安天发布《AbSent 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 COVID-19 为主题的钓鱼邮件传播 AbSent 窃密木马活动。AbSent 是一款具有反调试、反虚拟机和反沙箱检测的窃密木马。该窃密木马主要通过钓鱼邮件进行传播，目的是窃取用户个人信息。

该活动通过钓鱼邮件进行传播，附件中包含一个伪造成文档的可执行文件，该可执行文件一旦执行便会连接 C2 下载并运行 AbSent 窃密木马，该窃密木马将自身复制到 % TEMP % 路径下并重命名为 winsvchost.exe，创建计划任务达到持久性的目的。AbSent 窃密木马每 15 分钟与 C2 进行一次连接保持心跳。AbSent 窃密木马主要功能包括远程桌面控制、键盘记录、收集主机信息、获取进程路径、获取浏览器 Cookie 信息、上传可能包含敏感信息的文本文件、获取进程列表、结束指定进程、获取屏幕截图以及打开 CMD 等。

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。

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。

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、关联分析鉴定器、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、来源信息鉴定器、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、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	4d2207059fe853399c8f2140e63c58e3
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1023 KB
MD5	4D2207059FE853399C8F2140E63C58E3
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.ZedoPoo
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	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
检测自身是否被调试	★★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
读取自身	★★
自我复制	★★
获取计算机名	★
检索系统内存信息	★
获取系统信息（处理器版本、处理器类型等）	★
获取驱动器类型	★
添加计划任务	★★

◆衍生物分析

文件名	文件 MD5	家族相似性	yara 扫描
b23724855af6b07f_winsvchost.exe	4d2207059fe853399c8f2140e63c58e3	N/A	N/A

◆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 6 月 8 日 (总第 233 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

关注行业动态，聆听两会声音

5 月 28 日，两会落下帷幕，备受瞩目的《2020 年国务院政府工作报告》出炉，明确今年将重点支持“两新一重”（新型基础设施建设，新型城镇化建设，交通、水利等重大工程建设）建设。

“要加强新型基础设施建设，发展新一代信息网络，拓展 5G 应用，建设充电桩，推广新能源汽车，激发新消费需求、助力产业升级。”对于新型基础设施建设，网络安全已经从保障环节发展为必需的支撑要素。

今年的两会上，来自网络安全和信息化的代表、委员聚焦新兴基础设施建设，由疫情引出的网络安全应急保障问题出发，带来相关议案、提案。关注行业动态，聆听两会声音，让我们一起回顾一下今年两会的相关议案、提案。

聚焦“新基建”

全国人大代表、腾讯董事会主席兼首席执行官马化腾：

马化腾今年计划向两会提交七份书面建议，涉及产业互联网、乡村振兴、金融科技、医疗服务与医生获得感、中小微企业发展、区域发展、生态环保等热点问题。

其中，他提出了六项加快推进产业互联网建设的举措和建议：包括加强顶层设计，制定系统推进产业互联网发展的国家战略；加快推进云计算等新基建，筑牢数字经济发展的战略基石；以“数据中台”建设为重点和突破口，进一步推动数据开放共享，提高数字化治理水平；持续推进开源协同创新生态，打造产业互联网“朋友圈”，提升科研创新数字化水平，同时加大产业安全投入。

此外，更完善的网络信息安全体系是数字经济的高质量发展的基础，马化腾建议，要加大安全人才培养、核心技术突破、安全生态协同，充分发挥网络信息安全在数字经济建设中的核心保障价值，建设以产业为中心的、原生的、主动规划为特征的新型“产业安全”体系。

全国人大代表、联想集团董事长兼 CEO 杨元庆：

今年，杨元庆围绕建设新一代互联网医疗健康平台、推动新基建和智慧经济建设、加强教育信息化基础设施建设助力脱贫攻坚、5G+ 工业互联网等，向两会提交六份提案。

在 5G+ 工业互联网方面，杨元庆建议，加大智慧基建力度，支持民营企业积极参与各地工业互联网、5G、智慧城市等数字基础设施建设，提升公共服务能力，加速培育复合型人才，加强新学科建设，适当增加相关专业招生名额，同时加大高端人才引进力度，实现产业人才集聚。

互联网医疗方面，杨元庆称，中国近年来持续推行“互联网 + 医疗”，但信息技术与医疗健康的深度融合还不足。对此，杨元庆建议，加快建设覆盖“家庭 + 社区 + 医院 + 科研机构”的新一代互联网医疗健康平台，依托互联网、大数据、人工智能等新一代信息技术，打破医疗健康领域现有行业条块壁垒，为患者提供全生命周期的“互联网 +”医疗健康服务。

同时，杨元庆对于今年热门话题新基建建议，应大力发展以“新基建”为基础的智慧经济，稳定全球供应链产业链，以实现“中国制造”的“产业跃迁”。

全国政协委员、百度董事长李彦宏：

李彦宏的四份提案包括个人信息保护、构建人工智能新型基础设施、加快智能交通基础设施建设和鼓励继续教育。

在新基建方面，李彦宏提出构建人工智能新型基础设施，勾画智能经济发展蓝图的提案。他表示，国家应加快打造具备国际领先水平的人工智能新型基础设施，加强人工智能基础和应用人才培养，推进各行业积极应用自主可控的开源深度学习平台。同时，还应大力推进智能云工程，支持开放平台的建设，以此加速产业智能化。

在交通方面，李彦宏提出加快智能交通基础设施建设，助力交通强国战略的提案。他建议国家应加强政策引导，鼓励各地政府加大探索和投入，以及建设全国性的新一代智能交通治理平台，加快形成安全可靠的现代化交通治理体系。

在教育方面，李彦宏认为疫情加速产业结构调整的同时将重塑人才结构，应鼓励各行业从业人员通过继续教育丰富能力，适应经济发展趋势。

关于个人信息保护，李彦宏表示，针对新冠肺炎疫情期间采集的个人信息设立退出机制，加强对已收集数据的规范性管理，研究制定特殊时期的公民个人信息收集、存储和使用的标准和规范。

聚焦“网络安全保障”

全国政协委员、安天创始人、首席架构师肖新光：

新冠疫情的爆发使得社会运行高度依赖互联网基础设施，远程办公成为普遍模式，导致重要的信息资产暴露面增加，防御难度加大。肖新光今年的提案重点关注网络安全应急能力，立足于应对重大社会风险综合应急保障需要，国家相关部门应完善重大社会风险协同研判指挥机制等。

面对网络空间风险程度和关联影响呈现动态变化的特性，肖新光认为，当前我国对网络安全与各种传统安全、非传统安全的渗透转化机理的研究不够深入、系统，重大社会风险研判中对网络安全维度重视程度不够，对“敌情想定”认识不足，联席研判机制需要完善。其次，应对网络空

（下转第三版）

每周安全事件

类 型	内 容
中文标题	Trickbot 通过钓鱼邮件分发 BazarBackdoor 后门
英文标题	Trickbot Using BazarBackdoor to Gain Full Access to Targeted Networks
作者及单位	David Bisson
内容概述	安全研究人员观察到，Trickbot 操控者使用了一种名为“BazarBackdoor”的新后门，以获得对目标网络的完全访问权。Panda Security 解释说，Trickbot 试图通过鱼叉式网络钓鱼活动分发“BazarBackdoor”。攻击邮件利用了员工解雇通知、客户投诉和其他主题，诱使收件人点击位于谷歌文档上托管文件的链接。这些链接将受害者重定向到一个网站，该网站通知收件人他们需要直接下载文件才能正确查看文件。下载后，文档运行隐藏的可执行代码以调用加载程序。
链接地址	https://securityintelligence.com/news/trickbot-using-bazarbackdoor-to-gain-full-access-to-targeted-networks/

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	名称与发现时间	威胁等级	简要描述
活跃漏洞	Microsoft SharePoint 安全漏洞（CVE-2020-0920）	高	当 Microsoft SharePoint 无法检查应用程序包的源标记时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器帐户的上下文中运行任意代码。
	Microsoft Windows 和 Windows Server 安全漏洞（CVE-2020-1166）	高	当 Windows 不正确地处理对剪贴板服务的调用时，存在特权提升漏洞。成功利用此漏洞的攻击者可以在本地系统的安全上下文中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	Microsoft Windows Graphics Components 安全漏洞（CVE-2020-1153）	高	Microsoft 图形组件在内存中处理对象的方式中存在远程代码执行漏洞。成功利用该漏洞的攻击者可以对目标系统执行任意代码。若要利用该漏洞，攻击者需要诱使用户打开一个特制的文件。
较为活跃样本家族	Trojan/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	Trojan[Backdoor]/Win32.Wabot	中	此威胁是一种带有后门的木马类家族。该家族样本运行后，会添加注册表启动项，并将自身设置为隐藏、只读属性。该家族会为黑客打开后门，允许黑客窃取用户的信息。
	Trojan/Win32.Miancha	中	此威胁是一种收集用户击键信息的木马家族。该家族样本运行后连接远程服务器，收集用户信息上传至远程服务器，造成用户敏感信息泄露。
	Trojan[Backdoor]/Linux.Gafgyt	中	此威胁是一种 Linux 平台上的具有 DDoS 攻击功能的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作。
	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。
	Trojan[Spy]/Android.SmForw	中	此威胁是安卓平台上一种间谍类木马家族。该家族样本运行后，长久驻留系统，持续监控用户，收集用户系统信息，造成用户隐私泄露。

（上接第一版）

间的威胁行为中缺少网络应急人员规模化战备组织机制，可紧急动员、 统一指挥的弹性人员力量有限。

他建议以总体国家安全观为指引，充分考虑网络安全作为最典型的非传统安全的规律特点，在加强网络安全防御公共基础设施建设和提升政企机构网络安全防护能力的同时，完善重大社会风险协同研判指挥机制、建立政企结合、军民融合的网络安全应急与战备人员组织机制、建立网络安全技术装备和战备物资分级战略储备和运维机制。

此外，他还建议相关部委在机制流程、人员编制、经费预算等方面对建议实施予以专项保障，形成实战化演训体系，确保体系、人员和装备始终保持高水平实战化能力。

全国政协委员、原证监会信息中心主任张野：

张野今年带来的 3 个提案之一是“提高我国网络安全应急处置能力”。

他表示，由于我国网络安全基础薄弱，导致了网络攻击猖獗，难以实现有效的持续监控，供应链受制于人，网络安全信息收集、研判仍然分散，时效性较差，网络安全事件处置中资源协调调配效率较低，亟需对现有网络安全建设成果进行整合、统筹利用，建立统一的指挥调度系统，构建有效的网络安全防护处置体系，形成快速处置反应能力和网络威慑能力。

具体的研究建设中，张野认为，网络安全事件的发生具有传播快、影响范围广、需分析溯源等特点，在很多方面可以借鉴传染疾病的防控措施和手段。由于我国在公共安全领域的应急体系建设已经比较完备，《国家物资储备管理规定》等相关法律规章对物资储备、使用等也有明确的规定，因此，配套制定网络安全处置应急征用办法可以借鉴我国在公共安全领域的应急体系，特别是医疗卫生应急体系的建设经验。

全国政协委员、启明星辰董事长 严望佳：

严望佳今年的提案涉及人工智能、工业互联网、车联网、环境保护等多个方面。

她在“关于推动人工智能赋能工业互联网安全发展的提案”中表示，为了进一步加强对工业互联网的安全保障，确保其成为驱动工业生产发展和社会价值提升的可靠力量，应在大力推动工业互联网技术应用部署的同时注重与之相匹配的网络安全防御保障技术的研发，推动人工智能赋能工业互联网安全发展。

除此之外，她在“关于推进智能车联网安全风险评估的提案”中针对智能车联网进行常态化信息安全风险评估和车辆信息安全检测分析，保护智能车联网及交通安全提出了 7 点建议。

全国政协委员、360 集团董事长兼 CEO 周鸿祎：

今年两会，周鸿祎提交了四份提案，分别是“尽早构建新基建网络安全防护体系”“尽快制定《国家 5G 安全战略》”“加强信创网络安全保障能力建设”“加快推进工业互联网安全保障”。

关于构建新基建网络安全防护体系，周鸿祎提出了提出 4 点建议：运用整体思维，规划新基建网络安全防护体系顶层设计；同步建设新基建的安全基础设施，聚焦新基建安全防能力构建；强化大数据平台安全，实现安全的大数据协同计算；开展常态化网络安全攻防对抗演习，持续检验和提升新基建安全能力。

关于加快推进工业互联网安全保障，他建言加快推进工业互联网安全保障建设，为国家实体经济和社会保驾护航。

关于加强信创网络安全保障能力建设，他表示，信息技术创新应用作为我国信息技术领域打造自主创新生态的国家战略举措，也是新基建的重要抓手。

微信扫描二维码阅读原文

Trickbot 通过钓鱼邮件分发 BazarBackdoor 后门

安全研究人员观察到，Trickbot操控者使用了一种名为“BazarBackdoor”的新后门，以获得对目标网络的完全访问权。Panda Security解释说，Trickbot试图通过鱼叉式网络钓鱼活动分发“BazarBackdoor”。攻击邮件利用了员工解雇通知、客户投诉和其他主题，诱使收件人点击位于谷歌文档上托管文件的链接。这些链接将受害者重定向到一个网站，该网站通知收件人他们需要直接下载文件才能正确查看文件。下载后，文档运行隐藏的可执行代码以调用加载程序。

（原文链接：https://securityintelligence.com/news/trickbot-using-bazarbackdoor-to-gain-full-access-to-targeted-networks/）

NASA IT 承包商遭 DopplePaymer 勒索软件攻击

DopplePaymer勒索软件的操控者祝贺SpaceX和NASA首次载人火箭发射，然后立即宣布他们成功侵入了NASA的一个IT承包商Digital Management Inc. (DMI)的网络。目前尚不清楚DopplePaymer团伙入侵DMI网络的深度，以及他们成功入侵了多少客户网络。为了证明，DopplePaymer的操控者在该团伙运营的一个暗网网站上发布了20个存档文件。此外，DopplePaymer团伙还发布了一份包括2583台服务器和工作站的名单，黑客声称这些服务器和工作站是DMI内部网络的一部分，他们已经对其进行了加密，现在正勒索赎金。

（原文链接：https://www.zdnet.com/article/ransomware-gang-says-it-breached-one-of-nasas-it-contractors/）

研究人员发现 Cycldek 小组使用新的恶意软件

新发现的 USBCulprit 恶意软件是名为 Cycldek 的 APT 武器库的一部分，该工具针对政府实体。根据卡巴斯基的分析，Cycldek(又 名 Goblin Panda、APT 27 和 Conimes) 自 2013 年以来一直将目标对准东南亚各国政府，并一直在逐步增加更复杂的工具。该公司表示，就 USBCulprit 而言，已针对越南，泰国和老挝的目标进行了部署。卡巴斯基在周三发布的研究报告中称：“它拥有横向移动 (通过网络获取目标数据的能力) 和数据窃取能力。”

（原文链接：https://threatpost.com/info-stealer-air-gapped-devices-usb/156262/）