Internet Scanning

Current State and Lessons Learned

Mark Schloesser - Rapid7 Labs

@ BlackHat USA - August 6th 2014

$ id

- Mark Schloesser
  - Twitter @repmovsb
  - Security Researcher at Rapid7 Labs
  - Core developer for Cuckoo Sandbox
  - Research on botnets, malware
  - Lots of smaller sideprojects, dexlabs.org (Android), honeypots, protocols

Outline

- Quick Recap Internet Scanning
  - Intro / History / Motivation / Ethics / etc
- Project Sonar
- Research / Findings
- Asset discovery example use case

Large scale scanning
Internet wide data-gathering

Internet-wide scanning

- Internet Mapping Project, Bell Labs / Lumeta, 1998+
- IPv4 Census 2003-2006
- EFF SSL Observatory 2014
- Internet Census 2012 (the botnet)
- Shodan
- RIPE Atlas (slightly different)
- Critical.IO, 2012-2013
- University of Michigan
- Shadowserver
- ErrataSec (R. Graham / masscan)
- Rapid7, Project Sonar

Research / Finding history

- Top 3 UPnP software stacks contain vulnerabilities / are exploitable
  - Most widespread service on the Internet, millions of devices affected, patch rates low until today
- IPMI Server Management Protocol vulnerabilities
  - Server Management Controllers auth-bypass and other vulns
- Widespread misconfigurations
  - NTP DDoS amplification problems known since 2010
  - Open Recursors, Open SMTP relays, ElasticSearch instances, etc
- Mining Ps and Qs, UMich / UCSD
  - Weak keys used for SSL communication

WELCOME TO THE INTERNET!

SNMP – list processes, get credentials

username=sa password=Masterkey2011 LicenseCheck=Defne
DSN=sms;UID=XXX;PWD=XXXsys; DSN=GeoXXX;UID=XXX;PWD=XXXsys; 8383
password h4ve@gr8d3y
--daemon --port 8020 --socks5 --s_user Windows --s_password System
XXXX /ssh /auth=password /user=admin /passwd=admin_p@s$word
http://a.b.c/manage/retail_login.php3?ms_id=14320101&passwd=7325
a.b.c.d:3389 --user administrator --pass passw0rd123

Telnet: Router Shells

10,000+ Routers don’t even bother with passwords

```
jiuyuan_bt_nm_ah>
jiyougongsi>
jjcaisanxiaoxue>
jjda>
jjdc>
jjgd>
jjlhlianfangzhizao>
jjpzx>
jjshhshengangzhizao>
jjxjy>
jjxy>
jjxz>
jjyljuda>
jkx_sdl>
jnszy_2692>
joelsmith>
jsyh>
jt_net>
jtic>
jx123>
jzglkyzz>
kashiwa>
kbbmetro>
kd-ip>
mp1700-kslp>
mp1700E>
mp1762>
mp2600e>
mp2692>
mp2700>
msk-cat3>
mty-3500-1>
multivoice01>
mvy-rtr-01>
mx-fdc-dmz1>
mx-frtsw01>
mx-frtsw02>
nak2ama-east-ps>
nak2ama-north-ps>
nak2ama-ps>
nak2ama-south-ps>
nak2ama-west-ps>
naldi>
nanchang2621>
nanquc3550-02>
nanshigaosu_A5>
narashino>
nayana2>
telnet@AYRS-CES2k-1>
telnet@AdminVideoSW1>
telnet@BBG>
telnet@BEL-WIFI-1>
telnet@BGLWANSW01>
telnet@BGLWANSW02>
telnet@BI-RX-1>
telnet@BI-Solsi>
telnet@BIGION-CORE-1>
telnet@BR2-NET1-MLXe>
telnet@BRCD-ADX-2>
telnet@BSI01>
telnet@Backbone_Backup>
telnet@BigIron RX-4 Router>
telnet@BigIron RX-8 Router>
telnet@BigIron Router>
telnet@Bloco.A1.Core>
telnet@Bloco.B.Core>
telnet@Border40G-1>
telnet@Brocade_ABA_1>
telnet@CHD-BOU-CO-2>
telnet@CON-LONFESX4801>
telnet@CON-LONFESX4802>
S1-DNS-3560-NSGK>
```

Telnet: Windows CE Shells

3,000+ Windows CE devices drop CMD shells

```
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on ITP Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 4.20 \>
Welcome to the Windows CE Telnet Service on PicoCOM2-Sielaff Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 4.10 \>
Welcome to the Windows CE Telnet Service on G4-XRC Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on HMI_Panel Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on G4-XFC Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on PELOAD Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on MCGS Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on Db1200 Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on VEUIICE Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on Borne Cebus/Horus Pocket CMD v 6.00 \>
```

Telnet: Linux Shells

3,000+ Linux systems drop to root

```
MontaVista(R) Linux(R) Professional Edition 4.0.1 (0502020) Linux/armv5tejl
Welcome telnet root@~#
Local system time: Sun May 20 04:12:49 UTC 2012 root:#
root@(unknown):/#
root@routon-h1:/#
root@umts_spyder:/ #
root@vanquish_u:/ #
root@smi:/ #
root@dinara_cg:/ #
root@BCS5200:/#
root@edison:/ #
root@umts_yangtze:/ #
root@cdma_spyder:/ #
root@vanquish:/ #
root@scorpion_mini:/ #
root@qinara:/ #
sh-3.00#
~ #
```

Telnet: other stuff

License plate readers, on the internet, via Telnet

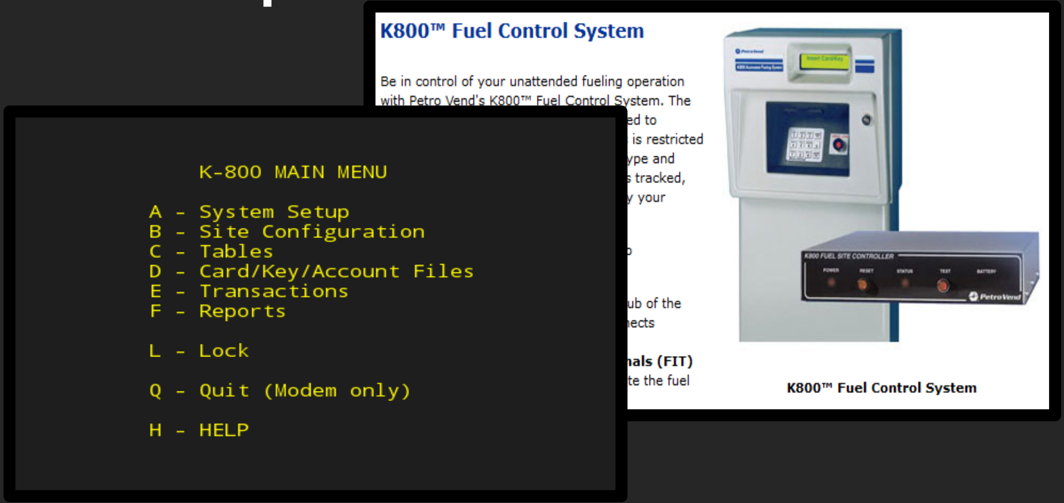
ATZ P372 application Aug 29 2008 16:07:45 P372 RAM: 128M @ 128M EPROM: 512k Flex capabilities 003f Camera firmware: 4.34 362 ANPR enabled for: USA Louisiana . Installed options: 00220018 * ... Compact Flash * ... Basic VES with no security * ... USA Licenceplate recognition * **PIPS Technology AUTOPLATE (tm) license plate recognition** * VES - (violation enforcement system)

Serial Port Servers

- Devices that make network-disabled devices into network-enabled ones.
- Doesn’t sound like a good idea…
- Most common access config (authenticated / encrypted methods available):
  - ☹ Unauthenticated clear-text TCP multiplex ports
  - ☹ Unauthenticated TCP pass-through ports

RAPID7

Example Remote Serial Ports

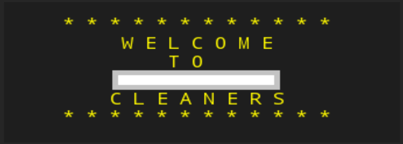


K800™ Fuel Control System

Be in control of your unattended fueling operation with Petro Vend's K800™ Fuel Control System. The ...ed to ... is restricted ...ype and ...s tracked, ...y your ...o ...ub of the ...ects ...als (FIT) ...te the fuel

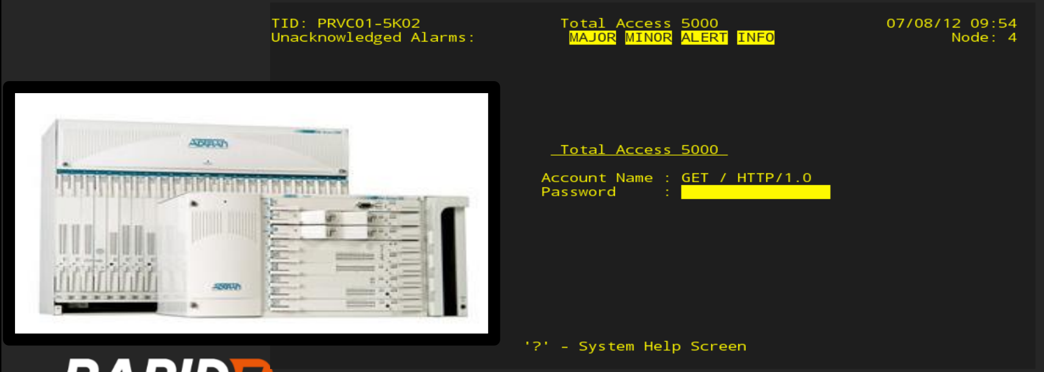
K800™ Fuel Control System

```
        K-800 MAIN MENU

    A - System Setup
    B - Site Configuration
    C - Tables
    D - Card/Key/Account Files
    E - Transactions
    F - Reports

    L - Lock

    Q - Quit (Modem only)

    H - HELP
```

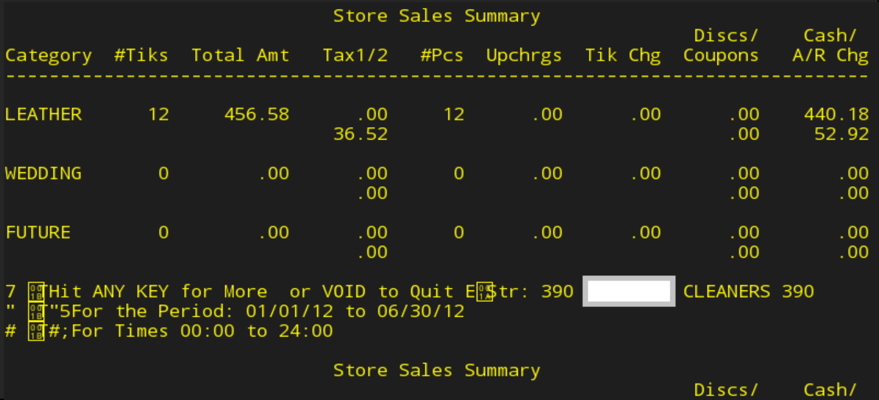


```
* * * * * * * * * * * *
      W E L C O M E
          T O
      [redacted]
    C L E A N E R S
* * * * * * * * * * * *
```

IPTV Headend system, sometimes left logged-in



```
TID: PRVC01-5K02                    Total Access 5000              07/08/12 09:54
Unacknowledged Alarms:               MAJOR MINOR ALERT INFO                 Node: 4



                                     Total Access 5000

                                   Account Name : GET / HTTP/1.0
                                   Password     :



                                '?' - System Help Screen
```



```
                          Store Sales Summary
                                                                      Discs/    Cash/
Category  #Tiks  Total Amt   Tax1/2   #Pcs  Upchrgs  Tik Chg  Coupons  A/R Chg
-------------------------------------------------------------------------------

LEATHER      12     456.58      .00     12      .00      .00      .00   440.18
                              36.52                               .00    52.92

WEDDING       0        .00      .00      0      .00      .00      .00      .00
                                .00                               .00      .00

FUTURE        0        .00      .00      0      .00      .00      .00      .00
                                .00                               .00      .00

7 ▯Hit ANY KEY for More  or VOID to Quit E▯$tr: 390 [redacted] CLEANERS 390
" ▯"5For the Period: 01/01/12 to 06/30/12
# ▯#;For Times 00:00 to 24:00

                          Store Sales Summary
                                                                      Discs/    Cash/
```

ElasticSearch, code execution is a feature

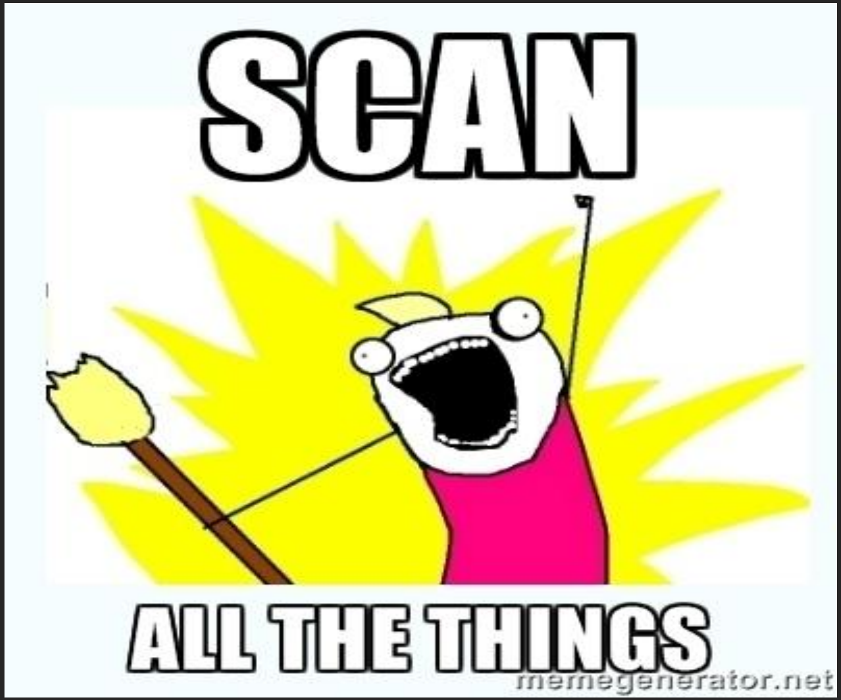
- By default allows “dynamic scripting”, executing code on the server
- Not a vulnerability, just misconfiguration when served on a public IP without filtering/protection

- Of course not the only example, see MongoDB, and all other SQL DBs without auth or default credentials

Finding issues and raising awareness about them is immensely valuable.

Rapid7 Labs starts *Project Sonar*

(announced by HD at Derbycon 2013)



Sonar – Data overview

- 443/TCP - SSL Certificates
- 80/TCP – HTTP GET / (IP vhost)
- Reverse DNS (PTR records)
- Forward DNS (A/AAAA/ANY lookups)
- Other SSL certificate sources, STARTTLS, etc

- Several UDP probes
  - UPnP, IPMI, NTP, NetBios, MDNS, MSSQL, Portmap, SIP, etc

Sonar – Data sizes and record counts

- 443/TCP - SSL Certificates – weekly
  - ~40M open ports, ~25M SSL certs, ~55GB in < 4 hours
- 80/TCP – HTTP GET / (IP vhost) - bi-weekly
  - ~70M open ports, average ~3.5Kb each, ~220GB in < 10 hours
- Reverse DNS (PTR records) – bi-weekly
  - ~1.1 Billion records, ~50GB in < 24 hours
- HTTP GET / (name vhost)
  - ~ 1.5 TB for ~200M names

- Running since November 2013 (roughly)

Recent findings – NAT-PMP

- Network Address Translation Port Mapping Protocol
  - Maintains port-mappings on NAT devices, typically expected to exposed to the inside of a NAT-network
  - Over 1 Million exposed on public addresses on the Internet
  - Either deployed incorrectly, or, more likely, suffer from one or more vulnerabilities in their respective NAT-PMP (or other) implementation
  - Functionality allows control of inbound and outbound traffic rules on a NAT device

Recent findings – MSSQL

- UDP/1434 – yields metadata about the database server
  - The most frequently observed version of MSSQL was 2005.sp4, nearly 9 years old
  - Over 25,000 machines running MSSQL 2000, well over 10 years old

Version	# hosts	CVEs (VDB)
2005.sp4	42092	CVE-2011-1280 CVE-2012-0158 CVE-2012-1856 CVE-2012-2552
2008.r2	38708	CVE-2011-1280 CVE-2012-0158 CVE-2012-1856
2000.Rtm	27700	CVE-2003-0230 CVE-2003-0231 CVE-2003-0232 CVE-2008-4110 CVE-2008-5416
2008.r2 sp1	15245	CVE-2012-1856 CVE-2012-2552
etc	etc	etc

Recent findings – DNS

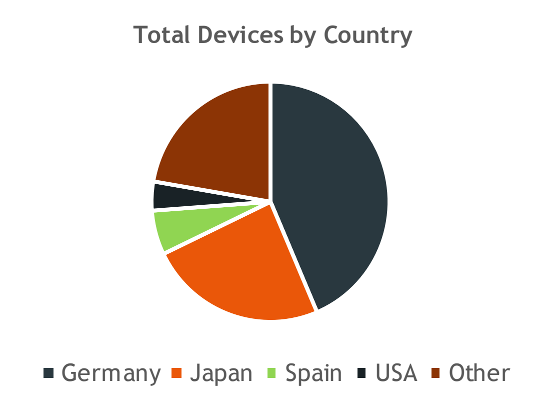
- DNS “ANY” lookups against ~800m hostnames
  - Basically a somewhat random sampling of DNS records used in the wild
  - Nothing too problematic found, odd configurations, a parser bug, etc

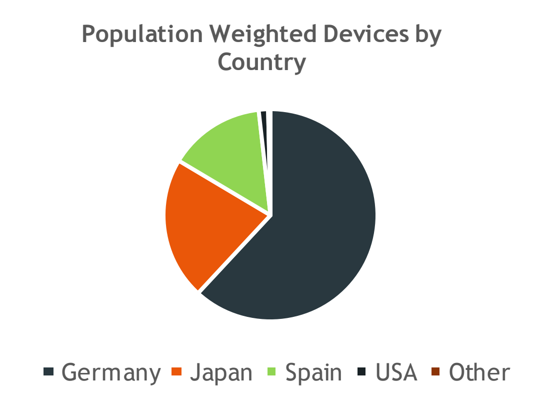
```
canireally.com,SRV,10 5 5060 sipserver.example.com
nashastrojka.ru,SRV,0 20 0 5222
pc-instruct.admin.mcmaster.ca,WKS,130.113.35.44,tcp telnet smtp 26 27
phil.uni-hannover.de,ISDN,"495117628311"
ncmmlin222.uio.no,HINFO,"IBM-PC","LINUX"
formacioncpa1.cpa.uam.es,HINFO,"PC","MS-WINDOWS-98"
66008585.com,HINFO,"Intel Pentium 133Mhz","Unix"
om240.ap.stolaf.edu,MB,D8C7C8CDBE96.ap.stolaf.edu.
aisys.co.il,MR,mail.aisys.co.il.
a2epc11.ens.fr,LOC,48 50 29.000 N 02 20 44.000 E 69m 100m 100m 10m
6283.ch,LOC,47 09 7.000 N 08 25 30.000 E 489m 1m 10000m 10m
aboc.com.au,LOC,37 48 15.000 S 144 59 14.000 E 30m 1m 10000m 10m
```

```
577465372 rtype_A
373934374 rtype_NS
218168613 rtype_MX
165939348 rtype_SOA
 53208892 rtype_TXT
 20291406 rtype_CNAME
 16680380 rtype_RRSIG
  7335137 rtype_AAAA
  5594760 rtype_NSEC
  3253593 rtype_DNSKEY
  1621625 rtype_PTR
  1098725 rtype_DS
   785770 rtype_NSEC3PARAM
   747874 rtype_HINFO
   700267 rtype_SPF
   115813 rtype_RP
    94949 rtype_LOC
    34966 rtype_NAPTR
    24000 rtype_SRV
    21799 rtype_SSHFP
          …
```

Recent findings – SIP / VoIP

- SIP OPTIONS query against UDP 5060
  - 14.5 Million responses
  - Most responses from Germany and Japan, followed by Japan, Spain, USA
  - Germany mostly "Speedport" and AVM "Fritz!Box"
  - Spain – "Orange LiveBox DSL Router"
  - Vulnerability analysis still ongoing, initial results indicate widespread use of outdated SIP implementations…





Other recent findings – in disclosure process

- More problems related to traffic amplification found in NTP
  - Not as bad as MONLIST, but still needs fixing
- RCE on more Network DVR devices
  - Metasploit module coming after disclosure, >100k devices exposed
- Some fallout from previous Supermicro / IPMI / BMC publications (still giving away root…)

Example Use-Case Asset Discovery

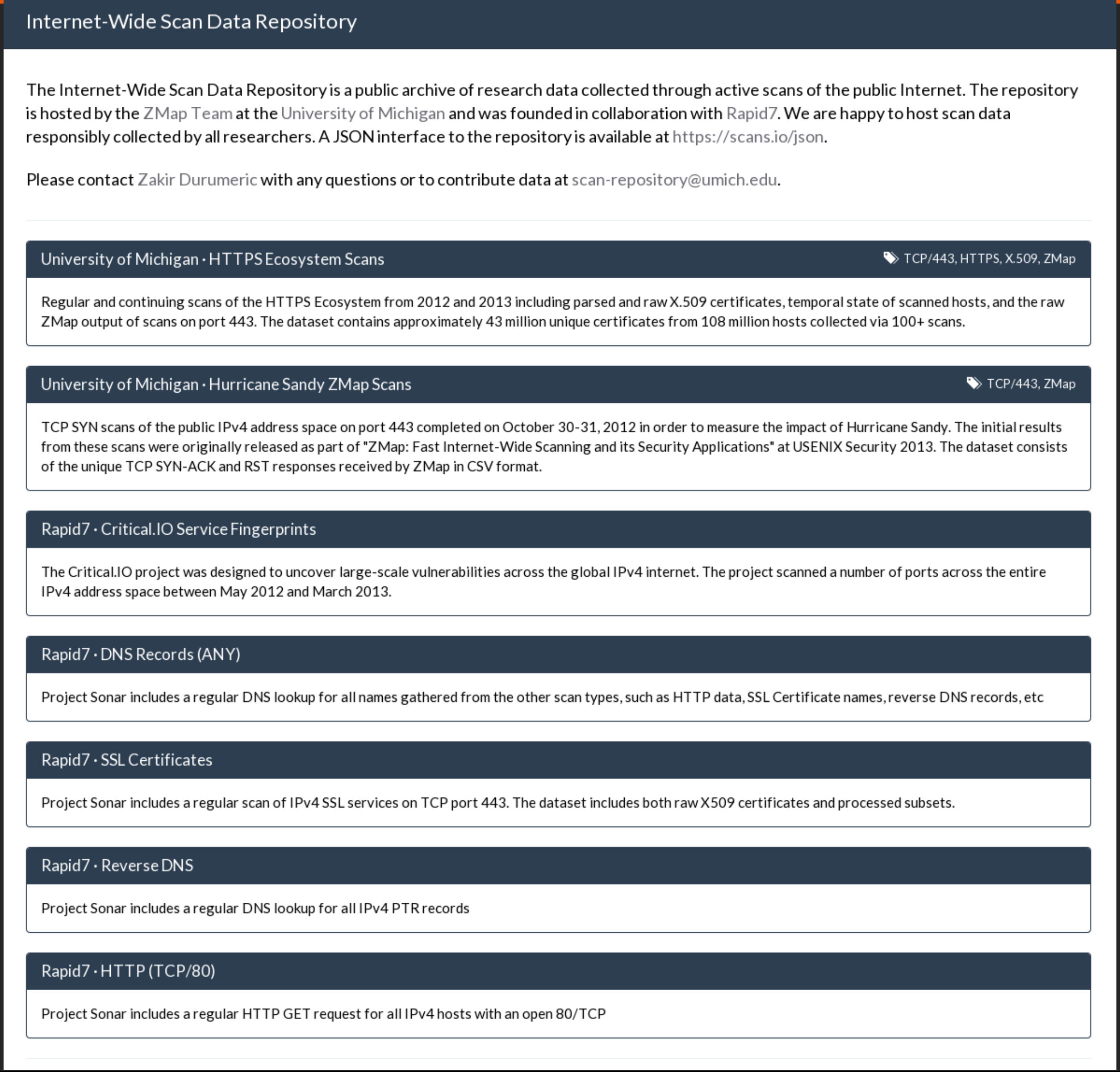
- Use scanning data to build lookup databases for IPs and names
- Start with an array of domain names and CIDRs and generate a report of associated assets / relevant data

- Quick Livedemo for Rapid7

Collaboration is highly important

- Make data available to the Security community
  - Collaboration with University of Michigan
  - Raw Scan data published at http://scans.io/
- Historical upload (critical.io, Michigan data)
- Almost-real-time upload of raw scan output

http://scans.io/



Internet-Wide Scan Data Repository

The Internet-Wide Scan Data Repository is a public archive of research data collected through active scans of the public Internet. The repository is hosted by the ZMap Team at the University of Michigan and was founded in collaboration with Rapid7. We are happy to host scan data responsibly collected by all researchers. A JSON interface to the repository is available at https://scans.io/json.

Please contact Zakir Durumeric with any questions or to contribute data at scan-repository@umich.edu.

University of Michigan · HTTPS Ecosystem Scans — TCP/443, HTTPS, X.509, ZMap

Regular and continuing scans of the HTTPS Ecosystem from 2012 and 2013 including parsed and raw X.509 certificates, temporal state of scanned hosts, and the raw ZMap output of scans on port 443. The dataset contains approximately 43 million unique certificates from 108 million hosts collected via 100+ scans.

University of Michigan · Hurricane Sandy ZMap Scans — TCP/443, ZMap

TCP SYN scans of the public IPv4 address space on port 443 completed on October 30-31, 2012 in order to measure the impact of Hurricane Sandy. The initial results from these scans were originally released as part of "ZMap: Fast Internet-Wide Scanning and its Security Applications" at USENIX Security 2013. The dataset consists of the unique TCP SYN-ACK and RST responses received by ZMap in CSV format.

Rapid7 · Critical.IO Service Fingerprints

The Critical.IO project was designed to uncover large-scale vulnerabilities across the global IPv4 internet. The project scanned a number of ports across the entire IPv4 address space between May 2012 and March 2013.

Rapid7 · DNS Records (ANY)

Project Sonar includes a regular DNS lookup for all names gathered from the other scan types, such as HTTP data, SSL Certificate names, reverse DNS records, etc

Rapid7 · SSL Certificates

Project Sonar includes a regular scan of IPv4 SSL services on TCP port 443. The dataset includes both raw X509 certificates and processed subsets.

Rapid7 · Reverse DNS

Project Sonar includes a regular DNS lookup for all IPv4 PTR records

Rapid7 · HTTP (TCP/80)

Project Sonar includes a regular HTTP GET request for all IPv4 hosts with an open 80/TCP

RAPID7

The Internet is broken.

- Widespread bugs, vulnerabilities, misconfigurations
- Weak credentials
- Lost and forgotten devices, embedded hardware piling up without update possibilities
- We’re not improving the overall “state of security”

Moving forward

- Can’t stress enough the importance of awareness and visibility
- Internet scanning is a powerful tool that can do a lot of good for the community
  - Identify / quantify vulnerabilities, build awareness before they are misused
  - Measure improvements continuously
- Collaboration is essential for data collection and analysis

Make sure to also check out

- ZMap at http://zmap.io/
  - ZMap Best Practices https://zmap.io/documentation.html#bestpractices
- J. Alex Halderman on “*Fast Internet-wide Scanning and its Security Applications*” at 30C3 (Germany)
- HD Moore’s keynote “*Scanning Darkly*” at Derbycon 2013
- http://sonar.labs.rapid7.com/

RAPID7

Thanks!

Rapid7 Labs

Mark Schloesser

mark_schloesser@rapid7.com

@repmovsb