安天智甲有效防护 Tellyouthepass 勒索软件

勒索软件名：Tellyouthepass 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.locked
支付与金额：通过邮箱与攻击者联系
免费解密工具：暂未发现

▲Tellyouthepass 勒索信

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Tellyouthepass 的勒索软件，该勒索软件最早发现于 2019 年 3 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，该勒索软件程序执行加密行为结束后会在 All Users 文件目录下创建日志文件记录加密文件情况。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 Tellyouthepass 勒索软件的加密行为。

Tellyouthepass 勒索软件样本运行后，在用户桌面弹出 CMD 命令行工具界面，片刻后开始写入内容，其内容为加密文件进度、是否成功以及数量，与此同时加密计算机上的文件，内容写入完成后，自动关闭命令行界面并完成加密，并在 C 盘目录下的 Users 文件目录中的 All Users 文件夹创建一个名为“dVBRr.txt”文件，文件内容为所有被加密文件的文件路径、文件名、加密失败信息和加密文件总数，在被加密文件原文件后追加“.locked”的后缀。在桌面和所有含有被加密文件的路径下创建名为“README.html”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 User_ID 等。

Tellyouthepass 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、关联分析鉴定器、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、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、关联分析鉴定器、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	ec7bae245d61cb7f7a9fa51f487a22e006109d628645f31b880fc72ac58f8027
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.96 MB
MD5	E1E41506DA591E55CEE1825494AC8F42
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Encoder
判定依据	BD 静态分析

◆危险行为

行为描述	危险等级
文件篡改	★★★★★
疑似查找游戏进程	★★★★

◆常见行为

行为描述	危险等级	行为描述	危险等级
加载运行时 DLL	★	获取计算机名	★
获取系统信息（处理器版本、处理器类型等）	★	查找窗口	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★	打开自身进程文件	★
获取驱动器类型	★	设置文件属性为隐藏	★★
创建挂起进程	★★	疑似桌面控制	★
设置调试器权限	★	检索系统内存信息	★
枚举窗口	★	释放 PE 文件	★

◆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 8 月 17 日 (总第 243 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天与卫士通签署战略合作协议

安天与卫士通信息产业股份有限公司（以下简称“卫士通”）在京签署战略合作协议，安天创始人、董事长肖新光，安天执行董事长、CEO 游小明，中国网安董事长、30 所所长、卫士通董事长卿昱，总经理王忠海等双方高管共同出席并见证签约仪式。双方将在网络信息安全产品与服务，信息系统集成，信息技术应用创新等领域开展深度合作，更好的服务于政企、军队、军工和关键信息基础设施用户[1]。

安天与神州慧安达成战略合作协议

安天与神州慧安科技有限公司（以下简称：神州慧安）在北京签署战略合作协议。在神州数码集团董事长兼总裁郭为与安天创始人、董事长、首席技术架构师肖新光的共同见证下，神州慧安董事长肖国汉，首席科学家张友平，安天执行董事长、CEO 游小明共同签署了战略合作协议。安天资深副总裁、首席科学家童晓渝，高级副总裁李家成等高管出席签约仪式。双方将聚焦信创与工业网络安全防护领域，整合双方技术及市场资源和优势，开展产品研发、集成开发和渠道赋能合作，提高双方整体竞争力。

安天与神州网信建立深度战略合作伙伴关系

安天和神州网信技术有限公司（以下简称“神州网信”）在京签署《战略合作备忘录》，结合双方在桌面操作系统领域的积累及在终端威胁检测与防御等网络安全领域的优势，建立深度战略合作伙伴关系，从而更好服务于广大政企用户。安天与神州网信将通过本次战略合作，基于 Windows 10 神州网信政府版操作系统平台，发挥各自在技术、产品、服务等方面的优势，进行操作系统、终端安全、网络防护等深度合作，为政府机构及关键信息基础设施领域用户提供技术先进、安全可控的计算平台和主动预防的安全防护服务。

Dharma 勒索软件提供黑客工具包以简化网络犯罪

Dharma 勒索软件即服务（RaaS）提供了几乎可以为他们做所有事情的工具包，使想要成为网络犯罪分子的人很容易实施勒索软件攻击。RaaS 是一种网络犯罪模型，开发人员负责勒索软件的开发和管理勒索支付系统。同时，会员可以部署勒索软件并对受害者进行勒索。
https://www.bleepingcomputer.com/news/security/dharma-ransomware-created-a-hacking-toolkit-to-make-cybercrime-easy/

每周安全事件

类 型	内 容
中文标题	Group-IB 称 APT 组织 RedCurl 主要从事商业间谍活动
英文标题	Rent a hacker: Group-IB uncovers corporate espionage group RedCurl
作者及单位	Pierluigi Paganini
内容概述	总部位于新加坡的全球威胁情报公司 Group-IB 已发布有关先前未知的 APT 组织 RedCurl 的分析报告，该组织主要从事商业间谍活动。在不到三年的时间里，RedCurl 袭击了世界各地的几十个目标——从俄罗斯到加拿大。这个讲俄语的组织使用一套独特的工具对多个行业的私营企业进行了有计划的攻击。攻击者试图窃取包含商业机密和员工个人数据的文件。根据 Group-IB 专家的说法，到目前为止，商业间谍活动在黑客领域还是一个罕见的现象，但近期此类攻击的频率表明，它很可能在未来变得更加普遍。
链接地址	https://securityaffairs.co/wordpress/107094/apt/redcurl-hacking-group.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		简要描述
活跃漏洞	Microsoft Windows Codecs Library 安全漏洞（CVE-2020-1457）	高	当 Microsoft Windows Codecs 库处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以执行任意代码。攻击者需要程序处理经特殊设计的文件才能利用此漏洞。
	Microsoft Windows Graphics Device Interface 安全漏洞（CVE-2020-1435）	高	Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	Linux GRUB2 安全漏洞（CVE-2020-10713）	高	GRUB2 在处理配置文件 grub.cfg 时发生缓冲区溢出，存在本地代码执行漏洞。一旦该漏洞被利用，攻击者可以在 UEFI 执行环境中获得任意代码执行权限，该代码可以用于运行恶意软件，更改启动过程，直接篡改 OS 内核数据或执行许多其他恶意操作。
较为活跃样本家族	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.Gofot	中	此威胁是一种具有窃密行为的木马家族。该家族的样本在执行后会连接远程服务器以发送 其在用户设备上收集到的数据。
	Trojan[Banker]/Win32.Banbra	中	此威胁是一中专门用于盗取银行信息木马家族。该家族木马运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行监控，在被窃取的信息发送到金融网站之前就被传送到远程服务器上。
	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[Backdoor]/Linux.Gafgyt	中	此威胁是 Linux 平台上的具有窃密行为的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作，并且会收集机器上的信息上传给远程控制端。
	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。
	Trojan/Android.SmForw	中	此威胁是安卓平台的一类木马家族。该家族样本运行后开机自启动，安装后隐藏图标，监听收件箱并删除接收到的短信，后台私自上传设备信息、短信、收件箱信息。且还具有远程控制功能，会造成隐私泄露，资费消耗。

供应商管理：远程工作的七个安全建议

苏·波伦巴 / 文 安天技术公益翻译组 / 译

第三方供应商管理会威胁到企业的数据和网络安全。企业使用供应商的服务，同时要求供应商在访问其网络时采用符合其标准的安全最佳实践。但是那时候，大多数员工都在现场工作，能够受到更严格的网络安全监管。

而现在，远程工作已经成为常态。与企业各部门相同，第三方供应商也存在远程工作的安全风险。其员工可能正在使用个人设备、共享设备、在不良的家庭安全措施下工作、使用不安全的 WiFi 等等。

首席信息安全官和其他安全决策者必须重新考虑远程工作安全标准，以保证远程员工的安全性。同样，他们还需要确保第三方供应商遵守这些标准。企业可以参考以下七个建议，评估在员工远程工作的情况下第三方供应商的安全性。

重新评估供应商管理风险

现在正是重新评估每家供应商整体安全状况的好时机。企业应考虑，其供应商在 2019 年的安全标准如何？他们是否是近期数据泄露的受害者？他们有哪种安全计划？他们对企业网络和数据具有哪种访问权限？他们将数据存储在哪里？他们有哪些防止数据丢失或服务中断的规程，尤其是在诸如病毒传播或自然灾害等危机情况下？

如果供应商不符合企业的安全标准，那么企业是时候考虑结束这种服务关系了。

了解远程工作带来哪些风险

Digital Shadows 指出，第三方供应商风险主要分为三类：运营风险、交易风险和合规 / 监管风险。为避免受到这些风险的影响，企业应确保，供应商在员工开始远程工作时及时更新安全标准。企业应具备应急计划；这样一来，

即使供应商的安全措施失败，企业也可以保证其业务连续性。企业应采取必要的措施，满足行业和政府标准中的所有合规性要求。

询问供应商如何管理网络安全

恰当的供应商管理包括，供应商与企业领导就双方如何管理安全性进行持续对话。双方都应了解，企业有多少远程工作的员工，哪些员工在现场工作？总体安全覆盖范围如何？远程 vs 现场解决网络事件需要多长时间？这些对话中应包括之前的所有安全标准，例如加密服务或恶意软件检测软件。

了解所有供应商

企业了解所有的第三方供应商吗？如果答案是否定的，那么企业是时候好好了解一下他们有哪些供应商以及如何与供应商进行交互了。云服务提供商能够访问企业的基础架构，这不同于临时访问企业网络、访问权限受限的顾问；也不同于每月参加一次视频电话会议的独立承包商。企业应了解能够以某种方式访问其网络的所有个人或公司，这有助于企业更好地维护网络安全和检测潜在威胁。企业可能会发现，他们的一些第三方供应商拥有本不应拥有的访问权限和凭证。

更新服务级协议

企业已经与供应商签订了协议，这是供应商管理的一部分。企业可以考虑在协议中添加涉及远程工作安全问题的修订条款。如果企业不确定修订条款需要包含哪些内容，可以参考其内部安全策略。企业需注意，任何能够访问企业敏感信息的人士（无论他在公司内部还是外部）都应遵循相同的安全规程。可以添加到协议中的内容包括“远程服务位置的限制、维持所需性能有困难（或不可能）、服务交付成本增加，以及客户无法在家庭工作环境中实施的安全保障措施等”，一篇 Lexology 博客指出。

对远程工作的员工实施多因子身份鉴别

现场工作的情况下，第三方供应商可能会亲自访问企业网络上的应用程序。而在远程工作的情况下，这可能无法实现。虽说企业应始终实施多因子身份鉴别，但是在第三方供应商远程工作并使用未知设备访问企业网络时，这一点尤其重要。每个人的访问凭证都应该是唯一的，这样能够防止凭证窃取。如果员工离职或调职，其继任者不应沿用同样的凭证。此外，企业应考虑使用他们可以控制的第二或第三因子，例如射频识别（RFID）或生物识别因子，而非短信或电子邮件。与供应商的业务关系终止后，企业需立即关闭相关账户。

了解安全系统如何影响供应商

网络安全问题并非凭空出现。如果供应商给企业增加了安全风险，企业应考虑其员工是否向供应商打开了安全风险之门。企业应制定恰当的安全策略，来处理第三方供应商可能受到的影响。鉴于企业的响应团队可能远程工作，且包括法律、市场营销、人力资源、信息技术和安全团队等各部门的代表，因此企业应预先制定紧急响应计划，这将使相关人员迅速了解情况，并以有组织的方式迅速解决问题。

原文名称	Vendor Management: 7 Tips for Security During Remote Work
作者简介	苏 · 波伦巴（Sue Poremba）。苏 · 波伦巴是一位作家，擅长网络安全和技术领域。
原文信息	2020 年 8 月 10 日发布于 Security Intelligence 原文地址 https://securityintelligence.com/articles/vendor-management-remote-work/
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。