安天发布《GandCrab 勒索病毒变种分析报告》

近期，安天捕风小组发现 GandCrab 勒索家族在国内呈爆发趋势，福建、浙江、山西、吉林、贵州、天津等省份均出现了该病毒家族的感染案例。其最新变种 GandCrab5.0.4 已造成国内部分医疗行业出现业务瘫痪，影响医院的正常问诊治疗。

GandCrab5.0.4 变种的攻击流程依然采取了 GandCrab5.0.3 的框架，同样采用 RSA+AES 加密算法，将系统中的大部分文档文件加密为随机后缀名的文件，然后对用户进行勒索。GandCrab5.0.4 主要通过 RDP（远程桌面协议）爆破、邮件、漏洞、垃圾网站挂马等方式进行传播，其自身不具备感染传播能力，不会主动对局域网的其他设备发起攻击，但会加密局域网共享目录文件夹下的文件。

攻击者首先会 RDP 爆破其中一台主机，成功获取到该主机的控制权后，上传一整套工具，包括进程管理工具、内网扫描工具、密码抓取工具、暴力破解工具以及勒索工具。由于其中某些工具容易被杀毒软件查杀，因此攻击者对其进行了加密压缩处理，压缩密码为“123”。工具上传完成后，攻击者感染主机的第一个动作是用进程管理工具“ProcessHacker”结束杀毒软件进程。之后，为了控制更多的内网主机，攻击者会使用内网扫描工具“KPortScan”、“nasp”、“NetworkShare”来发现更多潜在目标。

同时，攻击者会使用 mimikatz 抓取工具抓取本机密码，用 WebBrowserPassView 抓取工具抓取浏览器密码。由于内网中普遍存在密码相同的情况，因此抓到的密码很有可能能够直接登陆其他主机。之后使用 DUBrute 暴力破解工具对内网主机进行 RDP 爆破。黑客上传的勒索工具中包含了勒索病毒体 HW.5.0.2.exe 以及一个文本文件“HW.txt”，“HW.txt”文件记录了用于无文件勒索的 powershell 命令。攻击者可直接运行勒索病毒体或者执行 powershell 命令进行勒索。

安天建议广大用户，发现勒索现象时请尽快对感染主机进行断网隔离；安装杀毒、防毒软件（参考安天智甲工具）并及时升级系统和修补设备漏洞；对重要的数据文件进行备份，避免弱口令的使用，避免使用统一的密码；GandCrab 勒索软件会利用 RDP 进行传播，如果业务上无需使用 RDP，建议将其关闭。

目前，安天追影产品已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、文件来源信息分析鉴定器、数字证书鉴定器、文件元数据鉴定器、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 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	da66cbc9ae879173f9e38d51a2cffdb8
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	139 KB
MD5	DA66CBC9AE879173F9E38D51A2CFFDB8
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Ransom
判定依据	BD 静态分析鉴定器

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=DA66CBC9AE879173F9E38D51A2CFFDB8

◆ 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

◆ 常见行为

行为描述	危险等级
遍历进程	★
获取计算机名称	★
获取驱动器类型	★
扫描磁盘类型	★★
获取系统信息（处理器版本、处理器类型等）	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
访问文件尾部	★
文档篡改	★★
设置自启动项	★★

◆ 进程监控

PID	创建	命令行
476	target.exe	"c:\9ec725801e464588f93dfbd82c7eb5c98\share\target.exe"
392	cmd.exe	"c:\WINDOWS\system32\cmd.exe" /c vssadmin delete shadows /all /quiet
464	vssadmin.exe	vssadmin delete shadows /all /quiet

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 12 月 03 日 (总第 162 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天携手北京理工大学共建网络安全自动化分析联合实验室

近日，安天与北京理工大学共同建立的“北理工－安天网络安全自动化分析技术实验室”在北京理工大学信息科学实验大楼举行揭牌仪式，并召开了首次实验室学术会议。


实验室揭牌仪式合影

北理工信息系统及安全对抗实验中心主任、北理工－安天联合实验室联席主任罗森林教授主持揭牌，北理工信息与电子学院党委书记薛正辉与安天合伙人、集团技术委员会副主任何公道为揭牌仪式致辞。北理工徐特立学院院长张笈、信息与电子学院副院长陈禾、安天研发高级副总裁王小丰、安天政府事务部总监罗云峰、实验室团队成员等共同参加了揭牌仪式。

北理工信息与电子学院党委书记薛正辉在致辞中表示，北理工是国家首批建立信息对抗专业的院校，在网络安全、数据挖掘、文本安全、媒体安全等方面具有一流的科研教学基础。安天是引领威胁检测分析能力发展技术的领导企业，是国家级网络安全应急服务支撑单位，希望通过与安天共建实验室，促进强强联合，将科研教学与工程技术实践更加紧密结合，共同推动产学研协同创新发展。

安天合伙人、集团技术委员会副主任何公道在致辞中指出，为应对日益严峻的网空安全形势，安天不断强化威胁检测引擎和支撑平台体系传统优势，更致力于打造战术型态势感知平台体系和系列能力型安全产品。安天较早将深度学习技术应用于后端样本的自动化分析工作。北理工在信息安全和人工智能结合领域的研究上处于领先地位，通过成立联合实验室，可以将北理工的科研教学人才优势与安天的工程能力优势相结合，推动人工智能在网络安全领域的实战化应用。

在揭牌仪式后的首次实验室学术会议上，北理工与安天研究人员先后分享了题为《基于人工智能的恶意软件分析》和《机器学习在工程技术上的实际应用》的技术报告，并进行了热烈的交流讨论。

安天长期致力于将人工分析与自动化手段结合提升威胁分析效率，2001 年安天提出了借鉴工业流水线思想，进行工序化的恶意代码样本处理，并实现了二进制样本的特征自动化提取；2004 年安天实现了全量样本的自动化分析判定，之后陆续完成了集成分析环境的开发，在后台逐步实现了自动化分析对人工分析的有效降维和人工分析经验向自动化分析的迭代。当前安天每日对百万量级新增文件样本进行自动化分析，对其进行动静态自动化分析，将每个样本拆解为数千个分析向量，日汇聚分析处理非样本类感知数据总数据量亦超过 10T。

随着高级威胁不断浮出水面，安天认识到安全厂商不仅要加快自身威胁捕获、威胁分析和能力发布的效率，更要把自我闭环模式，转化成赋能客户，建立与对手的闭环模式。提升威胁发现的能力，缩短威胁发现的时间周期，提升安全策略对行动支持的有效性。

依托安天与北理工共建的网络安全自动化分析联合实验室，双方将共同推进人工智能、数据挖掘等技术在威胁分析等领域的前沿探索，在科研合作、资源共享、学术交流、联合课题申报等方面扎实深入合作，积极推动自主先进技术成果的网络安全实战化应用，形成校企共建、培养复合人才、输出有效工程成果和先进学术成果的模式。

高校和企业受到自身角色和模式影响，过去在形成高水平成果方面有一定的局限条件。高校的网络安全研究多数缺少成熟工程能力支持，部分研究变成对网络安全企业已经完成工作的低水平重复；而在网络安全企业中，工程师多数投入到产品和支撑能力开发，工作往往缺少前瞻性，缺少跟进和转化先进理论的动力。在校企合作科研工作中，安天坚持优势互补、窄带聚焦、实战导向、追求领先的原则。安天针对合作高校的特点，选择自身有工程能力和数据基础、高校有学术积累的窄带专业方向进行合作，以形成具有实际防护价值的工程成果为目标，与重点高校开展专业方向的深度聚焦合作。在合作中，充分发挥高校科研理论优势，发挥安天的基础工程能力和数据优势，直接由企业技术带头人对接高校学术带头人，安天提供平台资源、工程资源和安全大数据资源支撑，助力高校形成具有前瞻性和实用前景的高水平学术成果，推动科研成果向有效的安全价值转化。

每周安全事件

类 型	内 容
中文标题	研究人员发现新的 Linux 挖矿木马 BtcMine
英文标题	New Linux crypto-miner steals your root password and disables your antivirus
作者及单位	Catalin Cimpanu
内容概述	研究人员发现一种新挖矿木马。这种新的恶意软件应用程序没有明确的命名，但通常以 Linux.BtcMine.174 被检测到。该木马是包含 1000 多行代码的巨型 shell 脚本，该脚本是在受感染的 Linux 系统上执行的第一个文件，会在磁盘上找到一个具有写权限的文件夹，然后复制自己，并下载其他模块。一旦木马下载完成，就会使用 CVE-2016-5195（也称为 Dirty COW）和 CVE-2013-2094 两种特权升级漏洞中的一种获取 root 权限从而获得对操作系统的完全访问权限。然后该木马将自己设置为本地守护进程，如果该实用程序不存在，会下载 nohup 实用程序来实现此操作。木马完全控制主机后，会进行加密货币挖掘。它还会下载另一种木马 Bill.Gates，这是一种已知的 DDoS 恶意软件，具有许多类似后门的功能。该木马还会收集有关受感染主机通过 SSH 连接的所有远程服务器的信息，并尝试连接到这些计算机进行传播。
链接地址	https://www.zdnet.com/article/new-linux-crypto-miner-steals-your-root-password-and-disables-your-antivirus/

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.JcSpy.b[prv,exp] 2018-11-26	该应用程序伪装成检查机关，显示用户涉及犯罪行为的虚假界面。后台监听短信并上传，联网获取号码和短信内容，私自发送短信，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.Kmtedc.a[rmt] 2018-11-27	该应用程序运行请求超级权限，接收远程指令，执行重启、下载、安装、卸载、更新本地配置文件等行为，影响用户正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeKakao.c[prv] 2018-11-28	该应用程序伪装成聊天软件 Kakao，运行会窃取用户输入的账号密码和手机号码信息联网上传，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.E4ABAH.a[fra]	该应用程序伪装木马生成器，运行锁定屏幕，诱导用户添加 QQ 授权，警惕该程序诱导用户付费造成用户财产损失，建议卸载。（威胁等级中）
		RiskWare/Android.KernelAds.a[exp]	该应用程序运行动态释放子包，子包会联网下载未知文件反射调用，可能是广告相关插件，会造成用户流量资费损耗，请谨慎使用。（威胁等级低）
		Tool/Android.Applock.a[prv,sys]	该应用程序为家长监控应用，设置限制使用的 APP 列表，设置密码并在密码多次输错的情况下拍照、定位、发送短信，请谨慎使用，若非自主安装建议卸载。（威胁等级中）
		Trojan/Android.nbank.b[prv]	该应用程序伪装金融类 APP，运行会上传用户短信记录、通话记录、联系人信息等聊天信息到远程服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SmartSpy.a[prv,spy]	该应用程序运行请求激活设备管理器，隐藏桌面图标，获取用户的短信信息、通话记录、通话录音、位置信息、WhatsAPP 等信息并发送至指定邮箱，会造成用户的隐私泄露，建议卸载。（威胁等级中）
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-2018-8539）	当 Microsoft Word 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft Word 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。（威胁等级高）
	较为活跃样本	RiskWare[Downloader]/Win32.InstallVibe	此威胁是一种具有下载行为的风险软件类程序。该病毒家族的样本会在执行后启动一个下载器，在后台下载其他恶意代码文件并执行。与此同时，该病毒家族的样本会释放出一个恶意的 DLL 文件到 %TEMP% 文件夹中。（威胁等级中）
		GrayWare[AdWare]/MSIL.Solimba	此威胁是一种具有下载行为的风险软件类程序。该病毒家族的样本会在执行后下载大量第三方的应用程序并安装，并且该病毒家族的样本会注入其他的进程使自己难于清除。（威胁等级低）
		GrayWare[AdWare]/NSIS.ConvertAd	此威胁是一种使用 Nullsoft 安装程序打包器的具有广告行为的灰色软件类程序。该病毒家族的样本以下载器的形式体现，在下载用户要求的软件同时，在后台下载并安装含有广告的软件。（威胁等级低）
		RiskWare[Downloader]/MSIL.Temonde	此威胁是一种可以下载推广应用的风险软件家族。该家族样本运行后连接远程服务器下载推广应用并安装，占用系统资源，影响用户使用。（威胁等级中）
		RiskWare[WebToolbar]/Win32.Perinet	此威胁是一种具有安装浏览器扩展工具栏行为的风险软件类程序。该病毒家族的样本会在执行后安装一个浏览器扩展工具栏。并且该病毒家族的样本会注入其他的进程使自己难于清除。（威胁等级低）

通过钓鱼模拟减小用户攻击面

Theo Zafirakos / 文 安天技术公益翻译组 / 译

没有任何一种安全解决方案能够 100% 地保护机构，但是如果你采用多层次的方法，将员工作为第一道防线，将会是一个不错的起点。

作为首席信息安全官（CISO），你应该从什么地方着手，来推动最终用户的行为改变，使其提高安全意识并履行合规义务呢？关键在于通过“及时的”安全意识和强化工具来强化用户的正确行为，并使他们从错误行为中吸取教训。首先，你需要为员工创建一套常识指南。其次，你需要构建一个包括网络钓鱼模拟和安全意识培训在内的全面计划。

钓鱼模拟的基本要求：看起来真实，感觉真实

在钓鱼模拟中，你发送的邮件应该很像最终用户收到过的真实钓鱼邮件。这些邮件应该来自机构内外部，已知和未知源。将用户收件箱中所有来自外部的邮件标记为“外部邮件”，是一种不错的警告方法。但是，对于伪装为外部合作伙伴，或已经感染内部帐户并进一步利用该帐户的攻击者，这种方法就没什么效果了。

最终用户拥有手机和平板电脑等设备，并在这些设备上登录各种社交媒体帐户，因此他们需要了解这些设备对其个人信息和机构造成的威胁。让用户提交报告，有助于你实时查看他们发现和上报钓鱼企图的情况，了解需要开展更多教育培训的领域。此外，这也有助于你调整钓鱼模拟策略，使其更像真实的网络钓鱼，并随着时间的推移不断增加其复杂程度。

从错误中吸取教训

每个人都会犯错，那么用户为何不在不造成重大损害的前提下，从错误中吸取教训呢？

通过部署钓鱼模拟策略，最终用户可以成为网络钓鱼检测专家，他们会定期报告可疑的恶意链接、文档、短信和社交媒体帖子。这样一来，他们就不会随意点击链接，让安全团队措手不及了。很快，最终用户将开始应用他们学到的安全措施，并自动执行这些措施，例如：

- 为智能手机上的每个应用（包括企业电子邮件）设置不同的口令，以防止身份盗用。
- 了解黑客的最大目标是有效凭证。
- 应用“干净桌面原则”，删除包含用户名和口令的便签。
- 以保护机构支付卡数据的方式，来保护机构的知识产权。
- 识别社会工程手段，实施访问控制和物理安全措施；要求陌生人提供通行证和 ID，防止他们贴在别人身后进入机构。
- 充分了解机构的信息分类策略以及他们应如何管理信息生命周期。
- 重视隐私并在网络上实施保密措施。
- 将自己视为移动用户，保护移动过程中的安全。

影响高管团队

作为首席信息安全官，你的众多职责之一是影响利益相关者的管理、定位和沟通。你必须想方设法，让董事会像你一样思考。如果你能够取得成功，他们就会批准你的安全解决方案所需的资金和资源。最重要的是，你需要确保高管们看到你的提议的优势所在。

在季度高管会议中，你需要提交简洁清晰的报告，准确地为董事会提供“最大攻击面”（即用户）的最新状况。你还可以向他们展示持续的改进，让他们意识到，要想保护企业，钓鱼意识和持续测试是非常重要的投资领域。

构建钓鱼模拟计划

构建网络钓鱼模拟计划时，可以采用以下八种方法。

- 明确定义钓鱼模拟策略，包括模拟目标、沟通和响应线等。
- 为机构内的特权用户（例如 IT 管理员，财务人员）制定高频且复杂的方案。
- 向所有利益相关者明确说明，谁、何时会收到钓鱼测试通知。
- 不要重复使用钓鱼模拟邮件，防止用户与同伴交流邮件内容，降低模拟的有效性。
- 在进行模拟之前，执行验证并清理电子邮件地址。
- 确定安全团队的响应策略。当用户检测到钓鱼企图并上报时，能够及时响应。
- 模拟完成后，将结果提交给管理层和用户。
- 不建议对未通过初始测试的用户进行惩罚。相反，我们应该花些时间教他们识别网络钓鱼，并让他们知道应该如何应对。

没有任何一种安全解决方案能够 100% 地保护机构，但如果你采用多层次的方法，将员工作为第一道防线，对他们进行教育培训，使其能够轻松检测到网络钓鱼企图，那么你将会大幅减小“最大攻击面”。

原文名称	Reducing the Human Attack Surface with Phishing Simulations
作者简介	Theo Zafirakos。Theo Zafirakos 是一位注册信息系统安全专家。
原文信息	2018 年 11 月 26 日发布于 Dark Reading。 原文地址 https://www.darkreading.com/endpoint/reducing-the-human-attack-surface-with-phishing-simulations/d/d-id/1333328
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。