基于 Serverless 的反溯源技术应用研究

韩 杰[1],冯美琪[2],李建欣[2]
(1. 北京航天万源科技有限公司,北京 100176;
2. 中国民航信息网络股份有限公司 运行中心,北京 101318)

摘 要:随着网络逐渐成为意识形态较量的主战场,攻防双方的技术手段在不断博弈中日渐精进,现有的反溯源手段无法避免防守方多维多技术的溯源手段,更易被防守方溯源反制。该文提出了一种基于 Serverless 的反溯源技术应用思路,利用 Serverless 的事件驱动和自动伸缩特性,使得用户在请求目标时,自动调用不同可用区域的 IP 地址,以此达到隐藏自身真实 IP 的目的。同时,由于 Serverless 实现应用开发与服务器分离,攻击者可直接进行攻击代码编写,也更加利于隐藏身份。通过利用 Serverless 中的云函数和 CobaltStrike 软件进行试验验证其可行性,发现其能很好地隐藏攻击源,防守方无法溯源到真实的攻击源。同时从防守方角度,详细分析流量特征,基于特征值和访问统计特征两个维度,构建攻击检测模型。通过模拟实际攻击行为和正常业务行为,验证了检测模型能够很好地发现攻击行为,并能区分攻击行为和正常业务行为,在一定程度上可以减少误报,降低对正常业务的影响,提高安全事件的处置效率,为防守方的入侵检测提供了检测思路。

关键词:网络攻防;攻击溯源;反溯源;Serverless;攻击检测
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2023)12-0143-06
doi:10.3969/j.issn.1673-629X.2023.12.020

Research on Application of Anti-traceability Technology Based on Serverless

HAN Jie[1],FENG Mei-qi[2],LI Jian-xin[2]
(1. Beijing Aerospace Wanyuan Science & Technology Co.,Ltd.,Beijing 100176,China;
2. Operation Center,TravelSky Technology Limited,Beijing 101318,China)

Abstract:With the network gradually becoming the main battlefield of ideological competition,the technical means of both sides of the attack and defense are increasingly refined in the continuous game. The existing anti-traceability means cannot avoid the multi-dimensional and multi-technology traceability means of the defense side,and are more likely to be countered by the defense side. We propose an application idea of anti-traceability technology based on Serverless,which makes use of the event-driven and auto-scaling features of Serverless to make users automatically call the IP address of different areas when requesting the target,so as to achieve the purpose of hiding their own real IP address. At the same time,because Serverless realizes the separation of application development and server,attackers can directly write attack code,which is more conducive to hiding identity. By using the cloud function in Serverless and CobaltStrike software to test and verify its feasibility. It is found that it can well hide the source of attack and the defender cannot trace the source of the real attack. At the same time,from the perspective of the defender,the traffic characteristics are analyzed in detail,and the attack detection model is built based on the two dimensions of the characteristic value and the access statistical characteristics. By simulating the actual attack behavior and the normal business behavior,it is verified that the detection model can well detect the attack behavior,and can distinguish the attack behavior and normal business behavior. To some extent it can reduce the false alarm,reduce the influence on normal business,improve the processing efficiency of security events,and provide a detection idea for the defense's intrusion detection.

Key words:network attack-defense;attack traceability;anti-traceability;Serverless;attack detection

收稿日期:2023-02-15 **修回日期**:2023-06-16
基金项目:国家重点研发计划(2021YFB3101900)
作者简介:韩 杰(1976-),男,高级工程师,硕士,研究方向为网络安全和信息安全;通信作者:冯美琪(1994-),女,助理工程师,硕士研究生,研究方向为安全分析、大数据分析。

0 引 言

在全球化和信息化的时代背景下,网络逐渐成为意识形态较量的新战场[1],其主要表现形式为网络攻防战[2]。在网络攻防战中,由于攻击来源的追踪查找是抵御网络攻击的一项主动防范技术,因为攻击者最为在意的就是如何隐藏自身真实身份[3],不被防守方溯源反制。在前期攻击者使用的反溯源技术较为单一,手段多为删除各种日志或者不断更换网卡,效率较低,也更易被发现。随着攻防技术的演进,攻击和防守在持续的博弈中各自精进,现有溯源技术呈现多维、多技术的综合特征,主要溯源技术有:基于 OmegaLog 框架[4]、基于网络流量风险数据聚类[5]、基于攻击图谱的溯源分析技术[6]、基于大数据技术的多层溯源框架[7]等。溯源技术多维和多技术的特征让攻击者在各个渗透阶段都有可能暴露自己的真实身份,现有手段已无法完美地隐藏自己,存在较高的暴露风险,此时云服务化和 Serverless 架构为攻击者提供了反溯源的新思路。

针对现有反溯源技术的不足,该文利用 Serverless 架构中的云函数实现攻击地址的隐藏进而验证其可行性,同时深入分析访问时的流量数据,与正常访问时的数据进行对比分析,选取存在显著差异的特征作为主要指标,构建威胁检测模型,提供利用云函数进行网络攻击的检测思路。

1 反溯源技术研究分类

1.1 匿名通信技术

匿名通信技术通过隐藏通信双方 IP 地址、物理位置等实体信息和通信关系的通信技术,使窃听者无法直接获知或推导得知通信双方的通信关系或某一方的信息,从而更好地保护网络用户的通信隐私[8]。匿名通信系统主要分为基于 Mix 算法、基于 OnionRouting 算法和基于泛洪算法。当前关于匿名通信技术的研究主要集中在提供匿名性能,而其在网络攻击中的应用实例主要是 Tor 匿名网络,由于低延时、易于配置和使用、服务稳定可靠等优点,是目前互联网中最成功的公共匿名通信服务[9]。

1.2 跳板攻击技术

跳板攻击技术是目前攻击方的普遍攻击形式,其主要的作用就是隐藏攻击源。其常见的应用实例就是跳板机。所谓跳板机就是一台可以联网的服务器,攻击者通过自己的本机控制跳板机,通过一个跳板机或多个跳板机对目标实施攻击行为,从而达到隐藏自身的目的。其主要分为两种利用形式[10]:一是简单经过,即数据包内容基本在经过跳板前后不改变,一次经过跳板机完成攻击;二是完全控制,即数据包基本内容经过跳板前后无必然关联,攻击者通过多种控制形式操作跳板机实施攻击。由于攻防技术不断精进,常用跳板攻击技术多为完全控制方式。但由于现有很多安全产品均有追溯功能,理论上在三跳以内的跳板攻击基本可以通过代理跳板主机找到攻击源主机。

1.3 代理技术

代理也称为网络代理,是一种特殊的网络服务,允许一个网络终端通过该服务与另一个网络终端进行非直接的连接。代理服务器是一种加密的匿名代理,不仅可以更改 IP 地址,还可以对会话进行加密,常被攻击者利用来隐藏攻击源。攻击者主要的利用方式就是匿名代理服务器但其安全性取决于代理商。

2 Serverless 介绍

2014 年 Serverless 首次以云服务的概念被提出[11],实现应用开发与服务器分离,同时消除底层设备差异对上层应用造成的不良影响[12]。Serverless 服务主要包括函数即服务 FaaS(Function as a Service)以及后端即服务(Backend as a Service)。其主要特征如下:

(1)基于函数,即轻量化、细粒度和短周期的函数,使其系统简易、稳定和性能高;

(2)无状态,即函数实例互相独立,具有一定容错能力;

(3)自动伸缩性,即函数实例可以从活跃节点直接扩容,以应对批量事件,提升系统吞吐性能;

(4)事件驱动,即触发器定义并量化事件-业务关系,提供实时事件监听服务;

(5)高兼容性,即提供对异构基础设施、运行环境和编程方式等多层次[13]的兼容机制。

云函数实际是 FaaS(函数即服务,Function as a Service)的具体体现,是指运行在云服务器的代码,无需实体服务器进行承载,开发者使用相应工具编写代码后上传部署至云端[14]之后即可运行在云服务器端的函数,其实际提供的是计算能力。从物理设计层面来讲,一个云函数可以由多个文件组成,各个云函数之间完全独立,可部署在不同地区。云函数可以被端侧调用,也可以互相调用。云函数主要特点是基于事件的、无服务器零运维[15],也正因如此,云函数能跨多个物理服务器平衡工作负载,可以创建多个容器动态扩展应用程序的实例[16],这也就使得用户在请求目标时,会自动调用不同可用区域的 IP 地址。以事件函数为例,云函数调用示意图如图 1 所示。

目前云函数广泛应用于数据 ETL 处理、文件处理及通知、移动及 Web 应用、小程序、业务流转等,而其在网络攻防中的应用场景主要是防溯源,如 C2 地址

隐藏、制作防溯源的 Webshell 等。其在网络攻防中的应用与 CDN 相比,二者都是与域名资源绑定,但 CDN 是建立并覆盖在承载网之上,主要应用在内容加速方面,但云函数提供无服务器执行环境,攻击者可直接进行攻击代码编写,也更加利于隐藏自己的真实 IP 地址。

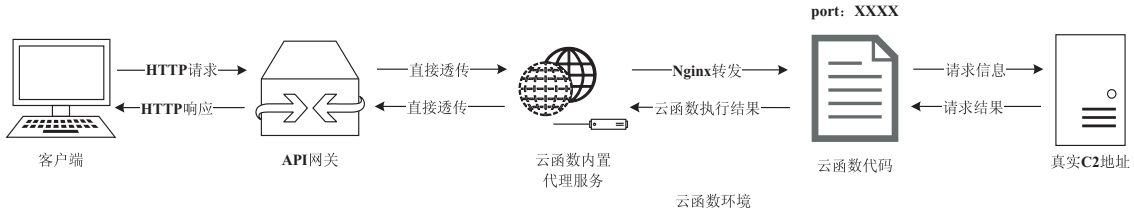

图 1　云函数调用示意图

3　云函数在反溯源方面的应用实例

结合攻击者的攻击思路,此次实验以 C2 地址隐藏为例,利用 CobaltStrike 软件创建后门程序,使用云函数转发 HTTP 请求,从而达到隐藏真实 IP 地址的目的,避免被防守方溯源追踪。

(1)云函数创建。

云函数有 2 种类型:一是事件函数,通过事件触发函数运行,纯粹纯托管 FaaS;一是 Web 函数,主要是应对主流的 Serverlessful 多线程开发模式,解决传统 Web 框架 FaaS 化改造成本高的问题,用户可以直接发送 HTTP 请求到 URL 触发函数执行。考虑到攻击者在实际应用过程中的选择,本次实验选择事件函数类型,转发 HTTP 请求。云函数基本信息如图 2 所示。

图 2　云函数基本信息

(2)后门程序创建。

CobaltStrike 共支持 5 种后门程序,此处暂不详细介绍,选择 Windows Executable 类型木马即可达到实验目的。构建木马程序时,Shell 反弹的主机为申请的云函数域名。

(3)功能实现。

功能实现的前提是已经通过其他攻击手段将木马文件植入到目标主机并运行,此次实验则直接将生成的木马文件拷贝至目标主机并执行,此时在 CobaltStrike 页面中可以监听到目标主机点击了木马文件,同时双击可进入到 Shell 页面,通过执行系统命令(ls)获取当前目录下的所有文件以确认是否成功与目标主机建立连接,命令执行结果表示已成功与目标主机建立连接。详细信息如图 3 所示。

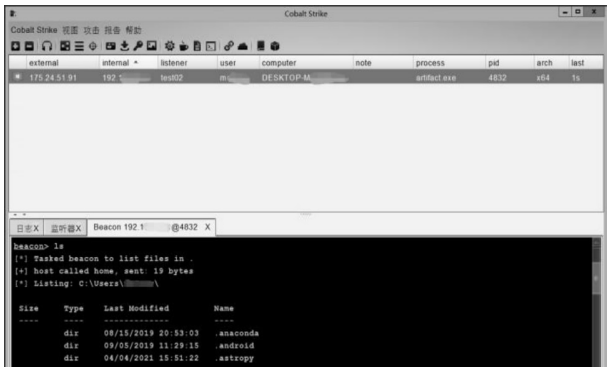

图 3　获取 Shell 权限并成功执行 ls 命令

通过观察 CobaltStrike 监听器中的信息,发现 external 地址不断变化,该现象也间接说明云函数具备内置的代理功能,在不重启木马进程的情况下,同一客户端会访问同一 API 网关地址,但是经过云函数内置的代理转发后,CobaltStrike 监听到的攻击地址为代理 IP 地址,即腾讯云地址,并非真实的攻击地址。IP 地址在访问过程中的变化情况如图 4 所示。在木马程序反连过程中,所有外网的 IP 地址经查询均为腾讯云地址,无法进一步溯源到实际的攻击者,到此就达到了隐藏真实 IP 地址的目的,避免攻击者被溯源反制。

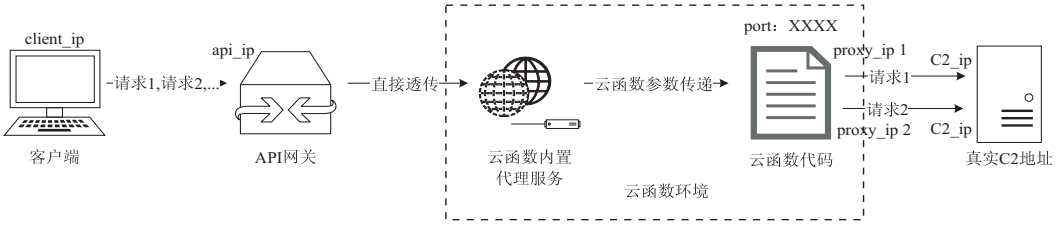

图 4　云函数使用中 IP 地址变化情况

4 攻击检测模型构建及实验分析

4.1 流量分析

通过模拟攻击者的攻击手段,利用云函数技术隐藏自己真实 IP 地址,创建钓鱼邮件中的恶意木马程序,在用户运行木马程序时会自动与 C2 地址建立连接。对运行过程中产生的 HTTP 流量数据进行分析,总结出如下特征。

4.1.1 域名首次出现并带有云厂商特征

用户在点击木马程序后,木马程序自动与 C2 地址建立连接,HTTP 请求头信息如图 5 所示。通过观察 HTTP 请求头信息,发现 Host 字段的值为云函数生成的域名 xxxxxxxxxxxxxxx. apigw. tencentcs. com,且该域名对用户来说是首次访问,其中 apigw. tencentcs. com 为腾讯云函数域名的特征。

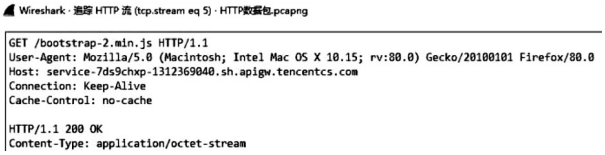

图 5 HTTP 请求包头信息

4.1.2 目标主机定时向攻击机发送数据包

木马在运行时需要通过网络与攻击机保持通信,以达到持续控制的目的。如表 1 所示,木马程序会定时发送 HTTP 请求包进行心跳检测,约 1 min 发送一次 GET 请求,保证与攻击机正常通信。其用于心跳检测的 HTTP 请求包具有相同的 URI、请求方法和请求包大小。

表 1 目标主机发送数据包的详细信息

时刻	URI	请求方法	请求包大小
02:35:19.787263	/dpixel	GET	444
02:36:19.876765	/dpixel	GET	444
02:37:19.975181	/dpixel	GET	444
02:38:20.067602	/dpixel	GET	444
02:39:20.199916	/dpixel	GET	444
02:40:20.429115	/dpixel	GET	444
02:41:20.538458	/dpixel	GET	444
02:42:20.650954	/dpixel	GET	444
02:43:20.740088	/dpixel	GET	444

4.2 攻击检测模型构建

4.2.1 特征提取

通过对流量数据的分析,提取相关特征作为模型中的检测特征。主要分为两个方面:一个是关键字匹配。目前常见云厂商的云函数都具有较明显的特征,可通过此特征确定是否使用了云函数。另一个方面是特征检测。使用云函数不代表其为攻击行为,可能为正常业务操作,因此还要结合访问特征进行进一步判断。特征提取阶段共提取出 1 个关键字特征和 5 个访问特征,访问特征分别是:新域名、时间间隔离散程度、请求包大小离散程度、URI 频次和请求方法。

(1)特征值检测。根据 HTTP 数据包中的特征,访问时数据包中会包含云函数生成的域名,不同的云厂商具有不同的特征。目前中国主要的云计算公司有:阿里云、腾讯云、百度智能云等,基本都提供云函数服务,其云函数生成的域名也有不同的特征。详细如表 2 所示。

表 2 部分云厂商云函数访问域名的特征

序号	厂商	云函数访问地址特征
1	腾讯云	apigw. tencentcs. com
2	阿里云	aliyuncs. com
3	百度智能云	gz. baidubce. com
4	金山云	ksyun. com

(2)访问特征检测。通过模拟攻击者的攻击手法,使用云函数生成的域名构建木马程序进行远程木马攻击,分析攻击流量,总结出攻击者具有如下访问特征。

①通过分析某一 IP 地址访问的域名是否为近 6 个月首次出现来确定是否为攻击者构造的域名。其计算公式为:

newHost = IF(该 IP 地址近 6 个月首次出现) (1)

②通过分析某一 IP 地址 10 分钟内 HTTP 请求的 URI 频次来确定该 URI 是否为访问最频繁的 URI,后续指标计算将以此 URI 为前提进行统计。其计算公式为:

freqUri = uri(IF(该 IP 地址 10 分钟内 HTTP 请求次数 > 10)) (2)

③通过分析某一 IP 访问最频繁 URI 在 10 分钟内请求间隔时间的离散程度辅助确定是否为攻击行为。其计算公式为:

$$\sigma_t(\text{freqUri}) = \sqrt{\frac{\sum_{i=1}^{n}(t_i - \bar{t})^2}{n}} \tag{3}$$

其中,t_i 表示该 IP 地址频繁 URI 的第 i 个 HTTP 请求与第 $i-1$ 个请求的时间间隔,n 表示 10 分钟内该 IP 地址 HTTP 请求间隔次数,$\bar{t}$ 表示 10 分钟内该 IP 地址频繁 URI 的第 i 个 HTTP 请求与第 $i-1$ 个请求的时间间隔的均值。

④通过分析某一 IP 访问最频繁 URI 在 10 分钟内请求包大小的离散程度辅助确定是否为攻击行为。其计算公式为:

$$\sigma_l(\text{freqUri}) = \sqrt{\frac{\sum_{i=1}^{n}(l_i - \bar{l})^2}{n}} \tag{4}$$

其中,l_i 表示该 IP 地址频繁 URI 的第 i 个 HTTP 请求包大小,n 表示 10 分钟内该 IP 地址 HTTP 请求包数量,$\bar{l}$ 表示 10 分钟内该 IP 地址频繁 URI 请求包大小的均值。

⑤通过分析某一 IP 访问最频繁 URI 的请求方法是否为 GET 来辅助确定是否为攻击行为。其计算公式为:

reqMethod = IF(该 IP 频繁 URI 的 HTTP 请求方法为 GET)　　(5)

4.2.2　检测流程

检测特征无法直接应用于攻击检测,需要结合攻击检测流程模型进行应用。根据 4.2.1 节提到的 6 个特征,制定相关的检测流程,如图 6 所示。

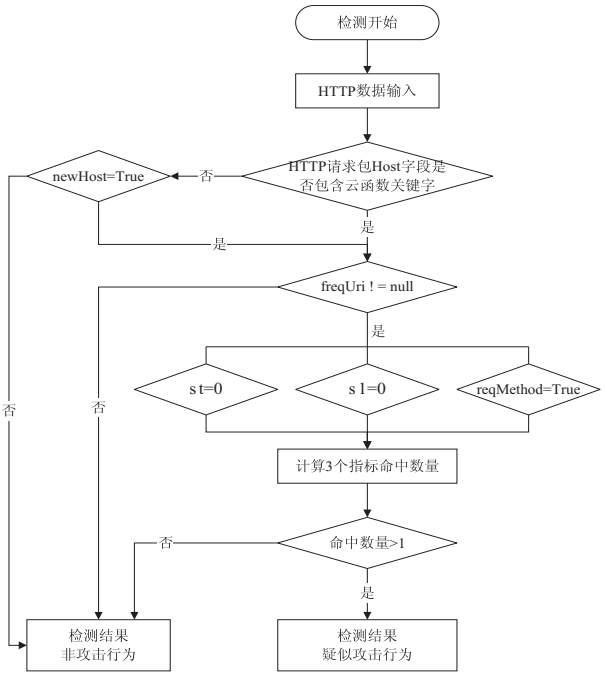

图 6　检测流程

首先通过关键字匹配确定是否使用了已知厂商的云函数服务,若无法确认进一步通过域名出现的时间进行辅助判断,若使用了云函数或者首次访问该域名,则通过统计特征进一步判断是否为攻击行为。在判断是否为攻击行为前,需要根据访问特征寻找访问最频繁的URI,若存在,则需要进一步判断是否为攻击行为,若不存在,则判定为非攻击行为。在进一步判断是否为攻击行为时,对 3 个统计指标进行投票,若命中指标数大于 1 时,则判定其疑似为攻击行为,转为人工研判及处置,否则判定为非攻击行为,暂不处置。

4.3　实验结果分析

根据 4.2.2 节的检测流程,通过计算 6 个特征,辅以检测模型,判断是否为攻击行为。以实际的一个攻击行为和 2 个正常业务行为为例进行实验。

攻击行为:内部演练期间,攻击队利用社工钓鱼的攻击手段,成功控制一台办公终端,并利用该办公终端作为跳板机,进行内网横向渗透。在进行溯源分析时发现,攻击者一般都会利用国内常见云厂商的云函数,在 HTTP 请求包中的 Host 字段都会包含云函数的特征,但仅靠该特征无法与正常业务行为区分,因此相关统计特征仍是较为明显的特征。该行为相关字段的详细信息见表 3。

表 3　攻击行为相关字段信息

时刻	URI	请求方法	请求包大小	备注
12:34:05.200872	/api/x	GET	485	CS 心跳检测
12:34:10.314678	/api/x	GET	485	CS 心跳检测
12:34:15.414834	/api/x	GET	485	CS 心跳检测
12:34:20.555054	/api/x	GET	485	CS 心跳检测
12:34:25.664651	/api/x	GET	485	CS 心跳检测
12:34:30:773122	/api/x	GET	485	CS 心跳检测
12:34:35.892324	/api/x	GET	485	CS 心跳检测
12:34:41.029965	/api/x	GET	485	CS 心跳检测
12:34:46.147142	/api/x	GET	485	CS 心跳检测
12:34:57.102904	/api/y	POST	954	CS 中执行 ls
12:34:56.305724	/api/x	GET	485	CS 心跳检测

正常业务行为 1:研发人员利用腾讯云函数转发 HTTP/HTTPS 请求,实现代码轻量级部署。

正常业务行为 2:研发人员利用腾讯云函数转发 HTTP/HTTPS 请求,并绑定已有域名,即云函数/云对象 URL 化,实现代码轻量级部署。

以上 3 个测试行为经过 4.2.2 节的检测流程进行检测后,得到如表 4 的指标值和检测结果。

表 4　实验结果

行为	云函数特征	newHost	freqUri	σ_t	σ_l	reqMethod	检测结果
攻击行为	是	True	/api/x	0	0	True	疑似攻击
业务行为 1	是	True	无	—	—	—	正常业务
业务行为 2	否	False	—	—	—	—	正常业务

对比已有的检测方法,单纯依靠特征值检测,业务行为经常被判定为攻击行为,增加了人工研判的工作量并对正常业务造成一定影响,而利用文中检测方法,可以进一步对攻击行为进行判断,在一定程度上可以降低对正常业务的影响,提高安全事件的处置效率。通过试验分析,也进一步证明了文中分析方法的正

确性。

为了进一步体现文中检测方法的可行性,参考《网络安全产业高质量发展三年行动计划(2021-2023年)(征求意见稿)》中提到的“提升安全编排与自动化响应技术应用水平”的要求,从发现、响应和分析 3 个环节分析文中检测方法的时间性能。现有方法和文中方法的时间性能对比如表 5 所示。

表 5 时间性能对比结果

安全运营环节	现有检测方法		文中检测方法	
	攻击行为	业务行为	攻击行为	业务行为
发现	<1 秒	<1 秒	2 秒	<1 秒
响应	5 分钟	5 分钟	<1 秒	无需响应
分析	10 分钟	10 分钟	2 分钟	无需分析

通过表 5 的对比分析结果发现,在安全运营流程中,文中检测方法虽然在发现过程中由于需要时间计算指标而导致时间效率高于现有方法,但其在后续响应及分析过程中能够大大缩减时间,使得整个安全运营流程的时间缩短,并实现自动化响应及分析。此时再结合人工研判,在大大缩短时间的同时,也降低了误报率,提高了响应及处置效率。

5 结束语

Serverless 解决了系统层面运维问题,但由于其事件驱动、自动伸缩以及应用开发与服务器分离的特性,在简化运维工作的同时,也容易被攻击者恶意利用,增加网络安全风险。该技术应用在网络安全领域中可实现隐藏自身真实身份的目的,对于防守方来说可以保护服务器不被互联网上的 IP 扫描软件发现,但对于攻击者来说也能避免其真实身份被溯源,增加防守方溯源反制难度。因此可以利用 Serverless 简化运维工作以及保护服务器 IP,但也要同时关注利用 Serverless 的网络攻击的日常检测。文中通过试验验证了该技术实现隐藏身份的可行性,同时通过分析网络流量,总结特征,从特征值检测和访问行为特征检测两个方面给出了检测模型,并通过试验对检测模型的正确性进行了验证。由于云函数技术仍处于起步阶段,其主要应用领域集中在代码开发领域,在网络安全方面暂时没有广泛应用和深入研究,可能应用场景和检测模型都有一定的局限性和误报,还需要结合人工进行研判分析,后续将持续探索云函数技术在网络安全中的应用以及 HTTPs 情况下的检测方法研究。

参考文献:

[1] 生忠军. 新时代网络意识形态安全治理:挑战,原则和优化路径[J]. 邓小平研究,2020,29(3):81-88.

[2] 李丁夏. 面向攻防实战的网络安全防护体系建设[J]. 网络安全技术与应用,2022(6):4-5.

[3] 周海龙,周 颖,冯雪山. 关于 IP 地址隐藏的专题分析[J]. 电脑知识与技术,2019,15(11):73-75.

[4] HASSAN W U, NOUREDDINE M A, DATTA P, et al. OmegaLog:high-fidelity attack investigation via transparent multi-layer log analysis[C]//Network and distributed system security symposium. California: Internet Society and Lawrence Livermore National Laboratory,2020:1-16.

[5] 葛维静,冯园园,刘宗洋,等. 一种基于网络流量风险数据聚类的 APT 攻击溯源方法[J]. 通信技术,2022,55(10):1354-1362.

[6] MILAJERDI S M,GJOMEMO R,ESHETE B,et al. Holmes: real-time APT detection through correlation of suspicious information flows[C]//Proc of the 40th IEEE symp on security and privacy. San Francisco:IEEE,2019:1137-1152.

[7] 王 涛,张 淋,邹初建. 基于大数据技术的攻击溯源研究[J]. 信息安全与通信保密,2021(11):106-116.

[8] 赵 娜,苏金树,赵宝康,等. 匿名通信系统隐藏服务定位技术研究综述[J]. 计算机学报,2022,45(2):393-411.

[9] 梁 湛. Tor 匿名通信系统的流量伪装技术研究[D]. 成都:电子科技大学,2022.

[10] 王 禾. 跳板攻击场景下的嵌入式系统的攻击路径分析[D]. 西安:西安电子科技大学,2021.

[11] HANDY A. Amazon introduces Lambda,Containers at AWS re:Invent[EB/OL]. 2014[2023-04-23]. https://sdtimes.com/amazon/amazon- introduces-lambda-containers/.

[12] 杨柏蔼,赵 山,刘 芳. 无服务器计算技术研究综述[J]. 计算机工程与科学,2022,44(4):611-619.

[13] MALAWSKI M,GAJEK A,ZIMA A,et al. Serverless execution of scientific workflows:experiments with HyperFlow, AWS Lambda and Google cloud functions[J]. Future Generation Computer Systems,2020,110:502-514.

[14] 喻向阳. 基于云函数的操作指令生成方法、装置、设备及存储介质:中国,CN202011306060.8[P]. 2021-02-23.

[15] 吴绍岭,田春岐,万 兴,等. 一种面向云函数的超轻量运行时环境构建方法[J]. 计算机科学与应用,2020,10(11):1993-2005.

[16] 张国生. 基于无服务器架构的云原生应用软件研究[J]. 中国电子科学研究院学报,2022,17(2):155-161.