安天发布《LooCipher 勒索软件分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 LooCipher 的新型勒索软件，LooCipher 最初是由国外安全研究员 Petrovic 发现的。该勒索软件主要通过垃圾邮件进行传播，邮件附件为包含恶意宏代码的 Word 文档 Info_BSV_2019.docm。该文档诱使用户启用宏以查看文档内容，宏代码的功能为连接 Tor 服务器并下载 3agpke31mk.exe，将该文件重命名为 LooCipher.exe，然后执行该文件。

勒索软件 LooCipher 执行后，会在桌面上创建一个名为 c2056.ini 的文件，该文件中包含 USER_ID、支付赎金的截止时间和比特币地址。LooCipher 会加密计算机上的文件，创建文件的加密副本，并追加后缀名“.lcphr”，LooCipher 只删除了原文件内容并未删除原文件。加密结束后，LooCipher 会创建一个名为“@Please_Read_Me.txt”的勒索信，勒索信中包含解密说明、比特币地址和勒索金额（300 欧元或 330 美元）。LooCipher 还会替换桌面壁纸，桌面壁纸内容与勒索信类似。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

灰色软件

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述灰色软件进行有效检测，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、关联分析鉴定器、静态特征检测鉴定器、智能学习鉴定器、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、反病毒引擎鉴定器、关联分析鉴定器将文件判定为灰色软件。

◆ 概要信息

文件名	43cfb0a439705ab2bd7c46b39a7265ff0a14f7bd710b3e1432a9bdc4c1736c49
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	5.38 MB
MD5	0C7E59536A7BE4A446BBE8B4F22E5880
病毒类型	灰色软件
恶意判定 / 病毒名称	GrayWare/Win32.Generic
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/vue/details?hash=0C7E59536A7BE4A446BBE8B4F22E5880

◆ 运行环境

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

◆进程监控

PID	创建	命令行
2212	target.exe	"c:\3cf6b1d32111469e8f9e27308ebe86c1\share\target.exe"

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.165	65127	224.0.0.252	5355
192.168.122.165	61764	224.0.0.252	5355
192.168.122.165	137	192.168.122.111	137
192.168.122.165	68	255.255.255.255	67
192.168.122.165	56930	224.0.0.252	5355
192.168.122.165	61340	224.0.0.252	5355
192.168.122.165	56667	224.0.0.252	5355
192.168.122.165	64558	224.0.0.252	5355
192.168.122.165	56602	224.0.0.252	224.0.0.252
.....	.....	.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 07 月 08 日 (总第 190 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布勒索软件 Sodinokibi 运营组织的关联分析

概述

2019 年 5 月，安天 CERT 监测到了多起利用钓鱼邮件传播 Sodinokibi 勒索软件的事件。Sodinokibi 最初由 Twitter 账号为 Cyber Security（@GrujaRS）的独立安全研究员发现，而 Sodinokibi 这个名称是根据首次出现样本的版本信息中的文件名命名的。这种命名方式并不规范，但由于 Sodinokibi 这个名称已经被广泛使用了，因此安天 CERT 也沿用这一名称。Sodinokibi 从 2019 年 4 月 26 日开始出现，其传播方式主要为钓鱼邮件、RDP 暴力破解和漏洞利用。

安天 CERT 分析人员通过代码、C2、邮件、漏洞利用等关联分析认为该勒索软件团伙是一个不断套用、利用其他现有恶意工具作为攻击载体，传播勒索软件、挖矿木马、窃密程序，并在全球范围内实施普遍性、非针对性勒索、挖矿、窃密行为的具有一定规模的黑产组织。该组织和 GandCrab 组织有着千丝万缕的关系，分析人员猜测 Sodinokibi 和 GandCrab 运营成员有重合部分，在 GandCrab 组织宣布停止运营之后，部分 GandCrab 成员不愿收手，继续运营新修改的勒索软件 Sodinokibi。

经验证，安天智甲终端防御系统（英文简称 IEP，以下简称安天智甲）可实现对 Sodinokibi 的有效防御。

事件背景

♦黑产组织伪装公安部发送钓鱼邮件传播 Sodinokibi 勒索软件

2019 年 5 月，安天 CERT 监测到多起伪造“中华人民共和国公安部”发送钓鱼邮件传播 Sodinokibi 勒索软件的攻击事件。该钓鱼邮件伪造邮件主题为“警察議程”，邮件内容称用户必须在 2019 年 5 月 23 日下午 3 点向“警察局”报到，参与调查。邮件附件名为“關於你案件的文件 .rar”。

黑产组织利用用户对邮件内容的恐惧和好奇心理，诱使用户下载附件并查看附件内容。附件解压后是两个伪装成 doc 文件的快捷方式，当用户查看伪造文件（实为快捷方式）时，便会运行快捷方式指向的勒索软件 Sodinokibi，导致用户主机中文件被加密。勒索软件以隐藏的方式存储在该目录下，若用户的系统未设置成显示隐藏文件，则并不会发现勒索软件文件。另外，隐藏的文件为双扩展名，若用户系统设置为不显示扩展名，则不能发现该文件为 EXE 可执行文件。

♦黑产组织伪装 DHL 快递公司发送钓鱼邮件传播 Sodinokibi 勒索软件

2019 年 6 月初，安天 CERT 监测到多起通过伪造 DHL 邮件传播 Sodinokibi 勒索软件的钓鱼邮件攻击事件。DHL，即敦豪国际航空快递有限公司，是全球知名的邮递和物流集团 Deutsche Post DHL 旗下公司，业务遍布全球 220 个国家和地区。该钓鱼邮件主题为“您的包裹将无法按时交付”，邮件内容称因为受害者提供了不正确的海关申报数据，因此不能按时交付受害者的包裹，要求受害者点击邮件中的链接，下载海关文件查看并签署。

2019 年 5 月，华为通过联邦快递（FedEx）发送的两份商业文件被拦截并送往美国孟菲斯的联邦快递公司。在业内人士对联邦快递发出质疑后，联邦快递在 5 月 28 日发布了道歉微博。5 月 22 日，传出 DHL 停收华为货物的通知，5 月 23 日，DHL 否认停运华为货物。在这个环境下，伪装成 DHL 的钓鱼邮件极有可能是在蹭该起事件的热点，利用该事件对大众造成的影响，诱导用户相信钓鱼邮件的真实性，从而增加用户点击链接的可能性。

邮件正文中的链接是一个使用 plip.io（短网址生成网站）生成的短网址，用户点击后会解析到另一个网址，之后会跳转到最终恶意网站下载勒索软件。邮件正文中虽提到存档中的密码为 DHL，但该压缩包不需要输入密码“DHL”便可以解压。

Sodinokibi 勒索软件的主要传播方式

- 利用钓鱼邮件传播
- 利用 RDP（远程桌面协议）传播
- 利用 WebLogic 漏洞传播

Sodinokibi 勒索软件详细分析

安天 CERT 对 Sodinokibi 勒索软件的样本标签、勒索信息、样本等内容进行了详细的分析解读。

关联分析

♦URL 情报分析——Sodinokibi 运营者传播窃密工具 KPOT Stealer

通过安天威胁情报分析系统关联到 webex.today 域名。攻击者利用 Powershell 从该网站下载窃密木马家族 KPOT Stealer。关联到的最新 KPOT Stealer 样本（MD5：70CE22275834C1E34E6EE52AC8E5DF31）会收集 Cookie 信息、浏览器登录凭证、进程信息、已安装软件信息、系统信息、屏幕截图以及受害者 IP，并通过 HTTP POST 方式回传窃密信息。

♦IP 关联拓线——Sodinokibi 运营者传播 Linux 挖矿、后门木马

在安天 CERT 监测到的多起安全事件中，部分 Sodinokibi 样本从 188.166.74.* 下载。通过对 188.166.74.* 进行关联，发现 GandCrabV5.2 也曾经使用这个 IP 作为下载地址，其中一个 Sodinokibi 样本存在两个下载地址，188.166.74.* 和 45.55.211.*。通过 45.55.211.* 关联到了 GandCrab V4 家族的另一个样本和 Linux 系统下一些后门挖矿木马。

通过对样本的 IP 进行拓线，分析人员发现用来下载 Sodinokibi 的 IP 地址从 2018 年开始传播 GandCrab、Linux 挖矿，2019 年开始传播 Linux 后门、Sodinokibi 勒索软件。

（下接第三版）

每周安全事件

类 型	内 容
中文标题	LooCipher 勒索软件通过带有恶意文档的邮件传播
英文标题	LooCipher: The New Infernal Ransomware
作者及单位	ZLAB-YOROI
内容概述	Yoroi 研究人员发现新勒索软件 LooCipher，与大多数勒索软件不同，LooCipher 通过恶意文档投递，恶意文档要求用户启用宏，一旦运行，它就开始加密除系统和程序文档以外的所有文件。加密后，恶意进程就会向 C2 发送有关受感染计算机的信息并检索 BTC 地址以显示在弹出窗口中。 每次勒索软件在“k.php”资源上联系其 C2 时，服务器都会生成一个新的 BTC 地址。恶意软件还会嵌入后备地址列表，以便在受害者计算机脱机无法访问 C2 时使用。
链接地址	https://blog.yoroi.company/research/loocipher-the-new-infernal-ransomware/

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.Locker.br[rmt,lck,spy] 2019-06-30	高	该应用程序会加密用户设备 SD 卡中的所有文件进行勒索，同时会窃取用户的短信、通话记录、浏览器历史记录、环境录音、地理位置信息等，会对用户的隐私安全和数据安全造成极大威胁，建议立即卸载。
		Trojan/Android.SmsSpy.bo[prv,exp] 2019-07-01	中	该应用程序伪装为银联相关应用，运行隐藏图标，发送特定短信并转发收到的短信至指定号码，造成用户的资费消耗和隐私泄露，建议卸载。
		Trojan/Android.9rpn.b[exp,rog] 2019-07-02	中	该应用程序安装无图标，联网获取广告数据，后台推送广告，还会下载安装未知应用，造成用户资费损耗，建议卸载。
	较为活跃样本	Tool/Android.Clevguard.a[prv]	中	该应用程序是一款家长监控应用，运行后上传被监控手机的短信、通话记录、浏览器历史、位置、社交应用消息、照片等至服务器，可能造成用户的隐私泄露，建议谨慎使用，非自主安装建议卸载。
		Tool/Android.ADTC.a[prv,rmt]	中	该应用程序为一款监控工具，运行后激活设备管理器，接收远程控制命令，进行拍照、录音、录像、发送短信、隐藏图标，还会收集用户手机短信、联系人、通话记录、地理位置等信息并上传。请谨慎使用，若非本人安装，建议卸载。
		Trojan/Android.InfoStealer.bc[prv]	中	该应用程序包含风险代码，运行获取用户的位置信息，后台上传用户录音和短信信息，造成用户的资费消耗和隐私泄露，建议卸载该应用。
		G-Ware/Android.GDowgin.ls[exp,rog]	低	该应用程序包含流氓广告插件，会在用户手机屏幕上匿名弹窗，强行推送广告，严重干扰手机正常使用，建议卸载。
		G-Ware/Android.CoinMiner.f[exp,rog]	低	该应用程序包含恶意代码，后台私自挖矿，消耗设备资源，影响用户正常使用，请卸载。
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-2019-1035）	高	当 Microsoft Word 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以利用此漏洞。成功利用漏洞的攻击者可在用户系统上执行任意代码。
	较为活跃样本	Trojan/Win32.Nurjax	中	此威胁是一种可以下载恶意代码的木马程序。该家族样本会劫持受感染计算机上的 Web 浏览器，可以下载额外的威胁。
		RiskWare[RiskTool]/Win32.HideProc	中	此威胁是一种风险软件类程序。该家族样本运行后会隐藏自身进程；在后台窗取用户击键信息、屏幕截图、运行的进程的信息，并将这些信息发送给攻击者。
		RiskWare[Downloader]/NSIS.SilentInstall	中	此威胁是一种使用 NSIS 制作的具有下载行为的风险软件类程序。该家族运行后，会与远程服务器连接，下载并安装其它的恶意软件到本地运行。
		RiskWare[WebToolbar]/JS.CroRi	中	此威胁是一种使用 JS 脚本语言编写并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。
		RiskWare[Downloader]/Win32.AdGazele	低	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。

（上接第一版）

♦ 多方位对比 ——Sodinokibi 和 GandCrab 异曲同工

本事件中的勒索软件使用的钓鱼邮件与 2019 年初 GandCrab 使用的钓鱼邮件内容相似，同时分析人员在对勒索软件 Sodinokibi 进行分析的过程中，发现其与 GandCrab 有多处相似。

• 代码相似

• 手法一致

• 同一机器产出，快捷方式生成时间分别为 5 月 6 日和 6 月 5 日

♦邮件广撒网——非针对性攻击的黑产行动

从对大量 Sodinokibi 的钓鱼邮件分析来看，邮件内容针对不同的国家使用不同的语言，而且使用了多种邮件主题，利用大量垃圾邮件、社工方式来大范围撒网。其发件人邮箱大部分为 *@gmx.com（全球著名免费邮箱网站），有的邮箱是真实存在的，有的则是伪造的。从收件人邮箱以及其他国家发生的类似事件来看，Sodinokibi 并未针对某一地区或公司亦或是某一领域，它所操作的，是以获利为目的的大规模的勒索行动。

♦攻击时间分析

2019 年 4 月 30 日，思科 Talos 情报小组披露了通过 WebLogic Server 漏洞传播的 Sodinokibi 勒索软件，并提到攻击者在部署 Sodinokibi 的同时也会部署 GandCrab V5.2[4]。分析人员对该报告中提到的样本的时间戳以及 2019 年 5 月份通过钓鱼邮件传播的部分 Sodinokibi 样本的时间戳进行对比，发现这些样本的时间戳大都在 2018 年期间。这说明这场勒索活动至少在 2018 年就开始策划了。

♦小结

通过本片报告的详细分析，猜测 Sodinokibi 和 GandCrab 运营成员有重合部分，部分 GandCrab 成员不愿收手，继续运营新修改的勒索软件 Sodinokibi。

总结

从针对 Sodinokibi 勒索软件的整体分析关联来看，该勒索组织具有一定规模，且组内成员分工明确，从投放载体到勒索收益形成一条完整的黑色产业链。从大量样本的时间戳来看，这场勒索行动至少在 2018 年就开始策划了。该组织不仅投放勒索软件、而且还夹带着窃密木马、挖矿木马，即包含勒索、窃取、挖矿等多种恶意行为。Sodinokibi 并未针对某一地区或公司亦或是某一领域，它所操作的，是以获利为目的的大规模的勒索行动。Sodinokibi 组织和 GandCrab 组织有着密切的关联，分析人员推测 Sodinokibi 的运营团队可能包含 GandCrab 组织的部分成员，现版本的 Sodinokibi 更像是 GandCrab 的新变种，Sodinokibi 的运营团队更像是 GandCrab 组织的接班人。

大部分勒索软件仍然是使用钓鱼邮件和相应漏洞进行传播。因此，安天 CERT 建议用户打好相应漏洞补丁，不要随意打开邮件附件，并使用防护软件如安天智甲进行有效防护。

安天智甲有效防护

安天智甲终端防御系统（英文简称 IEP，中文简称安天智甲）通过诱饵文件、行为分析、文件变化审计、进程身份识别等多种能力的结合，可实现对主流勒索软件的有效防护。经验证，安天智甲可实现对 Sodinokibi 的有效防护。

安天智甲简介

安天智甲是一款面向政府、军工、能源、金融、交通、电信等各行业用户的企业级终端防御产品，支持各种体系结构和操作系统平台，对桌面、工作站、服务器、移动终端、虚拟化等端点场景提供安全防护。为客户提供病毒与恶意代码查杀、威胁主动防御、补丁修复、配置加固等防护功能。对浏览器、电子邮件等入口进行交互防御， 对 Office 等软件遭遇的格式漏洞攻击进行特别保护，对 USB 等介质攻击进行保护。具有精准检测防御海量已知威胁的能力和较强未知威胁发现和主动防御的能力，可有效收缩终端受攻击面，有效支撑安天资产运维平台和战术型态势感知的数据采集和响应行动。

微信扫描二维码查看分析详情

IBM 披露其一系列产品中多个高严重性漏洞

IBM 披露了其一系列产品中多个关键和高严重性漏洞，其中最严重的漏洞存在于 IBM Spectrum Protect 工具中。该漏洞（CVE-2019-4087）CVSS 评分为 9.8，是一个基于堆栈的缓冲区溢出漏洞，源于组成 Spectrum Protect 的服务器和存储代理中的不正确边界检查。影响平台的 7.1 和 8.1 版本。IBM Spectrum Protect 中的另一个高严重性缺陷（CVE-2019-4088）可能允许本地攻击者获得受影响系统的提升权限。攻击者可以通过平台的“dsmqsan”模块加载特制的库来触发此漏洞。IBM Spectrum Protect 中的中等严重性漏洞（CVE-2019-4140）允许本地用户通过恢复旧数据来替换现有数据库。平台运营中心中最终的低严重性漏洞（CVE-2019-4129），可能允许远程攻击者获取敏感信息。IBM 防止数据库和仓库泄漏的工具 IBM Security Guardium 存在高严重性漏洞（CVE-2019-4292），CVSS 得分为 8.8（满分 10 分），可能导致攻击者在 Web 服务器上执行任意代码。IBM Planning Analytics 2.0（CVE-2019-4134）中的跨站点脚本漏洞可能导致凭证泄露，IBM Daeja ViewONE Virtual 5.0 - 5.0.5 中还存在信息泄露漏洞 CVE-2019-4260。IBM 已修补这些漏洞。

专攻银行系统的 Silence APT 开始走向全球，重点为亚太地区

据孟加拉当地媒体报道，荷兰孟加拉银行 ATM 遭到黑客攻击，导致 300 万美元被盗。这起网络攻击从数月前开始，最后阶段于 5 月 31 日发生在孟加拉首都达卡。7 月 3 日，专注于防范网络攻击的国际公司 Group-IB 已证实，幕后黑手很可能是俄罗斯网络犯罪集团 Silence APT，且银行实际失窃金额要比媒体报道的高的多。这是 Silence 最近发动的国际攻击之一，表明该团伙已经扩大了攻击面，并且走向全球，目前重点是亚太地区。