M3AAWG
MESSAGING MALWARE MOBILE

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

M³AAWG
MESSAGING MALWARE MOBILE

M³AAWG Training Video Series

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

(more than 2.25 hours of training)

This is Segment 1 of 6

The complete series is available at: https://www.m3aawg.org/activities/maawg-training-series-videos

Segment 1 **Top SP Security Essential Techniques** **(about 20 minutes)**	**Segment 2** **Types of Malware Problems ISPs Encounter** **(about 20 minutes)**	**Segment 3** **Understanding the Threat:** **A Cyber-Criminal's Work Day & Cyber-Criminal Behavior Drivers** **(about 30 minutes)**
Segment 4 **Turning Point** **(about 12 minutes)**	**Segment 5** **Remediating Violated Customers** **(about 35 minutes)**	**Segment 6** **U.S. FCC's Anti-Botnet Code of Conduct (ABCs for ISPs)** **Overview &** **Code on a Shoestring Budget** **(about 20 minutes)**

Top SP Security Essential Techniques

Segment 1 of 6

Barry Raveendran Greene, bgreene@senki.org

October 22, 2012, Baltimore, Maryland, USA

Barry Greene has over 30 years industry experience including having served as president of the ISC (Internet Systems Consortium). He is a pioneer in service provider security and operational security reaction teams.

Barry is currently a participant on the U.S. Federal Communications Commission's (FCC's) Communications Security, Reliability and Interoperability Council (CSRIC).

SP Security Primer 101

Peers working together to battle
Attacks to the Net

Barry Raveendran Greene
bgreene@senki.org

Goals

- Provide core techniques/task that any SP can do to improve their resistance to security issues.
- These core techniques can be done on any core routing vendor's equipment.
- Each of these techniques have proven to make a difference.

- New Drivers: New levels of security capability are being expected from Service Providers.
- Australia's I-code, FCC's CSRIC, expectations from the cyber-civic society and successful take downs are shaping these expectations.

“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Agenda

- Overview
- Understanding the Threat: *A Typical Cyber-Criminal's Work Day*
- Why Cyber-Crime is Institutionalized?
- A 2012 SP Security Strategy for Action
- Top 10 SP Security Techniques: The Executive Summary
  - Prepare your NOC
  - The New Internet "Civic Society": OPSEC Communities
  - Working with your Peers with "Out of Band" Communications: iNOC DBA
  - Point Protection
  - Edge Protection
  - Remote Trigger Black Hole
  - Sink Holes
  - Source Address Validation
  - Control Plane Protection
  - Total Visibility
- (cont_)

Agenda

- Prepare your NOC
- Operational Security Community
- Putting the Tools to Work – DDOS Attack
- Remote Triggered Black Hole Routing
- Sink Holes
- Remediating Violated Customers
- Summary

Expectations

- Today’s tutorial is about the fundamentals for which new solutions and technique can be built.
- Everything cannot be covered today (more than a week’s worth of materials).
- We cannot go in-depth on everything.

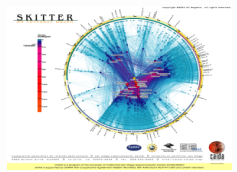
Invitation to Participate

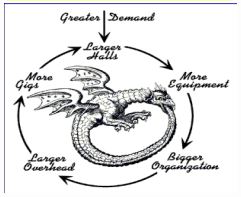
- The current materials are based on the contributions of many people from the industry. Cisco, Juniper, Arbor Networks, and many of the largest SPs in the industry have all been generous to add to the volume of materials.

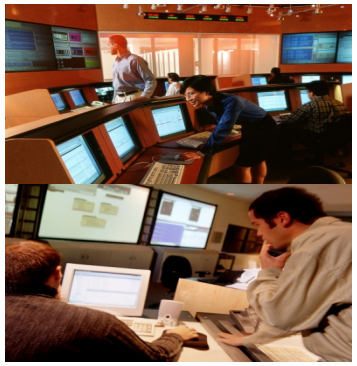
- The materials require refreshing.

- ***Invitation: If you are really interested in the security and resiliency of your network, please join the community who are working to craft and deploy the foundation techniques while creating new techniques that will security the network.***
  - E-mail: bgreene@senki.org

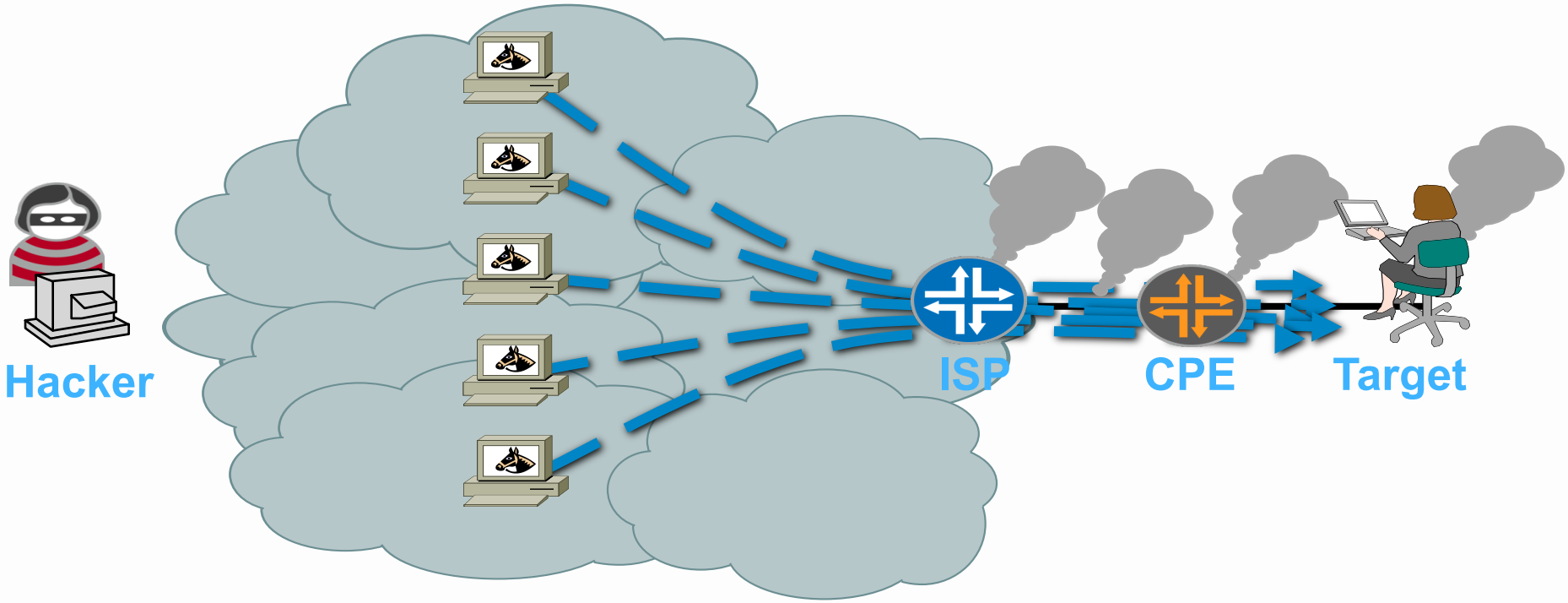
Overview


SKITTER


Greater Demand
Larger Halls
More Equipment
Bigger Organization
Larger Overhead
More Gigs



What Do You Tell the Boss?



The SP's Watershed – Feb 2000

The Vetted – Battling the Bad Guys

WIRED MAGAZINE: ISSUE 15.09

POLITICS : SECURITY RSS

Hackers Take Down the Most Wired Country in Europe

By Joshua Davis 08.21.07 | 2:00 AM

Defense minister Jaak Aaviksoo got help from NATO in the wake of the cyberattacks. *Photo: Donald Milne*

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology d been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

It is known as a botnet, and it had slipped into the country through its least protected border — the Internet

FEATURE

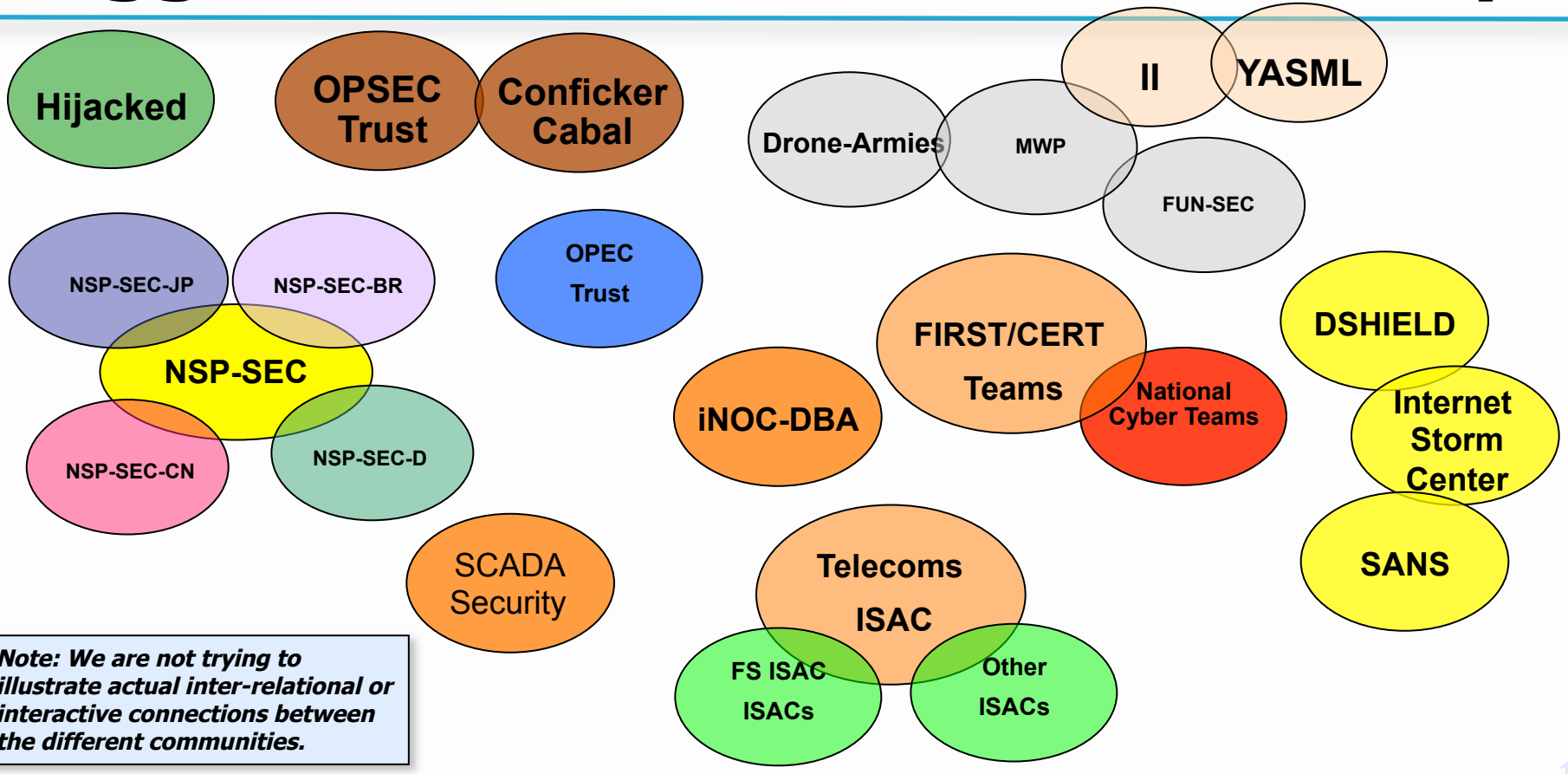
When Bots Attack

Washington Ignores

When BOTs Attack – Inter AS

http://www.wired.com/politics/security/magazine/15-09/ff_estonia_bots

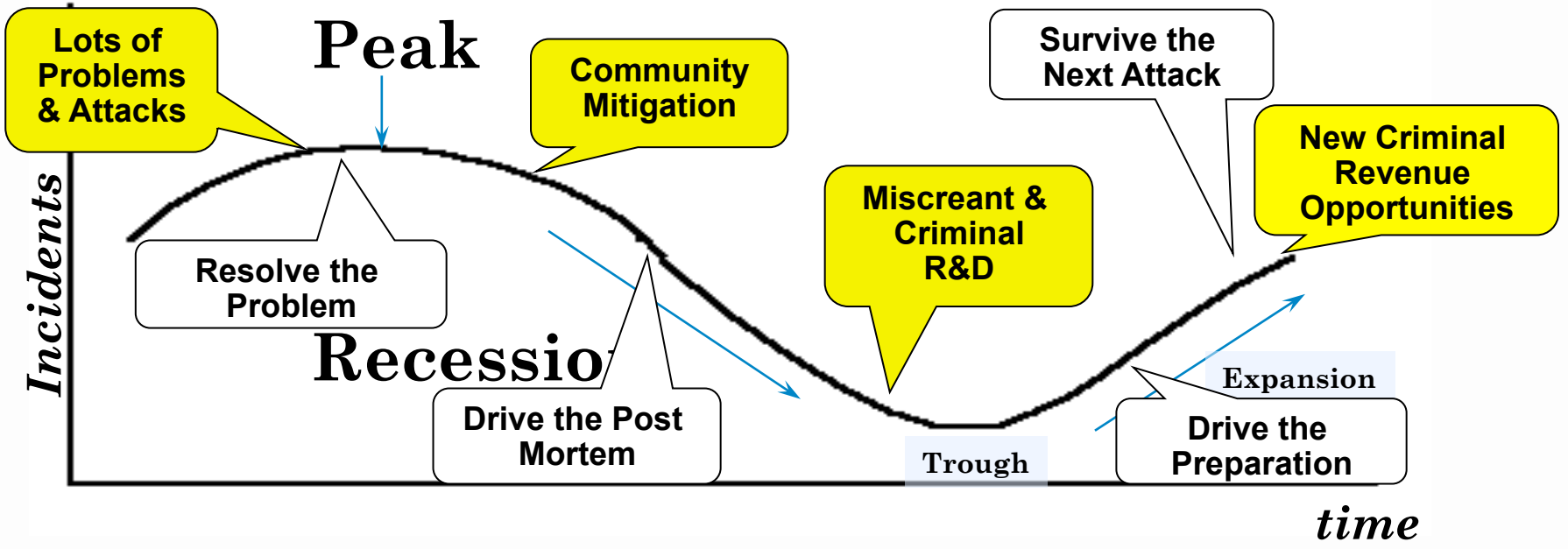
Aggressive Collaboration is the Key



What is NSP-SEC

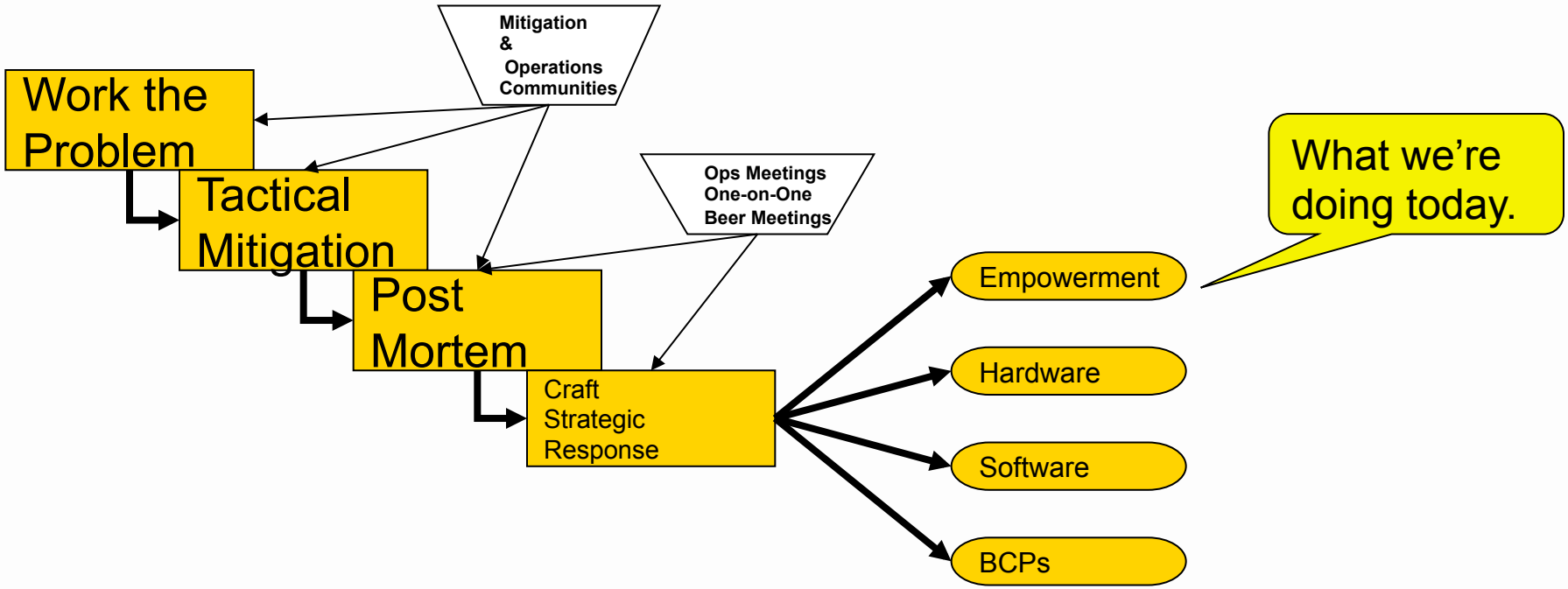
- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- http://puck.nether.net/mailman/listinfo/nsp-security

Miscreant - Incident Economic Cycles



These Cycles Repeat

Where is This Coming From?



Working the 40/40/20 Rule

- Sean Donelan's (back in his SBC days) [sean@donelan.com] rule for end point patching:
  - 40% of the customers care and will proactively patch
  - 40% of the customers may someday care and fix/ patch/delouse their machines
  - 20% of the customers just do not care and have never responded to any effort to fix them.

Top Ten List of SP Security Fundelmentals

1. Prepare your NOC
2. Mitigation Communities
3. iNOC-DBA Hotline
4. Point Protection on Every Device
5. Edge Protection
6. Remote triggered black hole filtering
7. Sink holes
8. Source address validation on all customer traffic
9. Control Plane Protection
10. Total Visibility (Data Harvesting – Data Mining)
11. Remediating Victimized Customers

The Fundamentals are Building Blocks for …

- Clean Pipes – DDOS Mitigation Services
- Malware Remediation Services

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu - Art of War

This has been the first of six video segments

View the entire

Techniques, Tools and Processes to Help Service Providers Clean Malware from Subscriber Systems

from the public training video pages on the M3AAWG website at:
https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Barry Raveendran Greene
for developing and presenting the material in this series
and allowing M3AAWG to videotape it for professionals worldwide.

This video is presented by the
Messaging, Malware and Mobile Anti-Abuse Working Group

For information about M3AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form