安天发布《PwndLocker 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 PwndLocker 的勒索软件，PwndLocker 勒索软件最早于 2019 年 12 月被发现，主要通过钓鱼邮件和 RDP 暴力破解进行传播。PwndLocker 勒索软件家族主要目标为市政和企业网络，近期针对多个城市和组织发动攻击。

PwndLocker 勒索软件执行后，会跳过部分文件夹加密计算机上的文件，在原文件名后追加名为“.pwnd”的后缀，在计算机所有目录下创建名为“H0w_T0_Rec0very_Files.txt”的勒索信，勒索信中包含一个电子邮件地址和 Tor 付款站点，用于获取付款说明和赎金金额。PwndLocker 勒索软件运行后结束与备份应用程序和数据库服务器有关的进程，禁用与数据库有关的 Windows 服务和安全软件服务。PwndLocker 勒索软件使用“AES+RSA”加密算法加密文件，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本。由于 PwndLocker 勒索软件存在缺陷，被加密的文件存在恢复的可能。

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口令；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、动态（Win7 x86）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、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	16A29314E8563135B18668036A6F63C8
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	17 KB
MD5	16A29314E8563135B18668036A6F63C8
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Peed
判定依据	BD 静态分析
检测虚拟机	★★★★★

完整报告地址：https://1.119.163.6/vue/details?hash=16A29314E8563135B18668036A6F63C8

◆ 操作系统

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

◆ 常见行为

行为描述	危险等级
加载运行时 DLL	★
枚举进程	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
访问文件尾部	★
文档篡改	★
查找指定内核模块	★
创建快捷方式	★

◆ 衍生物分析

文件名	文件 MD5	家族相似性	yara 扫描
db9fc7bbeac79ff4_kernelbase.dll.mui	915bb24644df8672fc4a085e5be5b0ef	N/A	N/A

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 03 月 16 日（总第 222 期）试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼（系列五）——捕风蜜罐系统

捕风蜜罐系统是安天自主研发的诱骗攻击者的威胁捕获和威胁情报生产装置，通过创建服务器类型、物联网类型、工控类型等仿真设备组建与用户环境相似的蜜网环境，支持常规与国产化操作系统仿真包括 Windows、CentOS、Ubuntu 和 NeoKylin 等多种系统级高交互蜜罐，服务仿真支持 web 服务、数据库服务、特定漏洞等多种环境模拟，通过暴露蜜罐存在的漏洞及服务来诱使攻击者对其攻击，对捕获到的攻击进行进一步的分析与展示，分析后可产出威胁事件、攻击链等描述信息，威胁事件包括攻击来源、攻击方法、攻击目标等，攻击链标识了入侵、安装、控制、意图等各个阶段的行为，可协助现场运维人员清晰地发现威胁、定位威胁、溯源威胁。

蜜罐技术的先行探索者 L.Spizner 曾对蜜罐系统作出一个最经典的定义：“蜜罐是一种资源，他的价值在于被攻陷”。捕风蜜罐系统就是这样一套拥有模拟资产与服务等能力的安全资源，以请君入瓮的方式，让攻击者原形毕露。捕风蜜罐系统是一套被严密监控的计算资源，希望被探测、攻击，用于诱骗攻击者入侵但不能被入侵者控制。在实际工作场景中通过 IP 设置使蜜罐系统暴露在实际工作 PC 机或服务器旁，让攻击者真假难辨。除能够有效的拖延攻击者，保护真实的主机外，蜜罐也是情报收集系统，记录攻击者的攻击路线，了解攻击者所使用的工具与方法，从而发现攻击并产生告警。捕风蜜罐系统所捕获的威胁行为数据、文件、分析数据等均可通过标准接口提供给蜜网平台进行汇总展示、关联分析，为后续威胁分析、取证、溯源、猎杀等工作提供必要的基础。

捕风蜜罐系统可为政府、军队、能源、金融、交通等行业客户提供威胁发现能力，支撑客户的重大活动安全保障、高级威胁定位和安全事件响应。

功能简介

安天捕风蜜罐系统是一款部署在网络环境中，用于诱骗攻击者的积极防御型网络安全产品，有实体设备和虚拟化部署两种形态。可仿真多种设备及系统环境，包括 PC 和服务器系统、工控系统等。捕风蜜罐系统可及时感知攻击活动从而进行预防，能够捕获攻击者利用的攻击载荷并记录攻击的全过程，尤其适用于感知内网威胁，如勒索软件、蠕虫、攻击者入侵漫游等。捕风蜜罐系统的主要功能包括威胁行为感知、受害主机告警、攻击链还原与展示、失陷主机感知、威胁情报生产，具有高低交互结合、精准行为预警等优势。捕风蜜罐系统可作为态势感知系统整体方案中的采集节点，为其采集原始及检测后的流量、系统行为等数据，通过在多 VLAN 环境下创建暴露弱点服务的高低交互虚拟蜜罐，引诱攻击从而得到更多的攻击数据。态势感知系统根据蜜罐捕获的攻击数据可与其它节点采集的数据进行关联分析还原完整的攻击过程，从而进行溯源，达到定位攻击者与攻击方法的目的。

附：捕风蜜罐产品历史沿革

- 2005 年，安天 ArrectNET 监控网络应用蜜罐作为蠕虫样本捕获的重要来源，为产品开启了技术积累之路。
- 2009 年，安天将开源蜜罐程序移植至 ARM 平台。
- 2017 年，捕风蜜罐系统初版发布，并成功部署于某机构，为其内网威胁感知工作做出较大贡献。
- 2018 年，捕风蜜罐系统共发布两个版本，在仿真能力、威胁识别能力、分布式部署能力方面均有较大提升，且在某客户处部署，成功感知威胁，为威胁处置赢得更多时间。
- 2019 年，捕风蜜罐系统在内部虚拟网络模式、IoT 仿真、web 服务仿真、流量转发、威胁行为规范等方面均有较大提升，多次参与某安全演练活动并被多个用户采购。

以上内容为精简版
扫描二维码可阅读全文

以冠状病毒命名的恶意文件传播 Remcos RAT

Yoroi 研究人员发现一个名为“CoronaVirusSafetyMeasures_pdf”的文件，实际为“.exe”恶意可执行文件，其初始传播媒介未知，最终用于投送 Remcos RAT。该恶意文件建立了一个 TLS 保护的链接，连接到一个的文件共享平台，这可能是为了避免下一代防火墙发出警告。然后，下载受加密保护的恶意文件。恶意文件在系统目录上写入“.vbs”和“.exe”两个文件，VBScript 用于运行恶意可执行文件，并通过设置注册表项维持持久性。恶意软件将收集敏感信息发送到 C2，C2 地址由美国托管提供商托管。研究人员在恶意软件通信过程中，发现了“ | cmd | ”分隔符的用法，最终确认最终分发的恶意软件是 Remcos RAT。

（原文链接：https://yoroi.company/research/new-cyber-attack-campaign-leverages-the-covid-19-infodemic/）

每周安全事件

类 型	内 容
中文标题	安全厂商控制 Necurs 僵尸网络的美国基础设施
英文标题	New action to disrupt world’s largest online criminal network
作者及单位	Tom Burt - Corporate Vice President, Customer Security & Trust
内容概述	微软宣布已控制 Necurs 垃圾僵尸用于进行恶意活动的美国基础设施，该僵尸网络已感染了全球超过 900 万台计算机。Necurs 是目前最多产的僵尸网络之一，研究人员在为期 58 天的调查中，观察到一台感染了 Necurs 的计算机向超过 4060 万潜在受害者，发送了总计 380 万封垃圾邮件。Necurs 被认为是由俄罗斯的网络犯罪组织操控，也被广泛用于各种网络犯罪攻击，包括自动转储股票欺诈、伪造的垃圾邮件电子邮件和“俄罗斯约会”欺诈。Necurs 还被用来攻击网络上的其它计算机、窃取在线帐户的凭据以及窃取个人信息和机密数据。Necurs 幕后组织还将受感染计算机设备的访问权出售或出租给其他网络罪犯，作为僵尸网络出租服务的一部分。Necurs 还以分发针对财务的恶意软件和勒索软件、挖矿而闻名，甚至还具有尚未激活但随时可激活的 DDoS 功能。
链接地址	https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.lojaok.c[prv,fra,exp] 2020-03-06	高	该应用程序伪装其他应用，程序运行隐藏图标，联网下载大量应用图标，打开钓鱼界面诱骗用户输入帐号密码信息并联网上传，会造成用户隐私泄露和资费消耗，建议立即卸载。
		Trojan/Android.Funtasy.c[pay] 2020-03-07	低	该应用程序运行后弹出 wap 付费订阅信息，用户可能在不知情的情况下完成订阅，会造成用户资费损失，建议立即卸载。
		RiskWare/Android.netPanel.a[prv,rog] 2020-03-08	低	该应用程序是一个信息调查软件，会在后台获取位置信息和浏览器历史记录并上传，存在隐私泄露风险，请谨慎使用。
	较为活跃样本	Trojan/Android.Joker2.ah[prv,pay,exp]	中	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息。造成用户隐私泄露和经济损失，建议卸载。
		RiskWare/Android.Sexjiaoyou.a[rog,exp]	中	该应用程序是色情交友、直播类应用，诱导用户充值使用，可能影响用户身心健康，请注意提示信息，谨慎使用。
		Trojan/Android.SmsSpy.co[prv,exp]	低	该应用程序伪装为正常应用，运行拦截用户短信，并私自转发至指定号码，造成用户的隐私泄露和资费消耗，建议卸载。
		G-Ware/Android.Dwnbocai.b[fra,exp,rog]	低	该应用程序伪装正常应用，运行私自下载博彩程序，造成用户资费消耗并且可能给用户的财产带来较大风险，建议卸载。
		G-Ware/Android.HiddenAds.kr[exp,rog]	低	该应用程序运行后隐藏图标，会在后台加载广告，造成用户流量资费消耗，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft ChakraCore 和 Edge 内存破坏漏洞（CVE-2020-0710）	高	Microsoft Edge (EdgeHTML-based) 和 ChakraCore 中存在远程执行代码漏洞。攻击者可利用该漏洞在当前用户的上下文中执行任意代码，损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限，如果当前用户使用管理用户权限登录，那么攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	Trojan/Win32.Pincav	中	此威胁是一种木马类程序。该家族通过安全漏洞入侵电脑，它会修改用户系统的默认设置，随机破坏系统文件。该家族还会为黑客打开后门，让黑客完全控制用户电脑。该家族常与免费软件、共享软件捆绑在一起。它还会窃取在线游戏账号信息，如用户 ID、密码等。
		Trojan[Downloader]/Win32.Dapato	中	此威胁是一种具有自动下载行为的木马类程序。该家族感染用户系统后，系统会自动连接到指定的网站，在本地下载并执行多种恶意软件。
		Trojan/Win32.Rozena	中	此威胁是一种木马类程序。该家族能够通过邮件、可移动存储设备、捆绑安装、网站挂马等方式传播。家族运行后会影响被感染计算机的性能，使用户承担信息泄露的风险。
		RiskWare[WebToolbar]/Win32.Zango	低	此威胁是一种风险软件类程序。该家族样本运行后会访问恶意网站，下载免费软件和垃圾邮件等。该家族还会将浏览器主页重定向到恶意网站，并占用大量的系统资源。
		RiskWare[Downloader]/NSIS.Agent	低	此威胁是一种使用 NSIS 制作的风险软件类程序。NSIS 打包工具将该家族与正常程序打包在一起。该家族会劫持浏览器和搜索引擎、弹出广告、下载推广软件等。

企业需要了解的硬件供应链安全信息

丹尼尔·伍德 / 文 安天技术公益翻译组 / 译

通过建立流程和框架，可以确保不会让更多的高级攻击者对您的环境为所欲为。

在邓白氏公司（Dun&Bradstreet）2019 年的《合规与采购观点调查报告》中，受访者表示，网络安全是他们最关心的问题，但仍有 48% 的受访者并未将相关风险整合到第三方风险管理中。尽管开发和实施供应链安全计划可能会是一项艰巨的任务，但它与重视硬件安全却应该是公司任务清单上的第一项，可这些却往往被忽视。

信息安全计划通常专注于管理软件补丁和及时更新反恶意软件引擎和网络安全设备。 因此，即使硬件组件也容易受到高级攻击者和民族国家威胁行为体的攻击，但它们却常常被忽略。 在构建阶段或运输阶段，对物理组件的篡改会对所有物理产品构成威胁。有缺陷的部件会被召回，而当全球系统都依赖于这些部件，并且部件中包含敏感数据时，潜在攻击的规模将呈指数级增长。对固件的成功攻击会造成攻击者一直觊觎的漏洞，因为，与大多数基于软件的攻击不同，这些攻击造成的漏洞可以通过将设备重置为默认值来修复，而针对许多硬件的攻击所造成的漏洞却可以在固件刷新或重新安装操作系统后继续存在。

对硬件供应链的威胁不是理论上的，安全团队需要制定更强有力的策略来缓解供应链的威胁和风险。确保供应链安全需要在各个层面上进行，因为每个层面都有其自身的复杂性。第一步是要确保供应链成为组织威胁模型的一部分。至少，对供应链相关风险有很好的把握可能会扩宽组织机构可承担的业务风险范围。

以下十个最佳实践可帮助您设计出强有力的供应链安全计划。

1．对业务进行风险分析：风险被定义为系统损失成本乘以通过恶意行为造成损失的概率。此类风险分析可以帮助组织机构对事件进行分类并确定缓解的优先级。从供应链中清除硬件植入是一个昂贵的过程，而风险分析的主要目的是看看解决风险的代价与造成的损失哪个大。即如果风险造成的损失是 100 元，但是解决这个风险需要花 200 元，这样从成本的角度，就不值得修复。如果你是做小本生意的，从成本角度考虑，也许并“不一定”需要关注来自硬件的威胁。在实施任何安全措施之前，首先要确定团队的风险分析。

2．创建和维护第三方硬件提供商的清单：这应该是对组织策略已经确定的硬件和软件清单的扩展。

3．识别提供关键业务功能和服务的设备：关键设备可被定义为任何硬件，如果这些硬件或者相关安全服务出现故障，则会造成组织的整个业务停止运行。

4．在每个关键的提供商或设备上执行第三方风险评估：如有必要，一旦评估完成，请重新评估合同条款，包括您的服务提供商需要履行的安全附录和条款，还有要求定期提供一直遵守安全标准的证明。

5．与每个关键提供商建立沟通计划：这应该是双向的，并在出现可能增加风险的问题时通知每个组织机构。

6．为组织的硬件构建和维护软件依赖关系追踪系统：通过这一点，您可以确定服务器或设备是否容易受到软件组件中的安全漏洞的影响，并与供应商讨论如何及时修补。

7．为交付给您的组织机构的第三方硬件建立评估流程：这包括测试硬件的安全性，在实验室环境中建立流量基线，以及审查第三方供应商的安全性。

8．进行入口过滤和出口过滤：在任何连接网络的组件上执行此操作，以阻止意外请求进入或离开操作环境。

9．对实现关键基础设施的设备要求评估文档和评估证明：设备应该具有弹性，能够抵御网络、本地和物理攻击。为专门防止硬件植入，应测试防篡改控件，并应通过技术控件对针对设备的逆向工程加以限制。

10．将供应商的供应链理解为系统选择过程的一部分：供应商应该告知每个设备组件的来源，并提供有关组件从制造商到客户如何得到保护的概述。

虽然这些建议不能完全阻止关键任务硬件受到攻击，但它们是帮助您降低总体风险的基础。

来自硬件的攻击是实实在在的威胁，大多数组织威胁模型和风险缓解策略必须将供应链安全评估纳入其中。能为攻击者提供持久性访问是硬件攻击的显著特征，而且解决这些问题非常困难和具有挑战性，几乎不可能彻底解决。通过建立解决这些问题的流程和框架，可以确保不会让更多的高级攻击者对您的环境为所欲为。

原文名称	What Your Company Needs to Know About Hardware Supply Chain Security
作者简介	丹尼尔·伍德（Daniel Wood）。丹尼尔·伍德是 Bishop Fox 公司的咨询副总裁助理。
原文信息	2020 年 2 月 27 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/what-your-company-needs-to-know-about-hardware-supply-chain-security-/a/d-id/1337084
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。