值得企业付出努力。

| 原文名称 | XDR - Unifying incident detection, response and remediation |
|---|---|
| 作者简介 | 奈尔什 · 德兰吉（Nilesh Dherange）。奈尔什 · 德兰吉是 Gurucul 的首席技术官。 |
| 原文信息 | 2020 年 11 月 24 日发布于 Help Net Security<br>原文地址 https://www.helpnetsecurity.com/2020/11/24/xdr-extended-detection-and-response/ |
| 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。 |