THE INVISIBLE INTERNET AND CYBER SECURITY

Ekaterina M. Konstantinova [1], Mihaela A. Karadocheva [2], Tsvetoslav S. Tsankov [3]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", mkaradocheva6@gmail.com*
[3] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", c.cankov@shu.bg*

***Abstract**: Technologies create countless new opportunities, and new products and services become an integral part of our daily lives. For our part, we risk becoming the victim of cybercrime is growing. The internet has a hidden part that is much larger than the one we use. Besides everyday websites we use, there is another huge online space invisible to traditional search engines! This is the dark and unlit part of the Internet that hides computer criminals, hackers, online drug dealers, illegal software and cyber terrorists. There are ways to access it safely or ensure the protection of our personal data in clever ways!*

***Keywords**: Cyber security, Dark Web, Deep Web, I2P, Internet, P2P, Security protocols, Surface Web, Tor*

НЕВИДИМИЯТ ИНТЕРНЕТ И КИБЕРСИГУРНОСТТА

Екатерина М. Константинова, Михаела А. Карадочева, Цветослав С. Цанков

Въведение

Когато повечето хора чуят Интернет, те си представят гледане на видео в стрийминг платформа, четене на новини, теглене на игри или филми, резервиране на стая в хотел. Под повърхността обаче се крие място, където дебнат терористи, престъпници и хора разобличаващи тайни проекти и правителствени грешки [12], [13], [14], [15], [16], [19], [20], [21], [22]. Погрешното разбиране на термини като Darknet, Dark Web и Deep Web е в основата на мистификацията на тъмната страна на Интернет. В света на киберсигурността тези термини се появяват на бял свят с излагането на техники, използвани от киберпрестъпниците за комуникация, сътрудничество и участие в злонамерени дейности. Нужно е по-добро разбиране на този подземен свят и начините на предпазване от кибервредители [1], [2], [3], [6].

Изложение

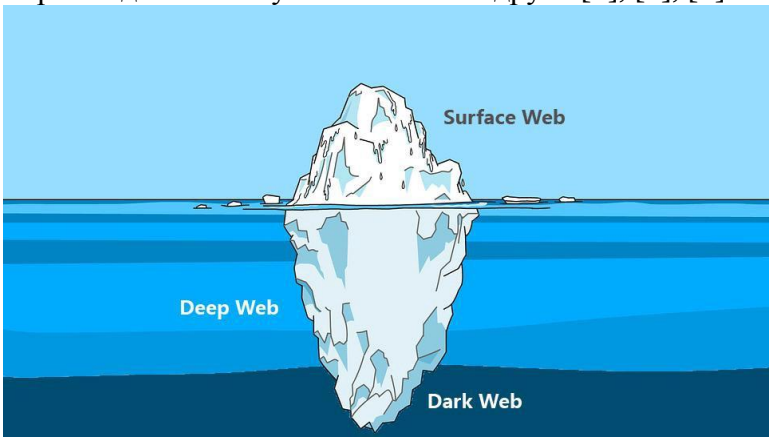
Видима мрежа

Световната мрежа е създадена като платформа за милиарди хора да си взаимодействат чрез Интернет. Най-често срещаната зона в мрежата, която е обществено достъпна, се нарича Surface Web, или Видимата Мрежа. Това включва всички уебсайтове или страници, които могат да бъдат намерени с помощта на търсачки като Google, Yahoo и Bing. Това се случва чрез метод наречен „индексиране”. Индексирането се обяснява най-добре чрез съвременната търсачка Google и нейната здрава, високоефективна система на индексиране. Методите за индексиране на Google до голяма степен разчитат на процес, наречен „обхождане“, който е близък до виртуална паяжина, която обхожда сред множеството страници на уебсайт, до който лесно се достига чрез връзки. Търсачките разполагат с модерни уеб скенери, които събират всички връзки от стотици милиарди уеб страници ежедневно и индексират всяка връзка за оптимизация на търсенето [10], [11], [12], [13], [14], [15], [16], [17], [18]. Процесът на индексиране категоризира всеки уебсайт и техните страници според съдържанието и текста на всяко място. Видимата мрежа включва търсените, индексирани уебсайтове и уеб страници.

Ако уебсайт не е индексиран от търсачка, до него можете да се получи достъп само чрез навигация директно до URL адреса чрез връзка или въвеждане на точния уеб адрес в браузъра. Търсачките имат достъп само до 16% от наличната информация в Интернет [6], [7].

Дълбоката мрежа

Следващото ниво в Световната мрежа е Deep Web, или Дълбоката мрежа (Фиг. 1). Тя е съставена от уебсайтовете или уеб страниците, които не позволяват на търсачките да ги индексират. Това се случва, когато уеб скенери не могат да получат достъп и да събират връзки от тези сайтове; следователно не могат и да ги търсят. Това може да бъде умишлено направено от собственика на уебсайта или страничен ефект поради естеството на уебсайта. Има няколко метода, които могат да се използват, за да запази информацията скрита и да се предотврати индексирането на страниците [1], [2], [3], [4], [5]. Някои от тези методи включват забраната на уебсайт на повърхността не съдържа връзки към страниците, ограничаване на достъпа до страниците чрез технически средства (например CAPTCHA кодове) или изискване за вход за достъп до страници. Добре е да се отбележи, че съдържанието на Дълбоката мрежа не винаги е незаконно и се провеждат множество дейности, които са изцяло в рамките на закона. Примери: социални мрежи, блогове, текстови и гласови чатове; международни турнирни игри (шах и табла); различни нетрадиционни клубове (клубове за края на света, фен клубове, клубове за видеоигри и др.); публична документация и сертификати; индекси на онлайн библиотеки; комуникация чрез криптирани съобщения, за гаранция на поверителността; състезания по караоке и пеене; групи за теории на конспирациите; курсове по компютърни и дигитални умения и много други [1], [2], [7].



Фигура 1: Представяне на мрежите в Интернет пространството

Тъмната мрежа

Dark Web [8], или Тъмната мрежа, е термин, който се използва за описване на криптирана мрежа, изградена под повърхността на Видимия интернет, до която може да се получи достъп само с помощта на специализиран софтуер. Уебсайтове не са индексирани, следователно Тъмната мрежа е част от Дълбоката мрежа. Тази мрежа е описана като тъмна, поради характеристиките си, тъй като помага на потребителите да скрият самоличността си и е популярна при подпомагането на незаконни дейности.

Когато се говори за разликите между Тъмната мрежа и Дълбоката мрежа, нещата добиват различен смисъл, За начало трябва да се спомене, че Тъмната мрежа е малка част от дълбоката мрежа - 0,1%. Основната и цел е да защитава поверителността, използвайки комбинация от маршрутизация и криптиране, и разбира се това може да се използва както за законни, така и за незаконни цели. Въпреки, че имат разлики, Тъмната и Дълбоката мрежа имат и своите прилики (Табл. 1). [2], [3], [6], [7], [13], [14], [15], [19], [20], [21].

Таблица 1: Прилики на Тъмната и Дълбоката мрежа

Вид съдържание	**Описание**
Съдържание с ограничен достъп	Уебсайтове до които се получава достъп само с JavaScript връзки.
Динамично съдържание	Динамични уебсайтове, които използват формуляри за филтриране на достъпа, т.е. captcha.
Страници без входящи връзки	Тези страници блокират роботи на търсачката и възможно индексиране.
Програмно съдържание	Страници, които са достъпни само чрез JavaScript връзки.
Без HTML съдържание	Кодирано мултимедийно съдържание или файлови формати, които не могат да бъдат четени от търсачките, с изключение на програми като TOR.
Частна мрежа	Уебсайтове, където е необходима парола за достъп.
Контекстуална мрежа	Уеб страници, които варират в зависимост от контекста, като използват параметри като клиентски адреси или предишни посещения.

За достъп до тъмната мрежа често е необходимо да се използват нестандартни комуникационни протоколи и портове – програми като Tor и Onion, които са способни да се свързват със структурата на мрежите, които са част от Тъмната мрежа.

Протоколи за сигурност

При сърфиране във Видимата мрежа, криптографският протокол, който осигурява конфиденциалност при комуникация със сървъра, е TLS (Transport Layer Security). Зеленото ключе в URL лента е уверение, но не и гаранция, че общуването е поверително. Докато TLS е проектиран да осигурява сигурност и идентичност, тъмните уеб протоколи са проектирани да осигуряват конфиденциалност и анонимност [8], [9], [10], [12], [16], [17], [18], [19]. Тъмните мрежи могат да бъдат организирани или под формата на мрежи за поверителност, като Tor или Freenet, или в мрежи от партньорски връзки, (като I2P или мрежи P2P) [1], [2], [3], [4], [5]. [11], [12], [13], [16], [17].

Tor

Маршрутизаторът Tor, или The Onion Router е създаден от Американската армия за целите на сигурността. Той достига популярността си поради високото ниво на криптиране, лекотата на използване, а също така и фактът че е безплатен. Целия софтуер може да бъде изтеглен и настроен за минути. Анонимността се постигна чрез маршрутизиране на мрежовия трафик през различни сървъри на Tor, разположени в целия свят. Това означава, че ако някой от пакетите във връзката бъде прихванат, потребителите изглеждат като случайни, отделни възли в мрежата на Tor, което прави идентифицирането им почти невъзможно. За съжаление този процес през прави скоростта значително по-ниска.

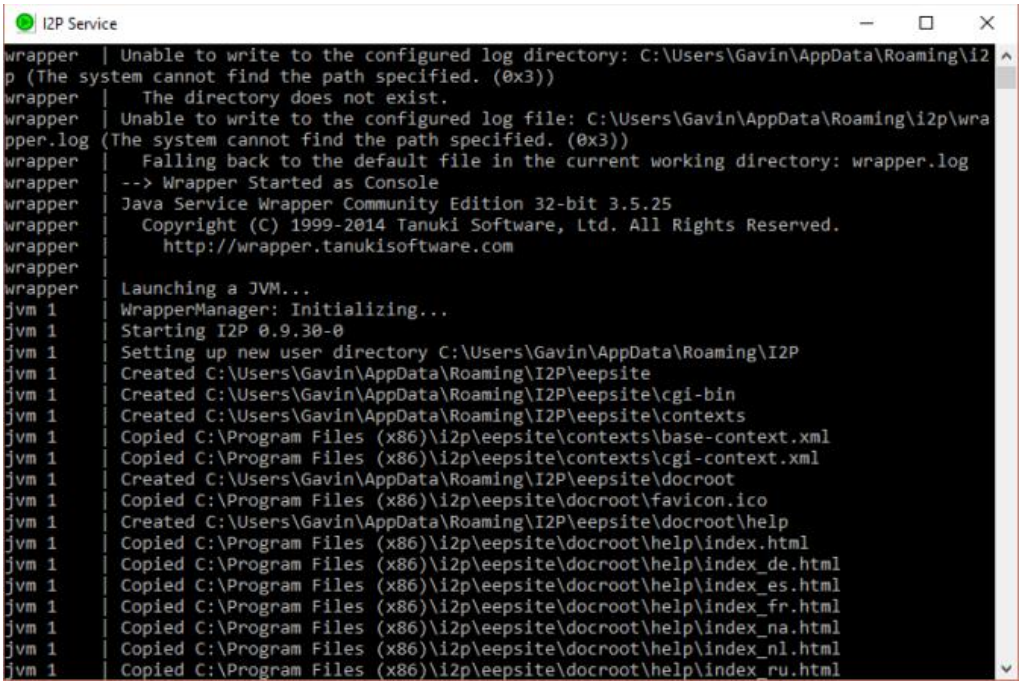
Много уебсайтове могат да бъдат достигнати само с Tor. Те имат домейн от първо ниво „onion“ (TLD), вместо да имат често използваните такива като „.com“, „.edu“, „.net“ и „.org“. Връзките към тези уебсайтове биват приети само от браузъри или приложения, които работят в мрежата Tor. За мобилни устройства това са приложенията Orbot и Orfox или разширения за уеб браузъри.

I2P

Има няколко алтернативни метода за достъп до Тъмната мрежа, като например използването на Invisible Internet Project (I2P). Това е услуга, подобна на Tor, но може да работи в уеб браузъри. Това, което го отличава от другите е целта на използване, която се фокусира върху сърфиране, съобщения или анонимно споделяне.

I2P Service

Invisible Internet Project (I2P) е чеснов протокол за маршрутизация. I2P е „анонимна мрежа със наслагване“. Работи като криптира множество съобщения заедно, за да направи труден анализ на трафика на данни, като същевременно увеличава скоростта му (Фиг. 2). Получава името си от растението чесън. Всяко съобщение е „скилидка“, а целия криптиран пакет е „главата“. Всяко криптирано съобщение има своя специфична инструкция за доставка и всяка крайна точка работи като криптографски идентификатор [8], [9], [10], [11], [12], [13], [14], [15] (прочита един от двойката публични ключове).



Фигура 2: I2P Service

Всеки I2P клиент (маршрутизатор) изгражда серия от входящи и изходящи връзки „тунели“ - директна мрежа „peer-to-peer“ (P2P). Основна разлика между I2P и други P2P мрежи е индивидуалният избор на дължина на тунела. Дължината на тунела е фактор за анонимността, латентността и личната пропускателна способност.

F2F

Мрежата "приятел-приятел" (F2F) е вид партньорска мрежа, която позволява свързването на конкретни пръстени от IP адреси и дава възможност на потребителите да забранят на всякакви други IP адреси да разберат за съществуването им. В допълнение към това, потребителите на F2F могат също да криптират информацията в мрежата, за да подобрят още повече своята сигурност и анонимност.

Заключение

Днес безброй Интернет потребители се опитват да влязат в Дълбоката и Тъмната мрежа. Някои търсят нещо по-специално, което не може да бъде намерено във видимата част на Интернет, а други са просто любопитни [4], [5].

Дълбоката мрежа, Тъмната мрежа и инструменти като Tor са обвити в мистерия. Въпреки сравнително скорошното им създаване, чарът, която притежават, е толкова стар, колкото и самото време. Човешката природа е заинтригувана от това, което не разбира и до което няма достъп.

Разликите между Тъмната и Дълбоката мрежа не се основават само на тяхната видимост, но и на здравословното разпределение на информацията по интернет.

Вярно е, че някои престъпници могат да използват предимството да бъдат почти анонимни в Тъмната мрежа, за да водят незаконни действия и това трябва да бъде спряно възможно най-скоро. От друга страна, без това разделение на управлението на информацията и поверителността, защитата в онлайн пространството би била невъзможна.

References

1. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на Киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни“, Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.
2. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.
3. Nikolov, L., Slavyanov, V. *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, “Vasil Levski” National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.
4. URL: https://digital.com/blog/deep-dark-web/
5. URL: https://www.itbusinessedge.com/articles/what-security-pros-need-to-understand-about-the-dark-web.html
6. URL: https://www.makeuseof.com/tag/i2p-vs-tor-vs-vpn-secure/
7. URL: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/
8. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС” „Новата парадигма за сигурност в киберпространството” Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
9. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни

трудове на Научна конференция „Проблеми на информационната сигурност”, гр. Шумен, 2010, ISSN 1314-0647.

10. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров”, 2012, ISSN 1312-2916.
11. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски“, Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
12. Савова, Ж., Боянов П., Сравнителен анализ на злонамерени уеб-базирани атаки, Научна конференция на тема „Защитата на личните данни в контекста на информационната сигурност”, Факултет "Артилерия, ПВО и КИС" при Националният военен университет „Васил Левски”, гр. Шумен, България, ISBN 978-954-9681-49-9, 6 - 7 Юни 2013, с. 178-183.
13. Boyanov, P., *A novel algorithm for detecting TCP/IP network attacks using hybrid firewall script applied in Linux operating system*, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 57, May 2019, pp. 33-41.
14. Boyanov, P., *Countermeasures against various types of cyber attacks in the context of the protection of the national security of Republic of Bulgaria*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Konstantin Preslavsky University Press, ISSN 1311-834X, Vol. VIII E, 2018, pp. 79-85.
15. Боянов, П., Христов, Хр. *Приложение на кибератаките за получаване на информационни отпечатъци и прилагане на разузнавателни техники срещу правителствени агенции, частни организации и академични институции*, Сборник научни трудове - Научна конференция с международно участие "MATTEX 2018" - 25-27 октомври 2018, ISSN: 1314-3921, т.2, ч.1, 2018, с.23-33.
16. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
17. Savov, I., Edin pogled varhu sashtnostta na kiberprestapleniyata, spisanie „Politika i sigurnost”,VUSI, 2017, ISSN 2535-0358, s. 36-47.
18. Savov, I., The collision of national Security and Privacy in the age of information technologies, European Police Science and Research Bulletin, European Union Agency for Law Enforcement Training, 2017, ISSN 2443-7883, p. 13-21.
19. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
20. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
21. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion*, Sibiu 2007.
22. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.