Big Data Analytics as a Tool for Advanced Persistent Threat Detection

Nikolaos Benias, Nikolaos Tsalis

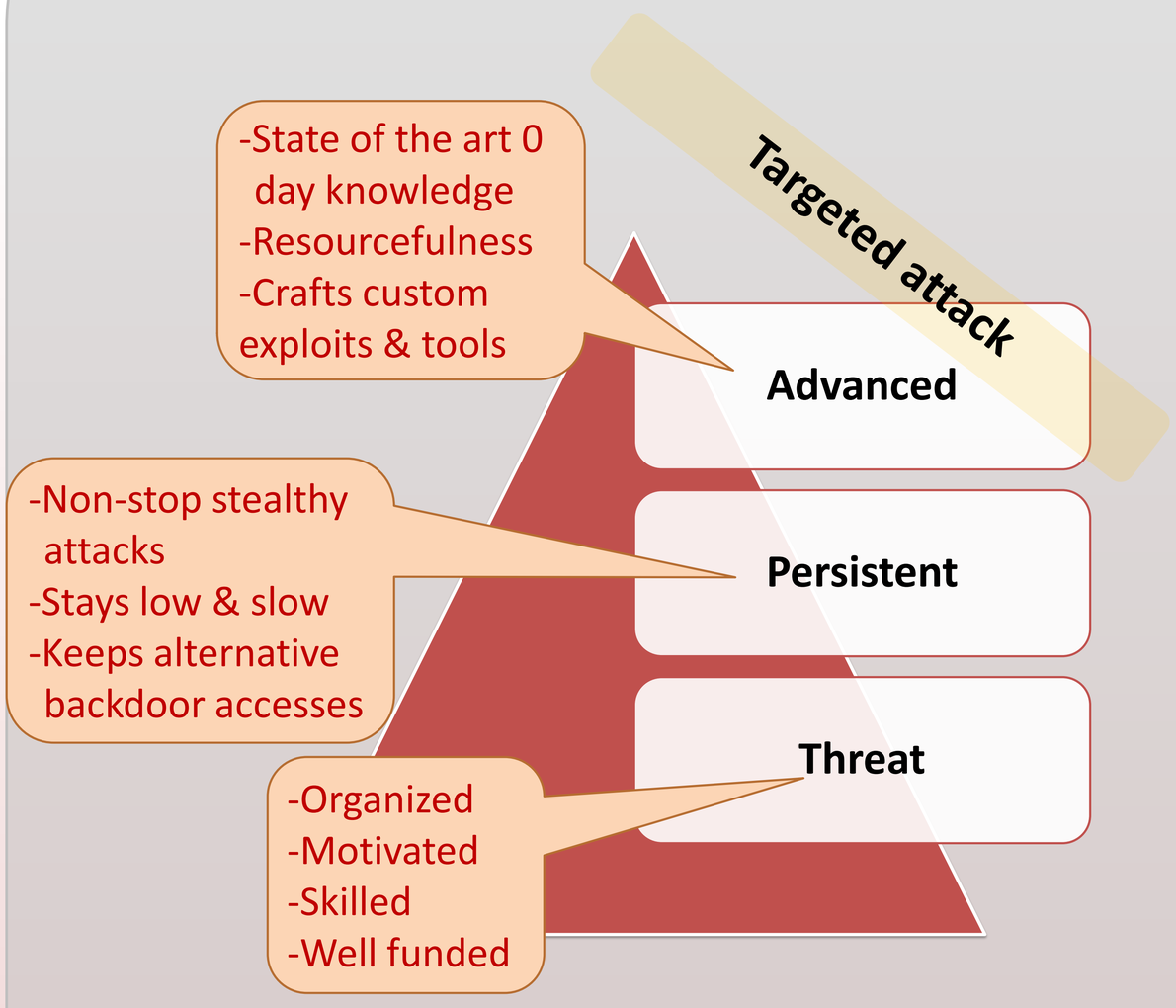
[1] *Dept. of Informatics, Hellenic Open University, Greece*

[2] *Information Security and Critical Infrastructure Protection Research Laboratory,*

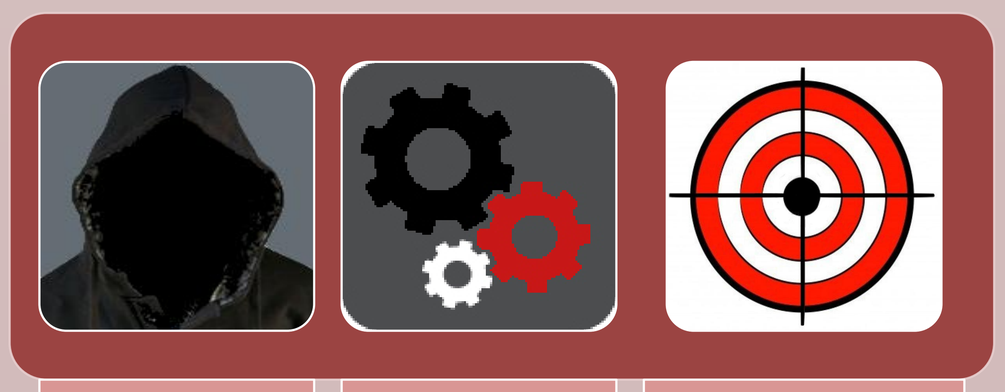
Dept. of Informatics, Athens University of Economics & Business, Greece

Advanced Persistent Threat (APT)

A group of people with both the capability and the intent to persistently and effectively target a specific entity.



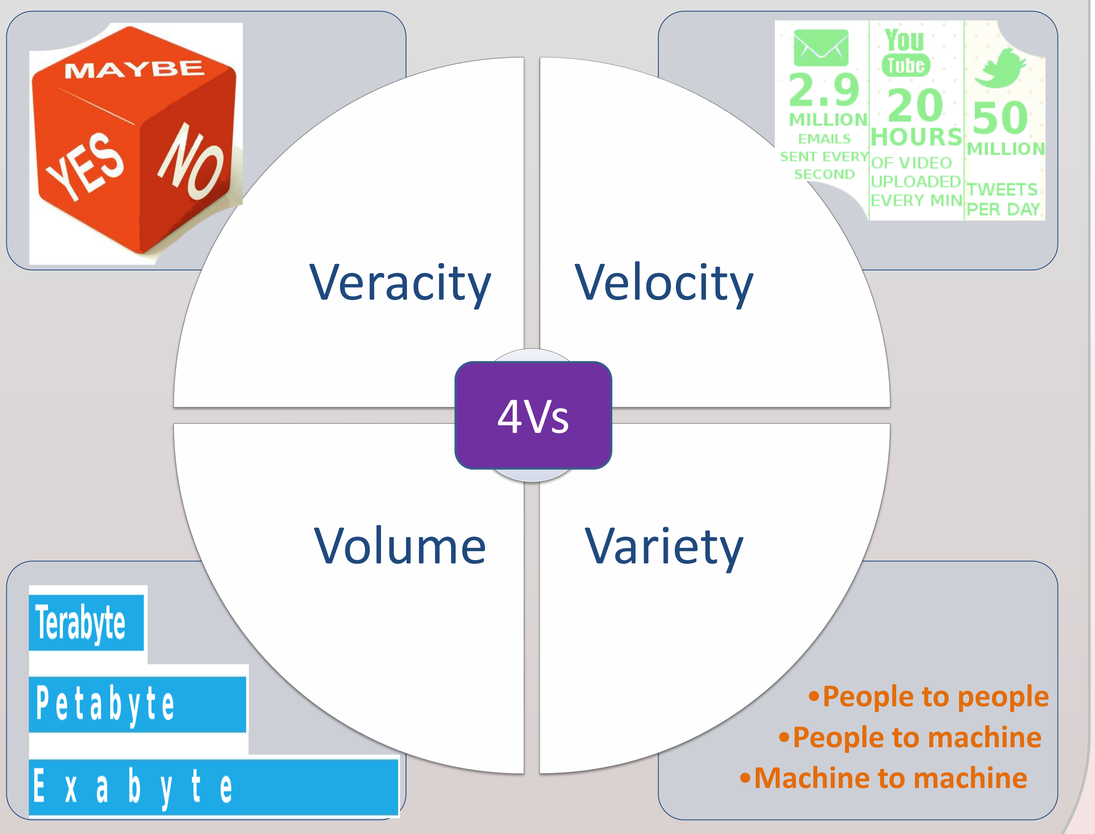
APT name	Stuxnet	Duqu	Flame	Red October	Mini Duke
Active since	June 2009 (2005)	November 2010	May 2012 (2006)	May 2007	June 2011
Detected	June 2010	September 2011	May 2012	October 2012	February 2013
PE executable	DLL		OCX	EXE	EXE
Initial infection	Unknown	MS Word	Unknown	MS Excel / Work, Java	PDF
Self-replication	Removable drives, Over the network	Manual replication only			
Rootkit functionality	Yes		No		
Key logging module	No	Yes			No
Targets sec. products	Yes			No	Yes
Encryption	XOR	XOR, AES-CBC	XOR, Susti		Unique per victim, XOR, ROL
Target	Sabotage	Information gathering			



Actors	Motives	Targets
Governments	Political	Countries
Organized crime	Military	Government agencies
Industrial spies	Espionage	Corporations
Hacktivists	Financial	Industries
	Reputation	Contractors
	Trade secrets	Think tanks
	Control foothold	High profile people

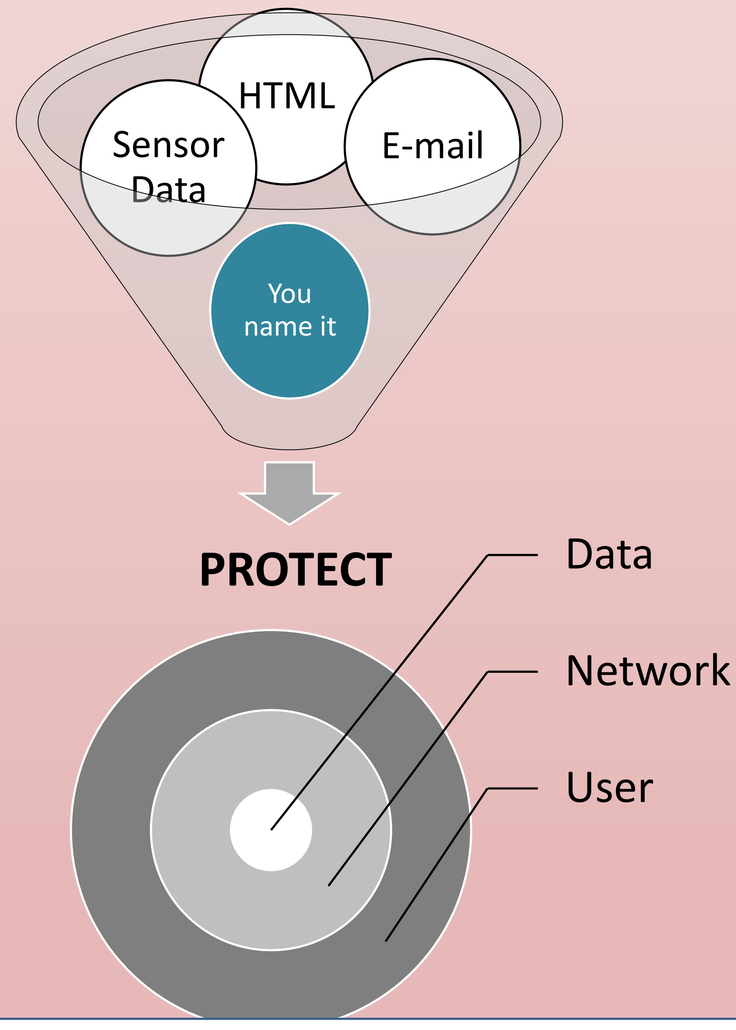
Big Data

Data that is too large, complex and dynamic for any conventional data tools to capture, store, manage and analyze.



Big Data Analytics

Allows analysts to spot trends and gives niche insights that help create value and innovation much faster than conventional methods.



References

1. Big Data Working Group, "Big Data Analytics for Security Intelligence", *Cloud Security Alliance*, 2013.
2. Cole, E., *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Waltham, Syngress, 2013.
3. Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, P., "Intrusion detection: Evaluation and performance issues of the SECURENET system", *Computers & Security*, Vol. 13, No. 6, pp. 495-508, 1994.
4. Doumas, A., Mavroudakis, K., Gritzalis, D., Katsikas, S., "Design of a neural network for recognition and classification of computer viruses", *Computers & Security*, Vol. 14, No. 5, pp. 435-448, 1995.
5. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An Insider Threat Prediction Model", *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business*, Springer, Spain, pp. 26-37, 2010.
6. Katsikas, S., Gritzalis, D., Spirakis, P., "Attack Modeling in Open Network Environments", *Proc. of the 2nd Communications and Multimedia Security Conference*, Chapman & Hall, Germany, pp. 268-277, 1997.
7. Katsikas, S., Spyrou, T., Gritzalis, D., Darzentas, J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
8. McClure, S., Scambray, J., Kurtz, G., "Hacking Exposed 7: Network Security Secrets & Solutions", McGraw-Hill, pp. 313-72, 2012.
9. Mylonas, A., Dritsas, S, Tsoumas, V., Gritzalis, D., "Smartphone Security Evaluation - The Malware Attack Case", in Proc. of the 8th International Conference on Security and Cryptography, pp. 25-36, SciTePress, Spain 2011.
10. Spirakis, P., Katsikas, S., Gritzalis, D., Allegre, F., Darzentas, J., Gigante, C., Karagiannis, D., Putkonen, H., Spyrou, T., "SECURENET: A Network-oriented intrusion prevention and detection intelligent system", *Proc. of the 10th IFIP International Information Security Conference*, 1994.
11. Virvilis, N., Gritzalis, D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", *Proc. of the 10th IEEE International Conference on Autonomous and Trusted Computing*, IEEE Press, Italy, pp. 396-403, 2013.
12. Virvilis, N., Gritzalis, D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", *Proc. of the 8th International Conference on Availability, Reliability and Security*, IEEE, Germany, pp.248-254, 2013.
13. Virvilis, N., Dritsas, S., Gritzalis, D., "A cloud provider-agnostic secure storage protocol", in *Proc. of the 5th International Conference on Critical Information Infrastructure Security*, pp. 104-115, Springer, Greece, 2010.