Technology Knowledge Base 2019-01

by bugnofree

Publish → 2019-01-01 Update → 2019-03-02

- 2019-01-01 https://linuxhandbook.com/curl-c...: Learn to Use CURL Command in Linux With These Examples
- 2019-01-02 https://arxiv.org/pdf/1812.10729...: Fine-grained Code Coverage Measurement in Automated Black-box Android Testing
- 2019-01-03 https://lwn.net/Articles/531114/: Namespaces in operation, part 1: namespaces overview
- 2019-01-04 https://lwn.net/Articles/531381/: Namespaces in operation, part 2: the namespaces API
- 2019-01-05 https://lwn.net/Articles/531419/: Namespaces in operation, part 3: PID namespaces
- 2019-01-06 https://github.com/divan/txqr/bl...: 二维码动图隔空传数据。

```
TXQR 通过二维码动图传递数据，不得不说什么人都有，思路清新，这种隔空传数据的方
式，给人耳目一新的感觉。
TXQR (Transfer via QR) is a protocol and set of tools
and libs to transfer data via animated QR codes. It uses fountain codes for
error correction.
```

- 2019-01-07 http://litten.me/2014/09/26/hist...: 浏览器野史，文笔幽默十分有意思
- 2019-01-08 https://blog.github.com/2019-01-...: GitHub 提供免费的个人私有仓库.

```
给大家简单传达一下中心思想.
1. 现在 github 提供免费的个人私有仓库，数量无限，每个仓库的合作者最多为 3 个.
    公开仓库则保持原有的规则不变.
2. 商业上则将 GitHub Business Cloud 和 GitHub Enterprise 统一为 GitHub
Enterprise.
```

- 2019-01-09:
  - Advance XSS Persistence With Oauth

```
https://github.com/dxa4481/XSSOauthPersistence
```

- 区块链安全知识库

```
Knowledge Base 慢雾安全团队知识库
https://github.com/slowmist/Knowledge-Base
```

- 最近发生的一次关于ETC的51%攻击事件追踪--慢雾团队

```
https://dwz.cn/2HWcol90
```

- 慢雾区主页

```
https://www.slowmist.com
```

- 2019-01-10 https://github.com/guitmz/virii: 上古时代的恶意病毒代码, 包含源码, 大多都是汇编写的.
- 2019-01-11 https://engineering.purdue.edu/k...

  普渡大学计算机网络安全课程课件
- 2019-01-12 https://github.com/AxtMueller/Wi...

  一个非开源的 Windows 内核研究工具

  A free but powerful Windows kernel research tool

  - Process management (Module, Thread, Handle, Memory, Window, Windows Hook, etc.)
  - File management
  - Registry management
  - Kernel-mode callback, filter, timer, NDIS blocks and WFP callout functions management
  - Kernel-mode hook scanning (MSR, EAT, IAT, CODE PATCH, SSDT, SSSDT, IDT, IRP, OBJECT)
  - User-mode hook scanning (Kernel Callback Table, EAT, IAT, CODE PATCH)
  - Memory editor and symbol parser (it looks like a simplified version of WINDBG)
  - Protect process, hide/protect/redirect file or directory, protect registry and falsify registry data
  - Path modification for driver, process and process module
  - Enable/disable some obnoxious Windows components

- 2019-01-13 https://shanetully.com/2013/12/w...

  Writing a Self-Mutating x86_64 C Program

- 2019-01-14
  - https://github.com/madhuakula/wi...

    Windows one line commands that make life easier, shortcuts and command line fu.

  - kvm 入门资料 @专注逆向-高中没毕业

    最近一直在构建基于qemu的恶意样本养殖系统。然后个人觉得下列的的qemu， kvm入门资料还挺不错的。

    分享一下主要内容就是命令行操作虚拟机的各个组件(命令参数跟docker的比较 类似，对docker比较熟悉的，应该能快速上手)，这里的组件主要是指虚拟机的 磁盘和网络。

    http://linux.dell.com/files/whit...

    http://linux.dell.com/files/whit...

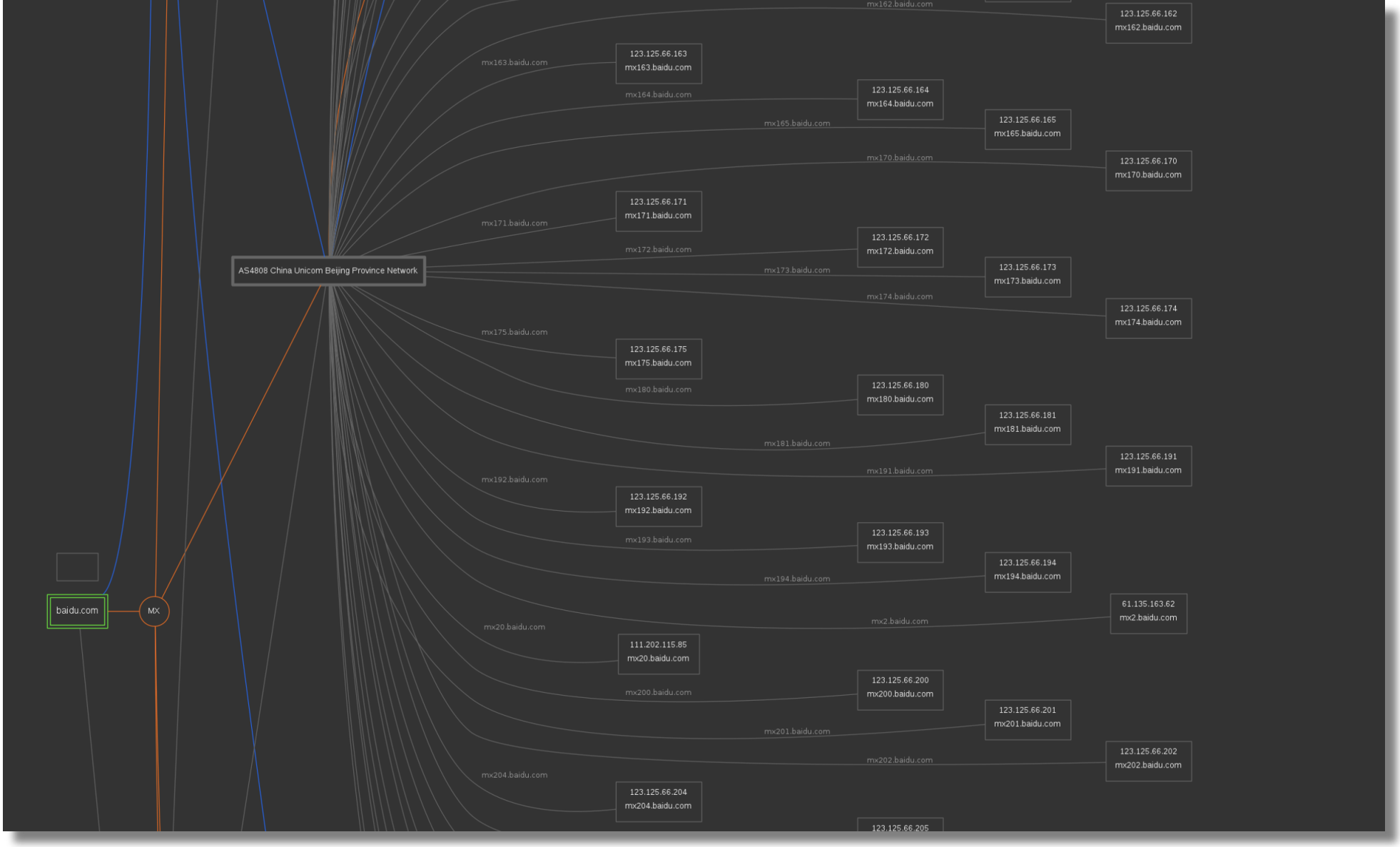
- 2019-01-15 https://github.com/0xgalz/Virtua...

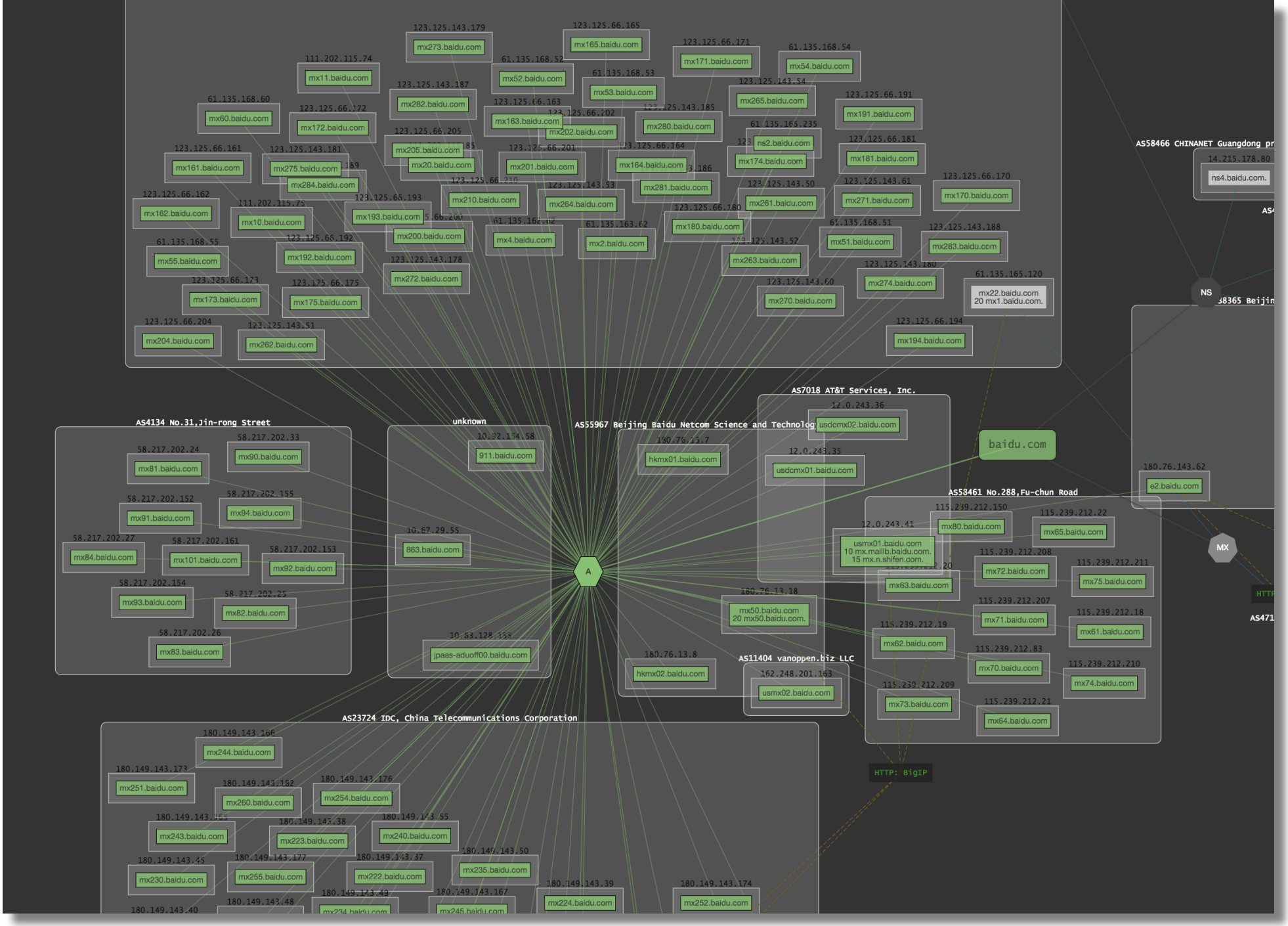
  IDAPython C++ 虚函数表重建

  这是一个 IDApython 工具, 用于重建 C++ 代码中的虚函数表, 适用平台是 Intel x86 和 x64 架构, 该用具由动, 静态两部分组成.

- 2019-01-16 https://dnsdumpster.com/

  免费的域名查找工具, 十分强大, 以百度为例, 看一下其域名分布关系图.


baidu.com
MX
AS4808 China Unicom Beijing Province Network
mx162.baidu.com
123.125.66.162
mx162.baidu.com
mx163.baidu.com
123.125.66.163
mx163.baidu.com
mx164.baidu.com
123.125.66.164
mx164.baidu.com
mx165.baidu.com
123.125.66.165
mx165.baidu.com
mx170.baidu.com
123.125.66.170
mx170.baidu.com
mx171.baidu.com
123.125.66.171
mx171.baidu.com
mx172.baidu.com
123.125.66.172
mx172.baidu.com
mx173.baidu.com
123.125.66.173
mx173.baidu.com
mx174.baidu.com
123.125.66.174
mx174.baidu.com
mx175.baidu.com
123.125.66.175
mx175.baidu.com
mx180.baidu.com
123.125.66.180
mx180.baidu.com
mx181.baidu.com
123.125.66.181
mx181.baidu.com
mx191.baidu.com
123.125.66.191
mx191.baidu.com
mx192.baidu.com
123.125.66.192
mx192.baidu.com
mx193.baidu.com
123.125.66.193
mx193.baidu.com
mx194.baidu.com
123.125.66.194
mx194.baidu.com
mx2.baidu.com
61.135.163.62
mx2.baidu.com
mx20.baidu.com
111.202.115.85
mx20.baidu.com
mx200.baidu.com
123.125.66.200
mx200.baidu.com
mx201.baidu.com
123.125.66.201
mx201.baidu.com
mx202.baidu.com
123.125.66.202
mx202.baidu.com
mx204.baidu.com
123.125.66.204
mx204.baidu.com
123.125.66.205



- 2019-01-17 https://www.msreverseengineering...

  A QUICK SOLUTION TO AN UGLY REVERSE ENGINEERING PROBLEM

- 2019-01-18 https://arxiv.org/pdf/1712.02950...

  CycleGAN, a Master of Steganography.

- 2019-01-19 http://diaphora.re/

  Diaphora A Free and Open Source Program Diffing Tool

- 2019-01-20 https://github.com/hasherezade/p...

  Scans a given process. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches)

- 2019-01-21 https://googleprojectzero.blogsp...

  Taking a page from the kernel's book: A TLB issue in mremap()

- 2019-01-22 https://research.digitalinterrup...

  A Deeper Look into XSS Payloads

- 2019-01-23 https://github.com/enovella/r2fr...

  Practical examples on how to use r2frida.

- 2019-01-24 https://github.com/sharkdp/hexyl

  A command-line hex viewer

- 2019-01-25 https://salls.github.io/Linux-Ke...

  Exploiting CVE-2017-5123 with full protections. SMEP, SMAP, and the Chrome Sandbox!

- 2019-01-26 https://speakerdeck.com/retme7/t...

  The Art of Exploiting Unconventional Use-after-free Bugs in Android Kernel

- 2019-01-27 https://wbenny.github.io/2018/11...

WoW64 internals ... re-discovering Heaven's Gate on ARM

- 2019-01-28 https://0xrick.github.io/lists/s...

  Steganography - A list of useful tools and resources

- 2019-01-29 https://www.youtube.com/watch?v=...

  Setting up IDA to analyze the ARM firmware and then find the entry-point through static and dynamic analysis

- 2019-01-30 http://www.zsythink.net/archives...

  iptables 详解, 十分不错的文章, 这是目前我在中文资料里看到的最好的解释.

- 2019-01-31 https://github.com/linuxthor/uul

  ELF binary that runs on several different *nix flavours. Works out which variant it's being run on and runs code specific to that.