安天发布《Agent Tesla 窃密木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现了利用鱼叉式钓鱼邮件传播 Agent Tesla 窃密木马活动。该活动主要针对能源、制造、运输等行业。Agent Tesla 是 2014 年公开售卖的窃密木马，该木马主要通过钓鱼邮件传播，目的是窃取用户敏感信息。目前，安天追影产品已经实现了对该窃密木马的鉴定；安天智甲已经实现了对该窃密木马的查杀。

该活动通过带有恶意附件的鱼叉式钓鱼邮件传播，一旦用户运行附件中的可执行文件便会启动 Agent Tesla 窃密木马。该木马执行后将自身路径添加到注册 表 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 键值下设置为开机自启动。Agent Tesla 运行后会窃取用户各种凭证包括 FTP 凭证、WiFi 登录凭证、电子邮件凭证、浏览器中存储的凭证等。除此之外，该木马还包括远程桌面控制、键盘记录、收集主机信息、获取进程路径、控制摄像头、获取屏幕截图、复制剪贴板内容、上传敏感信息文件、获取进程列表、结束指定进程和下载其他恶意文件等功能。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不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良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，如果业务上无需使用远程桌面服务，建议将其关闭。

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、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、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、静态特征检测鉴定器、安全云鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	c393
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	301 KB
MD5	D9A468687E5B8AE231D21B0C720D5234
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Razy
判定依据	BD 静态分析

◆ 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
修改本机 hosts 文件劫持域名	★★★★
通过 WMI 查询操作系统信息	★★★
检测虚拟机	★★★
通过 WMI 查询 CPU 信息	★★★
延时	★★★
检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
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	★
检测自身是否被调试	★★
获取驱动器类型	★
创建窗口	★
设置调试器权限	★
获取计算机名	★
访问文件尾部	★
自我复制	★★
Run 自启动	★
疑似桌面控制	★

◆进程监控

PID	创建	命令行
1332	target.exe	"c:\66ae65b85846440bb675c582e06b3334\share\target.exe"
164	netsh.exe	"netsh" wlan show profile

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2020 年 5 月 18 日 (总第 230 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

两会召开在即，全国政协委员肖新光继续为网络安全建言献策

受新冠疫情影响，每年 3 月召开的全国两会时间推迟，4 月 29 日，根据央视新闻官方消息，两会时间确定：

十三届全国人大三次会议将于 5 月 22 日在北京召开；

全国政协十三届三次会议将于 5 月 21 日在北京召开。

和其他委员一样，安天首席架构师、全国政协委员肖新光也在为今年的两会提案做最后的准备，下面让我们共同回顾一下近年来肖委员的“两会”提案。

2018——《在网络空间安全领域进行针对性投入和布局应对重大地缘安全风险的提案》

网络空间领域的斗争已经是大国博弈和地缘安全中的常态化存在，网络空间更是政治、军事、经济等领域斗争的首发战场。

2017 年 6 月，乌克兰包括政府首脑机关、金融、电信、交通、能源等计算机系统，遭遇了伪装成勒索病毒的大面积网络攻击，导致大量系统瘫痪，对社会生活和稳定造成了严重影响。已经发生的多起类似事件提醒我们，针对重要信息系统，特别是关键信息基础设施的入侵、信息窃取和毁瘫，已经是广泛存在的既定事实。

肖新光委员强调，当前我国所面临的全球和地缘安全风险，既以大国竞合为主旋律，同时又围绕地缘安全热点展开，地缘利益竞合方众多，多种矛盾复杂交织。我国遭遇的网络安全关键性威胁很大比例与上述风险相关。不同对手的攻击动机、攻击目标选择、攻击手段和攻击能力有很大差异。

他认为，网络安全威胁不是单纯的技术风险，其风险和事件研判也不是单纯的领域内研判，这与攻击发起方和潜在对手的战略意图、技术能力和综合国力等综合因素息息相关。我们对过去遭遇到的网络入侵攻击，往往将其作为单纯的网络安全事件看待，而缺少与总体国家安全的多个方面进行综合分析，对对手意图的分析深度不足。未来，需要对网络攻击行为给我国政治安全、军事安全、科技安全等带来的综合影响后果全面加强研判，实现综合分析、全面量损、有效止损。

未来的网络安全工作应遵循“网络安全是整体的而不是割裂的”、“是动态的而不是静态的”、“是开放的而不是封闭的”、“是相对的而不是绝对的”、“是共同的而不是孤立的”的主要特点，在进一步的投入中提升系统性、及时性和针对性，解决不平衡不充分的安全建设导致的国家安全能力短板和失衡。

2019——《关于通过系统规划指引、保障资源投入、加强问责落实，全面提升政府央企网络防护水平的提案》

肖新光认为：“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”是众多风险中的一项突出风险。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重要信息系统和信息基础设施的安全为基石。基石的稳固依赖于每个系统的安全防护能力，依赖于它的对应责任主体、建设运维机构，建设动态综合的网络安全防御体系。

他表示，无论作为需求方的政企机构，还是供给方的安全企业都存在一个共性问题——整体安全规划能力普遍不足。现行做法往往是满足合规要求基础上，简单堆砌部分产品应对各类单点威胁。但如何在系统规划、建设、运维中充分考虑网络安全问题、如何实现网络安全能力与信息化的深度结合、如何形成动态综合防御体系，缺少明确方法指引。

“过去把目光都放在增加投入上，但投入只是中段环节，没有足够的规划能力，投入就无的放矢，就无法保证能力有效落地，无法支撑预算框架和规模。”肖新光说，“不进行规划指引，单纯呼吁增加投入，很可能造成无效投入或虚假投入。”肖新光指出，能力建设离不开投入，投入离不开预算保障。越是面临严峻的风险挑战，提升国家安全能力的预算投入越需要优先保证。

他指出，安全规划能力普遍不足、缺少充足预算资源保障、网络安全责任制没有完全落地，是当前网络安全工作中的三个短板。对此，他建议：

应从落实网络强国的战略高度，为政企机构网络安全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。

应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、防护缺失填坑补课等给出硬性工作要求，确保有效投入。

应在现有考核、监管、检查机制基础上，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。

当前，网络安全所面临的风险挑战依然复杂严峻，随着网络强国战略不断推进实施，对能力型网络安全企业的使命要求也不断提高。过去，安天在尝试从单纯的反恶意代码视角提升至威胁对抗视角时遭遇了许多挫折，在经验教训中不断反思，提出了引入威胁框架作为自身新一轮能力建设导向的考虑。过去的一年里，安天团队在业内专家指导下，围绕威胁框架，根据实际情况不断完善各产品能力。安天正在从传统的反恶意代码小闭环中走出，切换到赋能客户、共建防御加威胁对抗的大闭环当中去。

每周安全事件

类 型	内 容
中文标题	白象组织使用 BackConfig 攻击南亚政府和军事组织
英文标题	Updated BackConfig Malware Targeting Government and Military Organizations in South Asia
作者及单位	Alex Hinchliffe and Robert Falcone
内容概述	在过去四个月中，Unit 42 研究人员观察到“白象”组织使用 BackConfig 恶意软件针对包括南亚政府和军事组织的攻击活动。初始感染使用武器化的 Microsoft Excel（XLS）文档，文档通过被入侵的合法网站提供。Excel 文档包含 VBA 宏代码，宏代码启用后，创建文本文件 Drive.txt，并将批处理文件写入另一个文本文件 Audio.txt，重命名为 Audio.bat 执行。批处理会清理与先前感染相关的所有文件和文件夹，并重新创建所需环境。批处理文件还创建两个计划的任务来引用两个尚不存在的文件 dphc.exe 每隔 10 分钟运行一次和 Drive.vbs 每隔 20 分钟运行一次。最后，在删除自身之前，批处理文件会将 Drive.txt 重命名为 Drive.vbs，Drive.vbs 将下载 BackConfig 可执行文件 dphc.exe。
链接地址	https://unit42.paloaltonetworks.com/updated-backconfig-malware-targeting-government-and-military-organizations/

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.x200portal.a[rmt,prv,spy] 2020-05-11	高	该应用程序运行后获取 root 权限，激活设备管理器并隐藏图标，后台接收短信和远程指令完成用户手机拍照、录像等；监听用户手机数据，上传用户短信、手机固件信息、联系人、社交应用等隐私信息，造成用户隐私泄露和资费损耗，请立即卸载。
		Trojan/Android.rootstv.a[exp] 2020-05-12	中	该应用程序是针对智能电视的恶意应用，程序运行会利用系统漏洞提权，静默安装未知应用，远程推送应用，造成用户资费消耗，建议卸载。
		Trojan/Android.Gugi.b[prv,exp,rmt] 2020-05-13	中	该应用程序伪装成其他应用，运行会隐藏图标，请求激活设备管理器，私自发送短信，监听短信拦截指定短信，利用钓鱼界面诱骗窃取用户的银行相关账号和密码，窃取用户短信、通讯录等信息，造成用户隐私泄露和资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.Mobilespy.f[prv,rmt]	中	该应用程序是一款间谍软件。手机重启后会在后台自动运行，能够监听用户的通话记录、短信记录、上网记录和图片库等信息，能够通过 GPS 定位知道用户的所在地等，并把信息上传到指定的网址，造成用户隐私泄露，建议立即卸载。
		Trojan/Android.QQspy.ck[prv]	中	该应用程序伪装成 qq 相关应用，运行后诱导用户输入 QQ 账号和密码并短信转发，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.GLocker.jm[rog,lck]	中	该应用程序为勒索软件，会锁定用户屏幕进行敲诈勒索，造成用户手机无法正常使用，建议卸载。
		Trojan/Android.xstd.a[pay,rmt]	中	该应用程序伪装成系统应用，运行时会向特定手机号发送激活短信，并注册远程服务器、联网获取配置信息，执行发送扣费短信、拦截回执短信、自动回复、屏蔽指定外拨号码等操作。此外，还会强制用户激活设备管理器，且无法正常取消激活进而卸载，给用户带来经济损失，建议卸载。
		Trojan/Android.GFakeSys.j[rog,sys]	低	该应用程序伪装为系统应用，安装无图标，包含风险行为代码，警惕后台私自下载并安装软件，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Server Message Block 安全漏洞（CVE-2020-0796）	高	Microsoft 服务器消息块 3.1.1 (SMBv3) 协议处理某些请求的方式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目标服务器或客户端上执行任意代码。
	较为活跃样本家族	Trojan[Downloader]/Win32.Busky	中	此威胁是一种具有下载行为的恶意木马类程序。它能够通过互联网下载到用户电脑，并开展了一系列的破坏性行动。它首先会添加自身到注册表启动项，能关闭正在运行的反家族软件进程，或直接禁用或损坏防家族程序及其相关文件。它会监视你，并记录用户个人信息，如用户名和密码。
		Trojan/Win32.FraudST	中	此威胁是一种恶意木马类程序。它与垃圾邮件广告的非法网上药店和诈骗涉及垃圾邮件推广假冒医疗产品有关。该家族已经与瞄准 Facebook 用户和 PayPal 用户的网络钓鱼攻击相关联。其主要目标是渗透到计算机系统，并允许黑客从远处控制它。这意味着，黑客利用它来迫使受感染的计算机发送垃圾邮件，它可以轻易地被用来执行分布式拒绝服务攻击，或者安装键盘记录器和其它数据盗窃的应用程序。
		Trojan[Banker]/Win32.VB	中	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序，允许对受影响的计算机进行未经授权的访问。该家族程序能够下载和执行由远程攻击者指定的任意文件。
		RiskWare[WebToolbar]/Win32.MutiBar	低	此威胁是一种可以安装浏览器扩展的风险软件家族。该家族使用特殊的安装程序，采用各种方法来获取权限，从而安装其它软件组件。
		GrayWare[AdWare]/Win32.4Shared	低	此威胁是一种有广告行为的灰色软件家族。该家族的样本在执行后会连接远程的服务器下载广告在用户的 PC 上弹出。该家族的样本具有较多种签名形式和变种。

开展远程办公应部署多因子身份验证的原因

丹·康拉德 / 文　安天技术公益翻译组 / 译

目前，全世界有三分之一的人正在远程办公，而且还不确定这种办公形式何时才会结束，因此企业必须调整其业务运营模式以支持长期的远程办公。

根据 Gartner 公司最近的一项调查，实现有效远程办公所面临的最大障碍是远程办公的技术和（或）基础架构落后。

随着企业更新其远程办公技术和基础架构，以支持不断增长的远程办公员工数量，如何解决安全问题成为了当务之急。居家办公或隔离使得员工的工作和私人生活之间的界限变得模糊，因此，企业实施的第一道安全防线非常重要。为了帮助降低潜在的风险，CISO 和 IT 管理者应部署多因子身份验证（MFA），以确保其员工在远程办公期间的网络安全。

为什么要部署多因子身份验证？

如今，63%的数据泄露事件与弱密码或重复使用密码有关，部分原因是许多企业使用了无效的身份验证策略，这些策略往往要求员工经常更改密码和使用特殊字符。

但同时，企业和员工希望在受到更少的干扰的情况下，快速获得完成工作所需的资源。

这要求企业在实现安全时，达成一种平衡。他们需要弄清楚如何建立强大的检查点，从而在减轻潜在威胁的同时，提高员工的工作效率。大多数传统的安全解决方案都达不到这一目标，而多因子身份验证可以帮助企业达成这种平衡。它需要的只是再添加一个可以验证用户身份的因素。

特权身份滥用是造成大多数数据泄露的常见原因，多因子身份验证针对潜在暴露点，提供了额外的保护层。当黑客将目标对准那些技术不熟练、刚刚居家办公的员工时，多因子身份验证可以阻止黑客的攻击。因为要想访问目标用户的网络，黑客必须使用用户用来生成其 MFA 验证码的设备，这对大多数黑客来说都是相当困难的（但不是不可能）。

在大多数员工在不安全的家庭和公共网络上办公的情况下，将多因子身份验证作为一种额外的保护措施，不仅可以减轻 IT 团队的负担，还可以使未受过安全培训的员工不易受到黑客的攻击。

企业在采用 MFA 解决方案之前需要考虑的四个问题

采用多因子身份验证的进程之所以缓慢，是因为它的集成成本通常很高，而且集成过程非常复杂，因此企业必须进行全方位的考虑，以确保它们与员工和业务需求保持一致。在购买之前，企业需要考虑以下因素：

1. 解决方案的用户友好度如何？

用户能否接受一种 MFA 方案的关键是看方案是否更改了用户习惯申请和分配令牌（用户标识自己的渠道）的方式，企业必须考虑员工在整个过程中的工作方式。

通过选择与员工登录其电子邮件或其他日常任务的方式一致的令牌，企业可以确保快速、平稳地部署解决方案。

2. 解决方案会对管理员产生什么影响？

管理员对于授予访问权限和运行日常操作至关重要，企业必须考虑部署解决方案会对管理员的日常工作产生什么影响？解决方案的易用性和可用性是企业需要考虑的两个重要因素。

在寻找解决方案时，许多企业应考虑受活动目录用户和计算机（ADUC）管理的解决方案。通过 ADUC，管理员不需要学习新的控制台，这意味着他们不必主导新软件的部署。该解决方案必须提供简化且快速的支持，以帮助管理员排除故障并解决可能发生的与用户相关的任何身份验证问题，这一点也很重要。

3. 解决方案如何扩展并适应企业当前的系统？

在确定解决方案会对员工产生什么样的影响之后，就该考虑解决方案如何与您当前的身份验证软件相协调。对于远程办公人员来说，企业需要知道是将解决方案集成到现有的身份数据库中，还是用户提供的新数据库中。

集成的成本和复杂性不仅阻碍了解决方案的成功集成，而且增加了员工的使用难度，因此企业必须考虑如何使其与其他身份验证软件相协调。使用灵活且可与其他工具集成的解决方案可以使 IT 团队放心，因为用户能够在他们的日常任务中实施新的安全措施。

4. 企业的最佳令牌选择是什么？

令牌的类型和功能不尽相同，因此您需要考虑的是，哪种令牌最适合企业的业务运营。为了确保您可以选择到正确的令牌类型，了解令牌的类型以及它是硬件令牌还是软件令牌非常重要。对于软件令牌，您应该弄清它是否与所有操作系统兼容，还有它是基于短信、电子邮件还是网络的。

如果您想要的是硬件令牌，则需要确定其是否与 OATH 兼容。作为一种开放的身份验证标准，OATH 确保了不同的身份验证供应商之间的互操作性。选择与 OATH 兼容的解决方案为您提供更多令牌设备的选择以及与不同系统的互操作性。

员工在没有受过基本安全培训的情况下进行远程办公使得企业更容易受到网络犯罪分子的攻击。而且远程办公人数众多，所以对于企业来说，部署多因子身份验证势在必行。

原文名称	Why you should be rushing to deploy multi-factor authentication to support remote work ?
作者简介	丹 · 康拉德（Dan Conrad）。丹 · 康拉德是 One Identity 公司的安全专家。
原文信息	2020 年 5 月 5 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2020/05/05/deploy-multi-factor-authentication/
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。