安天智甲有效防护 BitRansomware 勒索软件新变种

近日，安天 CERT 在梳理网络安全事件时发现一个 BitRansomware 勒索软件新变种。该勒索软件隶属于 BitRansomware 勒索软件家族，最早于 2020 年 10 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 BitRansomware 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，并为被加密文件添加 ".ReadMe" 字样的文件名后缀。加密完成后，尝试在遍历到的文件夹中创建一个名为“Read_Me.txt”的勒索信，该勒索信具体内容包含了勒索说明、联系邮箱。该勒索信中提供了两种联系攻击者的方式，一种是通过发送邮件到攻击者指定的邮箱，另一种是访问攻击者指定的网站。

▲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、关联分析鉴定器、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、关联分析鉴定器、动态行为鉴定器、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	LolKek.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	122 KB
MD5	3B6717EC0BE808F5D41AC46EC0056ACA
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Wacatac
判定依据	反病毒引擎

◆ 操作系统

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
检测虚拟机	★★★★★
堆喷射	★★★★★

◆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	★
扫描磁盘类型	★★
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	★★
打开自身进程文件	★
枚举窗口	★
创建快捷方式	★

◆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 14 日 (总第 258 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 红队工具失窃事件分析和思考

FireEye 红队工具被窃事件概述

2020 年 12 月 8 日，火眼公司（FireEye）在其官方网站发布公告称，“高度复杂的威胁行动者”攻击了其内网并窃取了用于测试客户网络的红队（Red Team）工具。红队机制是一组经过组织和授权的安全专家，模仿潜在的攻击者并使用工具对企业进行攻击，以评估企业的检测和响应能力以及系统的安全状况。FireEye 以高级网络威胁防护服务为自身定位的美国企业，为其客户提供红队工具，实现可以模拟多个威胁行为体活动以进行安全测试评估。

FireEye 表示，此次事件是由具有一流攻击能力的国家发动的攻击。攻击者专门制定了针对 FireEye 的攻击手段，使用了一些之前从未见过的新技巧。攻击者在战术方面受过高度训练，执行时纪律严明且专注，并使用对抗安全工具和取证检查的方法执行隐蔽的攻击行动。被窃取的红队工具的范围从用于自动化侦察的简单脚本到类似于 CobaltStrike 和 Metasploit 等公开可用技术的整个框架。FireEye 声称泄漏工具不包含 0day 漏洞利用工具，被盗取的部分红队工具此前已发布给社区，或已经在其开源虚拟机测试套件 CommandoVM 中。

FireEye 声称，目前正在与联邦调查局和包括微软在内的其他主要合作伙伴积极展开调查，且尚未看到任何攻击者泄露或使用这些被盗取的红队工具。但为了防止潜在攻击者利用被窃取的红队工具进行网络攻击，已针对 Snort、Yara、ClamAV 和 OpenIOC 等公开可用技术在 GitHub 上发布了 300 多种对策，并发布了需要更新补丁的 CVE 列表。公布的红队工具检测规则中分为 60 个大类，304 个小类。从检测规则的名称上看，对应的红队工具除 1 个 macOS 系统后门工具和 2 个 Linux 木马外均应用于 Windows 系统。规则文件主要采用了 Snort、Yara、ClamAV 和 OpenIOC 四 种开源安全检测框架规则编写，其中包括 29 个 Snort 规则文件、164 个 Yara 规则文件、23 个 ClamAV 规则文件、88 个 OpenIOC 规则文件。

安天的事件响应和对抗特点

安天在第一时间启动了应急分析和响应，并依托 FireEye 所公布的线索在安天赛博超脑分析平台中进行了关联数据提取，结合 FireEye 公布的相关信息，针对安天产品客户发布了对应本次事件的“高级威胁追溯包”。

从安天长期跟踪相关事件所获得的经验来看，军火级网络工具公开后再被利用时，通常会经过了免杀改造或社工构造，因此以流失武器的 HASH 值作为威胁情报信标，其效果通常是极为有限的，甚至是完全无效的。而从本事件来看，尽管 FireEye 除 Hash 外，也提供了 Snort、Yara、ClamAV 和 OpenIOC 相关规则，但依托开源工具进行规则匹配，其在规模化客户场景下的部署成本和使用代价都是较高的，对使用者也有较高要求。

安天 AVL SDK 反病毒引擎是目前国内唯一的全平台、全规则恶意代码检测引擎。安天认为，反病毒引擎是最高效精准的威胁情报驱动器。其将威胁情报的价值，从“痛苦金字塔”的 HASH 等简单机读信标规则，提升到有较高抗变换能力的层面，实现更强的武器 / 工具 (Tools) 的定性和指向能力。安天为战略客户开放反病毒引擎的多种规则扩展接口，使之可以转化 Yara 等多种开源格式规则，以及进行二进制级别的规则扩展，从而有效地发挥安天反病毒引擎在脱壳、解包、虚拟执行等深度预处理能力。同时采用黑白双控模式实现孤立可疑对象，可以全面提升恶意代码免杀的构造难度。

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）均能有效检出相关流失军火。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。

（本文为报告节选，完整报告请扫描下方二维码查看）

D-Link 路由器面临被零日漏洞远程接管的风险

Digital Defense 发现的关键漏洞可以让攻击者获得 root 访问权限，并接管运行相同固件的设备。根据 Digital Defense 周二发布的报告，受影响的是运行固件版本 3.14 和 3.17 的 D-Link 路 由 器 型 号 DSR-150、DSR-250、DSR-500 和 DSR-1000AC VPN。这些攻击依赖于研究人员确定的三个连锁漏洞，即未经身份验证的远程 LAN / WAN 根命令注入漏洞，经过身份验证的根命令注入漏洞和经过身份验证的 crontab 注入漏洞（CVE-2020-25757，CVE-2020-25759，CVE-2020-25758）已通过 D-Link 确认。

（原文链接：https://threatpost.com/d-link-routers-zero-day-flaws/162064/）

每周安全事件

类 型	内 容
中文标题	星巴克移动平台中发现了远程代码执行漏洞
英文标题	Remote code execution vulnerability uncovered in Starbucks mobile platform
作者及单位	Charlie Osborne
内容概述	这家美国咖啡巨头在 HackerOne 上运营一个漏洞奖励平台。Kamil "ko2sec" Onur Ozkaleli 于 11 月 5 日提交了一份新的漏洞报告，并于 12 月 9 日公开，报告描述了新加坡用户使用的 mobile.starbucks.com.sg 平台上发现的 RCE 问题。根据该通报，ko2sec 在 mobile.starbucks.com.sg 上发现了一个用于处理图像文件的 .ashx 断点。但是，断点没有限制文件类型的上载，这意味着滥用此问题的攻击者可能会上传恶意文件并远程执行任意代码。
链接地址	https://www.zdnet.com/article/remote-code-execution-vulnerability-uncovered-in-starbucks-mobile-platform/

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	Mozilla Firefox MCallGetProperty 代码问题漏洞 (CVE-2020-26950)	高	Mozilla Firefox 存在安全漏洞，攻击者可利用该漏洞通过 Firefox 的 MCallGetProperty 强制使用释放的内存区域，以触发拒绝服务，并可能运行恶意代码。
	HEVC Video Extensions 远程代码执行漏洞（CVE-2020-17107）	高	HEVC Video Extensions 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。
	Cellinx NVT Web Server 访问控制错误漏洞（CVE-2020-28250）	高	Cellinx NVT Web Server 5.0.0.014b.test 2019-09-05 版本存在访问控制错误漏洞，该漏洞源于身份验证是在客户端进行，远程攻击者可利用该漏洞通过 SetFileContent.cgi 以 root 身份运行命令。
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[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	Trojan[Proxy]/Win32.Qukart	中	此威胁是一种可以窃取用户信息并通过代理服务器回传信息的木马类家族。该家族样本收集系统的敏感信息，通过 http 请求发送到指定网页。该家族在后台会自动更新。
	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/Win32.Blamon	中	此威胁是一种可以窃取密码信息的木马家族。该家族样本运行后会窃取用户账户信息，记录键盘击键等。
	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 年企业如何保护远程办公的员工

艾萨克·科恩 / 文 安天技术公益翻译组 / 译

在企业转型方面，2020 年是独特的一年。在全球新冠疫情的影响下，人们不得不改变生活、工作等方面的运作方式。对于大多数企业而言，这意味着迅速全面地转向远程办公。

超过半数的员工快速过渡到远程办公，而且很显然，这不仅仅是一种临时性的改变。普华永道在 6 月份进行了一项调查，结果显示，即使疫情消退，仍有 83％的员工希望每周至少在家办公一次，而 55％的员工则希望一直远程办公。

疫情导致企业的营收减少，因此企业希望削减成本开支，并设法挖掘潜能，提高收入。鉴于此，远程办公将在当前和将来的工作中发挥核心作用。

远程办公能够带来诸多好处，但也会带来独特的网络安全挑战。就目前来看，数据泄露和网络安全事件的成本和后果削弱了这种新工作模式的优势。

幸运的是，企业可以采取措施缓解潜在威胁，以最大程度地降低风险，充分利用远程办公的优势。

下面，我们将介绍远程办公的三种风险，并给出相关缓解措施，以帮助公司在 2021 年增强防御态势。

1. 内部人员威胁

即使在远程办公普及之前，企业就面临着意外和恶意的内部人员威胁，这些威胁会对企业的数据安全带来严重的风险。举例来说，员工是受信的团队成员，他们具备访问公司和客户数据的高级权限；如果不对这些访问进行检查，公司、客户和员工的隐私就有可能会遭到破坏。

远程办公会放大这些风险。疫情对就业市场产生了影响，恶意内部人员更有可能利用公司数据来获取新的就业机会或额外收入。此外，内部人员在远程工作时更容易出错，这也会带来安全风险。

例如，许多员工模糊了个人与专业技术之间的界限，他们共享或访问敏感数据，这会破坏数据的完整性。为了应对这种威胁，公司需要积极主动地创建和执行清晰的数据管理指南。

在这方面，沟通是关键。而通过监控计划或其他措施执行问责制将有助于在过渡期间保护数据。这样一来，首席技术官（CTO）和 IT 管理员可以防止下述威胁。

- 意外或恶意的数据共享或泄露
- 未经授权的数据访问或移动
- 设备管理以确保专业设备的使用
- 危险的数据使用实践。

恰当的安全软件可以就可疑行为发出实时告警，使领导者可以与员工进行沟通和协作，从而创建可以提高整体数据安全性的良好沟通周期。

2. 访问控制

大多数公司已经花费了数年时间来增强 IT 基础架构以抵御网络威胁。在远程办公的情况下，员工离开了公司网络的安全保护和问责制——IT 管理员需要为员工提供这种安全保护和问责制，无论他们身在何处。

许多员工使用不安全的 Wi-Fi 连接，这可能会威胁数据隐私。同时，攻击者很容易利用数十亿被窃取的登录凭证来获取关键 IT 基础架构的访问权限。

因此，领导者需要为远程团队配备适当的工具，以控制对其账户和网络的访问。这包括：

- 账户口令标准。员工需要使用独特的强口令，并定期更新。
- 数据安全服务。企业应对所有账户提供受信 VPN 服务和双因子身份鉴别服务。
- 威胁检测和通知服务。企业应为员工配备数字工具，帮助员工了解数据隐私最佳实践，并提醒他们潜在的威胁。

通过上述措施，企业可以减少与网络和账户访问相关的网络风险。

3. 利用新冠疫情进行的网络钓鱼攻击

疫情期间，攻击者反应迅速，利用人们的利他性、脆弱性、恐惧和好奇心，执行了大量的诈骗攻击。

例如，网络钓鱼诈骗（攻击者发送看似真实的消息，旨在捕获受害目标的登录凭证）的数量增加了 667％，全球执法机构已发布了此类诈骗的告警。

当员工感到压力大、孤立和不知所措时，更有可能落入此类陷阱。不幸的是，疫情期间，员工的压力大增，而且这种情况不太可能很快消失。

尽管自动化和网络安全软件可以帮助降低这种风险，但是公司还应该将精力和资源投入到培训计划中，对员工进行风险培训，并向他们推广保护数据的实用策略。

● 保护远程员工

转型从来不是件容易的事，而且不会完美无缺。远程办公已经成为企业混合型劳动力的重要组成部分，它将在未来数月甚至可能数年内占据主导地位。企业要确保这种工作模式会带来收益，而非障碍。

可以肯定的是，威胁形势在不断扩展。但是通过解决最普遍的数据安全威胁，企业可以显著降低远程办公这种“新常态”引起数据泄露或网络安全事件的可能性。

原文名称	How can companies secure a hybrid workforce in 2021?
作者简介	艾萨克 · 科恩（Isaac Kohen）。艾萨克 · 科恩是 Teramind 研发副总裁。
原文信息	2020 年 12 月 07 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/12/07/secure-hybrid-workforce-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。