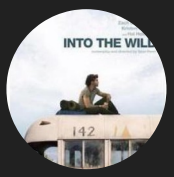

kenshin

DTA

七年一剑，360 DNS威胁分析平台

360Netlab (360 网络安全研究院) 自2014年成立以来，大网安全分析相关技术一直是我们的核心研究方向，我们是最早在国内提出从数据维度做安全的团队，并将大数据技术、AI技术和威胁情报应用于大网安全研究工...

· Oct 21, 2021 · 12 min read

Import 2022-11-30 11:16

MsraMiner 被曝光后72小时内的更新

3月16日，我们文章 中，提到了 MsraMiner，一个潜伏已久的挖矿僵尸网络。 DNSMon 在过去的72小时内，提示我们该僵尸网络有更新，如下： * 样本压缩包文件改名为 ProximityUntilCache32.tlb ，原来叫 MsraReportDataCache32.tlb * 矿机程序被重命名为 WUDHostServices.exe ，原来是 TrustedHostServices.exe * 样本里的 C2 Domain 被替换为 tsk.tknuv.com / err.tknuv.com / slo.tknuv.com ，原来是 ccc.njaavfxcgk3.club / rer.njaavfxcgk3.club / acs.njaavfxcgk3.club 新的矿池域名和挖矿账号如下，其中，jiovt.com 和


· Mar 19, 2018 · 2 min read

en

Memcache DDoS: A Little Bit More

This blog is a joint effort of 360 0kee Team, 360 CERT, and 360 Netlab. Memcache UDP Reflection Amplification DDoS (hereinafter referred as Memcache DRDoS) has attracted quite some attentions from security community this week. We are not going to repeat the public known facts, and this blog will only


· Mar 1, 2018 · 3 min read

DDoS

Memcache UDP反射放大攻击技术分析

本篇技术blog，由360信息安全部0kee Team、360网络安全研究院、360-CERT共同发布。 Memcache UDP反射放大攻击（以下简称 Memcache DRDoS）在最近的一周里吸引了安全社区的较多注意。以下介绍我们对该类型攻击观察到的情况。 在PoC 2017 会议上的原始报告 Memcache DRDoS，由360信息安全部0kee Team在2017-06 附近首先发现，并于 2017-11 在 PoC 2017 会议上做了公开报告。会议报告在 这里，其中详细介绍了攻击的原理和潜在危害。 在这份文档中，作者指出这种攻击的特点： * memcache 放大倍数超高，至少可以超过50k； * memcache 服务器（案例中的反射点）数量较多，2017-11时估算全球约有 60k 服务器可以被利用，并且这些服务器往往拥有较高的带宽资源。 基于以上特点，作者认为该攻击方式可以被利用来发起大规模的DDoS攻击，某些小型攻击团队也可能因此获得原先没有的大流量攻击能力。 在 DDoSMon 上观察到的现网趋势 自批露以来，


· Mar 1, 2018 · 5 min read

DDoSMon

CLDAP反射放大攻击超过SSDP和CharGen成为第三大反射型

DDoS攻击

作者：Xu Yang，kenshin 利用DDoSMon.net，我们实时并持续的监控全球DDoS攻击相关事件。长期以来，DDoS攻击的反射放大细分类型中，DNS、NTP、CharGen、SSDP是最经常被滥用的服务，过去一年中的排位依次是第1、2、3、4位。 近期我们注意到， 基于CLDAP的 反射放大攻击（以下称为CLDAP攻击）已经超过SSDP和CharGEN成为第三大反射型DDoS攻击。CLDAP攻击在过去365天和90天在反射放大类DDoS攻击中占据比例，对比如下图： 数据来源：DDoSMon。网站上Insight页面的内容可以覆盖本次blog中的大部分数据。CLDAP攻击首次出现是在去年10月底，到现在恰好一年。本篇blog中，我们对CLDAP攻击上升情况做一个回顾： * 在过去的一年中，我们累积观察到304,146次CLDAP反射放大攻击，涉及215,229 个独立IP，或者说受害者。CLDAP早已经成为现实存在的DDoS攻击威胁。 * 值得注意的是，最近两三个月以来，CLDAP攻击发展进入新的阶段。在我们的监测范围内，过去三个月内CLDA

· Nov 1, 2017 · 5 min read

en

CLDAP is Now the No.3 Reflection Amplified DDoS Attack Vector, Surpassing SSDP and CharGen

Author: Xu Yang，kenshin With our DDoSMon, we are able to perform continuous and near real-time monitoring on global DDoS attacks. For quite a long time, DNS, NTP, CharGen and SSDP have been the most frequently abused services in DDoS reflection amplification attacks. They rank respectively 1st, 2nd, 3rd and

· Nov 1, 2017 · 3 min read