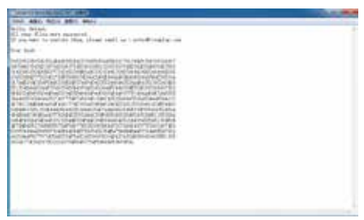
安天智甲有效防护 RegretLocker 勒索软件

勒索软件名：RegretLocker 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.mouse
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名为 RegretLocker 的勒索软件。该勒索软件最早于 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 RegretLocker 勒索软件的加密行为。

RegretLocker 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“.mouse”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“HOW TO RESTORE FILES.TXT”的勒索信，该勒索信具体内容包含了勒索说明、赎金金额、联系邮箱。该勒索软件利用 Windows Restart Manager API，终止在加密过程中使文件保持打开状态的进程或服务。



▲RegretLocker 勒索信

RegretLocker 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，即可实现对上述感染式恶意代码进行有效检测，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、关联分析鉴定器、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	RegretLocker.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	483 KB
MD5	3265B2B0AFC6D2AD0BDD55AF8EDB9B37
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.RegretLocker
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
删除全盘所有卷影副本	★★★★
查询系统硬盘大小	★★★
堆喷射	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
枚举进程	★
释放 PE 文件	★
获取计算机名	★
Run 自启动	★
获取驱动器类型	★
添加计划任务	★★
WMIC 调用执行	★★
获得计算机用户名	★
.....	.....

◆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 11 月 16 日 (总第 254 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天三个项目入选工信部 2020 年网络安全技术应用试点示范名单

11 月 9 日，工业和信息化部（以下简称工信部）公示了 2020 年网络安全技术应用试点示范名单，安天申报的“电力网络安全监测与指挥平台”、“智信零信任应用安全交付服务平台”、“网络空间威胁情报大数据共享开放平台”三个项目全部入选，现正在公示中。

其中“电力网络安全监测与指挥平台”项目入选《新型信息基础设施安全类 - 工业互联网安全》；“智信零信任应用安全交付服务平台”项目入选《新型信息基础设施安全类 - 智慧城市安全》；安天与中国科学院信息工程研究所等共同申报的“网络空间威胁情报大数据共享开放平台”项目，入选《网络安全公共服务类 - 威胁情报》。

附 件

2020 年网络安全技术应用试点示范公示名单

一、新型信息基础设施安全类

（二）工业互联网安全

序号	项目名称	申报单位
20	电力网络安全监测与指挥平台	安天网络安全技术有限公司

（四）智慧城市安全

序号	项目名称	申报单位
16	智信零信任应用安全交付服务平台	北京安天网络安全技术有限公司

二、网络安全公共服务类

（三）威胁情报

序号	项目名称	申报单位
1	网络空间威胁情报大数据共享开放平台	中国科学院信息工程研究所 奇安信网神信息技术（北京）股份有限公司 北京安天网络安全技术有限公司

工信部组织开展的“2020 年网络安全技术应用试点示范工作”，主要根据《工业和信息化部办公厅关于开展 2020 年网络安全技术应用试点示范工作的通知》（工信厅网安函〔2020〕190 号）进行评审核验，由工信部组织中国信息通信研究院、中国电子信息产业发展研究院、国家工业信息安全发展研究中心、工业和信息化部网络安全产业发展中心、中国工业互联网研究院等单位开展评审，并对符合要求的项目开展试点示范。试点示范期为 2 年。

工信部网络安全技术应用试点示范面向新型信息基础设施安全、网络安全公共服务、网络安全“高精尖”技术创新平台等重点方向开展，目的是挖掘新一代信息技术与网络安全技术融合创新的典型应用场景，提炼推广网络安全最佳实践和解决方案，促进网络安全教育、技术、产业融合发展，提升网络安全产业发展水平，强化新型信息基础设施安全保障能力。主要遴选具备创新性、先进性、实用性、可推广性的网络安全创新平台。

电力网络安全监测与指挥平台

“电力网络安全监测与指挥平台”由安天自主研发，通过协同各类数据源及安全人员，支撑平台高效发现内、外部威胁，协同动态防御体系进行威胁对抗，满足电力行业日常安全运营、重保、护网等多种典型场景需求。平台采用快速响应与定制方案结合的方式，指挥和协调单点安全设备及安全运维人员，有效实现对复杂威胁进行精准对抗与动态响应，全面提高电力行业网络整体防护水平。

智信零信任应用安全交付服务平台

“智信零信任应用安全交付服务平台”由安天移动安全自主研发。新冠疫情发生后，在全民抗疫的大环境下，多数企业都采取了远程办公的工作模式。安天移动安全依托自身的反病毒核心能力，以零信任安全架构为基础，构建“端—管—云”协同的服务平台，协助客户实现远程办公主机本地环境的安全加固与防护，构建零信任的虚拟安全边界、统一身份认证和动态的访问策略管控能力，增强内网安全监测管控与远程响应处置能力，解决政企机构构建移动化、数字化办公环境等的安全问题。

在开放的网络环境中，“智信”通过搭建虚拟安全边界，为政企机构筑起网络安全屏障，提供更加安全的访问环境，保障政企机构在享受移动办公高效便利的同时，有效保护终端、数据、业务和应用安全，并通过可视化呈现方式使网络安全可视、可控，为智慧城市、远程医疗和数字经济建设提供可靠安全保证。

智信零信任应用安全交付服务平台于今年 4 月 21 日，入选了工信部中小企业局发布的《中小企业数字化赋能服务产品及活动推荐目录（第一期）》网络和数据安全类产品首选推荐目录。

网络空间威胁情报大数据共享开放平台

“网络空间威胁情报大数据共享开放平台”，基于人机结合以及运用知识图谱等技术手段或方法，对海量碎片化的多源异构威胁情报数据进行细粒度的知识抽取，形成一体化的知识表达。对内支撑方面，安天基于该项目充分整合数据资源、情报资源、技术资源、能力资源以及威胁检测的成果积累，构建基于大数据平台和威胁知识图谱的威胁情报平台，同时也将平台能力向合作伙伴开放，共同构建运营平台。对外支撑方面，安天以可落地本地化的威胁情报系统，通过独立部署和集成于态势感知系统，为包括安全、能源、航空、军队等行业战略客户提供高质量的威胁情报服务支撑，有效达成威胁防护的客户价值。

2019 年，安天就有两项目成功入选试点示范名单，分别为：《网络安全态势感知和应急处置平台》和《民航网络与信息安全管理平台》；本年度有三项目再次入选，既是国家级部门给予的充分认可，也表明了安天在工业互联网安全、智慧城市安全、威胁情报领域的项目实践具有应用创新性、先进性、实用性及和可推广价值。未来安天将不忘初心，始终坚持网络安全关键技术突破、网络安全技术应用创新，为加快中国新型信息基础设施建设、网络安全公共服务发展贡献力量。

每周安全事件

类 型	内 容
中文标题	研究人员发现施耐德 PLC 中存在漏洞
英文标题	Claroty Details Vulnerabilities in Schneider PLCs
作者及单位	Dark Reading Staff
内容概述	研究人员发布了在施耐德电气可编程逻辑控制器 (plc) 中发现的身份验证和加密漏洞的新细节。如果利用这些漏洞，攻击者可在操作技术和关键基础架构系统上窃取数据，修改代码并执行命令。今年 6 月，研究人员私下向施耐德电气披露了 Modicon M221 plc 和 EcoStruxure Machine Expert Basic 的漏洞。根据一篇详细介绍调查结果的博客介绍，在所有情况下，攻击者都必须在 OT 网络上建立存在并监控设备之间的数据流，然后才能利用薄弱的加密实现来破解设备身份验证。
链接地址	https://www.darkreading.com/threat-intelligence/claroty-details-vulnerabilities-in-schneider-plcs/d/d-id/1339417

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 Office 即点即用特权提升漏洞（CVE-2020-16928）	高	Microsoft Office 中存在安全漏洞。Microsoft Office 即点即用 (C2R) AppVLP 处理特定文件的方式存在特权提升漏洞。成功利用此漏洞的攻击者可以获得特权提升。攻击者需要具备在系统上执行代码的能力。
	Microsoft Excel 远程代码执行漏洞（CVE-2020-16929）	高	Microsoft Excel 中存在安全漏洞。当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。
	Microsoft Office 远程代码执行漏洞（CVE-2020-16954）	高	Microsoft Office 中存在安全漏洞。当 Microsoft Office 软件无法正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。
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.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/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[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。

端到端加密通信可减轻企业安全风险并确保合规性

乔尔·沃伦斯特伦 / 文 安天技术公益翻译组 / 译

可以肯定，提供端到端加密（E2EE）的通信产品能够更好地保护数据。

但是，在考虑使用 E2EE 通信时，很多首席信息安全官（CISO）需要将合规性置于数据保护之前。在全球 1000 强公司中，大多数合规性安全团队能够访问其企业通信平台上的员工账户，以监督其活动，及时发现恶意攻击者。在受到严格监管的行业中，这种访问权限通常是必需的，但是 E2EE 被认为会阻断这种关键的访问权限。

不幸的是，大多数公司的安全和合规团队，都在使用未经批准的通信平台（如 WhatsApp）执行敏感业务，这违反了公司的安全策略。就在最近，摩根士丹利的高管因使用 WhatsApp 而被解雇。

员工已经知道，不只公司的 IT、合规性和安全团队能够访问其通信；Slack、微软、谷歌等服务提供商也能访问其数据和通信。这些服务提供商既保护用户，又监听用户。很多人不愿意在这样的系统上执行敏感业务，因此转向了消费级 E2EE 产品。

为何说消费级应用的普及对企业不利

在消费级产品上执行敏感业务是有风险的。这些消费级平台并非专门为安全和合规通信构建。它们优先考虑用户参与性和娱乐性，导致不断出现安全漏洞，例如中间人攻击和远程执行代码漏洞。多年来，WhatsApp 用户饱受这些安全漏洞的困扰。

CISO 只有两个选择：（1）对使用诸如 WhatsApp 之类消费级 E2EE 产品的员工睁一只眼闭一只眼；（2）制定例外策略，以期安抚监管机构（这样会更糟糕）。然而，这会放任员工长期使用不合格和不安全的消费级产品。

端到端加密比想象的更灵活

企业安全团队一直误认为 E2EE 是刻板僵化的。没有后门意味着，世界上最可靠的加密只有一种实现方法。而实际上，E2EE 非常灵活，可以在符合公司策略和行业法规的前提下进行部署。

CISO 无需在合规性和强大加密之间二选一。无论企业处于什么行业，都可以使用符合法规要求和内部策略，并与 IT 工作流集成的 E2EE。这意味着，企业使用 E2EE 可以保护数据免受攻击者、竞争对手和服务提供商的侵害，而且不用担心会违反法规。

选择支持 E2EE 的通信平台

在选择支持 E2EE 的通信平台时，安全专家需要评估供应商的声明、能力和动机。虽然某些主流平台宣传的是 E2EE，但它们仅加密从端点到服务器的流量，这称为客户端到服务器加密（C2S）。最典型的案例是，今年年初 Zoom 将其产品作为 E2EE 销售。

大多数理性的安全专家认为，Zoom 并非恶意欺骗最终用户，而是真的不了解加密的复杂性。该公司认为，尽管 C2S 架构容易受到中间人攻击，但其产品设置了“锁定”功能，绿色锁定符号能够使最终用户感觉安全。

不从事保护关键用户信息业务的提供商几乎都会声明，他们对加密的理解有限，提供的是“还不错的”解决方案而非严格的安全技术。

采用 E2EE 的 CISO 一定会受益。重要的是，要确保服务提供商有能力并致力于提供真正的 E2EE。

强大的 E2EE 解决方案包含三个重要支柱：

- 加密协议和第三方安全审查的结果都是公开的
- 其服务器不存储数据
- 服务提供商的业务模式不依赖于访问消费者数据

这就是说，CISO 的零信任安全策略可以扩展到服务提供商。如果企业的统一通信服务提供商可以访问、挖掘和分析其数据，那么他们就是潜在攻击面。我们知道，这种权限会导致未经授权的访问。强大的 E2EE 能够消除这种风险。

符合法规要求的 E2EE 是相对较新的产品。但是，对于 CISO 来说，权衡服务提供商访问企业数据的风险，以及在遵守公司合规性要求的同时控制其数据所带来的巨大收益，比以往任何时候都更加重要。

要想保护企业通信免受攻击，E2EE 是必需的。现在，企业可以在不违反法规的情况下实现 E2EE。如果企业前瞻性地部署 E2EE，就可以为员工提供所需和应有的安全性和隐私权，使员工不再依赖 WhatsApp、微信和 Telegram 等危险产品。

原文名称	End-to-end encrypted communication mitigates enterprise security risk and ensures compliance
作者简介	乔尔·沃伦斯特伦（Joel Wallenstrom）。乔尔·沃伦斯特伦是 Wickr 公司的首席执行官。
原文信息	2020 年 11 月 9 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/11/09/end-to-end-encrypted-communication-e2ee/
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。