安天发布《LockerGoga 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个名为 LockerGoga 的新型勒索软件。研究人员发现该勒索软件家族与其他勒索软件家族不同的是它能充分利用 CPU 的多核特性来加快破坏效率。

LockerGoga 需要以管理员身份运行并以主从（master/slave）配置模式进行工作。LockerGoga 通过在 %TEMP% 文件夹安装自己本身开启终端感染模式。之后会用 -m 参数开始一个新的进程。Master 进程以 -m 参数运行，负责创建要加密的文件列表和 slave。Slave 进程会以不同的参数来执行。每个 slave 进程只加密很少一部分文件，以防止被终端安全产品发现。要加密的文件列表通过 IPC 从主进程获取。在进行文件加密前，勒索软件首先会在回收站中搜索文件，然后 LockerGoga 会枚举系统中的所有文件夹和文件并开始加密，枚举完成后，勒索软件会在受害者系统上创建勒索信，并将加密的文件加上 .locked 后缀名。加密完成后，LockerGoga 会执行 cipher.exe 来删除可用空间以防止在受感染的系统中恢复文件。

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、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	7bcd69b3085126f7e97406889f78ab74e87230c11812b79406d723a80c08dd26
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.19 MB
MD5	7E3F8B6B7AC0565BFCBF0A1E3E6FCFBC
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Crypren
判定依据	反病毒引擎

完整报告地址：https://1.119.163.6/_lk/details.html?hash=7E3F8B6B7AC0565BFCBF0A1E3E6FCFBC

◆ 危险行为

行为描述	危险等级
延时	★★★

◆常见行为

行为描述	危险等级
获取系统信息（处理器版本、处理器类型等）	★
设置调试器权限	★
创建挂起进程	★★
获取驱动器类型	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
感染文件	★★
文档篡改	★★
设置文件属性为隐藏	★★
疑似桌面控制	★

◆ 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

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 05 月 27 日 (总第 184 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

赋能客户 有效防护 | 安天集团产品与解决方案全国巡展成都站纪实

近日，以“赋能客户，有效防护”为主题的安天集团产品与解决方案全国巡展首站于成都世纪城洲际大饭店成功举办。安天工程师围绕“战术型态势感知指控积极防御，协同响应猎杀威胁运行实战化”的年度主题，与客户共同研讨以有效防护为目标，构建动态综合网络防御体系的相关内容。

网络空间对抗进入体系化阶段

全球 APT 攻击组织、行动来源分布图（2018 版）

安天工程师尹尚书带来了题为《高级网空威胁带来的挑战》的分享，其从 NSA/CSS 网空威胁框架入手，向与会嘉宾介绍了网空威胁的发展演变，安天捕获分析的“白象”、“绿斑”、“方程式” 等高级网空威胁行为体典型案例分析，具有代表性的高级网空威胁行为体的支撑体系、攻击装备、作业特点等。

随着我国信息化的高度发展，网络安全风险也随之而来，国家机密和重要数据信息被窃取、工业生产被攻击破坏、金融资产被盗窃、科研成果被窃取抄袭，各种风险挑战接踵而至，从个体攻击者，到以超级大国为背景超高能力的网空威胁行为体都活跃其中，水平越高的威胁行为体攻击体系性越强。“物理隔离御敌于城门之外”是单点防御思维，无法对抗这种体系性的攻击威胁，需要以“敌已在内、敌将在内”作为敌情设定，构建动态综合的网络安全防御体系。

向指控积极防御迈出坚实脚步：安天战术型态势感知平台体系

安天战术型态势感知解决方案建设思路

安天工程师孙晋超以《战术型态势感知指挥控制积极防御》为题，阐述了当前网络空间安全防御工作中，安天态势感知解决方案的建设思路和落地案例。

安天从 2002 年起，从骨干网恶意代码全规则检测工作入手，开始了网络空间威胁监测的初步实践探索，并协助多个战略客户进行了监测型态势感知平台的建设实践。这种面向公共互联网和针对暴露资产的监测体系，可以一定程度上满足管理部门宏观层面上威胁捕获、研判和策略调整与展示的需求，但并不适合作为有效防御的指控中枢部署于重要信息系统和关键基础设施之中。随后推出的战术型态势感知平台，则可以将有效防御的指控中枢部署于重要信息系统和关键基础设施之中。

安天战术型态势感知平台，以“敌已在内、敌将在内”的敌情设定为设计前提，在完善并强化已有静态的防御机制实现兼顾结合面与覆盖面的综合防御能力体系同时，为客户打造“掌握敌情、协同响应”的动态积极防御体系。通过配备对抗攻击行动的装备系统和处置流程，展开协同响应与处置的积极防御，高效地实现威胁与脆弱性检测识别、安全事件理解分析、攻击与影响预测、协同联动处置、情报与知识生产，实现安全态势的全面感知与安全业务的融合贯通，对日趋复杂的网络攻击进行更为精准地发现与打击，从而保障响应行动的及时性和有效性，支撑协同联动的实战化运行，协助客户筑起可对抗高级威胁的网络安全防线。

资产、配置、漏洞、补丁打通式管理：安天资产安全运维平台

安天资产安全运维平台的功能价值与定位价值

安天工程师卢鹏针对安天资产安全运维平台展开介绍，他从信息资产规模和复杂度的成长对安全运维工作的挑战入手，分析了传统安全运维的困境，指出实现网络可防御性的基础是实现网络的可管理性，而对网络可管理性的重要基础支撑是实现资产、配置、补丁、漏洞等相关要素的全面打通，实现运维安全一体化。

资产是防御保障的对象，也是基础的防御阵地，现代信息系统是由软硬件资产及其复杂的拓扑关系，以及其所承载的业务和数据资产构成的，确保信息资产的机

（下转第三版）

每周安全事件

类 型	事件一	事件二
标题	美国网络司令部上传的恶意软件仍被用于攻击	ActiveX 控件中存在多个严重漏洞影响韩国用户
内容概述	研究人员表示上周美国网络司令部上传到 VirusTotal 的恶意软件样本仍然被用于主动攻击，攻击目标是中亚国家的外交组织。上传的恶意软件类似于 XTunnel，是俄罗斯组织 APT28 在 2016 年入侵 DNC 使用的工具。恶意样本最初上传到 VirusToal 时，卡巴斯基实验室和 ZoneAlarm 可以检测到，目前 VirusTotal 上 71 个引擎中有 41 个检测到恶意文件。恶意软件共享计划于去年启动，旨在加强对抗对手的防御。	大多数 ActiveX 控件具有非常低的代码成熟度，并且存在许多缓冲区溢出等基本漏洞，ActiveX 技术被认为是过时和不安全的。Microsoft 已经删除了对 Microsoft Edge 中 ActiveX 的支持，大多数网站也不再依赖 ActiveX 技术。但韩国依然使用 ActiveX 控件支持的 Internet Explorer，其在政府、银行和教育网站上也都依赖 ActiveX 控件。2019 年初，研究人员对韩国 ActiveX 控件就进行了研究，发现曾被用于攻击的零日漏洞依然存在部分控件中，并且 10 个 ActiveX 控件中存在 40 个漏洞，包括各种类型的缓冲区溢出和不安全的暴露功能，允许攻击者在用户系统上执行代码。

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 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.interapp.a[prv,spy] 2019-05-19	该应用程序是一款间谍类应用，运行会隐藏图标，联网上传用户通讯录、位置信息、WhatsApp 和 telegram 等隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.FakeJioPrime.a[exp,rog] 2019-05-20	该应用程序伪装成其他应用，包含风险代码，警惕其私自发送注册短信，还会诱导用户分享指定链接，可能用于刷单行为，建议卸载。（威胁等级）
		Trojan/Android.ichipspy.a[prv,spy] 2019-05-21	该应用程序伪装系统应用，运行隐藏图标，窃取用户通讯录、通话记录、短信、定位信息、应用列表和浏览器历史记录等信息，并通过网络上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	G-Ware/Android.FakeWG.b[prv,rog]	该应用哪个程序伪装游戏辅助工具，运行隐藏图标，通过发短信窃取用户短信、手机号码和固件信息，造成用户隐私泄露，请卸载。（威胁等级低）
		RiskWare/Android.xiaokuangyl.a[exp]	该应用程序运行访问风险网址，可能包含色情、博彩、灰产等内容，请注意提示信息，谨慎使用。（威胁等级中）
		Tool/Android.merchant.a[prv]	该应用程序是支付监控相关的工具类应用，运行会监听短信，获取收款转账支付交易相关的信息联网反馈到服务器，建议谨慎使用。（威胁等级低）
		G-Ware/Android.CoinMiner.e[exp,rog]	该应用程序伪装为正常应用，运行隐藏图标，后台私自挖矿，影响用户的正常使用，建议卸载。（威胁等级中）
		Trojan/Android.kicoSpy.a[prv,spy]	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、通话记录等隐私信息，造成用户隐私泄露，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	Windows 特权提升漏洞（CVE-2019-0734）	当 Windows 未能正确处理某些符号链接时，会触发特权提升漏洞。成功利用此漏洞的攻击者可提升用户权限。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Boran	此威胁是一种具有广告件行为的灰色软件家族。该家族的样本在执行后会在用户的计算机上弹出广告。并且该家族的样本还会下载其他恶意软件程序对计算机进行感染。(威胁等级中)
		Trojan[Backdoor]/PHP.Pbot	此威胁是一种使用 PHP 语言编写的带有后门的木马类程序。该家族基于 Linux 和 Windows 平台，该家族会在后台链接到 IRC 服务器获取恶意指令。该家族木马可以执行指定命令，下载任意文件。（威胁等级中）
		RiskWare[WebToolbar]/Win64.Agent	此威胁是一种具有安装浏览器扩展工具栏的风险软件家族。该家族样本基于 64 位系统，它并没有统一的行为与功能，是将大量基因片段定性的恶意代码进行归类。(威胁等级低)
		RiskWare[RiskTool]/Win32.Patcher	此威胁是一种可以释放恶意代码到计算机的木马家族。该家族样本使用 DNF 图标进行伪装，运行后会释放并启动多个可执行程序，版本信息显示为游戏多开程序，会窃取游戏账号密码。（威胁等级中）
		RiskWare[WebToolbar]/NSIS.Agent	此威胁是一种具有安装浏览器扩展工具栏的风险软件家族。该家族样本使用 NSIS 打包，NSIS（Nullsoft Scriptable Install System）是一个开源的 Windows 系统下安装程序制作程序。该家族样本通过 NSIS 打包可以捆绑其他恶意代码到用户系统中。该家族是以基因片段定性的恶意代码分类，该家族并没有统一的行为与的功能，而是像一个集合一样，将大量基因片段定性的恶意代码归类。（威胁等级中）

（上接第一版）

密性、完整性、可用性，保证业务系统的连续运行和可以弹性恢复的能力，是整个安全防御工作的目的。安天资产安全运维平台，对端点、网络设备、网络安全设备、其他外设和办公设备等各种资产要素信息进行采集，形成针对网络管理运维人员的管理视图，随时感知资产和业务变化，有效支撑态势感知平台形成实时网空威胁地形。

配置是最基础的安全策略，也是充分发挥信息资产自身安全能力，对系统资源代价占用最小的基本安全环节。但因配置涉及大量客户权限、服务起停、端口开闭等环节，因此也存在配置会与业务应用发生冲突的情况。安天资产安全运维平台，充分参考借鉴 STIG 标准，针对实际应用场景，协助客户定制客户安全分组策略，制定策略模板。

漏洞是软硬件资产脆弱性的典型表现，漏洞发现与处置的及时性和有效性是日常安全运维工作的重要衡量指标。漏洞处置需要融入风险评估的思想，结合漏洞的危害性、业务及资产的重要性等因素，综合判定漏洞处置的优先级及处置方式，最大程度减轻漏洞处置对业务造成的影响，支撑业务系统的连续正常运行。安天资产安全运维平台包括内网漏洞库、漏洞自动检测终端、漏洞处置验证环境、漏洞策略管理中心等模块，能够支撑规模化信息资产的统一漏洞处置能力。

补丁是对软硬件资产的安全漏洞和功能缺陷的修复机制。规模性信息资产的补丁策略非常复杂，需要考虑内部统一补丁源、补丁的集中获取与留存审计、补丁的兼容性与可靠性的验证、补丁更新的灰度策略与反馈等。同时还需要考虑一些节点因业务连续性等因素无法打补丁，或无法重启生效的情况。安天资产安全运维平台包括内网补丁源服务器、补丁验证环境、补丁策略管理中心等模块，能够支撑规模化信息资产的统一补丁能力。

卢鹏还针对微软于 2019 年 5 月 14 日发布的 Windows 远程代码执行漏洞 (CVE-2019-0708)，向与会嘉宾展示了安天资产安全运维平台的响应处置过程，并指出对于不被使用的端口和服务通过配置基准确保其不被开启，而不是在看到漏洞或蠕虫通报时才去关闭，协助客户完成“未雨绸缪”的工作，同时也对特殊的无法打补丁或关闭端口的资产予以掌控。在威胁情报和严重漏洞信息到来之时，资产安全运维平台可以迅速展示对应的脆弱性分布，帮助客户制定有效决策。

全平台端点防御：安天智甲终端防御系统

安天智甲终端防御系统的能力与价值

安天工程师尚超介绍了端点系统所面临的多种流行安全威胁，如勒索病毒、挖矿病毒、内核级木马、格式文档漏洞攻击等。安天智甲终端防御系统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。

智甲采用可信计算与安天下一代反病毒引擎组合构建的黑白双控模式，对引导链和执行对象的行为活动和网络通讯进行检测过滤，针对各种服务器、重要工作站、SCADA 站、ATM 等场景具有专用的防御策略模板。

安天智甲全面支撑各种国产 CPU 和操作系统组合的主机环境防护，参与了专用机病毒防治标准规范的研讨，并率先研发出符合专用机病毒防护要求的产品——安天智甲专用机版，其在国产 CPU 和国产操作系统的基础架构之上，深度契合专用机的系统特性，从行为、边界、网络等多个层面为涉密专用机提供了全面的安全防护能力。在国产化领域，安天智甲深度结合国产化系统特点，全面覆盖国产化系统平台。

全方位防护：专业化的安全服务保障

安天安全服务品类与关系

安天工程师尹尚书分享了安天在安全服务领域的能力与落地案例。他表示，在网络安全威胁不断升级的场景下，要防范高能力对手有针对性的攻击，不仅要有完整的安全防护体系，还需要为不同层面的网络安全产品提供防护，更需要与之对抗的安全团队提供专业化的安全服务。安天协助客户深入发现、跟踪、分析、处置、猎杀威胁，为客户提供包括安全咨询、监测分析、安全评估、应急保障、安全培训等五个方面的专业化安全服务，以实现综合全面的网络安全保障 。

网络安全是当前大国博弈的焦点领域，是持续性对抗的领域。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，依托自主先进核心技术与安全理念，为重要信息系统和关键信息基础设施提供实战化运行的战术型态势感知解决方案，全面覆盖了网络和信息化基础设施各个组成实体，实现全生命周期的资产集中安全运维；通过将威胁知识与客户专有多源安全数据结合，配套高阶威胁情报与持续追溯服务，持续将威胁应对经验转换为客户的防护与响应能力。

本次安天集团产品与解决方案全国巡展通过展示安天在技术领域不断创新突破的核心成果，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行的落地案例，希望秉承“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”的企业纲领，赋能客户筑起可对抗高级威胁的网络安全防线。