安天发布《TFlower 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 TFlower 的勒索软件。该勒索软件最早发现于 2019 年 7 月底，针对企业用户进行勒索，主要通过 RDP 暴力破解进行传播，并使用 PowerShell Empire 和 PSExec 进行内网横向移动。

TFlower 执行后，会通过控制台窗口显示加密文件时所执行的操作；连接 C2 发送主机名、状态信息和加密文件数；查找并结束 outlook.exe 进程，避免文件被该进程占用而导致不能加密的情况；修改注册表项以达到开机自启动的目的；不加密 windows 和 sample Music 文件夹，保证系统正常运行；删除卷影副本、禁用自动修复功能、删除本地计算机的备份目录防止受害者恢复已加密的文件。该勒索软件并没有追加后缀名而是在文件首段添加了包含“*tflower”标志的字符串。TFlower 会在桌面创建一封名为“!_Notice_!.txt”的勒索信，勒索信中包含邮件联系地址等信息。目前被加密的文件在未得到密钥前暂时无法解密。

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。

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、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器等鉴定分析。

最终依据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	6c.exe
文件类型	BinExecute/Microsoft.EXE[:X64]
大小	1.31 MB
MD5	53C923D4E39B966AB951F9A3B9D090BE
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.DelShad
判定依据	反病毒引擎

◆ 元数据信息

描述	值
File Size	1340 kB
File Type	Win64 EXE
MIME Type	application/octet-stream
Machine Type	AMD AMD64
Time Stamp	2019:08:24 18:33:18+08:00
PE Type	PE32+
Linker Version	14.16
Code Size	841728
.....	.....

◆ YARA 信息

类别名称	行为描述
Anti	The name of the yara rule that was hit
WeakPassword	

◆基础信息

类别名称	行为描述
Hash	哈希算法
KeyBoxConstant	Crypt algorithm
.....	.....

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 09 月 30 日 (总第 202 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天产品巡礼 (系列一)——智甲终端防御系统

智甲终端防御系统是安天研发的面向政企客户的端点综合安全防护软件，产品为办公机、服务器、虚拟化节点、移动设备、国产专用计算机、各类自助终端、工控上位机等各类端点场景提供多层次、全周期的动态防护能力。

功能简介

智甲产品内置安天自主研发的下一代威胁检测引擎，基于黑白双控模式的安全策略，有效支撑终端检测与响应（EDR）。智甲具有恶意代码查杀、实时主防监测、勒索病毒增强防护、溢出攻击和横向系统防护等综合威胁防御功能；融合主机防火墙、终端管控、外设管控、漏洞扫描、集中补丁修复等管理功能；支持对 Rootkit、感染式病毒、宏病毒等内网顽固威胁的有效处置，结合安天独家的高级威胁追溯包服务，可以实现全网威胁追溯。

场景适配

智甲支持适配客户不同的网络环境（互联网 / 隔离网 / 混合网络等）的快速部署，并且可以与网络内其他安全设备进行联动，同时支持端点场景全要素采集以支撑态势感知系统。

智甲产品主要由客户端软件与管理中心两部分组成，客户端是部署于终端内的 Agent 和安全组件，主要用来监控用户系统环境变化，对已知威胁精准定性、对未知威胁初判告警、捕获上报，对各类威胁进行阻断拦截，对已遂威胁清除处置，并可以执行管理中心下发的多重处置任务。

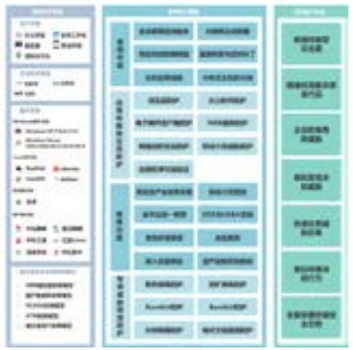
管理中心主要面向安全管理人员，对端点类资产进行统一安全管理，集中监测分析端点安全事件、制定和下发相关处置任务策略。管理中心通过智甲的信息采集形成端点资产地图、并可导入人员组织，建立端点资产部门和责任人归属。管理中心采用 B/S 架构，管理员使用浏览器即可访问管理中心。

智甲经过安天十余年的自主研发积累，形成了在恶意代码查杀、APT 防御、勒索软件防护、国产化平台防护支持方面的领先优势。

特点优势

• 支持为多平台、多场景提供安全防护能力

智甲支持防护多种操作系统平台，包括 Windows 桌面系统、Windows 服务器操作系统、Linux 系统、国产化操作系统、移动操作系统等，实现集中部署、实时监控、定时巡检、应急处置、威胁追溯等功能。支持针对网内不同重要程度或者防护等级的终端灵活设置防护策略。



▲智甲能力全景图

• 高级可持续威胁（APT）等防护能力

安天是国内高级威胁研究的领导厂商，通过对各种威胁行为体的作业手法、漏洞利用工具和高级木马的分析，安天不断改善威胁检测引擎和主动防御内核，通过扇区监控、内核服务和驱动监控、文件监控、注册表监控、浏览器和邮件客户端保护等机制，拦截格式文档攻击和横向移动。面对 APT 攻击，智甲采用“未知可疑程序捕获 + 管理端静态分析 + 文件关联分析 + 威胁清除追溯”的防护策略，终端会对新增的未知文件进行初步分析，针对发现的可疑程序会上报管理中心，管理中心集成有静态深度分析模块（安天下一代威胁检测引擎的分析模式），可以通过提取文件向量信息进行分析，判断文件是否为高危险文件，并且可结合安天追影威胁分析系统进行深度动态分析，包括呼叫安天支撑人员进行深度分析服务。一旦判断该文件为高级威胁载荷，可以通过文件关联分析排查出与该文件有关的其他攻击载荷，就可以针对相关威胁载荷进行统一清除，对其持久化进行处置。

▲APT 全网追溯（安天高级威胁追溯包服务）

▲2019 年 6 月 30 日起，安天智甲威胁告警体系已支持 ATT&CK 威胁框架

• 有效的勒索病毒防护

安天从 2014 年开始，持续跟进研究勒索病毒威胁机理，针对大量隔离网客户往往不能及时升级病毒库这一问题，力图使产品增强智能防护能力。安天采集归纳了近百种勒索病毒行为特征，构建了一个具有强大分析与判断能力的勒索病毒行为特征库，基于该特征库通过进程、线程行为分析，可以准确判断勒索软件删除和加密

（下接第三版）

每周安全事件

类 型	内 容
中文标题	APT28 组织在最近的攻击活动中增加了新组件
英文标题	No summer vacations for Zebrocy
作者及单位	ESET Research
内容概述	研究人员发现 APT28 组织于 2019 年 8 月 20 日针对他们以往的受害者的一项新攻击活动，这些受害者是东欧和中亚国家的大使馆和外交部。这项最新的攻击活动始于包含恶意附件的网络钓鱼电子邮件，该附件启动了很长的下载程序链，并以后门结尾。APT28 组织在其工具集中添加了一种新的开发语言，更准确地说是针对其下载器：Nim 语言。然而，他们的开发人员也忙于改进其 Golang 下载器，以及将其后门由 Delphi 重写为 Golang。
链接地址	https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

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

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	G-Ware/Android.FakeQB.k[rog,exp] 2019-09-22	中	该应用程序伪装成刷 Q 币工具，本身无实际功能，诱导用户分享推广该应用，会造成用户资费消耗，建议不要使用。
		G-Ware/Android.StealMoneyGame.eg[pay,rog] 2019-09-23	中	该应用程序是游戏应用，运行后弹出订购提示框，付费信息不明显，内嵌恶意支付插件，监听短信拦截指定短信，私自回复短信，会造成用户资费损耗，请卸载。
		G-Ware/Android.FakeFort.e[fra,rog] 2019-09-24	低	该应用程序伪装成黑客应用，无实际功能，运行问卷调查页面，请卸载。
	较为活跃样本	Trojan/Android.Banbra.b[prv]	中	该应用程序运行隐藏图标，诱导开启辅助服务，上传短信和程序安装列表信息，修改手机设置，访问指定 url，会造成用户隐私泄露，请卸载。
		RiskWare/Android.cocoam.b[prv]	中	该应用程序为特定模板生成，具有执行拨打电话、发送短信、发送邮件等操作的风险代码，还含有上传地理位置信息至远程服务器的敏感代码，会造成用户隐私泄露，建议卸载。
		RiskWare/Android.PJbocai.s[rog]	中	该应用程序为博彩类应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。
		G-Ware/Android.huaqindz.a[prv,rog]	低	该应用程序是一款偷拍工具，运行后私自打开相机，私自拍照并上传，可能造成用户隐私泄露，建议不要使用。
		RiskWare/Android.FakeQQ.at[fra]	低	该应用程序伪装成 QQ，无实际功能，会将用户输入的账号密码保存至本地，存在一定风险，请使用正版软件。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Excel 远程代码执行漏洞（CVE-2019-1297）	高	当 Microsoft Excel 软件无法正确处理内存中的对象时，该软件中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理员权限登录，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。
	较为活跃样本	RiskWare[RemoteAdmin]/Win32.RAdmin	中	此威胁是一个具有远程控制行为的风险软件家族。该家族可以对用户的设备进行集中管理，方便地进行远程控制。但对用户的隐私可能具有潜在的泄露风险。
		GrayWare[AdWare]/Win32.Kuaiba	中	此威胁是一种有广告行为的灰色软件家族。样本运行后会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。
		Trojan/VBS.Redirector	中	此威胁是一种使用 VBS 脚本编写的木马家族。该家族样本多为脚本或网页文件，运行后会重定向到有漏洞的恶意网页，窃取用户信息。
		Trojan[PSW]/Win32.Flystudio	中	此威胁是一种木马类程序。该家族可以连接网络，下载其他恶意代码或推广应用。它可以修改，并创建注册表项，在 Windows 启动时执行恶意代码。
		GrayWare[AdWare]/NSIS.ExtCrome	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，样本运行后会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。

（上接第一版）

文件行为并进行拦截，另外产品还具有文件锁定、文件备份等多种辅助手段，可以有效对各种已知和未知勒索病毒进行防护，在 2017 年 5 月爆发的 WannaCry 病毒，智

▲基于行为分析的勒索软件防护

甲 2016 年 1 月的版本即可实现有效防护。

• 领先的国产化防护能力

智甲是国内较早的支持为国产化操作系统提供安全防护的产品，具有可信验证、病毒查杀、进程防护、漏洞检测、虚拟补丁、终端管理、网络防护等多种功能。2015 年起，在国家相关部门的统一规划下，安天分别与中标麒麟、中科方德、银河麒麟等国产操作系统厂商进行了深入的代码级合作，实现了预装试点。2016 年，成功支撑了“型号首批万套部署”，获得了主管部门的高度认可。按照“国产硬件 + 国产化操作系统”的双国产组合计算，智甲已实现对近百种版本的环境良好适配，并且与中标麒麟、银河麒麟、中科方德、达梦数据库等厂商

▲部分产品互认证明

的产品具有兼容互认证明。

• 良好的运维管理能力与集成能力

除了恶意代码查杀功能外，智甲还具有漏洞与补丁管理、终端管控、USB 外设管控、移动介质专项管控、资产管理、数据采集、主机配置加固、主机防火墙等多种功能，可以全面提升端点资产可管理性、提升终端威胁对抗能力，降低终端违规行为事件发生可能。

同时，智甲不仅可以独立运行，还支持与其他安全产品进行集成，包括数据共

▲管理主界面图

享、指令调用等，形成联动防护能力。

• 可视化展示与管理

智甲具有专业的操作界面，并配合安天资产可视化管理中间件，实现形象直观的端点资产、威胁的展示：

基于网络拓扑和人员组织关系，通过 3D 可视化效果在控制中心页面展示整体资产分布、拓扑结构、当前整体威胁情况和 TOP 排名等；

查看资产细节信息、资产安全分组、资产人员归属等；

支持在可视化界面直接下发任务指令，进行威胁处置、漏洞修复、配置加固等操作，并能查看任务执行结果；

通过威胁追溯包，对特定威胁的内网横向扩散过程进行可视化分析展示，了解

▲可视化操作界面

威胁事件的攻击轨迹。

客户案例

安天智甲终端防御系统已在政府、军工、电力、能源、金融、制造业等领域广泛投入使用，典型案例包括：

• 某电力系统客户终端安全防护项目

产品自 2017 年初部署以来，稳定高效，帮助客户彻底清除了大量顽固的文件感染式病毒、有效解决了蠕虫在内网杀而复来的问题，对长期困扰客户的宏病毒实现了良好的查杀效果，并通过强大的病毒查杀与综合管控能力，极大提高了客户终端的安全性。

• 某电信运营商服务器安全防护项目

智甲虚拟化版本部署于运营商 DCN 和私有云网络内，为业务服务器提供恶意软件防护服务，通过安全策略模板，与客户业务环境良好适配，帮助客户多次有效防护了勒索病毒、挖矿木马等威胁，获得客户好评。

• 多家银行终端安全防护项目

为多家银行的办公机和 ATM 机提供病毒防护服务，其中针对办公机采用标准防护模式，针对 ATM 机采用“白名单 + 安全基线”的防护模式，产品不仅满足了客户安全防护需求，并且针对银行特殊的网络环境和终端环境，进行了良好适配。

• 某部队客户终端防护项目

安天智甲 2015 年开始部署，为某部队客户提供病毒防护服务，部署期间稳定可靠、防护能力真实有效，部署 4 年来，已保障各大基地多次任务。同时也为其态势感知系统提供数据采集和威胁处置支持。目前已是该客户网络中部署量最高的端点安全防护系统，并且近期已开始扩容。

• 某部门国产化终端防护项目

该项目中客户网内部署了大量国产操作系统终端，并且包括多个版本的操作系统，为了加强其终端的病毒防护能力，并实现防护能力全范围覆盖，该部门开始部署安天智甲终端防御系统。智甲系统部署后累计适配操作系统及子版本超过 30 种以上，安全防护方面不仅提供了病毒查杀、主动防御等基础功能，还提供了终端管控、外设管控、网络管控等加强能力，实现了良好的安全防护与管控效果。产品部署后，稳定可靠，与客户原有系统环境良好兼容。

微信扫描二维码阅读原文