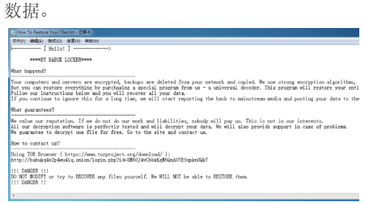
# 安天智甲有效防护 BabukLocker 勒索软件


近日，安天CERT在梳理网络安全事件时发现一个名为BabukLocker的勒索软件。该勒索软件最早于2020年12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BabukLocker勒索软件的加密行为。

BabukLocker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，在被加密文件的后缀名后追加以“.__NIST_K571__”命名的后缀。加密完成后，删除系统卷影副本，以防止恢复加密文件，并在加密文件所在的文件夹中创建一个名为“How To Restore Your Files.txt”的勒索信，该勒索信具体内容包含了勒索说明、暗网联系地址。为了迫使受害者尽快缴纳赎金，勒索信中威胁受害者如果长时间忽略此问题，其将向主流媒体和暗网中公布受害者数据。



▲BabukLocker 勒索信

BabukLocker勒索软件采用“AES+RSA”加密算法加密文件，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、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、动态（WinXP）鉴定器、动态（Win7 x64）鉴定器、信标检测鉴定器等鉴定分析。

最终依据静态特征检测鉴定器将文件判定为木马程序。

◆概要信息

| | |
|---|---|
| 文件名 | e10713a4a5f635767dcd54d609bed977 |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 31 KB |
| MD5 | E10713A4A5F635767DCD54D609BED977 |
| 病毒类型 | 木马程序 |
| 恶意判定 / 病毒名称 | Trojan/Win32.SGeneric |
| 判定依据 | 静态特征检测 |

◆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 |
|---|---|
| 删除全盘所有卷影副本 | ★★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 枚举进程 | ★ |
| 加载运行时 DLL | ★ |
| 获取驱动器类型 | ★ |
| 获取系统版本 | ★ |
| 获取系统信息（处理器版本、处理器类型等） | ★ |
| 扫描磁盘类型 | ★★ |
| 文档篡改 | ★★ |
| 枚举窗口 | ★ |
| 独占模式打开，防止复制读取，防止杀毒软件扫描上报 | ★ |

◆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01月11日(总第262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

# 安天获评 CNVD “漏洞报送突出贡献单位”

**CNVD是由CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识平台，是目前国内最权威的官方漏洞平台之一。**

2020年12月30日，由国家互联网应急中心（CNCERT/CC）主办的国家信息安全漏洞共享平台（CNVD）2020年度工作会议在线上成功召开。会议对2020年CNVD漏洞工作情况进行了全面总结，并对优秀单位进行了表彰。


安天多年来持续向CNVD报送漏洞信息，曾数次获CNVD嘉奖。多次获评“漏洞信息报送突出贡献单位”，是CNVD对安天参与建设CNVD安全漏洞的统一收集验证、信息发布和建立应急处置体系等工作的充分肯定。

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。在漏洞检测、威胁响应领域，安天拥有专业的研发团队和过硬的漏洞分析能力，重点监测可以被用于恶意代码传播、木马植入等相关漏洞的分布和被利用情况。

除了积极配合主管部门和向公众的漏洞上报、披露的工作，安天近年来不断建立健全漏洞发现、上报、分析和处置工作机制，还从产品、服务等方面提升漏洞安全风险防范及应对能力，推动构建漏洞发现和处置生态环境。

安天铸岳资产安全运维平台，通过网空资产探测、安全基线核查、漏洞识别与修复等功能，从资产、配置、漏洞、补丁等维度持续对资产安全情况进行动态评估，从而达到资产摸底、漏洞检测、漏洞通报、漏洞修复的全流程闭环。全面提升日常安全运维效率，有效收窄暴露面，完善基础结构安全和纵深防御层面的基础安全能力，对纵深防御和积极防御形成扎实的基础支撑。

另一方面，基于安天长期的载荷向量和知识图谱积累，通过构建AVML搜索引擎，安天推出威胁情报产品。在AVML搜索基础上，构筑了ATID威胁情报门户，为战略客户提供关联分析支持。

身为引领威胁检测与防御能力发展的网络安全国家队，安天将充分发挥自身技术优势，继续与行业主管部门保持密切协作和配合，及时发现安全漏洞，有力消除风险隐患。安天也将继续把习近平总书记关于“关口前移，防患于未然”的要求落到实处，为网络与信息安全保驾护航。

扫描上方二维码阅读原文

### 日产公司因Git服务器配置错误泄露源代码

日产北美公司因弱口令导致移动应用程序和内部工具源代码泄漏。从匿名来源获悉泄漏事件的工程师表示，泄露源于一个Git服务器使用了默认用户名和密码组合admin/admin，工程师通过分析日产数据，发现泄露的Git存储库包含源代码有日产NA Mobile应用程序、部分日产ASIST诊断工具、经销商业务系统 / 经销商门户、日产内部核心移动代码库、日产 / 英菲尼迪NCAR/ICAR服务、客户获取与保留工具、销售 / 市场研究工具+数据、各种营销工具、车辆物流门户、车辆联网服务 / 日产联网以及其他各种后端和内部工具。泄露数据本周一开始在Telegram和黑客论坛上传播后，该Git服务器已在周二下线。目前，日产发言人证实了这一事件，并表示正在进行调查。

（原文链接：https://www.zdnet.com/article/nissan-source-code-leaked-online-after-git-repo-misconfiguration/）

### 谷歌发布Android补丁更新共解决43个安全漏洞

谷歌在本周一发布了Android补丁更新，共解决了43个漏洞，这是本月Android安全公告的一部分。修复的严重漏洞包括Android系统组件中的远程执行代码漏洞CVE-2021-0316，Android Framework组件中的拒绝服务漏洞CVE-2021-0313。此外，还包括其框架中的13个漏洞、Media Framework中的3个漏洞、第三方组件中的3个漏洞、MediaTek组件中的1个漏洞、高通组件中的15个漏洞等。

（原文链接：https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/）

## 每周安全事件

| 类 型 | 内 容 |
|---|---|
| 中文标题 | 黑客组织 Thallium 针对股票投资者进行供应链攻击 |
| 英文标题 | North Korean software supply chain attack targets stock investors |
| 作者及单位 | Ax Sharma |
| 内容概述 | ESTsecurity 研究人员发现黑客组织 Thallium 通过更改私人股票投资通讯程序来进行供应链攻击。被注入特定命令的合法安装程序使用 Nullsoft 脚本安装系统（NSIS）重新打包，特定命令从恶意的 FTP 服务器上获取 XSL 脚本，并在 Windows 系统上通过内置的 wmic.exe 实用程序执行该脚本。然后，执行下一阶段的 VBScript，以在 %ProgramData% 目录下创建文件和文件名，并连接 C2 服务器，以接收其它命令。攻击者会对受感染的系统进行侦查并筛选受害者，部署 RAT 以进一步进行其它活动。 |
| 链接地址 | https://www.bleepingcomputer.com/news/security/north-korean-software-supply-chain-attack-targets-stock-investors/ |

## 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 | IBM Loopback 安全漏洞（CVE-2020-4988） | 高 | Loopback 8.0.0 版本存在安全漏洞，该漏洞允许攻击者操纵或污染 Javascript 值，并导致拒绝服务或执行代码。 |
| | Microsoft Azure Sphere 注入漏洞（CVE-2020-35608） | 高 | Microsoft Azure Sphere 20.07 版本存在安全漏洞，该漏洞源于常规签名代码执行功能允许任意代码执行。攻击者可利用该漏洞可以执行使用 PACKET_MMAP 触发此漏洞的 shellcode。 |
| | Apple macOS 缓冲区溢出漏洞（CVE-2020-27952） | 高 | Apple macOS 存在缓冲区溢出漏洞。该漏洞源于 FontParser 的一个未知函数。攻击者可利用漏洞导致任意代码执行。 |
| 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.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]/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[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。 |



# CISO 在 2021 年的六项重点工作

埃瑞卡·奇科夫斯基 / 文 安天技术公益翻译组 / 译

2021 年，富有远见的网络安全领导人将重点关注下述六项工作。

### 保护技术供应链

去年 12 月的 SolarWinds 攻击事件，是技术和软件供应链安全问题的典型案例。在过去的一年中，此类攻击日益严重。毫无疑问，SolarWinds 攻击是最严重的供应链攻击事件之一。但从造成的风险上来说，还有很多攻击能够与之媲美——最新报告显示，下一代供应链攻击飙升了 430%。我们以 2020 年爆发的 Ripple20 漏洞为例：Ripple20 是 TCP/IP 软件库中的一系列漏洞，对企业和工业环境中的数十个物联网（IoT）供应商造成了影响，安全行业的专家称该漏洞将在很长一段时间内影响企业的网络安全。这些事件说明供应链存在严重的安全问题，企业的首席信息安全官（CISO）应通过更好的软件组件跟踪、资产管理和漏洞管理实践来解决这些问题。

### 超越虚拟专用网络（VPN）

2020 年，全球企业迅速转向远程办公。这种趋势暴露了当今企业远程访问的诸多安全漏洞。对于很多企业而言，长久以来 VPN 的局限性阻碍了他们随时启动远程办公，同时又保持控制（控制员工的远程访问方式以及访问哪些资源）的能力。疫情期间，在确保远程办公的安全上，很多 CISO 举步维艰。2021 年，很多 CISO 将寻求部署更长久、更安全的远程访问解决方案。

### 将设计安全放在首位

2021 年，CISO 会更加重视软件和流程的设计安全。设计安全意味着减少内外部用户的安全冲突，并为其创建干扰性较低的安全控制和检查点；还意味着提高 IT 部门内部安全工具的可用性，以及将安全基础知识纳入开发要求中。美国银行和纳斯达克等领先组织正在采用设计安全方法实施数字化转型。信息安全论坛（ISF）等专业组织则表示，必须将设计安全纳入员工安全培训中，以帮助他们在数字和物理世界中做出更安全的选择。

### 通过自助服务安全实现更好的应用安全

毫无疑问，在 2021 年，很多 CISO 会更加重视应用安全。根据 2020 年的一项研究，有 10% 的企业承认其 Web 应用程序防火墙（WAF）——可能是某些企业应用安全的主力——却无法阻挡高达 90% 的攻击。很多企业已经开始实施 DevSecOps 实践，以帮助其开发人员和 DevOps 团队重新构建更安全的软件。获得成功的企业发现，帮助他们获得成功的一个重要因素是：使用自助服务安全性和合规性验证，通过诸如“安全即代码”等方法集成安全性，以向开发团队交付安全功能和要求。最近的一项研究显示，具有完整的安全集成和自助服务功能的 DevOps 团队，在一天之内修复关键漏洞的可能性超过 80%。

### 部署“基于域的消息认证、报告和一致性”（DMARC）协议

疫情期间，企业电子邮件泄密（BEC）和网络钓鱼攻击飙升，很多 CISO 开始考虑部署 DMARC 协议。长期以来，安全专家一直建议企业使用 DMARC 协议，以减少攻击者伪造企业域名、欺骗企业客户和员工（使他们认为收到了公司的邮件）的可能性。不幸的是，虽然使用 DMARC 协议的企业迅速增加，但这些企业仍然是少数。在大多数行业中，只有不到 10% 的企业使用该协议；而在全球 500 强公司中，仍有 85% 的企业未使用该协议。

### 降低勒索软件风险

年复一年，勒索软件风险不断加剧，变得更加可怕。2020 年，针对德国一家医院的勒索软件攻击导致医院瘫痪，一名病危患者不得不被转到其他医院，最终因延误治疗而身亡。随着勒索软件压力的加剧，很多企业开始采取多管齐下的方法，将更好的检测、更好的保险、主动威胁猎杀以及回归基础措施（改善灾难恢复、备份流程以及基础架构）等方法相结合，来降低勒索软件风险。

| 原文名称 | CISO New Year's Resolutions for 2021 |
|---|---|
| 作者简介 | 埃瑞卡·奇科夫斯基（Ericka Chickowski）。埃瑞卡·奇科夫斯基是 Dark Reading 的撰稿人。 |
| 原文信息 | 2020 年 01 月 04 日发布于 Dark Reading<br>原文地址 https://www.darkreading.com/vulnerabilities---threats/ciso-new-years-resolutions-for-2021/d/d-id/1339815 |
| 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。<br>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。 |