思科解决方案在攻击前、攻击中和攻击后均提供保护

思科云 Web 安全高级版帮助全球的石油及天然气公司发现并解决勒索软件感染这一频繁出现的问题。

挑战

当今，攻击的主要动机通常是盗窃或侵害企业数据，因此企业面临着前所未有的内容安全挑战。根据思科 2014 年度安全报告，思科研究员发现，他们分析的所有企业网络中都有流向存在恶意软件的网站的流量。[1] 利用对这项活动的观察结果，他们还确定，这些网络被攻击时，它们会在一段时间内受到危害，但客户却检测不到核心入侵。[2]

下列因素使安全团队很难预防和检测威胁：

- 如果没有适当的安全措施，**移动性和云**会降低可视性并提高安全复杂性。随着更多的组织采用云计算、虚拟化、移动和远程办公并加入自带设备 (BYOD) 趋势，越来越多的数据超出企业的控制范围。网络边界日益模糊，攻击方式日新月异。此外，随着越来越多的业务关键型服务迁移到云中并可以在公司的安全边界之外访问，攻击面只会不断扩大。
- 根据*思科 2014 年度安全报告*，**高级威胁**“积极主动地了解部署哪些类型的安全解决方案，并转向不太可见、内容不易检测的行为模式，因此它们的威胁十分隐蔽。”[3]此战略意味着让安全解决方案和专业人员检测到更少的“有用信息”，同时，组织将面临恶意攻击者制造的“更多的加密流量、更多的加扰及更高的随机性，使指挥和控制 (C&C) 行为与实际流量无法区分。”[4]

由于威胁环境的复杂性、不断演变，发现作为一种现代的内容安全方法比防御更具相关性。当今的企业必须关注内容检测、行为异常检测和高级调查分析，以便了解已存在于其网络（攻击后阶段）中的威胁。

客户信息

行业：石油及天然气
员工：大约 15,000 名
业务：全球
安全人员：12 名
其他安全措施：病毒、防火墙、入侵检测系统 (IDS)、安全信息和事件管理 (SIEM)

挑战

- 检测通过基于 Web 的流量传输的高级威胁，这些威胁能够避开安全解决方案并嵌入企业网络
- 开发可付诸行动的情报以便帮助安全团队确定威胁的优先级
- 确定可在分布式环境中部署的单一解决方案，与现有的安全基础设施集成，并且可在整个攻击过程中提供保护

解决方案

- Cisco CWS 高级版，包含 Cisco CWS 基本版中的所有功能
- 感知威胁分析 (CTA) 和高级恶意软件保护 (AMP)，自动化搜索 Web 流量中的高风险威胁，并提供对积极活跃在企业网络中的高级攻击的可见性

结果

- 识别并解决之前未发现的持续的恶意软件感染
- 现已在整个攻击过程中提供威胁保护
- 客户的安全团队现在可以专注于解决最重大的威胁

[1] *思科 2014 年度安全报告*：http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf。
[2] 同上。
[3] 同上。
[4] 同上。

图 1. 新的安全模式：攻击后的持续安全

思科® 云 Web 安全 (CWS) 高级版帮助组织应对在扩展网络中保持持续安全的挑战。思科 Web 安全的基于云的版本，即 Cisco CWS 是用来将网络安全扩展到移动设备和分布式环境的平台。它通过思科全球威胁情报、高级威胁防御功能和漫游用户防护为所有用户提供保护。它包含 Cisco CWS 基本版中的所有功能，还能结合使用两种创新的恶意软件检测系统来自动化搜索 Web 流量中的高风险威胁：

- **感知威胁分析 (CTA)** 是近实时网络行为分析系统，它利用机器学习和高级统计找到网络中的异常活动，即攻陷指标 (IOC)。CTA 发现异常，然后引导安全分析师找到潜在问题，这有助于他们减少工作量和确定威胁的优先级。
- **高级恶意软件保护 (AMP)** 结合使用文件信誉、文件沙盒和追溯性文件分析方法，在整个攻击过程中识别和阻止威胁。

通过结合使用这些解决方案，CWS 高级版能够识别新的指挥和控制通道，而安全行业以前检测不到此类通道。

此案例研究探讨 CWS 高级版如何帮助全球的石油及天然气企业实现以下目标：

- 更深入地了解大规模和日益增加的 Web 流量（每日超过 3500 多万条 HTTP/HTTPs 请求）。
- 生成可付诸行动的威胁情报，更便于威胁响应团队确定威胁的优先级。
- 部署可与现有安全基础设施集成的单个解决方案，并在整个攻击过程中（攻击前、攻击中和攻击后）提供防护。

解决方案

思科建议客户升级至包括 CTA 和 AMP 的 CWS 高级版，此版本让客户更深入地了解他们的网络并帮助威胁响应团队确定威胁的优先级。

AMP 的追溯性分析方法可以揭露通过边界防御时视为“clean”，但实际上是精心伪装的高级恶意软件的文件。AMP 立即向安全管理员发出警报，并提供有关网络中的哪些用户可能被感染以及何时感染的信息。

同时，CTA 检测到更加隐秘的威胁，此类威胁已经突破防御并积极活跃在企业网络中。CTA 是一种创新的恶意软件检测系统，它利用行为分析和异常检测查明受到危害的设备。CTA 依靠高级统计建模和机器学习功能独立确定新威胁，从它发现的情报中学习并随着时间的推移不断改变，无需调整或配置。

CTA 在客户网络中找到恶意活动的证据并报告。恶意软件包含由一个恶意软件实体控制的各种模块。在这种情况下，负载是指 Cryptolocker 勒索软件，这种类型的恶意软件对受害者计算机中的文件进行加密并“锁定”他们的设备，直至他们支付赎金。[5]

如图 2 所示，攻击者利用指挥和控制基础设施实施攻击。此活动涉及以下四个关键步骤：

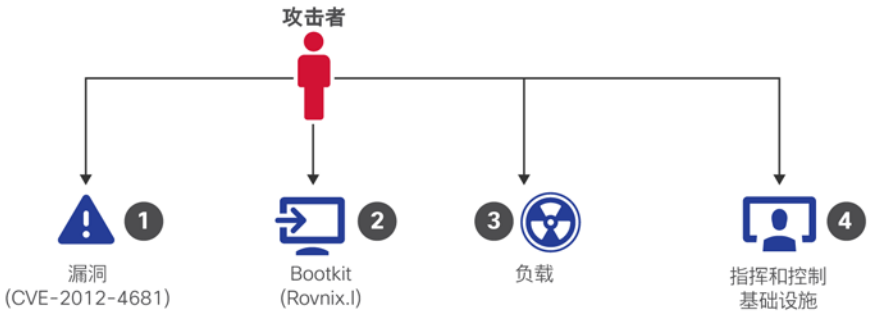
第 1 步： 攻击者利用漏洞 (CVE-2012-4681)，即利用 Oracle Java SE 7 Update 6 的 Java 运行时环境 (JRE) 组件中的漏洞；这样攻击者就能远程执行代码，绕过安全管理器。

第 2 步： 接下来，安装 bootkit (Rovnix.I) 以确保在机器上的持久性。

第 3 步： 然后传输负载，使恶意软件全面运行。（在这种情况下，负载是指 Cryptolocker 勒索软件。）

第 4 步： 攻击创建指挥和控制通道以保持有效运行。

图 2. 攻击中的四个关键步骤

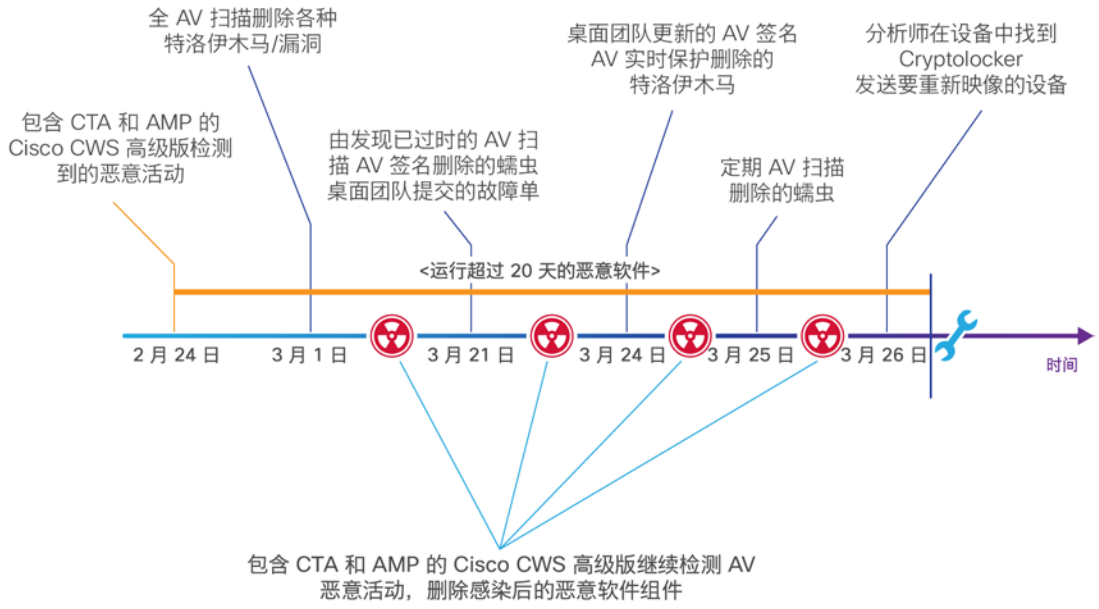


客户的安全团队尝试利用 AV 工具解决威胁。但是，由于这属于 rootkit 感染，恶意软件已深深嵌入被感染的系统中。AV 解决方案只能消除部分恶意软件组件。在完全解决感染之前，CTA 会一直警告安全团队存在持续的恶意活动。

图 3 列出从检测恶意活动到解决威胁的完整时间表。

[5] 恶意广告是用于传播恶意软件的在线广告，它在 Cryptolocker 的分发中发挥关键作用，一直都是被打击的对象；但恶意广告和勒索软件仍是普遍存在的威胁，被攻击者用来通过 Web 启动极具针对性的活动。有关详细信息，请参阅“思科 2014 年中安全报告”：http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf。

图 3. 恶意活动时间表：检测到解决



客户遇到的这种情况展示在攻击后阶段的运行中利用 CWS 高级版的重要性。它还强调使用 AV 产品减轻高级攻击为什么很难。CTA 系统提供持续活动的指挥和控制通道存在的证据。此外，它还发现数据泄露中使用的其他几个域。此类感染代表客户基础设施内隐藏的长期漏洞。

成果

在当今世界，安全团队每天都必须管理大量的事件，没有时间去“大海捞针”。安全团队需要关注最先进的攻击，而 CTA 系统正是用来检测此类攻击并将其分类。

一旦客户被 Cryptolocker 勒索软件感染，CWS 高级版即可检测到恶意活动，应用现有安全情报来阻止受感染设备尝试进入的一些指挥和控制通道。但是，攻击者然后使用其他具有未知信誉的 IP 地址；这种新的通道在整个感染过程中都处于运行状态。此示例重点介绍了仅依靠基于签名和基于 Web 信誉的检测方法的优势（自动阻止）和劣势（新通道未被阻止），以及为什么需要提供攻击后的持续防护。

下表列出对 CWS 高级版中的 CTA 系统发现的指挥和控制通道进行的分析，以及 Web 流量和统计信息示例：

表 1. 攻击基础设施

顺序	远程服务器	目标 IP：	目标国家/地区	请求数	活动状态
1	C&C 服务器 #1	109.XXX.XXX.XXX	荷兰	17（尝试次数）	被 Web 信誉阻止
2	**C&C 服务器 #2**	**94.XXX.XXX.XXX**	**卢森堡**	**75**	**活动通道**
3	C&C 服务器 #3	fistristy.com	卢森堡	175（尝试次数）	被 Web 信誉阻止
4	C&C 服务器 #4	ffeed5.com	俄罗斯	7（尝试次数）	被 Web 信誉阻止

表 2. 随后从设备中删除由 CTA 发现的威胁

威胁名称	已删除
Cridex 蠕虫	3 月 19 日
Cridex.E 蠕虫	3 月 19 日
Tesch.B 特洛伊	3 月 19 日
Java 漏洞/CVE-2012-4681	3 月 19 日
特洛伊下载程序 Win32/Upatre	3 月 19 日
Cridex 蠕虫	3 月 21 日
特洛伊 Win32/Viknok.C	3 月 24 日
Cridex 蠕虫	3 月 24 日
加密防御	3 月 26 日

到 C&C 服务器 # 1 (109.XXX.XXX.XXX) 的通信

通信特征：

- 向此服务器发出的尝试请求总数为 17；所有请求都是 C&C 通信并被信誉阻止。
- CTA 检测到这些请求，并视它们为将 URL 字符串用作通信通道 (C&C) 的尝试。URL（如下面的“HTTP 请求示例”中所示）表示已编码的消息。此攻击中使用的多个 URL 共享类似的 URL 字符串结构 (IP address/m/IbQ.*)。事实上，被信誉系统阻止的通信添加了更多的上下文证据。
- 在尚不属于信誉源的组成部分的服务器中，攻击者还会设置第二个 C&C 通道，以便确保恶意软件保持运行状态。URL 本身是已编码的消息。

HTTP 请求示例（匿名并被截断）

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM⋯

到 C&C 服务器 #2 (94.XXX.XXX.XXX) 的通信

通信特征：

- 向此服务器发出的请求总数为 75；所有请求都是 C&C 请求。
- CTA 检测到有两次 C&C 尝试，将它们视为**到 IP 地址的 HTTP 流量（未指定域名）**。此行为类别发现了代表到纯 IP 地址的无序通信的异常请求。此类活动可能是由恶意软件作为 “keep-alive” 检查执行的，这是为了确认恶意软件仍处于活动状态，或者只是泄露数据并接收来自其恶意基础设施 (C&C) 的其他指令。正常的互联网浏览并不会产生这种流量。
- 基于签名和基于信誉的技术并不能检测出所有这 75 个 C&C 请求。

HTTP 请求示例（匿名并被截断）

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT⋯

到 C&C 服务器 #3 (fistristy.com) 的通信

通信特征：

- 向 fistristy.com 域发出的请求总数为 175；所有请求都是 C&C 通信。
- 基于 Web 签名和信誉的技术能阻止所有这些请求。

HTTP 请求示例

hXXp://fistristy.com/aa/

到 C&C 服务器 #4 (ffeed5.com) 的通信

通信特征：

- 向 ffeed5.com 发出的请求总数为 7；所有请求都是被 CWS 高级版阻止的 C&C 通信。
- CTA 检测到其中 6 个请求，将它们视为**异常的 HTTP 流量**类别。此行为类别包括通常与 CTA 不间断分析创建的行为基线不相符的恶意软件行为。术语“基线”表示 CTA 系统创建的统计模型的状态，该系统“了解”经过分析的 Web 流量趋势和特征。CTA 随着网络的变化（例如，白天和黑夜）自动调整基线，以便提供最佳检测结果。
- CTA 使用长期的网络行为建模使看似不相干的活动相互关联。然后，它将这些数据与整个客户网络中的各个用户行为进行比较，从而增强发现功能来发现隐秘和持续的威胁。

HTTP 请求示例

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

总结

客户的安全团队需要一种更简单的方法来监控活动和确定安全事件的优先级，其中网络中存在 15,000 多个用户，平均每天生成 3500 多万个 Web 事务。客户还需要一个解决方案，它不仅能够阻止威胁，还能快速识别必然会穿过其他防御的威胁。客户所需的技术应能够在完全解除威胁之前，一直警告安全人员存在持续的恶意活动。

通过将 CTA 部署在 Cisco CWS 高级版中，客户现在拥有了近实时网络行为分析系统，该系统利用机器学习和高级统计找到网络中的 IOC。在感染 Cryptolocker 勒索软件的示例中，CTA 在安全团队完全解决感染之前，会一直发出恶意活动警报。此外，借助 CTA 提供的对恶意软件行为的见解，客户的安全团队仅专注于解决攻击前、攻击中和攻击后最重大的威胁。

了解更多

包含 CTA 和 AMP 的 Cisco CWS 高级版与思科战略保持一致，通过云中提供并在所有安全解决方案间共享的不间断分析和实时安全情报，帮助组织检测、了解并找到威胁，从而提高效率并有助于组织解决已知和新出现的安全挑战。通过结合使用这三个解决方案，CWS 高级版能够识别安全行业以前检测不到的、新的指挥和控制通道，并帮助组织解决在整个攻击过程中遇到的安全挑战。

如需了解有关 CWS 高级版的详细信息，请转到 http://www.cisco.com/go/cws。

有关 CTA 的详细信息，请参阅 http://www.cisco.com/go/cognitive。

有关 AMP 的详细信息，请访问 http://www.cisco.com/go/amp。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte, Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 中列出了各办事处的地址、电话和传真。

美国印刷 C36-733153-00 10/14