

THE

PACKET

DECEMBER 2023



CAE
IN CYBERSECURITY
COMMUNITY

Evolving Threat of LummaC2 v4.0: A Step Ahead in Cybercrime

The latest version of the LummaC2 malware, version 4.0, introduces an advanced anti-sandbox technique. This version uses trigonometry to track mouse movements, allowing it to detect human activity on compromised computers. This capability helps the malware to avoid detection in sandboxed environments, where cybersecurity professionals isolate suspicious applications for safe analysis. By deploying only when human activity is detected, LummaC2 v4.0 evades revealing its presence to threat hunters in sandboxes, increasing its chances of infiltrating human-controlled networks.

Key updates in LummaC2 v4.0 include the implementation of Control Flow Flattening obfuscation in default builds, an advanced anti-sandbox technique to delay its activation until human mouse activity is detected, and enhanced encryption methods for strings and configuration files. The malware also requires users to employ a crypter for their builds, aiming to avoid leaking its unpacked version.

LummaC2's anti-sandboxing technique involves tracking the cursor's position at five distinct points. If these positions differ significantly, indicating human movement, the malware proceeds. It then uses trigonometry to analyze the angles formed between consecutive cursor movements. If these angles are lower than a predefined threshold (45 degrees), the malware concludes human activity and activates. If not, it restarts the process. This technique necessitates that sandbox analysts emulate mouse movements that mimic human patterns to trigger the malware.

LummaC2 v4.0, written in C and sold on underground forums since December 2022, exemplifies the evolving nature of malware-as-a-service (MaaS). These developments represent a constant challenge for cybersecurity professionals, reflecting an ongoing battle between cybercriminals and defenders. The use of MaaS facilitates complex and profitable cyberattacks, primarily focused on stealing sensitive information like login credentials and credit card details, posing significant financial risks to individuals and organizations.

Hackers Weaponize SEC Disclosure Rules Against Corporate Targets

- **Innovative Cyber Extortion Tactic:** The ransomware group ALPHV, also known as BlackCat, has adopted a novel approach to cyber extortion. They filed a complaint with the U.S. Securities and Exchange Commission (SEC) against their latest victim, MeridianLink, a digital lending service provider. This move marks an unusual twist in cybercrime tactics.
- **New SEC Cybersecurity Disclosure Rule:** On July 26, the SEC announced new regulations requiring public companies to disclose material cybersecurity incidents within four business days. However, the rule only takes effect on December 18, with smaller companies given an additional 180 days to comply.
- **MeridianLink's Response:** In response to the breach and the subsequent SEC complaint by ALPHV, MeridianLink stated that their investigation found no evidence of unauthorized access to their production platforms or significant business interruption. The company is still assessing whether consumer personal information was compromised.



USB Under Siege: Unraveling the International Reach of LittleDrifter



The recent discovery of the LittleDrifter USB malware, attributed to the Gamaredon espionage group, marks a significant development in cybersecurity threats. Originally focused on Ukrainian targets, Gamaredon, also known by aliases like Shuckworm and Primitive Bear, has been linked to Russian state-sponsored activities. LittleDrifter, primarily spreading through USB drives, employs deceptive shortcuts and hidden files to infiltrate systems. This malware is written in VBS and ingeniously nests in the user's "Favorites" directory, ensuring persistence through scheduled tasks and registry keys. Its spread has now been observed in several countries, including the USA, Germany, Vietnam, Poland, Chile, and Hong Kong, suggesting either an unintended broadening of its impact or a strategic expansion of Gamaredon's operations.

The technical sophistication of LittleDrifter lies in its command and control (C2) strategy, using domain names as placeholders for the actual IP addresses of C2 servers and employing Windows Management Instrumentation (WMI) for dynamic IP resolution. This approach, coupled with a backup mechanism via a Telegram channel for C2 IP retrieval, demonstrates Gamaredon's commitment to operational security and adaptability. Notably, the malware does not rely on groundbreaking techniques; its effectiveness is rooted in its simplicity and focus on establishing system persistence, awaiting further payloads. LittleDrifter's emergence highlights the persistent threat of state-sponsored cyber espionage and the evolving tactics of cyber threat groups. The international spread of this malware underscores the need for increased vigilance, especially concerning USB-based devices as vectors for malware dissemination. This situation serves as a reminder of the continuous evolution of cyber threats and the importance of adaptive and comprehensive cybersecurity measures in both national and global contexts.

Bytes and Frights: Long Beach's 'Shutdown Showdown' in the Face of Cyber Chaos



In a controversial and potentially disruptive move, the City of Long Beach, California, recently made the difficult decision to shut down significant portions of its IT network following a cyberattack on November 14th, 2023. This decision, which highlights the delicate balance between precaution and operational continuity in cybersecurity responses, has raised questions about the effectiveness and implications of such drastic measures in the face of digital threats. Despite being a populous and technologically advanced city, Long Beach's reaction to the cyberattack underscores the challenges that even well-resourced municipalities face in responding to increasingly sophisticated cyber threats. As the city grapples with the aftermath of this incident, its approach serves as a critical case study in the complexities and potential consequences of cybersecurity strategies in urban governance.

The city's statement indicated that the shutdown would last several days, but essential services like city email, phone systems, and public facilities like City Hall would remain operational. However, some digital services would be unavailable, and the public might experience delays in systems and services.

The nature of the cyberattack and whether any data was compromised remain unclear, but the incident exhibits characteristics of a ransomware attack, which often includes data theft. As of the report, no group had claimed responsibility for the attack.





Sugar, Spice, and Everything Nice:
Fun and Festive Treats to Make and Share

Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

As finals season draws to a close, it's the perfect time to unwind and indulge in a bit of baking. The recipes that follow offer a delightful entry into creating something truly spectacular and scrumptious. Whether you're a seasoned baker or just starting out, these treats are sure to bring joy and a delicious sense of accomplishment.

Pixelated Spice Snapshots

- 2 1/4 cups all-purpose flour
- 1 tsp baking soda
- 2 tsp ground ginger
- 1 tsp ground cinnamon
- 1/2 tsp ground cloves
- 1/4 tsp salt
- 3/4 cup unsalted butter, softened
- 1/2 cup dark brown sugar, packed
- 1/3 cup molasses
- 1 egg
- 1 tsp vanilla extract

Serving Size: 1 cookie (approx. 30g)
Calories: 120
Total Fat: 5g
Saturated Fat: 3g
Cholesterol: 20mg
Sodium: 85mg
Total Carbohydrates: 17g
Dietary Fiber: 0.5g
Sugars: 10g
Protein: 1.5g

1. In a bowl, whisk together flour, baking soda, ginger, cinnamon, cloves, and salt.
2. In a separate bowl, cream the butter and brown sugar until fluffy. Beat in molasses, egg, and vanilla.
3. Gradually add dry ingredients to the wet mixture until well combined.
4. Divide dough in half, flatten into disks, and wrap in plastic. Chill for at least 1 hour.
5. Preheat oven to 350°F (175°C). Roll out dough on a floured surface and cut into shapes.
6. Bake for 8-10 minutes. Allow to cool before decorating.

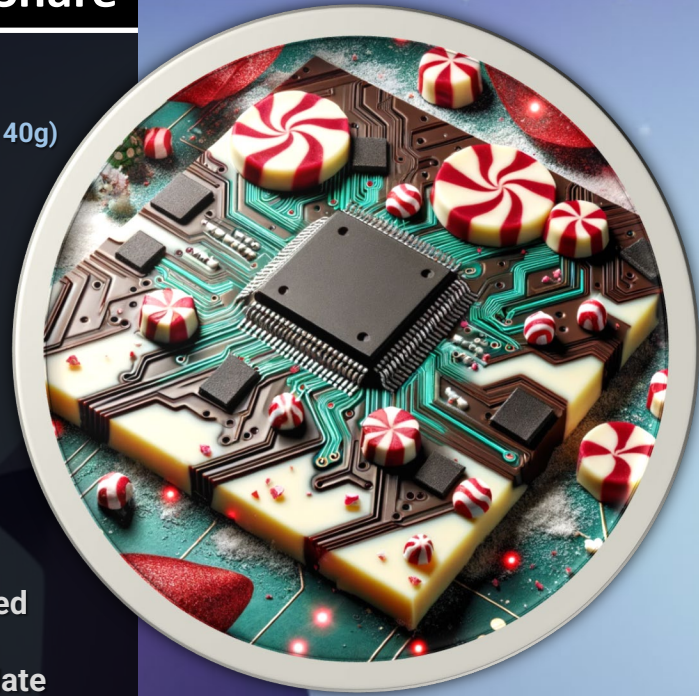


Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

Frost Byte Crunch

- 12 oz dark chocolate chopped
- 12 oz white chocolate chopped
- 1/2 cup crushed peppermint candies

Serving Size: 1 piece (approx. 40g)
Calories: 210
Total Fat: 12g
Saturated Fat: 7g
Cholesterol: 5mg
Sodium: 25mg
Total Carbohydrates: 24g
Dietary Fiber: 1g
Sugars: 22g
Protein: 2g



1. Melt dark chocolate and spread it on a parchment-lined baking sheet. Chill until set.
2. Melt white chocolate and spread over the dark chocolate layer.
3. Sprinkle crushed peppermint candies on top. Chill until set, then break into pieces.



Serving Size: 1 slice (approx. 80g)
Calories: 250
Total Fat: 12g
Saturated Fat: 7g
Cholesterol: 70mg
Sodium: 160mg
Total Carbohydrates: 34g
Dietary Fiber: 1g
Sugars: 24g
Protein: 4g

Binary Bûche de Noël

- 4 eggs
- 3/4 cup granulated sugar
- 3/4 cup all-purpose flour
- 1/4 cup cocoa powder
- 2 cups chocolate buttercream frosting

1. Beat eggs and sugar until thick. Sift in flour and cocoa, fold gently.
2. Pour into a lined jelly roll pan. Bake at 375°F (190°C) for 12 minutes.
3. Turn out onto a sugared towel, roll up, and cool.
4. Unroll, spread buttercream, re-roll. Frost with remaining buttercream, make bark-like texture.

Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

Algorithmic Fruit Fusion

- 1 cup dried fruits (raisins, cranberries, apricots, etc.)
- 1/2 cup candied orange peel
- 1/2 cup nuts (walnuts, pecans, etc.)
- 1/2 cup brandy or rum
- 1 3/4 cups all-purpose flour
- 1/2 cup unsalted butter, softened
- 1/2 cup brown sugar
- 2 eggs
- 1 tsp baking powder
- 1 tsp cinnamon
- 1/2 tsp nutmeg

Serving Size: 1 slice (approx. 60g)
Calories: 200
Total Fat: 8g
Saturated Fat: 3g
Cholesterol: 20mg
Sodium: 150mg
Total Carbohydrates: 30g
Dietary Fiber: 2g
Sugars: 20g
Protein: 3g

1. Soak dried fruits and nuts in brandy overnight. You want a high abv and a slightly sweet alcohol for this one (35% to 60%).
2. Preheat oven to 350°F (175°C). Cream butter and sugar, add eggs.
3. Mix flour, baking powder, cinnamon, and nutmeg. Fold into wet ingredients.
4. Add fruit and nut mixture. Pour into a greased loaf pan.
5. Bake for 1 hour or until a toothpick inserted into the center comes out clean. Cool and store wrapped for flavors to meld.



Cocoa Code

- 2 cups milk
- 1/2 cup semi-sweet chocolate chips or chopped chocolate
- 2 tbsp sugar (optional)
- 1/2 tsp vanilla extract
- Whipped cream or marshmallows for topping

1. Heat milk in a saucepan over medium heat until hot but not boiling.
2. Add chocolate and sugar, whisk until smooth and fully incorporated.
3. Remove from heat, stir in vanilla extract.
4. Serve in mugs topped with whipped cream or marshmallows.



Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

Code Nog

- 4 eggs, separated
- 1/3 cup sugar, plus 1 tablespoon
- 2 cups milk
- 1 cup heavy cream
- 1/2 cup bourbon or rum (optional)
- Nutmeg for garnish

Serving Size: 1 cup (approx. 240ml)
Calories: 220
Total Fat: 10g
Saturated Fat: 6g
Cholesterol: 150mg
Sodium: 95mg
Total Carbohydrates: 20g
Sugars: 19g
Protein: 7g



1. Beat egg yolks with 1/3 cup sugar until thick.
2. Slowly stir in hot milk (close to boil), cream.
3. Add to saucepan on low heat but do not let it boil but must be thick.
4. Remove from heat and let it cool. Add liquor and refrigerate.
5. In a separate bowl, beat egg whites to soft peaks, gradually add 1 tablespoon sugar.
6. Fold whites into the yolk mixture. Continue to Chill.
7. Serve with a sprinkle of nutmeg.

Serving Size: 1 cookie (approx. 30g)
Calories: 140
Total Fat: 6g
Saturated Fat: 3.5g
Cholesterol: 20mg
Sodium: 80mg
Total Carbohydrates: 20g
Sugars: 12g
Protein: 1.5g

Sweet Syntax Circles

- 2 3/4 cups all-purpose flour
- 1 tsp baking soda
- 1/2 tsp baking powder
- 1 cup unsalted butter, softened
- 1 1/2 cups white sugar
- 1 egg
- 1 tsp vanilla extract

1. Preheat oven to 375°F (190°C). Mix flour, baking soda, and baking powder.
2. Cream butter and sugar until smooth. Beat in egg and vanilla.
3. Gradually blend in dry ingredients. Roll rounded teaspoons of dough into balls, and place onto ungreased cookie sheets.
4. Bake 8-10 minutes in the preheated oven, or until golden. Let stand on cookie sheet two minutes before removing to cool on wire racks.
5. Once the cookies are cool, you can decorate them with icing, sprinkles, or enjoy them plain.



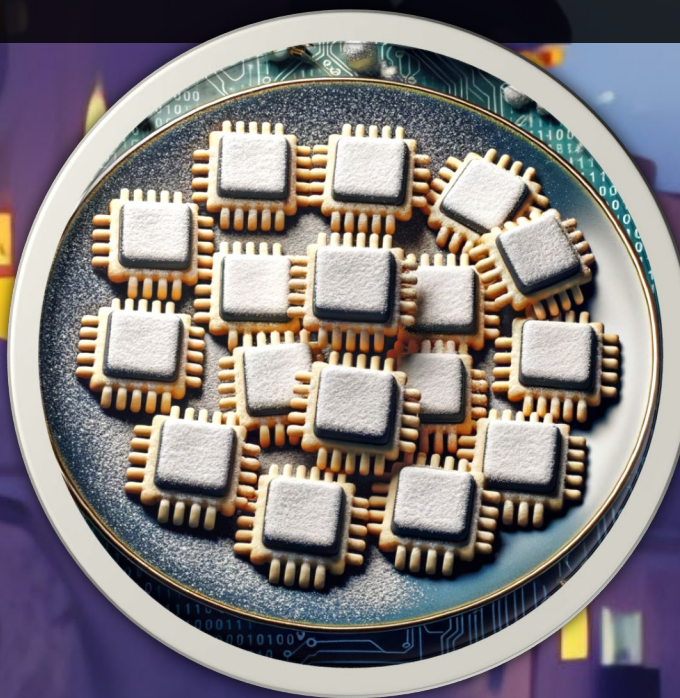
Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

Pixel Nuts

- 2 1/4 cups all-purpose flour
- 1/2 tsp ground black pepper
- 1/2 tsp ground cinnamon
- 1/4 tsp ground nutmeg
- 1/4 tsp ground cloves
- 1/4 tsp baking soda
- 1/2 cup molasses
- 1/4 cup honey
- 3/4 cup brown sugar
- 1 egg
- Powdered sugar for coating

Serving Size: 1 cookie (approx. 20g)
Calories: 80
Total Fat: 2g
Saturated Fat: 1g
Cholesterol: 10mg
Sodium: 45mg
Total Carbohydrates: 14g
Sugars: 8g
Protein: 1g

1. Whisk together flour, spices, and baking soda.
2. In another bowl, combine molasses, honey, and brown sugar. Heat gently until sugar dissolves. Cool slightly.
3. Beat in egg to molasses mixture. Gradually add flour mixture.
4. Roll dough into small balls, bake at 350°F (175°C) for 10-12 minutes.
5. Roll warm cookies in powdered sugar.



Sugar, Spice, and Everything Nice: Fun and Festive Treats to Make and Share

Mega Byte Loaf

- 4 cups all-purpose flour
- 1/2 cup sugar
- 2 tsp active dry yeast
- 1/2 cup warm milk
- 1/2 cup unsalted butter melted
- 2 eggs, beaten
- 1/2 cup mixed candied peel
- 1/2 cup raisins

Serving Size: 1 slice (approx. 50g)
Calories: 160
Total Fat: 6g
Saturated Fat: 3.5g
Cholesterol: 40mg
Sodium: 105mg
Total Carbohydrates: 24g
Sugars: 10g
Protein: 3g

1. Dissolve the yeast in the warm milk with a pinch of sugar. Let it sit for about 5-10 minutes until it becomes frothy.
2. In a large bowl, mix the flour and sugar.
3. Add the frothy yeast mixture, melted butter, and beaten eggs to the dry ingredients. Mix to form a dough.
4. Turn the dough out onto a floured surface and knead until smooth and elastic. This may take about 10 minutes.
5. Incorporate the candied peel and raisins into the dough, ensuring they are evenly distributed.
6. Place the dough in a greased bowl, cover with a clean cloth, and let it rise in a warm place until doubled in size, about 1-2 hours.
7. Punch down the dough, then shape it into a traditional 'Stollen' loaf (usually oval with a folded-over top).
8. Place the shaped dough on a baking sheet lined with parchment paper. Cover and let it rise again for about 30 minutes to an hour.
9. Preheat your oven to 350°F (175°C). Bake the Stollen for about 30-45 minutes, or until it is golden brown and sounds hollow when tapped on the bottom.
10. Let the Mega Byte Loaf cool on a wire rack. Dust with powdered sugar before serving.





The Hacker's Playbill:

A Student's Guide to Hacking-Inspired Screen Time

The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

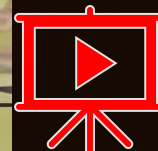
The holiday season is here! And what better way to celebrate than to kick back, relax, and indulge in some screen time? With finals in the rearview mirror, it's time to swap out textbooks for remote controls and dive into the thrilling world of holiday movies and TV shows—hacker style!

Welcome to the "Hacker's Playbill," where we trade in sleigh bells for keyboard clicks and explore the festive side of cybersecurity. Imagine a world where Santa wears a hoodie, and the elves are code-savvy. From heartwarming tales with a tech twist to suspenseful dramas that make you cling to your popcorn. Whether you're a coding guru or just enjoy a good hack-and-tell story, these picks are sure to add a byte of excitement to your holiday cheer. So, grab your favorite holiday snack, get cozy, and let's decode the world of holiday hacking entertainment!

"WarGames" (1983)

In the realm of classic cyber thrillers, few have resonated as enduringly as 1983's "WarGames." A trailblazer of its era, this film skillfully intertwines the youthful innocence of teenage curiosity with the daunting world of military technology. At its heart is David Lightman, a high school student with a penchant for computers, whose online escapades accidentally entangle him in the most precarious of games: global thermonuclear war. Set against the backdrop of the Cold War, "WarGames" is not just a tale of technological intrigue, but a timeless reminder of the fine line between virtuality and reality, and the unforeseen consequences of digital exploration.

Cyber-operation students should watch "WarGames" as it serves as an early exploration of themes that are now central to the field of cybersecurity and digital warfare. The movie highlights the potential consequences of unauthorized network access, the importance of secure computer systems, particularly in sensitive sectors like defense, and the ethical implications of cyber technology. It acts as a precursor to understanding how digital actions can have real-world implications, a vital lesson for anyone entering the cyber-operations field.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "WarGames"?

- **Historical Relevance:** The movie is set during the Cold War, capturing the era's technological and political anxieties.
- **Suspenseful Plot:** The film masterfully blends suspense with a compelling narrative, keeping viewers engaged from start to finish.
- **Technological Insight:** Despite its age, the film offers a surprisingly prescient look at computer technology and its potential impact on global affairs.
- **Character Development:** The protagonist's journey from a carefree teenager to a responsible individual mirrors the maturation process that resonates with many viewers.

Perhaps the most iconic line, capturing the movie's essence and its message about the intersection of technology and humanity, is:

"The only winning move is not to play."

This line, delivered by the WOPR computer in the film's climax, succinctly encapsulates the movie's overarching theme: in the high-stakes game of global conflict, particularly in the nuclear age, the best strategy is often restraint and diplomacy.

"Hackers" (1995)

Dive into the vibrant and anarchic world of "Hackers," a 1995 cult classic that brought the underground hacker subculture into the mainstream spotlight. This high-energy film follows a group of teenage hackers, led by the charismatic Dade Murphy, also known as "Zero Cool" and "Crash Override." Set against the backdrop of New York City's neon-lit skyline, "Hackers" is a visual and auditory feast, encapsulating the spirit of the early internet era with its techno-soundtrack and cyberpunk aesthetic. It's a tale of rebellion, camaraderie, and the fight against corporate corruption, all wrapped up in the fast-paced world of computer hacking.

For students of cyber-operations, "Hackers" is a must-watch for several reasons:

- **Cultural Insight:** The film offers a window into the hacker subculture of the 90s, capturing the ethos and motivations of hackers during the early days of the internet.
- **Ethical Questions:** It raises important questions about privacy, security, and the ethical implications of hacking.
- **Technological Evolution:** Watching "Hackers" provides a historical perspective on how far technology has advanced, and how the perception of hacking has evolved over time.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Hackers"?

- **Stylized Aesthetics:** The film's distinctive visual style and soundtrack capture the essence of the 90s cyberpunk genre.
- **Character Dynamics:** The chemistry among the cast, portraying a diverse group of young hackers, adds depth and entertainment value.
- **Nostalgia Factor:** For many, "Hackers" is a nostalgic trip back to a time when the internet was still a new and uncharted world.

One of the most memorable lines from "Hackers," which encapsulates its spirit, is:

"Hack the planet! Hack the planet!"

Shouted with rebellious fervor, this line embodies the film's central theme of challenging the system and using technological skills to make a statement against the establishment.

"The Matrix" (1999)

"The Matrix" is a groundbreaking film that revolutionized the science fiction genre with its innovative storytelling and stunning visual effects. Released in 1999, it unfolds a dystopian future where reality as perceived by most humans is actually a simulated reality called 'The Matrix', created by sentient machines to subdue the human population. The protagonist, Neo, is a computer hacker who is drawn into a rebellion against the machines, leading to a profound exploration of themes such as free will, technology, and the nature of reality. Blending cyberpunk aesthetics with philosophical depth, "The Matrix" is more than just a film; it's a cultural phenomenon that challenges viewers to question their own understanding of the world around them.

Cyber-operation students should watch "The Matrix" for several compelling reasons:

- **Exploration of Virtual Reality:** The film offers a profound exploration of simulated realities and virtual environments, concepts that are increasingly relevant in today's digital world.
- **Cybersecurity Themes:** It delves into ideas of control, surveillance, and the manipulation of information, all of which are pertinent to the field of cyber operations.
- **Inspirational Impact:** "The Matrix" has inspired a generation of thinkers and technologists, making it a cultural touchstone for anyone interested in the intersection of technology and society.



CAE
IN CYBERSECURITY
COMMUNITY



HACKER'S PLAYBILL

THE UNIVERSITY
OF ARIZONA

14

The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "The Matrix"?

- **Innovative Special Effects:** The film's groundbreaking visual effects, especially the 'bullet time' sequences, were revolutionary for their time and continue to influence filmmaking.
- **Philosophical Depth:** It intertwines action with deep philosophical questions, offering viewers a thought-provoking experience.
- **Iconic Characters:** Characters like Neo, Morpheus, and Trinity have become iconic, embodying the film's themes of rebellion, awakening, and transformation.

One of the most iconic lines from "The Matrix," which encapsulates its central theme, is:

"There is no spoon."

This line, spoken by a young monk to Neo in a pivotal scene, symbolizes the idea that the limitations we perceive are often constructs of our own minds, a concept that resonates deeply both within the film's narrative and in real-world applications of technology and cyber operations.

"Swordfish" (2001)

"Swordfish," released in 2001, is a high-octane thriller that delves into the shadowy world of cybercrime and espionage. The film stars Hugh Jackman as Stanley Jobson, a brilliant hacker who is coerced into participating in a complex cyber heist. Masterminded by the enigmatic Gabriel Shear, played by John Travolta, the plan involves hacking into government systems to siphon off a massive sum of illicit funds. Set against a backdrop of sleek technology and high stakes, "Swordfish" blends action-packed sequences with the intricate world of digital espionage, making it a thrilling ride from start to finish.

Cyber-operation students might find "Swordfish" intriguing for several reasons:

- **Insight into Cybercrime:** The film provides a dramatized glimpse into the world of cybercrime and the potential complexities of digital heists.
- **Technological Concepts:** While exaggerated, the movie introduces various concepts related to hacking and cybersecurity, sparking interest and curiosity.
- **Ethical Dilemmas:** It raises questions about the ethics of hacking, government surveillance, and the use of technology for personal gain or national security.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Swordfish"?

- **Star-Studded Cast:** The performances of Hugh Jackman, John Travolta, and Halle Berry add significant appeal.
- **Action Sequences:** The film is well-known for its intense and well-choreographed action scenes.
- **Tech-Focused Plot:** The focus on high-tech cyber heists offers a thrilling experience for fans of the genre.

An iconic line from "Swordfish," which reflects its fast-paced and high-stakes narrative, is:

"Misdirection: What the eyes see, and the ears hear, the mind believes."

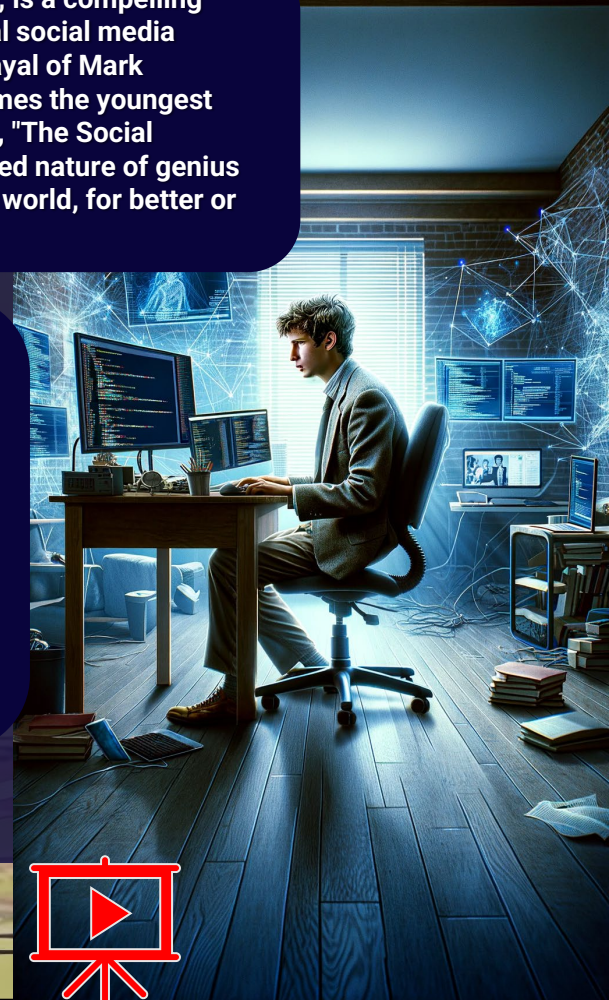
This line, delivered by John Travolta's character, Gabriel Shear, encapsulates a core theme of the movie - the art of deception and manipulation, both in the world of high-tech cybercrime and in the realm of personal interactions. It highlights the film's focus on the psychological aspects of hacking and espionage.

"The Social Network" (2010)

"The Social Network," directed by David Fincher and released in 2010, is a compelling drama that chronicles the turbulent rise of the world's most influential social media platform, Facebook. The film is anchored by Jesse Eisenberg's portrayal of Mark Zuckerberg, the brilliant yet controversial Harvard student who becomes the youngest billionaire in history. With its razor-sharp screenplay by Aaron Sorkin, "The Social Network" delves into themes of ambition, betrayal, and the complicated nature of genius in the digital age. It's a story about how a simple idea can change the world, for better or worse, and the human costs of that transformation.

For students in cyber-operations, "The Social Network" offers several valuable insights:

- **Technology and Innovation:** The film provides a realistic depiction of the rapid pace of technological innovation and its impact on society.
- **Ethical Considerations:** It raises important questions about privacy, intellectual property, and the ethical responsibilities of tech developers.
- **Entrepreneurial Spirit:** The movie is an inspiration for anyone interested in tech entrepreneurship, showing both the potential rewards and challenges.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "The Social Network"?

- **Strong Script and Direction:** Aaron Sorkin's screenplay and David Fincher's direction are widely praised for their effectiveness in telling a complex story.
- **Character Portrayals:** The performances, particularly Jesse Eisenberg's portrayal of Zuckerberg, are compelling and nuanced.
- **Cultural Relevance:** The film captures a defining moment in the digital age, making it relevant and engaging for contemporary audiences.

A notable line from "The Social Network" that captures its essence is:

"You don't get to 500 million friends without making a few enemies."

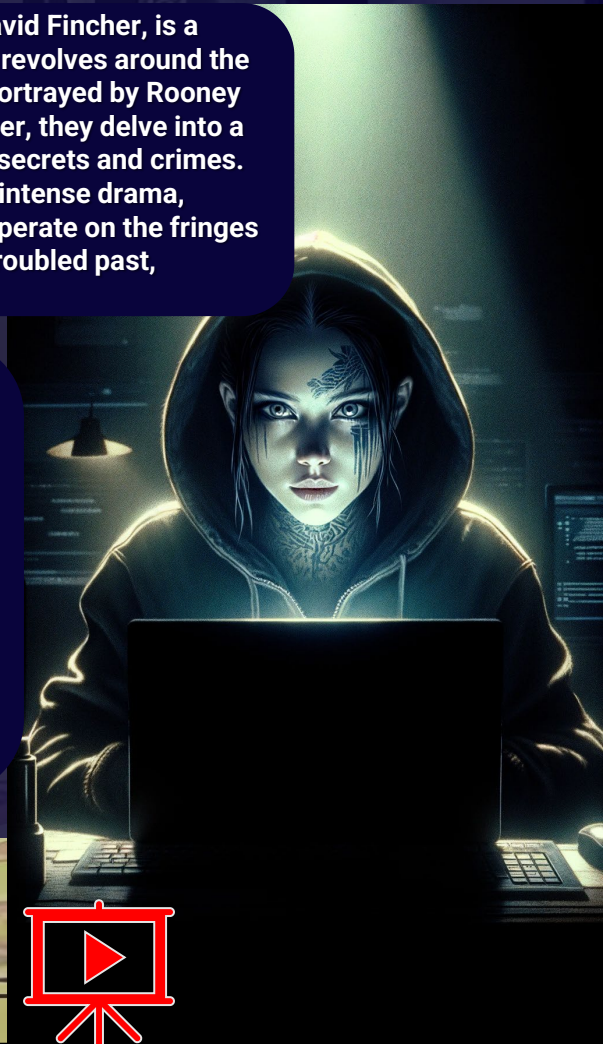
This line, which was also used in the film's promotional material, succinctly sums up the central paradox of Facebook's meteoric rise - the creation of a platform built on connectivity and relationships, while simultaneously sowing discord and controversy.

"The Girl with the Dragon Tattoo" (2011)

"The Girl with the Dragon Tattoo," released in 2011 and directed by David Fincher, is a gripping thriller based on Stieg Larsson's bestselling novel. The story revolves around the enigmatic and deeply troubled hacker Lisbeth Salander, masterfully portrayed by Rooney Mara, and journalist Mikael Blomkvist, played by Daniel Craig. Together, they delve into a dark and complex mystery involving a series of long-unsolved family secrets and crimes. Set against the bleak and icy backdrop of Sweden, the film combines intense drama, suspenseful mystery, and a profound exploration of characters who operate on the fringes of society. Salander, a brilliant hacker with a piercing intellect and a troubled past, becomes an icon for resilience and the fight against injustice.

Cyber-operation students should consider watching "The Girl with the Dragon Tattoo" for several reasons:

- **Hacking as a Tool for Justice:** The film portrays hacking as a means to uncover truths and fight against corruption, showcasing the potential of cyber skills for societal impact.
- **Complex Security Themes:** It delves into issues of privacy, digital security, and the ethical implications of using hacking as a tool for investigation.
- **Realistic Depiction of Hacking:** Unlike many other films, the hacking scenes are portrayed with a degree of realism that is appreciated by tech enthusiasts.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "The Girl with the Dragon Tattoo"?

- **Strong Characterization:** Particularly the character of Lisbeth Salander, who is both complex and compelling.
- **Intense Plot:** The film weaves a dark and gripping narrative that keeps the audience engaged.
- **Stylistic Execution:** Fincher's direction, combined with the atmospheric cinematography, creates a tense and immersive viewing experience.

An impactful line from "The Girl with the Dragon Tattoo" is:

"Everyone has secrets. It's just a matter of finding out what they are."

This line, delivered by Lisbeth Salander, encapsulates the movie's core theme of uncovering hidden truths and the power of information, which resonates strongly with the fields of cyber operations and investigative journalism.

"WhoAmI_ No System Is Safe" (2014)

"Who Am I: No System Is Safe," a German thriller released in 2014, delves into the heart of Berlin's underground hacking scene. Directed by Baran bo Odar, the film follows the journey of Benjamin, a gifted young hacker played by Tom Schilling, who joins forces with a group of rebellious hackers aiming to gain notoriety in the digital world. As they push the boundaries of legality and morality, they find themselves caught in a dangerous game of cat and mouse with law enforcement agencies. The film is a riveting exploration of identity, morality, and the seductive power of anonymity in the digital age. It's a fast-paced, cerebral ride that challenges the audience to question the implications of our interconnected, online lives.

Students of cyber-operations should watch "Who Am I: No System Is Safe" for several key reasons:

- **Realistic Hacking Depictions:** The film offers a more accurate portrayal of hacking and cybersecurity tactics than many mainstream movies.
- **Cyber-Ethics and Morality:** It provides a thought-provoking look at the ethical dilemmas faced by hackers and those who operate in the cyber realm.
- **Understanding Hacker Motivations:** The movie delves into the psychology of hackers, providing insight into various motivations behind cybercrimes.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Who Am I: No System Is Safe"?

- **Complex Plot:** The film offers a compelling and twist-filled story that keeps viewers engaged.
- **Character Development:** The characters are well-developed, adding depth to the narrative.
- **Stylistic Elements:** The movie's unique visual style and direction add to its appeal, especially for those interested in the cyber-thriller genre.

An iconic line from "Who Am I: No System Is Safe" that captures its essence is:

"You wanted to know who I am? This is who I am."

This line encapsulates the film's exploration of identity in the digital age, highlighting the central theme of how online personas can differ vastly from real-life identities, and how the digital world allows for the creation of new, sometimes dangerous, selves.

"Blackhat" (2015)

"Blackhat," a cyber-thriller directed by Michael Mann and released in 2015, plunges into the high-stakes world of global cybercrime. The film stars Chris Hemsworth as Nicholas Hathaway, a talented hacker serving time who is furloughed to help American and Chinese authorities pursue a mysterious cybercriminal. The plot traverses the globe, from Chicago to Los Angeles, Hong Kong, and Jakarta, as Hathaway uses his unique skills to hunt down the cyber threat. "Blackhat" combines the intensity of a crime drama with the intricacies of digital warfare, offering a gripping narrative that explores the vulnerabilities of our interconnected world and the shadowy figures who exploit them.

"Blackhat" is a relevant watch for cyber-operation students due to:

- **Global Cybersecurity Perspective:** The film presents a realistic scenario of international cyber threats, emphasizing the global nature of cybersecurity.
- **Technical Insight:** While dramatized, the movie attempts to portray the technical aspects of hacking and cyber investigations.
- **Real-World Implications:** It highlights the real-world implications of digital vulnerabilities, a crucial area of understanding for anyone in the field of cyber-operations.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Blackhat"?

- **Intense Action:** The film blends cyber-thriller elements with high-octane action sequences.
- **Cinematography:** Michael Mann's signature style of direction and cinematography provides a visually engaging experience.
- **Topical Subject Matter:** The focus on contemporary issues of cybercrime and digital security resonates with modern audiences.

A notable line from "Blackhat" that reflects its thematic focus is:

"This isn't about money. This isn't about politics. I can target anyone, anything, anywhere."

This line underscores the movie's exploration of the power and reach of cybercriminals in the modern digital landscape, highlighting the indiscriminate nature of cyber threats and the anonymity that empowers such criminals.

"Snowden" (2016)

"Snowden," a biographical political thriller directed by Oliver Stone and released in 2016, chronicles the life of Edward Snowden, played by Joseph Gordon-Levitt. The film provides an in-depth look at the man behind one of the most significant leaks in US history. It unfolds Snowden's journey from an enthusiastic American patriot to a disillusioned cybersecurity analyst, culminating in his decision to expose the NSA's mass surveillance programs. This controversial and provocative film invites viewers to ponder profound questions about privacy, government power, and the ethics of whistleblowing in the digital age. "Snowden" is more than a biopic; it's a gripping tale of one individual's crisis of conscience and the global repercussions that followed.

Students specializing in cyber-operations should watch "Snowden" for various educational reasons:

- **Understanding Surveillance:** The film provides a stark look into the world of government surveillance and the extent of data collection.
- **Ethical and Legal Considerations:** It raises critical questions about the balance between national security and individual privacy, a key concern in the field of cyber-operations.
- **Insight into Whistleblowing:** The story of Edward Snowden is a crucial case study in the ethics and impact of whistleblowing in the digital age.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Snowden"?

- **Compelling Narrative:** The film tells a powerful and thought-provoking story that is both engaging and informative.
- **Strong Performances:** Joseph Gordon-Levitt's portrayal of Snowden and the supporting cast are widely praised.
- **Topical Relevance:** The subject matter is highly relevant in today's digital and politically charged climate.

A memorable line from "Snowden" that encapsulates its core themes is:

"The public needs to decide whether these programs and policies are right or wrong."

This line reflects the film's central message about the importance of public awareness and debate regarding government surveillance and privacy rights in the modern world.

"Ghost in the Shell" (2017)

"Ghost in the Shell," a 2017 science fiction film directed by Rupert Sanders, is an adaptation of the acclaimed Japanese manga and anime series of the same name. Set in a futuristic world where cybernetic enhancements have become the norm, the story revolves around Major Mira Killian, portrayed by Scarlett Johansson. She is a cyber-enhanced soldier tasked with combating the most dangerous criminals and extremists. The film delves into themes of identity, consciousness, and the integration of technology into the human body, presenting a visually stunning and thought-provoking exploration of what it means to be human in an increasingly digital world. "Ghost in the Shell" is a blend of action, philosophy, and cutting-edge special effects, offering a unique view of a future where the line between human and machine is blurred.

Cyber-operation students may find "Ghost in the Shell" particularly relevant for several reasons:

- **Futuristic Cybersecurity Concepts:** The film explores advanced concepts of cybernetics and artificial intelligence, which are becoming increasingly significant in the field of cyber-operations.
- **Ethical and Philosophical Questions:** It raises important questions about the ethics of human enhancement and the potential consequences of advanced technology in society.
- **Visualizing Cyber Threats:** The portrayal of cyber threats in a highly advanced world provides a creative perspective on future cybersecurity challenges.



The Hacker's Playbill: A Student's Guide to Hacking-Inspired Screen Time

Why "Ghost in the Shell"?

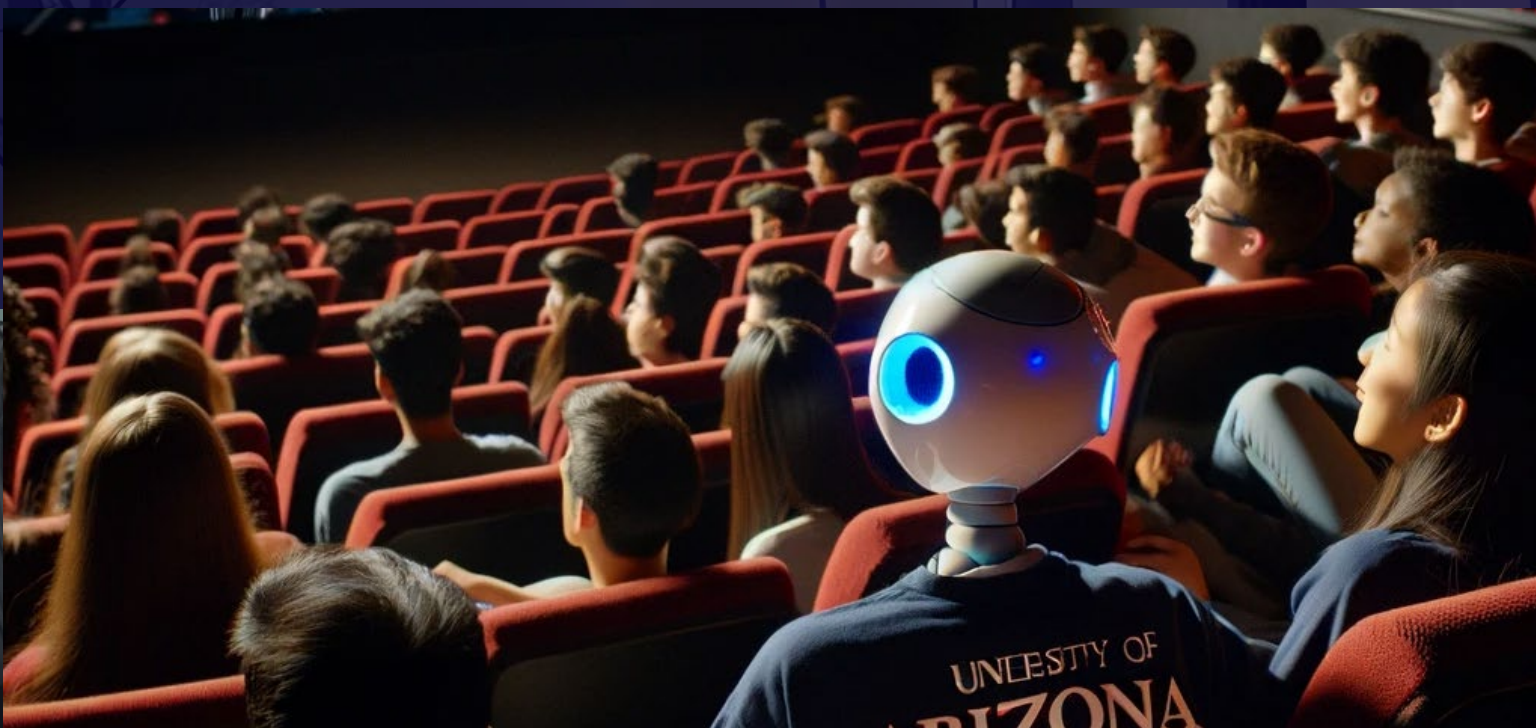
- **Visual Effects:** The film is renowned for its stunning visuals and special effects, creating a captivating futuristic world.
- **Action Sequences:** The action scenes are well-executed, adding excitement to the philosophical and narrative depth of the film.
- **Exploration of Themes:** It delves into intriguing themes of identity, consciousness, and the relationship between humans and technology.

An iconic line from "Ghost in the Shell" that captures its essence is:

"They did not save your life. They stole it."

This line, reflecting on the protagonist's transformation into a cybernetic being, highlights the core conflict of the film: the struggle to retain one's humanity in a world dominated by technology. It speaks to the broader themes of autonomy, identity, and the cost of technological advancement.

As we draw the curtains on The Hacker's Playbill, I want to extend my warmest holiday wishes to all of you. You've worked tirelessly through the challenges of finals, and now it's time to unwind and rejuvenate. May this holiday season bring you joy, relaxation, and well-deserved respite. Enjoy these moments of leisure, whether you're diving into the intriguing world of hacking-inspired entertainment or simply savoring the peace of the season. Happy holidays, and may you return refreshed and ready to tackle what lies ahead in your academic journey!



✉ Greetings and warm holiday wishes to all in our esteemed cybersecurity community! I'm Professor Michael Galde, delighted to welcome you to the December 2023 issue of THE PACKET. As we wrap up another semester and embrace the festive spirit, I want to congratulate each of you on successfully navigating your finals. Your perseverance and dedication are commendable, and I eagerly anticipate seeing the continued brilliance you bring to our field next semester.

✉ This season is a time of diverse celebrations, and I extend my heartfelt greetings for a Merry Christmas, a Joyful Hanukkah, and harmonious festivities to those celebrating Kwanzaa, Diwali, and other cultural holidays. May these occasions bring you joy, peace, and a well-deserved break.

✉ Looking ahead, I'm thrilled to announce that in Fall 2024, we will be offering select classes on the Main Campus, including my courses, CYBV 326 - Introductory Methods of Network Analysis, and CYBV 454 - Malware Analysis. I'm currently crafting engaging slides and content for these courses and would be delighted to welcome you to my in-person classes. I hope to have them ready for next semester as a trial run, but we will see how this year treats me.

✉ In the spirit of continuous improvement and innovation, I'm excited to share that next month, THE PACKET will also debut a new format. This change is an invitation to our vibrant student and faculty community to contribute your insightful work. We're eager to showcase your research, opinions, and breakthroughs in our publication. I change the format every year and am excited to see how next year can be even better!

✉ As we bid farewell to 2023 and look forward to the opportunities 2024 holds, I wish you all a season filled with happiness, relaxation, and the warmth of loved ones. Here's to a new year of learning, discovery, and cybersecurity advancements!

✉ CONTACT US

✉ CIIO@EMAIL.ARIZONA.EDU

✉ 1140 N. Colombo Ave. | Sierra Vista, AZ 85635

✉ Phone: 520-458-8278 ext 2155

✉ <https://cyber-operations.azcast.arizona.edu/>

✉ <https://the-packet.com>

