

2017年IoT僵尸网络C&C服务器数量翻倍

 [Andy](#)

2018-01-12

共38383人围观

无线安全

2017年，用于管理物联网僵尸网络的命令和控制（C&C）服务器数量增加了一倍多，从2016年的393台增至2017年943台。这个数字是根据Spamhaus提供的统计数据，它将滥用网络主机的数据作为黑名单的一部分进行汇总。

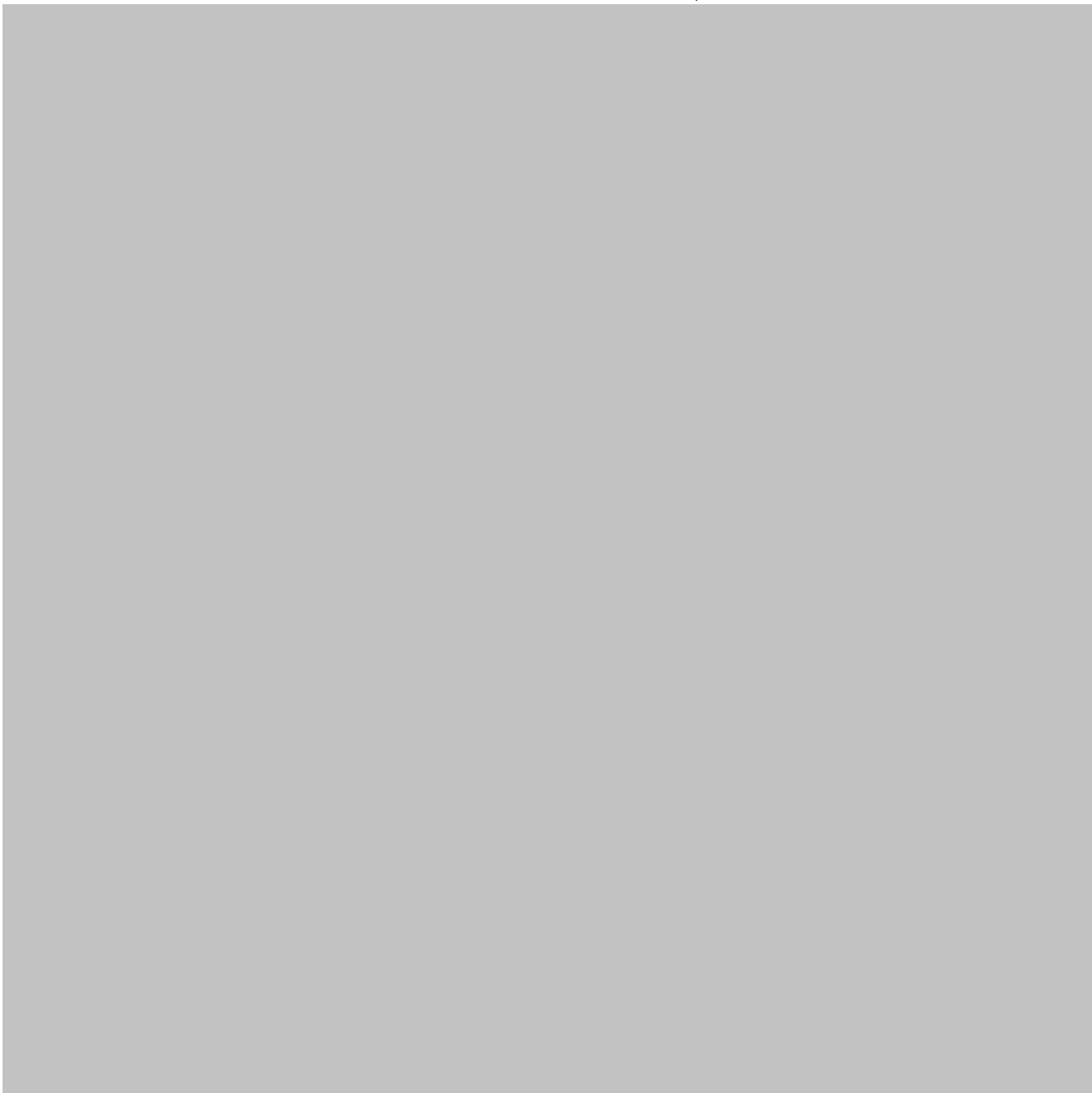


僵尸网络IP总量增长了32%

在过去一年的总结报告中，Spamhaus表示，2017年有超过9,500个新的僵尸网络C&C服务器，比上一年增加了32%。数字包括由多种设备组成的僵尸网络C&C服务器的IP地址，而不仅仅是物联网设备。

9,500+的数字还包括探测到的用于各种网络犯罪活动的C&C服务器，例如用于控制DDoS僵尸网络，垃圾邮件网络，行木马，还有骗子用来从网络钓鱼工具和infostealer恶意软件发送收集的数据的服务器。





骗子更热衷购买服务器而不是黑客

Spamhaus表示，在2017年突然出现的9,500个新僵尸网络C&C服务器中，绝大多数（6,588个IP地址，占总数的68%）是从Web主机供应商购买单个服务器的IP地址，专门用于托管恶意软件。

而其余部分则是被黑客入侵的服务器上托管的僵尸网络C&C服务器。据报道，用于恶意软件和网络犯罪活动购买的被黑的服务器比例与2016年保持一致。

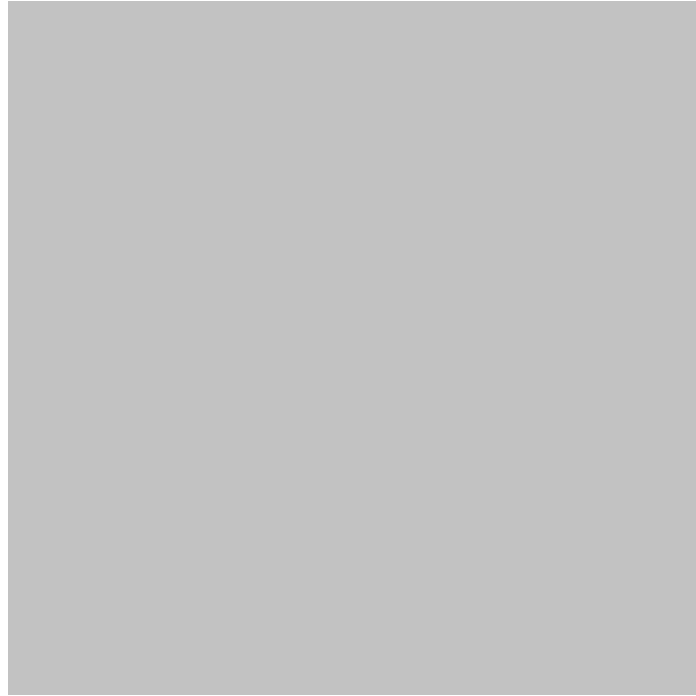
Pony在C&C服务器中应用最为普遍

被Spamhaus收录的C&C服务器最常见的一类被用于一种信息窃取木马Pony，它可以从受感染的设备收集密码，并选择安装其他恶意软件。



由于物联网恶意软件通常互相演化，恶意软件系列之间相互交织在一起，不同的物联网僵尸网络的探测也会被整合一起。在综合排名中，物联网僵尸网络在2017年发现最常见的C&C服务器中排名第二。

以下是Spamhaus收录的20种最常见的僵尸网络C&C服务器的图表，以及Spamhaus报告中发布的其他统计数据。



在2014年统治排行榜之后，被用于Zeus银行木马的C&C服务器跌出了TOP20；

Cerber位居第七名，而勒索软件从2016年开始排名就发生变化，Locky 和TorrentLocker勒索软件跌出TOP20；

基于Java的勒索软件在去年一整年都非常流行，像JBifrost (#6) 和 Adwind (#11)这两个基于Java的远程访问工具进入了TOP20；

OVH和亚马逊托管着最多的BCL记录。

C&C服务器域名的25%是通过Namecheap注册

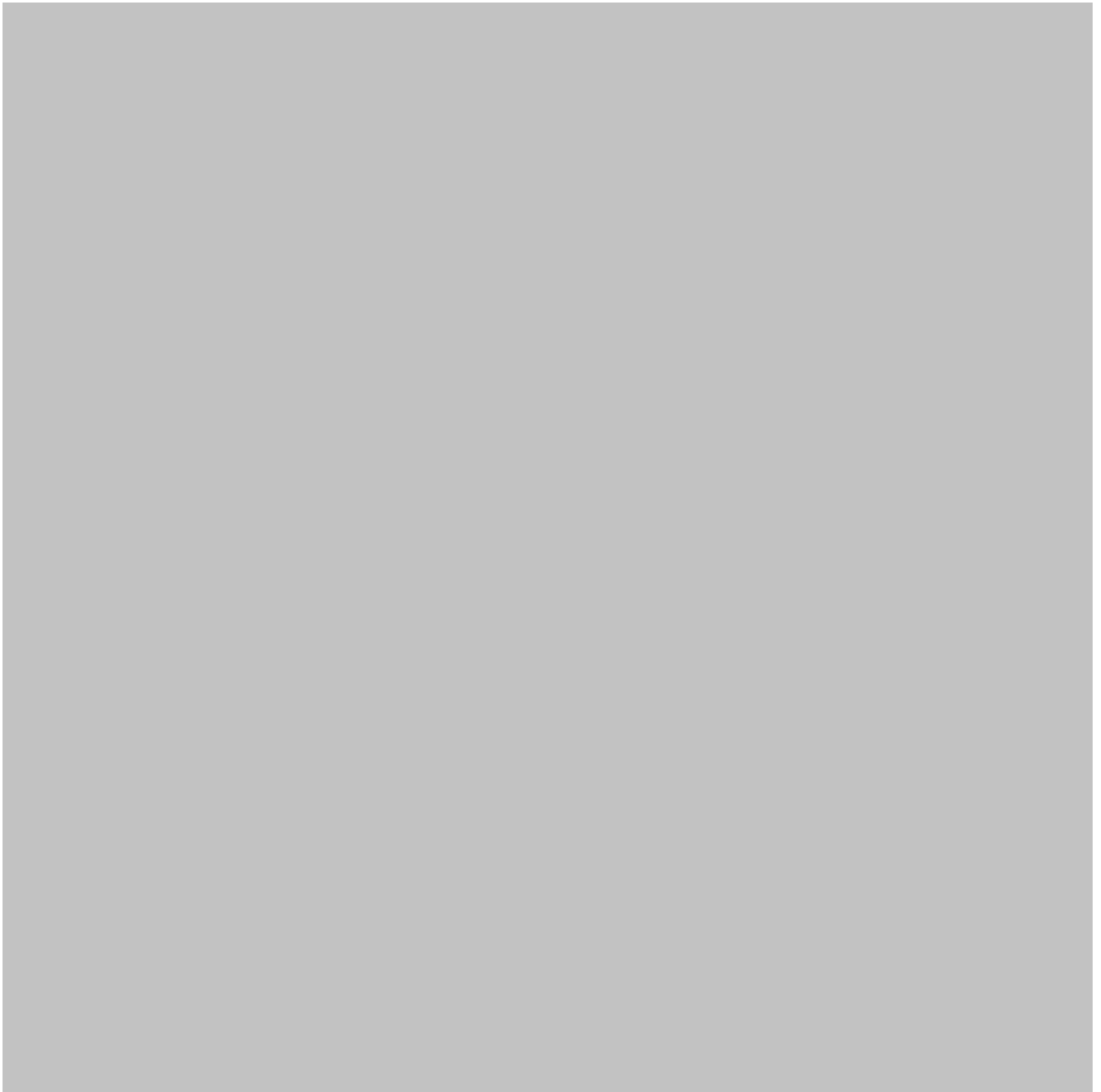
但除IP地址外，Spamhaus还跟踪并创建了一个域名黑名单—— Spamhaus DBL，以防骗子决定将C&C服务器隐藏在用域名而不是IP地址之后。

Spamhaus说，骗子通常更喜欢使用域名，租用VPS系统而不是IP地址和被黑的服务器。这些组织的专家解释如下：

为了托管他们的僵尸网络控制器，网络犯罪分子通常更愿意使用专门注册的域名。这是因为专用域名允许网络犯罪分子启动新的VPS，加载僵尸网络控制器工具包，并在他主机提供商关闭其C&C服务器之后立即重新联系僵尸网络。无需更改僵尸网络中每个受感染计算机的配置是主要优势。

在年终统计中，很容易看到这种C&C服务器使用域名而非IP地址的好处。据Spamhaus介绍，该组织的DBL在201





根据Spamhaus数据，骗子通常使用.com和.pw域名，并通过美国域名注册商Namecheap注册了超过四分之一的C&C网络服务器。

*参考来源：[bleepingcomputer](#)，FB小编Andy编译，转载请注明来自FreeBuf.COM

上一篇：[水滴事件后，你的摄像头就安全了吗？](#)

下一篇：[本篇已是最新文章](#)

选择文件 未选择任何文件



必须 您当前尚未登录。[登陆?](#) [注册](#)

昵称

请输入昵称

邮箱

请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



Andy

曾梦想仗剑走天涯，看一看世界的繁华。

26
文章数

10
评论数

最近文章

- [2017年IoT僵尸网络C&C服务器数量翻倍](#)

2018.01.12
- [BUF早餐铺 | Intel实测CPU漏洞补丁对性能影响不大；macOS再现严重漏洞；恶意软件LockPoS使用新的注入技术来避免检测；《绝地求生》国内外挂太多，国外玩家Steam刷屏求锁区](#)

2018.01.12
- [不止于小程序，APICloud推出React Native纯翻译模式的UI引擎](#)

2018.01.11

浏览更多

相关阅读

- [僵尸网络的全球分布图原来是这样的...](#)
- [使用OpenBTS基站测试物联网模块安...](#)
- [【BlackHat 2017】小米9号平衡车国际...](#)
- [1Tbps! OVH遭遇史上最大DDoS攻击](#)
- [俄罗斯僵尸网络幕后黑手被逮捕-控制6...](#)


特别推荐



极客DAY：手机文件直传U盘，三步教你做一根OTG传输线 <small>关注我们 分享每日精选文章</small> geekman 2014-12-27	独家分析：安卓“Janus”漏洞的产生原理及利用过程 顶象技术 2017-12-12	
量子计算从概念走入现实，公钥加密是否岌岌可危 Elaine_z 2017-07-18	快讯：联想官网被黑，内部邮件被劫持 hujias 2015-02-26	



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务

 css.php

