白皮书

利用 Akamai 企业安全套件打破勒索软件杀伤链

目录

简介

利用 Akamai 企业安全解决方案，在杀伤链的各个阶段击溃勒索软件攻击

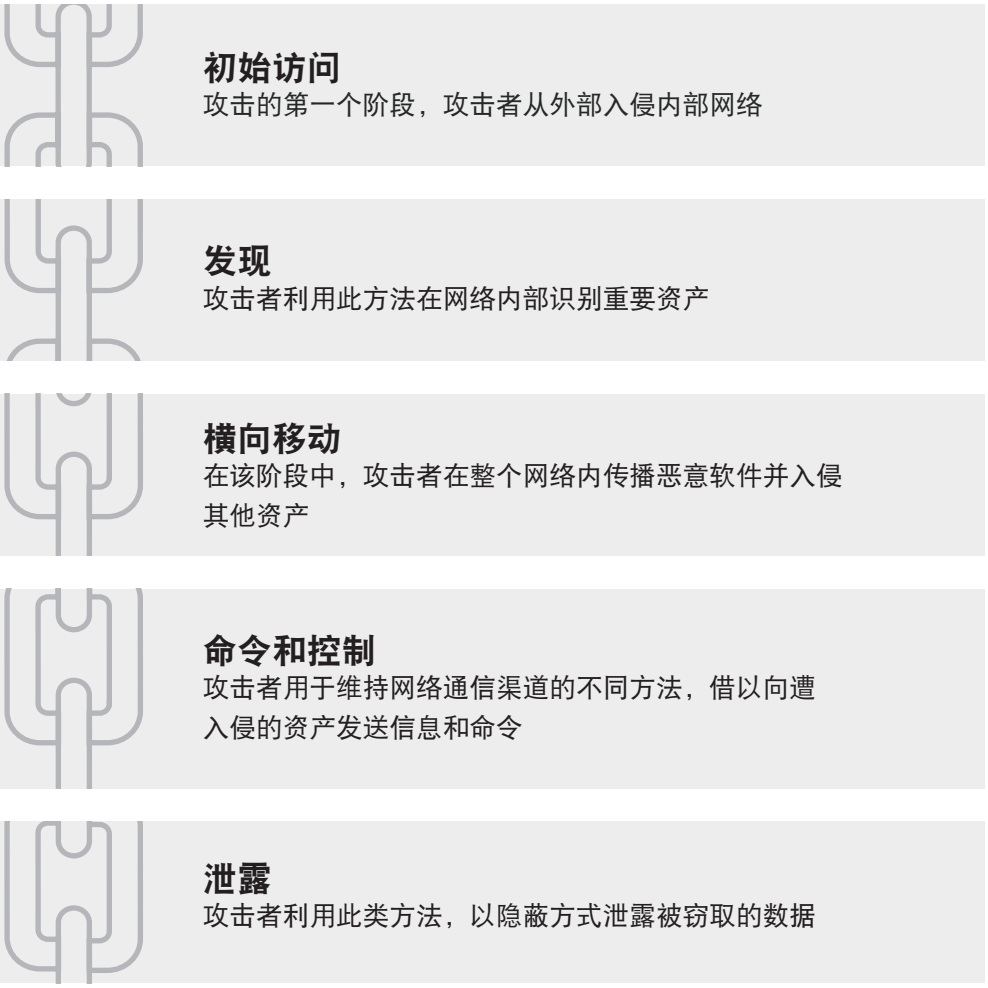
企业如今面临着诸多安全威胁，其中一种就是勒索软件，这种形式的恶意软件旨在对设备上的文件进行加密，使其变得无法使用。随后，恶意软件操纵者会以提供能够恢复文件原始数据的解密密钥或者软件为筹码，对企业提出勒索。近年来，勒索软件犯罪团伙的手段层出不穷，并且开始以外泄受害者数据作为额外筹码，威胁要公布这些数据或在暗网上出售。

要想能够抵御这类攻击，就必须了解勒索软件犯罪团伙是采用何种手段来实现其目标的。本白皮书将帮助您切实了解这方面的知识。

了解勒索软件杀伤链

勒索软件攻击的过程比较复杂，突破系统防御只是开始。为了尽量增强杀伤力，攻击者还必须将恶意工作负载扩散到整个网络，然后才开始加密。如果只是对一台计算机加密，攻击者就没有足够的筹码来勒索赎金。勒索软件攻击想要得逞，攻击者必须执行多个步骤，包括发现网络资产、横向移动等等。这些步骤就是通常所说的勒索软件杀伤链。

在这一链条的每个步骤中，都有许多机会能够检测和抵御攻击。利用 Akamai 企业安全套件提前为网络做好准备，从而减小攻击面，甚至提前一步帮助您抵御并控制勒索软件有可能造成的任何损害。本白皮书将详细介绍如何利用 Akamai Guardicore Segmentation、Enterprise Application Access 和 Secure Internet Access，从而在杀伤链的各个不同步骤中检测并阻止勒索软件活动。



初始访问
攻击的第一个阶段，攻击者从外部入侵内部网络

发现
攻击者利用此方法在网络内部识别重要资产

横向移动
在该阶段中，攻击者在整个网络内传播恶意软件并入侵其他资产

命令和控制
攻击者用于维持网络通信渠道的不同方法，借以向遭入侵的资产发送信息和命令

泄露
攻击者利用此类方法，以隐蔽方式泄露被窃取的数据

初始访问

每家企业都有着大量的互联网接口。这些接口可能会成为攻击者的切入点，让他们得以入侵网络。Akamai 可帮助您严密地保护这些接口，将攻击者拦截在网络之外。

保护面向互联网的服务器安全

利用 Secure Internet Access 有效负载分析功能，保护面向互联网的服务器免遭入侵

据 Kaspersky 介绍，攻击者最常用于获取初始访问权限的方法是入侵面向互联网的应用程序，并且通常是利用未经修补的系统上的一日漏洞。例如 Log4Shell (CVE-2021-44228) 和 ProxyLogon (CVE-2021-26855)，这些漏洞如今依然被广泛利用于入侵网络和部署勒索软件。

Enterprise Threat Protector 在经过配置之后，可以监控面向互联网的服务器上的所有入站 Web 流量。随后将对这些流量进行分析，从而识别并阻止任何恶意或异常活动。

阻止网络钓鱼 URL

利用 Enterprise Threat Protector 的 URL 检查功能，检测并阻止网络钓鱼企图

网络钓鱼是一种极其常见的网络入侵方法。攻击者常常会发送包含恶意附件链接的电子邮件，或者假冒登录页面以图窃取登录凭据。在您的端点上部署 Enterprise Threat Protector 客户端之后，您就能够实时扫描用户点击的每个 URL，从而识别并阻止任何恶意或异常链接。

减小 VPN 攻击面

利用 Enterprise Application Access，实现安全且具体到应用程序的 VPN 访问，同时减小外部攻击面

在当今的混合办公时代，远程办公已经成为常态，因此用户使用 VPN 登录企业网络的情况越来越普遍。攻击者也“顺势而为”，开始利用这一机会来获取企业内部网络的访问权限。他们常常会攻击员工的个人电脑并窃取其 VPN 凭据，然后用于访问企业内部网络。在某些情况下，攻击者还会攻击存在漏洞的服务器以窃取凭据。2022 年 11 月，攻击者就曾利用 Fortinet VPN 服务器中的漏洞获取初始访问权限，然后将勒索软件进一步扩散到了整个网络。

借助 Enterprise Application Access，您可以对网络实施基于角色且具体到应用程序的访问，从而显著降低这一风险。这款解决方案与传统 VPN 不同，它不会对用户授予整个网络的完全访问权限，而是仅允许用户对指定的应用程序进行有限访问。这样，即使攻击者成功窃取了用户凭据并绕过 MFA 保护，也仍然无法访问整个网络，只能访问有限的一组应用程序。

命令和控制

阻止命令和控制 (C2) 服务器

利用 Akamai Secure Internet Access，阻止已知的恶意命令和控制服务器

恶意软件（特别是勒索软件）通常需要与外部 C2 服务器进行通信，以从受到感染的网络资产发送命令并检索信息。通过对 Akamai 广泛的通信数据进行分析，我们将能够监控勒索软件和恶意 C2 域名，并持续跟踪新出现和不断发展演变的各类攻击活动。利用 Enterprise Threat Protector 客户端，我们能够实时监控您的整个 DNS 通信，并阻止与恶意域名的通信，从而防止恶意软件毫无阻拦地运行并达成其目标。

发现

攻击一旦侵入网络，就会尝试识别其他网络资产以了解网络结构，然后再开始横向移动。这通常需要进行内部通信，而 Akamai Guardicore Segmentation 就能检测到这些通信。

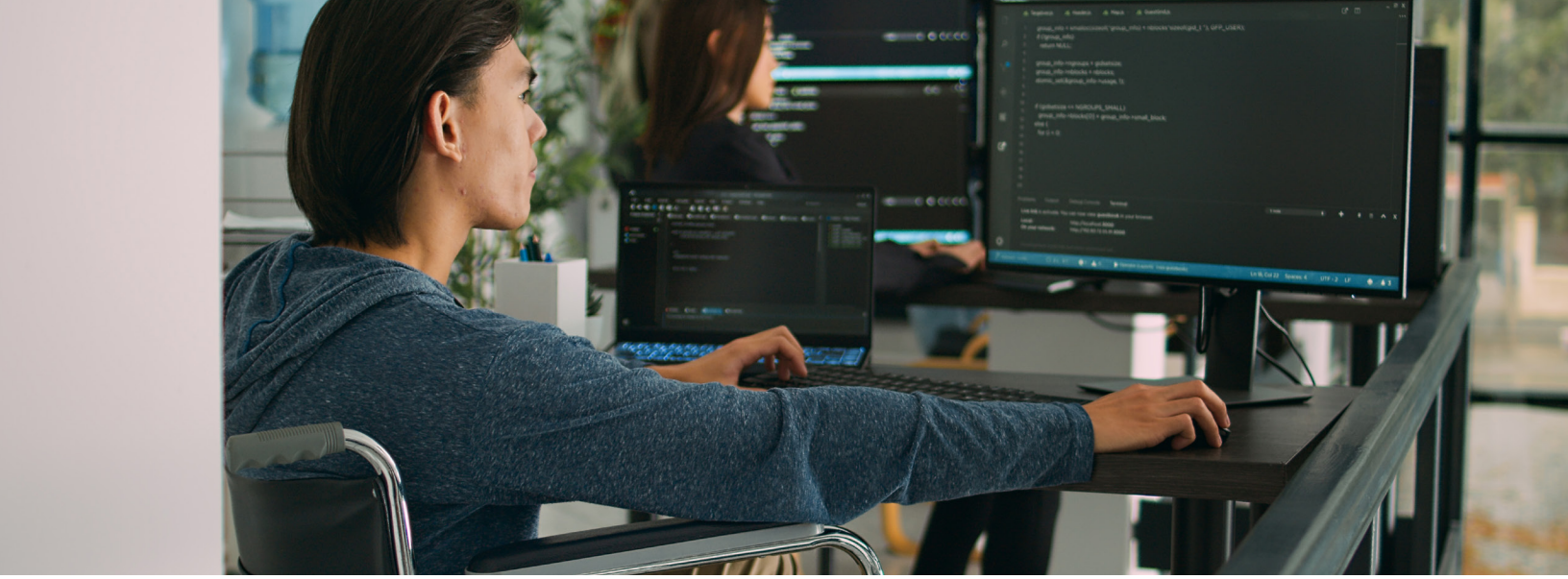
识别网络扫描

利用 Akamai Guardicore Segmentation 检测器，识别可疑的网络扫描

攻击者经常利用端口扫描来识别网络服务，从而达到执行网络发现的目的。据观察，许多勒索软件犯罪团伙都在使用开源网络扫描器。近期的一份关于 LockBit 3.0 勒索软件的 CISA 公告指出，该团伙使用了“SoftPerfect 网络扫描器”来执行端口扫描。另一个例子是 Nokoyawa 勒索软件犯罪团伙，观察发现他们在扫描网络以查找 SQL 服务器，以图访问其中的敏感数据。

Akamai Guardicore Segmentation 可以监控网络中的所有通信，同时其内置检测器还能识别此类扫描活动并发出告警，从而帮助您提前阻止恶意软件的传播。

图 1：Akamai Guardicore Segmentation 中的网络扫描事件



利用欺骗服务抵御发现企图

利用 Akamai Guardicore Segmentation 识别网络发现企图

当攻击者入侵网络时，他们事先并不知道网络的结构以及其中包含的各类资产。为了弥补这一不足，他们不得不以手动方式“摸黑探索”以图探明路线。在 Akamai Guardicore Segmentation 中，您可以通过欺骗服务对这一点加以利用，即引诱攻击者进入蜜罐服务器、监控其活动，并在检测到异常情况时向您发出告警。

例如，某位攻击者正在入侵网络，并且试图对某台 Linux 服务器的 SSH 凭据进行暴力破解。Akamai Guardicore Segmentation 会发现这一异常情况，并将攻击者引入一个动态生成的蜜罐。一旦落入蜜罐之中，攻击者的所有行动都将被记录下来，然后生成一则告警。

以下就是此类告警的一个示例：

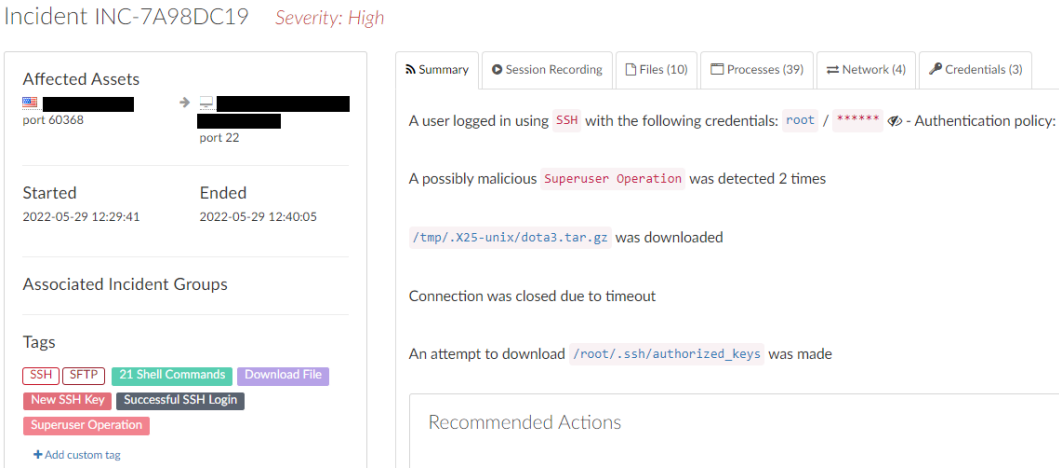


图 2：Akamai Guardicore Segmentation 中的欺骗事件

横向移动

攻击者获取网络访问权限并熟悉其拓扑结构之后，下一步可能就是利用网络来进行横向移动。现代勒索软件团伙会入侵网络并进行横向移动，以尽可能攻击更多的网络资产，将它们全部加密。利用 Akamai 企业安全产品，您可以对横向移动的可能性加以限制，从而尽可能缩小攻击范围。

识别可疑主机迹象

利用 Akamai Guardicore Segmentation 的 Insight 模块，通过各种方法识别可疑主机迹象

攻击者会利用 PowerShell 工具来达到各种目的，其中之一就是执行横向移动。PowerShell 传播程序极为常见，攻击者经常会将其用作在遭入侵资产上执行的第一段代码。最近发生的 Quantum 勒索软件感染事件正是采用这样的方法，即运行 PowerShell 代码以入侵 Windows Management Instrumentation (WMI)。

利用 Akamai Guardicore Segmentation 的 Insight 模块，您可以运行计划好的查询来扫描所有资产上的 PowerShell 事件日志，然后对存在恶意迹象的资产进行标记和隔离。

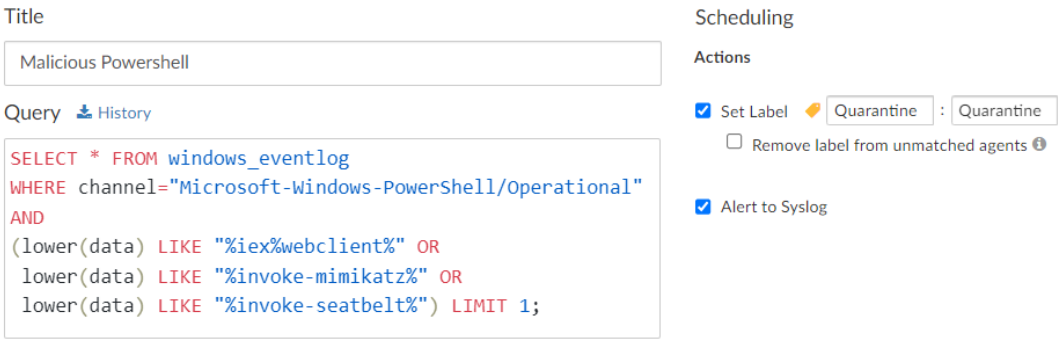


图 3：创建计划的 Insight 查询以检测恶意 PowerShell 事件

但是，PowerShell 只是可疑迹象的一个例子。您还可以利用 Insight 来扫描多种多样的横向移动迹象，并且使用现有的任何 osquery 表，例如：

- 使用 File 表，基于名称或哈希标签来检测恶意文件
- 使用 Startup Items 表，检测资产上的可疑自动运行条目
- 使用 Yara 表扫描资产上的文件，同时利用 yara 规则来检测恶意软件种类

阻止 LAN 攻击

利用 Akamai Guardicore Segmentation，检测并阻止本地网络协议上的攻击

在侵入网络上的零号目标之后，攻击者会利用 LAN 协议（例如 ARP）中的漏洞来攻击其他资产。如果是使用传统防火墙，此类攻击很容易就能躲过探测，因为它们是在第 2 层中执行的，而这种类型的通信并不会触碰到防火墙。

Akamai Guardicore Segmentation 采用基于软件的检测方法，使您能够监控并阻止传入或传出资产的所有流量，即使是通常不会触及强制性防火墙的本地流量，也同样无法避开检测。

限制管理端口

利用 Akamai Guardicore Segmentation 创建进程级别的策略，以减小敏感端口的攻击面

一旦成功入侵网络，攻击者通常会对遭入侵的资产执行特权提升，目的是为了窃取凭据。获得凭据之后，攻击者常常会使用 RDP、RPC、SMB 和 WinRM 之类的管理协议，在网络内的所有资产上执行勒索软件有效负载。然而，完全阻止这些端口的做法往往并不可取，因为管理员还需要使用这些端口来完成常规操作。

借助 Akamai Guardicore Segmentation，您可以应用进程级别的策略，确定哪些进程应该通过敏感的管理端口进行通信。以 WinRM 为例，这是许多管理程序所使用的端口，包括 Ansible。但是，常常也会有攻击者使用 Evil-WinRM 等工具，利用此端口来执行横向移动。我们可以使用 Akamai Guardicore Segmentation 来创建策略，仅允许来自 Ansible 进程的入站 WinRM 连接，同时阻止其他进程使用同一端口：

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

图 4：Akamai Guardicore Segmentation 的限制 WinRM 通信策略示例

泄露

近几年来，攻击者对其勒索手段进行了调整，开始将泄露受害者的敏感文件用作额外的勒索筹码。在泄露来自企业的数据时，他们会尝试融入到嘈杂的网络环境中，但在这一阶段中，往往仍然能够对其加以检测和阻止。

阻止泄露域名

利用 Akamai Guardicore Segmentation，限制访问可被利用进行数据泄露的服务

攻击者常常会使用公共工具来泄露网络上的数据，MEGA、Dropbox 和 Google Drive 等公共托管服务就是极为常见的例子。监控这些域的难点在于，它们通常是在网络内部得到合法的使用。例如，通过浏览器访问 MEGA 域可能会被视为合法操作，但如果使用的是 rclone 实用程序，则会被认为存有恶意，因为有些攻击团伙就常常使用该实用程序来泄露数据。

利用 Akamai Guardicore Segmentation，我们可以阻止这些工具访问所有不需要访问权限的端点，并且仅允许通过经认可的应用程序（例如，浏览器）进行访问，从而将这些工具造成的风险降至最低。

多层防御

攻击者需要经过多个不同的攻击阶段，才能达成自己所追求的目标。对防御者来说，每个步骤都有机会检测并阻止相关的恶意活动。通过使用不同的 Akamai 安全产品，防御者在勒索软件杀伤链的每个步骤都能采取抵御措施，从而阻止攻击者的行动并检测任何异常行为。

如需详细了解 Akamai Guardicore Segmentation，或者申请个性化产品演示，请访问 akamai.com/guardicore