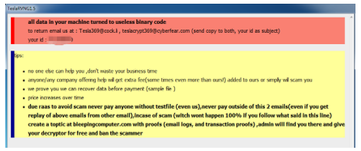
安天智甲有效防护 TeslaRVNG 勒索软件变种

勒索软件名：TeslaRVNG 勒索软件
传播方式：垃圾邮件
加密算法：AES + ECIES
后缀：.teslarvng1
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 TeslaRVNG 勒索软件新变种。最早于 2021 年 1 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 TeslaRVNG 勒索软件的加密行为。

TeslaRVNG 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，在被加密文件的文件名前添加“id[八位随机字符串].[Tesla369@cock.li].”，后缀名后追加以“.teslarvng1”命名的后缀。加密完成后，删除系统卷影副本，以防止恢复加密文件，并在加密文件所在的文件夹中创建一个名为“teslarvng1.5.hta”的勒索信，该勒索信具体内容包含了勒索说明、ID 以及联系邮箱。



▲TeslaRVNG 勒索信

TeslaRVNG 勒索软件采用“AES + ECIES”加密算法加密文件，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、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、等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	B6E54EA346552C980A8F86EADFA82B3A
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	403 KB
MD5	B6E54EA346552C980A8F86EADFA82B3A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Johnnie
判定依据	BD 静态分析

获取进程信息 API	★
线程操作函数	★
进程 / 线程是否处于调试状态	★
结束进程类函数	★
创建进程	★
进程调试 API	★
内存堆操作	★
窗口控制台模式	★
……	.....

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
枚举进程	★

◆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 02 月 01 日 (总第 265 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

第八届安天网络安全冬训营即将启幕

为深入理解网络安全对抗，提升防御水平，自 2014 年起，在国家主管部门指导下，安天以“直面真实威胁，形成价值落地”为导向，已连续承办了七届网络安全冬训营。冬训营已经由最初的小规模业内交流活动，逐步发展由融合威胁趋势和案例分析、客户运营经验分享、安全方法框架研讨、安全技术与实践争鸣等议题板块组成，带有独特风格特色的综合型技术论坛加实训活动。

由于疫情防控的原因，第八届安天网络安全冬训营将改为线上交流的形式，于 2021 年 2 月 3 日进行首播。本届冬训营营语为“长缨待展”，将以“威胁框架：细粒度对抗”为主题，分享威胁框架和防御矩阵的最新国际进展，分析全球抗击疫情背景下网空威胁活动的新情况，介绍安天引入威胁框架全面提升产品和服务能力的新进展，特别关注如何根据攻击技术和子技术遍历，细粒度的改善各防御环节。

“梅花欢喜漫天雪”，傲立只待报春来。安天将与网络安全同仁携手努力，共同打造赋能客户，达成有效安全价值的产品与服务，阻断、迟滞和呈现对手杀伤链。

已有“长缨”在，“待展”缚苍鹰。

（直播地址：http://live.163.com/room/235103.html）

扫描上方二维码观看直播

黑客暗网出售 1.76 亿巴基斯坦电信用户数据

黑客在暗网出售一个包含 1.76 亿巴基斯坦电信用户信息的数据库。该数据库声称是来自巴基斯坦不同电信公司的数据汇总，数据具体包括城市、姓名、完整地址、电话号码、IMSI 码、激活日期和状态、生物识别验证状态、国民身份证号（CNIC）、连接所属的电信公司的名称。研究人员已针对该事件通知有关当局，目前还未取得任何回复。

（原文链接：https://www.hackread.com/pakistani-mobile-phone-users-database-sold-online/）

每周安全事件

类 型	内 容
中文标题	执法部门拆除 Emotet 僵尸网络的基础设施
英文标题	Emotet Botnet dismantled in a joint international operation
作者	Pierluigi Paganini
内容概述	由欧洲刑警组织领导的全球执法行动拆除了 Emotet 僵尸网络的基础设施。Emotet 银行木马至少自 2014 年以来一直活跃，其僵尸网络活动由一个被跟踪为 TA542 的攻击组织操纵，还被用于以 COVID-19 为主题的垃圾邮件活动。此项行动由来自荷兰、德国、美国、英国、法国、立陶宛、加拿大和乌克兰当局和负责协调国际活动的欧洲刑警组织和欧洲司法组织共用参与执行。据欧洲刑警组织称，Emotet 的基础设施由世界各地数百台具有不同功能的服务器组成。C2 基础设施使幕后操控者能够管理参与恶意软件传播和向网络犯罪团伙提供恶意服务的受感染系统
链接地址	https://securityaffairs.co/wordpress/113933/cyber-crime/emotet-global-takedown.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	Cisco SD-WAN vManage 命令注入漏洞（CVE-2021-1299）	高	由于用户对设备模板配置提供的输入进行了不正确的输入验证。攻击者可以通过向设备模板配置提交精心制作的输入来利用这个漏洞。成功利用漏洞可让攻击者获得对受影响系统的 root 访问权。
	Microsoft splwow64 权限提升漏洞（CVE-2021-1648）	高	Windows 打印驱动程序进程 SPLWOW64.exe 中存在权限提升漏洞，由于缺少对用户提供的数据进行适当验证，导致可能出现越界读取，攻击者可利用此漏洞进行权限提升。
	Windows Win32k 权限提升漏洞（CVE-2021-1709）	高	Win32k 系统进程中存在一个权限提升漏洞，经过身份验证的本地攻击者可利用此漏洞在目标系统上提升其权限以执行任意代码。
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[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[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[Backdoor]/Win32.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	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[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	此威胁是安卓平台的一类木马家族。该家族样本伪装成知名游戏应用，运行后隐藏图标，诱导激活设备管理器，接收短信指令，上传通讯录和信箱等隐私信息，进行发送短信、回复短信、拨打电话、卸载指定 apk、联网下载 apk 并弹出诱导安装等操作。建议立即卸载，避免造成隐私泄露和资费损耗。

将防欺诈解决方案集成到工作流程中

约书亚·戈德法布 / 文 安天技术公益翻译组 / 译

如果企业想要减少欺诈造成的损失，需要考虑诸多方面。例如，企业需谨慎思考如何将欺诈检测和预防解决方案集成到其日常运营工作流程中。换句话说，切实可行的防欺诈解决方案，必须能够轻松集成到企业的安全和防欺诈运营中。

市场上有许多欺诈检测和预防解决方案，它们各有特色。在评估和采购此类解决方案时，企业通常不够重视“集成到现有运营工作流程”这个问题。在本文中，我将重点介绍这一点。

任何声称能够无缝集成到现有运营中的欺诈检测和预防解决方案，至少应提供下述三个“R”：

- **建议（Recommendation）：** 无论欺诈检测和预防解决方案采用何种类型的数据建模、人工智能（AI）、机器学习或分析技术，它们都应提供清晰简洁的建议。毕竟，如果企业无法轻松采纳建议，那么即使是世界上最先进的技术和最强大的功能，也将毫无用处。
- **理由（Reason）：** 没多少人喜欢“黑匣子”类技术。如果你希望企业采纳你的建议，那么你应该向其明确说明提出该建议的理由。企业不需要了解复杂的知识产权，但是需要你给出一个简单易懂的逻辑描述，以了解你提出某项建议的理由。
- **审查（Review）：** 在提出建议并给出相应的理由后，企业很有可能会审查与这些建议相关的数据和条件。良好的欺诈检测和预防解决方案，能够使企业轻松审查这些数据，了解其能够从该解决方案中获得哪些收益。

市场上有很多解决方案能够满足上述三个“R”，它们之间有相当大的差异。在选择此类解决方案时，企业应注意它们能否满足下述几个要求，以便将其轻松集成到运营流程中。

- **易于部署：** 不幸的是，很多欺诈检测和预防解决方案难以部署。如果解决方案的部署冗长而复杂，就无法无缝集成到企业的运营工作流程中。
- **易于使用：** 如果解决方案不易使用，那么即使世界上最好的数据和建议对企业也没有太大帮助。良好的欺诈检测和预防解决方案，应该使企业轻松访问相关数据和建议。此外，企业无需数月的专业服务协助，即可将输出结果整合到运营流程中。
- **易于运营：** 在审查欺诈解决方案的成本时，企业通常会忽视运营和维护成本。除了这些成本之外，企业还需要注意解决方案的“实用性”——如果解决方案的运营和维护需要多个全职员工，就会影响企业的生产力。本应用于识别、分析和响应安全和欺诈事件的宝贵资源，会被浪费在处理设计和架构不佳的解决方案上。这会严重阻碍企业将这些解决方案集成到日常工作流程中。
- **高保真：** 良好的防欺诈解决方案不仅应提出建议，而且应提出好的建议。企业应该对防欺诈解决方案提供的数据的质量和保真度充满信心。此外，防欺诈解决方案的漏报率应该很低——如果防欺诈解决方案遗漏了很大一部分欺诈事件，那么这种解决方案就称不上“好”了。
- **低噪音：** 大多数安全和欺诈团队都没有太多额外的时间。有价值的防欺诈解决方案应具有极低的误报率。如果防欺诈解决方案生成大量噪音，干扰了企业的工作流程，那该解决方案对企业就没太大用处。实际上，较高的误报率会分散安全和防欺诈团队的注意力，使他们花费大量的时间和资源处理误报。
- **可转化为行动：** 防欺诈解决方案发出的任何告警都应该“可转化为行动”。如果安全团队不需要对某件事采取任何措施，那为何要告诉他们呢？如果只是为了刷一刷防欺诈解决方案的存在感，那么请不要发出这些告警。安全团队只需要了解真正重要的问题。
- **投资回报率（ROI）：** 计算防欺诈解决方案效果的最直接方法是 ROI。如果解决方案的成本为 X 美元，防止了 Y 美元的欺诈损失，则 Y 应该是 X 的有效倍数。否则，欺诈检测和预防解决方案将无法达到预期的效果。

原文名称	Integrating Fraud Data Into Your Workflow
作者简介	约书亚 · 戈德法布 （Joshua Goldfarb ）。约书亚 · 戈德法布是 F5 公司的产品管理总监。
原文信息	2021 年 01 月 06 日发布于 Security Week 原文地址 https://www.securityweek.com/integrating-fraud-data-your-workflow
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。