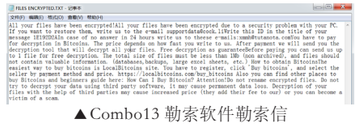
安天智甲有效防护 Combo13 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Combo13 的勒索软件。该勒索软件变种最早于 2021 年 4 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 Combo13 勒索软件的加密行为。

Combo13 勒索软件使用 .NET 框架开发，运行后会对 C:\Users 目录下“program files”、“program files (x86)”、“programdata”、“windows”以外的所有剩余目录中的除 exe、bat、com、sys、dll、avi、msi、bin、lnk、html 以外的所有类型文件进行加密，被加密的文件会被追加文件名后缀 ".id-1E192D2A.[xmmh@tutanota.com].combo13"。在加密完成后会向桌面位置释放两个文件：FILES ENCRYPTED.bat 与 FILES ENCRYPTED.TXT。前者用于勒索软件的自删除。后者为文本文档格式的勒索信，要求受害者向攻击者发送一封带有勒索软件 ID 的邮件并支付比特币以恢复文件，具体赎金及比特币钱包地址未说明。勒索信内容如下图所示：



▲Combo13 勒索软件勒索信

Combo13 勒索软件采用随机字符数据覆盖的方式覆盖文件原始数据，因此会造成文件数据的丢失。无论受害者是否缴纳赎金，攻击者都无法为受害者解密文件。但因该勒索软件没有删除卷影的行为，受害者可尝试通过卷影副本恢复数据。

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（WinXP）鉴定器、字符串分析鉴定器、文件相似分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（Win7sp1 x86）鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆概要信息

文件名	IS_room_start.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	8 KB
MD5	857E6E8A8D20B76066D72F432B7B1A71
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

报告地址：https://1.119.163.6/vue/details?hash=857E6E8A8D20B76066D72F432B7B1A71

◆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

◆危险行为

行为描述	危险等级
通过标记进程可执行堆绕过 DEP	★★★★★
疑似勒索软件篡改或加密文件	★★★★★
搜索文件	★★★★
修改文件后缀名	★★★★
在系统目录创建文件	★★★
映射内存方式注入	★★★
创建互斥量	★★★
查询软件限制策略	★★★
释放 PE 文件到临时文件夹	★★★

◆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 05 月 17 日（总第 278 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

安天连续发布两篇关于美燃油管道商遭勒索攻击事件的分析报告与建议

事件背景

2021 年 5 月 7 日，美国最大成品油管道运营商 Colonial Pipeline 遭到网络攻击，该起攻击导致美国东部沿海主要城市输送油气的管道系统被迫下线。安天及时跟进事件情况并发布《关于美燃油管道商遭勒索攻击关停事件的初步研判和建议》。当地时间，2021 年 5 月 10 日，美国联邦调查局确认 Darkside（黑暗面组织）勒索软件是造成 Colonial Pipeline 公司网络受损的原因。

研判分析

安天 CERT 认为，当前勒索攻击已经高度复杂，既有传统非定向勒索的大规模传播 -> 加密 -> 收取赎金 -> 解密模式，也有定向攻击 -> 数据窃取 -> 加密 -> 收取赎金解密 -> 不交赎金 -> 曝光数据模式的新型作业链条。

总体上，非定向勒索依然是按照“慢羊模式”传播的，难以击穿有相对扎实的基础防御能力和运营流程的信息体系；而定向勒索则有可能是极高水平的攻击团队发动的，更希望借助目标的价值达成巨额收益，因此可能投入更多的攻击资源，如 0day 漏洞和高级恶意代码，也包括可能获得内鬼的支持与配合。此外，以破坏为目的的攻击行动，同样可以伪装为定向勒索攻击行动，就像“伪必加”的勒索攻击一样。

安天 CERT 提出如下安全防护建议

1. 补丁和安全加固是最基础的安全必修课

多数勒索的攻击是依赖陈旧漏洞和系统配置缺陷得手的，这就使及时的补丁更新和安全加固能防御大多数攻击，特别是非定向攻击。在安全配置中，加固好关键配置点对于防御主流威胁是非常有效的。

尽管补丁工作非常重要，但在关键信息基础设施和工业生产等环境中，为了保证业务的连续性和可靠性，客观存在部分不能及时打补丁甚至不能打补丁的系统存在。而在大规模系统中，补丁的稳定性和兼容性验证、补丁的灰度策略、补丁的最优分发、海量端点和设备的合理安全配置管理等，依然是需要解决的问题。因此，需要建立完善的对资产漏洞、补丁与升级、安全配置加固等进行统一管理的安全机制和安全运行规范。包括建立资产漏洞库、补丁源、补丁可靠性验证、定制补丁升级预案、补丁灰度升级、留存审查机制和 STIG 标准的安全配置加固等安全措施，并按照安全运行规范规定的角色、职责、流程等严格执行，修好最基础的“安全必修课”，确保系统自身的安全性。

2. 从简单物理隔离到建立防御纵深

无论是类似“震网”这样的高水平定向攻击，还是类似台积电事件这样的勒索事件，都发生于传统认知中的物理隔离内网。在内外网或 IT 和 OT 间根据安全要求和对抗需求，将防火墙、网闸单向传输、入侵检测、深包检测还原与缓存等手段有机结合建立其安全屏障是必须的，同时要保障安全响应能力和安全维护能力通畅。在基础结构安全之上，依托网络纵深防线控制逃逸后的攻击路径，在其真正达成攻击目的之前通过态势感知与积极防御手段进行及时响应和快速处置。

3. 勒索威胁应对的重心是“有效防护”，而非事后处置

应对勒索软件，需要立足于有效防护，尽力使系统不被感染，数据不被加密。

勒索事件首先挑战的并不是应急处置能力，而是有效防护水平。勒索软件由于其对文件和扇区的加密以及删除操作，一旦发作，会造成数据损毁。数据恢复的方法只针对极少数的部分勒索软件有效，目前对多数主流的勒索软件是无效的。因此，不能把希望寄托在事后的解密与恢复上，必须打牢地基、扎紧篱笆，构建防御纵深，做好“防患于未然”工作。

对于类似威胁，仅仅依靠网络拦截是不够的，必须强化端点的最后一道防线，必须强调终端防御的有效回归。在终端侧应部署立足于有效防护的终端防御软件，如安天智甲终端防护系统，通过采用多维检测防护机制，构建“边界防护 + 主动防御 + 文档安全”的多维勒索防护架构，可有效防御勒索软件的勒索行为。

综合来看，在做好上述加强网络规划、做好补丁升级和配置加固、改善安全边界能力、建立防御纵深、增强安全运行维护能力、部署具有有效防护能力的终端安全防御软件并保持更新升级的情况下，一般性勒索软件的威胁是可以有效防护的。

4. 使用数据备份与灾难恢复应对勒索事件的事后处置

数据备份是信息系统安全的重要组成部分。备份的最佳做法是采取“3-2-1 规则”，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。根据数据的重要程度，建立合适的数据备份策略，定期进行数据备份。定期测试备份系统，保证数据备份成功，以便紧急情况下可以正常恢复数据，从而最大程度减少对业务的影响。建议采用“冷备份”方式备份重要数据。使用单独的文件服务器、移动硬盘等，备份完成后断开网络连接，实现物理隔离。如果使用了云服务器（ECS），一定要及时创建快照。在发生系统故障、错误操作或勒索攻击时，可以使用快照回滚云盘，快速恢复数据，保证业务正常运行。对重要的服务器设备采取冗余策略，即一台服务器遭受网络攻击失效后，另一台备份服务器可以迅速有效对接，确保核心业务不受影响。

（原文链接：https://mp.weixin.qq.com/s/bn59hNjv6c8yDXPvs8Uyag）

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	2019 年以来勒索软件团伙已泄露 2103 家公司的数据
英文标题	Ransomware gangs have leaked the stolen data of 2,100 companies so far
作者	Lawrence Abrams
内容概述	自 2019 年以来，勒索软件团伙已经在暗网数据泄露网站上泄露了 2103 家公司的被盗数据。一位暗网安全研究人员一直在跟踪 34 个勒索软件团伙的数据泄漏站点。在这 34 个团伙中，最活跃的 5 个团伙分别是 Conti（338 次泄漏）、Sodinokibi（222 次泄漏）、DoppelPaymer（200 次泄漏）、Avaddon（123 次泄漏）和 Pysa（103 次泄漏）。而某些勒索软件犯罪团伙已停止运营，例如 NetWalker、Sekhmet、Egregor、Maze、Team Snatch 等等。
链接地址	https://www.bleepingcomputer.com/news/security/ransomware-gangs-have-leaked-the-stolen-data-of-2-100-companies-so-far/

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 Edge 远程代码执行漏洞（CVE-2021-21197）	高	Microsoft Edge 存在远程代码执行漏洞。在 TabStrip 中处理不受信任的 HTML 内容时，由于边界错误而存在此漏洞。远程攻击者可以创建一个特制的网页，诱骗受害者打开它，触发基于堆的缓冲区溢出，并在目标系统上执行任意代码。
	Google Chrome 浏览器远程代码执行漏洞（CVE-2021-21199）	高	Google Chrome 存在浏览器远程代码执行漏洞。由于 Google Chrome 中的 Auray 组件存在 use-after-free 错误，使得攻击者可以诱骗受害者访问特制的网页，触发内存错误并在系统上执行任意代码。
	Microsoft Visual Studio 远程代码执行漏洞（CVE-2021-31213）	高	Microsoft Visual Studio 存在远程代码执行漏洞。由于 Visual Studio Code 远程容器扩展中的输入验证不正确，使得攻击者可以诱骗受害者打开特制文件并在目标系统上执行任意代码。
较为活跃样本家族	Worm/Win32.AutoRun	中	此威胁是一种蠕虫类程序。该家族能够在磁盘根目录或插入的可移动存储介质的根目录下创建一个 autorun.inf 文件并自我复制，该文件中包含可执行蠕虫的名字和路径。用户将磁盘或可移动存储介质接入电脑后，系统会自动执行 autorun.inf 中指定的可执行程序。该家族除了能够感染本地电脑外，还可以通过共享文件传播至远程电脑中。
	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan/Win32.Khalesi	中	此威胁是一种具有多种恶意功能的家族木马。该家族样本运行后，会窃取系统账户信息，记录键盘击键信息，下载其他恶意软件。该家族样本通过钓鱼邮件传播，通过添加计划任务持久驻留系统。
	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[Packed]/Win32.Upantix	中	此威胁是一种具有窃密行为的木马家族。该家族的样本通常以加壳的形式存在。该家族的样本在执行后会收集用户的数据，并通过网络回传给特定的服务器。
	Trojan[Backdoor]/Linux.Gafgyt	中	此威胁是一种 Linux 平台上的具有 DDoS 攻击功能的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作。
	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。

不考虑情境的威胁猎杀容易过时

鲍比·克里斯蒂安 / 文 安天技术公益翻译组 / 译

对任何行业来说，网络安全都是无可争议的焦点。但是，组织和企业应如何充分利用他们收集到的安全数据和信息，确保其业务免受网络威胁的侵害呢?

威胁猎杀的情境

普华永道（PwC）称，有 71% 的美国首席执行官（CEO）表示，他们“非常担心”网络威胁，其程度甚于当前的新冠疫情和其他健康危机。威胁猎杀是 IT 专家实施的新方法之一，用于在其网络上查找休眠或活动的威胁，以更好地了解和利用网络可见性，识别攻击者的入口点。但是，只有在广泛的安全情境下进行实践，该方法才能有效地发挥作用。

为此，企业需要实施更聪明的情报收集策略（相比于大多数组织当前部署的策略来说），该策略不仅要关注情报收集速度，还要关注威胁评估的准确性。

通过全面的数据可见性来了解网络环境，通过功能强大的关系型 MSSP 来利用多个平台，持续监控信息流和网络习惯，这些都与有效的威胁猎杀密不可分。如果没有这样的信息情境和外部合作伙伴，企业很容易忽视某些威胁，导致这些威胁无法得到解决，从而使黑客有足够的时间进行破坏。

企业对威胁猎杀的投资正在增加，但是要获得投资收益，可能还需要一段时间。威胁猎杀的主动性，使其成为保护网络的热门实践。从价值上来说，威胁猎杀的价值与在发现威胁的网络中收集的情境信息不相上下，而且需要更高明、更全面的威胁检测和识别方法。

现在，很多公司都想为其安全团队开展威胁猎杀培训，因此，实施威胁猎杀的明确部署和维护策略是当务之急。自动化、端点检测和响应、数据分析和威胁管理是大型现代化 SOC 的四个关键功能，旨在有效地在实施威胁猎杀。

自动化

仅依靠“人”无法及时响应数据所指示的内容，以及将 SOC 环境中生成的指数级数据进行情境化。自动化工具可以自定义，能够以多种方式减轻工作负载，解决简单任务以及更复杂的多步骤分析任务。智能自动化工具可以对“人”管理的威胁猎杀工作予以补充，从而增加另一层安全分析，否则该安全分析层很容易被忽略。

端点检测和响应（EDR）

在工作时间和非工作时间，安全团队都必须实时分析潜在的攻击行为。相对于攻击目标来说，攻击者可能来自不同的国家、时区、文化或表现出不同的个人习惯。

为威胁猎手和其他训练有素的安全分析师配备网络威胁情报和检测功能，安全团队就可以全天候地识别攻击活动，以迅速阻止攻击者。这样一来，安全团队就能进行明智的预测，而非总是摸瞎了。

数据分析

SOC 的安全边界在不断扩大，这可以从远程工作的显著（很可能是永久的）增加以及云迁移的受欢迎程度得到证明。如果不对来自多个日志记录区域的安全事件进行关联和交叉检查，则它们就无法满足任何实际的情境目的。

全面的网络可见性对于良好的威胁猎杀策略至关重要。SaaS、远程设备和其他安全环境都是可能被攻击的潜在弱点。要确定这些日志记录区域的活动，不仅需要训练有素的人员，还需要跨不同平台的有效软件管理。

威胁管理

将数据分析和自动化工具与分层 SOC 相结合，可以对潜在威胁的监控、管理和响应进行必要的隔离，同时保持每一层之间所需的通信以充分执行专门任务。由于现代化 SOC 的复杂性，在同一个安全环境中的数十个平台上，可能会发生无数个安全事件，因此需要跨网络委派职责，以避免混乱和拥塞。

将监控、管理和响应划分为三层，可以减轻负担过重的 IT 部门的工作量，使其不仅能够执行与 SOC 管理相关的任务，还能够开展威胁猎杀培训。

跟踪 IT 基础架构中的潜在漏洞是有很有必要的。但是，其有效性是通过“使用现有工具是否可以充分评估这些威胁”来衡量的。威胁猎杀将安全自动化、威胁检测和响应，以及关系型 MSSP 相结合，远比依赖于没有情境的一次性预测更有效。

强大的安全态势需要多管齐下的多层方法，这种方法可以通过良好的伙伴关系来实现，而这种伙伴关系可以有效地管理威胁，而且不会增加 IT 人员的负担。威胁猎杀本身并不是一种解决办法，但是企业可以对经验丰富的 IT 专家进行威胁猎杀培训，这样一来，企业不仅可以寻找网络中的异常行为，还可以以更有效、更主动、更全面的方式利用现有工具来缩小差距。

企业应采用一种促进及时性、数据关联性、自动化和分层威胁管理的方法，这样一来，企业就能为更好的威胁检测赋能，降低其总体风险。

原文名称	Why threat hunting is obsolete without context
作者简介	鲍比·克里斯蒂安（Bobby Christian），是 Deepwatch 公司的首席运营官兼首席技术官。
原文信息	2021 年 5 月 11 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/05/11/threat-hunting-context/
摘 要	对任何行业来说，网络安全都是无可争议的焦点。但是，组织和企业应如何充分利用他们收集到的安全数据和信息，确保其业务免受网络威胁的侵害呢？现在，很多公司都想为其安全团队开展威胁猎杀培训，因此，实施威胁猎杀的明确部署和维护策略是当务之急。自动化、端点检测和响应、数据分析和威胁管理是大型现代化 SOC 的四个关键功能，旨在有效地在实施威胁猎杀。
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。