

Capabilities and Limitations of Endpoint Security Solutions (CLESS)

IETF 104, Monday 25th of March 2019, Prague

Arnaud Taddei (Arnaud_[Taddei@symantec.com](mailto:Arnaud_Taddei@symantec.com))

Candid Wueest (Candid_Wueest@symantec.com)

Kevin Roundy (Kevin_Roundy@symantec.com)

Dominique Lazanski (dml@lastpresslabel.com)

Introduction to CLESS

- Why? A gap in the « codification » of endpoint security?
- Why now? Many « environmental » changes (technical, regulations, etc.)
- What?
 - In the long term, a full review of endpoint security in all its dimensions
 - Currently we started with
 - Endpoint Models
 - Threat Landscape
 - Endpoint security capabilities
 - An ideal endpoint security
 - Defence in depth
 - Endpoint security limitations
 - Example from production data
 - Regulatory aspects
- Status? An early draft on purpose, we seek feedback and future collaboration

Where to find it? Table of Content

<https://github.com/smart-rg/drafts/blob/master/draft-taddei-class-introduction-00.txt>

Table of Contents

1. Introduction	3	11. Learnings from production data	27	
2. Abbreviations	4	11.1. Endpoint only incidents	28	
3. Definitions	5	11.2. Security incidents detected primarily by network security products	29	
4. Disclaimer	6	11.2.1. Unauthorized external vulnerability scans	29	
5. Endpoints: definitions, models and scope	6	11.2.2. Unauthorized internal vulnerability scans	30	
5.1. Internal representation of an endpoint	7	11.2.3. Malware downloads resulting in exposed endpoints	30	
5.2. Endpoints modeled in an end-to-end context	8	11.2.4. Exploit kit infections	30	
6. Threat Landscape	8	11.2.5. Attacks against servers	31	
7. Endpoint Security Capabilities	10	12. Regulatory Considerations	32	
8. What would be a perfect endpoint security solution?	13			
9. The defence-in-depth principle	15			
10. Endpoint Security Limits	16			
10.1. No possibility to put an endpoint security add-on on the UE	17			
10.1.1. Not receiving any updates or functioning patches	18			
10.1.2. Mirai IoT bot	19			
10.2. Endpoints may not see the malware on the endpoint	19			
10.2.1. LoJax UEFI rootkit	19			
10.2.2. SGX Malware	20			
10.2.3. AMT Takeover	20			
10.2.4. AMT case study (anonymised)	21			
10.2.5. Users bypass the endpoint security	22			
10.3. Endpoints may miss information leakage attacks	22			
10.3.1. Meltdown/Specter	22			
10.3.2. Network daemon exploits	22			
10.3.3. SQL injection attacks	23			
10.3.4. Low and slow data exfiltration	23			
10.4. Suboptimality and gray areas	24			
10.4.1. Stolen credentials	24			
10.4.2. Zero Day Vulnerability	25			
10.4.3. Port scan over the network	25			
10.4.4. DDoS attacks	26			
		Taddei, et al.	Expires September 20, 2019	[Page 2]
		Internet-Draft	CLESS	March 2019
		12.1. IoT Security	32	
		12.2. Network infrastructure	33	
		12.3. Auditing and Assessment	33	
		12.4. Privacy Considerations	34	
		13. Human Rights Considerations	34	
		14. Security Considerations	34	
		15. IANA Considerations	34	
		16. Informative References	34	
		Appendix A. Contributors	39	
		Authors' Addresses	40	

Lessons Learnt Already

- Much harder than initially thought
- Couldn't find any satisfying:
 - Threat Landscape methodology for endpoint security
 - Capabilities list and methodology for endpoint security (not just 3rd party)
 - Good potential of work for SMART on both threat landscape and capabilities
- Production data from Managed Security Services
 - Interesting methodology
 - Study on the last 3 months on hundreds of enterprise customers
 - Endpoint only security gives a lot of results
 - Critical events not detected by endpoints

Questions for Future Development

- Endpoint modeling between 'UEs' and 'Hosts'
 - Better uniformity across the document
- Threat Landscape Methodology
 - Align with or fork from MITRE ATT&CK?
 - Should it be done in this I-D?
- Intrinsic Capabilities
 - Need a much deeper inventory
- Other Aspects
 - Should we have an economic section?
 - Regulations and Human Rights sections – need a good neutral balance
 - New Requirements, New Limits, New Constraints
 - Other real production data?

QUESTIONS ?

THANK YOU