安天智甲有效防护 Bagli 勒索软件

近日，安天 CERT 在梳理网络安全事件时发现了一个名为 Bagli 的勒索软件。该勒索软件变种最早于 2021 年 3 月被发现，主要通过垃圾邮件进行传播。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 Bagli 勒索软件的加密行为。

Bagli 勒索软件使用 .NET 框架开发，运行后创建名为 "ExcellToPdf" 的互斥体保证单实例运行，遍历 C:\Users\%UserName%\ 目录下的 "Desktop"，"Links"，"Contacts"，"Desktop"，"Documents"，"Downloads"，"Pictures"，"Music"，"OneDrive"，"SavedGames"，"Favorites"，"Searches"，"Videos" 文件夹，对常见后缀名的文本、文档、压缩包、图片、音视频等文件进行加密，采用的加密策略为使用随机数覆盖文件的前 0x10C350 字节数据，并追加文件名后缀 ".bagli"。因其采用随机数覆盖，所以无法对文件进行解密，但因该勒索软件没有删除卷影的行为，受害者可尝试通过卷影恢复数据。加密完成后在相应目录下以及启动项目录释放名为 "oxu.txt" 的勒索信，诱骗用户向指定比特币地址支付 350 美元的赎金，勒索信所使用的语言为阿塞拜疆语，因此可推测其主要目标为阿塞拜疆用户。

▲Bagli 勒索软件勒索信

Bagli 勒索软件采用随机数覆盖的形式加密文件，目前被加密的文件无法解密。

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（Win XP）鉴定器、动态（Win7 x86）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、安全云鉴定器等鉴定分析。

最终依据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	c3c186a46f9ef44f8f1aad2879058b982dd20cd53a92224f4591858f9274c2f4
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	15 KB
MD5	4CD9B0B9CDF1929849E6BDFC6FDABB45
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/MSIL.Filecoder
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=4CD9B0B9CDF192984 9E6BDFC6FDABB45

◆常见行为

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

行为描述	危险等级
检测自身是否被调试	★★
镜像劫持	★★
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息(处理器版本、处理器类型等)	★
获取系统版本	★
检索系统内存信息	★
获取计算机名	★
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

◆常见行为

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04月12日(总第273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

APP 广告乱象逐步向好，工具类应用作为用户刚需终将迈向良性发展

随着数字化进程的加速，国内移动互联网和智能终端得到广泛普及，移动互联网应用场景和媒体形态日益丰富，对用户的工作和生活带来了革命性转变。移动终端用户规模的不断扩大促使移动端流量快速攀升，为移动互联网广告提供了前所未有的广阔市场空间，移动互联网广告业务也因此成为炙手可热的业务模式之一。

放眼全球移动互联网生态，谷歌 Android 生态从重流量变现转变为加强对应用生态的管控。从 2015 年开始，Google 逐年加强广告商业业态的安全监管和治理，逐步提高 Android 开发者的安全开发规范行为。苹果应用生态从重产品（用户）开始逐步开放一定符合用户需求的功能，但对广告模式一直采取谨慎消极的态度，更看重应用增值服务（IAP）商业模式。

反观国内移动互联网生态，目前已形成大规模、多元化发展竞争的局面。安卓生态依赖于国内各大手机厂商的自我运营和终端管控，缺乏统一的标准，相比海外 Google 和苹果分管两大生态，国内移动互联网生态碎片化更加明显，加之垄断流量的超级媒体内部管控较之手机厂商更加宽松、自律性更低，这无疑加大了国内生态的治理难度，除了行业规范和标准的有序引导，也需要技术手段和行业自治相结合。

今年央视“315”曝出的清理类应用广告乱象问题，安天移动安全在持续保持关注，近期行业问题治理效果明显，经安天移动安全风险应用检测预警平台分析发现，APP 广告乱象不仅仅存在于清理类应用中，也广泛存在于 WIFI、日历、小游戏等生活服务类应用中，并且存在恶意广告行为的工具类 APP 数量在近几年呈阶梯式上升趋势。

4 月 6 日，工信部发布了“关于下架侵害用户权益 APP 名单的通报”。通报称，工信部向社会通报了 136 家存在侵害用户权益行为 APP 企业的名单，经第三方检测机构核查复检，尚有 60 款 APP 未按照要求完成整改，依据相关法规对其进行下架处理。其中就包括 WiFi 全能助手、手机万年历、计步赚钱等日历、WIFI 类工具类应用。

工具行业由于门槛较低、用户粘性较差且无法正常通过增值变现等方式实现盈利，因此对商业广告变现依赖性极强，这些行业特点都导致在流量红利期结束时，工具行业作为依赖流量变现的典型行业首当其冲，尤其在超级媒体入局原供应链，不断挤压中小开发者生存空间的局面下，激进、粗暴的变现方式就成为其重要的生存手段。

广告乱象问题不仅会导致行业劣币驱逐良币的畸形格局，伤害整个行业生态的可持续发展，还会过度伤害用户的合法权益，成为行业从流量变现走向通过高质量服务进行增值变现道路上的绊脚石。当前，无论是监管部门、手机厂商还是安全厂商都在持续关注移动恶意广告乱象问题，移动互联网生态良性有序发展离不开行业相关规范和标准的引导，以及海量发现、关口前移的技术手段进行治理和约束。

对工具类应用来说，做工具开始并不意味着做工具结束，工具类应用作为用户刚需，仍然有较大的发展空间和变现潜力有待挖掘。只有建立健全相关行业标准规范，通过技术手段强化监管能力和提高行业自律性，才能确保移动互联网生态良性有序发展，还用户一个纯净、健康的网络环境。

（原文链接：https://mp.weixin.qq.com/s/o_qnrnETzSLjnmCkkBHbDw）

扫描上方二维码阅读全文

Aurora 运动：使用多个 RAT 攻击阿塞拜疆

Malwarebytes 研究人员发现使用多个 RAT 攻击阿塞拜疆的活动，并将该活动称为 Aurora 运动。研究人员发现的恶意文档以阿塞拜疆政府为目标，使用 SOCAR（阿塞拜疆共和国石油天然气公司）信件模板作为诱饵。文档日期是 2021 年 3 月 25 日，文档创建时间为 2021 年 3 月 28 日，研究人员认为此次攻击发生在 2021 年 3 月 28 日至 30 日之间。文档中嵌入的宏将提取使用隐写术嵌入在文档图像中的 Python RAT 并最终执行。

（原文链接：https://blog.malwarebytes.com/threat-analysis/2021/04/aurora-campaign-attacking-azerbaijan-using-multiple-rats/）

每周安全事件

类 型	内 容
中文标题	APT 组织正积极利用 Fortinet VPN 漏洞
英文标题	FBI: APTs Actively Exploiting Fortinet VPN Security Holes
作者	Tara Seals
内容概述	FBI 和 CISA 发布警报称，APT 组织正在积极利用 Fortinet FortiOS 网络安全操作系统中的已知安全漏洞，漏洞影响该公司的 SSL VPN 产品。攻击者正在扫描端口 4443、8443 和 10443 以获取存在漏洞 CVE-2018-13379、CVE-2019-5591 和 CVE-2020-12812 的设备。一旦被利用，攻击者就会向横向移动并对目标进行侦察。警报中并未透露有关 APT 组织的相关信息。
链接地址	https://threatpost.com/fbi-apts-actively-exploiting-fortinet-vpn-security-holes/165213/

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	Apache OFBiz 代码问题漏洞（CVE-2021-26295）	高	Apache OFBiz prior to 17.12.06 存在安全漏洞。由于该应用在处理序列化数据时对输入数据验证不严谨，使得攻击者可以将特制数据传递给应用程序，然后在目标系统上执行任意代码。
	Microsoft Windows 错误报告安全漏洞（CVE-2021-24090）	高	Microsoft Windows 错误报告存在本地权限提升漏洞。由于应用程序未在 Windows 错误报告中正确施加安全限制，从而导致绕过安全限制和特权升级。
	Microsoft Windows 容器执行代理安全漏洞（CVE-2021-26865）	高	Microsoft Windows 容器执行代理存在本地权限提升漏洞。由于应用程序未在 Windows 容器执行代理中正确施加安全限制，从而导致绕过安全限制和特权升级。
较为活跃样本家族	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[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/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[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.Hiddapp	中	此威胁是安卓平台上一种具有隐藏功能的木马类家族。该家族样本运行后，会隐藏图标，使用不同的方法向用户显示尽可能多的广告，包括安装新的隐藏广告软件。通过利用超级用户权限，该家族样本可以隐藏在系统文件夹中，清除难度较大。

2021 年五大关键网络安全风险及应对方法

A·N·安南斯 / 文 安天技术公益翻译组 / 译

在过去的一年中，企业发生了巨大的变化。很多企业拥有了大量远程办公员工，他们开始采用新技术，并全面进行数字化转型。这为中小型企业带来了很多机遇，也带来了诸多网络安全挑战。

为了应对这些挑战，企业必须解决一些潜在漏洞。接下来，我们将概述企业在其 2021 年网络安全战略中必须予以规划的领域，以最大程度地降低风险。

1. 端点威胁

超过 70 % 的威胁通过端点进入。很多远程员工依赖于一直联网的笔记本电脑和服务器，VPN 和基于云的 SaaS 服务等进行办公。因此，企业应了解如何实施全面覆盖的解决方案，这一点非常重要。

企业应使用全面、分层的网络安全策略，以降低与远程办公人员相关的风险，增强或者替换无法应对当今威胁的传统反病毒工具。企业可以通过将“安全信息和事件管理”（SIEM）扩展到每个端点，为易受攻击的设备增加深度防御功能，利用整体性的威胁预防、检测和响应策略，使 SIEM 策略充分发挥作用。

2. 居家办公的漏洞

远程办公能够带来诸多优势，包括灵活性和适应性等。不幸的是，这也会带来许多新的攻击向量。在迅速转向居家办公的情况下，企业拥有了大量分散设备和新网络，这会带来潜在的安全问题。

原本的网络安全策略已不再适用于移动设备和远程员工。实施安全的远程连接和多因子身份鉴别（MFA），对于维护企业运营的安全性至关重要。

3. 云安全风险

随着疫情爆发和居家办公（WFH）时代的到来，企业将重心转移到了业务连续性上。对于许多企业来说，这意味着加快云迁移的速度。这种变化使云安全成为重中之重，因此，企业对云中内置的安全功能抱有很大的期望。将关键业务数据迁移到云中，企业需要更多地依赖云平台控制和管理功能。在这种情况下，企业需要注意，保护与云计算相关的数据、应用程序和基础架构与保护本地 IT 架构同样重要。

企业应寻求具备云知识的合作伙伴或安全托管服务提供商（MSSP），以帮助自己选择符合目标的云安全方法，实现合规性。

78 % 的 Microsoft 365 管理员并未启用 MFA。由此可见，云计算的另一个重要威胁是人为错误，包括可能导致数据泄漏的配置错误。增强云监控和可见性，有助于应对此类威胁，确保数据安全，检测可疑行为并跟踪意外事件和操作。

4. 人才和技能短缺

如今，网络安全技术比以往任何时候都更加先进和多样化，这导致一些企业过度依赖单点解决方案来抵御威胁。虽说在抵御威胁方面，技术至关重要，但企业不能只依赖某一种解决方案。通常，中端市场企业缺乏有价值的专用网络安全资源。疫情期间，随着企业的网络版图扩展到包括家用 PC 和其他 WFH 接入点在内的威胁面，这种技能短缺进一步加剧。

Verizon《数据泄露调查报告》指出，在 2020 年，几乎三分之一的数据泄露涉及小型企业；企业要想缓解威胁，需要将人员、流程和技术进行有计划的结合。企业对安全专家的需求不断增长，但是雇用更多的安全专家，成本会非常高昂。

与其投资于内部全天候的安全运营中心（SOC），不如将这项工作外包——这种方法具有成本效益，是企业防御策略必不可少的补充。外包团队可以将不同的技术与流程结合起来，以创建独特、清晰的可见性点。

5. 新威胁

随着检测和响应技术越来越强大，攻击者也在不断调整攻击方法。勒索软件或“低端低速”攻击等多阶段攻击，已成为企业面临的新威胁。攻击者通常利用窃取的凭证来启动此类攻击，之后利用这些凭证进行侦察以渗透公司系统和数据。

企业应采取主动措施来应对这些威胁。例如，MFA 有助于防御利用被盗凭证的攻击。托管威胁防护解决方案可以提供从预测和预防到检测和响应的端到端安全，能够在攻击造成损坏之前向企业发出告警。

提前做好计划

攻击者的手段会越来越更高明，新技术会带来更多的漏洞，而人为错误也是无法避免的。但是，企业可以采取一些方法，将这些威胁带来的风险降至最低。

对于许多企业而言，这意味着与合作伙伴合作。这些合作伙伴能够帮助企业增强网络安全成熟度并实现其安全目标。对于其他企业来说，这意味着通过新的框架、流程和 IT 人员增强网络安全态势。

要想实现良好的网络安全，企业首先应确定最值得关注的领域，比如说，最敏感的数据存放在哪里？

原文名称	5 key cybersecurity risks in 2021, and how to address them now
作者简介	A · N · 安南斯（A.N. Ananth），是 Netsurion 公司总裁兼首席执行官。
原文信息	2021 年 04 月 02 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2021/04/02/key-cybersecurity-risks-2021/
摘 要	在过去的一年中，企业发生了巨大的变化。很多企业拥有了大量远程办公员工，他们开始采用新技术，并全面进行数字化转型。这为中小型企业带来了很多机遇，也带来了诸多网络安全挑战。本文概述企业在其 2021 年网络安全战略中必须予以规划的领域，以最大程度地降低风险。
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。