安天发布《新型 sLoad Downloader 宏病毒样本分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一种新型的 Office 宏病毒。它不需要用户手动打开文档，只需要用户在预览窗口模式下，或者在 Outlook 的预览模式中选中该文档，即可触发恶意行为。

这种恶意文档被嵌入到电子邮件的附件中，通过钓鱼邮件进行传播。如果用户的计算机中启用了 Windows 的预览窗格功能，只要在资源管理器中选中一个文档，便可以在右边生成一个对该文档的预览窗格，显示文档的大致内容。为了生成预览，系统会提前解析文档，并且在解析过程中把宏设置为禁用状态，所以原本 Office 文档中的宏代码是不能被触发的。但是，当预览这个样本时却可以触发恶意宏。通过分析发现，这个样本本身并不含有宏代码，但是它利用了 RTF 文档允许内嵌 Excel，使用“\objupdate”强制更新的特性，来触发恶意宏。该 Word 样本的页脚部分内嵌了五个 Excel 工作簿，每个工作簿都含有宏代码，并且在它们的 G135 单元格中有一串 Base64 编码的文本，当宏代码执行时，会读取此单元格的内容，将文本转化为一段 PowerShell 可执行的脚本，通过运行脚本而触发恶意行为。

安天 CERT 提醒广大政企客户，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。

目前，安天追影产品已经实现了对该类恶意代码的检出。

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、文件来源信息鉴定器、文件元数据鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、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	4AA1BB25D985845219454882583 6DB66.doc1
文件类型	Document/Microsoft.RTF[:Rich Text Format]
大小	574 KB
MD5	4AA1BB25D985845219454882583 6DB66
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Downloader]/MSOffice.SLoad.gen
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=4AA1BB25D985845219454882583 6DB66

◆ 运行环境

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
RTF 内嵌 OLE 对象	★★★
dll 劫持	★★★★★

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
af1f0ed351329098_padministratorsx.dat	be7cf5e9a01f79a0f6a47fc00bf730d7	N/A	N/A
e42363d94291d77a_mstag.tlb	3ed771a7a1ac97343db7c2aaf18d6e3d	N/A	N/A
3dedffbaa82c9e83_mso.dll	251c11444f614de5fa47ecf7275e7bf1	N/A	N/A
7bbf9dee5d9dbe3f_pintlgd.imd	2874af236772fd4826898a1f5f1fbc5f	N/A	N/A
3fea120d39b1f0b6_target.rtf	4aa1bb25d9858452194548825836db66	N/A	N/A
44f476e63fa37991_pintlgc.imd	fa965f67e39d09c395c38b3a4c0555b9	N/A	N/A
f7af879401bf3413_pintlgvr.imd	e6bff67cf47625a0c4995a6632bb5f5b	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 2019 年 03 月 18 日 (总第 175 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

肖新光委员：规划、预算、问责三结合 全面提升网络安全防护水平

全国政协委员、安天创始人肖新光与人民网副总裁宋丽云女士合影

3 月 13 日，全国政协委员、安天科技集团创始人、首席技术架构师肖新光做客人民网，就网络安全等相关话题进行了交流。他建议，通过系统规划指引、保障预算投入、加强问责落实，形成良性发展大环境，全面提升政府、央企网络安全防护水平。

“今年政府工作报告中多次提到信息以及信息技术的发展，我们国家的信息化发展速度是非常快的。信息化有大量增量建设部分，包括新技术应用的部分，包括像 5G 网络、大数据平台，以及人工智能技术的更大范围的探索和应用等等。越是在信息化高速发展的过程中，网络安全越需要同步建设，越需要在所有信息系统的规划、建设、运维全生命周期考虑网络安全问题；对于存量部分的防护不足，也需要‘填坑补课’。这样才能确保我们的信息基础设施是安全的，才能保障我们信息社会机体是健康的，才能保障我们信息社会的大厦是坚固的。重要信息系统和信息基础设施处于‘低水平防护’，甚至无效防护的状态中，是国家安全与稳定的严重隐患，影响到国家的战略主动性。作为一个网络安全行业的从业者，在信息化高速发展中，我们心中有更大的紧迫感，有更强的危机意识，希望能够进一步加速把我们相关的工作做好。”面对信息化建设高速发展，肖新光说出了网络安全工作者的责任感和使命感。

反思：“缺少系统规划指引，就不能有效将预算投入转化为防护能力”

在当前情况下，我国面临着复杂严峻的内外部形势，在众多的风险挑战中，“网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击”是一项突出的风险。网络安全防控能力以国家大型工程为主干，以各政企机构建设管理的每一个重要信息系统和信息基础设施的安全为基石。基石的稳固性依赖于每一个重要信息系统和信息基础设施的安全，要形成防护能力，就依赖于它的对应的责任主体，依赖于它的建设运维机构，依赖于建设动态综合的网络安全防御体系。

肖新光指出，当前网络安全工作中，存在三大短板：安全规划能力普遍不足、缺少充足的预算资源保障、网络安全的责任制没有完全落地。

肖新光指出，当前无论是从作为需求方的政企机构，还是作为供给方的安全企业都存在一个共性问题，就是整体安全规划能力普遍不足，难以贯彻总书记“树立动态、综合的防护理念”的工作要求。现行做法往往是在满足一般性合规要求的基础上，再简单堆砌部分产品应对各类单点威胁，对于如何在系统规划、建设、运维中都充分考虑网络安全问题，如何实现网络安全能力与信息化各个层次与环节的深度结合、全面覆盖，如何形成动态综合防御体系，缺少明确的方法指引。

过去我们往往把目光放在增加投入上。但投入是一个中段环节，若没有足够规划能力，把“敌情想定”下的防护能力体系准确描绘出来，规划出所有的安全环节及与信息化的结合覆盖方式，规划出这些安全环节的协同联动关系和统一管理分析机制，规划出管理运行保障机制，投入就无的放矢，既无法保证能力有效落地，也无法支撑预算框架和规模。肖新光说，“如果不进行规划指引，单纯呼吁增加投入，可能产生两种情况：一是无效投入，花了冤枉钱，但没有形成防御能力；二是虚假投入，号称作出了相应的投入，但实际上是用来应付检查的。”

形成合理规划后，需要有充分的资源投入来落实，而投入来自充足的预算保障。传统预算思路中，把网络安全视

（下接第二版）

（上接第一版）

为信息化的附属部分，在经济下行压力加大的大环境下，政企机构信息化投入普遍放缓，导致网络安全建设缺少预算支撑。根据调研了解的情况：部分国企强调“所有信息化立项建设必须填写‘内部受益部门’”，以投入对业务盈利的支撑作用为是否批准上项目的主导依据，而网络安全作为基础保障能力，看起来没有明显的“内部受益部门”，导致网络安全建设“师出无名”。加之一些单位认为“网络安全建设就是在合规基础上尽量降低成本”，导致网络安全项目纷纷延误或压缩。但越是在国家面临严峻的风险挑战时，提升国家安全能力的预算投入，越需要得到优先保证。

肖新光说，“网络安全不能只依靠国家统一攻关和统一大工程，我们必须把网络安全责任制落实到每一个机构身上去。如果我们的问责导向都是以出了事情来问责，如果我们的考评导向都是以经济性指标来考核，网络安全就不太可能作为一种重点投入。当前在网络安全的问责机制中，多数由一般性检查和事件触发，容易使政企机构产生应付的状态或者是撞大运的心理，对落实网络安全责任制中的渎职怠职、消极不作为、落实不到位等问题，还缺少深度问责机制。同时在政企机构内部，往往缺少承接网络安全责任制的内部机制，对网络安全责任权属不清，职责不明，影响规划设计、实施和运维应急机制的建立执行。

建议：三方面全面提升网络安全防护水平

肖新光在今年两会的提案中，针对短板问题提出了三点切实建议。

一是建议网信办、国资委等机构联合发文，为各级政企单位提出**清晰的战略指引和体系化、框架性防护规划指引**，将网络安全防护工作引导到全面建设所有必要的网络安全防御能力，并将其有机结合以形成动态综合网络安全防御体系的**能力导向建设模式**。

二是建议网信办、国资委、财政部对网络安全预算投入给出清晰的**结构性保障要求**，建立综合考虑信息资产价值、防护等级要求、敌情想定、防护效果的预算规划机制，对网络安全和信息化同步规划建设，对防护缺失“填坑补课”等工作给出硬性工作要求，确保有效投入。

三是建议在现有相关主管部门考核、监管、检查的基础上，**积极探索通过国家监察体系对网络安全责任制的落实实施监督审查**，对政企机构在网络安全工作中是否及时有效制定规划、配置资源、执行预算，是否达成有效防护效果等督查问效，形成深度问责机制。并将政企机构网络安全责任融入本单位“三定”工作中，明确各部门职责规范。

必须多部门协同，把规划、预算、问责转化成一个可落地的闭环，这样才有网络安全发展的大环境，才能有效驱动政企机构网络安全防护水平的全面加速提升。

政府：把网络安全防御能力建设提升到落实网络强国的战略高度

针对政府机构在网络安全工作中扮演的责任，肖新光表示，建议网信办、国资委等机构联合发文，以总体国家安全观为引领，**明确网络强国建设目标、信息化发展、网络空间安全防护三者间的辨证关系**，将包括央企在内的政企机构的网络安全防御能力建设提升到落实网络强国建设目标的战略高度。

肖新光表示，一方面，政府机构中有网络安全的主管部门、责任部门和关联部门。为提升我国的网络安全，这些部门做了大量扎实的、基础的工作，推动网络安全从无到有，对安全威胁风险组织应急应对。在此基础上如何从有到优，相关部门不能只停留在检查视角或惩戒视角，更要强化帮扶赋能视角，集中优势能力，形成高质量的规划指引，推动引领安全防护水平的整体提升。

另一方面，政府的各个机构部门本身也是一个需要网络安全保障的用户。政府部门承载着整个社会的管理、治理和运行，如果自身信息系统遭遇了入侵、窃取、控制、毁瘫等，对整个国家安全和社会运行，包括人民群众的福祉都会产生重大的威胁。所以，政府部门要率先做好自身的网络安全防护工作。从企业的角度来看，无论是央企还是民企，很多是我们国家重要信息系统和关键系统、基础设施（包括像能源、电力、金融、交通）的建设者、运营者，社会运行命脉、全民隐私信息、先进科研成果，都承载在这些网络体系之上，与国家安全和社会安全息息相关。重要政企机构的信息系统面临的威胁方，不只是低层级的威胁行为体，而是带有政府背景的高能力甚至超高能力的威胁行为体，需要站在关乎国家安全和社会安全的高度做好自身所管理运维的重要信息系统和关键基础设施的安全防护，需要更高的防护水平。从企业的自身经营发展角度，比如说一个企业的科研成果，假定它被竞争方窃取，进行仿制，也会对企业自身的生产经营，对企业自身的发展产生不利的甚至毁灭性的影响。

网络安全与总体国家安全的每个方面都发生着密切的关联，不同政企机构有自身情况的差异性，但都责任重大。

万豪透露连锁酒店数据泄露事件调查细节

针对去年连锁酒店大规模数据泄漏事件，万豪 CEO 透露调查细节。万豪 2018 年 9 月 8 日第一次发现异常，当时管理喜达屋客户预订数据库的 IT 公司埃森哲联系了他们。万豪 9 月 10 日展开了调查，一周后发现了 Starwood IT 系统上的恶意软件，是一种远程访问木马，允许攻击者秘密访问、监视，甚至控制计算机。10 月份，调查人员发现了渗透测试工具 Mimikatz。11 月，调查人员发现自 2014 年 7 月以来黑客一直活跃在喜达屋的 IT 网络上，早在万豪收购之前，黑客已经入侵了网络。万豪首席执行官表示，调查工作尚未发现证据表明黑客获得了支付卡的解密密钥，这意味着大多数受损的支付卡号码对攻击者来说仍然无用。

（来源：https://www.zdnet.com/article/marriott-ceo-shares-post-mortem-on-last-years-hack/）

医疗机构如何应对网络安全问题

Brad Spannbauer / 文　安天技术公益翻译组 / 译

网络安全一直是医疗机构关注的问题，然而在过去的一年中，他们并未采取什么有效的措施。2017 年，美国卫生与公众服务部的民权办公室（OCR）报告了 359 起数据泄露事件，每一起事件都泄露了 500 条或更多的医疗记录，总量累计已超过了 500 万条。而在 2018 年，数据泄漏事件达到 350 起，泄露的医疗记录几乎增加了两倍，达到约 1300 万条。这意味着，数据泄露事件导致更多的人面临身份盗窃等风险。

虽说占据头条新闻的往往是影响大型医疗机构的“大规模数据泄露事件”，但是很多未被关注的事件也会对患者造成严重的危害。

不幸的是，对于医疗机构来说，打击网络犯罪并没有万能“银弹”。对抗现有和未来的威胁（无论大小）都需要一种融合了适当技术、严密策略和灵活实践的方法。

不断进化的威胁和防御措施

随着网络犯罪分子的攻击方法越来越先进和具有欺骗性，医疗机构需要相应地调整和改进防御措施。当今医疗机构面临的最大网络威胁之一是勒索软件。根据 Verizon 公司《2018 年数据泄露调查报告》，在所有与恶意软件相关的数据泄露事件中，有 39%涉及勒索软件，同比翻了一番。

医疗行业特别容易受到此类攻击，这是因为：如果无法及时访问或更新患者的电子病历，或者推迟其治疗，患者就会面临生命危险。

电子邮件网络钓鱼——多种恶意软件（如勒索软件）的典型传递机制——越来越先进，犯罪分子使出浑身解数诱骗毫无戒心的员工点击恶意链接、打开附件、提供登录信息或其他敏感信息。

为了降低网络钓鱼风险，医疗机构不仅要投资于恰当的安全工具，还要定期培训员工，帮助他们识别潜在的威胁（故意发送特制的“钓鱼”邮件给员工，看看哪些员工会“中招”）。此外，员工必须熟悉基本防范策略和相关操作规程，确保遇到威胁时，能正确高效处置。

投资于恰当的安全工具

鉴于医疗行业存在很多网络安全漏洞，因此投资于恰当的工具尤为重要。除了满足各种工作流程和效率要求外，用于处理、共享或存储患者受保护医疗信息（PHI）的所有工具或应用必须严格遵守《健康保险可携性与责任法案》（HIPAA）。

例如，由于缺乏一致的访问控制和强制加密策略，很多电子邮件运营商并不遵守 HIPAA 的安全要求。由于类似的原因，专为消费者通信设计的移动应用（如 WhatsApp）或流行的云存储解决方案（如 Dropbox）也不适合医疗机构。虽然这些应用价格低廉、使用方便，但是它们本身就存在风险，会为攻击者提供入侵点，更不用说人为错误导致的风险了。此外，这些应用可能会出于各自的目的秘密收集用户数据。为了降低此类风险，医疗机构必须投资于恰当的工具。

关注内部风险

在提及网络安全泄露事件时，大多数人会想到外部犯罪分子。但是，造成最大威胁的通常是最接近数据的内部人员。根据 Verizon 公司《2018 年数据泄露调查报告》，医疗行业是唯一一个内部人员造成的网络安全威胁远超外部威胁的行业。

内部威胁经常由人为错误（35%）或系统滥用（24%）引发——这两种情况都可以通过员工培训和教育来预防。未能识别并应对这些内部风险的医疗机构会面临严重的威胁。

越来越多的“自带设备”（BYOD）、灵活的工作地点，以及商业活动和个人在线活动界限的日益模糊，导致了内部威胁的飙升。设备丢失或被盗，非安全通信和设备使用（例如，与其他人共享设备）等问题也在增加。

医疗机构必须慎重考虑其安全实践，并实施严格的策略和规程来减少潜在的安全和隐私漏洞（例如，确保所有便携式设备都执行数据加密并实施强口令策略）。

医疗机构不仅要关注内部员工；还要关注商业伙伴和供应商，因为他们也会带来风险和后门。2018 年，在 OCR 收到的数据泄露报告中，有四分之一涉及商业伙伴，影响到近 600 万人。虽然第三方商业伙伴为医疗机构提供重要的服务，但是许多商业伙伴缺乏合规性和隐私要求，是网络安全链条中的薄弱环节。

如果医疗机构与第三方商业伙伴合作，则应确保所有伙伴都遵守其安全标准和数据保护规则，并与其签订商业伙伴协议（BAA）类书面协议，以明确其要求。虽然这已经成为法定要求，但是不签订 BAA 的情况仍然很普遍。

好消息是，尽管数据泄露事件不断增加、安全漏洞持续存在，但是整个医疗行业的风险意识正在增强。意识到风险是防御风险的第一步，因此在 2019 年，医疗机构应开展员工培训，并为其提供有效、安全开展工作所需的工具。

原文名称	How can healthcare organizations remedy their cybersecurity ailments
作者简介	Brad Spannbauer。Brad Spannbauer 是 eFax Corporate 公司产品管理高级总监。
原文信息	2019 年 3 月 11 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2019/03/11/healthcare-organizations-cybersecurity/
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。