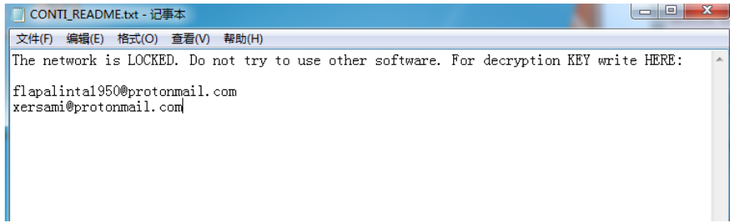
安天智甲有效防护“Conti 勒索软件”



▲Conti 勒索信

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Conti 勒索软件。该勒索软件最早发现于 2020 年 2 月，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 Conti 勒索软件的加密行为。

Conti 勒索软件运行后，调用 cmd.exe 实现如下行为：关闭 SQL Backups、SQLsafe Backup Service、SQLsafe Filter Service、Sophos AutoUpdate Service、Sophos Clean Service、Sophos Device Control Service 等服务；删除卷影副本；禁用修复；删除本地计算机的备份目录等。之后采用并发线程来对受感染计算机上的文件进行快速加密，在被加密文件原文件名后追加名为“CONTI”的后缀。Conti 在计算机桌面上创建名为“CONTI_README.txt”的勒索信，该勒索信内容包含勒索说明和联系邮箱等。

Conti 勒索软件采用 AES-256 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病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

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、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、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	eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	101 KB
MD5	B7B5E1253710D8927CBE07D52D2D2E10
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.AntiAV
判定依据	BD 静态分析

◆运行环境

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	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
删除全盘所有卷影副本	★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取驱动器类型	★
获取系统版本	★
枚举进程	★
访问文件尾部	★
文档篡改	★

◆扫描二维码查看完整报告

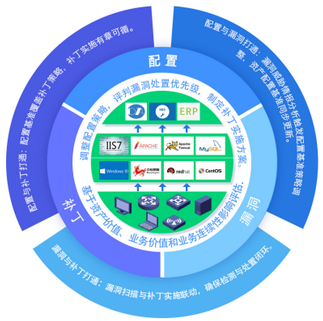
安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 8 月 24 日 (总第 244 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天资产安全运维平台获“2020 年优秀网络安全创新产品奖”

为贯彻落实习近平总书记关于网络安全工作“四个坚持”的重要指示，促进我国网络安全产业自主创新能力，推进产业结构化升级，为广大用户选择网络安全解决方案和网络安全产品提供参考依据，中国网络安全产业联盟（CCIA）组织开展了“2020 年优秀网络安全解决方案和网络安全创新产品评选活动”，并于近日公布了最终获奖名单。

安天资产安全运维平台顺利通过专家评审组和风评专家组初评、网安用户线上投票、现场答辩复评等环节，凭借自身优秀的设计理念、成熟的产品能力和技术创新能力，荣获 CCIA“2020 年优秀网络安全创新产品奖”。

安天资产安全运维平台是一个综合管理平台，面向规模化的信息资产管理场景，提供安全运维门户、资产管理、配置管理、漏洞与补丁管理、日志与告警管理、日常安全管理等功能，协助管理人员摸清资产底数，建立统一高效的补丁更新体系，形成能与资产与业务融合的整体安全策略调整机制，实现集约化、自动化、精细化的资产安全运维管理。



产品优势

平台基于资产价值、业务价值和业务连续性影响评估，调整配置策略，评判漏洞处置优先级、制定补丁实施方案。

平台通过主动及被动探测，避免空间上的盲区，从资产入网至资产退役全程监控，避免时间上的盲区，实现全生命周期的管理。

平台根据不同业务场景，充分考虑补丁的兼容性与可靠性验证等因素，有效保障业务连续性。

平台融合国内外多个安全配置基准，遵循 SCAP 规范，提供标准化的配置定义方式，实现配置基准的高效扩展，支撑安全加固的自动化。

平台通过资产价值、业务价值、业务连续性综合分析给出处置优先级，采用人机结合的方式进行修复，及时高效的完成漏洞处置工作。

应用场景

- **综合网空加固**

完善基础结构安全和纵深防御层面的基础安全能力，有效保障业务弹性。

- **态势感知协同**

支撑态势感知、威胁研判、攻击反制，形成实时化网络空间地形全方位防护。

扫码了解完整获奖名单和通知原文

加拿大军校数据被 DopplePaymer 勒索软件团伙泄露

最近，安全研究人员发现了一个泄密帖子，如下图所示，DopplePaymer 勒索软件团伙声称其入侵了加拿大皇家军事学院（RMC）。RMC 大约 1GB 的数据被泄露，泄露的数据包括向皇家军事学院捐赠的详细文件、采购设备和餐厅用品的发票、录取通知书和商业购买法律合同等。

https://cybleinc.com/2020/08/18/dopplepaymer-ransomware-operators-allegedly-struck-royal-military-college-of-canada/

新型 P2P 僵尸网络已感染全球五百万台 SSH 服务器

安全公司 Guardicore 实验室的研究人员发布消息，他们发现了一个之前从未被探查的僵尸网络，该网络使用异常先进的措施，秘密地将全球数百万台 SSH 服务器作为攻击目标。这个僵尸网络被 Guardicore 实验室命名为 FritzFrog。研究人员表示，Guardicore 实验室是在今年 1 月份首次发现这个僵尸网络的。从那以后，FritzFrog 已经锁定了政府机构、银行、电信公司和大学的数千万个 IP 地址。截至 8 月份，僵尸网络已经成功地感染了 500 台服务器，这些服务器服务于美国和欧洲的知名大学，以及一家铁路公司。FritzFrog 僵尸网络使用专有软件感染服务器，并将它们捕获到一个 P2 网络中，将其管理分散在许多受感染的节点上，而不是依赖控制服务器发送命令和接收窃取的数据。由于该网络没有指挥和控制 (CNC) 服务器，因此更难被发现，也更难关闭。

https://thehackernews.com/2020/08/p2p-botnet-malware.html

每周安全事件

类 型	内 容
中文标题	新型加密挖矿蠕虫可扫描和窃取 AWS 凭证
英文标题	TeamTNT placing its logo on the terminals of systems it infects.
作者及单位	Cado Security
内容概述	近日安全研究人员发现了疑似首个加密挖矿恶意软件，可以从受感染的服务器中窃取 AWS 凭证。这种新型数据窃取功能是 TeamTNT 网络犯罪组织使用的恶意软件。该组织至少从 4 月开始就已经开始活跃，根据报告，TeamTNT 的运作方式是在互联网上扫描那些被错误配置的 Docker 系统，并在没有密码的情况下将其管理 API 暴露在互联网上。该组织会访问 API，并在 Docker 安装内部署服务器，运行 DDoS 和加密挖矿恶意软件。
链接地址	https://www.zdnet.com/article/crypto-mining-worm-steal-aws-credentials/

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 NetLogon 安全漏洞（CVE-2020-1472）	高	当攻击者使用 Netlogon 远程协议 (MS-NRPC) 建立与域控制器连接的 Netlogon 安全通道时，存在特权提升漏洞。成功利用此漏洞的攻击者可以在网络中的设备上运行经特殊设计的应用程序。要利用此漏洞，未通过身份验证的攻击者需要将 MS-NRPC 连接到域控制器，以获取域管理员访问权限。
	Microsoft Windows 和 Windows Server 安全漏洞 (CVE-2020-1464)	高	当 Windows 不正确地验证文件签名时，存在欺诈漏洞。成功利用此漏洞的攻击者可以绕过安全功能，并加载不正确签名的文件。
	Microsoft Windows Media 安全漏洞 (CVE-2020-1339)	高	当 Windows Media 音频编解码器不正确地处理对象时，存在远程代码执行漏洞。成功利用该漏洞的攻击者可以控制受影响的系统。攻击者可能通过多种方式利用此漏洞，包括诱使用户打开经特殊设计的文档或诱使用户访问恶意网页。
较为活跃样本家族	Trojan[Downloader]/HTML.JScript	中	此威胁是一种可以下载恶意代码的木马程序。该家族样本一般为 html 格式，其中包含恶意 js 脚本，运行后可以下载其他恶意代码及推广应用并运行。
	Trojan[Dropper]/Win32.Agentb	中	此威胁是一种可以释放恶意代码到本地的木马类程序，其样本运行后生成恶意代码载荷文件并执行，可能会连接远程服务器下载其他恶意代码或回传系统敏感信息。
	Trojan/Win64.Sofacy	中	此威胁是一种木马类程序。该家族样本基于 64 位系统，网络间谍攻击组织 Sofacy 通过使用模块化恶意软件，将后门程序的一些功能放在不同的模块中，从而可以更好地在受攻击系统中隐藏自身的恶意行为。
	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	此威胁是一种 Linux 平台上的具有窃密行为的后门家族。该样本运行后会在 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[Dropper]/Android.Hqwar	中	此威胁是一种基于安卓系统的木马家族。该家族会在后台下载其他恶意程序到设备中。
	Trojan[SMS]/Android.Opfake	中	此威胁是一种基于 Android 的恶意应用程序。该家族没有统一的行为与功能，一般会窃取用户短信、发送包含恶意 URL 的短信或进行其他与短信有关的恶意操作。

四种方法缓解 Ripple20 导致的供应链安全风险

柯蒂斯·辛普森 / 文 安天技术公益翻译组 / 译

新冠疫情为企业带来了新的第三方安全风险。现在，许多公司开始使用外部服务提供商来管理基本运营或存储敏感信息。例如，企业依靠数据中心存储其数据；依靠 SaaS 平台处理企业管理和其他业务功能；依靠外部服务提供商处理支付流程等等。

疫情造成的经济损失，迫使许多第三方服务提供商停业、出售某些部门，甚至完全停止运营。这导致的结果是，他们维护流程和数据安全性的能力降低了。

与此同时，一款名为 Ripple20 的漏洞广泛传播，给企业和第三方服务提供商带来了更大的安全风险。至少 50 家制造商的设备中已经发现了该漏洞，其代码旨在将设备连接到企业网络和互联网。依赖于联网设备（为支持关键运营，这些设备的使用期限延长到 5 年或以上）的供应链，受到的影响最为严重。

企业必须意识到，第三方服务提供商带来的安全风险日益严重。他们必须迅速采取措施了解并解决这一问题。

第三方数据泄露的成本高昂

疫情期间，第三方服务提供商的风险涉及多个领域，其后果可能会很严重。离职或休假的员工可能会渗漏包含敏感客户信息（例如口令）的企业文档或电子邮件。为应聘新工作，员工经常会将企业文档发送到个人邮箱中。即使不是恶意的，这些行为也会在家庭网络和个人账户上留下敏感信息——攻击者很容易攻陷这些网络和账户并窃取信息。

被迫停业的服务提供商，可能不会继续采取防护措施来保护客户数据或将其安全删除。此外，即使企业终止了合同，第三方服务提供商使用的后门程序、账户和硬件可能也会继续存在。如果公司无法识别和监控这些后门程序，或者在合同终止后将其清除，那么这些后门很可能会被攻击者利用。

企业必须采取积极主动的方法来评估和应对这些威胁。四个方法供安全领导者借鉴：

1. 确定高风险供应商

企业应了解，哪些第三方服务提供商会对企业产生最大的影响或面临最大的风险，列出一个清单，然后优先对这些提供商进行安全验证。例如，如果第三方提供商在疫情之前就面临经济危机，或者可以访问企业的敏感数据或关键资产，则应将其视为高风险。通过该清单，企业可以将有限的精力用在刀刃上。

2. 尽快采取行动

在进行缓解风险的规划和预算时，企业可迅速采取一些措施。例如与服务提供商约定，如果提供商的员工离开公司或更改职位，提供商要如何以及何时通知企业；确定如何接收和处理这些通知；优化上述流程，以确保当员工离开公司时，企业能够立刻知情并删除其账户。

另外，对连接到企业网络、应用程序和服务的所有第三方，实施多因子身份鉴别。企业应监控身份鉴别服务，并将相应的日志提取到 SIEM 或类似解决方案中；查找用户首次尝试执行操作或访问资产的实例；监控多个地理位置访问的账户或以前未用于访问账户的设备。

最后，企业应通过访问管理解决方案和多因子身份鉴别来保护第三方（通过交互账户和服务账户）使用的权限。

3. 获得所有网络设备的可见性

诸如打印机、HVAC 控制器、制造设备或工业冰箱之类的联网设备，对于业务运营至关重要，而且通常由第三方引入或管理。这些设备难以跟踪或监控，因此很难确定设备何时受到攻击或被滥用。企业必须不断识别、记录和评估连接到其网络的每台设备是否存在漏洞。

新发现的 Ripple20 漏洞使此需求更加迫切。数百万受影响的数据中心、制造和其他第三方环境中使用的基本设备都受到了该漏洞的影响。有漏洞的代码已被厂商和制造商广泛部署，以至于许多公司可能不知道自己已被感染。因此，持续的可见性和风险评估成为当务之急。

4. 实施安全访问代理技术

第三方应实施安全和透明的远程访问，这对于减轻风险非常重要。企业应考虑使用 VPN 安全访问代理技术。（译者注：在本司翻译的《危害企业网络安全的五大常见问题》一文中，作者指出 VPN 为过时的技术。）

许多第三方服务提供商通过专用 VPN 连接到企业网络，或通过用户特定的 VPN 连接到高度扁平的网络。这意味着，只要获得对第三方环境和客户凭证的访问权限，就可以广泛访问该环境中的其他资产。

相比之下，远程用户与企业服务、应用程序和服务器之间存在访问代理。用户不必连接到企业网络，只需连接到代理，该代理通过安全通道代表用户与企业应用程序、服务和系统进行交互。该代理可以提供对所有远程访问的可见性，并且可以遏制任何可疑或恶意行为。

现在，企业应集中精力和资源制定短期和长期计划，以减轻第三方风险。如果攻击者利用第三方特权账户或设备进行攻击，企业需付出大量精力进行响应；与此相比，主动管理风险相关的成本、工作量和影响则小得多。通过战术和策略手段来评估和管理这些漏洞，企业可以大大减轻当前和长期存在的第三方风险。

原文名称	Four Ways to Mitigate Supply Chain Security Risks From Ripple20
作者简介	柯蒂斯 · 辛普森（Curtis Simpson）。柯蒂斯 · 辛普森是 Armis 公司的首席信息安全官。
原文信息	2020 年 8 月 18 日发布于 Dark Reading 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。