# 安天智甲有效阻断 VoidCrypt 勒索软件


近日，安天 CERT 在梳理网络安全事件时发现一个名为 VoidCrypt 勒索软件，该勒索软件最早发现于 2020 年 4 月，主要通过垃圾邮件进行传播。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 VoidCrypt 勒索软件的加密行为。

VoidCrypt 勒索软件运行后，调用 cmd.exe 实现如下行为：关闭 SQLWriter、SQLBrowser、MSSQLSERVER、MSSQL$CONTOSO1、MSDTC、SQLSERVERAGENT、vds 服务；关闭当前网络防火墙；删除卷影副本；禁用修复；删除本地计算机的备份目录等。之后开始加密计算机上的文件，在被加密文件原文件名后追加名为“Void”的后缀。VoidCrypt 在计算机桌面上创建名为“Decryption-Info.HTA”的勒索信，该勒索信内容包含勒索说明、联系邮箱和 Case_ID 等。


▲VoidCrypt 勒索信

VoidCrypt 勒索软件采用 AES+RSA 加密算法，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软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

## 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、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、关联分析鉴定器、信标检测鉴定器将文件判定为木马程序。

◆ 概要信息

| | |
|---|---|
| 文件名 | 052e5b2b806fb084632ef52b18f9fa296dcbff8e0751a095f1aaeb84b24e0c90 |
| 文件类型 | BinExecute/Microsoft.EXE[:X86] |
| 大小 | 993 KB |
| MD5 | 53C8F2FDA54EBA508C533283A8C2896F |
| 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 |

◆ 操作系统

| 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 |

◆危险行为

| 行为描述 | 危险等级 |
|---|---|
| 在启动时禁用 Windows 错误恢复 | ★★★★ |
| 通过 WMI 查询操作系统信息 | ★★★ |
| 通过 WMI 查询 CPU 信息 | ★★★ |
| 查询系统硬盘大小 | ★★★ |
| 文件篡改 | ★★★★★ |

◆常见行为

| 行为描述 | 危险等级 |
|---|---|
| 加载运行时 DLL | ★ |
| 创建挂起进程 | ★★ |
| 获取驱动器类型 | ★ |
| 获取系统信息（处理器版本、处理器类型等） | ★ |
| ..... | ..... |

◆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 2020 年 8 月 3 日 ( 总第 241 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 II
# 威胁框架在捕风蜜罐中的落地实践


安天捕风蜜罐系统是一款用于诱骗攻击者对其进行攻击从而捕获威胁并展示威胁信息的网络安全设备。该系统支持设备、资产、服务、漏洞仿真。通过创建与真实资产环境相似的高交互虚拟蜜罐和业务系统动态仿真蜜罐诱骗攻击者对其进行攻击，并对捕获到的数据进行分析，帮助企业客户发现内网威胁事件、攻击链、攻击阶段、攻击工具。安天率先将 ATT&CK 威胁框架应用到欺骗防御产品的研发与能力验证工作中，不仅使产品在仿真丰富性和未知攻击事件捕获方面的能力大幅度提升，还可以支持以攻击链形式展现网内威胁事件，并能对事件进行多维关联分析。

## 多维度提升对抗能力，有效应对威胁

随着攻击手段的不断变化，攻击手段呈现复合的、多载荷的特性，且攻击隐藏性很强，很多都是利用未知漏洞、自定义工具、或者社工、钓鱼等方式获取系统管理员帐号和权限，凭借合法身份、正常操作实施入侵，使得传统的安全防御手段失效，无法及时发现以及有效应对威胁。

攻击技术和手段日益更新，但对抗的安全产品更新速度慢，企业更新产品的周期也相对漫长，难以应对多变攻击手段、新型威胁。因此亟需能够应对变化的攻击手段和适应业务变更的新技术，通过对照 ATT&CK 框架可以看出，优秀的蜜罐类产品在面对装备最为精良、火力最为密集的攻击时，需具有以下能力：

(1) 丰富的仿真能力：能够在网络、资产、服务、漏洞等不同层级进行仿真，灵活支持业务系统的动态仿真，适应企业内部多样性的业务系统仿真需求；通过仿真成有漏洞的服务（web 服务、数据库、系统服务等）、操作系统等，欺骗攻击者，在和攻击者“交锋”的过程中，不仅保护了企业的真实资产，同时捕获攻击数据，用于进一步的研究。除了单节点蜜罐，还有多个蜜罐组成的可延展、可配置的蜜网，仿真企业网络活动，迷惑攻击者，使其被困在蜜网中。

(2) 全面的数据采集能力：能够采集从流量到系统，从系统底层到应用层的日志，原始的文件和网络数据包等数据。

(3) 深入的分析能力：能够识别单个战术技术行为，展示攻击的完整链条和行为阶段。蜜罐被用来感知内网威胁，需要具备威胁感知与捕获的能力，还要能够对攻击者溯源，需要知道攻击者做了什么、意图是什么、攻击者是谁从哪儿来。攻击行为的分析通常包括：捕获攻击数据包、记录攻击流量、保存攻击者上传的文件、识别攻击指纹等。攻击溯源多是对攻击数据的关联与整合，结合威胁情报与大数据等资源，对攻击者进行人物画像或是精准溯源。

为了提升安天捕风蜜罐系统的以上能力，引入 ATT&CK 威胁框架无疑是现

（下转第三版）

## 每周安全事件

| 类 型 | 内 容 |
| --- | --- |
| 中文标题 | 安全厂商披露 Lazarus 四个 macOS 恶意软件家族 |
| 英文标题 | Four Distinct Families of Lazarus Malware Target Apple’s macOS Platform |
| 作者及单位 | Phil Stokes |
| 内容概述 | Sentinelone 介绍与 Lazarus 组织相关的针对 macOS 平台的四个恶意软件家族。第一个为 DaclsRAT 恶意软件，通过被木马化的“一次性密码”（OTP）应用程序 TinkaOTP 传播，DaclsRAT 嵌入了开源 MinaOTP 项目的副本，以掩盖其恶意活动。第二个为 CoinGoTrade 和 Cryptoistic，通过建立的虚假网站，诱使用户下载恶意加密货币应用程序来传播。第三个为 OSX.Casso，是轻量级的后门二进制程序家族，主要是用 Objective-C 和 C 编写的，大量使用了内置在操作系统中的标准 C 库，通过恶意 Album.app 传播。第四个是研究人员所发现的 WatchCat 和 MediaRemote 的恶意软件样本。 |
| 链接地址 | https://www.sentinelone.com/blog/four-distinct-families-of-lazarus-malware-target-apples-macos-platform/ |

## 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 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

| 恶意代码类别 | 名称 | 威胁等级 | 简要描述 |
| --- | --- | --- | --- |
| 活跃漏洞 | Microsoft Windows 和 Windows Server 安全漏洞（CVE-2020-1436） | 高 | 当 Windows 字体库不正确地处理经特殊设计的字体时，存在远程代码执行漏洞。对于除 Windows 10 之外的所有系统，成功利用此漏洞的攻击者可以远程执行代码。对于 Windows 10 系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在 AppContainer 沙盒上下文中执行代码。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。 |
| | Microsoft Word 安全漏洞（CVE-2020-1447） | 高 | Microsoft Word 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的安全上下文中执行操作。例如，文件可以代表登录用户使用与当前用户相同的权限执行操作。 |
| | Microsoft Windows Graphics Device Interface 安全漏洞（CVE-2020-1435） | 高 | Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。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。 |
| 较为活跃样本家族 | Trojan[Backdoor]/MSIL.Bladabindi | 中 | 此威胁是一种使用 C# 语言编写的具有后门行为的木马家族。该家族木马为 NJ Rat 所生成的被控制端，在执行后会与远程服务器通讯并接收远程服务器的控制。该木马具有窃密行为和其他恶意行为。 |
| | Trojan[Backdoor]/Win32.CosmicDuke | 中 | 此威胁是一种后门类木马家族。该家族木马具有很多功能，例如记录键盘击键、获取剪切板信息、监视用户屏幕、窃取聊天软件、电子邮件账号密码，收集系统文件信息，将收集到的信息通过 FTP 发送到远程服务器，从远程服务器下载恶意程序等。 |
| | Trojan/Win32.Salgorea | 中 | 此威胁是一种可以窃取密码信息的木马家族。该家族木马运行后会窃取用户账户信息，记录键盘击键信息并将相关信息回传服务器。 |
| | Trojan[Backdoor]/Linux.Mirai | 中 | 此威胁是一种 Linux 平台上的僵尸网络家族。该家族木马主要是利用漏洞传播并组建僵尸网络。 |
| | Trojan[Backdoor]/Linux.Gafgyt | 中 | 此威胁是一种 Linux 平台上的具有 DDoS 攻击功能的后门家族。该家族样本运行后会在 Linux 上开启一个后门并允许远程控制端执行任意操作。 |
| | Trojan/Android.Fakeapp | 中 | 此威胁是一种伪装类木马家族。该家族样本通常伪装为主要应用程序（Fackbook 等），诱导用户输入账号密码，通过 firebase 联网上传或发送短信等方式窃取用户的账号密码，造成用户隐私泄露和资费消耗。 |
| | Trojan/Android.Hqwar | 中 | 此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。 |



（上接第一版）

阶段效果较好的一种选择。

从认识上来说，ATT&CK 可以帮助安全厂商对威胁有更深入的认知，由单载荷、单环节的层面提升到多个战术环节、多种攻击技术的层面，由被动防守的视角转变为以攻击者的视角去理解威胁。网空杀伤链框架采用攻击者视角对离散威胁事件形成整体性分析，以 TTP（Tactics, Techniques and Procedures；战术，技术与过程）为核心分析要素，针对攻击的行为特征而展开分析，指导蜜罐在诱饵布局，仿真资产服务、采集检测方面不断提升对抗能力。

从欺骗者角度来说，以威胁框架阶段的攻击行为路径指导蜜罐诱饵布局。例如攻击者对真实资产进行扫描，可以利用真实服务器的空闲端口进行流量转发，真假结合的方式迷惑攻击者。针对内网横向移动场景，则需在每个网段部署蜜罐探针，针对系统的浏览器、登录帐号或授权信息留下诱饵，进而吸引攻击。

从能力提升来说，框架着重于“突破后”分析，将防御重点由网络边界转为网络内部，针对内部扩散，攻击的系统行为可以指导蜜罐仿真和采集能力的方向，使仿真能力和系统采集能力有针对性的增强。以现实场景下的现实攻击行动为知识的分析来源，依据对真实 APT 攻击进行追踪分析，提炼出技术点，不断积累知识库，促使该框架基于可能遇到的实际威胁来完善，帮助产品不断丰富检测新的攻击手段的检测方法。

### 威胁框架在捕风蜜罐系统中的落地实践

通过演练复现攻击和威胁框架涉及的 TTP 方法，持续提升捕风蜜罐的仿真服务、系统仿真、网络仿真能力。提升相关捕获采集能力和行为识别能力。

▲初版蜜罐 ATT&CK 覆盖度

通过典型安全事件在 ATT&CK 的映射关系和捕风蜜罐的威胁框架覆盖度对比，可以清晰的认知到当前蜜罐对于攻击事件的感知存在不足。这为捕风蜜罐的能力点提升提供了明确的指导方向。在威胁框架中的各个阶段，除渗出阶段外的其他阶段蜜罐均有覆盖，但是覆盖的点比较单一。参考典型安全事件映射关系，可以通过攻防演练的方式对蜜罐进行感知能力测试，收集蜜罐采集的数据，定位蜜罐能力缺失的原因是基础数据采集能力不足，还是对威胁事件的判定不够全面。对于基础数据采集不足的情况，通过完善数据采集模块，提升蜜罐的仿真度和蜜罐对不同漏洞服务的版本支持，确保蜜罐对外具备一定的甜度，能够引诱到攻击者的攻击。对于判定能力不足的情况，通过丰富威胁事件判定的单点特征来提升判定能力。

通过归纳总结，安天捕风蜜罐系统覆盖了属于威胁框架中初始访问中利用有效帐户、网页挂马等威胁点，具体实例为对某服务漏洞攻击、暴力破解、web 服务资源篡改等威胁事件。ATT&CK 框架中的执行阶段主要是攻击者在目标环境中投放有效载荷进行执行。执行的方式有多种，主要通过调用系统工具及命令达到执行载荷的目的。常见的有：在 Linux 系统中使用 Wget、Curl 等系统工具进行恶意代码的下载、执行、提权等操作，在 Windows 中通过 vbs 脚本下载者，执行恶意代码，Office 打开附件执行恶意代码，也包含了 Mshta、Powershell、Regsvr32、Rundll32、计划任务、服务执行等多种执行方式，参考这些执行方式，蜜罐加强了系统工具执行的采集力度，感知到更多的系统威胁事件。

从 ATT&CK 对攻击阶段的划分结合蜜罐目前能够感知的到攻击威胁事件，对蜜罐的仿真环境进行了补充并优化了数据采集能力，新增了蜜罐内部网络之间的共享目录，允许恶意代码在蜜罐与蜜罐之间传播，开放了高交互蜜罐对应系统的远程管理功能，加强对内网传播常用应用端口探测事件的敏感度，例如：3389、445、139、3306 等，有效的增强了蜜罐对入侵事件的捕获与威胁传播的感知。

通过与 ATT&CK 能力的映射，捕风蜜罐的能力在以下方面实现了提升：

（1）增强安天捕风蜜罐的仿真能力。参考 ATT&CK 威胁框架，捕风蜜罐对照其规范的详细攻击阶段进行对照补足，从检测能力的补充进而丰富蜜罐的仿真能力，覆盖设备仿真、资产仿真、服务仿真等多方面的仿真能力。

（2）增强安天捕风蜜罐攻击事件的回溯能力。参考 ATT&CK 威胁框架知识，捕风蜜罐能够增强包括文件变化、进程操作、注册表、系统组件工具调用等方面的日志采集范围，利用日志以及威胁框架知识指导攻击事件检测，将捕获的攻击事件中使用的攻击技术映射到 ATT&CK，更好的理解攻击者的攻击手段及攻击目的。

（3）增强对威胁数据的精准判断能力。参考 ATT&CK 威胁框架知识，安天捕风蜜罐对攻击留下的日志、数据进行专项采集，例如：用户登录信息采集、外设文件利用采集、常用端口探测流量、自启动服务创建、自启动注册表新增动作采集，通过专项采集对威胁事件进行精准告警。

### 经验总结及威胁框架在蜜罐实践中的展望

ATT&CK 威胁行为框架提供了丰富且持续扩展的攻击方式划分，能够指导捕风蜜罐产品对安全事件进行系统科学的新增、分类。同时，威胁行为框架是基于攻击者视角包含全链路攻击的威胁框架，为攻击链路的回溯提供指导方法。

ATT&CK 威胁行为框架使我们对安天捕风蜜罐系统的威胁感知能力有了更清晰认知和衡量标准。通过威胁框架可以系统、科学的检验捕风蜜罐对于威胁感知的有效性，并持续的补充完善及优化。

微信扫描二维码关注公众号查看原文