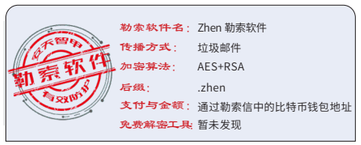
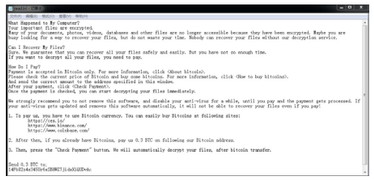
安天智甲有效防护 Zhen 勒索软件



近日，安天 CERT 在梳理网络安全事件时发现一个名为 Zhen 的勒索软件。该勒索软件最早发现于 2020 年 9 月，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。该勒索软件运行后，将在短时间内完成对计算机文件的加密操作。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 Zhen 勒索软件的加密行为。

Zhen 勒索软件样本运行后，首先，拷贝自身到 %programdata% 目录下，将拷贝后的文件路径加入到注册表启动项中，实现开机自启动；其次，创建一个以此拷贝后的文件为主体的子进程，创建后父进程退出，子进程在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.Zhen”命名的后缀；加密完成后，该勒索软件在 %programdata% 创建一个名为“read.ini”的勒索信，并在桌面创建一个名为“Read For Decryption”的勒索信快捷方式，同时更换系统桌面为该勒索软件的勒索提醒图片，勒索信和勒索提醒图片中包含了勒索说明、比特币购买教程、赎金金额（0.3BTC）和勒索者比特币钱包地址。



▲Zhen 勒索信

Zhen 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。

感染式恶意代码

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述感染式恶意代码进行有效检测，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、动态（WinXP）鉴定器、字符串分析鉴定器、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、YARA 自定义鉴定器、关联分析鉴定器、将文件判定为感染式恶意代码。

◆概要信息

文件名	zhen.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	7.11 MB
MD5	D5F9FA1A8DCA5319432F51A5891F 7794
病毒类型	感染式恶意代码
恶意判定 / 病毒名称	Virus/Script.AGeneric
判定依据	BD 静态分析

◆操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、 Flash、WPS、FoxitReader、Adobe Reader

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取系统信息（处理 器版本、处理器类型 等）	★
创建窗口	★
打开自身进程文件	★
读取自身	★★
释放 PE 文件	★
释放 PE 文件	★★
创建挂起进程	★★
获取主机内存信息	★★
获取计算机名	★
.....	.....

◆扫描二维码查看完整报告

安天周观察
安天官方微博 安天官方微信

安天在网安周期间分享《以威胁框架为参照系的产品能力演进》主题报告

2020 国家网络安全宣传周期间，全国政协委员、中国网络安全产业联盟理事长、安天集团创始人、董事长肖新光在“2020 年国家网络安全宣传周——网络安全产业创新发展主题论坛”和“2020 年民航网络安全年会”上分享了主题报告《以威胁框架为参照系的产品能力演进》。

以下为报告摘选，完整内容请扫描二维码查看。

当前网络安全正在经历能力导向建设模式的变革。网络安全规划方法不断系统化和完善；大量机构都在建设态势感知管理平台等顶层能力；新技术、新理念、新产品，也不断涌现。在这种热潮中，我们仍需要看到，如果安全产品本身无法满足威胁捕获、检测、防护、分析、处置的基础功能需求，无法达成有效的安全能力价值，就很难有效支撑起解决方案中的角色定义，使安全规划成为空中楼阁。因此安全产品对抗威胁的能力的有效性提升，同样迫在眉睫，威胁框架对此提供了非常好的指引作用。

从安天自身对抗的经验来看威胁框架的意义

在笔者所从事的恶意代码检测与威胁对抗领域，过去 20 年，经历了威胁形态、样式、种类的高速裂变。我们以恶意代码种类为例：

我们将国际知名厂商卡巴斯基的命名列表作为一个度量衡，来看一下从 2000 年到2018年间恶意代码命名数量的总量情况，可以看到在近 20 年的时间里，恶意代码种类数量膨胀了超过 400 倍以上。

而从载荷检测的反病毒规则上来看，以安天自身为例，从 2000 年的不足 1 万条规则，到目前已经超过 5000 万条的本地化规则，已经膨胀了 5000 倍左右，这还不包括数以十亿计算的云端规则。但这其中还有一个很重要的矛盾，那就是反病毒引擎所输出的病毒名称，例如 Trojan/Win32.Lmi.a 尽管包含了分类、平台、家族名称、变种号等信息，但其对安全分析的决策支撑作用非常有限。为此，安天引擎不仅输出有效的分类命名，还进一步提供部分知识标签信息，比如格式标签和核心行为标签等，但我们在态势感知的研发中，依然认为相关信息距离分析与决策所需要的更丰富的对载荷的技战术的能力评价还相距甚远。

从网络检测能力的相关变化和相应事件分类的情况来看，以国际知名的开源 IDS 软件 Snort 为例，通过观察它的威胁分类从 2003 年到 2019 年的相关变化，可以看到从网络侧检测恶意攻击行为的分类有部分能力增补，同时也有一些包括漏洞号、协议、格式等相应标签的输出。但其提供的信息依然是有限的。其对相关事件的风险价值，属于既遂还是未遂的攻击，属于杀伤链的何种阶段，都未能给出清晰的信息。

因此安全产品如果只能输出对威胁的分类信息和简单的辅助信息，是不足以支撑攻击分析的，而需要构建起检测能力和杀伤链、技战术动作的标签化输出能力，包括对载荷的技战术动作的评价能力。

在这个过程中，安天曾提出威胁认知模型的思路，也试图和 STIX 建立一种映射，但最终我们意识到，实际的问题并非我们的模型是否足够的完备和先进，而是不同厂商都在试图推动一种自己的认知分类、知识化标签以及 TTP 描述方式，导致了难以实现有效的相互通联。在这个情况下，就需要有统一的技战术描述方法和分析架构。从目前来看，ATT&CK 框架已经成为基于威胁框架角度的一个具有丰富实战细节的标准，其本身构建于洛马杀伤链模型基础之上，通过矩阵化扩展而提供更细粒度的分析能力，因此我们决定全面靠拢 ATT&CK 框架。

▲ 安天智甲终端防御系统
基于 ATT&CK 的分析结果输出

从整个 ATT&CK 框架的结构来看，主要包括 ATT&CK for Enterprise 和 PRE-ATT&CK。我们可以看到其与杀伤链模型的映射，以及主要的 12 个攻击战术与相关攻击技术的构成关系。但其所展开的矩阵是一个攻击者可选择的丰富的攻击组合，并没有绝对的时间顺序的关系，而且它可能是多次的反复调用或者是前后搭配衔接。

.....

每周安全事件

类 型	内 容
中文标题	Samba 发布了一个安全补丁解决 Zerologon 漏洞
英文标题	Samba addresses the CVE-2020-1472 Zerologon Vulnerability
作者及单位	Pierluigi Paganini
内容概述	Samba 团队已经发布了一个安全补丁，以解决 Microsoft Windows Netlogon 远程协议（MS-NRPC）中的 Zerologon（CVE-2020-1472）漏洞。根据警告，Samba 也只在用作域控制器时容易受到 NetLogon 漏洞的攻击，Active Directory DC 设备受到的影响最大。仅将 Samba 作为文件服务器运行的默认安装不会直接受到影响。
链接地址	https://securityaffairs.co/wordpress/108659/security/samba-addresses-zerologon-vulnerability.html

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 Excel 安全漏洞（CVE-2020-1594）	高	Microsoft Excel 中存在授权问题漏洞。该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足。攻击者可以利用该漏洞获得与当前用户相同的用户权限。
	Microsoft Dynamics 365 和 Microsoft Dynamics 安全漏洞（CVE-2020-16862）	高	Microsoft Dynamics 365 (on-premises) 存在远程代码执行漏洞。该漏洞允许攻击者向易受攻击的 Dynamics 服务器发送特制的请求，从而导致攻击者可以在 SQL 服务帐户中运行任意代码。
	Microsoft Windows 安全漏洞（CVE-2020-1319）	高	Microsoft Windows Codecs 存在安全漏洞，该漏洞源于处理内存中的对象，存在远程执行代码漏洞。攻击者可利用该漏洞获取信息，从而进一步入侵用户系统。
较为活跃样本家族	Trojan[Backdoor]/Win32.Tiny	中	此威胁是一种窃密类木马家族。该家族木马运行后连接远程服务器下载恶意代码并执行，可以窃取用户敏感信息。
	Trojan/Win32.SelfDel	中	此威胁是一种对恶意木马家族。该家族木马的主要功能是对抗反病毒软件或安全工具，通常会关闭反病毒软件或安全工具的进程。该家族木马同时还具有删除反病毒软件的病毒库、文件或安全工具的功能。
	Trojan[Packed]/Win32.Krap	中	此威胁是一种窃取账号信息的木马类家族。该家族木马运行后会注入系统进程，并监视正在运行的窗口标题，利用键盘 hook、内存截取或者封包截取等方式窃取账户信息并将这些信息发送到指定的服务器。
	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.Patched	中	此威胁是一种窃密类木马家族。该家族木马运行后，打开 IE 浏览器，并将木马中的 shellcode 读到内存中并执行，具体操作为记录 WINDOWS 登陆账户信息，试图窃取 SQL 账号密码信息，以 URL 方式发送到作者服务器中。
	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。

增强网络弹性的五种方法

安德鲁·鲁宾 / 文 安天技术公益翻译组 / 译

在家工作的情况不会很快消失，这会导致漏洞数量不断增加。这意味着，网络弹性对企业的弹性恢复能力至关重要。

新冠肺炎疫情迅速改变了我们的生活和工作方式。医生在餐桌上指导远程医疗，高管使用家庭网络管理整个企业，成千上万的银行家使用自己的笔记本电脑在家中管理全球经济。

现实情况是，大多数企业并没有为如此大规模的数字化转型做好准备。因此，攻击者有了可乘之机。随着企业转向数字化技术（特别是笔记本电脑），连接变得更加不稳定，网络也未受到妥善保护。众所周知，利用一台笔记本电脑执行一次勒索软件攻击，就会使企业的业务陷入停顿。

显然，在可预见的未来，远程工作仍会是一种重要的工作方式。当员工在办公室之外工作时，就无法受到企业的保护，企业的安全性就会变弱。不断增加的漏洞意味着，网络弹性对企业的弹性恢复能力至关重要。企业领导者可以采取以下五种方法来缓解风险和保护企业。

实施“零信任”框架

企业应抱有“假定出现攻击”的心态，并实施“零信任”框架，这是迈向弹性恢复能力的第一步。不要盲目信任网络内的流量，而是要假定一切流量都有可能是危险或恶意的。通过部署零信任框架，企业能够消除对任何内部或外部源的自动访问，转而采用白名单模型——仅允许端点连接到绝对必要的端点，并且不允许未经授权的横向移动。这意味着，即使有一个端点被感染，其他端点也不会受到影响。

采用最低权限原则

企业要进行网络监管，这是实施零信任框架的起点。企业应按照最低权限原则，规定员工能够访问什么内容以及哪些地方。管理员应确定允许在网络上通信的授权应用程序和服务。此外，企业要监控其网络，以确保没有错过任何内容。最后，启用“强制执行”以阻止任何不允许的操作。通过实施最低权限原则，管理员能够阻止不必要的网络通信。

多个安全层

在当今世界，仅一个安全层是远远不够的。企业需要考虑，如果其第一道防线失败，会发生什么。企业应采取什么措施，来降低初始攻击的影响？企业可以考虑将零信任原则扩展到边缘以保护其端点，实施多因子身份鉴别或单点登录以 增强口令安全，或者利用网络分段来补充防火墙。企业必须面面俱到才能有效保护企业，而攻击者只需找到一个漏洞就能发动攻击了。不幸的是，攻击者有的是时间，因此企业需要尽一切努力来增强已有防御。

通过网络分段阻止横向移动

如果企业认为将要发生攻击，则必须努力将其造成的损害降至最低。网络分段可防止攻击者和威胁横向移动（从一台笔记本电脑移动到另一台笔记本电脑）。这和潜艇上的隔间是一样的概念。潜艇被划分为多个单独的舱室，即使一个舱室发生漏水，其他舱室及其乘员的安全也能得到保障，整个潜艇不至于沉没。在网络安全中，我们可以对各个端点进行分段。即使勒索软件感染甚至禁用了一台笔记本电脑，也无法利用该电脑来感染其他电脑。该勒索软件只能局限在第一台受感染的笔记本电脑中，其他电脑可以继续运行。通过这种方法，即使企业未能阻止入侵，也不会发生灾难性事件。

专注于最重要的因素

企业可以采取很多措施来提高其安全性，但是企业的资源通常是有限的。因此，企业应专注于对其整体安全状况产生最大影响的因素，这一点至关重要。首先，企业要确定其关键任务资产，并围绕这些资产实施零信任框架——为了保护企业的高价值数据，这一点一定要做到。其次，企业应部署其他安全控制措施。这样，即使第一道防线失败了，也能够保护企业及其数据的安全。另外，企业应确定业务优先事项，并制定反映这些优先事项的现实策略。

原文名称	5 Steps to Greater Cyber Resiliency
作者简介	安德鲁·鲁宾（Andrew Rubin）。安德鲁·鲁宾是 Illumio 首席执行官兼创始人。
原文信息	2020 年 9 月 21 日发布于 Dark Reading 原文地址 https://www.darkreading.com/risk/5-steps-to-greater-cyber-resiliency/a/d-id/1338893
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。