SMART

Stopping Malware and Researching Threats

IETF Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.
The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:
BCP 9 (on the Internet Standards Process)
BCP 25 (on the Working Group processes)
BCP 78 (on the IETF Trust)
BCP 79 (on Intellectual Property Rights in the IETF)
Also see: http://www.ietf.org/about/note-well.html:

Agenda

- Chair Time, Charter & Group Setup (Kathleen / Kirsty) - 20 minutes
- Problem Space in Cyber Security (David McGrew) - 10 minutes
- Threat Landscape in Cyber Security (Arnaud Taddei) - 15 minutes
- Testing for the good of the internet (Simon Edwards) - 20 minutes
- BGP hijacking (Toma Gavrinchenkov) - 20 minutes
- CLESS draft on endpoint security (Arnaud Taddei) - 15 minutes
- One Snake (NCSC Senior Speaker) - 20 minutes)

SMART RG - Headlines

- Advisory research group on attack defence.

- Research methods to efficiently and effectively detect, mitigate, prevent or eliminate threats.
- Guide IETF protocol development.
- Become the authority on attack defence and prevention in the IETF/IRTF.

What research we would like to see

- case studies of previous incidents and attacks: how they were prevented, detected, mitigated
- best practice, e.g. use of DMARC, to prevent phishing
- new methods for prevention, detection and mitigation – including automation
- reports and statistics on the current threat landscape
- how to spot slow and bulk data exfil from a network reliably
- endpoint detection capabilities and limitations
- threat detection on encrypted traffic
- or research we are completely unaware of!

Draft Charter

The Stopping Malware and Researching Threats Research Group (or SMART RG) will research the effects, both positive and negative, of existing, proposed and newly published protocols and Internet standards on attack defence. It will gather evidence from information security practitioners on methods used to defend against attacks and make this available to protocol designers, implementers and users. As a result, designers, implementers and users of new protocols will be better informed about the possible impact on attack prevention and mitigation. The SMART RG aims to guide IETF protocol development and become the hub of expertise on attack defence in the IETF/IRTF.

> https://github.com/smart-rg/drafts/blob/master/draft-charter.md

Further links

- Wiki page: https://trac.ietf.org/trac/irtf/wiki/smart
- Mailing list: https://www.irtf.org/mailman/listinfo/smart
- Datatracker: https://datatracker.ietf.org/group/smart/about/
- Github: https://github.com/smart-rg
- CARIS2: https://www.internetsociety.org/events/caris2

Coordinating Attack Response at Internet Scale (CARIS 2) Workshop

Kathleen Moriarty

ISOC Workshop
ISOC & Dell EMC sponsored

Some presented Research and Development Work

- OpenC2
- NICT - Security Automation and Visualization
- Incident response coordination - various groups presented
- IPv6 aggregation - MAPRG

Liability
Legal aspects
Engagement from stakeholders
Liability
Profit
PROFIT
Volume & Velocity of threats
Inter Connectedness
Trust in the Incident Response community
RG chairs and contributors
Company interests
Not invested here
DYNAMIC THREAT LANDSCAPE
Liability
Calibration - privacy - vocabulary - TOE
Bifurcation of Internet
Govt mandate / Regulation
inability to measure security to define targets
Prioritising threats
Complexity - can info always be shared in bullets/one page
attacker cost advantage
COMMERCIALIZATION
Erosion of trust in IR
Supply Chain Risk. Equipment pre-infected coming out of Box
LACK OF QUALIFIED ANALYSTS
Sensitivity of intelligence
TRUST
Driven by different stakeholders
MISSING FRAUD LOSS DATA & ANALYSIS
Solutions: Too little, Too late
MISUNDERSTANDING OF TRUE VS. PERCEIVED RISKS
Privacy, Secrecy of commun.
Speed to MKT
Right to Repair
General Counsel
LEGAL IMPEDIMENTS TO INFO SHARING
clarity of interests in info sharing
New Technology
Lack of expertise
Over-centralization of Internet resources (easy to attack)
New protocols

Incident Response Today

Supporting

- Trust in incident response teams
- Need to protect network as a forcing function
- Current efforts supported by profit
- FEAR - initially a burst of wind, but eventually leads to complacency

Dragging

- Too many standards
- Regional border impact data flows
- Lack of Resources/Participation
- Monoculture

Looming problems ahead

- Dynamic threat landscape
- Liability
- Bifurcation of Internet
- Lack of skilled analysts
- Sensitivity of Intelligence/trust

Breakout Brainstorming, may lead to work for SMART

- Fingerprinting
  - packet comparisons
- SNARC - uses trust indicator to make decisions about good/bad actors
  - builds on zero trust networking
  - research visual aspect and underlying principle
  - similar theme on IP reputation/BGP ranking
- Attack coordination solutions/automated security
- Cryptographic Rendezvous
- L2 discovery