Janet CSIRT

John Green
2 June 2015

Janet CSIRT

- Established in 1993 (Janet CERT)
- Team of 6
- Nominated security at each customer organisation

- Email irt@csirt.ja.net
- Telephone 0300 999 2340
- Available 0800-1800 Weekdays
- Oncall
  - 1800-0000 Weekdays
  - 0900-1700 Weekend

Janet CSIRT

- AS786
- Member of FIRST
- Accredited by Trusted Introducer
- Two distinct functions
  - Abuse handling
  - Incident coordination

Abuse Handling

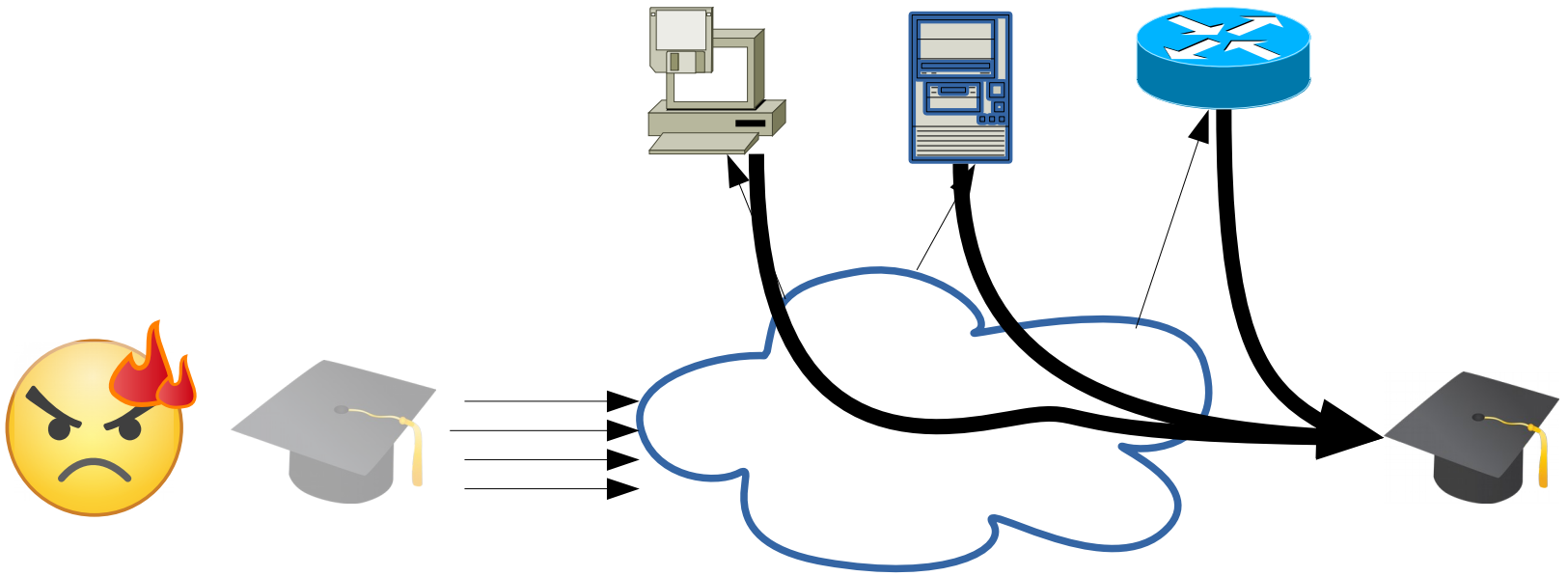
- Reports of abuse originating from Janet
  - Unsolicited Bulk Email
  - Abusive/malicious communications
  - Requests from law enforcement
  - Reports of malware infections
  - Misconfigured devices
  - Copyright complaints

Incident Coordination

- Incidents targeting Janet
  - Denial of Service
  - Phishing
  - Targeted attacks
  - UK-Security mailing list
  - Advice and support
  - Annual conference

UDP Reflection

- UDP where a request can generate large reply
- Attacker spoof requests from target



Amplification

- Typical amplification rates
  - NTP x500
  - SSDP x30
  - DNS x30-x60
  - Chargen x350
  - SNMP x6
- Others protocols include
  - QOTD, NetBios, Quake, Steam, BitTorrent...

NTP

- Mode 7 (monlist)
  - Largest amplification
  - ntpdc -n -c monlist 192.168.1.1
- Mode 6 (readvar)
  - 14:56:44 IP client.41496 > server.ntp: NTPv2, Reserved, length 12
  - 14:56:44IP server.ntp > client.41496: NTPv2, Reserved, length 228
  - Also information disclosure
  - ntpq -c rv 192.168.1.1

SSDP

- Used for UPnP
- HTTP like protocol over UDP
- Used by
  - Printers
  - NAS
  - IP Cameras
  - TV

DNS

- Open resolvers
  - Large domain for maximum amplification
  - Sometimes crafted (TXT) or DNSSEC
  - dig @192.168.1.1 large.domain ANY
- Upward referrals
  - 28 byte query (dig @ip . ns)
  - 472 byte response (a-m.root-servers.net)

SNMP

- Simple Network Management Protocol
- *GetBulk* with default community strings
- Used by
  - Networking equipment
  - PDU
  - Printers
  - Video conferencing
- snmpwalk -c public -v 1 192.168.1.1
- snmpbulkget

Fixing

- General
  - Access control
  - Patching
  - Configuration hardening
  - Network monitoring
  - BCP38 and BCP84
- Common problems
  - Outsourcing
  - Legacy equipment

Statistics

- Generally successfully at hardening Janet

Protocol	March 2014	June 2015
NTP Monitor	40	5
NTP Readvar	6500	480
SNMP	420	80
DNS Openresolver	225	75
SSDP	360	230

But...

Protocol	March 2014	June 2015
NTP	4.7M	4.5M
SNMP	8.0M	5.2M
DNS Openresolver	25M	17M
SSDP	19M	13M

As a service

- Not everyone is as conscientious

  “"example.com is the best ip stresser/booter money can buy. I have had a lifetime account with them for the past year and they have been nothing but great! All the other booter and ipstresser sites are always down or without power. Network stresser doesn't have that problem because their staff is dedicated to providing a good service. They are easily the strongest booter that i have ever used!"”

Mitigation

- Typically easy to block...
- Once characterised
- DNS most problematic
- Policers and rate limiting for long term defence

Flow data

- Originally developed by Cisco
- Represents unidirectional traffic flow
  - in/out interface
  - source/destination IP
  - protocol
  - source/destination port
  - octets
  - packets
  - start/end time
  - TCP flags

Netflow

- Exported by routers
- Or generated by software flow meters
- Versions
  - 5 (IPv4 only)
  - 9 (template based)
  - IPFIX
- Collected at
  - Customer Edge
  - Transit Routers

Collectors

- Many tools available
  - Flowtools
  - Nfsen
  - Silk
- Considerations
  - Data volumes
  - Majority of flows are not of interest

Silk

- Developed by Network Situational Awareness (NetSA) group at CMU
- Packs flows based on criteria
  - in/out interface
  - source/destination IP
  - ports (web vs non-web)
  - start time
- Written in C with Python API

Storage Structure

- in
  - 2015
    - 06
      - 02
        - in-servers_20150602.01
        - in-servers_20150602.02
        - in-finance_20150602.01
        - ...
- int2int
- inweb
- out
- outnull
- outweb

WHERE

- Selection
  - type
  - sensor
  - start-date/end-date
- Partitioning
  - saddress/daddress/any-address
  - stime/etime/active-time
  - sport/dport/aport
  - protocol

rwfilter

rwfilter –sensors=ORG1234 --start-date=2015/06/02:11 --end-date=2015/06/02:13 --type=in

--proto=17 --dcidr=192.168.0.0/16 --port=0,19,53,123,1900

--pass=-

SELECT

```
rwcut --fields=stime,etime,sip,sport,dip,dport
--num-recs=10
```

GROUP BY / LIMIT

rwstats --fields=sport,dip --count 20 --bytes

ORDER BY

rwsort --fields=stime

COUNT

rwcount --bin-size=60

Pipeline

```
rwfilter --sensors=ORG1234 --start-date=2015/06/02:02 --end-
date=2015/06/02:06 --type=in --proto=17 --sport=0,19,53,123,161,1900 |
rwstats -fields=sport,dip --count 20 --bytes


INPUT: 1884897 Records for 114 Bins and 22300163960 Total Bytes
OUTPUT: Top 5 Bins by Bytes
sPort|            dIP|               Bytes|    %Bytes|   cumul_%|
    0|  212.219.x.2|        11380198049| 51.031903| 51.031903|
 1900|  212.219.x.2|         7180902108| 32.201118| 83.233021|
   53|  212.219.x.2|         3530706443| 15.832648| 99.065669|
   19|  212.219.x.2|          207245539|  0.929345| 99.995014|
  123|  212.219.x.2|             479332|  0.002149| 99.997164|
```

Or

```
rwfilter --sensors=ORG1234,ORG2345 --start-
date=2015/06/02:09 --end-date=2015/06/02:12
--type=in,inweb --daddress=192.168.1.1
--pass=- | rwfilter --input-pipe=-
--sport=80,443 --sipset=trusted.set --fail=- |
rwsort --fields=bytes | rwcut --num-recs=3
--fields=sip,sport,dport,bytes,flags,stime,dur
ation
           sIP|sPort|dPort|     bytes|   flags|                  sTime|
duration|
  185.2.x.147|   80|12676| 255195479|   PA   |2015/05/16T04:46:50.930| 1022.080|
  37.77.x.117|   80|62683| 244325200| S PA   |2015/05/16T04:07:49.992|  981.024|
  185.2.x.147|   80|61166| 242522541| S PA   |2015/05/16T04:46:50.930| 1022.144|
```

Alternatives

- Bro IDS
  - Adds application layer metadata
  - Who downloaded file with the hash?
  - Who visited SSL website with self signed cert?
  - Who received an email with a ZIP attachment?
  - Support for GridFTP

Alternatives

- Logstash
  - Parses log messages
  - Elasticsearch
  - Kibana
  - ELK stack
- Apache Spark etc

?