Raccoon 窃密木马分析报告

近日，安天 CERT 在梳理网络安全事件时发现了一起利用鱼叉式网络钓鱼传播 Raccoon 窃密木马的活动。该活动主要针对小型企业、制造企业等。Raccoon 窃密木马是 2019 年 4 月公开售卖的远控木马，该木马主要通过钓鱼邮件进行传播，目的是窃取用户信息。

该木马通过鱼叉式网络钓鱼邮件进行传播，诱使用户执行附件中的 hta 文件，一旦执行便会添加注册表，创建计划任务连接网络下载有效载荷 Raccoon 窃密木马。该木马针对除俄语国家以外的国家进行攻击，主要功能包括键盘记录、收集主机信息、获取浏览器 Cookie 信息、邮箱登录信息、虚拟货币钱包密码、上传可能包含敏感信息的文本文件、获取屏幕截图等。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该窃密木马的鉴定；安天智甲已经实现了对该窃密木马的查杀。

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

最终依据 BD 静态分析鉴定器、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	c596d7f7dafb69fc7ae13646828924d2e0727ada126516b0cd1853ab0726ca18
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	573 KB
MD5	9C22ED2C1E95E3896E695038BE6E5A5B
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[PSW]/Win32.Racealer
判定依据	BD 静态分析

报告地址：https://1.119.163.6/vue/details?hash=9C22ED2C1E95E3896E695038BE6E5A5B

◆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、Office2003、Flash、WPS、FoxitReader、AdobeReader

◆信标信息

信标类型	信标内容	检测结果
url	http://110.43.90.34/updateserver/update?v=m2FJ4%2FfPHCuCimBztM9uuWaQ9hNzBKxcktQTl4BQLzuTLHndFBUcFYqHdjFJBrVUbNjaDZpcjl1wviBMWPHuYA==	未知
ip	128.121.146.235	未知
	120.92.59.191	未知
	31.13.67.33	未知
	110.43.67.232	未知
	110.43.90.34	未知
ip	128.121.243.228	未知
domain	update.wps.cn	安全
	kae.wpsdns.com	安全
	telete.in	安全
	notify.wps.cn	安全

◆危险行为

行为描述	危险等级
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
使用 HTTP 协议	★★
疑似桌面控制	★
加载运行时 DLL	★
使用 windows COM 库 API	★★
获得计算机用户名	★
获取系统版本	★
加载资源模块	★

◆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 06 月 14 日 (总第 282 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

模仿 Locky 的中文勒索软件分析

概述

近日，安天 CERT 发现了一个勒索语言为中文的勒索软件。该勒索软件采用 .net 语言编写，模仿 Locky 勒索软件，对加密的文件追加“.locky”后缀名。其最早出现于 2020 年 9 月，试图采用非对称加密 RSA、对称加密 AES 和 XOR 加密三种加密方式任意一种方式进行加密。由于其非对称加密 RSA 和对称加密 AES 部分功能未完善，安天 CERT 推测该样本可能为测试版本。本次分析的样本采用的加密策略是 XOR 加密，通过该方式加密的文件可以解密。

安天 CERT 在分析的过程中发现该勒索软件包含解密程序，在勒索窗口中存在一个按键“查询当前付款状态及解密”。当用户点击该按键时，该勒索软件获取比特币钱包地址，连接比特币官网查询当前该账户钱包余额是否大于等于 0.045BTC，若大于则进行相应的解密操作，同时发现目前有一个比特币钱包地址收到了 0.05BTC。

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该勒索软件的加密行为。

样本分析

病毒名称	Trojan/MSIL.locky
原始文件名	Leen.exe
MD5	B0E68A3352D31A9DD403A5ACAE6387A0
处理器架构	Intel 386 or later, and compatibles
文件大小	127.50 KB (130，560 字节)
文件格式	Win32 EXE
时间戳	2069-12-23 16:26:41（伪造）
数字签名	无
加壳类型	无
编译语言	.NET
VT 首次上传时间	2020-09-19 17:36:41
VT 检测结果	51/70

▲ 样本标签

（原文链接：https://mp.weixin.qq.com/s/vhqnXQajv6kQw05i-mGwMQ）

扫描右侧二维码阅读全文

鸿蒙 HarmonyOS 倾力打造纯净安全的应用生态 安天移动安全提供多项关键能力

作为新一代智能终端操作系统，HarmonyOS 自问世以来一直备受国人关注。刚刚发布上线的 HarmonyOS 2，将通过强有力的生态管控、严格的权限和访问控制策略解决用户终端的威胁问题，尤其是在移动互联网生态领域，HarmonyOS 致力于构建纯净安全的应用生态，从而为用户提供一个安全可靠、体验更好的应用使用环境。

安天移动安全基于十余年攻防实战经验和技术积累，在系统生态安全领域与华为进行了深度合作，提供了多项关键能力和技术。安天移动安全将应用检测和感知能力应用于 HarmonyOS，在 HarmonyOS 生态的应用分发和终端运行两个关键阶段对应用安全性进行识别，从安全管控和治理的角度解决未来 HarmonyOS 潜在的应用和用户终端威胁问题。

作为网络健康生态助推者和用户生态安全的守护者，安天移动安全始终以“守护移动智能时代安全”为己任，今后将一如既往配合政府监管，携手广大终端厂商，协同上下游促进移动安全生态持续向好，共筑纯净移动互联网健康生态。（原文链接：https://mp.weixin.qq.com/s/LsjlU7Ifb_r1hFxx867Glw）

扫描右侧二维码阅读全文

针对美燃油管道商遭勒索攻击关停事件总结

概述

2021 年 5 月 7 日（美国当地时间），美国最大成品油管道运营商 Colonial Pipeline 遭到网络攻击，此次攻击事件导致提供美国东部沿海主要城市 45% 燃料供应的输送油气管道系统被迫下线。安天 CERT 针对该事件进行持续关注和分析，分别在 5 月 10 日发布《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》[1] 和 5 月 11 日发布《关于美燃油管道商遭勒索攻击事件样本与跟进分析》[2] 两篇报告。安天 CERT 后续也在关注该事件始末，据彭博社报道，知情人士透露，Colonial Pipeline 公司于 5 月 7 日就已向 DarkSide 勒索软件组织支付了 440 万美元赎金。该组织在收到赎金后，为 Colonial Pipeline 公司提供了解密工具，用以恢复内部被加密的计算机系统。但是，解密工具恢复速度过慢，Colonial Pipeline 公司最后使用备份数据恢复了系统。5 月 10 日，Colonial Pipeline 公司在与美国能源部磋商后，开始将部分管道系统重新上线，并逐步分阶段恢复相关供应服务。17 日，该公司的汽油、柴油及航空燃油供应恢复到正常水平。

安天 CERT 预测，未来勒索软件依旧是网络安全主要威胁之一，继从最早的破坏数据开始，逐渐演变至加密数据和勒索赎金，再到窃取数据、加密数据和勒索赎金。未来可能会在窃取数据、加密数据和勒索赎金“双重勒索”的基础上，利用所窃取的数据信息对有意向者出售或敲诈勒索窃密数据中涉及到的相关人员，以此获得更多赎金，转而演变为“三重勒索”。（原文链接：https://mp.weixin.qq.com/s/I4u9KzcqTQgV0ambj6txeQ）

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	Windows 容器恶意软件针对 Kubernetes 集群
英文标题	Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments
作者	Daniel Prizmant
内容概述	2021 年 3 月，研究人员发现了第一个已知的针对 Windows 容器的恶意软件，并将恶意软件命名为 Siloscape，因为它的主要目标是容器逃逸，在 Windows 中这主要是由服务器 silo 实现的。Siloscape 是一种经过高度混淆的恶意软件，通过 Windows 容器针对 Kubernetes 集群。它的主要目的是打开一个后门进入配置不良的 Kubernetes 集群，以便运行恶意容器。
链接地址	https://unit42.paloaltonetworks.com/siloscape/

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 远程代码执行漏洞（CVE-2021-31175）	高	Microsoft Office 存在远程代码执行漏洞。由于 Microsoft Office 中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件并在目标系统上执行任意代码。
	OpenText Brava 远程代码执行漏洞（CVE-2021-31502）	高	OpenText Brava 存在远程代码执行漏洞。由于该应用在解析 PDF 文件时存在 use-after-free 错误，使得攻击者可以欺骗受害者打开特制文件并在系统上执行任意代码。
	Debian 平台的 Thunderbird 远程代码执行漏洞（CVE-2021-29967）	高	Debian 平台的 Thunderbird 存在远程代码执行漏洞。由于该应用在处理 HTML 内容时的存在边界错误，使得攻击者可以创建一个特制的网页，诱使受害者打开它，触发内存损坏并在目标系统上执行任意代码。
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[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/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.Hqwar	中	此威胁是安卓平台的一类木马家族。该家族样本伪装成知名游戏应用，运行后隐藏图标，诱导激活设备管理器，接收短信指令，上传通讯录和信箱等隐私信息，进行发送短信、回复短信、拨打电话、卸载指定 apk、联网下载 apk 并弹出诱导安装等操作。建议立即卸载，避免造成隐私泄露和资费损耗。

增强物理供应链的安全以降低网络风险

IFSEC Global / 文 安天技术公益翻译组 / 译

Genetec 公司的区域经理尼克·史密斯（Nick Smith）详细介绍了物理安全专家如何通过审查与其在供应链中合作的人员的网络安全策略，来提高他们对网络攻击的抵御能力。这些人员包括从组件供应商到安装人员和工程师的所有人。

对于各种规模的企业来说，网络攻击都是一项重大的业务风险。美国国家网络安全联盟（National Cyber Security Alliance）发现，超过 60% 的网络攻击针对的是中小型企业。其研究还表明，在遭受攻击的小公司中，有 60% 在六个月仍无法恢复业务运营。

然而，网络攻击并不总是直接针对企业的。企业通常依赖于第三方供应商和服务提供商，例如关键安全组件供应商或会计等服务的提供商。许多网络攻击是通过这些供应商进行的。

现在，多达 80% 的网络攻击始于供应链。即使是针对最小供应商的攻击，也会对大型企业的运营产生重大影响。因此，全球物理安全供应链中的每个企业，都必须更加了解这些问题，增强相互关联，以降低网络风险。一旦发生攻击，即使在最乐观的情况下，也会给企业带来巨额罚款和永远无法完全修复的声誉损失。

降低风险的基本措施

Genetec 公司最近的一份报告指出，67% 的物理安全专家，包括 Genetec 的最终用户、集成商和合作伙伴，计划在 2021 年将网络安全战略作为优先事项。自新冠疫情爆发以来，英国的网络犯罪增加了 31%。许多物理安全专家已经认识到，针对物理安全系统的网络攻击是真实存在的，这些系统是黑客的理想切入点。

IP 安全摄像头和其他安全设备本质上是连接到互联网的。这样一来，用户就可以远程访问这些设备，以查看其业务；而制造商无需上门就可以更新设备软件。但是，这一特点也带来了致命的弱点。如果不能正确保护安全摄像头或访问控制设备等物联网（IoT）设备，那么不仅是用户想与之共享访问权限的人能够远程访问它们，其他人也可以。

减少企业网络漏洞的一种方法是：仔细分析企业的供应链并建立可信供应商网络。有效的供应链风险管理（SCRM）对于确保企业业务的连续性和盈利能力至关重要。但是，为企业物理安全系统提供各种组件的供应商，甚至是那些安装或维修企业设备的供应商，也应采取相同的措施。

首先，企业应向供应商和其他第三方服务提供商询问其网络安全和隐私策略 / 实践。其次，企业应进行渗透测试，以捕获在产品开发过程中可能遗漏的任何漏洞。另外，当发现漏洞时，企业应积极主动、快速地部署最新固件和安全更新，以确保系统的安全。

此外，在与系统集成商合作开发或维护物理安全解决方案时，企业应从一开始就明确阐述其对网络安全的担忧点。系统集成商必须将网络安全视为重中之重，并且应只推荐来自可信制造商（这些制造商同样致力于定期保护企业的系统）的产品。

在最佳实践框架内运营

针对 IoT 设备的网络攻击对企业的影响越来越大，但是很容易阻止。举例来说，确保安全摄像头使用最新版本的固件并定期部署安全更新，就是保持良好网络安全的一项基本措施。不过，Genetec 公司的数据显示，在试图连接到其系统的安全摄像头中，有 68% 的固件已经过时。其中，54% 存在已知漏洞，这意味着它们很容易被恶意网络犯罪分子攻破。

这就是我们为什么说，每个人都要在保护物理安全系统免受网络攻击方面发挥作用。企业应选择那些使用智能策略（例如渗透测试）且值得信赖的供应商。此外，企业应只与致力于防御网络威胁的系统集成商合作。企业业务的成功可能就取决于这些措施。

原文名称	Hardening the Physical Security Supply Chain to Mitigate the Cyber-Risk
作者简介	IFSEC Global
原文信息	2021 年 6 月 9 日发布于 Dark Reading 原文地址 https://www.darkreading.com/physical-security/hardening-the-physical-security-supply-chain-to-mitigate-the-cyber-risk/a/d-id/1341251
摘 要	针对 IoT 设备的网络攻击对企业的影响越来越大，但是很容易阻止。举例来说，确保安全摄像头使用最新版本的固件并定期部署安全更新，就是保持良好网络安全的一项基本措施。企业应选择那些使用智能策略（例如渗透测试）且值得信赖的供应商。此外，企业应只与致力于防御网络威胁的系统集成商合作。企业业务的成功可能就取决于这些措施。
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。