RAPID7

INTERNET SCANNING

Research on 0/0

hack.lu, Oct 23, 2014 – good to be back ☺

$ 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 (Honeynet Project), custom protocols

LARGE SCALE PORT-SCANNING, INTERNET WIDE DATA-GATHERING

Related work

- Internet-wide studies since 1998, research-focused mostly
- Most active nowadays are
  - Shodan
  - Shadowserver
  - University of Michigan
  - Erratasec
- Interesting case: Internet Census 2012

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 with arguments

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

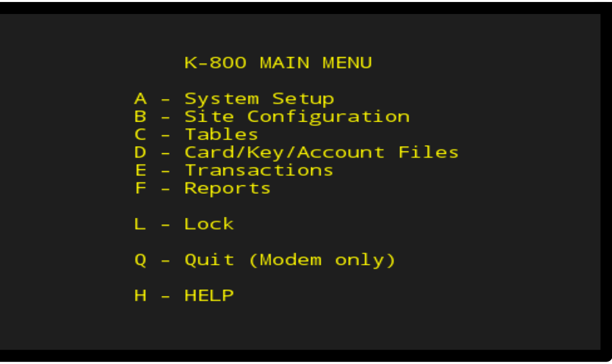
License plate readers, on the internet, via Telnet

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)

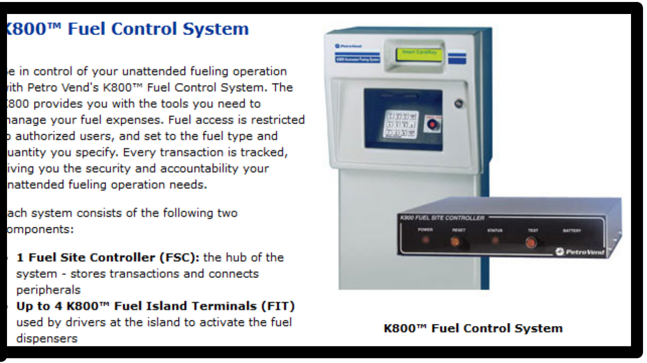
Serial Port Servers

- 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

Example Remote Serial Ports



```
        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
```



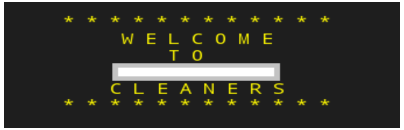
K800™ Fuel Control System

e in control of your unattended fueling operation
ith Petro Vend's K800™ Fuel Control System. The
800 provides you with the tools you need to
anage your fuel expenses. Fuel access is restricted
o authorized users, and set to the fuel type and
uantity you specify. Every transaction is tracked,
iving you the security and accountability your
nattended fueling operation needs.

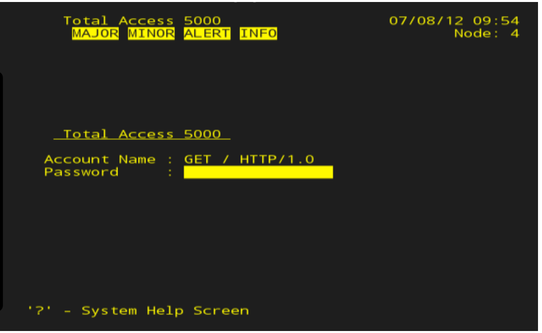
ach system consists of the following two
omponents:

- **1 Fuel Site Controller (FSC):** the hub of the system - stores transactions and connects peripherals
- **Up to 4 K800™ Fuel Island Terminals (FIT)** used by drivers at the island to activate the fuel dispensers

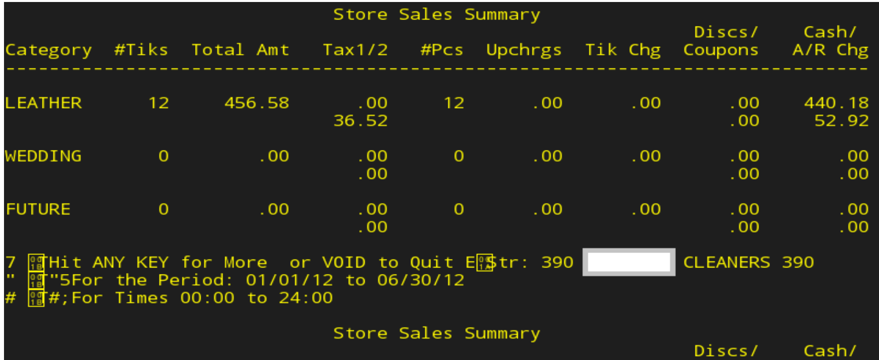
K800™ Fuel Control System



```
* * * * * * * * * * * *
     W E L C O M E
         T O

   C L E A N E R S
* * * * * * * * * * * *
```



```
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 EStr: 390           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 collection overview

- 443/TCP - SSL Certificates – weekly
  - ~40M open ports, ~25M SSL certs, ~55GB in < 4 hours
  - Other SSL certificate sources, STARTTLS, etc
- 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
- Forward DNS (A/AAAA/ANY lookups)
- HTTP GET / (name vhost)
  - ~ 1.5 TB for ~200M names
- Several UDP probes
  - UPnP, IPMI, NTP, NetBios, MDNS, MSSQL, Portmap, SIP, etc

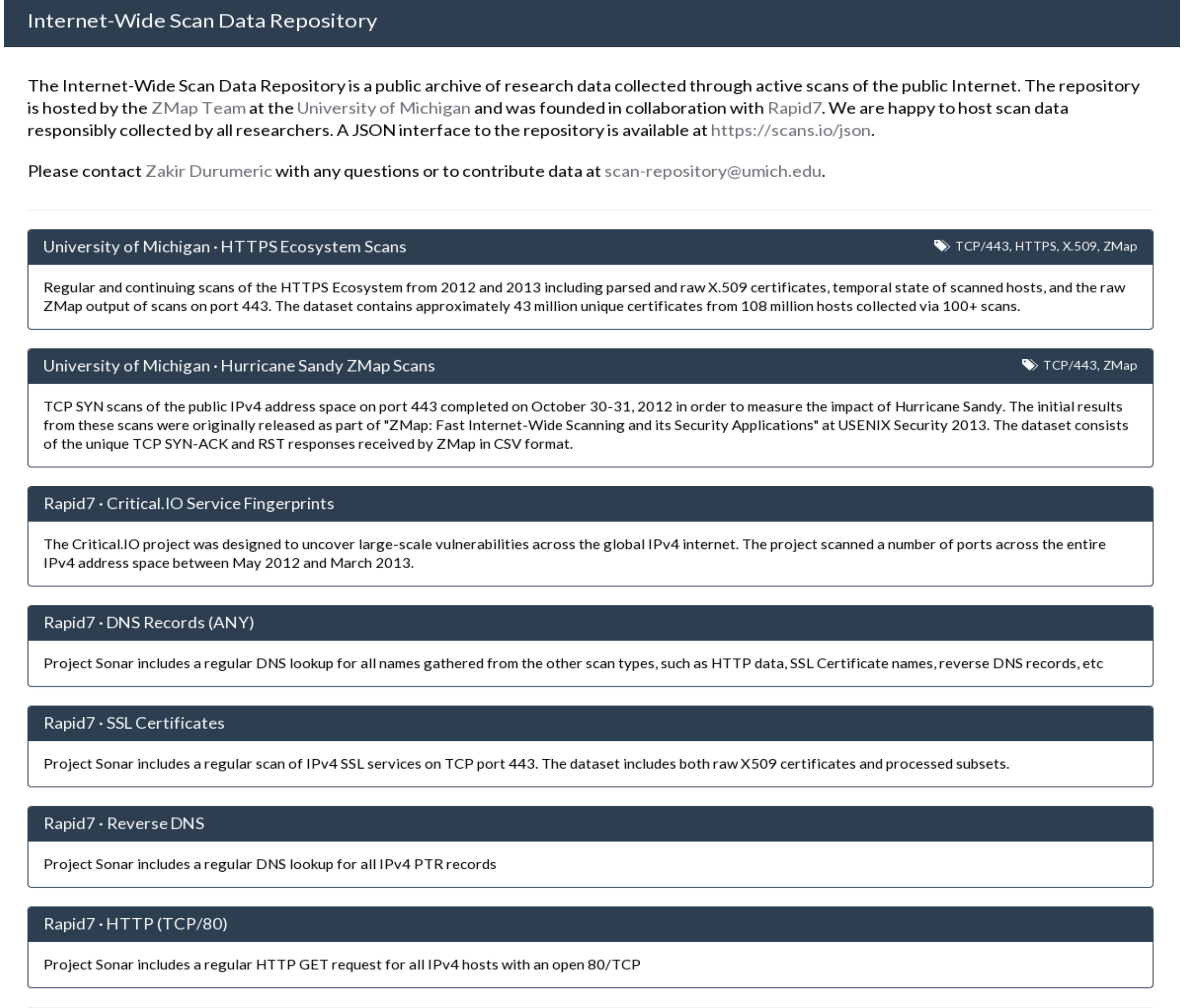
Recent findings, random selection

- NAT-PMP issues / misconfigurations
  - >1M public IPs
- MSSQL, vulnerable never-patched deployments
  - ~50k run 2005.sp4 (9 years old), >25k run 2000.xyz (over 10y old)
- DNS, parser issues, weird in-the-wild records and types
  - URI record type, lots of GPS records, HINFO (`"Intel Pentium 133Mhz","Unix“`)
- SIP / VoIP, very widespread in some countries, outdated libraries
- NTP, more amplification problems
- More RCE on $random_vendor embedded device, over 100k on public IPs

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)
- Near-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

THE INTERNET IS BROKEN

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”

Going 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