ARBOR NETWORKS

The Security Division of NETSCOUT

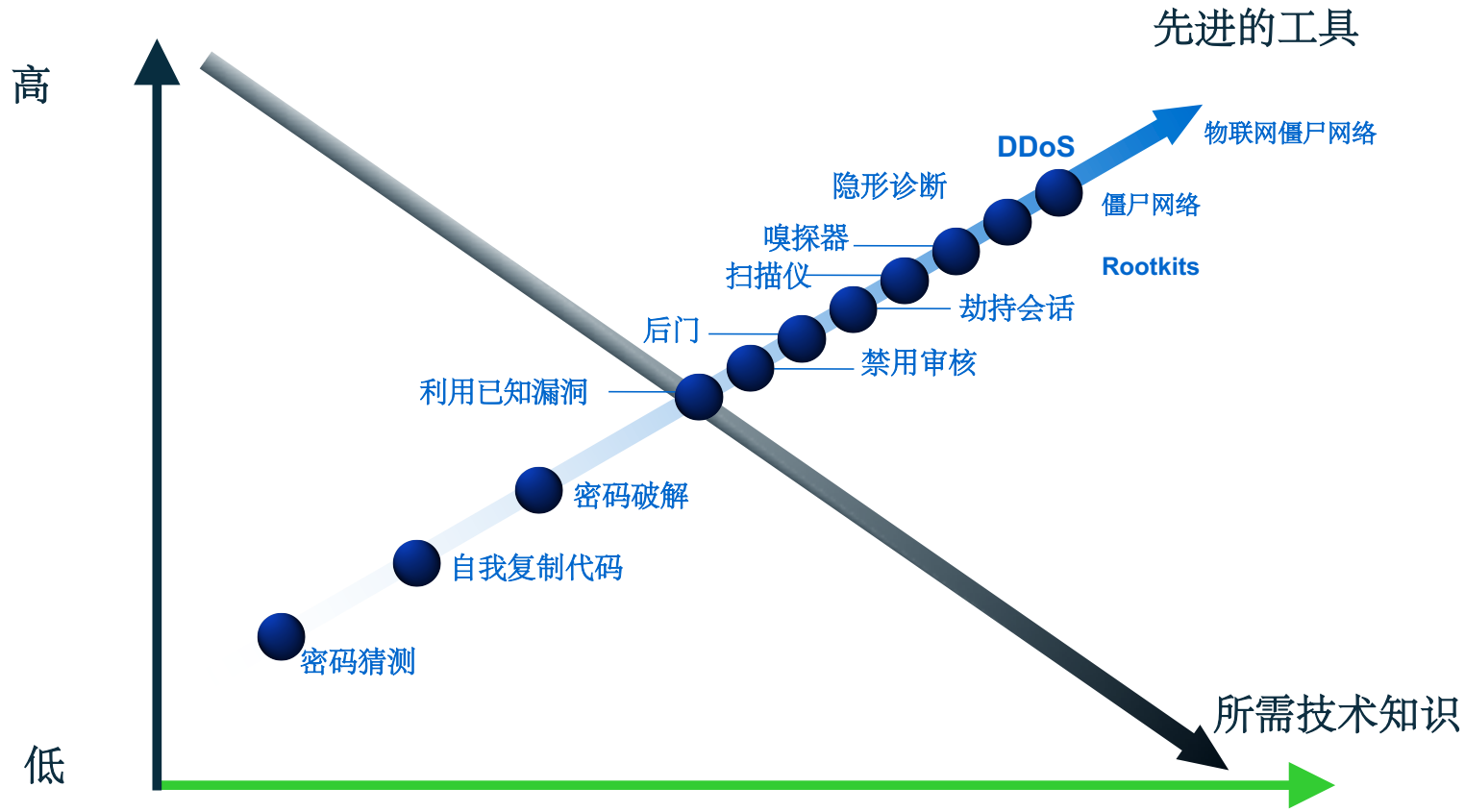
收获旋风

Mirai时代的分布式拒绝服务防御

Roland Dobbins, *首席工程师*
<rdobbins@arbor.net>

简介与背景

威胁和漏洞利用的演变


先进的工具
高
低
所需技术知识
物联网僵尸网络
DDoS
僵尸网络
隐形诊断
Rootkits
嗅探器
劫持会话
扫描仪
后门
禁用审核
利用已知漏洞
密码破解
自我复制代码
密码猜测

僵尸网络 - 第一大在线安全威胁

僵尸网络维基百科： 一组受到感染的计算机（称为僵尸计算机）（或僵尸机器人），它们在通用命令和控制基础结构下运行程序，通常称为蠕虫，特洛伊木马或后门程序。

僵尸网络是所有这些活动的主要推动者：

- 分布式拒绝服务
- 勒索
- 广告点击欺诈
- 虚假销售
- 身份盗用和金融欺诈（网络钓鱼，从个人计算机窃取信息等）
- 商品/服务盗窃
- 间谍活动/信息窃取
- 垃圾邮件操纵股市

ARBOR NETWORKS

分布式拒绝服务攻击 – 互联网生活实况

- 分布式拒绝服务攻击每天24/7/365发生–简直是互联网上的生活。
- 任何组织，任何场所，任何个人都可能受到分布式拒绝服务的影响，无论是直接目标还是间接损害。
- 出站分布式拒绝服务对入站分布式拒绝服务就像对终端客户和服务提供商一样具有破坏性–宽带接入网络，企业网络和IDC内部的僵尸主机会影响源网络和目标。
- 态势感知是关键-新闻中发生了什么？今年/每月/每周/今天发生什么周年纪念日？
- 恶意行为经常相互攻击-附带损害！

ARBOR NETWORKS

皇帝的新云

- 我们依赖于实验室环境中使用的已有34年历史的协议，几乎/根本不考虑安全性是我们全球互联网基础设施的基础。
- 尽管在运营安全（opsec）和可扩展互联网体系结构方面有大量工作要做，但在泄密方面的荣誉超过在实际部署中的荣誉。
- 网络架构师，应用程序设计师，运营团队，安全团队，管理人员之间持续不断的脱节。
- 波兰人对安全的态度-“为什么有人攻击我们？”
- 缺乏问责制–是否有人因可避免的安全事件而被解雇？
- 安全区/安全蛇油的普遍性。
- 无法/不愿适当评估抽象威胁模型-必要的心理防御机制？

分布式拒绝服务背景

什么是分布式拒绝服务（DDoS）攻击？

- 尝试消耗有限的资源，利用软件设计或实施中的弱点或利用基础设施容量不足
- 针对计算和网络资源的可用性和实用性
- 攻击几乎总是分布得更明显 (i.e., DDoS)
- 攻击造成的附带损害可能与攻击本身同样严重，甚至更严重
- 分布式拒绝服务攻击会影响可用性！没有可用性，没有应用程序/服务/数据/互联网！没有收益！
- 分布式拒绝服务攻击是针对容量和/或状态的攻击！

ARBOR NETWORKS

三种安全特性

- 安全的目标是维持这三个特征

ARBOR NETWORKS

三种安全特性

- 分布式拒绝服务防御的主要目标是面对攻击时保持可用性

ARBOR NETWORKS

几乎所有安全支出/精力都集中在机密和完整性上

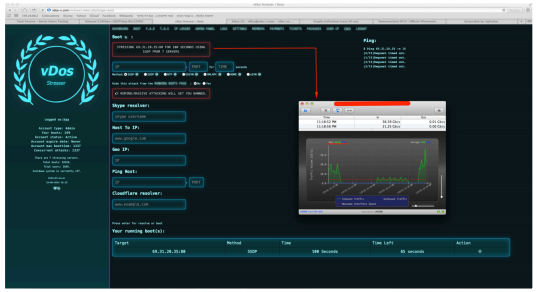
- 机密性和完整性是相对简单的概念，非专业人员容易理解
- 在实践中，机密性和完整性几乎等同于加密-同样，非专业人员很容易理解
- 现实情况是，加密技术比加密技术具有更多优势，但要宣告胜利，这很容易-“我们有防病毒软件，有磁盘加密技术，符合PCI规范，呜呼！”
- 然而，亿万个僵尸主机；完全渗透了各个行业各种规模的企业网络，窃取了知识产权，泄露了防御机密等。等
- 可用性无法满足需求-网络服务器/域名系统服务器/ VoIP PBX启动或关闭。无法针对实际，现实世界的安全状态混淆/夸大/预夸。
- 可用性要求运营安全（opsec）从业人员了解TCP / IP和路由/交换；谁了解网络服务器；谁了解域名系统服务器；谁了解安全性；谁了解第7层。
- 这些人很少，而且价格不菲。大多数组织甚至不了解寻找和雇用合适人员所需的技能和经验范围

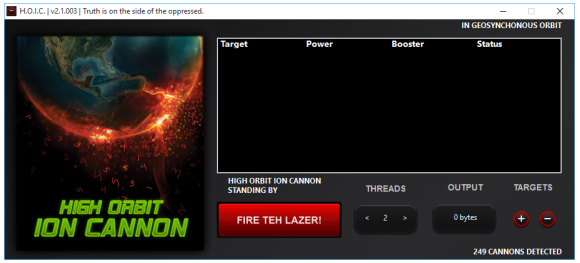
可用性很难!

- 面对攻击时保持可用性需要技能，体系结构，运营敏捷性，分析能力和缓解能力的结合，而大多数组织根本不具备这些能力
- 实际上，大多数组织在设计/规范/构建/部署/测试在线应用程序/服务/属性时从未考虑可用性
- 实际上，大多数组织从未在维持可用性和业务连续性之间建立逻辑联系
- 在实践中，大多数组织从不对应用程序/服务堆栈进行压力测试，以确定可扩展性/弹性不足并进行修复。
- 实际上，大多数组织没有减轻分布式拒绝服务的计划；或者，如果有计划，则永远不会排练!

分布式拒绝服务武器化

“武器化”：转换为武器使用/简化为武器使用

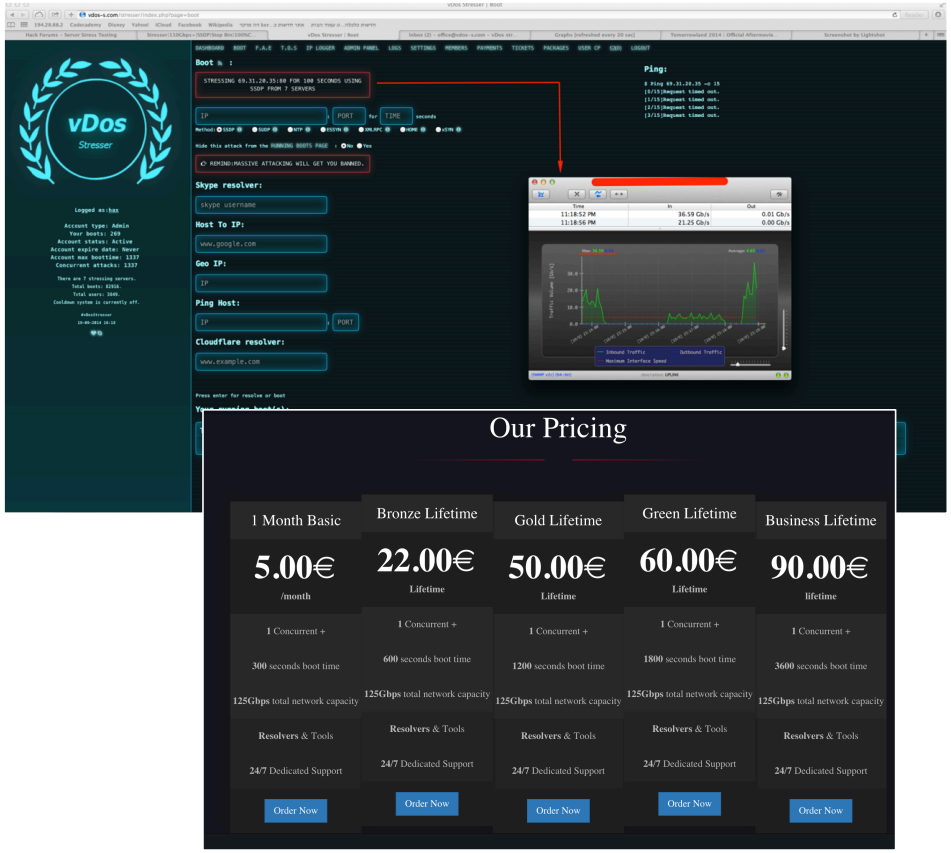




- “ Stresser Tools” /“Booters”的可用性得到提高，可以结合使用非欺骗性放大和欺骗性放大攻击进行高度分布式攻击。通常与机器人农场相关。

- 开发供自愿加入攻击者使用的工具：
  - 低轨离子炮用于执行非欺骗UDP /ICMP攻击
  - 高轨道离子炮向多个站点发送非欺骗性HTTP请求

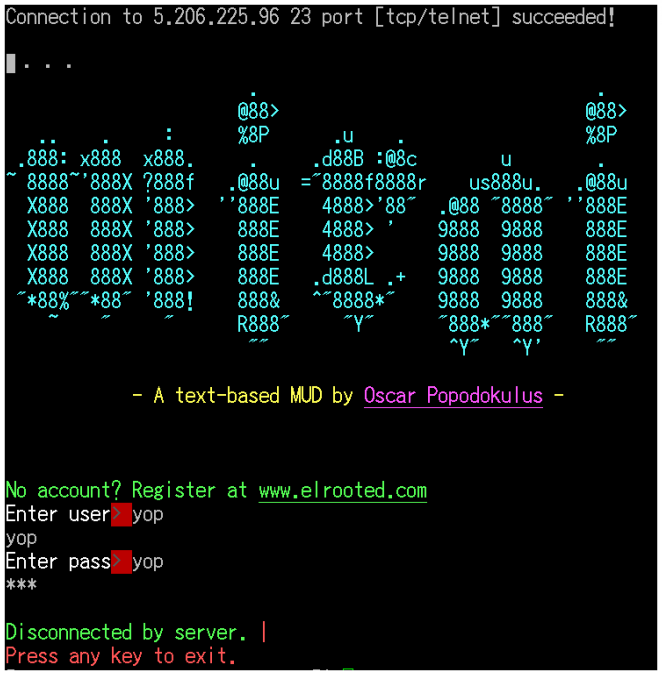
面向大众的分布式拒绝服务工具



- 现在，任何能够单击按钮的人都可以发起分布式拒绝服务攻击。
- 便宜且易于使用：
  - VIP帐户！
  - 终身订阅！
  - 24x7全天候客户支持！
- 最初主要由玩家相互攻击使用，但最近我们一直看到它们用于攻击高度可见的目标。

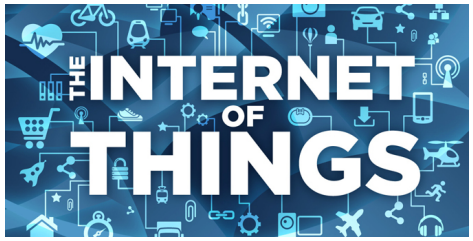
物联网形势

物联网



ARBOR NETWORKS

物联网（IoT）



维基百科：物联网（IoT）是物理设备，车辆，建筑物和其他物品的网络，嵌入了电子，软件，传感器和网络连接，使这些对象能够收集和交换数据

但这是新的营销手段吗？

- 例如，“特洛伊木马室咖啡壶”于1993年连接到互联网。

更精确的定义：*物联网设备（嵌入式设备）本质上是一台具有CPU，内存，软件和专用于特定角色或任务的接口的计算机。*

ARBOR NETWORKS

缺省用户名和密码！！！

https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.csv

```
Username/Password,Manufacturer,Link to supporting evidence
,,
admin/123456,ACTi IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko,ANKO Products DVR,http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass,"Axis IP Camera, et. al",http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv,Dahua Camera,http://www.cam-it.org/index.php?topic=5192.0
root/888888,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/666666,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
666666/666666,Dahua IP Camera,http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox,Dreambox TV receiver,https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx,EV ZLX Two-way Speaker?,?
root/juantech,Guangzhou Juan Optical,https://news.ycombinator.com/item?id=11114012
root/xc3511,H.264 - Chinese DVR,http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518,HiSilicon IP Camera,https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin,IPX-DDK Network Camera,http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system,"IQinVision Cameras, et. al",https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm,Mobotix Network Camera,http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321,"Packet8 VOIP Phone, et. al",http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-
phones/4119+&cd=21&hl=en&ct=clnk&gl=us
root/00000000,Panasonic Printer,https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek,RealTek Routers,
admin/1111111,Samsung IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc,Shenzhen Anran Security Camera,https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin,SMC Routers,http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb,Toshiba Network Camera,http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt,Ubiquiti AirOS Router,http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor,VideoIQ,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>,Vivotek IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111,"Xerox printers, et. al",https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521,ZTE Router,http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html
```

物联网安全性（或缺乏安全性）

物联网安全问题：

- IoT设备通常具有有限的机载功能，并且经常需要外部配置和控制。
- 其中许多设备堆栈未正确固定：
  - 硬编码的用户名/密码
  - 默认情况下启用不必要的服务（Chargen，SSDP，DNS转发器）
  - 不安全的管理接口（Web，SNMP，TR-069等）
  - 软件更新功能有限或没有
  - 部署后很少打补丁或更新
- 到2020年，物联网设备数量估计约为20-30亿个，但我们已经在线超过6B，每天增加550万个1！

1) Gartner research: http://www.gartner.com/newsroom/id/3165317

数百万易受攻击的物联网设备+武器化=？

物联网僵尸网络！

物联网僵尸网络的历史

物联网僵尸网络实际上并不是什么新鲜事物：

- 第一个僵尸网络创建于1993年，当时Robey Pointer创建了一个名为“eggbot”的互联网中继聊天（IRC）机器人，用于通过对不需要的用户发起泛洪攻击来防御IRC通道。该机器人还用于使用CTCP和DCC协议攻击其他渠道攻击。机器人的多个实例可以在“僵尸网络”中共同努力。
- 在2003年，首次使用IoT设备对威斯康星大学的分布式拒绝服务攻击是由于700.000 Netgear DSL/电缆调制解调器中的NTP硬编码地址。即使发布了新软件，攻击仍持续了好几年，直到最后一台设备被扔进垃圾箱。
- 2008年，首次记录的分布式拒绝服务IoT僵尸网络攻击是使用基于Linux的CPE宽带路由器的僵尸网络完成的。
- 2012年，一位不知名的研究人员发布了一份名为“2012年互联网普查”的报告。该报告中使用的数据是通过使用默认凭证入侵全球约420,000个CPE设备而收集的[1]

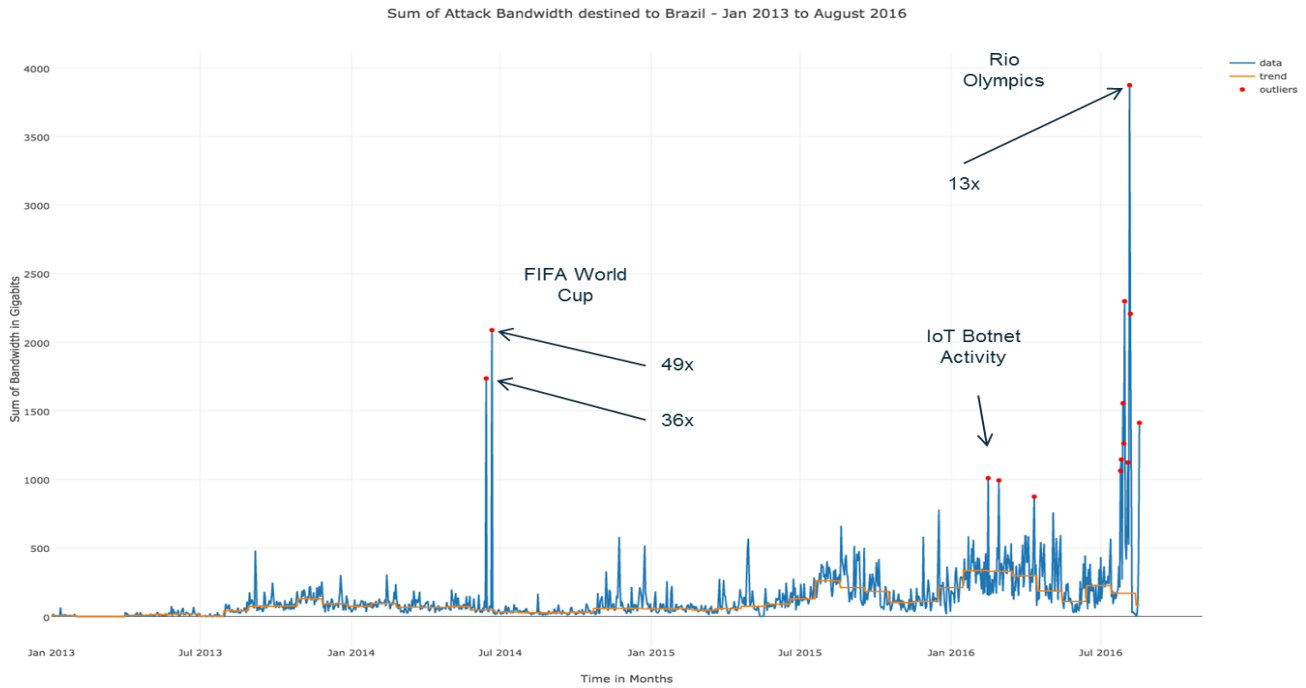
1) https://en.wikipedia.org/wiki/Carna_botnet

物联网僵尸网络的现状

物联网僵尸网络现已配备武器，可通过引导程序/压力测试服务使用：

- 2016年，使用Lizardstresser代码的IoT僵尸网络攻击了巴西的站点，攻击量达400GB / 秒。
- 同一僵尸网络由大约10.000个网络摄像头组成，用于在2016年夏季对奥林匹克附属组织发起540gb / s持续攻击。
- 2016年11月，针对安全记者布莱恩·克雷布斯的分布式拒绝服务攻击使用了基于Mirai代码库的IoT僵尸网络，峰值速度为620gb / sec。
- 2016年11月，针对使用授权的域名系统提供商Dyn进行的攻击中使用了基于Mirai代码的IoT僵尸网络。LizardStresser机器人和Mirai机器人的源代码已经被广泛使用，并产生了多个新变体。

LizzardStresser Bot袭击巴西



- 不仅对体育赛事基础设施发起攻击，还对相关赞助商，金融和政府机构发起攻击。

处理物联网僵尸网络

物联网僵尸网络感染媒介– Mirai示例

1. 受到威胁的设备将创建一个单独的扫描线程，使用随机IP扫描TCP端口23,2323,23231,37777和7557（+5555）（TR-069 / TR-064 SOAP接口）上的其他设备。
2. 如果设备响应，将尝试使用一组常见的用户名/密码组合登录
3. 如果成功，则将易受攻击设备的IP地址发送到C&C服务器。
4. C&C服务器将登录设备，下载适当的恶意软件并破坏设备。设备现在将开始扫描，转到第1个

- 按照目前的情况，有漏洞的设备将在连接到互联网后的几分钟内被感染。
- 易受攻击的设备主要来自中国的3个制造商，其中一个在2014年发布了补丁，但仅提供其软件的英语版本。

MIRAI僵尸网络

全球约有500,000台设备

- 中国，香港，澳门，越南，台湾，韩国，泰国，印度尼西亚，巴西和西班牙的高浓度

Krebs，OVH Dyn和利比里亚攻击中使用的同一僵尸网络恶意软件

- 并不意味着是相同的对手

多个可能的分布式拒绝服务攻击媒介

至少已感染了一种变体！

物联网僵尸网络分布式拒绝服务攻击功能– Mirai

Flash更新2016年12月15日
Mirai的一个新变种出现在狂放的欺骗流量中。攻击包括SYN泛洪攻击，域名系统反射/放大攻击和TCP反射放大攻击

攻击类型：

- UDP泛洪
- 气门源发动机溢流
- TCP ACK泛洪
- TCP“Stomp”攻击（已建立的TCP连接上的ACK泛洪，旨在绕过分布式拒绝服务缓解设备）
- TCP SYN泛洪
- GRE数据包泛洪
- HTTP请求泛洪（GET，POST，HEAD）
- 域名系统伪随机标签前缀（“域名系统酷刑”）

Mirai恶意软件在用户空间中运行，到目前为止，尚未使用欺骗性IP地址，禁止其进行欺骗性和反射攻击。

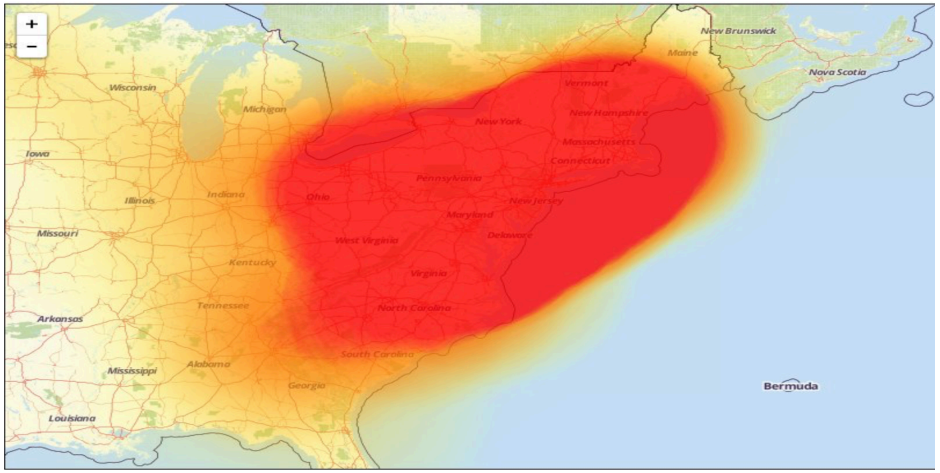
ARBOR NETWORKS

DYN攻击10月21日

针对**Dyn**托管域名系统基础设施的三大攻击**Dyn**客戶包括

- Netflix Twitter, Reddit, Github, Spotify, PayPal, Airbnb, NYT, 等.

这些攻击导致**Dyn**客户大规模停电，即使客户没有受到直接攻击



ARBOR NETWORKS

DYN攻击时间表

攻击1
开始: 11:10 UTC

持续时间: 2小时20分钟

攻击2
开始 : 15:50 UTC

持续时间 : 1小时10分钟

攻击3
从一开始就缓解

目的地：亚太地区，南美，东欧，美国西部和美国东部地区中断

ARBOR NETWORKS

了解和缓解攻击

多个高度分散的攻击媒介

Dyn最初报告“数千万个IP地址”

后来更正为估计的100,000

级联效应

原始攻击造成的域名系统服务中断产生合法的重试活动

这就是导致Dyn最初过度报告攻击IP数量的原因。

缓解措施：

ACLs, S/RTBH, flowspec, IDMS

ARBOR NETWORKS

利比里亚袭击– 10月31日开始

SC Magazine US > News > Analysts mixed on reason for Liberia Mirai attack

by Bradley Barth, Senior Reporter

November 04, 2016

Analysts mixed on reason for Liberia Mirai attack

A barrage of Mirai botnet-fueled distributed denial of service (DDoS) attacks reportedly incapacitated Internet operations across the West African coastal nation of Liberia earlier this week, bu industry researchers had mixed views on the rationale behind the attack and damage inflicted.

A large botnet operation dubbed Shadows Kill targeted Liberian IP addresses with a DDoS attack over several days this past week, prompting speculation as to the perpetrators' true motive.

In a Thursday post on the publishing site *Medium*, independent researcher Kevin Beaumont reported a series of "continued short duration attacks" – perpetrated by a Mirai botnet composed of Internet of Things devices such as CCTV cameras – that may have crippled Liberia's Internet infrastructure. Beaumont linked the attacks to the same actor that launched a massive attack against the DNS service Dyn on Oct. 21, knocking out such websites as Amazon, Reddit and Twitter.

~~物联网~~僵尸网络分布式拒绝服务缓解

物联网僵尸网络并不是什么新鲜事物，所使用的攻击也不是什么新鲜事物。
相同的分布式拒绝服务缓解方法仍然适用！

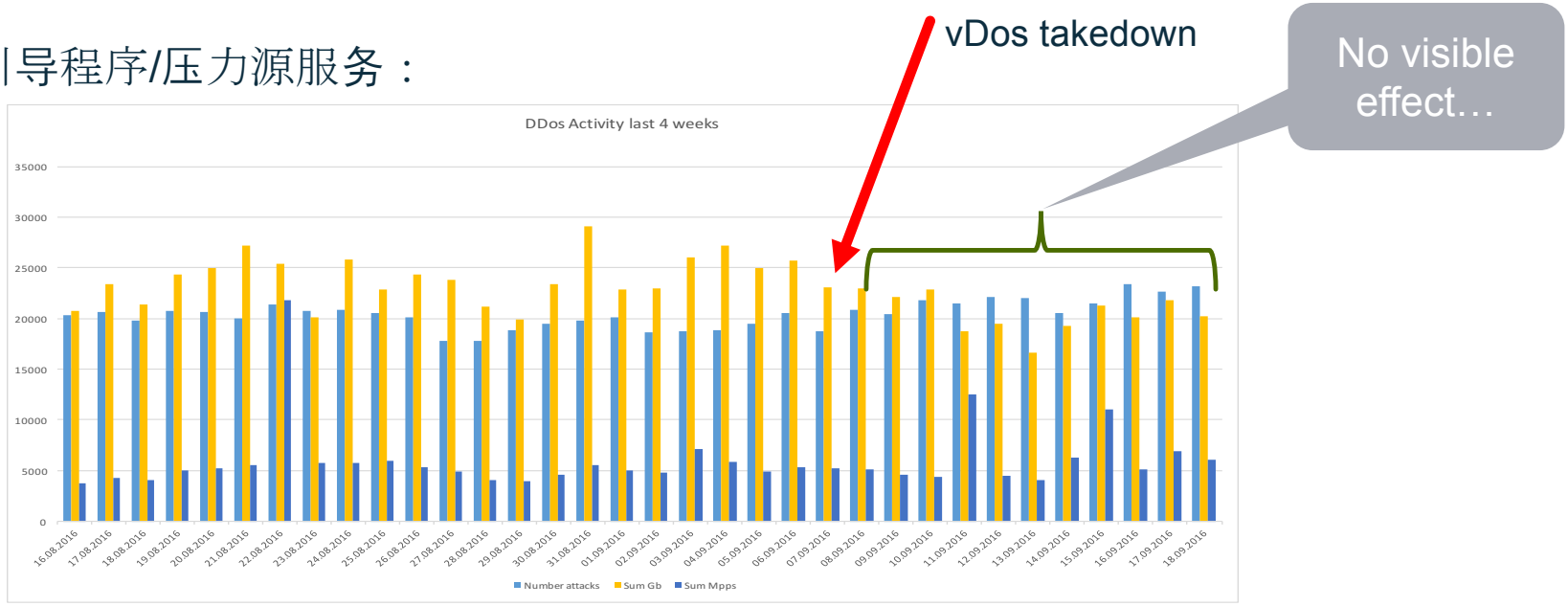
- 为基础设施，主机/应用程序/服务和域名系统服务器实施最佳实践（BCP）。这包括为常见服务器类型指定网络访问策略。
- 使用流量遥测技术检测，分类和追溯分布式拒绝服务流量。
- 使用S /RTBH，flowspec，智能分布式拒绝服务缓解解决方案（IDMSes）缓解攻击。
- 规划和实践应对分布式拒绝服务攻击。

ARBOR NETWORKS

如何减少物联网僵尸网络的威胁

物僵尸网络今天很流行，因为物联网设备容易受到攻击，并且可以轻松使用用于感染和颠覆攻击的工具。

1. 关闭引导程序/压力源服务：



如何减少物联网僵尸网络的威胁（续）

2. 停止销售和部署易受攻击的物联网设备：
   - 谁来强制执行此操作？
   - 谁为此支付费用？
   - 人们是否在乎自己的网络摄像头正在攻击他人？

3. 修补易受攻击的物联网设备：
   - 您上次升级CPE设备的时间是什么时候？智能电视？咖啡壶？您的智能灯泡？
   - 攻击威斯康星大学的Netgear路由器从来没有打过补丁，只有在将最后一台设备扔进垃圾箱后，攻击消亡了。

4. 如果无法固定（或信任）物联网设备，请将其与互联网隔离开来，并创建障碍！

ARBOR NETWORKS

Steinthor的家庭网络如何隔离物联网设备！ ☺

2011年，Steinthor将3个IP网络摄像头连接到了他的家庭网络。这些设备与Synology NAS通信，后者提供视频门户并存储所有视频记录。

网络分为两个领域：

- 用户VLAN
- 视频子网，（旧的）Cisco ASA 5505控制网络摄像头和NAS之间的所有通信。

VideoCameras (5 incoming rules)

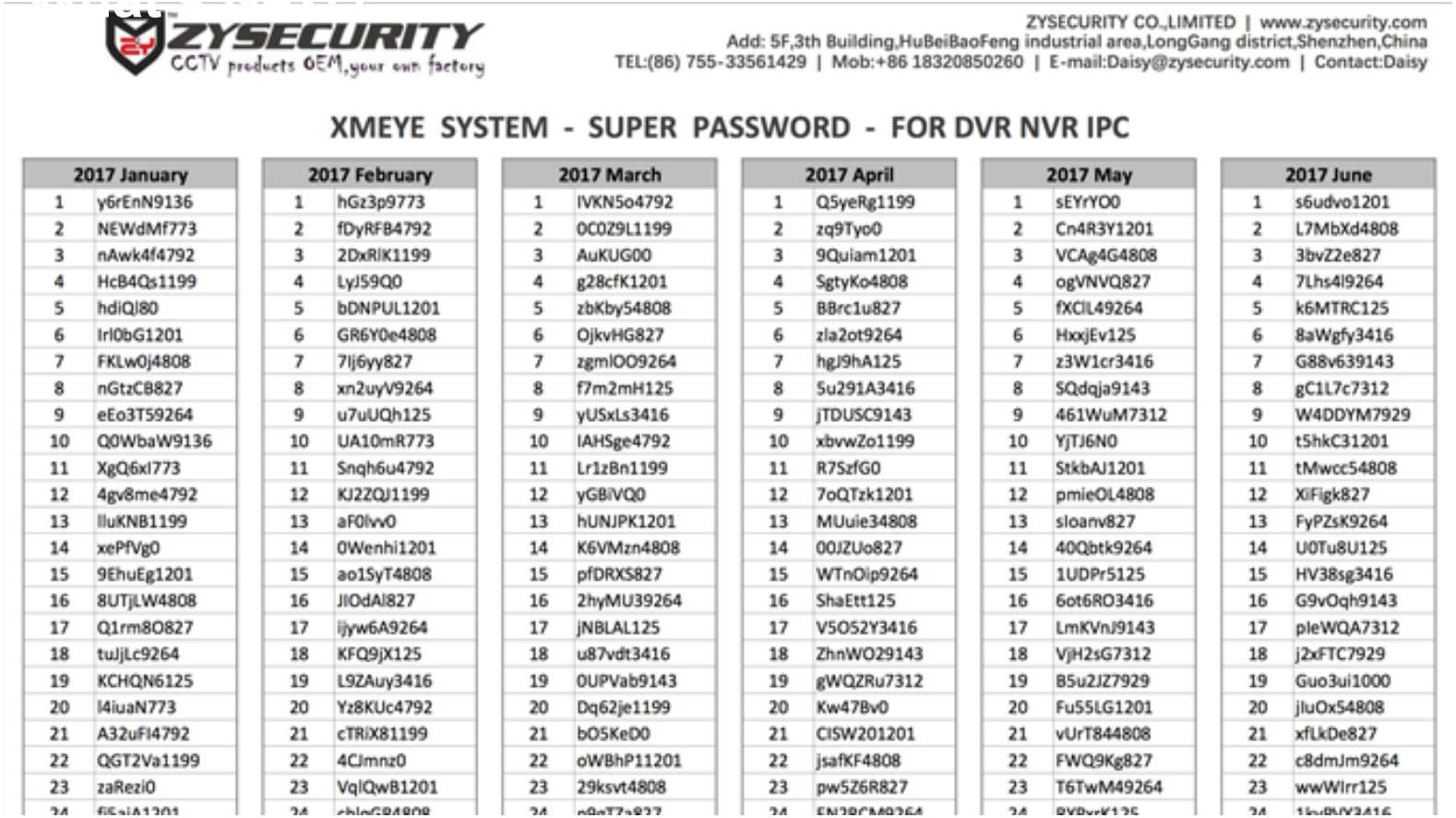
1	☑	any	SynologyNAS	ip	Permit	TOP 10	3975813		
2	☑	any	any	echo-reply	Permit		0		
3	☑	any	any	domain	Permit		0		
4	☑	any	any	ntp	Permit		160		
5		any	any	ip	Deny				Implicit rule

L3 VPN用于允许远程访问Synology上运行的网络摄像头门户。

1) See also http://robert.penz.name/1341/ready-your-home-network-for-iot/

接下来是什么？

接下来是什么？



ZYSECURITY
CCTV products OEM, your own factory

ZYSECURITY CO.,LIMITED | www.zysecurity.com
Add: 5F,3th Building,HuBeiBaoFeng industrial area,LongGang district,Shenzhen,China
TEL:(86) 755-33561429 | Mob:+86 18320850260 | E-mail:Daisy@zysecurity.com | Contact:Daisy

XMEYE SYSTEM - SUPER PASSWORD - FOR DVR NVR IPC

	2017 January		2017 February		2017 March		2017 April		2017 May		2017 June
1	y6rEnN9136	1	hGz3p9773	1	IVKN5o4792	1	Q5yeRg1199	1	sEYrYO0	1	s6udvo1201
2	NEWdMf773	2	fDyRFB4792	2	0C0Z9L1199	2	zq9Tyo0	2	Cn4R3Y1201	2	L7MbXd4808
3	nAwk4f4792	3	2DxRlK1199	3	AuKUG00	3	9Quiam1201	3	VCAg4G4808	3	3bvZ2e827
4	HcB4Qs1199	4	LyJ59Q0	4	g28cfK1201	4	SgtyKo4808	4	ogVNVQ827	4	7Lhs4l9264
5	hdiQl80	5	bDNPUL1201	5	zbKby54808	5	BBrc1u827	5	fXCIL49264	5	k6MTRC125
6	Irl0bG1201	6	GR6Y0e4808	6	OjkvHG827	6	zla2ot9264	6	HxxjEv125	6	8aWgfy3416
7	FKLw0j4808	7	7lj6yy827	7	zgmlOO9264	7	hgJ9hA125	7	z3W1cr3416	7	G88v639143
8	nGtzCB827	8	xn2uyV9264	8	f7m2mH125	8	5u291A3416	8	SQdqja9143	8	gC1L7c7312
9	eEo3T59264	9	u7uUQh125	9	yUSxLs3416	9	jTDUSC9143	9	461WuM7312	9	W4DDYM7929
10	Q0WbaW9136	10	UA10mR773	10	IAHSge4792	10	xbvwZo1199	10	YjTJ6N0	10	t5hkC31201
11	XgQ6xl773	11	Snqh6u4792	11	Lr1zBn1199	11	R7SzfG0	11	StkbAJ1201	11	tMwcc54808
12	4gv8me4792	12	KJ2ZQJ1199	12	yGBiVQ0	12	7oQTzk1201	12	pmieOL4808	12	XiFigk827
13	lluKNB1199	13	aF0lvv0	13	hUNJPK1201	13	MUuie34808	13	sloanv827	13	FyPZsK9264
14	xePfVg0	14	0Wenhi1201	14	K6VMzn4808	14	00JZUo827	14	40Qbtk9264	14	U0Tu8U125
15	9EhuEg1201	15	ao1SyT4808	15	pfDRXS827	15	WTnOip9264	15	1UDPr5125	15	HV38sg3416
16	8UTjLW4808	16	JlOdAl827	16	2hyMU39264	16	ShaEtt125	16	6ot6RO3416	16	G9vOqh9143
17	Q1rm8O827	17	ijyw6A9264	17	jNBLAL125	17	V5O52Y3416	17	LmKVnJ9143	17	pleWQA7312
18	tuJjLc9264	18	KFQ9jX125	18	u87vdt3416	18	ZhnWO29143	18	VjH2sG7312	18	j2xFTC7929
19	KCHQN6125	19	L9ZAuy3416	19	0UPVab9143	19	gWQZRu7312	19	B5u2JZ7929	19	Guo3ui1000
20	l4iuaN773	20	Yz8KUc4792	20	Dq62je1199	20	Kw47Bv0	20	Fu55LG1201	20	jluOx54808
21	A32uFI4792	21	cTRiX81199	21	bO5KeD0	21	CISW201201	21	vUrT844808	21	xfLkDe827
22	QGT2Va1199	22	4CJmnz0	22	oWBhP11201	22	jsafKF4808	22	FWQ9Kg827	22	c8dmJm9264
23	zaRezi0	23	VqlQwB1201	23	29ksvt4808	23	pw5Z6R827	23	T6TwM49264	23	wwWlrr125
24	fiSajA1201	24	cblgGR4808	24	n9gTZa827	24	FN2RCM9264	24	RYRxrK125	24	1hvPNX3416

接下来是什么？

消费级“ IoT”设备的类别很多很多，包括灯泡，恒温器，“智能电表”等。等

大型运营商级和企业路由器以前曾遭到入侵，用于ICMP泛洪分布式拒绝服务攻击，分布式拒绝服务和垃圾邮件路由劫持（cisco / cisco证书，甚至用于Juniper路由器）

NAT /防火墙后面的物联网设备多阶段扫描/破坏！

现在我们有了NETCONF和各种SDN API。 。 。

。 。 。以及在路由器本身上运行任意代码的能力。

网络基础设施BCP比以往任何时候都更加重要！

所有路由器都是“ IoT”嵌入式设备，包括大型路由器！智能手机也一样！

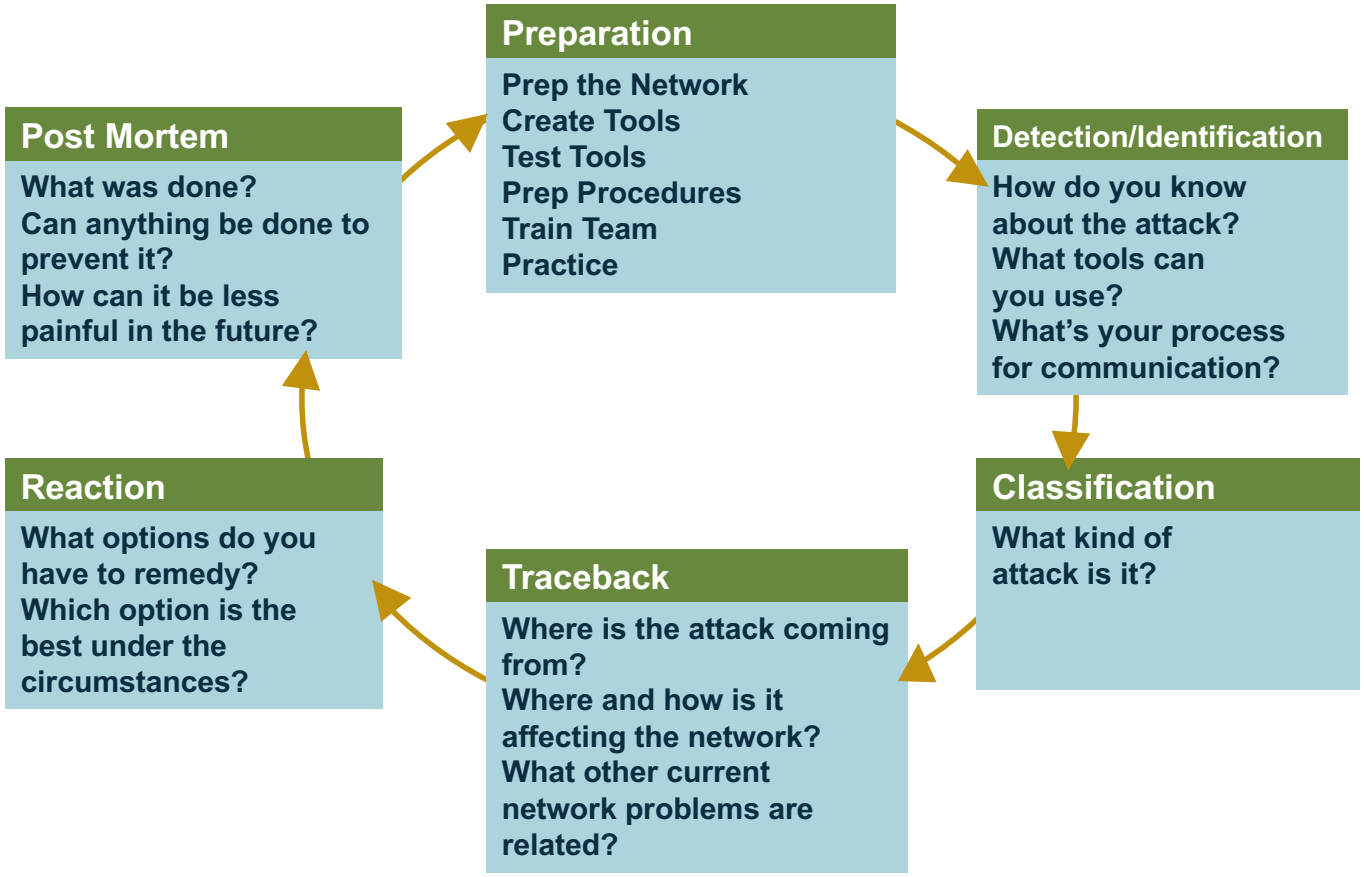
我们该怎么办？

网络/应用程序可用性：保护基础设施

- 安全是互联网络未来的核心。我们已经从隐性信任互联网转变为普遍不信任互联网
- 没有数据包是可以信任的。所有数据包都必须通过网络设备检查和实施策略的能力赢得信任
- 保护基础设施是最基本的安全要求
- 所有高可用性设计中均应包括基础设施保护
- 安全的基础设施为持续提供服务奠定了基础

ARBOR NETWORKS

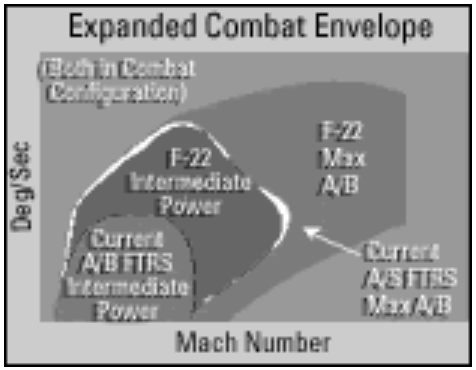
事故响应的六个阶段

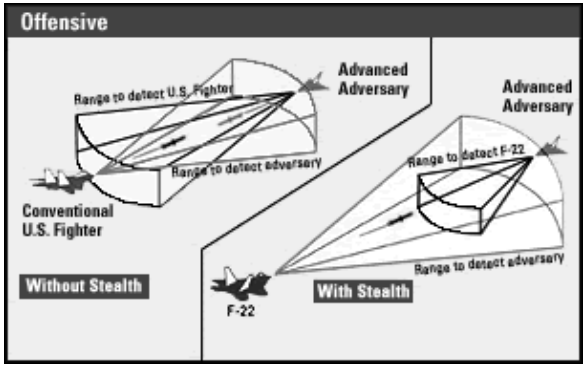

Preparation
Prep the Network
Create Tools
Test Tools
Prep Procedures
Train Team
Practice
Detection/Identification
How do you know about the attack?
What tools can you use?
What's your process for communication?
Classification
What kind of attack is it?
Traceback
Where is the attack coming from?
Where and how is it affecting the network?
What other current network problems are related?
Reaction
What options do you have to remedy?
Which option is the best under the circumstances?
Post Mortem
What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

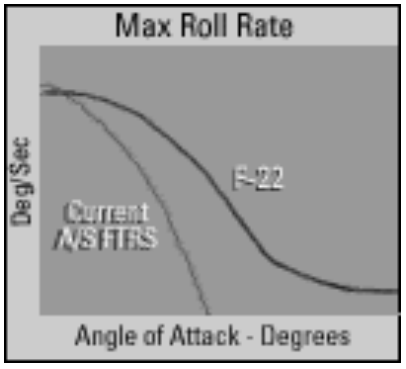
您是否在使用信封？

了解您的设备和基础设施！

- 了解所有设备（路由器，交换机，服务器等）的性能指标。您需要知道设备的真正功能！
- 了解网络功能。如果可能，进行测试。在安全事件期间，惊喜并不有趣
- pps vs. bps vs. qps vs. cps vs. tps-以及启用功能如何对其产生影响





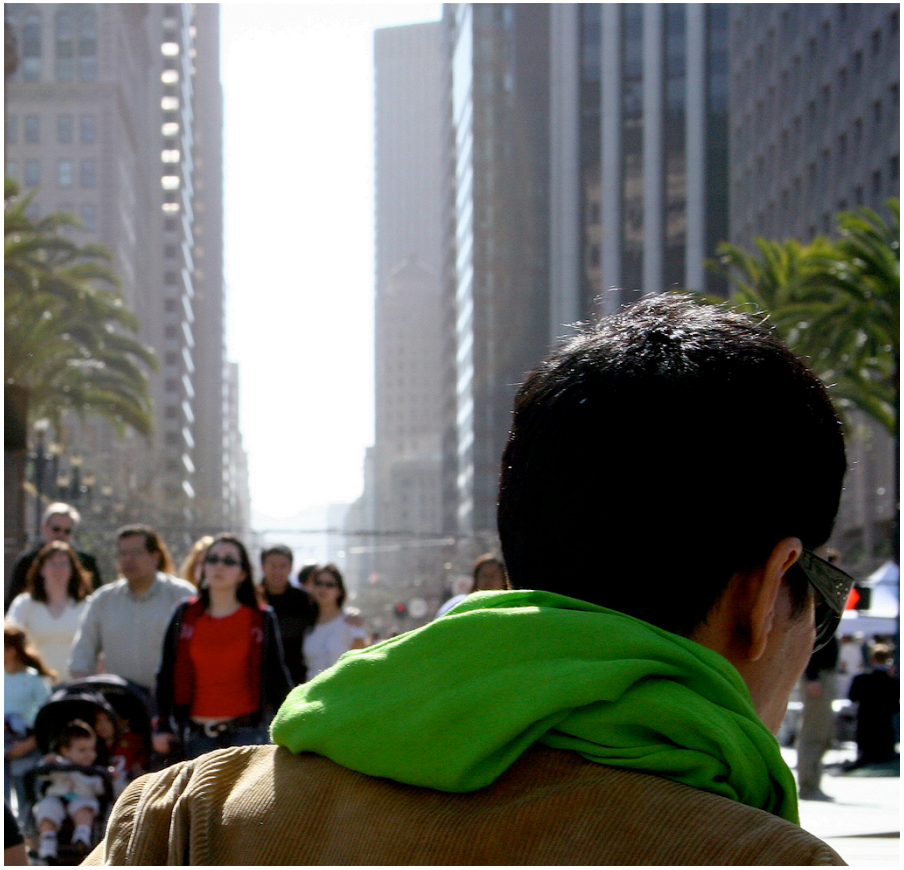


ARBOR NETWORKS

架构

适合工作的合适工具

合适的人选对的工作



OPSEC团队技能要求

OPSEC团队需要知道：

骨干工程师知道的一切

网络管理工程师知道的一切系统管理员/网站管理员

知道的一切

域名系统（DNS）/ DHCP /地址工程师知道的一切

企业信息安全专家知道的一切

本质上，您正在寻找混合主干/安全工程师的超级工程师。

基础设施最佳实践（BCP）

- 应在相关网络边缘（对等/传输，客户聚合边缘等）使用接口ACL（iACL）保护网络基础设施本身；应使用其他特定于服务的部分，将发往面向互联网的服务器的流量限制为与那些服务器上的服务和应用程序相关的端口和协议。

- 在这些攻击中使用GRE（IP协议47）是一种常见的机制，攻击者绕过仅包含与诸如TCP，UDP和ICMP等通用协议相关的策略声明的ACL的常见机制。有效的互联网协议有254种，无关的协议应通过ACL在边缘进行过滤。

- 还应该部署其他网络基础设施BCP，例如控制平面和管理平面自我保护机制（rACL，CoPP，GTSM，MD5密钥等）。

- 所有网络基础设施设备都只能通过指定的管理主机访问，并且应该通过专用的带外（OOB）管理网络促进访问。在高影响力分布式拒绝服务攻击期间，专用管理网络可确保在生产网络上不受条件影响的情况下对设备进行管理，并确保流量遥测和SNMP等重要机制不中断，从而确保在事件期间持续可见攻击流量

ARBOR NETWORKS

基础设施BCP（续）

- 应当在所有网络边缘启用流量遥测技术，如思科NetFlow，瞻博网络cflowd和sFlow，并将其导出到收集/分析系统。
- 基于源的远程触发黑洞（S /RTBH）是一种强大的反应技术，可根据其源地址快速对成百上千的攻击源IP（通过流分析，日志文件等分类）。 S /RTBH利用BGP作为控制平面机制，立即向边缘设备发送信号，开始丢弃攻击流量。 Flowspec支持第4层粒度-通过BGP即时部署ACL！
- 智能分布式拒绝服务缓解系统（IDMS）应部署在拓扑适合的清洁中心，以保护服务器/服务/应用程序。应将它们放在负载平衡器的北向；如果组织坚持在服务器前串联防火墙和IDS/“ IPS”，请保护这些有状态分布式拒绝服务扼流点及其背后的一切！
- 请勿在服务器前放置防火墙和IDS /'IPS'-
在定义为未经请求的每个传入连接的服务器环境中，防火墙和IDS /IPS均不提供任何安全价值。它们是分布式拒绝服务的瓶颈，会降低网络和应用程序的运营安全状况。
- 策略应由基于硬件的路由器/交换机中的无状态ACL实施！

ARBOR NETWORKS

主持最佳实践（BCP）

- 应以强化方式配置面向公众的服务器，并禁用不必要的服务，OOB管理访问，特定于服务的配置强化，IP堆栈调整和其他相关机制。

- 通过tcpwrappers对服务器进行无状态过滤是一种有用的策略执行机制。对于网络服务器，Apache模块（如mod_security和mod_evasive）带来了附加功能。

- 禁止在面向互联网的服务器前部署状态防火墙或其他检查设备，如IDS /IPS。根据定义，由于每个到互联网连接服务器的传入连接都是不请自来的，因此有状态检查不会增加服务器的安全状况，而且由于状态表规模（即使最大/最大的/当今市场上最快的防火墙和IDS / IPS。

  在这些特定的攻击以及许多其他攻击过程中，观察到目标服务器前面的防火墙发生故障，同时接收到的攻击流量相对较低，从而使分布式拒绝服务攻击程序能够成功地使攻击者仅花费很少的精力就使服务器不可用。

ARBOR NETWORKS

主机BCP（续）

- 负载平衡器还实例化状态，使负载平衡器后面的真实服务器更容易受到分布式拒绝服务攻击。在这些攻击中，观察到负载均衡器由于攻击流量导致状态耗尽而失效。应该使用S / RTBH，flowspec，反向代理缓存和IDMS保护负载平衡器及其背后的真实服务器。

- 域名系统（DNS）基础设施应部署在模块化的，有隔板的架构中，并分隔权威服务器，内部解析器，外部解析器，仅缓存解析器等功能，并应采用IPv4任播寻址等技术进行适当扩展。应使用Flowspec，S /RTBH，DNS服务器自防御机制（如RRL和IDMS）保护DNS免受故意攻击和/或附带损害。

我们注定要失败吗？

- 不！部署现有的众所周知的工具/技术/ BCP，可以大大改善安全状况，并提供可衡量的结果。
- 抵御这些攻击的防御技术演变表明，有可能实现积极变革-目标组织和防御ISP / MSSP改变了架构，缓解技术，流程和程序，可以成功缓解此类攻击。
- 缓解能力正在扩展，以满足和超过攻击量–部署架构，转移/重新注入带宽，利用网络基础设施至关重要。
- 自动化是一件好事，但无可替代的有弹性的架构，有洞察力的规划和聪明的opsec人员，如今，这些人员比以往任何时候都更加重要！

总结

- 今天的情况类似于Windows XP是最常用的操作系统，有很多易受攻击的设备，对防御威胁的防御措施也很少。通过发布更具弹性的软件来解决此问题，逐渐使易受攻击的设备数量减少。但是，我们仍然有易受攻击的Windows XP计算机连接到互联网…
☹ . . . 现在我们有了数量级更高的易受攻击的物联网设备！
- 僵尸机器人越来越智能，拥有更先进的功能。基于Windows的Medusa机器人会产生IE浏览器线程来执行高级HTTP和HTTP / S攻击。 → 需要更多情报来应对这些攻击，而我们有！
- 必须在攻击发生之前实施防御措施！
- 每天都有成功的分布式拒绝服务防御高容量，高复杂度攻击！
- *我们知道该怎么做！*

谢谢!

Roland Dobbins, *首席工程师*
<rdobbins@arbor.net>

ARBOR NETWORKS
The Security Division of NETSCOUT