安天智甲有效防护 Scarab 勒索软件新变种

勒索软件名：Scarab 勒索软件新变种
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.Bioawards
支付与金额：需通过邮箱与勒索者联系
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 Scarab 勒索软件新变种。该勒索软件隶属于 Scarab 勒索软件家族，最早于 2020 年 11 月被发现，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。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 Scarab 勒索软件新变种的加密行为。

该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，将被加密文件的文件名替换为随机的 14 个字符的字符串组合并追加以“.Bioawards”命名的后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“DECRYPT FILES.TXT”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱。为了诱导受害者尽快缴纳赎金，勒索信中强调了在加密的 96 小时后仍未付款，解密密钥将被自动删除。

▲勒索信

该勒索软件采用“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、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、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	Bioawards.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	250 KB
MD5	DB167BD026A292ACFBA3EBE1A598361A
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Scarab
判定依据	反病毒引擎

◆ 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
执行 HTML 应用程序	★★★★★
删除自身	★★★★
检测沙箱	★★★★★
检测虚拟机	★★★★★
获取剪切板内容	★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取驱动器类型	★
读取自身	★★
自我复制	★★
创建窗口	★
获取当前激活的窗口	★★
枚举进程	★
.....	.....

◆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 2020 年 12 月 21 日 (总第 259 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

FireEye 红队工具失窃事件跟进分析

火眼公司（FireEye）红队工具失窃事件曝光后，安天 CERT 迅速跟进，发布《FireEye 红队工具失窃事件分析和思考》，报告中以威胁框架视角对失窃的工具进行了功能点评，回顾了历史上多起网络军火失窃和扩散事件，并对本次事件做出谨慎地分析猜测。随着针对该事件的深入分析，安天 CERT 重新梳理了本次失窃工具对应的 ATT&CK 能力映射图谱，并对相应的能力进行评估与研判。

安天 CERT 利用 FireEye 的开源虚拟机测试套件 CommandoVM 线索与公开的规则对样本库进行扫描筛选，梳理了一些疑似 FireEye 的失窃工具并结合情报对工具进行初步分类：基于开源项目的工具、基于内置 Windows 二进制文件的工具（利用白文件实现免查杀功能的工具）、FireEye 红队自研工具以及目前未确认的部分工具。其中自研工具包括侦查工具、持久化工具、内存转储工具、恶意宏模板工具以及利用 D 语言、Golang、C# 等语言编写的后门程序。安天 CERT 对其中 FireEye 的部分自研工具进行了分析并评估可能产生的影响，同时针对部分相关规则使用了小规模白名单集合测试其误报率和规则质量。

目前，安天全线产品包含安天智甲终端防御系统（IEP）、安天探海威胁检测系统（PTD）、安天追影威胁分析系统（PTA）均能有效检出相关工具。安天威胁情报客户，亦可以通过安天威胁情报综合分析平台（ATID）查询相关工具的关联信息。安天 CERT 会持续跟进该事件最新情况与动态，持续公开针对泄露工具的分析与评估。

（本文为报告节选，完整报告请扫描下方二维码查看）

SolarWinds 旗下软件被用于供应链攻击事件分析

2020 年 12 月 13 日，美国网络安全公司 FireEye 发布分析报告称，SolarWinds 旗下的 Orion 基础设施管理平台的发布环境遭到黑客组织入侵，黑客对文件 SolarWinds.Orion.Core.BusinessLayer.dll 的源码进行篡改添加了后门代码，该文件具有合法数字签名会伴随软件更新下发。后门代码伪装成 Orion OIP 协议的流量进行通信，将其恶意行为融合到 SolarWinds 合法行为中。FireEye 称已在全球多个地区检测到攻击活动，包括北美、欧洲、亚洲和中东的一些政府、咨询、技术公司。SolarWinds 已在其官方网站发布安全公告 [2]，公布受影响版本为 2019.4 HF 5 - 2020.2.1，并提示用户升级至 2020.2.1 HF 1 版本。

由于重要信息系统都依赖一个庞大的 IT 供应链运行，因此供应链即威胁的入口，也是一个极为庞大的防御正面。而在供应链风险中，由于网管软件使用群体的是高权限的网络管理者，攻击者很乐于针对此类软件的开发者发起攻击，使之成为入侵其他高价值目标的跳板。

使用 SolarWinds Orion 软件的用户当前应尽快升级到 2020.2.1 HF1 版本。2020 年 12 月 15 日（星期二）另再升级到具备针对性安全加固功能的 2020.2.1 HF2 版本。当下处于受感染版本无法完成安全更新的应暂停使用该软件或以防火墙阻断该软件的外网访问，或将其策略配置在受限 IP 访问。

该事件被曝光后，安天第一时间升级了病毒库、威胁情报库、安全策略库，并对订阅安天高级威胁追溯服务客户发布了高级威胁专用追溯包。安天智甲终端防御系统可以在升级后检测到相关样本。

安天探海威胁监测系统可以对相关威胁的 C2 进行发现拦截。安天已经发布用于进行威胁排查处置的 AVL PK 特别版本。

如有客户发现相关威胁，可以拨打安天客户支持电话（400-840-9234），安天将提供工程师进行指导。

（本文为报告节选，完整报告请扫描下方二维码查看）

挪威邮轮公司 Hurtigruten 遭到勒索软件攻击

挪威邮轮公司 Hurtigruten 宣布，其全球数字基础设施遭到网络攻击。该公司在周日至周一通宵发现了该攻击，公司的系统感染了勒索软件。该公司的网站当前显示一条消息，“抱歉，该网站目前无法正常工作”。Hurtigruten 公司发现安全漏洞后立即通知了当地政府。目前尚不清楚攻击该公司的勒索软件。

（原文链接：https://securityaffairs.co/wordpress/112320/malware/cruise-company-hurtigruten-ransomware.html）

每周安全事件

类 型	内 容
中文标题	超过 300 万用户安装了 28 个恶意 Chrome 或 Edge 扩展
英文标题	Three million users installed 28 malicious Chrome or Edge extensions
作者及单位	Catalin Cimpanu
内容概述	安全公司 Avast 今天表示，据信超过 300 万的互联网用户安装了 15 个 Chrome 恶意扩展和 13 个 Edge 恶意扩展。Avast 发现的恶意代码功能有：将用户流量重定向到广告和钓鱼网站、收集个人数据（如出生日期、电子邮件地址和活动设备）、收集浏览历史以及下载更多的恶意软件到用户的设备上。Avast 表示，该公司上个月发现了这些扩展，并发现有证据表明，其中一些扩展至少从 2018 年 12 月开始一直处于活跃状态，当时一些用户首次报告被重定向到其他网站时出现了问题。
链接地址	https://www.zdnet.com/article/three-million-users-installed-28-malicious-chrome-or-edge-extensions/

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 Exchange Server 安全漏洞（CVE-2020-17132）	高	由于 Exchange 对 cmdlet 参数的验证不正确，会触发一个 Microsoft Exchange 服务器中的远程代码执行漏洞。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 安全漏洞（CVE-2020-17118）	高	SharePoint 中存在一个安全漏洞。经过身份验证的攻击者通过发送特制请求包，可在 SharePoint Web 应用中执行任意 .NET 代码。
	Microsoft Excel 安全漏洞（CVE-2020-17122）	高	Microsoft Excel 中存在安全漏洞。当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件将会执行远程代码漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。
较为活跃样本家族	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.Delf	中	此威胁是一种后门类木马家族。该家族是通过开发语言 Delphi 来命名的。该家族样本运行后，会在被感染的电脑中打开后门，黑客利用后门窃取用户的隐私信息。
	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.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/Win32.Cosmu	中	此威胁是一种下载类木马家族。该家族木马会从指定的服务器下载多种恶意软件和广告软件。该家族还会在系统后台定时访问指定的站点，以提高这些网站的访问量，为木马制作者获取利益。
	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[Dropper]/Android.Wroba	中	此威胁是安卓平台上的一种恶意代码释放类木马家族。该家族木马运行后激活设备管理器、隐藏图标。接收短信指令，根据指令拦截指定短信，伪造新版本通知释放恶意 apk 同时卸载正常程序，上传手机用户隐私信息至远程服务器地址。

2021 年安全预测：预算将减少

劳伦斯·皮特 / 文 安天技术公益翻译组 / 译

某些垂直行业将预算增长视为数字业务的成本。而对于其他行业（例如零售和金融业）而言，证明其对数据保护和监管重视程度的能力本身就是一项竞争优势，这反过来也会促使企业进一步增加投资。

2021 年预算将发生变化

新冠疫情爆发时，企业网络安全团队不得不迅速采取行动。仅仅几天之内，员工就开始在家办公了，安全团队则从管理受控的办公环境转向确保远程办公的安全性——为员工提供安全的远程连接，确保其能够高效地工作等。在远程办公的情况下，企业面临的威胁超出了其安全控制的范围，这些威胁隐藏在家庭 Wi-Fi 或员工使用个人计算机和平板电脑进行的下载中。此时，可见性对于防止威胁就至关重要了。

这导致的后果是，IT 安全团队不得不减少原计划于 2021 年开展项目的预算，将资金划拨给与疫情相关的业务和员工队伍。现在，企业正处于收紧预算以弥补业务损失，努力在 2021 年保持良好财务状况的阶段。

这些变化的最终结果是，企业在 2021 年的安全预算将会减少。预算增长不一定会降到零，但是相比于目前安全预算增长率超过 10% 的情况，来年的增长率可能会低至 6%。企业开展的任何项目都要快速获得回报。因此，安全团队必须采取不同的思路——寻求更有效的方法，利用现有基础架构以最低的投资来改善整体安全状况。

1. 更好地保护网络流量

远程办公改变了企业开展业务的方式。疫情出现之前，交易的至少一端由办公室中的某人在公司安全控制的保护下进行。

以续签保险为例：在 2019 年，你可以致电保险公司，与提供帮助的呼叫中心专家进行交谈。而如今，这些专家在家办公，其网络环境可能与家人或室友共享。我们如何确保进出其家庭 Wi-Fi 的流量是安全的，或者其室友未访问植入了恶意软件的风险网站呢？

远程办公不应影响企业的安全状况。但现在，安全团队需要在不断增加的攻击面上实现可见性、过滤告警并进行威胁预警。

2. 保护远程办公的员工

在考虑增强对远程员工的保护时，许多企业采用了一种“一刀切的”方法。他们面临的挑战是，要么安全措施不足（可能会导致数据泄露或丢失），要么安全措施过于严格，使员工难以顺利履职。

保护远程员工的第一步是确定其角色和需求，然后考虑各访问层级的不同安全需求。这样一来，企业就可以根据需要提供保护，而不必依赖同一种方法了。这种模式如何运行呢，大家可以参考以下示例。

- 对于某些用户，VPN 加以多因子身份鉴别或令牌身份鉴别，就足以对托管在虚拟桌面映像上的电子邮件或企业应用程序进行安全访问了。
- 使用敏感数据或下载文档的员工需要更高的访问权限，企业可为其提供受监管的 Wi-Fi。这样一来，这些员工就能够访问公司数据了（就像他们处在受监管的网络上一样），而且接收告警的安全团队也更具可见性。
- 一些员工（例如开发人员和 VIP 高管）需要完全受保护的网络访问权限。在这种情况下，他们需要安全的解决方案，例如家庭防火墙或 Wi-Fi 上的虚拟网络支持等。这类似于远程用户直接连接到公司网络，同时能够确保他们不会引起安全问题并能为安全团队提供最佳的可见性。

3. 安全的 DNS 服务

自今年年初以来，网络犯罪激增。常见的攻击（包括网络钓鱼、勒索软件和窃取个人数据的伪造网站等）不断增加。在家办公的员工有时会对其访问的网站放松警惕，例如在办公设备上打开个人电子邮件。因此，安全团队面临严峻的安全挑战。

一种简单的方法是使用安全的 DNS 服务。我们许多人依赖互联网服务提供商（ISP）或服务提供商提供的 DNS 服务。这种方法很不错，但是在如今的情况下却不理想。其网站可能会被劫持，简单的拼写错误也可能导致重定向到加载了恶意软件的伪造网站。

诸如 Quad9 这样的安全 DNS 服务很容易集成到任何环境中，并且可以作为公司 DHCP 服务的一部分自动传递到端点设备。安全的 DNS 服务使用多种威胁源来验证互联网地址，阻止和报告高风险站点，同时保护用户隐私。

用更明智的预算实现更好的安全性

上述解决方案提供了管理远程用户的安全方法。即使我们在 2021 年慢慢恢复到正常工作状态，这些投资仍将是有益的。

使用安全的 DNS 服务，可确保网络上流量的声誉，从而降低网络攻击风险，增强网络安全性。为远程办公的员工提供不同级别的安全保护措施，有助于根据员工需求提供保护，同时帮助安全团队增强可见性并在出现问题时简化支持。

2021 年，安全预算的减少将会带来挑战。但是，采用更明智的方法有助于减轻这些挑战。

原文名称	Security Predictions for the New Year: Budgets will Suffer in 2021
作者简介	劳伦斯 · 皮特（Laurence Pitt ）。劳伦斯 · 皮特是 Juniper Networks 的全球安全策略总监。。
原文信息	2020 年 12 月 07 日发布于 Security Week 原文地址 https://www.securityweek.com/security-predictions-new-year-budgets-will-suffer-2021
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。