安天发布《GoldBrute 僵尸网络分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 GoldBrute 的僵尸网络开始活跃，GoldBrute 通过传统的 RDP 爆破方式进行传播，对全球超过 150 万个设备进行扫描，被该病毒感染的主机会受 C&C 服务器 104.156.249.231 操控，僵尸网络之间的通信交流则通过端口 8333 进行。

首先，被控端通过扫描互联网找到那些暴露了 RDP 的 Windows 主机，一旦找到暴露了 RDP 的主机，受控端便会向 C&C 服务器报告，如果累计达到了 80 台主机，那么 C&C 服务器将分配一个目标来发动暴力攻击，并且每个受控端只对目标尝试一个用户名和密码，每次身份验证尝试都来自不同的地址，以避免被检测到。一旦攻击成功，它就会下载一个带有 Java 环境的压缩文件，解压缩后运行一个名为“bitcoin.dll”的 jar 文件，然后新的受控端开始扫描互联网上开放的 RDP 服务器，如果发现新的暴露了 RDP 的 Windows 主机，那么它将继续报告给 C&C 服务器，如果累计依旧达到了 80 台主机，那么 C&C 服务器就会启用暴力破解 RDP 服务器，在暴力破解阶段，受控端不断从 C&C 服务器获取用户名和密码组合进行破解。

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。确保所有的计算机在使用远程桌面服务避免使用弱密码，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类恶意代码的鉴定；安天智甲已经实现了对该恶意代码的查杀。

黑客工具

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述黑客工具进行有效检测，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、元数据信息鉴定器、动态（Win7 x86）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黑客工具。

◆ 概要信息

文件名	af07d75d81c36d8e1ef2e1373b3a975b9791f0cca231b623de0b2acd869f264e
文件类型	Archive/Sun.JAR[:Java ARchive]
大小	17.78 MB
MD5	EF6CAC1E56AC78559E23716CBDA7229B
病毒类型	黑客工具
恶意判定 / 病毒名称	HackTool/Java.RDPBrute
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=EF6CAC1E56AC78559E23716CBDA7229B

◆ 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

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	137	192.168.122.255	137
192.168.122.155	138	192.168.122.111	138
192.168.122.111	138	192.168.122.255	138
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.111	123	40.74.70.63	123
192.168.122.111	137	192.168.122.155	137

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1032	192.168.122.155	139

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 06 月 24 日 (总第 188 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

哈工大、莫斯科钢铁合金学院、安天共建“阿斯图中俄信息安全联合研究中心”

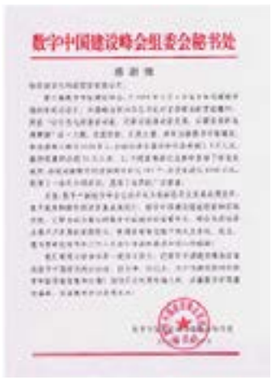
近日，由中国教育部、黑龙江省人民政府指导，教育部学校规划建设发展中心主办，黑龙江省教育厅、哈尔滨工业大学、黑龙江大学承办的 2019 国际产学研用合作会议（哈尔滨）在哈尔滨万达嘉华酒店成功举办，来自哈尔滨工业大学、中国科学技术大学、浙江大学，俄罗斯莫斯科鲍曼国立技术大学、白俄罗斯国立大学、乌克兰材料问题研究所等中外高校、科研机构以及华为、腾讯等企业的 200 多位学者和工程技术专家一同参与本次会议。

会议现场举行了系列签约仪式，哈尔滨工业大学、莫斯科钢铁合金学院、安天集团三方共同签署战略合作协议，携手共建阿斯图中俄信息安全联合研究中心。

莫斯科钢铁合金学院是俄罗斯冶金教育和研究领域最好的大学，在半导体制造等领域也具有雄厚基础，在应用数学等基础领域功底扎实。哈尔滨工业大学是国家 985 重点院校，在信息安全领域成果卓著。在后续三方合作中，安天将与哈工大、莫斯科钢铁合金学院共同加强工业基础设施信息安全相关研究，依托自身的基础工程能力和威胁分析研究积累，持续提供平台资源和工程能力支撑，助力联合研究中心形成具有前瞻性和在工业场景中具有实用前景的高水平科研成果，并推动安全价值的有效转化。安天将充分发挥企业在科技成果转移转化中的重要作用，促进优势互补、共赢发展，积极参与共同构建中俄乌白产学研用国际合作交流新格局，服务国家和区域创新驱动发展。

安天获数字中国建设峰会组委会感谢信

近日，安天收到来自第二届数字中国建设峰会组委会秘书处发来的感谢信，信中对参与本次峰会安保工作的安天工作人员表示了感谢。



第二届“数字中国”建设峰会由国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、福建省人民政府共同主办，安天作为引领威胁检测与防御能力发展的网络安全国家队为峰会提供专业的网络安全保障服务，助力此次峰会的顺利进行。

安天以“达成客户有效安全价值，提升客户安全获得感，改善客户的安全认知”为企业纲领，已连续五届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一。

在本次峰会中，安天积极与各友商合作，共同赋能客户，为峰会提供了全天候的恶意代码安全监测能力与应急响应处置的有力保障。

大规模钓鱼活动针对德国多行业安装 Remcos

Check Point 的研究人员在 6 月初发现针对德国所有行业公司的新大规模网络钓鱼活动，目标是在受害者计算机上安装远控工具 Remcos。电子邮件伪装成来自德国各地的几家合法公司，包含主题为发票或紧急订单附件，扩展名为“，PDF”，实际为可执行文件，运行后 Remcos 将静默执行并允许攻击者完全控制受害者的计算机。攻击者使用 DDNS（动态 DNS）掩盖与 C2 的通信。

Ryuk 勒索软件新变种添加 IP 和计算机名称黑名单

研究人员发现了使用数字证书签署的 Ryuk 勒索软件新变种，其添加 IP 和计算机名称黑名单，以跳过匹配计算机，免受加密。该变种通过 arp -a 命令输出检查 IP 地址，还将计算机名称与字符串“SPB”、“Spb”、“spb”、“MSK”、“Msk”和“msk”进行比较，如果具有匹配值则不加密。研究人员表示该种行为可能是避免加密俄罗斯的计算机。

Oracle 为 WebLogic 中远程代码执行漏洞发布补丁

Oracle 针对 WebLogic 服务中的一个关键远程代码执行漏洞发布了紧急补丁。该漏洞为 CVE-2019-2729，是 Oracle WebLogic web 服务中 XMLDecoder 可远程利用的反序列化漏洞，攻击者无需身份验证即可远程利用。该漏洞 CVSS 评分为 9.8，影响 WebLogic 版 本 10.3.6.0.0、12.1.3.0.0 和 12.2.1.3.0。由于此漏洞的高严重性，建议用户尽快进行补丁更新。

每周安全事件

类 型	内 容
中文标题	研究人员发现针对中东的移动网络间谍活动
英文标题	Mobile Cyberespionage Campaign ‘Bouncing Golf’ Affects Middle East
作者及单位	Mobile Threat Response Team
内容概述	趋势科技研究人员发现了针对中东国家的移动网络间谍活动“Bouncing Golf”。恶意代码嵌入到被重新打包的合法应用程序中，托管在网站上，通过社交媒体进行推广。最终传播 Android 恶意软件 GolfSpy，GolfSpy 具有信息窃取和执行远程命令功能。研究人员通过监控其 C2，目前已经观察到超过 660 台感染了 GolfSpy 的 Android 设备。被窃取的信息多数与军事有关。该活动与之前报道过的“Domestic Kitten”活动有关，二者具有相似的代码串的结构和盗窃的数据格式。
链接地址	https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/

每周值得关注的恶意代码信息

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.rima.a[prv,rmt,spy] 2019-06-17	高	该应用程序是一款间谍软件，伪装谷歌云服务，后台接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置、浏览器记录、手机存储文件信息等大量隐私信息，监听用户短信和通话，私自拍照、录音、录像、截屏，并将用户隐私上传至服务器。造成用户隐私泄露，建议立即卸载。
		Trojan/Android.Ervadark.a[prv,rmt,spy] 2019-06-18	高	该应用程序运行后隐藏图标，接收远程指令，上传用户短信、联系人、通话记录、照片、app 列表、银行卡等隐私信息，还会执行发短信、下载安装未知应用、照相、录音等危险行为，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.FakeGoogleSys.h[prv,rmt,spy] 2019-06-19	高	该应用程序包含风险代码，运行上传用户手机信息，接收网络远程指令，上传用户服务提供商的信息、登录信息、验证码图片，获取订阅信息并私自订阅，造成用户隐私泄露和资费消耗，建议卸载。
	较为活跃样本	G-Ware/Android.FakeApp.gl[exp,rog]	中	该应用程序伪装正常应用，无实际功能，运行隐藏图标，后台推送广告，会造成用户流量资费损耗，请卸载。
		Trojan/Android.haoapp.a[prv,spy]	中	该应用程序运行后隐藏图标，窃取用户通话记录、屏幕截屏，私自拍照，录像，并将用户隐私上传。造成用户隐私泄露，建议卸载。
		Trojan/Android.FakeFB.ac[prv,exp]	中	该应用程序伪装成 Facebook，诱导用户输入账号密码，通过联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗。建议立即卸载。
		RiskWare/Android.SexApp.bq[rog,exp]	低	该应用程序运行访问色情网站，其内容可能影响用户身心健康，请注意提示信息，使用绿色软件。
		Trojan/Android.FakeInst.fj[pay]	低	该程序伪装色情视频应用，本身无实际功能，私自发送付费短信，可能造成用户资费损失，建议立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Word 远程代码执行漏洞（CVE-2019-0953）	高	当 Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。攻击者可通过向用户发送经特殊设计的文件，并诱使用户打开该文件利用此漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。
	较为活跃样本	RiskWare[Downloader]/Win32.Express	中	此威胁是一种具有下载行为的风险类程序。该家族会自动下载并运行未经用户不知情或不允许安装的软件，同时它也可以不断地检查更新文件本身。
		GrayWare[AdWare]/MSIL.OutBrowse	中	此威胁是一种用 MSIL 语言编写的灰色软件程序。该家族运行后，会在用户浏览网页时弹出广告，还可以重定向用户的搜索结果、监测用户行为、在系统中下载应用程序并运行，并将用户信息发送给黑客。该家族通常放置在程序网站上，或与一些第三方软件的安装程序捆绑在一起。
		RiskWare[WebToolbar]/Win32.Rubar	低	此威胁是一种可以安装浏览器扩展的风险软件家族。一种用于 IE 工具栏通常位于菜单栏下方的表格的顶部。工具栏可以由浏览器帮助对象被创建。它们允许恶意软件程序来监控网络活动。
		GrayWare[AdWare]/NSIS.AGeneric	低	此威胁是一种有广告行为的灰色软件家族。该家族通过 NSIS 打包，该家族没有统一的行为与功能，是以启发式检出的恶意代码。
		GrayWare[AdWare]/Win32.Bromngr	低	此威胁是一种广告类的灰色软件程序。该家族样本运行后会劫持浏览器，在浏览器（IE、火狐、谷歌）插件中加入支持广告功能。

保护新的、多样的网络边缘设备

John Maddison/ 文 安天技术公益翻译组 / 译

网络边缘正在迅速发展。这对 IT 团队提出了新的要求，以确保系统和数据的安全，同时又不会影响其性能。

网络边界已经被一系列边缘网络环境和设备所取代。这些环境和设备或者并非企业所有，如云基础设施，“软件即服务”（SaaS）应用或用户所有的移动设备；或者不再依赖于监测流量以进行检查的“星型”（hub-and-spoke）连接模型。IT 团队面临的挑战在于确保这些环境之间的一致性——尤其是当 DevOps 和 Web 团队向不同的业务线报告时。

保护所有边缘设备的安全

首先，企业需要部署根据开放标准构建的安全解决方案，以便查看其他设备（无论设备是何种形态或部署在分布式网络的哪个位置），共享和关联威胁情报，以及参与协调响应。

此外，这些解决方案还需要适应当今新边缘环境的独特要求。

多重云平台

不同的云平台具有其独特的控制和管理接口，需要配置专门的安全解决方案才能本地运行。但是，在云环境中本地运行的安全工具，可能会遇到与在其他平台上本地运行的版本互操作的挑战。作为覆盖解决方案部署的安全设备可能会丧失其功能，导致难以实现一致的策略。

为了应对这一挑战，IT 团队需要选择能够跨各种云平台本地运行的安全解决方案，包括跨网络环境实现一致的策略编排和实施的连接器。

影子 IT 应用

用户在网络中部署的应用通常比 IT 团队知道的多 15 倍。（译者注：此数据来源于 Securing Today’s New and Varied Network Edges 一 文，原 文 链 接 https://www.networkcomputing.com/network-security/securing-today%E2%80%99s-new-and-varied-network-edges）

安全解决方案需要识别这些“影子 IT”（译者注：Shadow IT，影子 IT 是指未经企业统一，而在企业内建立和使用的 IT 系统和解决方案）应用；确保关键的工作流程、数据以及应用由安全、受监控的网站处理，而不是哪些不安全、未被监控的网站来处理。

物联网设备

绝大多数物联网（IoT）设备都有固有的不安全性，有的甚至无法更新或打补丁，这就是为什么它们沦为了网络犯罪分子的首选目标。

安全解决方案需要在访问设备时动态识别它们，应用策略和分段规则，并在分布式网络中共享这些策略。

移动员工设备

单个用户同时将多台设备连接到网络的情况并不罕见。这些用户还经常将个人和公司数据、应用和配置文件混合到同一台设备上，使企业面临风险。

针对端点设备的全面安全策略需要涵盖 VPN 解决方案、网络访问控制和分段解决方案、与网络策略相关的端点安全解决方案，以及可以自动保护连接并远程擦除设备驱动器的移动设备管理（MDM）解决方案。

生产设备

随着 IT 和生产（OT）网络的融合，攻击面大大扩展，而且每个环境都面临来自另一个环境的新风险。在 OT 方面，新部署的 IT 解决方案连接了原本隔离的设备和资源，使这些设备和资源面临威胁。此外，脆弱、老化的解决方案通常包含可利用的漏洞，而攻击者通常利用这样的平台来发动攻击。

保护 OT 边缘需要采用“零信任”模型，即在 OT 和 IT 网络之间建立安全控制，并部署访问控制和分段策略，以保护脆弱或高风险的应用、设备和控制系统。

广域网设备

分支机构的星型模型已经退出舞台，而新的“软件定义的分支”（SD-Branch）则允许远程位置作为扩展广域网（WAN）的完全集成组件运行。许多分支机构有自己的局域网（LAN），包括固定和移动设备、IoT、云连接和多个公共互联网链路，因此企业的解决方案需要支持 LAN-WAN-LAN 环境的复杂组合。

要想保护 WAN 边缘，企业需要一种通过“零接触”部署模型轻松移入和跨越所有这些环境的安全解决方案。SD-WAN 解决方案需要一套完全集成的安全工具，以便将一致的安全功能、性能和实施扩展到远程位置，然后与本地分支 LAN 无缝互操作。

新兴 5G 设备

5G 有望实现联网汽车、智慧城市和边缘网络。在 5G 环境中，设备可以共享关键信息，接收丰富的媒体流，运行数据量庞大的应用并做出实时本地决策。

这需要将安全策略迁移到边缘，并将其嵌入边缘网络和 IoT 设备中，以避免往返进行数据检查和策略决策。

实施新一代安全方案的时机已到

第二代安全解决方案已经无法再保护企业的安全，企业需要部署为当今的数字市场设计的第三代安全方案。该方案具备高性能、高适应性、跨设备和跨平台的互操作性，以及自学习功能，不仅能实时查看和响应威胁，还能在威胁发生之前加以预测。该方案将使企业自配置、自操作、自学习、自调整和自纠正其安全状态，以成功抵御不断扩大的攻击面。

原文名称	Securing Today’s New and Varied Network Edges
作者简介	John Maddison。John Maddison 是 Fortinet 公司产品和解决方案执行副总裁。
原文信息	2019 年 6 月 11 日发布于 Network Computing 原文地址 https://www.networkcomputing.com/network-security/securing-today%E2%80%99s-new-and-varied-network-edges
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。