**Find a dozen news and/or magazine articles about hackers from mainstream media from the past few years.**

Step 1: Hacker news.

First of all, I am not editing the news let us discuss on by one

1.The Iranian government-backed actor known as Charming Kitten has added a new tool to its malware arsenal that allows it to retrieve user data from Gmail, Yahoo!, and Microsoft Outlook accounts.

Dubbed **HYPERSCRAPE** by Google Threat Analysis Group (TAG), the actively in-development malicious software is said to have been used against less than two dozen accounts in Iran, with the oldest known sample dating back to 2020. The tool was first discovered in December 2021.

Charming Kitten, a prolific advanced persistent threat (APT), is believed to be [associated](https://thehackernews.com/2022/05/iranian-hackers-leveraging-bitlocker.html) with Iran's Islamic Revolutionary Guard Corps (IRGC) and has a history of conducting espionage aligned with the interests of the government.

HYPERSCRAPE requires the victim's account credentials to run using a valid, authenticated user session the attacker has hijacked, or credentials the attacker has already acquired," Google TAG researcher Ajax Bash [said](https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/).

Written in .NET and designed to run on the attacker's Windows machine, the tool comes with functions to download and exfiltrate the contents of a victim's email inbox, in addition to deleting security emails sent from Google to alert the target of any suspicious logins.

2. With cybersecurity researchers raising the spectre of a [cyber-attack](http://www.nbcnews.com/news/us-news/white-house-readies-fight-election-day-cyber-mayhem-n677636) on Election Day, state and local officials are doubling down on a different message: no matter what, the final vote will be legitimate.

“If there’s one message we want be heard loud and clear, it’s that these elections will be fair,” Denise Merrill, the president of the National Association of Secretaries of State and the Secretary of State of Connecticut, told TIME. “It might take longer to count every vote, there might be more hurdles, but it’ll be fair.”

In the event that hackers attack voting systems, state and local officials have paper-based back-up plans in place, she said.

In the event that hackers shut down larger targets, like parts of the power grid, government buildings, electrical facilities, water systems, street lights, dams or bridges, all of which are now connected to the internet, state and local election officials can implement other contingency plans, election officials told TIME.

3. The Department of Homeland Security is investigating a hack that exposed Leslie Jones’ personal information and posted explicit photos on her website.

“The investigation is currently ongoing,” the agency told TIME in a statement. “In order to protect the integrity of the case, no further details are available at this time.”

Hackers on Wednesday posted photos of the *Ghostbusters* star’s driver’s license and passport to her website, along with a photo of the gorilla Harambe and [photos of Jones naked](http://motto.time.com/4464720/leslie-jones-hack/).

Jones’ website was taken down after the attack.

4.Grayson Barnes had just started working at his father’s law firm in Tulsa, Oklahoma when a note popped-up on one of the computer screens. It informed him that all the files on the firm’s digital network had been encrypted and were being held ransom. If he ever wanted to access them again, he had to pay $500, in the Internet currency Bitcoin, within five days. If he didn’t, the note concluded, everything would be destroyed.

“It wasn’t just a day’s worth of work,” Barnes told TIME. “It was the entire library of documents, all the Word documents, all the Excel.”

Uncertain of what to do next, Barnes called the police and then the Federal Bureau of Investigations. Everyone he spoke to told him the same thing: there was nothing they could do.

If he paid the $500, there was no guarantee he’d get the files back, they said.

5. A suspected Iranian threat activity cluster has been linked to attacks aimed at Israeli shipping, government, energy, and healthcare organizations as part of an espionage-focused campaign that commenced in late 2020.

Cybersecurity firm Mandiant is tracking the group under its uncategorized moniker **UNC3890**, which is believed to conduct operations that align with Iranian interests.

"The collected data may be leveraged to support various activities, from hack-and-leak, to enabling kinetic warfare attacks like those that have plagued the shipping industry in recent years," the company's Israel Research Team

6. Investigative journalist Brian Krebs, the author of the blog, has exposed — at personal risk — data breaches at Target, Home Depot, P.F. Chang's and many others. His reporting has abbreviated cybercrime schemes that have saved thousands for consumers and helped rescue identities. And he's just getting started. Brian Krebs was hacked! Back in 2001, he was fooling around with an old computer and decided it would be fun to learn Linux and build websites. "But I didn't keep up with the operating system updates, and one day woke up to find the system I was using as my network firewall was compromised by a network worm," he says in an interview with Fraud Magazine. "After that, I became intensely interested in learning everything I could to ensure that such a thing would never happen to me again, and it's an obsession that hasn't released its grip on me yet."

7. Details of an eight-year-old security vulnerability in the Linux kernel have emerged that the researchers say is "as nasty as Dirty Pipe."

Dubbed **[DirtyCred](https://github.com/markakd/dirtycred" \t "_blank)** by a group of academics from North-western University, the security weakness exploits a previously unknown flaw) to escalate privileges to the maximum level.

First, rather than tying to a specific vulnerability, this exploitation method allows any vulnerabilities with double-free ability to demonstrate dirty-pipe-like ability," the researchers [said](https://www.blackhat.com/us-22/briefings/schedule/#cautious-a-new-exploitation-method-no-pipe-but-as-nasty-as-dirty-pipe-27169).

"Second, while it is like the dirty pipe that could bypass all the kernel protections, our exploitation method could even demonstrate the ability to escape the container actively that Dirty Pipe is not capable of."

9. Bitcoin ATM manufacturer General Bytes confirmed that it was a victim of a cyberattack that exploited a previously unknown flaw in its software to plunder cryptocurrency from its users.

"The attacker was able to create an admin user remotely via CAS administrative interface via a URL call on the page that is used for the default installation on the server and creating the first administration user," the company [said](https://generalbytes.atlassian.net/wiki/spaces/ESD/pages/2785509377/Security+Incident+August+18th+2022) in an advisory last week. "This vulnerability has been present in CAS software since version 2020-12-08."

10. Budget Android device models that are counterfeit versions associated with popular smartphone brands are harbouring multiple Trojans designed to target WhatsApp and WhatsApp Business messaging apps.

The malware, which Doctor Web first came across in July 2022, were discovered in the system partition of at least four different smartphones: P48pro, radmi note 8, Note30u, and Mate40, was

"These incidents are united by the fact that the attacked devices were copycats of famous brand-name models," the cybersecurity firm [said](https://news.drweb.com/show/?i=14542&lng=en) in a report published today.

11. Researchers have disclosed multiple vulnerabilities impacting Ultra-wideband (UWB) Real-time Locating Systems enabling threat actors to launch adversary-in-the-middle (AitM) attacks and tamper with location data.

"The zero-days found specifically pose a security risk for workers in industrial environments," cybersecurity firm Nozomi Networks [disclosed](https://www.nozominetworks.com/blog/nozomi-networks-researchers-reveal-zero-day-rtls-vulnerabilities-at-black-hat-22/) in a technical write-up last week. "If a threat actor exploits these vulnerabilities, they have the ability to tamper with safety zones designated by RTLS to protect workers in hazardous areas."

12. Organizations in the Spanish-speaking nations of Mexico and Spain are in the crosshairs of a new campaign designed to deliver the **Grandoreiro** banking Trojan.

"In this campaign, the threat actors impersonate government officials from the Attorney General's Office of Mexico City and from the Public Ministry in the form of spear-phishing emails in order to lure victims to download and execute 'Grandoreiro,' a prolific banking Trojan that has been active since at least 2016, and that specifically targets users in Latin America," Zscaler [said](https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals) in a report.

**How are hackers described, as criminals or heroes? Give examples.**

Step 1:

An individual who employs computer, networking, or other abilities to solve a technological issue is known as a hacker. The phrase can also be used to describe someone who uses their skills to break into systems or networks without authorization in order to commit crimes.

Step 2; Hackers as heroes

The one thing ethical hackers have in common is that they appreciate the mental challenge of ingeniously surmounting obstacles. Hackers are people who embody a specialized set of knowledge, skills, and ethos. They all have a great desire to learn about and explore the internet, and many of them are skilled at spotting potential security holes and weaknesses in various systems. Contrary to popular assumption, these hackers frequently cooperate with one another and share information.

This is not the outmoded, unfavourable picture that we frequently see in the media and popular culture. A recent research found that many in the security sector today think the media's frequent negative portrayal of the hacker community needs to change.

Good hackers not only assist in exposing system flaws but also help fix them before criminals have a chance to exploit them. They are a crucial component of the cybersecurity ecosystem and frequently uncover critical undiscovered flaws in systems more effectively than any security solution ever could.

Step 3: Hackers as criminal

Cybercriminals are those who commit crimes using computers or the internet. Black-hat and gray-hat hackers may violate the law, turning themselves into online criminals. Computer system damage or disruption is covered under laws on computer crime in each of the 50 states.

Cybercriminals are people or groups of people who utilise technology to carry out nefarious acts on digital networks or systems with the aim of stealing confidential business information or personal data and making money.

Example

Identity theft and privacy invasion. Internet scamming ATM theft. Wire fraud Torrenting and file sharing. Falsification and counterfeiting juvenile pornography. Hacking. viruses on computers. threats to a denial of service. Email hacking, spam, and steganography. Sabotage.

**Find a use of biometrics in your city. Describe the application and its benefits and risks.**

Step 1:

Identification and authentication are the primary functions of biometric systems and tools. Security, banking, mobile access and authentication, law enforcement, public transportation, schools, home helpers, and building access are where biometric devices are most frequently employed.

Step 2:

It is utilised in programmes and systems like national identity cards for identification and health insurance schemes that make use of fingerprints for identification. airport safety This industry occasionally makes use of biometrics like iris recognition.

A person's biological traits are used by biometric technology to confirm that they are who they claim to be. This could thwart hack attempts and other security risks to a person's accounts, profiles, etc. And it can significantly improve workplace security.

There are several benefits to using biometric authentication in contemporary technological and digital applications, including: High security and assurance - Biometric identification helps confirm identity by answering the questions of "something a person possesses and is." User Experience – Convenient and fast.

Step 3: Application

High assurance and security -

By confirming a measurable, in-person characteristic as something the user is both as well as something the user possesses, biometrics give suppliers higher degrees of assurance that a person is real. Due to the likelihood that the majority of user passwords, PINs, and personal identification information have been exposed in a data breach, fraudsters who have access to the traditional authentication methods can access billions of accounts.

user encounter opportune and quick

Although the internal procedures for biometric authentication are technically complex, from the perspective of the user, they are remarkably simple and rapid. It takes less time to place a finger on a scanner to unlock an account than it does to type a lengthy password with numerous special characters.

Non-transferable

Biometric authentication demands the presence of its input during authorization. The only way to use the majority of biometric authentication systems is with a physical application; you cannot transfer or exchange a physical biometric online.

Near spoof-proof

It is nearly hard to recreate biometrics like face patterns, fingerprints, iris scanning, and others using the technologies available today. The likelihood of your fingerprint exactly matching someone else's is one in 64 billion.

Step 4:

improving access for staff

Staff can access hospital systems more quickly by deploying biometric technologies rather than using hardware tokens and other authentication techniques. They won't need to submit an SMS security code or a six-digit token anymore.

Unfortunately, despite how widely used biometric authentication is, there are certain issues with its accuracy.

Several security threats

Fingerprints have occasionally been successfully tricked or gotten around. Because of this, several IT and security engineers use less risky biometric methods. For instance, more secure alternatives include retina scanners that identify distinctive patterns in the eye and palm scanners that use the distinctive vein patterns in a person's hand to authenticate.

Despite claims that they have been successfully tricked, some more recent facial recognition technologies, such as Microsoft Windows Hello or Apple Face ID, have both demonstrated successful outcomes.

Certain software specifications

Unfortunately, biometric authentication requires additional software. If EHR platforms and hospital systems are incompatible with the technology, this might lead to issues and leave many hospital CIOs with little options. For instance, Windows Hello enables operating system access using facial recognition. Since it requires Windows 10 and many hospitals are still upgrading to the newest Windows OS, it hasn't been widely used in healthcare.

Access to protected systems and software is not the only application for biometric technologies. Countries like India rely on a national identity system that enables its residents to access government benefits following a successful fingerprint authentication against a national database. Hospitals are realising that utilising this identification form factor improves their security and lowers the chance of identity theft, despite certain worries about biometric technology.