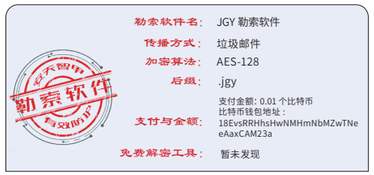
安天智甲有效防护 JGY 勒索软件



近日，安天 CERT 在梳理网络安全事件时发现了一个名为 JGY 的勒索软件。该勒索软件最早于 2020 年 12 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 JGY 勒索软件的加密行为。

JGY 勒索软件使用 .NET 框架开发，运行后首先将自身复制到启动目录以实现开机自启动，创建名为 "cuteRansomeware" 的互斥体保证单一实例运行，该勒索软件采用 AES-128 算法对桌面和用户文档目录下常见后缀的文本、文档、图片、数据库、源代码等文件进行加密，加密后的文件内容会被保存到原文件同目录下文件名为 7~13 位随机数、后缀名为 ".jgy" 的新文件，随后删除原文件。加密完成后弹出窗口展示勒索信，要求受害者向指定 BTC 地址支付 0.01 个比特币以解密文件。该勒索软件没有回传或记录密钥的功能，即使受害者按要求支付赎金也无法获得密钥解密文件，但因其没有删除卷影，受害者可尝试通过卷影恢复数据。

▲JGY 勒索软件勒索信

JGY 勒索软件采用“AES-128”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、动态（Win XP）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、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	fbbfb30d10babf67d1d6d86cc44af7e9bf2a10fe731d8fa1f1a1e4d4d17f71fe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	151 KB
MD5	68EAA965952BF2F1505C33E2B0EBB456
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/MSIL.Trumper
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=68EAA965952BF2F1505C33E2B0EBB456

◆常见行为

行为描述	危险等级
创建进程	★
使用 HTTP 协议的 URL	★
IPV4 地址	★
系统配置	★
同步机制	★
可执行文件	★
.....	.....

◆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、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆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 04 月 26 日 (总第 275 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

安天完成对国泰网信并购，拓展战略布局

4 月 12 日，安天与国泰网信签订协议进行深度合作，安天通过并购，获得国泰网信的控股权。安天科技集团又增加一支网络安全技术、产品、服务的有生力量。

安天以威胁检测防御能力为核心，有效应对安全威胁。在 20 年的创业发展中，从反病毒检测引擎和分析支撑体系起步，逐渐构筑了由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，可以为客户构建资产运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等基础安全能力。特别针对军工、军队、政企和关键信息基础设施行业等提供高等级的安全产品和服务，提升客户统一安全运维水平，通过大规模感知体系、快捷精准的威胁情报持续完成客户赋能。

国泰网信成立于 2015 年，聚焦于密码应用与工业安全的场景结合。产品包括密码机、密码卡、数字证书系统、密码检测平台、电力系统安全监测等，有较强的软硬件一体化产品研发能力。同时，国泰网信长期注重工业控制系统安全技术研发及安全产品研制，已形成完整的工控安全解决方案，对工业场景，特别是能源场景有着深刻的理解，为电力、能源等关键信息基础设施客户提供优秀产品和网络安全解决方案。

安天创始人、董事长肖新光表示，“安天人的使命是达成客户有效安全价值，致力于把底层能力转化为能够稳定、可靠、安全、高效运行于客户场景中的安全产品，国泰网信和安天走到一起，不只是一个加法式的合作，而是一个乘法式的变革，一个指数级的裂变。”

国泰网信总经理李欣表示，“相信国泰与安天的携手，将进一步完善国泰网信的技术与产品框架体系，赋能国泰网信产品的威胁检测与安全对抗能力，整合出平台级产品与安全能力。同时国泰网信优秀的行业纵深能力，能够为安天提供更丰富的用户需求与场景。确信此次合作能使双方获益，并为国家网络安全做出更大贡献”。

本次合作，是一场深耕工业用户场景的有效组合，是一次威胁对抗技术与密码可信应用的深度融合，也是一次底层能力和产品化运营管理的优势互补。同时，也为安天扩展工控、密码、产品运营等战略版图，未来双方将进一步整合发挥技术、市场优势，立体化协同，高效经营，开创业界技术、产品、市场融合创新的典范。（原文链接：https://mp.weixin.qq.com/s/7oiM7LLpCj80B1hmkwsSVQ）

扫描右侧二维码阅读全文

Xdef 论坛闭幕，安天完成 4 场演讲，1 个分论坛

2021 年 4 月 16 日 -17 日，第九届全国网络与信息安全防护峰会（XDef）在湖北武汉东西湖华美达酒店盛大召开。

本次峰会由国家计算机网络应急技术处理协调中心（CNCNERT/CC）、教育部高等学校网络空间安全专业教学指导委员会指导，空天信息安全与可信计算教育部重点实验室（武汉大学）主办，武汉大学国家网络安全学院承办。Xdef 此前已经成功举办了八届，致力于构建信息安全领域的“政产学研用”交流合作平台，促进国内网络空间安全力量的密切合作，以有效推动我国的网络空间安全防护工作。安天一直持续积极参与 Xdef 论坛，多次分享网络安全研究与最新安全技术发展。

本次峰会由专家报告、多方论坛、全国大学生信息安全类竞赛优秀作品展以及企业优秀安全产品展等多个环节组成。安天在本次峰会中，受邀在主论坛、分论坛分享特邀报告 4 场，承办了“高级威胁（APT）分析”论坛，并参与优秀安全产品展。

主论坛

▲ 安天科技集团董事长、首席技术架构师肖新光做主题演讲

肖新光：多域作战背景下的网空挑战

在主论坛上，公安部网络安全保卫局处长祝国邦做了题为《网络安全等级保护和关键信息基础设施安全保护制度政策解读》的主题演讲，360 集团副总裁、首席安全官杜跃进做了题为《数智时代安全的挑战与变革》的主题演讲，安天科技集团董事长、首席技术架构师肖新光做了题为《多域作战背景下的网空挑战》的主题演讲，浙江大学百人计划研究员周亚金做了《以太坊智能合约攻击分析和检测》的主题演讲。（原文链接：https://mp.weixin.qq.com/s/EinmvCz_qcaBevufPP1qcQ）

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	研究人员发现 HabitsRAT 的 Linux 版本变种
英文标题	HabitsRAT Used to Target Linux and Windows Servers
作者	Joakim Kennedy
内容概述	Intezer 研究人员曾在 Windows 版本 HabitsRAT 攻击 Microsoft Exchange 服务器时首次报道该恶意软件，研究人员近日发现了 HabitsRAT 更新的 Windows 版本和针对 Linux 环境的变种。HabitsRAT 使用 Go 语言编写，多数代码在 Windows 版本和 Linux 版本之间共享。该恶意软件允许攻击者远程控制受感染的计算机。为了恶意软件不被他人接管，攻击者执行的命令使用只有攻击者才能访问的私钥进行签名，恶意软件不会执行未经正确密钥签名的命令。在研究人员撰写这篇文章时，VirusTotal 上的所有防病毒引擎均未检测到 Linux 版本 HabitsRAT。
链接地址	https://www.intezer.com/blog/malware-analysis/habitsrat-used-to-target-linux-and-windows-servers/

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 Exchange Server 远程代码执行漏洞（CVE-2021-28481）	高	Microsoft Exchange Server 存在远程代码执行漏洞。由于 Microsoft Exchange Server 中的输入验证不严谨，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
	Visual Studio Code 远程执行代码漏洞 (CVE-2021-28477)	高	Visual Studio Code 存在远程代码执行漏洞。由于该应用在处理输入数据验证过程中不严谨，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
	Microsoft Internet Messaging API 远程代码执行漏洞（CVE-2021-27089）	高	Microsoft Internet Messaging API 存在远程代码执行漏洞。由于微软的 Internet Messaging API 代码在处理输入内容验证过程中不严谨，使得攻击者可以发送特制请求并在目标系统上执行任意代码。
较为活跃样本家族	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[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[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.Salgorea	中	此威胁是一种可以下载恶意代码的木马类家族。该家族样本运行后连接网络下载恶意代码并执行。
	Trojan/Win32.Yakes	中	此威胁是一种恶意木马家族。该家族木马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。该家族木马具有下载恶意程序、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[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.Hiddapp	中	此威胁是安卓平台上一种具有隐藏功能的木马类家族。该家族样本运行后，会隐藏图标，使用不同的方法向用户显示尽可能多的广告，包括安装新的隐藏广告软件。通过利用超级用户权限，该家族样本可以隐藏在系统文件夹中，清除难度较大。

战略性地实施零信任安全模型

托斯滕·斯塔布 / 文 安天技术公益翻译组 / 译

随着企业数字化转型的加速，其攻击面也在呈指数级增长。传统的基于边界的安全措施已不再奏效，企业是时候重新评估其安全措施并考虑采用零信任模型了。

但是，采用零信任模型面临诸多挑战。其中最大的挑战是复杂性，特别是企业需要仔细地进行规划。零信任模型需要互为补充的用户、设备、工作负载、数据和网络安全技术，所有这些必须共同运行，才能有效地抵御内外部网络威胁。虽说企业在某些方面可以快速获得成功，但是在部署零信任安全模型方面，并没有什么灵丹妙药或捷径。

美国国家安全局（NSA）发布了关于零信任安全模型重要性的最新政府和行业指南，详细分析了实施该模型的复杂性。通过该指南，企业领导者可以更全面地了解实施零信任模型的艰巨性和必要性。

该指南指出，实施零信任模型需要大量的时间和资源，其规模之大，远超企业领导人的预期。虽说实施零信任模型并不是一个简单或快速的过程，但可以通过以下措施逐步实现。

获得领导层的长期支持

在企业范围内实施零信任安全模型，需要周密的策略和大量的资源。实施零信任模型的第一要素是领导层的长期支持。零信任是一种模型，而非单一的技术或产品，因此企业首先要具备实施该模型所需的心态。与领导层进行关于部署零信任模型的对话是很困难的，但是很有必要。

需要注意，不要在零信任模型的实现时间或功能上给予过高的承诺。要让所有

利益相关者意识到，对于大多数企业而言，实施零信任模型都需要若干年的时间，无法一蹴而就。从首席执行官到员工的所有企业成员，都应时刻保持警惕，以实现在这方面投资的价值。正如 NSA 在其最新指南中所述：“即使将基本或中层的零信任功能集成到网络中，也必须进行后续操作，以使这些功能成熟起来，实现最大的价值。”

了解现有的 IT 基础架构和安全漏洞

实施整体性零信任策略的第一步，是确定现有的 IT 基础架构和网络安全控制措施中哪些与零信任模型兼容或可以轻松更新或替换。

没有人愿意从头开始，或向其已经存在的大量昂贵而复杂的网络安全解决方案中添加更多工具。在许多情况下，企业可以先采取一些简单的措施，例如网络微细分，这并不需要购买额外的硬件或软件。

许多企业可能已经准备好了必要的零信任构建基块（例如 MFA）。通过采用这些构建基块，重新安排其中一些基块并评估可以进行改进的地方，可以逐步实现具有成本效益的零信任模型。

如果企业需要在 IT 安全基础架构中添加新的零信任解决方案，可以寻找与最新的零信任标准（例如 NIST SP 800-207）兼容的解决方案。随着技术的快速变化，企业还应确保零信任架构是模块化且灵活的，以简化将来的升级，防止被捆绑在一家供应商身上。

从小处着手，然后进行扩展

正如 NSA 指南所述，不建议企业一次性地实现零信任模型。零信任之路是漫长的，需要仔细进行规划，并分阶段推广。大型企业预计将需要近 10 年的时间，才能真正实现全面的多层零信任安全模型。在开始零信任旅程之前，企业应获得领导层的支持，然后制定战略和阶段性的实施计划。

不要试图“一步到位”，不要一次性地进行太多更改。在扩展到其他领域（如零信任网络、设备、工作负载或数据）之前，应选择一个重点领域，例如零信任身份的实施。

企业应根据风险和当前漏洞情况，确定实施的优先级。然后，及时地将零信任安全模型全面应用于所有用户、设备、网络、应用程序、服务和数据。忽视这些领域中的任何一个，都会造成安全盲点和漏洞利用。

每周，我们都会看到有关大规模攻击事件的新闻报道。传统的基于边界的安全方法已无法保护我们的系统免受网络威胁。使用“设计安全”方法，正确实施多层零信任安全解决方案，可以最大程度地减少内外部攻击者可能造成的损害。

通过多级监控和情境化的多域行为分析，基于零信任的安全平台可以很好地与最高级的攻击者抗衡。那些尚未开始零信任之旅的企业，应认真考虑尽快将其作为头等大事了。

原文名称	Approaching zero trust security strategically
作者简介	托斯滕·斯塔布（Torsten Staab），是 Raytheon Intelligence & Space 首席工程研究员。
原文信息	2021 年 04 月 20 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/04/20/zero-trust-strategy/
摘 要	随着企业数字化转型的加速，其攻击面也在呈指数级增长。传统的基于边界的安全措施已不再奏效，企业是时候重新评估其安全措施并考虑采用零信任模型了。虽说实施零信任模型并不是一个简单或快速的过程，但可以通过以下措施逐步实现：（1）获得领导层的长期支持；（2）了解现有的 IT 基础架构和安全漏洞；（3）从小处着手，然后进行扩展。
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。