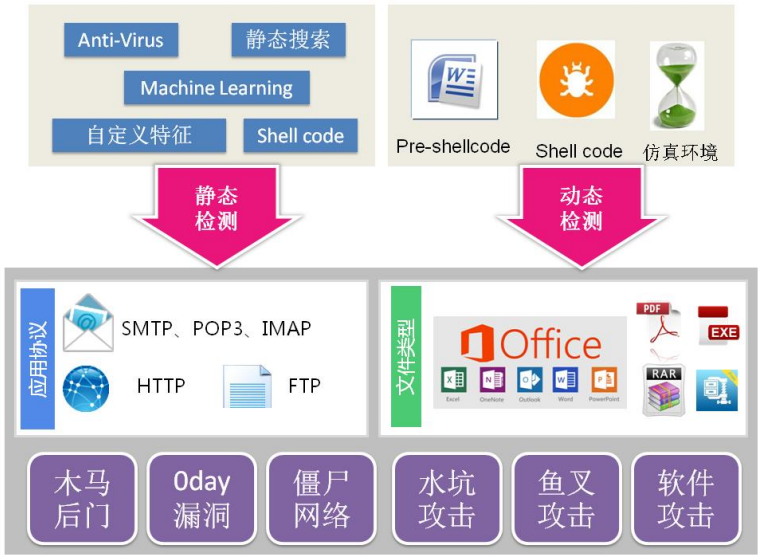
天阗高级持续性威胁检测与管理系统 V2.0

天阗高级持续性威胁检测与管理系统 V2.0（以下简称“天阗 APT”），是一款针对恶意代码等未知威胁具有细粒度检测效果的专业安全产品，可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测，由启明星辰集团独立自主研发。

天阗 APT，采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤，同时，产品可结合人工服务，有效发现 APT 攻击。



通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

一、核心功能

全面支持已知威胁检测

当前发布的天阗 APT，只需要添加入侵检测与管理系统功能模块，就可以实现已知威胁加未知威胁的全面检测，包括但不限于：病毒、蠕虫、木马、DDoS、扫描、SQL 注入、XSS、缓冲区溢出、欺骗劫持等攻击行为以及网络资源滥用行为（如 P2P 上传/下载、网络游戏、视频/音频、网络炒股）、网络流量异常等威胁具有高精度的检测能力，产品对已知威胁事件库完美融合。

对恶意文件的静态检测

静态检测是指通过一定的特征比对或算法对被检测文件的二进制内容进行匹配或计算的检测方法，静态检测并不真实的运行被检测文件。静态检测的方法有很多种，天阗 APT 针对未知 PE 文件特别设计了专用检测方法，主要包含通用检测方案和非通用检测方案。通用检测方案针对非 PE 文件内嵌恶意代码的特点进行检测，主要包含内嵌脚本检测、内嵌 PE 检测、内嵌 shellcode 检测三种检测方案。

对恶意文件的动态检测

系统使用多种虚拟机环境运行被检测文件，检测文件打开后的各种行为和系统环境等以确定文件是否具有恶意行为。动态检测的优点是检测率高、误报率低。

动态检测能在很大程度上克服静态检测的通过代码混淆，压缩加密等方式便被绕过的特点，直接把样本放到真实环境中模拟运行，并观察样本的恶意行为。当样本存在可疑漏洞利用行为、可疑文件动作行为以及可疑网络行为时则报警提示给用户。经过启明星辰研发团队对于漏洞攻击多年的研究经验，我们将漏洞样本的行为分为了上述三种，并针对上述三种行为设计了漏洞利用检测引擎，文件行为分析检测引擎和隐匿通道检测

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

引擎。

YARA 规则检测

支持 yara 规则检测，可自定义规则进行文件检测，同时支持导入 yara 规则，提升恶意样本检测的灵活性。

对 PCAP 文件回溯检测

支持手工导入 pcap 文件，进行离线流量检测。可以根据 pcap 包中的时间戳进行检测，回溯到流量当时发生的时间进行上报攻击。同时支持特征检测、文件还原、文件检测，做到全方位的回溯检测。

二、核心优势

动态静态检测，让恶意代码无处遁形

天阗 APT，针对 APT 攻击常常采用复合文档攻击的特点，本系统的动态检测系统创造性的采用了两大检测系统进行 APT 攻击检测：基于二进制的漏洞利用检测系统和针对 PE 文件的传统行为分析系统。之所以采用双系统检测 APT 攻击，是因为传统的行为分析系统在分析利用漏洞的复合文档时存在明显缺陷。

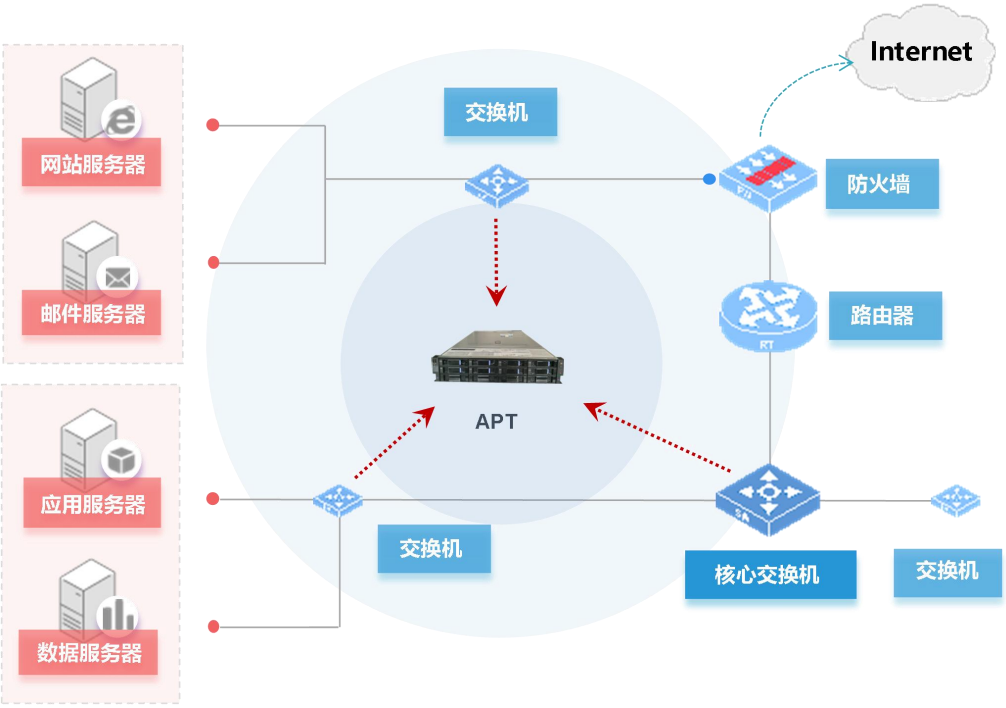
威胁情报应用，快速精准发现攻击威胁

通过内置公司自有的 VenusEye 威胁情报，可通过情报碰撞快速发现攻击威胁。情报种类覆盖 120 个 APT 组织、560 种家族信息、34 种情报大类。根据 IP、域名/URL、MD5 快速判断攻击威胁，提升检测效率。同时通过联网可进行云端威胁情报查询，可以利用情报实时进行云端检测。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

三、产品部署

天阗 APT 可支持单级或多级部署，通过 SPAN/TAP 部署方式，将设备并联到网络当中。天阗 APT 根据用户需求，提供多级部署方案，保证用户网络安全，也可提供与其他网络完全设备提供联动接口。



通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

二、产品规格

产品名称	**天阗高级持续性威胁检测与管理系统 V2.0**
产品型号	**APT3000-GCF-JL**
产品用途	主要用于针对恶意代码等未知威胁检测的系统，用于实现对未知恶意代码、嵌套式攻击、木马蠕虫病毒、隐秘通道等多类型未知漏洞(0-day)利用行为的检测。并对文件、数据报文等进行沙箱运行及分析，检测文件行为及调用异常行为；支持对进程行为、注册表行为、文件行为、可疑网络行为的检测，并生成恶意代码行为报告。
产品配置	国产化硬件设备，标准 19 英寸 2U 机架式设备；CPU 为 FT-2000+/64 核，操作系统为银河麒麟 V10；配置 4 个千兆电口（100/1000M 自适应），4 个千兆光口(含单模模块)，2 个万兆光口(含单模模块)，4 个接口扩展槽位；配置 128G 内存，8T 硬盘容量。配置双冗余电源（1+1 冗余电源，220V ±10%；50Hz±2Hz，单电源也可进行正常工作)，产品功率≤900W。
产品性能	文件检测量：2.5 万/天。
	网络层吞吐量：4Gbps。
	应用层吞吐量：4Gbps
	最大 HTTP 并发连接数：60 万
	每秒新建 HTTP 连接数：4 万
	检测文件格式种类：≥120 种。
产品功能	1、具备 120 种以上格式的文件检测能力，涵盖 Windows、Linux、麒麟 V10 操作系统等虚拟沙箱操作系统，支持自定义文件类型。
	2、具备 6 种检测机制，包含静态检测、动态/行为检测、情报检测、黑名单检测、YARA 检测、漏洞检测等，每种检测机制检测流程可自定义配置。
	3、不少于 10 种样本检测工作流配置，每种工作流可自定义选取相应的样

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	本格式，共计 129 条样本检测配置流。
	4、具备 40 种以上虚拟沙箱检测环境的能力。
	5、支持反沙箱检测不少于 6 种行为。
	6、具备恶意样本库、隐蔽信道库、威胁情报库的能力。
	7、具备检测流程配置模板。
	8、支持报文下载，支持下载匹配上特征检测策略的原始报文信息。
	9、具备事件特征库超过 5000 条，并且可以按照协议类型、攻击类型、安全类型、流行程度、事件级别等分类编排事件特征。
	10、具备策略集，包括失陷主机、行为分析、攻击路径策略集等。
	11、具备弱口令检测，口令配置项不少于 10 种。
	12、支持样本检测工作流配置，支持配置静态检测、静态检测+动态检测组合方式，静态检测告警再进行动态检测等，每种工作流可自定义选取相应的样本格式，检测流支持批量修改。
	13、具备邮件检测、HTTP 检测、FTP 检测、SMB 检测，支持可疑样本手动上传检测和接口上传检测。
	14、具备钓鱼邮件检测，自动识别邮件正文二维码、正文 URL 进行威胁鉴定，识别邮件代发、邮件仿冒。可自动提取正文中密码对已加密的附件进行解密检测。
	15、支持邮件正文内容提取并展示，可提取邮件正文中的 URL。
	16、具备流量过滤功能，可对不关注流量进行过滤不检测，可添加源 IP、源端口、目的 IP、目的端口进行过滤条件创建。
	17、具备违规连接监测，自定义监测条件可配置违规原因、源目 IPv4 或源目 IPv6、IP 别名、协议类型、源目端口等，触发违规连接条件后进行专项告警监测。
	18、支持离线流量检测能力，可上传 PCAP 报文进行威胁分析，可检测到

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	特征、域名、样本数据并进行威胁分析，记录上传时间、md5、检测日志数量，日志数量可进行下钻。
	19、支持检测 WEB 应用的攻击，如 SQL 注入、XSS 攻击、木马上传、系统配置等注入攻击，支持检测其他类型的 WEB 攻击，如目录遍历、弱密码、权限绕过、信息泄露、文件写入攻击、序列化攻击等。
	20、支持基于 webshell 函数的攻击特征检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含 preg_replace 代码执行等。
	21、支持识别抓取行为的扫描工具，如：Appscan、Burpsuitescanning、AcunetixWebVulnerabilityScanner、Netsparker 等。
	22、支持对协同联动设备提交的可疑样本文件展示其检测结果、检测时间、来源、类型、状态等信息，开放 API 上传接口。
	23、支持对文件运行产生的 C&C 地址的威胁情报检测机制，通过威胁情报标注样本的家族类型。
	24、支持加密压缩文件解密，支持压缩文件子文件单独检测，支持解压层最大 10 层。
	25、支持中文标签展示恶意代码类型，并支持按照中文标签检索。
	26、支持对文件样本的网络行为检测，记录文件运行时的网络通信会话，并支持在线查看源 IP、源端口、目的 IP、目的端口、数据长度、原始数据和 ASCII 编码数据等通信会话详情。
	27、支持 YARA 规则库的管理配置，支持自定义 YARA 规则进行检测，可以进行自定义 YARA 规则的创建、编辑、删除操作，可统计 YARA 规则下碰撞的告警统计。
	28、具备 WEB 攻击事件研判能力，能够明文展示攻击点请求头、请求体、响应头、响应体等报文内容，可以下载匹配上特征检测策略的原始报文。
	29、具备 FTP 加密方式外发样本，以及支持样本检测报告等自定义信息的

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	外发。
	30、支持对恶意样本进行动态行为分析，对恶意样本的进程行为、威胁行为、系统破坏、网络探测、恶意域名等行为进行监测分析，同时记录恶意样本的释放物信息。
	31、具备事件合并能力，并且可根据“周期”“次数”自定义配置。
	32、支持提供恶意代码行为的详细报告，能够显示进程/线程状态、注册表项操作、文件操作、互斥量操作、网络操作、服务相关、关键 API 调用等行为等信息供分析
产品环境	工作温度：5℃~35℃
	存储温度：-20℃~60℃。
产品可靠性	平均故障恢复时间≤30 分钟
配套资料、配件	提供完整的用户手册（提供纸质或电子版本的操作手册等技术资料），含纸质版 1 套和光盘 1 张。
	配件含万兆光纤 2 根，普通直连网线 2 根，电源线两根。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博