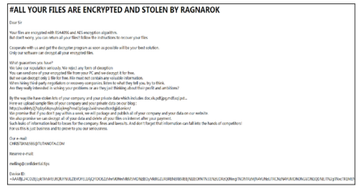
安天智甲有效防护 Hela 勒索软件新变种

近日，安天CERT在梳理网络安全事件时发现了一个名为Hela的勒索软件新变种。该勒索软件隶属于Ragnarok勒索软件家族，最早于2021年7月被发现，主要通过垃圾邮件进行传播。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勒索软件的加密行为。

Hela勒索软件运行后，结束包括Word、Excel、PowerPoint在内的多个进程，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“.五位随机字符串.hela”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“!!Read_Me.五位随机字符串.html”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱等。Hela勒索软件调用命令行命令防止受害者恢复已加密的文件，具体操作为删除卷影副本、删除本地计算机的备份目录等。

Hela勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂时无法解密。



▲Hela勒索软件勒索信息

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(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、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(WinXP)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、动态行为鉴定器将文件判定为木马程序。

◆概要信息

文件名	e7fe3b83e1730593d372b5a848e84066c07d75ee4790395a258822cfb8502412
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	169 KB
MD5	65C3956288E16BDCC55E3C9C6B94BA5B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=65C3956288E16BDCC55E3C9C6B94BA5B

◆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、Office2003、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
通过标记进程可执行堆绕过DEP	★★★★★
创建互斥量	★★★
搜索文件	★★★★
修改文件后缀名	★★★★
疑似勒索软件篡改或加密文件	★★★★★
删除卷影副本	★★★★
通过文件检测布谷鸟沙箱	★★★★★
映射内存方式注入	★★★

◆常见行为

行为描述	危险等级
创建挂起进程	★★
.....	.....

◆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 2021年08月09日(总第290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

安天移动安全上线“App用户权益保障合规检测”服务（限免）

近年来，随着大数据在云计算、物联网、人工智能等新服务领域广泛应用，大数据的商业价值被逐渐挖掘出来，用户个人信息成为一项重要资源。在商业利益的驱动下，个人信息被不当收集、恶意篡改、非法使用的事件屡见报端，甚至催生出包含公民隐私在内的各类个人信息的肆意采集和地下交易的灰色产业，隐私保护和个人信息安全等问题日益突出，全面加强个人信息保护已经迫在眉睫。

安天移动安全上线“App用户权益保障合规检测”服务

为了保障用户权益和个人信息安全，同时帮助广大开发者更好地理解用户权益保障规范，在开发过程中实现自助合规整改，力求快速达到合规要求，安天移动安全凭借丰富的移动应用威胁治理经验、成熟的沙箱化安全检测自研技术以及运营能力，正式上线并推出“App用户权益保障合规检测”服务。

App用户权益保障合规检测项中，不仅涵盖常见的违规收集用户个人信息行为，还包括当前政策文件重点关注的多项App违规行为，其中，超过半数以上的检测项得到主管部门认可与应用。安天移动安全风险检测预警平台在开放开发者信誉查询服务且广受好评之后，再次免费开放隐私检测服务，其他服务后续将陆续开放。

PC端输入下方链接，注册登录免费试用：https://dev.avlsec.com/login

产品介绍

基于安天移动安全多年来对恶意、风险软件，以及应用不规范行为的识别、分析、评估和判定的技术积累，App用户权益保障合规检测融合了自然语言处理和机器学习等技术手段，通过对隐私政策和应用行为的识别来判断App是否有侵害用户权益的行为。

检测服务系统总体采用SaaS服务形态，通过云端接口投放并回调检测结果。整体服务包含隐私政策判定和语义分析服务、静态检测服务、动态沙箱检测服务等多个业务模块，通过集群化部署和管理对投放任务进行高效的检测。

产品优势

成熟的沙箱检测技术

早在2015年，安天移动安全就开始自研沙箱检测技术，在真机部署仿真沙箱运行模拟环境拥有成熟的技术架构和研发体系，对于真机集群的系统适配、桩点预埋、任务调度等方面拥有丰富的积累，重点体现在：

1. 集群化的系统适配、部署和调试
2. 基于AOSP适配了不同Android系统的版本，能快速部署上线
3. 成熟的工程化业务流转流程，采用独立的功能模块，可支持产品敏捷迭代

在真机沙箱环境中，通过预置污点数据，并从系统设置、预装应用、网络环境等多个维度模拟用户真实使用场景，保证应用违规收集用户数据的行为能充分的激发暴露。

（原文链接：https://mp.weixin.qq.com/s/B89zi9whDm2e1WYTD1du3A）

扫描右侧二维码阅读全文

“2021年网络安全优秀创新成果大赛－武汉分站赛”成功举办

8月4-5日，由中央网信办网络安全协调局指导，中国网络安全产业联盟（CCIA）主办的“2021年网络安全优秀创新成果大赛”武汉分站赛成功举办。武汉分站赛由武汉市网络安全协会承办，武汉光谷现代服务业园建设服务中心、武汉安天信息技术有限责任公司协办。

为响应国家防疫号召，本次分站赛采用申报单位线上答辩，北京、武汉两地专家线下集中评审的形式，来自武汉高校、科研机构、行业部门的专家与CCIA专家委专家、网络安全投资机构专家一起组成评审专家组。

正式开赛前，武汉网安协会会长、安天移动安全CEO潘宣辰代表承办单位发言，他谈到：新时代中各种科技革命和技术创新层出不穷，网络安全产业面临巨大历史机遇和挑战。促进技术与产品创新，加强网络安全人才能力建设，推动网络安全产业发展，是协会与网络安全企业义不容辞的责任和义务；很荣幸这次能够承办此次大赛，为广大企业创新成果提供展示、比拼的平台。预祝本次大赛圆满成功。

来自全国40余家网络安全企业提交的近50项解决方案和创新产品参加了本次比赛。经过评审，武汉分站赛最终评选出“2021年网络安全优秀创新成果大赛”解决方案入围奖10项和创新产品入围奖10项。

“2021年网络安全优秀创新成果大赛”是CCIA在连续三年组织开展“优秀网络安全解决方案和创新产品评选活动”基础上进行的创新评选活动。大赛首次采用分站赛形式，赛程分为分站赛初赛、半决赛和总决赛三个阶段，致力于推选我国网络安全产业优秀创新成果，激发网络安全企业加强自主创新能力，搭建网络安全企业、技术、人才和资本合作的平台，推动网络安全产业高质量发展。

（原文链接：https://mp.weixin.qq.com/s/VGxODSbC5HZo1HNKnlEUJg）

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	APT 组织 PrayingMantis 正在攻击 Microsoft IIS 服务器
英文标题	New APT Hacking Group Targets Microsoft IIS Servers with ASP.NET Exploits
作者	Ravie Lakshmanan
内容概述	作为一系列有针对性的网络入侵攻击的一部分，一个新的强大而持久的黑客组织一直在瞄准美国主要的知名公共机构和私人，利用 IIS 服务器渗透他们的网络。识别出该活动的以色列网络安全公司 Sygnia 将其命名为“PrayingMantis”。PrayingMantis 使用定制的恶意软件框架，围绕一个通用核心构建，为 IIS 服务器量身定制。该工具集是完全易失的，会反射性地加载到受影响机器的内存中，并且在受感染的目标上几乎没有留下任何痕迹。该组织还使用一个额外的隐蔽后门和几个后利用模块来执行网络侦察、提升特权和在网络内横向移动。
链接地址	https://thehackernews.com/2021/08/new-apt-hacking-group-targets-microsoft.html

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 Excel 远程代码执行漏洞（CVE-2021-34518）	高	Microsoft Excel 存在远程代码执行漏洞。由于 Microsoft Excel 中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件并在目标系统上执行任意代码。
	Microsoft Defender 远程代码执行漏洞（CVE-2021-34522）	高	Microsoft Defender 存在远程代码执行漏洞。由于 Microsoft Defender 中的输入验证不正确，使得攻击者可以发送特制的请求并在目标系统上执行任意代码。
	Oracle WebLogic Server 远程代码执行漏洞（CVE-2021-2397）	高	Oracle WebLogic Server 存在远程代码执行漏洞。由于 Oracle WebLogic Server 的核心组件中的输入验证不正确，使得未经身份验证的攻击者可以利用此漏洞执行任意代码。
较为活跃样本家族	Trojan[Ransom]/Win32.Crypmodadv	高	此威胁是一种勒索软件家族。该家族的样本在运行后，会加密系统上多种文件格式的文件，并将文件的扩展名更改为 .remind。在加密后，该样本会在全部的文件夹下各放置一封 HTML 格式的勒索信说明情况。
	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/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.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	Trojan[Downloader]/NSIS.Adload	中	此威胁是一种下载类木马家族。该家族木马通常使用 NSIS（开源的 windows 系统下的程序制作工具）将木马与正常程序捆绑在一起，主要功能是通过网络下载其他恶意软件。
	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.Hqwar	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

云备份应作为安全实践的一部分

大卫·福伦德 / 文　安天技术公益翻译组 / 译

勒索软件威胁无处不在，网络犯罪分子不断改进其攻击战术，以期尽可能地造成破坏。最近的 Kaseya 攻击事件给企业敲响了警钟：当勒索软件攻击发生时，不仅企业的数据会面临危险，企业的业务也会面临危险。此外，最近 Sophos 调查发现，在 2021 年，每起勒索软件攻击的平均补救成本（包括失去的业务）增加到近 200 万美元，大约是赎金本身的 10 倍。

首席信息安全官（CISO）和实际操作的安全专家正在实施多种策略来保护他们的企业，这些策略包括主动威胁猎杀，以及诸如多因子身份鉴别等技术防御措施。

这些策略很有帮助，但是存在一个问题：它们的关注点是防止攻击发生。而企业面临的严酷现实是“黑客何时会攻入企业”，而非“黑客是否会攻入企业”。既然企业面临如此多的风险，为何还要将“数据恢复和存储”置于安全实践的次要位置呢？实际上，数据恢复和存储可能是安全武器库中最有价值的工具。

转变观念：备份是优先事项

企业很难保证其网络始终不会被黑客入侵。IT 主管必须假设，攻击者将能够突破他们的防御并部署勒索软件。他们最终是否需要支付数百万美元才能拿回部分数据，完全取决于他们从备份中恢复所有系统的能力。

由于大多数 IT 运营已转移到虚拟机上的容器中，因此恢复所有系统、数据和应用程序应该是一个简单的过程。

如果企业从一开始就将数据存储和云备份纳入安全计划中，就可以通过清除系统并在几乎不停机的情况下迅速恢复数据，轻松摆脱勒索软件攻击并迅速恢复过来。但这是一个耗时的技术过程，因此 IT 团队应该进行实践和准备，就像他们应对应用程序中断或维护问题一样。

举例来说，许多备份可能不完整，因此从备份恢复系统的过程会失败。对企业的灾难恢复计划进行测试，可以了解企业当前的安全态势如何，以及在真正的灾难发生时能否保持这种安全态势。

云备份和安全

如果企业已经将数据备份到云中，黑客将不得不渗透到云服务中并找到一种方法来擦除或加密数据。云中“不可变性”的另一个优势是，可防止在固定时间段内对受保护数据进行任何修改或删除。

安全团队需要注意，并非所有的不可变性都是一样的。硬件供应商多年来一直提供不可变性，但是任何可以侵入系统管理员面板的人员都可以轻松击败这种“不可变性”功能。

许多企业（包括一些大型企业）的云服务也是如此。企业的漏洞通常来自外部，但有时也会涉及心怀不满的员工或有权访问管理职能的人员。在考虑将备份存储到云中时，“不可变性”应该意味着任何人（包括 IT 主管或系统管理员）都不能在数据写入后再对其进行更改。

回归基本安全措施

大多数安全实践关注的是入侵防御和检测。但是，企业不仅存在技术性漏洞，还有“人的”漏洞（员工经常会被诱骗犯错）。因此，企业应关注基本的安全措施，否则难以在对抗勒索软件的战斗中获得胜利。

企业与其沉迷于最新的防火墙技术或入侵检测软件，不如将所有内容完全备份，以便在发生勒索软件攻击时，可以简单地清除系统并进行恢复，以最大程度地减少停机时间。通过部署具有不可变性和云备份的强大数据保护策略，企业可以避免其运营陷入停顿。

原文名称	Why isn’t cloud backup part of common security practices?
作者简介	大卫·福伦德（David Friend），是 Wasabi 公司的首席执行官。
原文信息	2021 年 7 月 30 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/07/30/cloud-backup-security-practices/
摘　要	大多数安全实践关注的是入侵防御和检测。但是，企业不仅存在技术性漏洞，还有“人的”漏洞（员工经常会被诱骗犯错）。因此，企业应关注基本的安全措施，否则难以在对抗勒索软件的战斗中获得胜利。企业与其沉迷于最新的防火墙技术或入侵检测软件，不如将所有内容完全备份，以便在发生勒索软件攻击时，可以简单地清除系统并进行恢复，以最大程度地减少停机时间。通过部署具有不可变性和云备份的强大数据保护策略，企业可以避免其运营陷入停顿。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。