

Ứng Dụng Natural Language Processing(NLP) Để Thu Thập Tri Thức An Ninh Mạng Trên Trình Duyệt Web

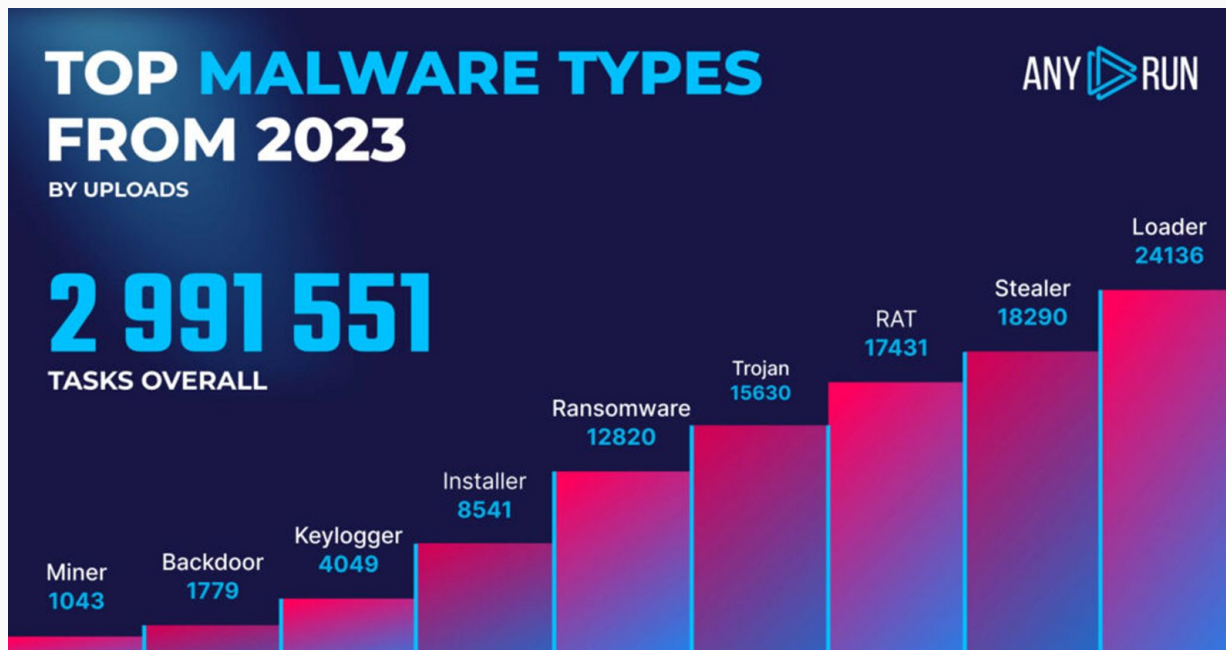
Sử Chấn Hoài Bảo - 230202003

Tóm tắt

- Lớp: CS2205.CH181
- Link Github:
- Link YouTube video:
- Ảnh + Họ và Tên: Sử Chấn Hoài Bảo
- Tổng số slides không vượt quá 10



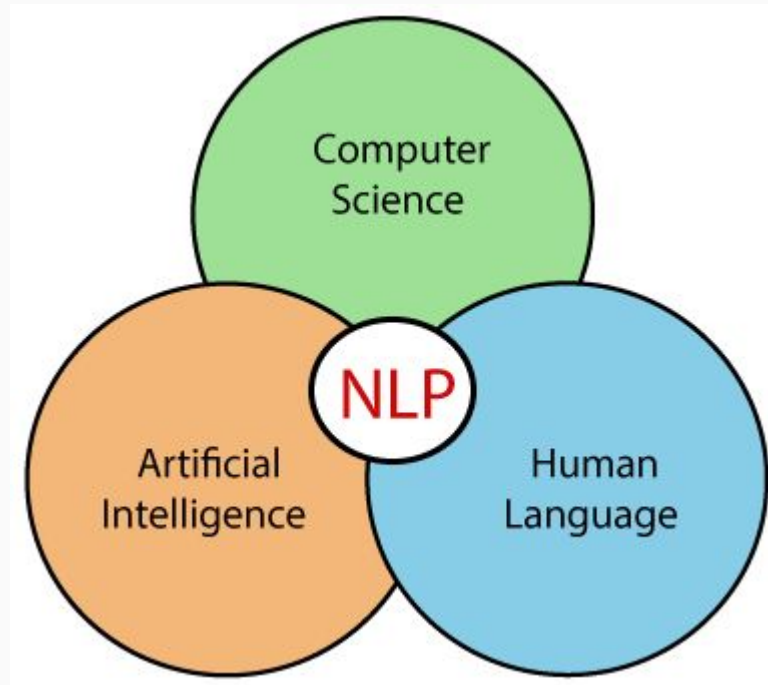
Giới thiệu



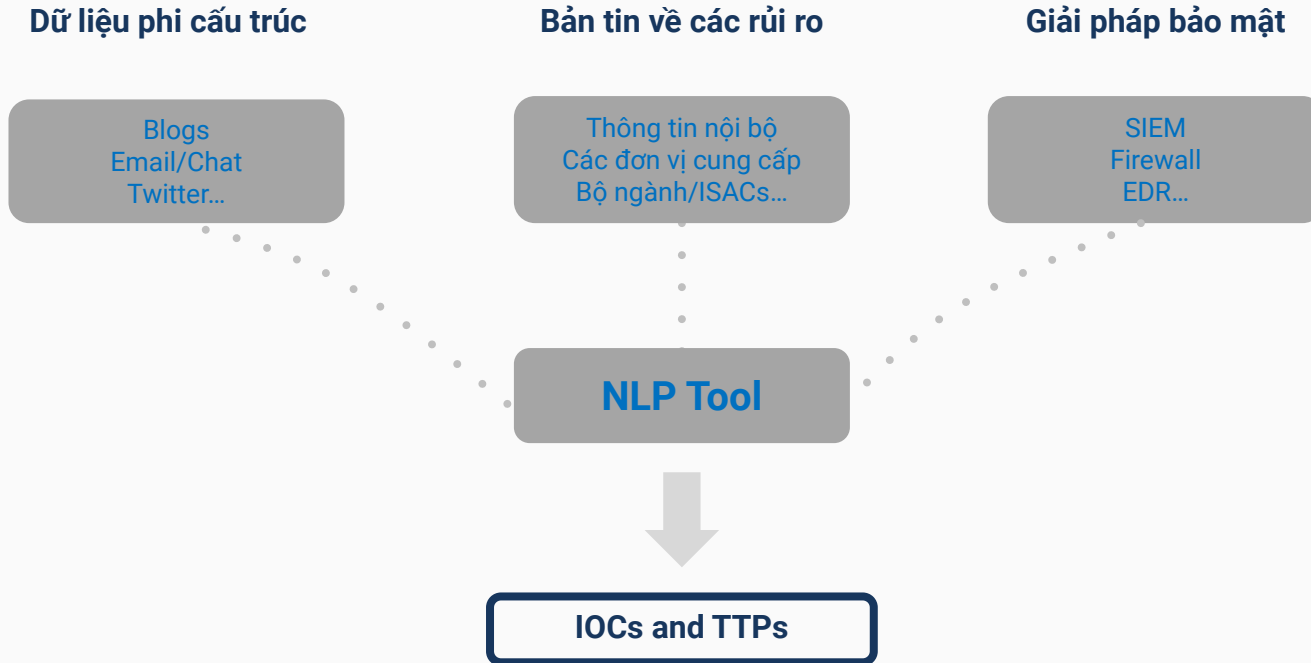
- Ai đang nhắm vào tổ chức của chúng ta?
- Tổ chức của chúng ta có bị tấn công hay chưa?
- Tổ chức của chúng ta đang bị tấn công bằng phương thức nào?

<https://any.run/cybersecurity-blog/malware-trends-2023/>

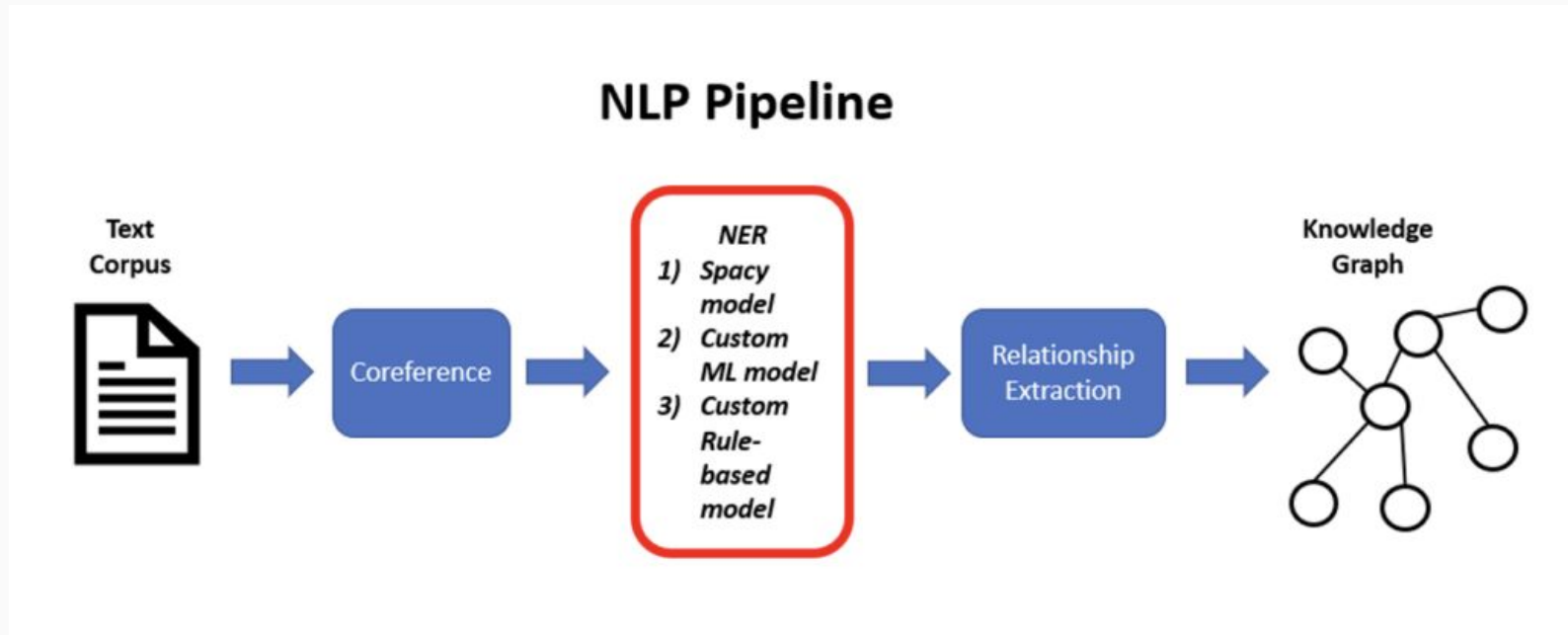
Giới thiệu



Mục tiêu



Nội dung và Phương pháp



Nội dung và Phương pháp

STT	Nội dung
1	Xác định vấn đề và mục tiêu phát triển
2	Thu thập dữ liệu
3	Xử lý dữ liệu
4	Xây dựng mô hình NLP phù hợp
5	Triển khai và đánh giá
6	Tinh chỉnh và cải tiến

Kết quả dự kiến

threatpost Cloud Security / Malware / Vulnerabilities / Privacy / HackerOne Spotlight

Microsoft to Kill Updates for Legacy OS Using SHA-1 GitHub Increases Rewards, Scope For Bug-Bounty Program

Microsoft: Russia's Fancy Bear Working to Influence EU Elections

ACTOR

Sighted in Anomali Enterprise

Severely: High Confidence: 85 C&C type: Type Base Score: 4.6 Exploitability Score: 3.9 Impact Score: 4.6 Version: 2.0

TAGS: APT-28 STONTIUM Sofacy

View in ThreatStream 14 Sightings

As hundreds of millions of Europeans prepare to go to the polls in May, **Fancy Bear** ramps up cyber-espionage and disinformation efforts.

Author: Tara Seals February 20, 2019 / 11:16 am

3:30 minute read

Write a comment

The tech giant said on Tuesday that it has observed a recent series of attacks on organizations "working on topics related to democracy, electoral integrity and public policy and that are often in contact with government officials," including campaigns targeting employees of the German Council on Foreign Relations, The Aspen Institutes in Europe and The German Marshall Fund.

EDITOR'S PICKS

When Cyberattacks Pack a Physical Punch February 20, 2019

Where's the Equifax Data? Does It Matter? February 20, 2019

Ever-Changing Emotes Evolves Again with Fresh Evasion Tactic February 19, 2019

Threatpost Poll Data: Over Half of Firms Asked Struggle with Mobile Security February 14, 2019

ThreatList: Banking Trojans Are Still The Top Big Bad for Email February 13, 2019

Newsletter

Subscribe to Threatpost Today

Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter

WinRAR has patched a serious 19-year-old security flaw on its #Windows data compression platform. 500 million user... https://t.co/110Fj3LbcZ 66 mins ago

Follow @threatpost

10 Entities 0 Matches 8 Active 0 Inactive 2 Unknown

Actor APT 28 Active

TAGS

Reported: 1 feed(s) Tsar Team Threat Group-4127 S... 6 more...

DESCRIPTION

The Advanced Persistent Threat (APT) group "APT28" is believed to be a Russian-sponsored group that has been active since at least 2007. The group displays high levels of sophistication in the multiple campaigns that they have been attributed to, and various malware and tools used to conduct the ope...

View Details

Fancy Bear

Malware (1)

PoetrAT

CVEs (1)

CVE-2020-1472

Tài liệu tham khảo

- [1]. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, et al., “Meltdown: Reading kernel memory from user space,” in 27th { USENIX } Security Symposium ({ USENIX } Security 18), pp. 973–990, 2018.
- [2]. C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, “An analysis and classification of public information security data sources used in research and practice,” Computers & security, vol. 82, pp. 140–155, 2019.
- [3]. B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “Mitre att&ck: Design and philosophy,” Technical report, 2018.
- [4]. M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, “A literature review on mining cyberthreat intelligence from unstructured texts,” in 2020 International Conference on Data Mining Workshops (ICDMW), pp. 516–525, IEEE, 2020.