The Impacts of DNS Protocol Security Weaknesses

Willian A. Dimitrov and Galina S. Panayotova
University of Librarian Studies and Information Technologies, Sofia, 1784, Bulgaria
Email: v.dimitrov@unibit.bg, panayotovag@gmail.com

Abstract**—**Global DNS infrastructure is a major component for the services exposed in the internet. The purpose of the study is understanding the cyber security status of DNS ecosystem. As part of the research, a statistical analysis based on vulnerability repositories has been created to provide a view toward the level of DNS security in general. It can help organizations to understand, assess and mitigate DNS risks. It's made short review of most used attacks against DNS and mitigation: amplification, reflection, floods, DNS exploits, and analysis for the DNS security incidents trend. The statistics implicitly reflect the degree of adoption of new DNS security standards and technologies.

Index Terms**—**Attack, cyber, DNS, security, weakness dnsdumpster

I. Scope of the Protocol DNS Security

Cybercrime is steadily accompanying the explosive growth of the information space. One of the deep problems of this process is the security state of the DNS protocol.

DNS is the backbone of the Internet. Many other assets in the digital world depend on the DNS. This service supports the operation of all network applications. It is an invariable element in their architecture. The operation of many exchange protocols depends on the DNS. For example HTTP (Hypertext Transport Protocol), SMTP (Simple Mail Transfer Protocol), MTA (Message Transfer Agent), SIP (Session Initiation Protocol), VoIP (Voice over IP), FTP (File Transfer Protocol). The list is large and includes protocols that have been created in recent years, for example, 5G.

Problems in the operation of DNS lead to disruption of network services and applications. This necessarily has an adverse effect on institutions and businesses. The consequences are spreading through supply chains. If a successful hacker attack on the ISP (Internet Service Provider) stops the DNS service, then all customers of the provider experience a business interruption.

Basic network services were implemented a long time ago. Then ICT (Information and Communication Technologies) security perceptions did not have contemporary meaning. For example, ARP (Address Resolution Protocol), DHCP (Dinamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol), and PXE (Preboot Execution Environment) are known for their poorly cyber protection. PXE can be used if a user can access the BIOS configuration. These services work before others exist. The compromise of basic network services can lead to global implications for the whole ICT infrastructure. In addition to outdated protocols, the weaknesses of DNS are also reflected in advanced technologies. This could lead to reduced trust in the security of Cloud environment, Artificial Intelligence (AI), Virtual Reality and Augmented Reality (VR/AR), Distributed Ledger Technology (DLT), Containers, Microservices and Microfunctions.

The purpose of this paper is to analyze the scope of DNS weaknesses impact. In order to achieve this goal, we present the necessary background knowledge on DNS security and malicious activities leveraging DNS.

The question our research answers is "What is the extent of the threat surface that arises under the influence of DNS weaknesses?" The threat surface covers the multitude of all vulnerabilities. It includes infrastructure weaknesses too. We consider that certain aspects of this impact have been poorly studied.

In our view, the weaknesses in the ecosystem of this protocol are behind all malicious activities using DNS. The review of the attacks on DNS is based on this idea [1].

DNS intersects entire internet infrastructure and applications delivery. Continuous DNS attacks demonstrate true weaknesses in the DNS ecosystem that served as a wakeup call for the states governments and supply chain partners [2].

Security disadvantages of the DNS are analyzed in [3], [4]. DNS roots are controlled by ICANN (Internet Corporation for Assigned Names and Numbers), a non-profit organization with roots tied in one country. This challenges the concept of net neutrality. DNS queries usually don't carry any information about the clients who initiated it.

DNS is a highly sensitive part of every ICT system. If attackers can take control of DNS it would give them unlimited possibilities to abuse the organization at different aspects. DNS is a key component in the concept of multilayered security.

II. Methodology of the Study

We have made an analysis of the current state of the DNS by aggregating data from institutional sources and arrays of leading companies in the cybersecurity industry. The classification of attacks against DNS is based on scientific publications and reports from corporate laboratories. For data aggregation we use National

Manuscript received March 6, 2020; revised September 4, 2020.
Corresponding author email: panayotovag@gmail.com
doi:10.12720/jcm.15.10.722-728

Vulnerability Database (NVD), Common Vulnerability Enumeration (CVE), Common Vulnerability Scoring System (CVSS), exploit-db, bugtrack, vulners.com. To realize the goal of the study we leaned back on empirical experience from many in the IT industry and telecommunications, creating solutions for cyber protection of complex ICT (Information and Communication Systems), discussions in direct contact with developers of companies introducing new forms of DNS protocol protection. The last section provides a brief critical analysis of the applicability of advanced security modifications of DNS in interoperability and change management in corporate environments.

Our contribution is added knowledge of the scope of the impact of security weaknesses in the DNS protocol.

III. DNS from the Viewpoint of Security

The main Internet protocols were created without security requirements. The current situation with various crimes and abuses in to digital space is due to this fact. It's hard to add security features after so much time and in the huge park with technologies already installed. The DNS is deceptively simple and often underutilized as a security tool. There is a wealth of possibilities that can be used. 1) As an early warning system to predict new targeted attacks. 2) For mitigation against attacks utilizing the DNS infrastructure. 3) Implementing DNS as a security tool [5].

Threat actors need to establish an infrastructure to conduct their attacks, and the main element is DNS. A piece of malware may include a hardcoded domain name that is seemingly legitimate. To execute an attack, a threat actor may change that domain’s DNS record to resolve to a malicious IP to deliver a payload or to encrypt data through ransomware.

Attackers create an infrastructure to originate their attack as well as set up servers to communicate with their malware. Often, attackers register multiple domains at the beginning of an attack campaign for use during all phases of their operations. Using domain registration information, an organization can unmask an attacker’s infrastructure by linking a suspicious domain to other domains registered using the same or similar information.

An example of a virtualization dynamics problem is the re-assignment of an IP address. Once the client frees an IP address, the DNS immediately uses it and assigns it to another client's resource. From this point on, the old user on the same IP address cannot tell that network access to his resource has been terminated. Following are periods of DNS server caches update, the ARP tables and their corresponding caching schedules expire. This means that there is a period of time in which the network interface of the virtual machine of the previous user of the IP address is available [6].

We separate DNS weaknesses in two classes: those due to protocol and infrastructure vulnerabilities. The infrastructural ones include the weaknesses due to the construction of the Internet, the related dependent protocols, the innovative proposals for encryption of DNS, supply chain risks, the algorithms for generating domain names and the arrays with names of malicious domains.

A. *The Scope of DNS Vulnerabilities Exposure*

Sometimes the attack surface is increased out-of-band. This means that organization might open up to an attack which didn’t consider. The use of external DNS resolution services leads to internet exposure. This leads to the risk that most organizations don`t realize. It is an attack surface added to the one that the remaining assets in the companies create. External DNS transactions are rarely protected from surveillance, and while such protection is now being developed, that protection will come in the form of added complexity. This paradox of cybersecurity is famous. The attack surface increase after implementation of cybersecurity solutions or additional technologies.

The best way to avoid having one's DNS transactions observed, tracked, or analyzed by third parties is to not externalize those transactions in the first place [7].

An intersection in MITRE ATT@CK Navigator shows the types of techniques used from malicious actors against DNS. The types are Domain Fronting, Endpoint Denial of Service, and Exfiltration over Alternative Protocol, LLMNR/NBT-NS Poisoning and Relay, Network Denial of Service, Standard Application Layer Protocol. In this list Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Windows protocols based on DNS.

B. *The Usual Ways Attackers Use DNS*

The most commented are uses of **DNS as a covert communication channel to bypass firewalls and DoS (Denial of Service).** Attacker tunnels other protocols like SSH (Secure Shell) within DNS. This enables attackers to easily insert malware, pass stolen data or tunnel IP traffic without detection. A DNS tunnel can be used as a full remote control channel for a compromised internal host.

Weaknesses in UDP multiply the effect of DoS attacks. There exist just a few companies that offer DNS Intelligence solutions. Farsight Security passive DNS data is considered the industry standard and has played a key role in advancing cyber investigations, both high-profile and cloaked, protecting brands and preventing cyberattacks from zero-days. They demonstrating DNSDB using Maltego, Chrome and Firefox, and Newly Observed Domains (NOD) tool [8].

Early Protection from Unknown Domains. New domains are created and published every day as part of the Domain Name System (DNS) – but not all of them are created for legitimate purposes. Bad actors use new domains for criminal activities such as spam, malware distribution or botnets in the first minutes of creating them.

Security teams need real-time information regarding new domain usage so that they can apply rules to block access until security providers have time to analyze the domains – and threats can be avoided. Security analysts don’t have a way to gather and analyze this information in a timely manner because it is broadly distributed across name servers around the world [8].

Large-scale spam campaigns often are conducted using newly-registered domains or hacked email addresses, or throwaway domains. The trouble is, spam sent from these assets is trivial to block because anti-spam and security systems tend to discard or mark as spam any messages that appear to come from addresses which have no known history or reputation attached to them. However, in both the sextortion and bomb threat spam campaigns, the vast majority of the email was being sent through Web site names that had already existed for some time, and indeed even had a trusted reputation. Not only that, but new research also shows many of these domains were registered long ago and are still owned by dozens of Fortune 500 and Fortune 1000 companies. That’s according to Ron Guilmette, a dogged anti-spam researcher. Researching the history and reputation of thousands of Web site names used in each of the extortionist spam campaigns, Guilmette made a startling discovery: Virtually all of them had at one time received service from GoDaddy.com, a Scottsdale, Arizona based domain name registrar and hosting provider [9].

External public servers offer malicious actors the ability to create DNS content to serve their online crimes.

Adversaries abused the high potential of massive DRDoS (Distributed Reflection Denial of Service) attacks recently. The bandwidth amplification factor (BAF) computes the bandwidth multiplier in terms of a number of UDP payload bytes that an amplifier sends to answer a request, compared to the number of UDP payload bytes of the request. The packet amplification factor (PAF) is the packet multiplier in terms of a number of IP packets that an amplifier sends to answer a request. [10].

In May 2012, attackers targeted a real-time financial exchange platform with a 167 Gb/s DRDoS attack. In March 2013, attackers launched 300 Gb/s DRDoS attack against Spamhaus.org. In August 2013, presumably politically-motivated attackers brought down Green Net, an ISP hosting human rights groups, with a 100 Gb/s DRDoS attack. In these known examples, attackers abused open DNS resolvers to amplify their attack traffic. The attackers issued specially-crafted ANY requests to thousands of open resolvers and specified the victim’s IP address as packet source. In turn, after successful name resolution, the resolvers sent several-kilobyte-large responses to the victim, exceeding its bandwidth capacity. With these attacks, DNS has been practically proven to be vulnerable to DRDoS abuse. One of the reasons for this vulnerability is the recent deployment of EDNS0 and DNSSEC, which significantly increases the DNS response sizes [10]. As a consequence, developers and administrators increasingly harden DNS servers against abuse, e.g., by closing millions of open resolvers and limiting the request rate per client. However, DNS is not the only widely-deployed service, and little is known about angles for amplification of other popular network protocols.

Network operators have become aware of this kind of abuse and the number of open DNS resolvers is gradually decreasing. However, there is an increasing number of authoritative name servers that include larger resource records in their responses. One of the reasons is the deployment of DNSSEC [11], in which each resource record is accompanied by a typically 1024-bit-wide signature in a special RRSIGrecord.

With the increase in the number of connected devices from the Internet of Things, the entry of robots, AI, AR/VR, containers, and microservices, **the amount of external traffic can be saved by installing an internal DNS server.** Internal DNS service allows additional benefits for DAST (Dinamic Application Security Testing), because of possibilities for debugging port 53 traffic.

C. *The Attacks Using DNS Weaknesses*

Hackers rely on DNS and domain names just like everyone else. Threat actors need to establish an infrastructure to conduct their attacks, and one of these infrastructure elements is often DNS. For example, a piece of malware may include a hardcoded domain name that is seemingly legitimate. To execute an attack, a threat actor may change that domain’s DNS record to resolve to a malicious IP address to deliver a payload or to encrypt data through ransomware. Attack scenarios include infrastructure to host staging, command and control, and exfiltration destinations. To varying degrees, attackers may use compromised assets of other unwitting organizations or infra-structure they directly control. But they have to be ready to move when their virtual hideout is discovered, shutdown or added to a threat Intel list. The IP addresses of their C&C (Command and Control) servers and related infrastructure may change frequently. They use the same technology everyone else uses to find the current IP address for a given resource – domain names.

Even if they didn’t have to worry about IP addresses changing, it’s difficult to stay under the radar if phishing emails and other links are bare IP addresses. The bad guys rely on DNS and domain names just as much as the honest world. And that’s a weak spot we can exploit. Often, attackers register multiple domains at the beginning of an attack campaign for use during all phases of their operations.

Transport-layer attack vectors. DNS water torture: This technique tricks an ISP’s recursive DNS server into launching an attack on a target’s authoritative DNS server. In this technique, infected IoT devices send to the ISP’s DNS resolver a small number of well-formed DNS queries that contain the target domain name prefixed with random values (for example, 123.targetdomain.com, 124.targetdomain.com, xxx.targetdomain.com). The ISP's DNS server sends these requests to the target's authoritative DNS server. Once the authoritative DNS server is flooded with such queries from the ISP's DNS server, it becomes unresponsive to the ISP's DNS server. The ISP's DNS server then automatically retransmits the DNS queries to additional authoritative DNS servers.

DNS amplification attacks. DNS participates in a lot types of attack described in [12]. The DNS amplification DDoS malware is written in C, the bot agent has a small binary's size and relies on its own obfuscation and packing algorithm, all the communication to the C&C are encrypted making more resilient the botnet.

The service includes a built-in DNS scanner; the feature allows the scanning for misconfigured DNS servers to recruit for the attacks. The price for the DNS amplification DDoS service is $2,500, the vendor also offers further options including bulletproof hosting for control server and the option to host the actual archive, encrypted, on a server of choice based on the customer's preferences [12].

DNS hijacking attacks. A proof from ENISA Report DNS states that this type of attack is used to spread malicious mobile applications [13].

Tthrough dns hijacking email in transit can be intercepted.

NXDOMAIN attacks is a simple methods where attackers would send a flood of queries to a DNS server to resolve a non-existent domain name. After that flood the DNS server disappear from internet. New technologies for caching prevent this type of attack. This caused attacker to change tactics. Sophisticated version use phantom domains and name servers that are set up as part of the attack. They also prepend randomly generated subdomain strings to DNS requests. It again means they requests subdomains that don't exist. The volume and type of attack is depends from target. It can be either the recursive DNS server or the authoritative server of a target domain. For the recursive server the goal is to consume available resources of the server and pollute the cache with NXDOMAIN results. For the authoritative server of another legitimate domain, it causes DdoS, impact performance [14].

Zero-Day Vulnerability attacks with exploits takes advantage of DNS security holes in software for which no solution is currently available.

DNS-based Exploits attacks exploiting bugs or flaws in DNS services, protocol or on operating system running DNS services.

Protocol Anomalies is DNS attacks based on malformed queries intending to crash the service.

DNS Rebinding is a combination of javascript and IP subnet discovery in order to attack local network IP devices through the browser. This attack is mainly used for discovery of unsafe devices (targeting IoT) on the network, and for data exfiltration.

DNS covert channel and DNS tunneling attacks are similar. Without going into the differences, it is necessary to specify that this class of attacks is developed by malicious actors and researchers from the beginning of the century. In 2004, Dan Kaminsky demonstrated the feasibility to bypass restricted networks that allow all DNS traffic [15]. Today already exists the famous tools OzymanDNS, NSTX, iodine,

Cache poisoning adversaries trick a resolver to accept fraudulent DNSrecords as legitimate responses from authoritative name-servers. DNS cache is intrinsically vulnerable to record injection because a recursive resolver cannot ensure whethera received response is from a legitimate authoritativenameserver or a miscreant entity. [16]

Redirection Hijackinging Content Delivery Networks. Domain fronting technique takes advantage of routing schemes in Content Delivery Networks (CDNs) and other services which host multiple domains to obfuscate the intended destination of HTTPS traffic or traffic tunneled through HTTPS. [1] The technique involves using different domain names in the SNI field of the TLS header and the Host field of the HTTP header. [17]. Attackers use Tor plugin that tunnels communications with Tor through HTTPS connections to to hide the destination of C2 traffic [18].

Attackers use Domain Generation Algorithm (DGA) so that they can quickly switch the domains that they're using for the malware attacks. Attackers do this because security software and vendors act quickly to block and take down malicious domains that malware uses. Attackers developed DGA specifically to counter these actions [19].

Avant-garde attacks using DNS. Here we include sophisticated malicious methods with participation of state-of-the-art technologies. Fbot tracking Crypto mining Botnets is new type of malicious DNS utilization. At the end of 2018, researchers from Netlab observed a new botnet activity with three specific interesting characteristics: aimed at removing crypto mining related malware/botnets, using blockchain based DNS to resolve C2s (Command and Control) servers and quite bounded to the original Satori botnet.(*) Another refined attack is a covert channel in TTL field of DNS packets [20].

The scope of the opportunities that DNS provides to hackers can be judged by their actions in certain situations. In times of crisis, malicious actors create huge amounts of new domains. These domains are designed to service their operations. A recent example is Covod-19 crisis. From 9 March 2020 to 26 April 2020, Unit 42 fro Palo Alto Network analyzed 1.2 million newly registered domain names containing keywords related to the COVID-19 pandemic. 86,600+ domains were classified as "risky" or "malicious", spread across various regions.

On average, 1,767 malicious COVID-19 themed domains were created every day [21].

D. Malicious Activity Utilizing DNS

Malicious actors utilize DNS for payload distribution, DDoS, criptojacking, data exfiltration, ransomware, and BEC (Business Email Compromise). The visibility and control over internal and external DNS traffic are different from the viewpoint of security. DNS directional policy management allows the control of the DNS resolution path. This makes it easier to manage complicated hybrid infrastructures through a simple action. Instead setting up and maintaining complicated and customized DNS resolvers and forwarders. DNS based security transcends the traditional idea that security barriers are effective against network intrusions. By monitoring and controlling every part of the network and casting equal suspicion on abnormal activity regardless of where it originates. DNS based security covers the entire enterprise with strong, enforceable policies that dramatically minimize the operational space for malicious activity.

Adversaries abused the high potential of massive DRDoS attacks recently. In May 2012, attackers targeted a real-time financial exchange platform with a 167 Gb/s DRDoS attack. In March 2013, attackers launched 300 Gb/s DRDoS attack against Spamhaus.org [22]. In August 2013, presumably politically-motivated attackers brought down Green Net, an ISP hosting human rights groups, with a 100 Gb/s DRDoS attack. In these known examples, attackers abused open DNS resolvers to amplify their attack traffic. The attackers issued specially-crafted ANY requests to thousands of open resolvers and specified the victim’s IP address as a packet source. In turn, after successful name resolution, the resolver sent several-kilobyte-large responses to the victim, exceeding its bandwidth capacity. With these attacks, DNS has been practically proven to be vulnerable to DRDoS abuse. One of the reasons for this vulnerability is the recent deployment of EDNS0 and DNSSEC, which significantly increases the DNS response sizes. As a consequence, developers and administrators increasingly harden DNS servers against abuse, e.g., by closing millions of open resolvers and limiting the request rate per client [23]. However, DNS is not the only widely-deployed service, and little is known about angles for amplification of other popular network protocols.

Network operators have become aware of this kind of abuse and the number of open DNS resolvers is gradually decreasing. However, there is an increasing number of authoritative name servers that include larger resource records in their responses.

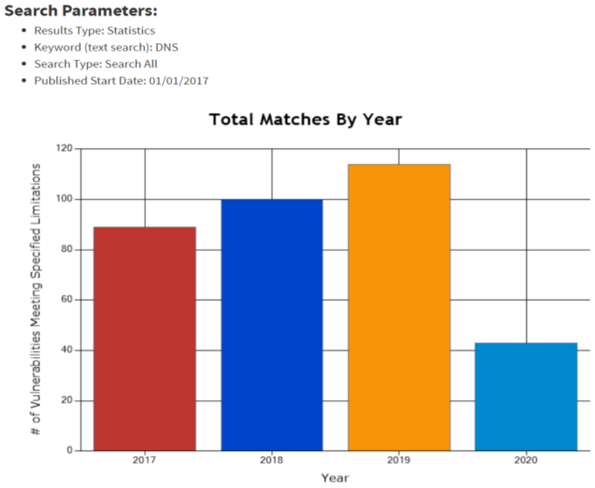
One of the reasons is the deployment of DNSSEC [23], in which each resource record is accompanied with a typically 1024-bit-wide signature in a special RRSIG record.

Other approaches for securing DNS: DNS-over-TLS (DoT); DNS-over-HTTPS (DoH); Do53; Recursive DoT (RDoT); Authoritative DoT (ADoT); Applications Doing DNS (ADD); DNSCurve–DNSCrypt–DNS; Hop-by-hop authentication. In general all they are channel security mechanisms.

DNS attacks against advanced technology-based applications based on DLT are analyzed in the publications [24] and [25].

E. Analysis of the DNS Security Vulnerabilities Trends

The intersection in nvd.nist.gov (see Fig. 1.) show DNS vulnerabilities for last years.



Search Parameters:

- Results Type: Statistics
- Keyword (text search): DNS
- Search Type: Search All
- Published Start Date: 01/01/2017

Fig. 1. DNS vulnerabilities from last years

The trend of increasing vulnerabilities in DNS is sustainable (see Table I). The cross section also includes hits for encrypted versions of DNS.

TABLE I: INCREASING RECORD ABOUT DNS IN NVD

Year	Matches	Total	Percentage
2016	11	6,447	0.17%
2017	89	14,645	0.61%
2018	100	16,514	0.61%
2019	114	17,307	0.66%
2020-05-12	43	7,342	0,59%

Number of vulnerabilities according intersection with key strings from first row in Rapid7 site are presented on Table II. The number of DNSSEC vulnerabilities is a part of total number of DNS vulnerabilities.

TABLE II: A NUMBER OF VULNERABILITIES ACCORDING RAPID7

DNS	DNSSEC	EDND0	DNSCrypt	DoT
1450	186	9	1	437

The pressure upon DNS providers comes from many sides: law regulation for security and confidentiality; the emerging advanced technologies, increased law and business requirements. Including those for cyber security insurance services. The attention to security of DNS lags behind the innovation of hybrid application based on cloud infrastructure. It, creating cracks for possible exploitation. DNS traffic encryption is part of the efforts to remove pure text from internet traffic. This leads to the need to investigate unknown complications related to crypto key management [26], [27], productivity and changes in the regulatory framework. Managing DNSSEC keys can be complex, costly and time-consuming, as security teams must manually generate, administer and validate the many DNSSEC keys required by an organization. This effect amplifies because of complicated DNS supply chain relations and a lack of enough security experts.

The results from searches with a string “CDN DNS” in exploit repositories shows the next numbers exploit.db: 174, and bugtrack:150. We recommend a future researches of weaknesses that are die to the mass entry of CDN.

IV. Conclusions

Our holistic view over DNS weaknesses shows the need for understanding the width and depth of risks related to this protocol. **We introduce the concept for the multidimensionality of DNS security.** The main dimensions are shown in Fig. 2.

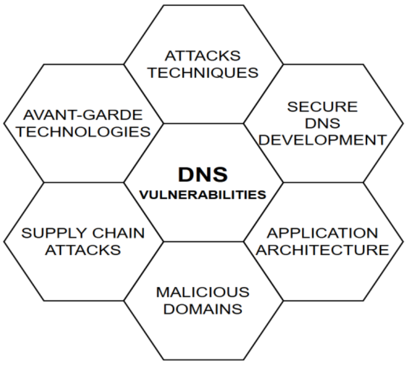


Fig. 2. A holistic view on impact of DNS vulnerabilities

Perimeter network security was evolved to zero-trust strategy. DNS security together with threat intelligence is a basis of successful zero-trust strategy.

Just a few companies offer dns intelligence solutions today. Farsight security passive dns data is considered the industry gold standard and has played a key role in advancing cyber investigations, both high-profile and cloaked, protecting brands and preventing cyberattacks from zero-days. They demonstrating dnsdb using maltego, chrome and Firefox, as well as showcase our newly observed domains (NOD) tool. Operating the local DNS resolution servers is one of the simplest and lowest-cost things an IT administrator can do to monitor and protect applications, services, and users from potential risks; Building DNS Firewalls with Response Policy Zones (RPZ).

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

W. Dimitrov concuted the research; G. Panayotova analyzed the data and wrote the paper. All authors had approved the final version.

Acknowledgment

This work was supported in part by a grant from PPNP-2020-18 “Analysis and research of non-parametric data systems from the Internet of Things ecosystems”.

References

[1] F. Zou, S. Zhang, W. Rao, and P. Yi, “Detecting malware based on DNS graph mining,” *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–12, 2015.

[2] R. Trifonov, G. Pavlova, R. Yoshinov, and B. Jekov, “Methodology for assessment of open data,” *International Journal of Computers*, vol. 2, pp. 28-37, 2017.

[3] J. Bushart and C. Rossow, “Dns unchained: Amplified application-layer dos attacks against dns authoritatives,” in *Research in Attacks, Intrusions, and Defenses*, M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis, Eds. Cham: Springer International Publishing, 2018, pp. 139–160.

[4] M. K. Speaker. (2019). Early Detection of Malicious Activity—How Well Do You Know Your DNS? RSA Conference. [Online]. Available: https://-www.rsaconference.com/videos/early-detection-of-malicious-activityhow-well-do-you-know-your-dns

[5] S. K. Tim Mather and S. Latif, Cloud Security and Privacy, S. K. Copyright B© 2009 Tim Mather and S. Latif, Eds. O’Reilly Media, Inc., 1005 Gravenstein Highway North, Se-bastopol, CA 95472, 2009.

[6] Tripware. (2014) Unbalanced Security is Increasing Your Attack Surface the State of Security. [Online]. Available: https://www.tripwire.com/state-of-security/featured/-unbalanced-security-increasing-attack-surface-2

[7] P. Vixie. (2018) Benefits of DNS Service Locality. [Online]. Available: https://¬www.darkreading.com/¬vulnerabilities—threats/-benefits-of-dns-service-locality/¬a/¬d-id/¬1333088

[8] B. Jekov, P. Petkova, and E. Shoikova, “Blockchain in the Telecom Industry,” in *Proc. XXVI Conference Telecom*, Sofia, Bulgaria, 2018, pp.110-115

[9] B. Jekov, P. Petkova, E. Shoikova, and S. Denchev, “Conceptual modeling of DLT and Blockchain for transforming public administration,” in *Proc ICERI 2018*, Seville, Spain, 2018.

[10] G. P. Dimitrov and G. Panayotova, “Aspects of website optimization,” in *Proc. Union os Scientist - Ruse, Book 5, Mathematics, Informatics and Physics*, 2015, pp. 106-114.

[11] G. Panayotova and G. P. Dimitrov, “Modeling and data processing of information systems,” in *Proc. International Conference on Artificial Intelligence and Pattern Recognition*, Sept. 19-21, 2016.

[12] X. Lin, L. Lei, Y. Wang, J. Jing, K. Sun, and Q. Zhou, “A measurement study on linux container security: Attacks and countermeasures,” in *Proc. 34th Annual Computer Security Applications Conference*, New York, NY, USA: ACM, 2018, pp. 418–429.

[13] ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. Final Version 1.0, ETL 2018, January 2019.

[14] INFOBLOX. (2015). Understanding NXDOMAIN Attack Methods. [Online]. Available: https://¬blogs.infoblox.com/¬company/¬understanding-nxdomain-attack-methods

[15] D. Kaminsky, *Black Ops of DNS. InBlack Hat Briefings, LasVegas*, NV, USA, July 2004.

[16] S. Hao, Y. Zhang, and H. Wang, "University of delaware; angelos stavrou, end-users get maneuvered: Empirical analysis of redirection hijacking in content delivery networks, george mason university," in *Proc. 27th USENIX Security Symposium*, Baltimore, MD, USA, August 15–17, 2018.

[17] D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson, "Blocking-resistant communication through domain fronting," *Proc. on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 1–19, 2015.

[18] M. Dunwoody and N. Carr. (September 27, 2016). No Easy Breach DerbyCon 2016.

[19] Threat Brief: Understanding Domain Generation Algorithms (DGA). [Online]. Available: https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/

[20] C. Hoffman, D. Johnson, B. Yuan, and P. Lutz, "A covert channel in TTL field of DNS packets," in *Proc. International Conference on Security and Management*, Las Vegas, NV, USA, July 2011.

[21] 86,600+ malicious COVID-19 domains registered in seven weeks. (2020). [Online]. Available: https://disruptive.asia/malicious-covid-19-domains-registered/

[22] [Online]. Available: https://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016

[23] J. Happa, M. Glencross, and A. Steed, "Cyber security threats and challenges in collaborative mixed-reality," *Frontiers in ICT*, vol. 6, Apr. 2019.

[24] A. Davenport, S. Shetty, and X. Liang, "Attack surface analysis of permissioned blockchain platforms for smart cities," in *Proc. IEEE International Smart Cities Conference (ISC2)*, Sep. 2018.

[25] A. Andrei, Hacking Humans: The Evolving Paradigm with Virtual Reality, 2019.

[26] ICS. (2019). Building DNS Firewalls with Response Policy Zones (RPZ) - BIND 9. [Online]. Available: https://kb.isc.org/docs/aa-00525

[27] Krebson Security. (2019, 8) Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com — Krebs on Security. [Online]. Avail-able: https://¬krebsonsecurity.com/¬2019/¬01/¬bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com

Galina Panayotova is a Doctor of Mathematics and Professor of Mathematical modeling in the State University of Library Studies and Informational technologies, Sofia, Bulgaria and University "Prof. Dr. As. Zlatarov"- Burgas, Bulgaria

Research interests

- Mathematical and Computer Modeling;
- Big Data
- Use of information technologies and applications in education;

Prof. Panayotova is the author of more 110 scientific publications, books and textbooks.

Willian Dimitrov is a Doctor of Information Technologies and Associated Professor of Cyber security in the State University of Library Studies and Informational technologies, Sofia, Bulgaria

Research interests

- Cyber security and complex cyber protection architectures;
- Data analytics;
- Use of information technologies and applications in education;

Assoc. Prof. Dimitrov is the author of more 50 scientific publications, books and textbooks.