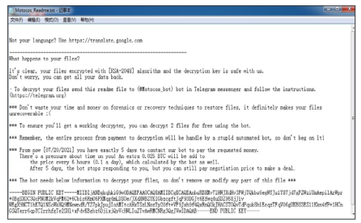
安天智甲有效防护 Motocos 勒索软件

勒索软件名：Motocos 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.mo2
支付与金额：支付金额：勒索时开始每6小时，增加0.025个比特币，5天内(包括5天)可按这种方式计算。5天后，需通过谈判支付具体金额 联系方式：Telegram 机器人账号(@Motocos_bot)
免费解密工具：暂未发现

近日，安天CERT在梳理网络安全事件时发现了一个名为Motocos的勒索软件。该勒索软件最早被发现于2021年5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Motocos勒索软件的加密行为。

Motocos勒索软件由Delphi语言编写，该勒索软件运行后分多步完成其既定任务。第一监控任务管理器进程，一旦该进程启动，立即结束；第二在加密前，持续枚举进程大概10分钟；第三遍历文件并对特定后缀名的文档、压缩包、图片、音视频、非系统应用程序等文件进行加密，加密后的文件名为“原始文件名+.mo2”；第四在加密过程中在每个逻辑盘根目录和系统桌面文件夹上释放以“Ransomware_Readme.txt”、“Motocos_Readme.txt”和“Readme.txt”命名的勒索信，三封勒索信内容一致，内容有勒索信翻译指南、勒索说明、加密方式、RSA公钥、Telegram联系方式和勒索金额，其中勒索金额从勒索时开始每六小时增加0.025个比特币；最后调用vssadmin.exe、wmic.exe、bcdedit.exe和wbadmin.exe命令删除系统卷影副本、禁用系统修复功能和删除系统备份目录，防止恢复被加密的文件，调用powershell命令删除有关应用、系统和安全的日志信息。



▲Motocos 勒索软件勒索信息

Motocos勒索软件采用“AES+RSA”加密算法组合的形式加密文件，目前被加密的文件暂时无法解密。

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，下为其自动生成的分析报告：

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、动态(Win7sp1 x86)鉴定器、字符串分析鉴定器、文件相似分析鉴定器、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(WinXP)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、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	88af65ad6b23ee2f9745ddacff604748
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.23 MB
MD5	88AF65AD6B23EE2F9745DDACFF604748
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Agentb
判定依据	反病毒引擎

报告地址：https://1.119.163.6/vue/details?hash=88AF65AD6B23EE2F9745DDACFF604748

◆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、Office2003、Flash、WPS、FoxitReader、AdobeReader

◆危险行为

行为描述	危险等级
映射内存方式注入	★★★
创建互斥量	★★★
延时	★★★

◆常见行为

行为描述	危险等级
创建可执行文件	★★
检测自身是否被调试	★★
资源释放	★★
……	……

◆扫描二维码查看完整报告

安天周观察
安天对外开放资料平台 安天官方微信
主办：安天 2021年07月26日(总第288期)试行 本期4版 扫描上方二维码查询安天所有对外开放资料

安天对“超高能力网空威胁行为体”系列分析回顾

安天自2010年以来，不断跟踪分析全球APT组织活动，特别是持续跟进分析研究美NSA下属“方程式组织”等超高能力网空威胁行为体的攻击活动、攻击装备、支撑工程体系，提出A²PT等术语用以标定相关攻击组织活动。发布过多篇高质量研究报告。2020年3月4日，为方便研究者和读者，我们曾发布名为《安天对“超高能力网空威胁行为体”系列分析回顾》的内容索引。近日外方又掀起抹黑所谓“中国发动网络攻击”的高潮，安天公众号重发此文，以便读者了解我国面临的网络安全风险。

背景概述

网空威胁行为体是网络空间攻击活动的来源，它们有不同的目的和动机，其能力也存在明显的层级差异。国家/地区行为体所发动的网络攻击，通常被称为APT（高级持续性威胁）攻击。而其中以美情报机构NSA下属“方程式组织”等为代表的超高能力国家/地区行为体，或称为超高能力网空威胁行为体，拥有严密的规模建制，庞大的支撑工程体系，掌控体系化的攻击装备和攻击资源，可以进行最为隐蔽和致命的网络攻击。安天将此类威胁行为体发动的网络攻击（如震网、方程式等）特别命名为A²PT（即高级的高级持续性威胁），在过去近十年（自2010年7月起）的时间里，对此进行了持续的关注和深入的逆向分析工作。其中部分工作成果已在安天官网或微信公众号公开，或刊载于技术媒体、安天技术文章汇编。为便于研究者深入了解A²PT攻击，本篇文献按照公开时间顺序将安天的分析成果形成如下索引摘要，便于网络安全工作者集中阅读参考。

2010-2012 以样本分析视角启动 APT 分析 跟进震网——APT 分析的起点

2010年7月震网事件曝光，伊朗铀离心设施遭遇长时间网络攻击，导致严重后果，引起全球关注。7月15日，安天启动分析工作，经过两个月的分析。2010年9月27日，安天发布《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》。报告中对Stuxnet蠕虫的攻击过程、传播方式、攻击意图、文件衍生关系进行分析，分析其利用的多个零日漏洞，总结该蠕虫的攻击特点，并给出解决方案，最后做出评价和思考。该报告是国内较早的通过逆向工程系统分析震网的全面报告，成为国内公众了解Stuxnet蠕虫攻击真相和细节的重要参考资料，报告内容也被多本书籍文献引用。

2013-2017 走向高级恶意代码体系分析 分析组件结构和持久化方法

2013年开始，安天逐步从单纯的样本模块分析走向攻击装备的整体分析，并深度跟进A²PT组织的新的恶意代码。2015年初，卡巴斯基曝光了美国情报机构NSA下属“方程式组织”所使用的能够对硬盘固件进行持久化的木马。这也给安天公开发布分析成果创造了契机。2015年3月，安天中英文双语发布第一篇关于“方程式组织”的分析报告《修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件》。报告对“方程式组织”相关组件：EquationLaser、EquationDrug、DoubleFantasy、TripleFantasy、Fanny和GrayFish的关联做了独家分析，并基于卡巴报告的指引，对硬盘固件重新编程机理和攻击模块nls_933w.dll做了强化分析，验证了超高网空行为体可在一切可持久化场景种实现持久化的能力。

2018- 至今 引入威胁框架 构筑态势感知能力

“方程式组织”攻击SWIFT服务提供商EastNets事件复盘分析报告

2019年1月，在第六届网络安全冬训营上，安天首次介绍了“方程式组织”对中东金融服务机构EastNets进行攻击的过程。这是安天将针对“方程式组织”的历史分析成果与“影子经纪人”泄露资料相结合形成的新的分析成果。2019年6月1日，安天正式发布公开报告《“方程式组织”攻击SWIFT服务提供商EastNets事件复盘分析报告》，报告精准还原了受到攻击影响的IT资产全景和拓扑关系，完整再现了杀伤链的全过程，详尽梳理了行动中使用的武器和作业流程，并以可视化方式予以复现。在报告中，安天在有关专家建议下，以“TCTF威胁框架”V2为参考，首次使用威胁框架对超高能力网空威胁行为体攻击行动的各阶段行为进行标准化描述和分类映射，协助分析这些行为体的意图和行为，为相关防御工作的开展提供借鉴。2020年1月，在第七届网络安全冬训营上，安天以态势感知和防御体系建设视角，对此事件做了重新梳理和解读。

小结

以上将安天在与超高能力网空威胁行为体所发动的A²PT攻击分析对抗中，以逆向分析为基础的公开成果按照时间关系进行了梳理呈列。除此以外，安天积极跟进与超级网空威胁行为体活动相关的信息，与业内专家携手，力求客观严谨进行分析验证，对改善防御提出建议。亦先后发布了《委内瑞拉大规模停电事件的初步分析与思考启示》、《实战化威胁猎杀，让威胁无处遁形——“美向俄电网植入恶意代码”等有关报道带来的启示》等报告。这些工作对推动用户改善防护，对我们自身提升核心产品能力均起到了积极的作用。同时，回看这些工作，还有很多不完备之处，还需要进一步的改进。(原文链接：https://mp.weixin.qq.com/s/RGIfplSiDK8_AQekn-nImA)

扫描右侧二维码阅读全文

每周安全事件

类 型	内 容
中文标题	CNCERT 发布 2020 年中国互联网网络安全报告
英文标题	无
作者	国家互联网应急中心 CNCERT
内容概述	2021 年 7 月 20 日，国家计算机网络应急技术处理协调中心（CNCERT/CC）编写的《2020 年中国互联网网络安全报告》正式发布。《2020 年中国互联网网络安全报告》汇总分析了 CNCERT 自有网络安全监测数据和 CNCERT 网络安全应急服务支撑单位报送的数据，具有重要的参考价值，内容涵盖我国互联网网络安全态势分析、网络安全监测数据分析、网络安全事件案例详解、网络安全政策和技术动态等多个方面。其中，报告对计算机恶意程序传播和活动、移动互联网恶意程序传播和活动、网站安全监测、DDoS 攻击监测、信息安全漏洞通报与处置、网络安全事件接收与处置等情况进行深入细致的分析，并对 2020 年的典型网络安全事件进行了专题介绍。此外，本报告还对网络安全组织发展情况和 CNCERT 举办的重要网络安全会议和活动等情况进行了阶段性总结，并对 2021 年网络安全关注方向进行预测。
链接地址	https://mp.weixin.qq.com/s/jAhWZzaq6mpyYt50L78Bhg

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 DNS 管理单元远程代码执行漏洞（CVE-2021-33750）	高	Microsoft Windows DNS 管理单元存在远程代码执行漏洞。由于该管理单元中的输入验证不正确，使得攻击者可以发送特制的请求并在目标系统上执行任意代码。
	HEVC 视频扩展远程代码执行漏洞（CVE-2021-33775）	高	HEVC 视频扩展存在远程代码执行漏洞。由于 HEVC 视频扩展中的输入验证不正确，使得攻击者可以发送特制的请求并在目标系统上执行任意代码。
	Microsoft Word 远程代码执行漏洞（CVE-2021-34452）	高	Microsoft Word 存在远程代码执行漏洞。由于 Microsoft Word 中的输入验证不正确，使得攻击者可以欺骗受害者打开特制文件并在目标系统上执行任意代码。
较为活跃样本家族	Trojan[Backdoor]/Win32.Padodor	中	此威胁是一种后门类木马家族。该家族样本会利用系统漏洞打开后门，为用户电脑带来更多威胁；它同时允许黑客远程进入并控制用户电脑。
	Trojan/Win32.Mansabo	中	此威胁是一种可以窃取密码信息的木马类家族。该家族的样本运行后会窃取用户账户信息，记录键盘击键信息，造成用户隐私泄露。
	Trojan/Win32.Vilsel	中	此威胁是一种窃密类木马家族。该家族木马通过垃圾邮件或恶意网站进行传播。该家族木马感染用户电脑后，会为黑客建立远程连接以控制用户电脑，窃取用户敏感信息（账号和密码等），同时会下载并运行其它恶意程序。
	Trojan[Dropper]/Win32.Miner	中	此威胁是一种可以释放比特币挖矿机的木马家族。该家族样本运行后释放恶意代码到本机 并运行，连接网络下载比特币挖矿机，占用系统资源，影响用户使用。
	Trojan[Downloader]/NSIS.Adload	中	此威胁是一种下载类木马家族。该家族木马通常使用 NSIS（开源的 windows 系统下的程序制作工具）将木马与正常程序捆绑在一起，主要功能是通过网络下载其他恶意软件。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan/Android.Boogr	中	此威胁是安卓平台上的伪装类木马家族。该家族木马通常伪装成游戏或流行应用程序，运行后可以下载其他恶意文件，将 SMS 消息发送给高价软件，或将受害者的智能手机连接到攻击者的命令和控制服务器。

实现 XDR 架构的三种方法

马克·所罗门 / 文 安天技术公益翻译组 / 译

在 2020 年，“扩展检测和响应”（XDR）解决方案开始受到关注。企业的首席信息安全官（CISO）将其列为需要了解的 TOP 1 技术趋势，以提高企业的检测精度、安全运营效率和生产率。安全供应商也迅速赶上潮流，将其产品重新塑造为 XDR 解决方案。

随着企业的安全运营中心（SOC）逐渐执行更多的威胁检测和响应任务，他们开始将 XDR 作为实现这一目的的方法。如果企业正在考虑采用 XDR 解决方案，则关于 XDR 的许多不同定义和方法可能会让他们感到困惑。在本文中，我们将介绍实现 XDR 架构的三种方法，以便为企业提供指导。

锁定一家供应商

该方法通常被大型安全供应商吹捧为“最佳路径”，能够促进安全产品（通常是基于云的产品）集成套件的使用。该方法强调简单性和全面的覆盖，听起来很有吸引力。但是该方法也面临着一些挑战。例如，企业通常使用许多不同的技术来保护自己，包括来自不同供应商的防火墙、IPS/IDS、路由器、Web 和电子邮件安全产品，以及端点检测和响应解决方案。此外，企业通常还会部署 SIEM 等工具，用以处理内部威胁和事件数据，包括票务系统、日志管理存储库和案例管理系统等。他们可能依靠“大型供应商”来处理大部分安全任务，但也会使用“最佳供应商”来处理大型供应商没有涉及或不擅长的领域。最近的一项研究发现，企业平均拥有超过 45 种不同的安全工具，而这些安全工具在大多数情况下都无法协同工作。出现这种情况的原因是：不同团队和部门会不断做出独立的决策和预算。

供应商必须要认识到，并非每个企业都会从一家提供商那里采购工具，且有些企业近期替换安全产品的兴趣也不大。此外，随着新用例、威胁和威胁向量不断出现，新的供应商和解决方案也会不断出现。

从供应商的核心技术开始扩展

该方法从供应商的核心技术（例如“端点检测和响应”[EDR] 或“网络检测和响应”[NDR]）开始扩展，然后通过与其他安全工具集成来添加额外的 XDR 功能。该方法能够为企业提供选择“检测和响应技术”领导者的机会，但也面临着一些挑战。举例来说，创建 XDR 架构的关键是集成；但是，供应商很有可能会侧重于核心技术的持续创新，从而破坏集成。此外，如果集成不是供应商的核心竞争力，则识别互操作工具与执行深度集成也需要大量的时间。

提供专注于集成的平台

供应商可以提供一个专注于集成的平台，跨不同攻击面和安全架构部署安全工具。该方法可以作为现有安全技术（包括供应商提供的 XDR 解决方案）之间的导管，能够提供功能更加丰富的 XDR 解决方案。该方法要求供应商的核心竞争力聚焦于集成和系统之间的数据流。如果企业并不是从零开始的，且各部门和团队拥有各种各样的解决方案，就可以选择该方法，以实现开放、可扩展的架构，使现有工具（包括 XDR 供应商不熟悉的产品）能够相互集成和互操作。该方法使用标准接口进行输入和输出，可以在几小时内写入和部署自定义连接器，以连接新的安全控制措施（解决新兴威胁）和内部老旧工具。

上述每种方法都有各自的利弊。如果企业决定通过供应商来实现 XDR 功能，则无论其采用哪种方法，都需要了解各供应商的聚焦点和核心竞争力、在向 XDR 过渡方面付出的精力，以及可能出现的分心情况。只有这样，企业才能确保选定的供应商可以提供 XDR 功能，以便跨所有架构和攻击向量实现检测和响应目标。

原文名称	Three Approaches to an XDR Architecture
作者简介	马克·所罗门（Marc Solomon），是 ThreatQuotient 公司的首席营销官。
原文信息	2021 年 7 月 15 日发布于 Security Week 原文地址 https://www.securityweek.com/three-approaches-xdr-architecture
摘 要	在 2020 年，“扩展检测和响应”（XDR）解决方案开始受到关注。企业的首席信息安全官（CISO）将其列为需要了解的 TOP 1 技术趋势，以提高企业的检测精度、安全运营效率和生产率。随着企业的安全运营中心（SOC）逐渐执行更多的威胁检测和响应任务，他们开始将 XDR 作为实现这一目的的方式。如果企业正在考虑采用 XDR 解决方案，则关于 XDR 的许多不同定义和方法可能会让他们感到困惑。在本文中，我们将介绍实现 XDR 架构的三种方法，以便为企业提供指导。
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。