http://hdl.handle.net/2022/21736

SECURITY RISK ASSESSMENT OF THE R&E NETWORK

Paul Howell
Chief Cyberinfrastructure Security Officer
phowell@internet2.edu

BACKGROUND

- In 2013, Internet2 leadership and board of trustees were concerned by the increasing sophistication of attacks
- Internet2 did not have a security program in place designed to defend the national R&E network from attack
- Many NRENs do not have mature security programs in place
- In early 2014, Internet2 created the role of Chief Cyberinfrastructure Security officer to develop and lead a security program that would protect the national R&E network and its members

SECURITY RISK ASSESSMENT APPROACH

1. Gathered information
   - NIST SP 800-53 Security & Privacy Controls – Moderate (268 questions)
   - Technical interviews of engineers
   - Reviewed logs, policies, configurations, visited PoPs, Internet2 and Level3 NOCs
2. Identified threats and vulnerabilities
3. Analyzed risks and proposed corrective actions
4. Presented findings to leadership for decisions
5. Began implementation of improvements

THREATS

Threat Actors

- Nation States
- Criminals
- Disgruntled Insiders
- Vandals

Capabilities

- Targeting & Ops Design
  - Open source
  - Social engineering
- Network penetration
  - Known exploits
  - 0-day exploits
  - Phishing and water-holes
- Data Collection
  - High Bandwidth collection and exfiltration
  - Close access collection
- Physical penetration operations
- Insider compromise
- Supply chain manipulation
- Remote control devices

Cause effects from outside

•Damage reputation
•Access content
•Disrupt / degrade bandwidth on demand
•Redirect traffic path on demand
•Steal bandwidth
•Weaponize infrastructure

Cause effects as a subscriber

•Access core content
•Degrade or interrupt core on demand

Threat Motivation

Compromise Confidentiality

- Nation State (high)
- Criminals (med)
- Disgruntled Insiders (med)
- Vandals (low)

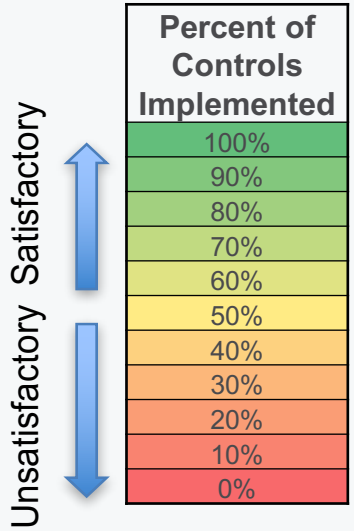
Compromise Availability

- Nation States (high)
- Criminals (med)
- Disgruntled Insiders (med)
- Vandals (med)

BASELINE SECURITY ASSESSMENT FINDINGS

- Current security practices would not resist intentional targeting and exploitation by well-resourced and determined adversarial threats
- It is likely that such a threat would be able to successfully compromise both the confidentiality and availability of the network
- Current security practices were primarily designed to address human error, environmental hazards, and to enable rapid recovery and reconstitution of services
- Security practices have evolved organically, are not formally stated, documented, shared or monitored throughout the enterprise
  - The lack of a formal security program introduces opportunities for significant exploitable gaps in protection
- Inadequate protection of the management network is the most exploitable vulnerability discovered during the assessment

High Threat Potential	Initial	Current	Target
Security Assessment and Authorization			
Security Planning and Privacy Impact			
Risk Assessment			
Audit and Accountability			
Incident Response			
Identification and Authentication			
Medium Threat Potential			
System, Communications and Availability Protection			
System and Information Integrity			
Access Control			
Awareness and Training			
Physical and Environmental Protection			
Low Threat Potential			
Configuration Management			
Contingency Planning			
Maintenance			
Media Protection			
Personnel Security			
System and Services Acquisition			



Ref: NIST SP 800-53

SHORT TERM IMPROVEMENTS

- Reduced the number of staff from 100 to 28 that have administrative privileges to network systems (routers/switches/controllers)
- Improved user authentication by using two-factor authentication on the network systems (routers/ switches/controllers)
- Removed operationally sensitive information (e.g., IP addresses of AuthN servers) from public view
- Designed an out-of-band secure management network
- Dedicated security team formed
- Developed security operations capabilities including security log analysis

SHORT TERM IMPROVEMENTS CONTINUED

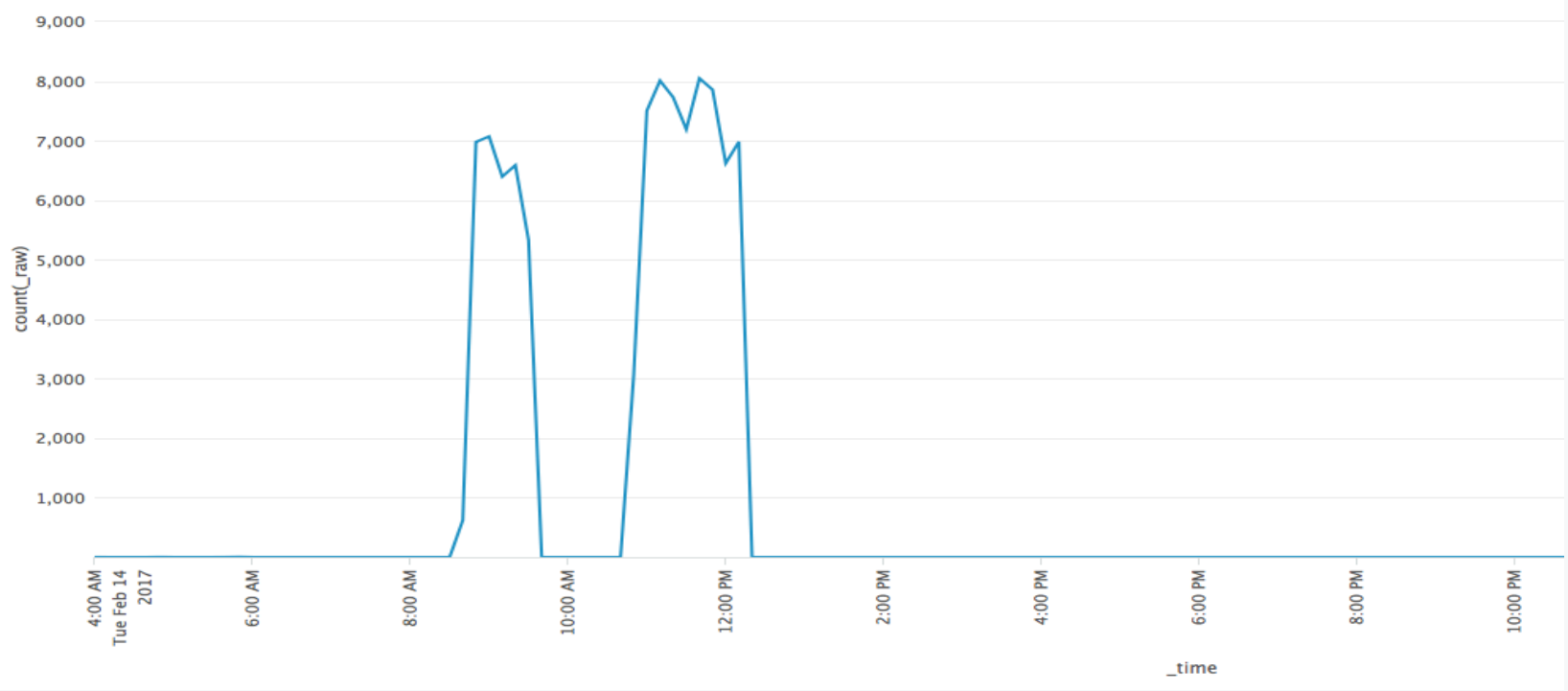
- Developed quarterly procedure to review ACLs for in-band management and removed over half of stale entries during the first review
- Credentialed scanning of NOC servers and core packet forwarding systems (i.e., routers and switches)
- Consistent ticketing of DDoS attacks as security tickets
- ARP spoof monitoring in public exchanges
- Incident response procedure implemented

LONG TERM IMPROVEMENTS

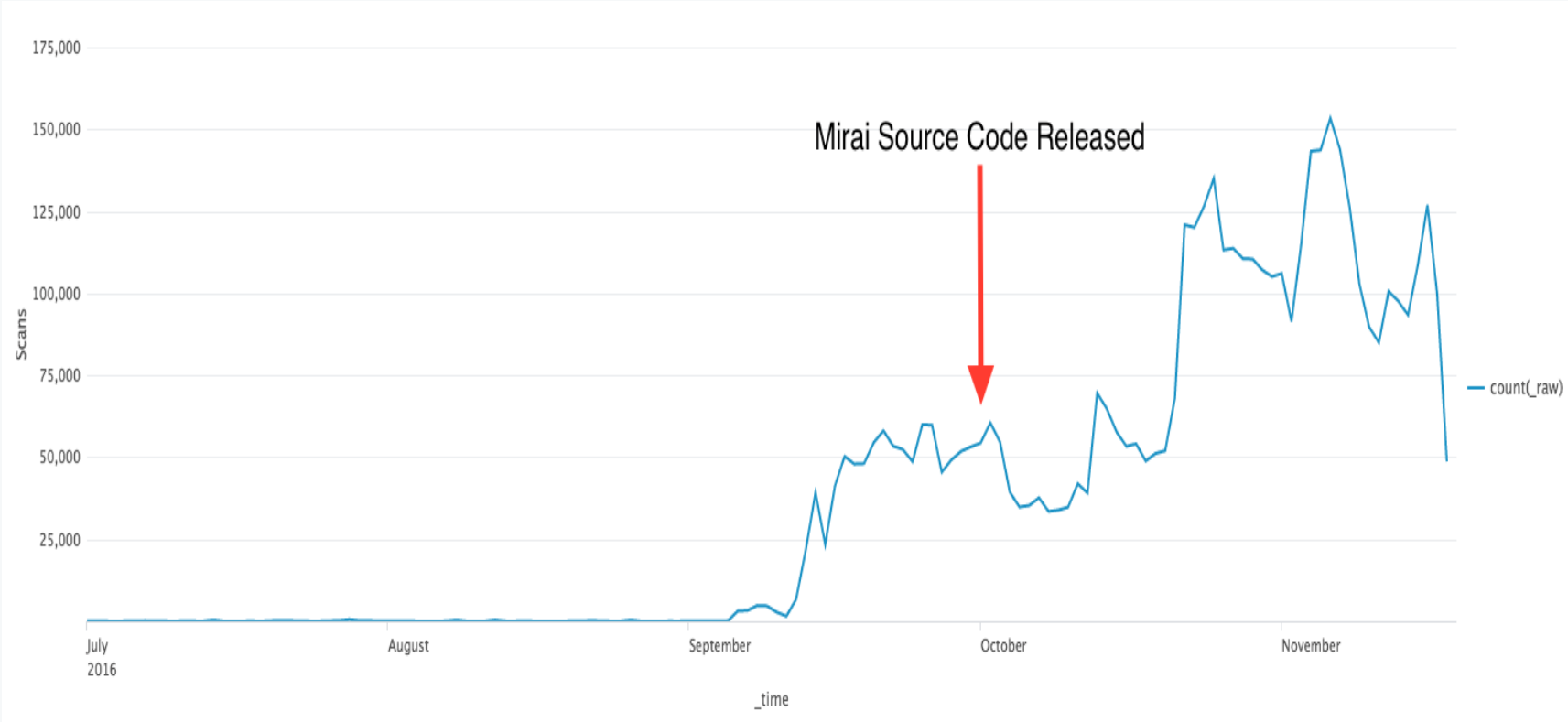
- Security awareness education for staff based on SANS Securing the Human
- Periodic security assessments performed
- Implementation of out-of-band secure management network
- Promote adoption of improved routing security methods (e.g., GTSM, RPKI, BCP38)
- Improve physical security at physical sites
- DDoS mitigation (strategy at http://www.internet2.edu/blogs/detail/12234)
  - Commercial scrubbing services
  - Flowspec
  - RTBH

NTP REFLECTION DOS ATTACK FROM A MISCONFIGURED ROUTER

xntpd[21521]: sendto(<Target IP>): No route to host
xntpd[21521]: too many recvbufs allocated (40)



MIRAI PORT SCANNING SCANNING



IPV4 DISCARDS BY SOURCE ASN AND DEST PORT

✓ 658,549 events (4/20/17 12:00:00.000 PM to 4/21/17 12:38:39.000 PM)

Job | Fast Mode

Events | Patterns | Statistics (10,000) | Visualization

100 Per Page | Format | Preview

< Prev 1 2 3 4 5 6 7 8 9 ... Next >

src_asn	src_country	dstport	sparkline	count
AS4134 Chinanet	China	443		54013
AS87 Indiana University	United States	22		20895
AS4538 China Education and Research Network Center	China	443		17905
AS4837 CNCGROUP China169 Backbone	China	443		14307
AS4808 China Unicom Beijing Province Network	China	443		10834
AS4812 China Telecom (Group)	China	443		8634
AS4134 Chinanet	China	23		7858
AS28719 PJSC Rostelecom	Russian Federation	23		7477
AS4847 China Networks Inter-Exchange	China	443		6052
AS12389 PJSC Rostelecom	Russian Federation	23		5985
AS4134 Chinanet	China	1433		5658
AS6828 PJSC Rostelecom	Russian Federation	23		5476
AS20115 Charter Communications	United States	443		5144
AS5786 University of Puerto Rico	Puerto Rico	161		4786
AS3462 Data Communication Business Group	Taiwan	23		4354
AS7497 Computer Network Information Center	China	443		4191
AS9808 Guangdong Mobile Communication Co.Ltd.	China	443		3424
AS4134 Chinanet	China	81		3412
AS4766 Korea Telecom	Korea, Republic of	23		3183
AS33302 Data 102, LLC	United States	80		2958
AS9121 Turk Telekom	Turkey	23		2769
AS28573 CLARO S.A.	Brazil	23		2745

DISCARDS MINUS DNS, BFD, BGP