ITU Workshop on Advanced Cybersecurity Attacks and Ransomware

Geneva, Switzerland, 28 August 2018

Takeaways and Conclusions

1. Necessity to be open to all groups and participants working in this landscape
2. Need to identify gaps in standards
3. Need to define procedures for victims of ransomware attacks
4. Need to identify existing frameworks
5. Need to share information and cyber threat intelligence
6. Need to identify imminent threats

Suggestions to ITU-T SG17

- ❑ Establish cooperation with current activities in ISO/IEC in this field
- ❑ Perform an gap analysis of the standards landscape in this field
- ❑ Adopt existing frameworks and best practices for preventing and responding to advanced cybersecurity attacks
- ❑ Develop standards in this field as needed

Session 2: Advanced cybersecurity attacks and ransomware attack scenarios

Takeaways and Conclusions

1. Actionable cybersecurity information sharing is extremely important
2. Concepts of getting humans out of the loop and machine speed information sharing need to be better understood and broadly implemented
3. Adoption of existing standards and frameworks is important (e.g., STIX/TAXII, MITRE ATT&CK, etc.), to avoid duplication

Suggestions to ITU-T SG17

- ❑ Develop best practices to share information about targeted cyber attacks and ransomware
- ❑ Adopt OASIS STIX/TAXII specifications into ITU-T Recommendations
- ❑ Important to collaborate with other standards organizations to find common structures to share actionable information to mitigate the risks of cyber attacks (e.g., OASIS, IETF, etc.)

Session 3: Technical, organizational and administrative countermeasures

Takeaways and Conclusions

1. Take advantage of many standards developed but let people 1) know them and 2) use them
2. Need to identify observables and adversary behaviors and simulation/new generation of honeypot helps
3. Targeted Attacks and its inherent infrastructure is more and more sophisticated (yet sometimes execution of attacks is surprisingly showing mistakes)
4. but Machine Learning contributes to the security weaponry and the detection
5. There are good rationales to fight unknown threats but again it requires a) an abstraction level and semantic model b) machine learning and AI and c) ways to help supervised and unsupervised learning
6. Finally, human beings need to be properly organized with both good planning and operational maturity in place and a good framework for the right service catalog to support and orchestrate tools and products. It's about 'actionability' and Course of Actions
7. No, we cannot remove the Human Being!
8. Note: Many details would need a deeper distillation (impact of pervasive encryption, how to enforce security in IoT, DGA and DNS aspects, Ransomware on Big Data (Hadoop), etc.

Suggestions to ITU-T SG17

- ❑ Share several key aspects of workshop outcome to the transformation of security studies
- ❑ Need to develop a security framework and architecture in Q2/17 that can support the various mitigations solutions reviewed? Simulation, Sandboxing, ATP, AI/ML, etc.?
- ❑ AI and Machine Learning is required to support core security techniques and informs directly Q4/17
- ❑ Mail is still a problem and phishing and spam are a major vector with ATP solutions required in the messaging infrastructure(s) and informs directly Q5/17
- ❑ Yet targeted attacks and their solutions are common to both Q4/17 and Q5/17
- ❑ Organizational and Administrative aspects are directly informing the new Cyber Defense Center approach in Q3/17
- ❑ Many other aspects relevant to Q6/17 (IoT), Q8/17 (Infrastructure and Big Data), Q7/17 (Application Security), Q12/17 (Formal languages, semantics, etc.) that would need deeper analysis

Session 4: Panel discussion – Future directions on cybersecurity standardization activity

Takeaways and Conclusions

1. Identified security subjects: security for advanced cybersecurity attacks and ransomware attacks
2. Relevant Questions in SG17: Q2/17, Q3/17, Q4/17, Q5/17, Q10/17 - Cybersecurity Framework, Risk assessment, countermeasure for cybersecurity, and incident response
3. Need to define Terminology and identify existing frameworks in this field
4. Need to collaborate with ISO/IEC JTC 1/SC27/WG 4

Suggestions to ITU-T SG17

- ❑ Establish cooperation with OASIS CTI TC for adopting the STIX/TAXII specifications
- ❑ Important to collaborate with ISO/IEC JTC1 SC27 and other groups for the development of standards in the field
- ❑ Define common terminology that is understood in both the public and private sectors and focus on adoption of existing frameworks