The Silent Danger:

Understanding the Severity of Zero-Day Exploits

Jasmin Azemovic
Head of SecOps | University Professor | Microsoft MVP

Speaker

- University Professor
  Since 2011
- CISO|Head of SecOps
  Since 2019
- Award
  Microsoft Security MVP
  - **Since 2009**

MVP Microsoft® Most Valuable Professional

Agenda

- Session Introduction
- Why This Matters Now?
- Defining Zero-Day Exploits
- Anatomy of a Zero-Day Attack
- History
- Evolution of the Threat Landscape
- Corporate Research & Vulnerability Discovery
- Zero-Days and the Dark Web Market
- State-Sponsored Cyber Warfare
- Case Study 1 – Pegasus Spyware
- Case Study 2 – MOVEit
- Case Study 3 – Google Chrome
- Consequences of Zero-Day Attacks
- Strategic Impact
- Prevention Strategies
- Best Practices for Defense
- Collaboration and Global Efforts
- Birght (not so) Future
- Stay Vigilant... rather than a conclusion

Session Introduction

- Understanding the Unseen Threats
  - *Zero-day vulnerabilities represent the most elusive dangers in cybersecurity today. Hidden, unpredictable, and potentially catastrophic, they demand our full attention.*
- Mission Today:
  - Uncover the hidden world of zero-days
  - Understand their real-world impact
  - Learn how to defend against the “undefendable”

Why This Matters Now?

- The Rise of Zero-Day Exploits
  - Surge in zero-day attacks over the past 5 years
  - Increasing sophistication and availability
  - Used in nation-state conflicts, corporate espionage, ransomware

- High Stakes
  - Critical infrastructure at risk
  - Billions lost annually in damages
  - Zero-days = strategic cyber weapons

Defining Zero-Day Exploits

- What is a Zero-Day Vulnerability?
  - A software flaw unknown to the vendor
  - No available patch or fix at the time of discovery
  - **Exploited before detection and remediation**

Anatomy of a Zero-Day Attack

- Initial Discovery:
  - Vulnerability found via fuzzing, reverse engineering, or insider access
- Exploit Development:
  - Crafting stable, undetectable code
- Target Selection:
  - Government, enterprise, supply chain, critical services
- Attack Execution:
  - Often silent, no alerts, no known signatures
- Objectives:
  - Espionage, sabotage, data exfiltration, long-term persistence

History – The Beginning of Zero-Days

- Early Days of Zero-Days
  - Term first used in underground hacker communities (1990s)
  - Originally exploited in pirated software ("0-day warez")
  - Transitioned to security flaws in widely used software

- From Curiosity to Cyberwarfare
  - 2000s: Emergence of commercial exploit markets
  - 2010: Stuxnet, a turning point
  - 2013+: Rise of APTs and cyber weaponization

Evolution of the Threat Landscape

- **The Professionalization of Cybercrime (2010s)**
  - Formation of global cybercrime syndicates
  - Exploit kits for sale (e.g., Angler, Nuclear)
  - Monetization through ransomware-as-a-service (RaaS)

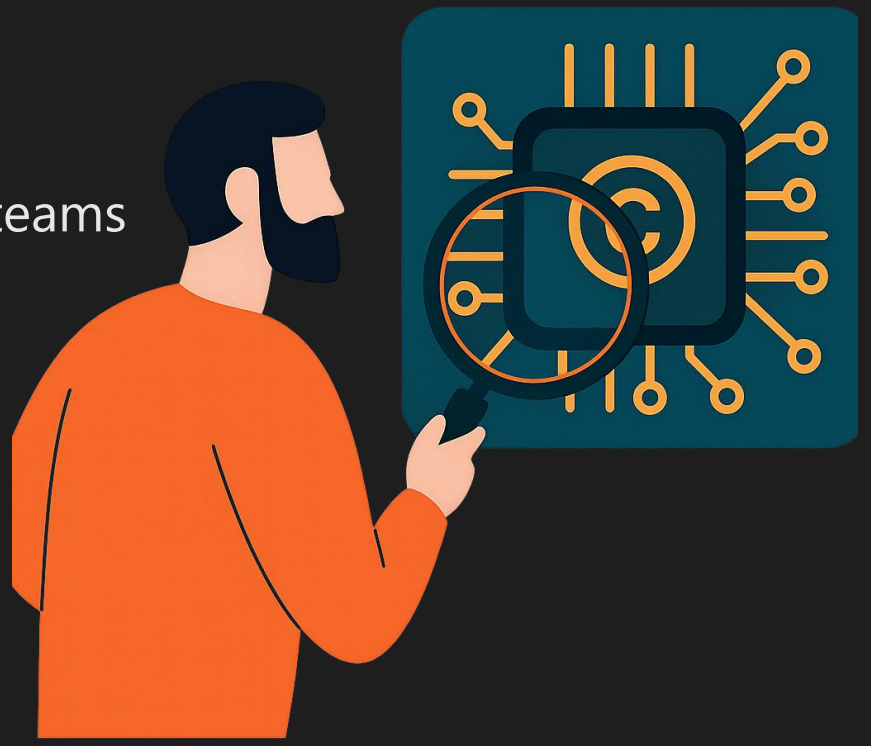
- **State-Backed Operations and Brokers (2020s)**
  - Government-funded exploit research units
  - Emergence of exploit brokers (Zerodium, Exodus, etc.)
  - Strategic buying of vulnerabilities (iOS, Windows, ICS)

- **Modern Attack Dynamics (Zero-days as core element in)**
  - Supply chain compromises (e.g., SolarWinds)
  - Ransomware campaigns (e.g., MOVEit, Kaseya)
  - Targeted surveillance (e.g., Pegasus)
  - Private sales reaching $1M+ per exploit

Corporate Research & Vulnerability Discovery

- Defensive Innovation
  - Google Project Zero: focused on zero-day detection
  - Microsoft, Apple, and others: in-house security response teams
  - Bug bounty platforms (HackerOne, Bugcrowd)

- The White Hat Effort
  - Coordinated Vulnerability Disclosure (CVD)
  - Public zero-day tracking (e.g., MITRE ATT&CK, CISA KEV catalog)
  - Incentivizing ethical hacking over underground sales



Zero-Days and the Dark Web Market

- A Lucrative Underground Economy
  - Private forums, invite-only marketplaces
  - Prices range from $50,000 to over $2 million
  - High demand for iOS, Windows, and ICS/SCADA vulnerabilities

- Buyers and Sellers
  - Brokers, cybercriminals, nation-state proxies
  - Ethical gray zones: legitimate researchers vs. mercenaries
  - Exploits often sold with "support" and update services

State-Sponsored Cyber Warfare

- Zero-Days as Instruments of State Power
  - Used for espionage, sabotage, and influence operations
  - Often remain undetected for months or years
  - Blurred lines: cyber operations vs. acts of war

- Known Operations:
  - Stuxnet – First cyberweapon to cause physical damage
  - NotPetya – Disguised as ransomware, targeted Ukraine
  - APT10 – Global supply chain infiltration campaigns

Case Study 1 – Pegasus Spyware

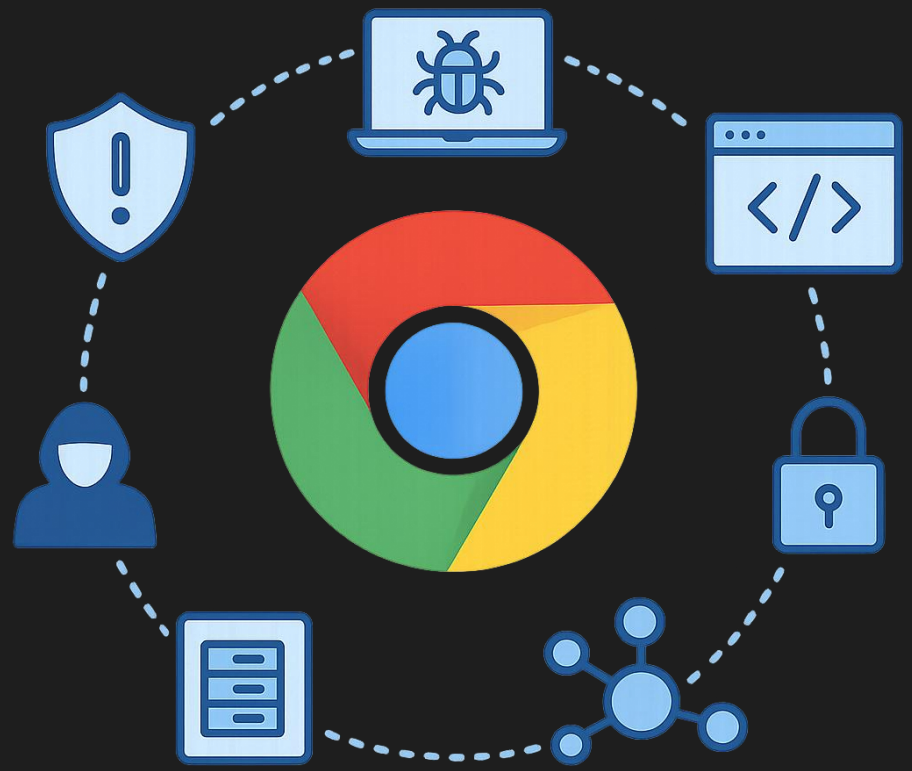
- Zero-Days for Silent Surveillance
- Developed by NSO Group
- Used iOS zero-days to silently infect devices
- No click required (“zero-click” exploits)
- Targets: journalists, activists, diplomats, government officials

Case Study 2 – MOVEit Transfer Vulnerability (2023)

- A Modern Supply Chain Zero-Day
- Discovered in May 2023
- Zero-day in managed file transfer software (Progress MOVEit)
- Exploited by Cl0p ransomware group
- Affected hundreds of organizations across sectors
- Supply chain impact: from government agencies to universities and banks

Case Study 3 – Google Chrome Zero-Days

- A Constant Target
- Over 50 zero-days patched in Chrome since 2021
- Attackers exploit browser engines (Blink, V8)
- Often chained with other exploits for full system access
- Browser-based zero-days = high reward, wide reach



Consequences of Zero-Day Attacks

- Technical Consequences
  - System compromise and lateral movement
  - Disruption of critical services (e.g., healthcare, energy)
  - Data theft, espionage, ransomware deployment

- Business & Societal Impact
  - Financial losses: fines, lawsuits, downtime
  - Loss of public trust and reputational damage
  - National security implications in strategic sectors

Strategic Impact

- Tools of Strategic Disruption
- Targeting critical infrastructure:
  - energy, water, transportation, healthcare
- Exploiting national digital dependencies
- Undermining public trust in essential services
- Cyber attacks are now part of hybrid warfare
- The Cyber Arms Race
  - Zero-days as strategic national assets
  - Governments investing in offensive cyber capabilities
  - Private brokers fueling demand and secrecy
  - No treaties. No transparency. No accountability.

Prevention Strategies - You Can’t Patch What You Don’t Know

- Threat hunting and anomaly detection
- Continuous vulnerability assessments
- Endpoint Detection & Response (EDR) with behaviour analytics
- Threat intelligence feeds and IOC correlation
- Focus on detecting effects, not just known signatures

Best Practices for Defense

- Building Resilience Against the Unknown
- Implement Zero Trust Architecture (ZTA)
- Enforce least privilege access and network segmentation
- Prioritize timely patch management
- Conduct red teaming and tabletop exercises
- Promote security awareness training across all levels
- Resilience is built before the attack, not during it.

Collaboration and Global Efforts

- Fighting Zero-Days Requires Collective Defense
- Public-private partnerships (e.g., CISA, ENISA, CERTs)
- Cross-industry threat intelligence sharing
- International calls for cyber norms and export control
- Transparency in vulnerability disclosure policies
- No one is immune, so no one should be isolated.

Birght (not so) Future

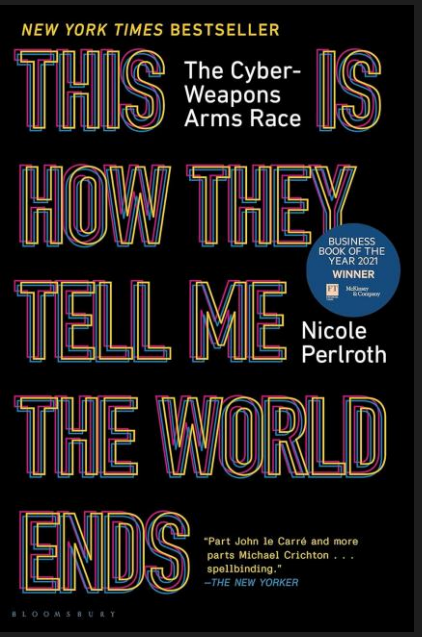
- What the Future Holds
  - More zero-days, shorter exploit-to-weaponization time
  - AI-powered vulnerability discovery and attack automation
  - Greater pressure for transparency and cyber diplomacy
  - **Need for resilience: assume breach, reduce impact**
- Will nered to learn to defend faster than they learn to break us?

Stay Vigilant… rather than a conclusion

- Zero-Days Are Not Just Bugs, They Are Weapons
- Invisible, unpredictable, and devastating
- Used by criminals, governments, and mercenaries alike
- No system is 100% safe, but every system can be made resilient
- Awareness. Preparedness. Collaboration.

Book Recomendation

- Nicole Perlroth
  - This Is How They Tell Me the World Ends:
    The Cyberweapons Arms Race, Bloomsbury Publishing, 2021.
- „The Cyberweapons Arms Race Has Already Begun"



References

- Google Project Zero – https://googleprojectzero.blogspot.com
- CISA (Cybersecurity & Infrastructure Security Agency)
- MITRE ATT&CK Framework – https://attack.mitre.org
- The Pegasus Project – Amnesty International & Forbidden Stories, 2021
- Mandiant / FireEye – Annual Threat Intelligence Reports
- Microsoft Digital Defense Report (2023)
- Recorded Future / Insikt Group – Dark Web Zero-Day Market Analysis
- Reports on exploit pricing and underground forums
- SolarWinds Attack Analysis – CISA, Microsoft, CrowdStrike joint publications
- Rapid7 – Vulnerability Intelligence Reports
- ...


101
101
110
Q&A
0101
100
110
101
101
101