УДК 004.056.5

Куринный Ф.А., Дейнека Р.С.[1]
Университет таможенного дела и финансов

Программные методы борьбы с распределённым воздействием на информационно- технические сети и телекоммуникационную инфраструктуру Центров обработки информации с целью отказа в обслуживании

В ходе реализации концептуальных норм кибербезопасности в применении к ведомственным сетям различного назначения постоянно изучаются технологические и методологические аспекты борьбы с различными негативными воздействиями на государственные информационные ресурсы. Основной задачей является снижение вероятности негативного воздействия с целью распределённого воздействия на сети и телекоммуникационную инфраструктуру с целью отказа в обслуживании (DDOs).

Одним из оригинальных программных решений, принципы которого могут быть использованы при построении одноранговой ведомственной сети является технология торрентов и блок-чейнов, которая позволяет строить сети без центральных серверов и традиционной доменной и адресной системы.

Идея технологии блокчейн максимально проста — это огромная база данных общего пользования, которая функционирует без централизованного руководства. Эта технология в виде тестового проекта отрабатывается основными мировыми банками. Она позволяет создавать внутренние межбанковские сети и скрывать от мониторинга конкурентов все транзакции. В случае с биткоином (цифровыми межбанковскими деньгами), проверкой транзакций занимаются так называемые майнеры — участники системы, которые подтверждают подлинность совершенных действий, а затем формируют из записей транзакций блоки.

Это обеспечит важный элемент комплексной системы кибербезопасности – отсутствие об'екта воздействия – серверов и традиционных доменов. Вероятность негативного воздействия на сети или их элементы снижается в несколько раз, что подтверждает математическое моделирование и статистическая оценка таких моделей.

В прикладном значении это приемлемо, так как построение одноранговой ведомственной сети регионального органа Таможенной службы при выполнении обмена служебной информации не требует высоких скоростей передачи данных (достаточно 50 Мбит) в реализации служб документооборота и (100 Мбит) в обеспечении видео- стримов служебных камер наблюдения.

Из многообразия программных продуктов оригинальным является продукт, опубликованный на сайте GitHub.com интересный проект — web2web. Он представляет из себя веб-страницу, которая загружает своё содержимое с помощью технологии торрентов и блокчейнов и может работать без центральных серверов и доменов.

Идея создания одноранговой сети существует уже давно, и выглядит она довольно многообещающие.

1. Защита от традиционных форм негативных воздействий несанкционированная авторизация и идентификация. Из-за отсутствие в одноранговой сети серверов и систем массового доступа к базам данных.

2. Низкая вероятность возможности блокировки рессурсов при помощи распределённых Dos атак на ресурсы сети. Провести Ddos воздействие на всех клиентов одноранговой сети невозможно.

[1] *под редакцией доктора технических наук, проф. Мороза Б.И.*

3. Высокая степень вероятности восстановления утерянных данных, так как информационные пакеты распределяются по всем клиентам одноранговой сети. Для стран с жёсткой регуляторной политикой в сфере пользования Интернет — это возможность избегать блокировки интересующих IP адресов и вести скрытый от мониторинга обмен данными.

4. Низкая стоимость хранения данных и большой об'ем виртуального хранилища этих данных. В настоящее время для блокировки передачи данных через торренты необходимо блокировать весь канал. Это намного усложняет и вопросы мониторинга отдельных клиентов.

Важным преимуществом именно этого программного решения, это то что оно совместимо с любыми системами и может работать в любых доступных пользователю браузерах. Это их отличает от аналогичных проектов Maide safe, ZeroNet на основе программного обеспечения BitTorrent. Все эти приложения требуют установки клиентского программного обеспечения и имеют низкую степень защиты от троянских мониторинговых программ.

Неоспоримым достоинством является простота работы с системой:

Вы открываете html-страницу (вы можете получить её любым способом — как по URL адресу, так и с любого носителя информации) любым браузером. На этой странице вы увидите сообщение с просьбой подождать несколько минут. В это время js-скрипт запросит по определённому bitcoin-адресу последнюю исходящую транзкацию, через OP_RETURN. Это скрипт будет содержать информацию для скачивания новой страницы через торрент. После скачивания эта страница заменит собой старую (с просьбой подождать).

Пока существует только proof-of-concept данного проекта, но оригинальный алгоритм позволяет решить большое количество проблем, связанных с кибербезопасностью информационных и телекоммуникационных систем различного назначения требует изучения и создания программно аппаратных решени

Список использованных источников

1. *Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с.*
2. *Eric Vyncke, Christopher Paggen. LAN Switch Security: What Hackers Know About Your Switches? – Cisco Press, 2007. – 340 p.*
3. *D. Kouřil, T. Rebok, T. Jirsík, J. Čegan, M. Drašar, M. Vizváry J. Vykopal. Cloudbased Testbed for Simulation of Cyber Attacks. In Proceedings of NOMS, 2014.*
4. *Jelena Mirkovic, Gregory Prier, and Peter Reiher. Attacking DDoS at the source. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), pages 312–321, 2002.*
5. *John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense against DDoS attack. In Proceedings of the Network and Distributed System Security Symposium (NDSS), 2002.*
6. *Yanxiang He, Wei Chen, Wenling Peng, and Bin Xiao. An efficient and practical defense method against DDoS attack at the source-end. In Proceedings of the 11th International Conference on Parallel and Distributed Systems - Workshops - Volume 02, pages 265–269, Washington, DC, USA, 2005. IEEE Computer Society.*
7. *Lei Liu, Xiaolong Jin, Geyong Min, and Li Xu. Real-time diagnosis of network anomaly based on statistical traffic analysis. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 264– 270, June 2012.*
8. *Haiqin Liu and Min Sik Kim. Real-time detection of stealthy DDoS attacks using time-series decomposition. In Proceedings of IEEE International Conference on Communications 2010, May 2010.*
9. *J. W. Haines, R. P. Lippmann, D. J. Fried, M. A. Zissman, E. Tran, and S. B. Boswell. 1999 DARPA intrusion detection evaluation: Design and procedures. Technical Report 1062, Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusetts, U.S.A., February 2001.*
10. *Haiqin Liu, Yan Sun, Victor C. Valgenti, and Min Sik Kim. TrustGuard: A flow-level reputation-based DDoS defense system. In Proceedings of the 5th IEEE International Workshop on Personalized Networks, Las Vegas, January 2011.*
11. *Tu Xu, Da Ke He, and Yu Zheng. Detecting DDoS attack based on one-way connection density. In Proceedings of the 10th IEEE Singapore International Conference on Communication systems, October 2006.*
12. *Haiqin Liu, Yan Sun, and Min Sik Kim. Fine-grained DDoS detection scheme based on bidirectional count sketch. In Proceedings of IEEE International Conference on Computer Communication Networks, Hawaii, August 2011.*