安天发布《Anatova 勒索软件分析报告》

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名为 Anatova 的新型勒索软件木马。该木马由经验非常丰富的作者编写，采用 RSA+Salsa20 的方式加密，中招后想自行解密的概率非常低，并且它还预留了模块化扩展功能，这在未来可能演变成巨大威胁。

Anatova 使用游戏或应用程序图标来伪装自己欺骗用户下载，运行时会申请管理员权限，然后对用户文件进行快速加密，并要求用户支付 10 DASH 加密数字货币（约 700 美元）来解密文件。木马运行时会动态生成一个 RSA 密钥对，并随机生成一个 32 位密钥和 8 比特字节作为加密算法的 Key 和 IV，使用 Salsa20 算法对文件加密。在整个加密过程中，程序会解密一段来自攻击者的 RSA 公钥，用它对之前动态生成的密钥进行加密，将结果进行 Base64 编码后写入勒索信中。随后清除内存缓冲区域，防止有人从内存中恢复密钥信息。Anatova 会搜索所有逻辑磁盘和远程共享磁盘，因此可能感染整个网络。为了快速加密，它只会加密文件的前 1MB 字节。加密完成后，还会快速删除卷影副本 10 次，用户将难以通过系统还原来恢复文件。

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、数据证书鉴定器、文件元数据鉴定器鉴定器、聚类分析鉴定器、防病毒引擎鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）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	170fb7438316f7335f34fa1a431afc1676a786f1ad9dee63d78c3f5efd3a0ac0
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	307 KB
MD5	596EBE227DCD03863E0A740B6C605924
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win64.Anatova
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=596EBE227DCD03863E0A740B6C605924

◆ 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	1026	192.168.122.1	53
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1026
192.168.122.1	53	192.168.122.111	1025
0.0.0.0	68	255.255.255.255	67
192.168.122.155	138	192.168.122.111	138
192.168.122.111	123	52.173.193.166	123
192.168.122.111	137	192.168.122.255	137
192.168.122.111	137	192.168.122.155	137
192.168.122.111	138	192.168.122.255	138
192.168.122.1	67	192.168.122.111	68

◆ TCP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1035	120.92.59.191	80
192.168.122.111	1036	192.168.122.155	139
192.168.122.111	1027	120.92.59.191	80
192.168.122.111	1028	114.112.66.35	80

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 02 月 25 日 (总第 172 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

中央统战部副部长全国工商联党组书记徐乐江一行莅临安天参观指导

近日，中央统战部副部长、全国工商联党组书记徐乐江率考察组一行莅临安天参观指导，安天技术负责人进行了汇报。

在汇报中，安天技术负责人向来宾介绍了安天的发展历程、现状以及技术分布，展示了安天在网络安全领域取得的各项资质和荣誉，并对安天威胁检测引擎的覆盖情况进行了说明。在安天安全研究与应急处理中心，考察组观看了安天赛博超脑靶场的现场演示与实时工作情况，安天技术负责人对安天持续与网络安全威胁对抗的情况进行了汇报，重点介绍了安天针对“APT-TOCS（海莲花）”、“白象”等攻击组织对我方 APT 攻击情况、所使用的攻击装备等的分析进展。同时，安天负责人向徐乐江等领导汇报了集团近几年的党建工作情况。

在听取了各项工作汇报后，徐乐江等考察组领导对安天多年来的艰苦创业经历和取得的荣誉给予了肯定与赞赏，同时也表达了对安天的鼓励与期望，希望安天牢记总书记的指示，不忘初心和使命，在网络安全领域继续奋进。

WinRAR 存在长达 19 年的严重安全漏洞

安全团队发现并公布了存在于 WinRAR 中长达 19 年的严重安全漏洞。WinRAR 对 ACE 格式文件的支持，代码主要存在于 unacev2.dll 文件中，但是 unacev2.dll 使用的仍是 2006 年没有保护机制的旧版 dll 文件，而且其中针对 ACE 文件头结构中“filename”字段处理也出现了问题，再加上过滤函数问题和对目标路径的错误解析（CVE-2018-20250、CVE-2018-20251、CVE-2018-20252 和 CVE-2018-20253），导致攻击者可以自由决定文件释放路径，如将可执行文件释放到 Windows 系统的 Startup 目录中，那么下次 Windows 启动运行将会自动执行该程序，从而导致代码执行的安全问题。该漏洞影响 WinRAR 5.70 Beta 1 之前所有版本，建议用户尽快更新至 WinRAR 5.70 Beta 1 或以上版本。

（来源：https://research.checkpoint.com/extracting-code-execution-from-winrar/）

品牌冒充将成为最常见的网络钓鱼攻击形式

最新报告指出，品牌冒充将成为黑客最常用的网络钓鱼攻击形式。品牌冒充攻击是一种网络钓鱼攻击形式，攻击者假装来自受信任的品牌或公司，并向其目标受害者发送恶意电子邮件。该攻击形式占 2018 年第四季度记录的高级电子邮件攻击的 50%，其中 70% 是通过冒充微软来实现。黑客使用以下三种方式继续攻击：购买类似于知名品牌的域名；冒充合法 URL；使用伪造来源的电子邮件地址。

（来源：https://cyware.com/news/heres-a-close-view-of-brand-impersonation-attack-that-is-increasingly-gaining-popularity-among-the-hackers-b9584884）

分析显示 7 成银行未准备好应对网络攻击

Group-IB 基于 2018 年安全事件，对高科技网络犯罪进行了分析。分析显示，黑客仍然以金融业为目标，而 74% 的银行尚未准备好应对网络攻击，29% 的银行有活跃的恶意软件感染，52% 的案例中存在重复感染，包括“连锁反应”的跨境袭击，导致金融机构多次感染。超过 60% 的银行无法集中管理其网络，特别是在地理位置分散的基础设施中，大约 80% 的金融机构对于超过一个月的事件，没有进行深度日志记录，超过 65% 的金融机构协调部门之间的工作效率低。与 2017 年相比，事件总数增加了一倍以上，活动类型包括针对性攻击、间谍活动、勒索软件攻击、挖矿。

（来源：https://securityaffairs.co/wordpress/81341/cyber-crime/russian-banks-cyber-attacks.html）

每周安全事件

类 型	内 容
中文标题	美国军方发布五角大楼人工智能战略计划
英文标题	What the Pentagon’s new AI strategy means for cybersecurity
作者及单位	Justin Lynch
内容概述	2月12日，美国军方发布新五角大楼人工智能战略计划，该战略显示美国军方将如何依靠人工智能作为防御工具。战略中指出作为安全使用人工智能的先决条件，将把重点放在硬件和软件平台的防御性网络安全上；为了确保国防部人工智能系统的安全性、可靠性和稳健性，将资助对事故风险较低的人工智能系统的研究，包括防御黑客攻击和对抗性欺骗。新战略的一个重点是研究“紧急效应”，即当两个人工智能系统相互作用时会发生的情况。有研究人员表示，在网络攻击中使用人工智能是带有特殊风险的，五角大楼计划正试图打击其它国家对机器学习的重大投资。
链接地址	https://www.fifthdomain.com/dod/2019/02/13/what-the-pentagons-new-ai-strategy-means-for-cybersecurity/

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

关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.SexPay.j[exp,rog] 2019-02-18	该应用程序为色情应用，包含多个支付插件，运行后会频繁联网，私自发送支付信息，后台私自下载其它应用，造成用户资费消耗，同时影响用户身心健康，建议使用绿色健康软件。（威胁等级高）
		Trojan/Android.StealMMScreen.a[prv] 2019-02-19	该应用程序伪装色情应用，运行后会监听微信运行广播，私自截屏用户聊天信息、收付款界面，获取用户手机号码、固件信息并联网上传，会造成用户隐私泄露，危害用户财产安全，建议立即卸载。（威胁等级中）
		Trojan/Android.MalBus.a[prv,exp] 2019-02-20	该应用程序包含风险代码，运行后释放恶意so文件，私自下载恶意插件加载，诱导用户访问钓鱼界面并窃取用户Google账号密码，释放恶意代码，上传敏感文件，造成用户隐私泄露和资费损耗。（威胁等级高）
	较为活跃的样本	RiskWare/Android.FakeApp.ft[fra]	该应用程序伪装为其他应用，无实际功能，运行后会隐藏图标，存在一定风险，建议使用官方正版应用。（威胁等级低）
		RiskWare/Android.SmsSpy.ax[prv,rog]	该应用程序伪装为国家电网相关应用，包含风险代码，触发后可以执行获取用户短信、插入短信、发送短信、获取联系人等操作，会造成用户的隐私泄露，建议卸载。（威胁等级中）
		RiskWare/Android.bdpack.a[exp,rog]	该应用程序是一款在线刷量平台，运行后会请求root权限，通过用户操作，下载刷量脚本和刷量信息，会收集用户手机信息，存在一定风险，建议不要使用。（威胁等级中）
		Trojan/Android.BankerSpy.n[prv,rmt]	该应用程序伪装银行类应用，运行后会利用虚假银行类界面信息诱骗用户输入银行账号密码等相关隐私信息，然后联网上传，监听、拦截和上传短信信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		G-Ware/Android.FakeApp.fu[prv,rog]	该应用程序伪装其他应用，无实际功能，运行后会请求激活设备管理器，联网上传设备固件信息和位置信息，造成用户隐私泄露，建议卸载。（威胁等级低）
PC平台恶意代码	活跃的格式文档漏洞、0day漏洞	Microsoft Word 信息泄漏漏洞（CVE-2019-0561）	当未正确使用Microsoft Word宏按钮时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可以从目标系统中读取任意文件。（威胁等级高）
	较为活跃样本	RiskWare[RemoteAdmin]/Win32.WinVNC-based	此威胁是一种具有远程控制行为的风险软件家族。该家族的样本在执行后会让远程控制端可以通过VNC访问并控制自己的机器，可能对用户的设备造成潜在的安全危害。（威胁等级高）
		RiskWare[WebToolbar]/Win32.Webatla	此威胁是一种会安装浏览器扩展工具栏的风险软件家族。该样本的家族在运行后会在未经用户允许的情况下安装一个浏览器扩展工具栏。（威胁等级低）
		GrayWare[AdWare]/Win32.4Shared	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，在用户的PC上下载并弹出广告窗口。该家族的样本具有较多种签名形式和变种。（威胁等级低）
		RiskWare[WebToolbar]/Win64.SearchSuite	此威胁是一种在64位Windows平台上的、具有安装Web扩展工具栏行为的风险软件家族。该家族的样本在运行后会安装一个Web扩展工具栏，并且会连接网络下载其他的应用程序到用户的计算机中。（威胁等级中）
		GrayWare[AdWare]/Win32.InstallBrain	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本通过一些被修改过的软件安装程序所传播（例如Codec Pack等），在执行后会在用户的机器上弹出广告。（威胁等级低）

ICS/SCADA 攻击持续恶化

Kelly Jackson Higgins / 文 安天技术公益翻译组 / 译

随着攻击者的攻势更加猛烈和隐蔽，一些工业网络运营商开始努力对抗威胁。

关于工业互联网，有一个坏消息和一个好消息。坏消息是：在过去的一年中，针对工业网站的攻击更加猛烈了。好消息是：越来越多的工业控制系统（ICS）运营商正在采取更主动的防御措施，来对抗针对其网络的攻击。

本周，Dragos公司发布了2018年工业客户的ICS威胁调查报告。“此类威胁正在恶化，”该公司首席执行官兼联合创始人罗伯特·李（Robert M. Lee）说，“但是企业在对抗此类威胁方面也更加积极了。也许不仅是工业企业，其他企业也开始关注此类威胁了。一些真正具备前瞻性的公司已经迈向正确的方向。”

2018年，Drago公司进行了大量的事件响应（IR）。其中，在近40%的事件中，大约25%的事件响应是为了确定网络攻击是否是造成停电或其他事件的原因。

李指出，“现在，在发生工业事件后，企业至少会考虑是否是网络攻击。对他们来说，这是一个重大的进步。

李表示，“即便如此，目前北美只有约20%至30%的ICS企业通过实时网络监控来检测和阻止攻击。这是我们向ICS/SCADA企业推荐的最佳安全实践，而北美则领先于其他地区采用了这些实践。”

2018年，Dragos公司向客户提供的大部分服务是主动威胁猎杀（threat hunting）和网络基础设施映射：在所有服务中，33%是事件响应，其他的则主要是威胁分析、评估和桌面演习。

IT-OT 薄弱环节

渗透工业网络最简单的方法之一是利用其IT基础设施，这是一种常见的初始攻击向量。例如，通过成功的网络钓鱼和用户账户感染来创建据点，攻击者可以更好地访问ICS网络上的系统。

工业安全公司Claroty的威胁研究副总裁戴维·温斯坦（David Weinstein）表示，去年的ICS攻击趋势“没有太大变化”。“在过去的两到三年里，攻击者利用IT系统进入OT系统的确很有效，但并非总是如此。这是因为在以前，这些系统是相互独立的。”

李表示，更多的攻击组织正在瞄准工业网络。“我们看到了更多的数据泄露、攻击手段和受害者。”

攻击者最大的转变是，他们开始使用所谓的“靠山吃山”（living off the land）的方法，不过运作方式与在IT网络中并不相同。例如，他们并非执行远程桌面协议（RDP）类攻击，而是使用本地工业协议。

Dragos公司跟踪的威胁组织，大多采用此类伪装方法。此外，他们也开始使用合法的渗透测试工具，如Mimikatz、Metasploit和PowerShell Empire。

打补丁的难题

对于许多工业企业而言，“打补丁”还是“不打补丁”仍然是一个难题——去年发现的ICS漏洞和补丁的数量都有所增加。OT系统不同于IT系统，相比于放弃更新，有时候为OT系统打补丁会带来更大的破坏和风险。

“你必须了解攻击者如何利用这些漏洞并采用基于风险的修复方法。”李指出。

2018年，Dragos公司分析了约204个公开的ICS漏洞，发现82%的漏洞没有与ICS系统直接交互。李说，这是因为大多数漏洞研究都不关注ICS系统漏洞。在去年修复和披露的网络漏洞中，约34%是ICS漏洞；其他的则是典型的IT协议（如HTTP和FTP）漏洞。李说，这可能是因为研究人员缺乏ICS知识以及测试ICS协议的工具。

但从整体上看，去年在ICS系统中发现的漏洞，超过一半可用于执行危险的网络活动：“它们可能会导致企业失去对系统的可见性和控制，”李说。Dragos公司还发现，漏洞公告中的大部分缓解建议都不充分甚至完全不准确。

现实情况

根据Dragos的数据，在2018年，约72%的ICS漏洞公告涉及工程工作站系统、人机界面（HMI）和工业网络组件。该公司指出，这些公告有点多余。这是因为，即使没有可利用的漏洞，这些系统也是重要的攻击目标。

“这些协议的大多数在设计上都不安全。”李解释道，“如果利用协议的漏洞就能够在HMI上提权，攻击者何必关心HMI的默认状态是否已经在管理模式下运行了呢——在这种情况下，攻击者根本无需利用HMI的漏洞。”

原文名称	ICS/SCADA Attackers Up Their Game
作者简介	Kelly Jackson Higgins。Kelly Jackson Higgins担任Dark Reading的执行编辑。
原文信息	2019年2月15日发布于Dark Reading 原文地址 https://www.darkreading.com/threat-intelligence/ics-scada-attackers-up-their-game/d/d-id/1333893
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。