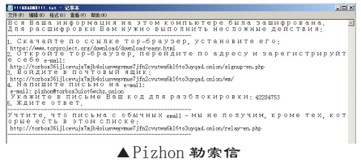
2020 年 11 月 2 日 (总第 252 期 试行)
邮箱：antiynews@antiy.cn

安天智甲有效防护 Pizhon 勒索软件

勒索软件名：Pizhon 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.pizhon-16 位随机字符串
支付与金额：需在指定网站注册邮箱账户与勒索者联系
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 Pizhon 的勒索软件。该勒索软件最早发现于 2020 年 10 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。该勒索软件运行后，将在短时间内完成对计算机文件的加密操作。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 Pizhon 勒索软件的加密行为。

Pizhon 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“.pizhon-十六位随机字符串”命名的后缀。加密完成后，该勒索软件在操作系统上的每个文件夹下创建一个名为“!!!README!!!.txt”的勒索信，该勒索信由俄文书写，具体内容包含了勒索说明、联系邮箱、解锁码、Tor 浏览器下载链接和邮箱注册链接，其中强调了联系勒索者时，邮箱账户必须使用由勒索信中提供的邮箱注册地址进行注册，然后将解锁码发送到联系邮箱，否则将收不到回复。



▲Pizhon 勒索信

Pizhon 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，安天追影威胁分析系统已经实现了对该类勒索软件的鉴定；安天智甲终端防御系统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、动态（Win7 x64）鉴定器、反病毒引擎鉴定器、字符串分析鉴定器、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、信标检测鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	pizhon.exe
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	2.28 MB
MD5	3FA08A11D59047A429DD90FCC15 A6A87
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[HEUR]/Win32.Ransom
判定依据	BD 静态分析

◆ 操作系统

操作系统	内置软件
Win7 x64 6.1.7601 Build 7601	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
堆喷射	★★★★★

◆常见行为

行为描述	危险等级
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
加载运行时 DLL	★
获取计算机名	★
检索系统内存信息	★
获取当前激活的窗口	★★
枚举进程	★
获取主机内存信息	★★
创建快捷方式	★

◆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 2 日 (总第 252 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天参与 2020 中国石油石化企业信息技术交流大会

10 月 21 日 -23 日， 2020 中国石油石化企业信息技术交流大会暨数字化转型、智能化发展高峰论坛在京召开。共有来自国家工信部、国资委、国家网信办等有关部委领导，中国科学院、中国工程院院士，中国石油、中国石化、中国海油、国家管网、国家能源、中国中化、中国航油、延长石油、油气资源调查中心等单位的主管领导、企业专家和技术人员，国际石油石化企业、油服单位信息技术负责人 1000 余人出席大会。

大会以“大力推进石油石化企业数字化智能化转型，助力业务高质量发展”为主题， 围绕新一代信息技术与石油石化行业融合创新的解决方案作了专题报告和交流研讨，并将各单位技术创新成果和应用经验进行了集中展示和分享。

在技术创新成果展上，安天展示了以智甲终端防御系统、探海威胁检测系统、追影威胁分析系统、捕风蜜罐系统、拓痕工具箱等安全产品，与安天态势感知解决方案为主的产品架构体系，并进行相关应用案例的分享。

安天安全研究员侯方勇在“网络安全论坛”上分享了《以威胁框架为参照系的产品能力演进》的主题演讲。

他表示，当前网络安全正在经历能力导向建设模式的变革，网络安全规划不断系统化和完善，态势感知管理平台等顶层能力被广泛构建，各种安全新技术、新理念、新产品也不断涌现。在这种安全建设热潮中，需要看到，如果安全产品本身无法满足威胁捕获、检测、防护、分析、处置的基础功能需求，尤其是无法实质达成有效的安全能力价值，就很难支撑起解决方案中的角色定义，从而使安全规划成为空中楼阁。因此安全产品对抗威胁能力的有效性提升与检验，是本质性和迫在眉睫的问题。

石油石化是大型关键政企机构，其安全稳定至关重要，需要安全产品具有切实可靠的对抗威胁能力、尤其是对抗高水平定向攻击能力。以威胁框架为指引和参照，系统、清晰地剖析安全产品能力体系的水平与不足，进而对相关工作形成具有明确能力导向的建设指导，促进产品安全能力提升的科学性、规划性、可检验性与可持续性，对于石油石化网络防御体系的构建具有重要价值。

面对日趋复杂的网空威胁，安天以阻断、迟滞和呈现威胁杀伤链为目标，构筑了高级威胁对抗时代的产品体系，并通过威胁框架为参照系，不断完善安全引擎、产品能力和分析支撑工作。

多年来，安天积极关注能源领域网络安全发展建设，产品与服务为石油石化企业安全运行提供了有效安全保障，为企业数字化智能化转型提供了有力支撑。

每周安全事件

类 型	内 容
中文标题	跨国能源公司 Enel Group 遭到勒索软件攻击
英文标题	Multinational energy company Enel Group has been hit by Netwalker ransomware operators that are asking a $14 million ransom.
作者及单位	Pierluigi Paganini
内容概述	意大利跨国能源公司 Enel Group 遭到 Netwalker 勒索软件攻击，这是该公司今年遭受的第二次勒索软件攻击。Netwalker 勒索软件操控者要求 Enel Group 支付 1400 万美元赎金来获取解密密钥，黑客声称已从公司窃取了 5TB 文件，并威胁说如果不支付赎金，则将其泄露。
链接地址	https://securityaffairs.co/wordpress/110067/malware/enel-group-netwalker-ransomware.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	Microsoft Outlook 远程代码执行漏洞（CVE-2020-16947）	高	Microsoft Outlook 中存在安全漏洞。当 Microsoft Outlook 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系统用户的上下文中运行任意代码。
	Microsoft SharePoint 远程代码执行漏洞（CVE-2020-16951）	高	Microsoft SharePoint 中存在安全漏洞。当软件无法检查应用程序包的源标记时，Microsoft SharePoint 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 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。
	Microsoft 图形组件远程代码执行漏洞（CVE-2020-16923）	高	Microsoft 图形组件在内存中处理对象的方式存在远程代码执行漏洞。成功利用该漏洞的攻击者会对目标系统执行任意代码。
较为活跃样本家族	Trojan[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	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/Win32.Diztakun	中	此威胁是一种使用 .NET 开发的木马类程序。该家族样本运行后会获取系统信息、用户信息和机密数据等，并将这些数据发送到远程服务器。
	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[Clicker]/Win32.Cycler	中	此威胁是一种带有点击行为的木马类程序。该家族侵入用户系统后，会像浏览器发送指定的命令，或通过修改系统文件，使用户系统访问特定的网络资源（通常为网站）。该家族能被用来增加网站的点击量，或者针对特定目标进行 DDoS 攻击。
	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。

保护在线学习环境的五种方法

托弗·特波 / 文 安天技术公益翻译组 / 译

新冠疫情出现之后，很多办公室和呼叫中心员工转向了远程办公。今年秋，大多数学生开始恢复上课。很明显，在可预见的将来，很多学校还会采用远程授课的方式进行教学。去年春，芝加哥的哥伦比亚学院、加利福尼亚大学，甚至加利福尼亚山景城高中等学校，遭受了诸如 Zoom Bombing（译者注：Zoom Bombing 是指有人闯入视频会议，显示色情或其他一些破坏性内容）和数据泄露等问题，导致网络教育安全受到质疑。

保护在线学习

疫情期间，从幼儿园到大学的教育机构都在努力开展网课，有几种方法可以确保教职员和学生的安全以及数据的安全。

●及时更新应用

确保数据和个人安全的最简单方法之一就是及时更新应用。大多数更新包括安全补丁，以防止不安全的代码被利用。在某些情况下，更新甚至包括新功能，以便实现更好的控制，防止今年春被利用的 Zoom 漏洞等。及时更新所有软件（包括操作系统），可以为所有已知漏洞打补丁，防止它们被攻击者利用。

虽说学校只能对自己拥有的设备进行更新，但是对于他们可以控制的任何系统，都应该制定地区范围的更新策略和规程。除此之外，学校还应向未成年学生及其父母进行培训，以确保其家庭网络上的所有软件和设备均能及时更新。

●控制访问

尽管已经有了许多访问控制功能，但是某些访问很容易被忽略。用于网络教育的任何应用程序都应包含 URL 过滤功能，以防止用户访问已知恶意网站或 IP 地址以及那些可能不适用于教育环境的网站。虽然学校或地区范围的解决方案能够满足大多数访问控制需求，但是教师可能需要调整其各自班级的要求，以便进行 URL 过滤。

●安全文件共享

无论是在小学、中学还是大学，参加网课的学生都需要采用一种安全的方法将文件提交给教师和同学。这意味着，学校需要制定数据保留策略，规定学生提交的文件在服务器上能够保留多长时间。此外，学校还应采取措施确保服务器上和传输中数据的安全。学生只能通过安全连接（例如，通过 HTTPS 或授权的 VPN）上传文件。上传后，应在服务器上对数据进行加密，以确保即使发生数据泄露，这些数据也不可用。

文件共享需要考虑最终用户。高中和大学生能够理解如何正确地遵循流程，但是小学生可能需要更易于使用的解决方案。不同年龄段或班级类型的学生可能需要定制的解决方案，以适应其需求。

●进行备份

除了提供足够的网络保护以防范漏洞和恶意软件外，备份也是确保数据安全的关键措施。根据 Verizon《2019 年数据泄露调查报告》，在 2019 年网络教育恶意软件感染中，勒索软件占 80%，而且 75%的被盗数据是个人数据。集成反恶意软件保护功能的备份解决方案可以防止大多数恶意软件攻击，包括针对备份系统的恶意软件攻击，并帮助用户在攻击后较短时间内恢复系统。

学校还需要考虑，一旦发生暴风雨，网络教育该如何运行。今年是有记录以来暴风雨最多的年份，飓风、龙卷风和洪水等会导致电力中断等破坏，关键系统可能会暂时关闭。但是，拥有备份数据可将停机时间降至最短，并在最短时间被恢复至正常运行，无需重新创建数据或处理数据丢失。尽管所有学校和学区系统都需要备份，但是学校还应该考虑一种用于还原班级备份的简单解决方案。

●备灾

在网络安全世界中，我们有句谚语：假设发生攻击。这并不是说，我们要对每个异常情况几近偏执，或整夜不眠地担忧漏掉了哪些问题可能会导致攻击者进入网络。而是说，我们要时刻准备着应对数据泄露，并制定计划，确定由谁来处理哪些方面的问题以及如何处理。对于任何企业来说，正确的事件响应和灾难恢复计划都是必不可少的。对教育机构而言，这一点更为重要。

适当的事件响应计划和灾难恢复计划，应明确说明由谁进行哪些响应以及如何进行响应。这包括地区、校园和教室级别的响应。该计划还应规定何时、如何传达信息以及不同的事件应提交给谁，以及恢复访问和服务的步骤。

很多学校会继续开展网课，现在是时候考虑采取措施来保护学校、学生和教职员工了。学校主要是为面对面的教学而设计的，所采取的大多数安全措施都集中在行政系统上。这是一个很好的开始，但是现在必须将这些措施进行扩展，使其不仅涵盖地区和校园网络保护，还要涵盖虚拟教室和个人保护。

原文名称	5 Ways to Protect Online Learning Environments
作者简介	托弗·特波（Topher Tebow）。托弗·特波是一位网络安全分析师。
原文信息	2020 年 10 月 19 日发布于 Security Boulevard 原文地址 https://securityboulevard.com/2020/10/5-ways-to-protect-online-learning-environments/
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。