Information & Security

D. Dimov & Y. Tsonev
vol. 47, no. 3 (2020): 317-327
https://doi.org/10.11610/isij.4723

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Observing, Measuring and Collecting HDD Performance Metrics on a Physical Machine During Ransomware Attack

Dimo Dimov (✉), *Yuliyan Tsonev*

Department of Information Technologies, Nikola Vaptsarov Naval Academy, Varna, Bulgaria, http://www.naval-acad.bg/en

ABSTRACT:

Ransomware is a type of malicious activity aiming to prevent users from accessing their data by encrypting it. For the purposes of analysis of the behaviour of the crypto viruses, objectively collected data is required. Getting metrics from a virtual machine would be resembling the original behaviour of the ransomware on a physical device. Observing, measuring, collecting and extracting data on a physical device during and after encryption is challenging, since all the data would be corrupted once the encryption process is complete. By utilizing two user profiles, members of the local admin group and custom access control lists on certain recourse, a lab laptop is infected with five different samples of ransomware crypto viruses that do not require connection to the command and control server in order to function as intended. A data set of HDD metrics is successfully collected and extracted.

ARTICLE INFO:

RECEIVED: 28 APR 2020
REVISED: 16 MAY 2020
ONLINE: 18 MAY 2020

KEYWORDS:

measurement, extraction, ransomware, encryption, malware, malicious, cybersecurity

Creative Commons BY-NC 4.0

1. Introduction

Main focus of this paper is the measurement and extraction of raw feasible HDD metrics on a physical device during an ongoing crypto virus attack. Performing such measurement on a virtual machine would be considerably easier, since the attacked environment could be paused, refreshed or if needed restored in a

✉ E-mail: dimo.b.dimov@gmail.com

matter of seconds. Virtual machine however would measure a "suggested" metrics of a virtually provisioned storage that is technically a tiny part of a different, bigger storage or even part of a JBOD. Measurement performed on a physical device, but not on a guest machine on a hypervisor, would result on trusted quality quantitative results.

Because of the propagation mechanism of the generic cryptolockers – gaining logged in user privileges on a Windows based operating system results in encryption of all the files where the respective user is owner or has write permissions, it is a challenge to obtain any files that are containing the measured metrics data, without being encrypted. Our target got further – measuring and extracting performance metrics data from a physic device where the ransomware has captured an administrative (full system access) account or is executed by an account member of the local admin group.

2. Lab Environment and collected metrics

2.1. Device hardware, operating system, data, user profiles

Five different ransomware crypto locker samples were tested on a mid-class laptop device (CPU: Intel Core i5-3320M 2.60GHz, RAM: 4096MB DDR3 SDRAM SO-DIMM, HDD: 320GB HDD Serial ATA). Overall time needed for collecting the malicious samples, creating a lab Windows 7 image, deploying the image, executing the payload, making the measurement, extracting the data (not always successfully) and re-imaging the device was about 34 hours. The image deployed had a bare Windows 7 x86 (without Service Pack 1), missing any critical or security updates, no antivirus application, firewall was disabled. 10GB of dummy documents were created with extensions .doc, .xls and .ppt.

Two customized user profiles were created – "measure" and "victim." Both users were part of Local Admin Group e.g. are local administrator on the system. Access control lists were customized in a manner so the "victim" will run a malicious file and allow the virus to execute the payload and engage the environment.

Custom performance counter set was created, where the default permissions on the output file were modified. Inheritance of the object was disabled for an explicit list of permissions to be defined. Local admin group was removed. System account remained as it was needed to write to the output file.

Before the virus sample is run by "victim" the performance monitoring tool recoding is started in the context of "measure" and usual user activity is simulated – web browsing, document/spreadsheet work. Two minutes after the performance monitor is started, the malicious payload is executed.

After the full encryption of the dummy documents the performance monitor is stopped so a ".blg" file is properly saved and closed. System is gracefully shut down. HDD is detached from the lab laptop and accessed offline from another device in order to avoid potential contamination or virus escape.

2.2 Collected metrics by Performance Monitor

2.2.1 %ProcessorTime

% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the percentage of time that the processor spends executing the idle thread and then subtracting that value from 100%. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity and displays the average percentage of busy time observed during the sample interval.[1]

2.2.2 Avg. Disk sec/Read

The Avg. Disk sec/Read counter (PhysicalDisk\Avg. Disk sec/Read) tracks the average amount of time it takes in milliseconds to read from a disk.[2]

2.2.3 Current Disk Queue Length

Current Disk Queue Length is a direct measurement of the disk queue present at the time of the sampling.

2.2.4 Avg. Disk sec/Write

The Avg. Disk sec/Write counter (PhysicalDisk\Avg. Disk sec/Write) tracks the average amount of time it takes in milliseconds to read from or write to a disk.[2]

2.2.5 Disk Bytes/sec

Perfmon captures the total number of bytes sent to the disk (write) and retrieved from the disk (read) over a period of one second. If the Perfmon capture interval is set for anything greater than one second, the average of the values captured is presented. The Disk Read Bytes/sec and the Disk Write Bytes/sec counters break down the results displaying only read bytes or only write bytes, respectively.[3]

2.2.6 Avg. Disk Queue Length

Shows the average number of both read and writes requests that were queued for the selected disk during the sample interval.[4]

2.2.7 Disk Transfers/sec - (Disk Reads/sec, Disk Writes/sec)

This is the rate of operations (I/Os per second) for the selected disk during the sample interval. If this value rises above 100 for a single physical disk and the Avg. Disk sec/Transfer is higher than your baseline, it is the disk drive that is the bottleneck.[5]

3. Tested Samples – short behaviour description and measured results

Focus of this paper is the successful extraction of measured data from a physical device after a completed ransomware lockdown. However short behaviour description of the malicious samples will be provided with a reference to the results extracted from the lab device – see Table1.

All of the virus samples showed similar behaviour – enumeration the data on the device, encryption of all the files where the targeted active user had ‘write’

or 'full' permissions in the ACL, change of the file extensions of the encrypted files. Some samples performed a search for a possible SMB path to spread further. Considering the different approach on choosing the encryption algorithm

Table 1. Measured performance metrics.

Counter	Colour	Scale	Min	Max	Avg.	Duration (min:sec)
Processor time (TeslaCrypt)		1.0	0.859	79.643	17.175	19:54
Processor time (Cerber)		1.0	0.000	19.451	8.933	8:54
Processor time (WannaCry)		1.0	0.000	31.250	13.911	25:10
Processor time (CryptoShield)		1.0	2.109	32.516	11.529	15:35
Processor time (Vipasana)		1.0	0.000	62.796	36.606	57:55
Avg. Disk sec/Read (TeslaCrypt)		1000	0.000	0.156	0.053	19:54
Avg. Disk sec/Read (Cerber)		1000	0.001	0.065	0.034	8:54
Avg. Disk sec/Read (WannaCry)		1000	0.002	0.118	0.050	25:10
Avg. Disk sec/Read (CryptoShield)		1000	0.000	0.196	0.041	15:35
Avg. Disk sec/Read (Vipasana)		1000	0.000	0.046	0.017	57:55
Current Disk Queue Length (TeslaCrypt)		10	0.000	5.000	1.138	19:54
Current Disk Queue Length (Cerber)		10	0.000	13.000	4.352	8:54
Current Disk Queue Length (WannaCry)		10	0.000	10.000	1.993	25:10
Current Disk Queue Length (CryptoShield)		10	0.000	13.000	3.133	15:35
Current Disk Queue Length (Vipasana)		10	0.000	6.000	0.596	57:55
Avg. Disk sec/Write (TeslaCrypt)		1000	0.000	0.016	0.02	19:54

Avg. Disk sec/Write (Cerber)		1000	0.000	0.074	0.031	8:54
Avg. Disk sec/Write (WannaCry)		1000	0.000	0.068	0.021	25:10
Avg. Disk sec/Write (CryptoShield)		1000	0.000	0.114	0.040	15:35
Avg. Disk sec/Write (Vipasana)		1000	0.000	0.013	0.002	57:55
Disk Bytes/sec (TeslaCrypt)		0.000001	0.000	28420023	20124543	19:54
Disk Bytes/sec (Cerber)		0.000001	231209.632	79547525	42963691	8:54
Disk Bytes/sec (WannaCry)		0.000001	260003.629	46545317	22583531	25:10
Disk Bytes/sec (CryptoShield)		0.000001	314712.870	53732741	25607843	15:35
Disk Bytes/sec (Vipasana)		0.000001	3373.971	15631676	2334152	57:55
Avg. Disk Queue Length (TeslaCrypt)		10	0.000	3.494	1.197	19:54
Avg. Disk Queue Length (Cerber)		10	0.005	8.714	4.176	8:54
Avg. Disk Queue Length (WannaCry)		10	0.009	6.184	2.958	25:10
Avg. Disk Queue Length (CryptoShield)		10	0.009	7.824	2.622	15:35
Avg. Disk Queue Length (Vipasana)		10	0.000	3.136	0.607	57:55
Disk Transfers/sec (TeslaCrypt)		0.1	0.000	161.915	95.652	19:54
Disk Transfers/sec (Cerber)		0.1	3.200	452.784	127.177	8:54
Disk Transfers/sec (WannaCry)		0.1	3.195	255764	91.060	25:10
Disk Transfers/sec (CryptoShield)		0.1	3.195	381275	64.371	15:35
Disk Transfers/sec (Vipasana)		0.1	0.599	1354.393	68.075	57:55

type/strength, payload delivery and execution the time needed for the ransomware to encrypt all the 10GB dummy documents was varying between 5 and 60

minutes. Following topics are presenting a glance over the malware actions with short description of the process followed by the extracted performance indicators metrics.

3.1 TeslaCrypt

TeslaCrypt reaches users through e-mail and encrypts many files in the system after execution of its payload found in the e-mail attachment. It demands ransom to allow access to encrypted files of the user.[6]

Once the malware is executed, it duplicates itself at %AppData% naming itself with a randomized seven string noncomplex character name (e.g. flttstb.exe). Initially, as most of the ransomware samples, volume shadow copies are deleted from the system and registry key is loaded in "HKLM\SOFTWARE\ Microsoft\Windows\CurrentVersion\Run" with the name and full path as stated in %AppData%. Same registry key is placed under current user hive at the targeted user profile.

TeslaCrypt uses the Advanced Encryption Standard (AES-256) algorithm to encrypt files, but the malware misrepresents its file encryption in two ways:

- It renames encrypted files with an "ecc" extension, which suggests use of an Elliptic Curve Cryptographic (ECC) algorithm. The malware uses the algorithm when generating Bitcoin addresses, but not to encrypt files.[7]
- Splash screen messages and files left on compromised systems claim to use the RSA-2048 encryption algorithm.[7]

The encryption process initiates with the malware utilizing the GetLogicalDriveStrings() API function to enumerate storage on volume drives (C:,D:…). The GetDriveType() API call then selectively targets DRIVE_FIXED drives (HDD,SSDs) and DRIVE_REMOTE drives (network shares that are mapped). The malware recursively swipes the drives for files with specific extensions, and then each file is opened, read, and encrypted. The encrypted data is forged to the original file, so the potential possibility of forensic tools can recover the original data is minimized.

"Avg. Disk sec/Read" extensive action shows the reading process after the enumeration of the environment and prior encryption along with the "Disk Transfers" considerably high metrics. As the quick encryption algorithm and the lack of sophisticated post-encryption processes the Avg. and Current Disk Queue Lengts are almost negligible – Ref. Figure 1, Table 1.

3.2 Cerber

Once executed, file is copied to %Appdata% with randomized name, original file is deleted. A shortcut is created at "%APPDATA%/Microsoft/Windows/Start Menu/Programs/Startup" to ensure file is started upon next startup. Before encryption process starts the executable starts a few other threads of itself that would 'load balance' the encryption of the files.

Working on the files encryption in parallel instances significantly reduces the time of the complete environment encryption (compared to all the measured malware samples) in exchange for extensive Avg. and Current Disk Queue

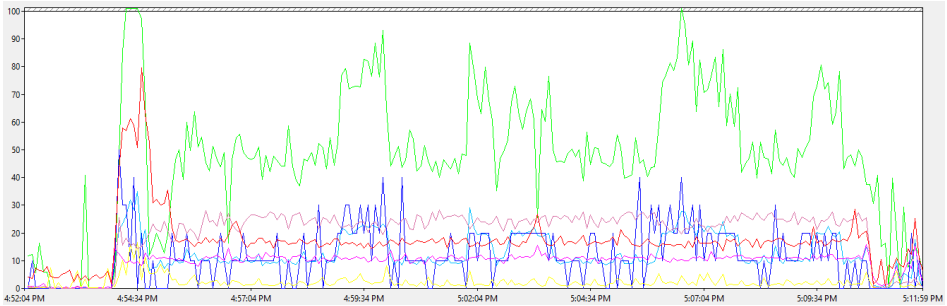

Figure 1: TeslaCrypt ransomware HDD performance metrics diagram screen.

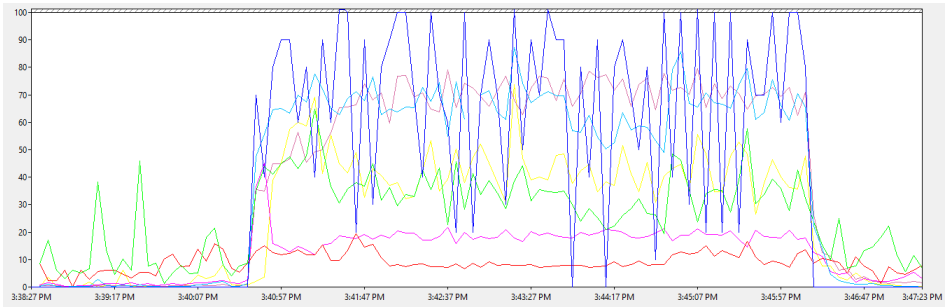

Figure 2: Cerbert ransomware HDD performance metrics diagram screen.

Lengths and Disk Transfers. In this experiment the encryption concluded with the shortest time of 8:54 min – Ref. Figure 2, Table 1.

3.3 WannaCry aka WCry

Ransomware Wannacry attacked many hospitals, companies, universities and government organization across at least 150 universities, having more than 200000 victims. It locked all computers and demanded ransom.[9]

Ransomware overwrites the contents of the original file by opening the file, reading its contents, writing the encrypted contents in-place, then closing the file.[10]

File is copied under "C:\Windows" directory and upon execution is deleting the volume shadow copies. It runs bcdedit ("bootstatuspolicy ignoreallfailures" and "recoveryenabled no") commands to ensure that the system will be able to boot properly in the event of an unexpected reboot or shut down. The malware kills tasks related to sql and Microsoft exchange to ensure DB files will be editable.

WCry uses a combination of the RSA and AES algorithms to encrypt files. It uses the Windows Crypto API for RSA encryption and random key generation; however, a third-party implementation of AES is statically linked within the malware. Prior to encryption, WCry enumerates all available disks on the system. This enumeration includes local drives (e.g., hard disks), removable drives (e.g.,

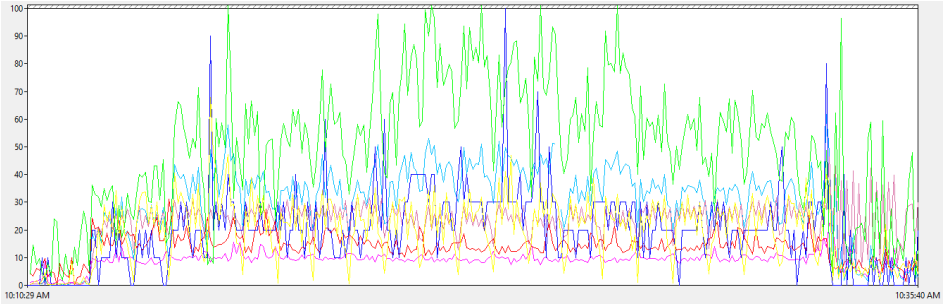

Figure 3: WannaCry ransomware HDD performance metrics diagram screen.

USB thumb drives), and network drives (e.g., a remote file share mapped to a drive letter). WCry generates a private RSA-2048 key pair specific to each infection and stores it on the local disk with an .eky extension (e.g., 00000000.eky) after encrypting it with an embedded RSA public key. This generated RSA key is used to encrypt the random AES-128 key generated for each encrypted file.[11]

Each targeted file is opened, read, encrypted in memory, and then written to a new file in the malware's working directory using the filename format <random number>.WNCRYT. The files are then renamed to their original filename followed by the ".WINCRY" extension and moved to their original directory. The taskdl.exe process launched by the malware periodically deletes the remaining WINCRYT temporary files. The encryption process does not directly overwrite file data, so forensic recovery of file contents may be possible depending on the environment. The entire contents of the file are encrypted and saved with a custom header.[11]

Those multiple recursive iterations running in a single threaded operation are reflected in the numbers gathered during an actual infection on the physical device. All metrics are "in the middle of the chart" of the data gathered during the experiment with prevalent disk transfers and high "Avg. Disk Queue Length" - Ref. Figure 2, Table 1.

3.4 CryptoShield

Similarly to WCry, this ransomware deletes VSS copy and runs same bcdedit commands. It targets a variuos number of file extensios (including audio and video). Files are encrypted using AES-256 encryption algorithm and renamed using simple substitution cypther ROT-13. "CRYPTOSHIELD" extension is added to the filename. Final result for a file previusly named "presentation.ppt" would be "cerfragngvba.ccg.CRYPTOSHIELD".

Since the single type of encryption and the significantly lower number of iterations – no files are deleted or created, no key is apended to the files header, etc. the overall encryption process and and performance metrics are lower comared to WCry – overall time for completion is 15 minutes – ref Table 1.

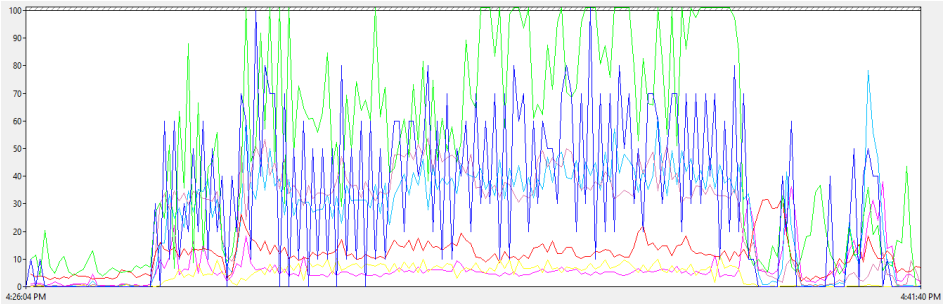

Figure 4: CryptoShield ransomware HDD performance metrics diagram screen.

3.5 Vipasana

Vipasana ransomware is innovative yet an old malicious crypto-locker. It does not require internet connection to send the private key to the attacker. Public key needed for the encryption is embedded to the malicious sample and is the enough for an encryption process to be initiated. Vipasana is not using 'traditionally' AES, but a stream cypher encryption algorithm. For each file a block of 2048 characters is used for filling a list 512 positions to be deployed as an internal state for a 'proprietary' PRNG (Pseudo Random Number Generator).

The way this PRNG works is that it uses and manipulates the internal state during the generation of random bytes. If we start the PRNG with the same internal state, the PRNG will always generate the same bytes as a result. And the result of this operation is the keystream of the Vipasana stream cipher. The bytes of the keystream are combined with the bytes of the plaintext file. The way this is done is as follows: There is an additional block of 20 characters (all numbers) in the file. For every byte of the plaintext file and the keystream, the next character of this additional block decides how they are combined. The fact that the state block source and the global algorithm key are encrypted with RSA makes it very hard to create a decryption tool for this type of ransomware, or in other words, to break the encryption.[12]

All the long and sophisticated calculations are captured by the performance monitor and are resulting in tremendous amount of time and considerable processing power – 3 to 5 times higher average processor time consumed (during 2-10 times longer period) compared to the other measured samples.

4. Conclusion and Further Development

Measuring and extracting data from a physical device could not be achieved if preliminary profile and environment customization takes place. Diverse samples were tested yet similar behaviour is observed. Despite the various attacks approach, the final stage consists of multiple encrypted unusable files. Almost all the tested samples tried to spread across any other storage that could be potential attack surface for the extortionist. Higher chance to stop ransomware

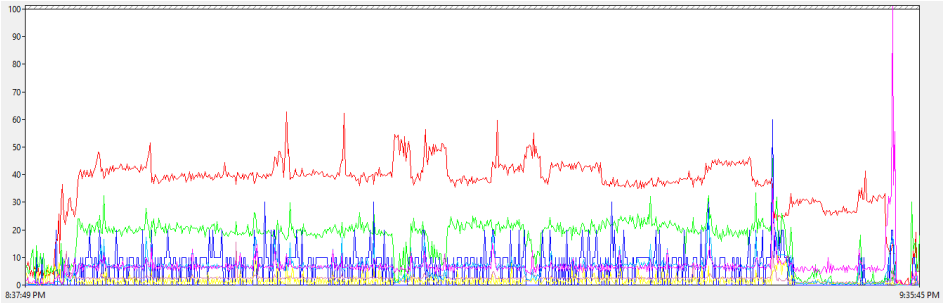

Figure 5: Vipasana ransomware HDD performance metrics diagram screen.

attack from spreading across a network is to harness any heuristic methods possible and detect the malicious behaviour at the very beginning of the payload execution. Measuring, extracting and analysing performance metrics of a hard disk drive during an active ransomware attack would allow us to get the system response behaviour during the malicious encryption. Further, the data extrapolated from the measurement corelated with the existing instant indicators of compromise would get us leverage to isolate the threat before the malicious content propagates and exploits deeper the resources on the network. Performing more sophisticated analysis and getting repetitive positive results are inconceivable without authoritative and integrative data.

References

1 Hemanth Tarra, "Understanding Processor (% Processor Time) and Process (%Processor Time)," *Microsoft TechNet Articles*, 13 Aug 2012, https://social.technet.microsoft.com/wiki/contents/articles/12984.understanding-processor-processor-time-and-process-processor-time.aspx.

2 Grant Fritchey, "Disk Performance Analysis," *SQL Server*, 2017, Query Performance Tuning, https://doi.org/10.1007/978-1-4842-3888-2.

3 Flavio Muratore, "Windows Performance Monitor Disk Counters Explained," *Microsoft Ignite*, 2012, https://blogs.technet.microsoft.com/askcore/2012/03/16/windows-performance-monitor-disk-counters-explained/.

4 Mohammed A. Alnatheer, "Secure Socket Layer (SSL) Impact on Web Server Performance," Journal of Advances in Computer Networks 2, no. 3 (2014): 211-217.

5 Jerry L. Rosenberg, "Measuring and Monitoring NT Performance," *CMG Conference, 2001*.

6 Ilker Kara, "Detection, Technical Analysis and Solution of Teslacrypt Ransomware Virus," *International Journal of Management Information Systems and Computer Science* 2, no. 2 (2018): 87-94.

7 "Dell Secureworks Counter Threat Unit Threat Intelligence," Threat Analysis report on *TeslaCrypt Ransomware,* May 12, 2015, https://www.secureworks.com/research/teslacrypt-ransomware-threat-analysis.

[8] Ade Kurniawan and Imam Riadi, "Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior," *International Journal of Network Security* 20, no. 5 (2018): 836-843, https://doi.org/10.6633/IJNS.20180920(5).04.

[9] Savita Mohurle and Manisha Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," *International Journal of Advanced Research in Computer Science* 8, no. 5 (May-June 2017), https://doi.org/10.26483/IJARCS.V8I5.4021.

[10] Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin R.B. Butler "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *IEEE 36th International Conference on Distributed Computing Systems*, 2016.

[11] Counter Threat Unit Research Team, "Threat Analysis report on WannaCry," May 18, 2017, https://www.secureworks.com/research/wcry-ransomware-analysis.

[12] Christian Olbrich, "A Close Look at Ransomware by the Example of Vipasana," October 7, 2016, https://www.boxcryptor.com/en/blog/post/a-close-look-at-ransomware-vipasana-part-i/https://www.boxcryptor.com/en/blog/post/a-close-look-at-ransomware-vipasana-part-i/.

About the authors

Dimo **Dimov** holds a master's degree from the Technical University of Sofia (2013) and is currently PhD student at the Nikola Vaptsarov Naval Academy since 2016. He has experience as an engineer or senior consultant for enterprise wise organization Coca Cola HBC, Hewlett-Packard Enterprise, ATOS, and currently – as cybersecurity analyst for Bulgaria's Air Traffic Services Authority. He is certified Security and Microsoft expert – CISSP (ISC2), SSCP (ISC2), CEH (EC-Council), ISO27001, MCSE, MCSA, MCP.

Dr. Yuliyan **Tsonev** is Colonel, Associate Professor at the Nikola Vaptsarov Naval Academy in Varna. He graduated from the Artillery and Air-Defence Academy in 1986 with major in "Military Cybernetics" with honours. He leads the IT department of the Naval Academy since 2014.