安天智甲有效防护 Dharma 勒索软件新变种

近日，安天 CERT 在梳理网络安全事件时发现一个 Dharma 勒索软件新变种。该变种最早于 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 Dharma 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“.id-八位随机字符串 .[259461356@qq.com].259”命名的后缀。加密完成后，弹出一个标题为“259461356@qq.com”的勒索信窗口，其具体内容包含了勒索说明、联系邮箱。该勒索软件还会在硬盘根目录下创建一个名为“FILES ENCRYPTED.txt”的勒索信，该勒索信的内容中再一次强调了交付赎金的方式。

▲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、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、动态行为鉴定器、智能学习鉴定器、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	Dharma.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	93 KB
MD5	A8884F621898726F414FB4F66167142A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Crysis
判定依据	反病毒引擎

◆ 操作系统

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

◆危险行为

行为描述	危险等级
文件篡改	★★★★★
检测虚拟机	★★★★★
创建可疑进程	★★★★
删除全盘所有卷影副本	★★★★

◆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	★★
枚举进程	★
打开自身进程文件	★
读取自身	★★
释放 PE 文件	★
释放 PE 文件到系统目录	★★
Run 自启动	★
设置自启动项	★★
.....	.....

◆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 23 日 (总第 255 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

中国网络安全产业全景图发布，安天全栈技术布局显现

11 月 16 日，国内第三方安全研究机构 FreeBuf 咨询正式发布《CCSIP（China Cyber Security Industry Panorama）2020 中国网络安全产业全景图》（以下简称 CCSIP 全景图）。此次 CCSIP 全景图共涵盖 19 个一级分类，79 个二级分类，覆盖 550+ 家安全厂商，展现 2000 余次。所有调研及设计工作由 FreeBuf 咨询团队主导完成，上百家厂商提供数据支持。

安天凭借先进的自主研发实力和领先的产品技术架构能力，入选 CCSIP 全景图中 8 个一级分类：漏洞检测与管理、事件管理与响应、调查取证、威胁检测与捕获、安全服务、安全情报、计算环境安全、移动安全；20 个二级分类：漏洞管理、SOC、SIEM、UEBA、NTA/NDR、APT 高级威胁检测 / 恶意软件检测沙箱、渗透测试与评估、风险评估、安全靶场、攻防演练、威胁情报、主机安全 /AV、IDPS、主机安全 /EDR、欺骗诱捕 / 蜜罐、移动终端管理、移动应用安全、移动业务安全、手机防病毒、安全咨询与培训教育。

达成有效客户安全价值，构筑能力型产品矩阵

安天在 20 年的发展历程中，始终致力于有效应对安全威胁，全面提升客户的网络安全防御能力。通过 20 年自主研发积累，安天形成了威胁检测引擎、移动场景安全、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势。构筑了由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，为客户构建资产安全运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置、零信任接入等安全基石。安天通过为客户建设态势感知平台体系，形成网络安全运行的神经中枢，提升客户统一安全运维水平，通过大规模感知体系、大规模支撑平台，以及快捷精准的威胁情报持续赋能客户。

安天的产品和服务为战略客户以及关键信息基础设施提供有力安全保障，自 2015 年以来，已保障了包括载人航天、探月工程、空间站对接、火星探测等重大型号发射任务的安全，同时，在民航、电力等关键信息基础设施场景中为客户构建态势感知平台和全面安全解决方案。

以威胁对抗为能力成长主轴，渐进形成全栈防御安全能力

“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”安天坚持以威胁对抗为能力成长主轴，以系统和流量为基础对抗场景，渐进形成了威胁对抗的完整技术栈。

安天在系统安全方面有 20 年渐进积累，创业伊始，即在反病毒引擎研发的基础上，推出了融扫描、主防、工具集于一体的 Antiy Ghostbusters 反木马软件（安天智甲终端防御系统前身），构筑了安天在系统安全侧的能力基础，成为首个登上全球 AntiVirus TOP50 的中国产品。

从 2002 年起，安天承担高速网络的高速恶意代码检测能力的科研攻关为起点，构筑了零拷贝捕包和高速协议栈体系，创立 VDS（恶意代码检测系统）细分产品品类，最终发展成为安天探海威胁检测系统。探海威胁检测系统进行细粒度的格式识别和解析还原，基于 13 元组标定，通过安天 AVL SDK 反病毒引擎实现海量已知恶意代码精准检测和可疑文件标定，通过行为引擎和威胁情报检测相关攻击活动，标定攻击组织和攻击基础设施，并以全要素采集能力为基础，实现按需采集，为态势感知供给分析数据。安天基于大规模沙箱后台进行海量分析的自动化运营经验，封装沙箱和下一代引擎的动静态检测能力，构筑了追影威胁分析系统，有效推动客户的私有化威胁情报生产和对抗运维。基于长期的蜜网系统建设所积累的经验，形成了捕风蜜罐系统产品。基于工程师攻击场景取证和应急处置积累的自研工具，形成了拓痕应急响应工具。

安天积极对标威胁框架提升产品能力，在 2019 年 6 月 30 日，安天引擎和全线产品已将事件类型和标签体系切换到 ATT&CK 威胁框架，安天态势感知平台可双标支持 ATT&CK 和 TCTF 两种威胁框架。

坚持打造工程平台支撑能力，面向大规模威胁情报客户赋能

安天在创业之初，提出了借鉴工业流水线模式的大规模样本自动化分析的技术构想，于 2004 年实现了全量样本的自动化分析处理能力，并将决策树等方法应用到后端分析中。为了进一步提升复杂分析作业的效率，安天研发了融合反汇编调试、数据包分析、十六进制编辑和标签提取的集成化人工分析环境，通过将分析能力与流水线融合，实现了席位化的分布式人工协同分析能力。安天始终坚持工程平台支撑能力的研发，基于后台流水线的大规模自动化分析，形成了海量样本分析能力，并于 2013 年通过第二代流水线实现了人工分析与大规模自动化分析的快速经验迭代。

安天定义了 AVML 格式，用以标准化存储样本动静态分析成果，并通过构建 AVML 搜索引擎，奠定了威胁情报的框架基础。在 AVML 搜索基础上，安天基于长期的载荷向量和知识图谱积累，构筑了 ATID 威胁情报门户，为战略客户提供关联分析支持。安天通过为战略客户构建大规模海量样本动静态分析系统、对照扫描系统、深度学习聚类判定系统、多席位联合人工分析系统等，有效支撑了战略客户的需求。

安天通过全栈技术布局，将全面赋能客户，提升客户的网络安全防御能力，有效应对安全威胁。

每周安全事件

类 型	内 容
中文标题	思科发布了 Cisco Security Manager 关键漏洞的安全公告
英文标题	Researcher Discloses Critical RCE Flaws In Cisco Security Manager
作者及单位	Ravie Lakshmanan
内容概述	在网络设备制造商 Cisco 悄悄发布了 Cisco Security Manager（CSM）的 4.22 版补丁程序后的一周，思科发布了多个有关 Cisco Security Manager 关键漏洞的安全公告。研究人员近日公开披露的概念验证（PoC）代码中，涉及多达 12 个影响 CSM Web 界面的安全漏洞，这使得未经身份验证的攻击者有可能实现远程代码执行（RCE）攻击。Cisco Security Manager 是一种端到端企业解决方案，它使组织能够执行访问策略并管理和配置网络中的防火墙和入侵防御系统。
链接地址	https://thehackernews.com/2020/11/researcher-discloses-critical-rce-flaws.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	Windows cng.sys 权限提升漏洞（CVE-2020-17087）	高	Windows Kernel 中存在一个本地权限提升漏洞，未授权的攻击者通过诱使用户运行恶意的二进制程序，最终造成权限提升。
	Windows NFS 远程代码执行漏洞（CVE-2020-17051）	高	Windows NFS 是一种网络文件系统，用户可以通过 NFS 访问网络上的文件并将它们像本地文件一样操作。攻击者可以利用此漏洞来访问系统，并远程执行恶意代码。
	Windows Exchange Server 远程代码执行漏洞（CVE-2020-17084）	高	Windows Exchange Server 中存在一个远程代码执行漏洞，未授权的远程攻击者通过向 Exchage 服务器发送特制的请求包来进行漏洞利用，利用成功后便可获得服务器完整控制权限。
较为活跃样本家族	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan/Win32.Blamon	中	此威胁是一种可以窃取密码信息的木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键等。
	Trojan/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	Trojan/Win32.Cometer	中	此威胁是一种后门类木马程序。该类木马样本主要以 CobaltStrike、MSF 框架生成的相关后门为主，通常利用 powershell 脚本将恶意载荷注入到内存中，不在文件系统中落地，绕过一些反病毒软件。样本具有一定的远程控制功能。
	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.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

“新常态”下的统一端点管理

乔尔·沃伦斯特伦 / 文 安天技术公益翻译组 / 译

新冠疫情永久性地改变了世界。禁足令发布后，几乎一夜之间，美国全职在家办公的人数从约 7%（根据美国劳工统计局 2019 年的数据）增长到约 42%（根据斯坦福大学经济政策研究所的数据）。

在家办公的最初目的是阻断新冠病毒的传播，它影响了几乎所有使用数字安全的企业。疫情很有可能会继续存在。部署统一端点管理（UEM）解决方案有助于保持强大的安全性，使用户在“新常态”下安全办公。

为远程办公人员部署 UEM

尚未支持广泛远程办公的企业马上就会面临问题。一夜之间，培训和支持在家工作的员工并为其赋能，变得至关重要。但是，很少有企业能够按计划进行过渡。许多员工发现很难学会使用远程会议和远程访问业务 IT 资源的新工具。在很多情况下，IT 主管缺少远程诊断和修复被上报问题所需的工具。

这导致员工的生产力下降，使其感到沮丧。即使对远程交付 IT 服务进行了数月的改进，为在家办公的员工提供与在办公室相同水平的的数字便捷性仍然很困难。

不断变化的在家办公授权带来了新的风险，也扩展了现有的威胁向量。之前，敏感数据受到企业防火墙的保护；而现在，远程办公人员需要访问或下载这些数据。对于那些员工使用 BYOD 设备（例如家用台式 PC）进行远程办公的企业来说，这个问题尤其严重。在这些情况下，企业仅能有限地保护设备。而攻击者也利用恶意软件、勒索软件和网络钓鱼等手段，对家庭用户（而非企业）发动猛烈的攻击。通常，如果远程办公人员的设备遭到感染，那么企业也会受到感染。

平衡用户体验和安全性

有人认为，企业安全和用户友好是相互矛盾的。换句话说，随着安全性的提高，用户友好性必须降低，反之亦然。但是，企业管理协会（EMA）的研究表明，事实并非总是如此。部署使用户更轻松的 IT 服务和流程可以提高安全性。这是因为，在此基础上，用户倾向于使用那些受保护的资源，而不是绕过它们。

UEM 是弥合安全性和用户友好性之间鸿沟的一种战略性方法。其他以设备为中心的客户端生命周期管理方法，对用户行为和条件的了解很少。此外，UEM 解决方案可以跨用户设备（即台式机、笔记本电脑、平板电脑和智能手机）收集数据，以发现安全风险和情境数据。然后，该解决方案处理收集的数据，以开发和执行针对用户的自定义策略。

UEM 解决方案的优势

为了更好地说明此方法的价值，我们以收集相关安全数据的 UEM 解决方案为例进行说明。该解决方案了解用户、设备、操作系统、活动进程、网络、位置以及活动 IT 服务在做什么。该方案使用智能工具（例如分析、语言处理或认知计算），快速确定用户设备的风险级别。如果风险级别（风险评分）超过预设的阈值，则网络安全团队可以采取相关措施来降低风险。例如，他们可以禁用对特定服务的访问或实施更严格的访问策略。

相反，如果风险级别较低，则可以取消访问和使用限制，允许更大的用户自由度和性能改进。这样一来，安全措施就能与确定的风险级别保持一致。只有在风险级别上升的情况下，才会实施更严格的访问限制。

如何让 UEM 为企业服务

为了获得成功，安全团队必须对其 UEM 解决方案具有高度的信心。确保 UEM 平台直接或通过第三方解决方案收集大量情境数据，可以实现这一点。研究用户行为有助于预测危险行为和生产力下降的情况。此外，这使工具可以快速解决问题并提高用户友好性。

最后，安全团队将必须学会适应“新常态”。毕竟，这种新常态不会消失。全世界的员工都已经体验到在家办公的优势。即使在新冠疫情之后，很多人也不愿放弃这种工作模式。此外，企业领导者已经被迫投资于远程办公工具。疫情之后，他们不情愿舍弃这些工具。实际上，企业支持在家办公的实力，可能会成为吸引和留住人才的关键因素。

但是，员工必须安全地进行远程工作，不要给企业带来更严重的安全和合规问题。通过收集情境数据和创建基于数据的策略，为自适应 UEM 赋能，可以在不影响安全性的情况下提高员工生产力和用户友好性。

原文名称	Unified Endpoint Management for the New Normal
作者简介	瑞安 · 施瓦兹（Ryan Schwartz）。瑞安 · 施瓦兹是一位产品营销经理。
原文信息	2020 年 11 月 13 日发布于 SecurityIntelligence 原文地址 https://securityintelligence.com/posts/unified-endpoint-management-for-the-new-normal/
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。 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。