Zero-Day Vulnerabilities: The Underground Market

Stefano Falco 343739
Politecnico di Torino

ABSTRACT

Let's take a moment imagining a castle that looks **impossible to breach**: thick stone walls, a deep moat, a drawbridge that groans shut every night, guards pacing the ramparts with lanterns swinging at their sides. The lord sleeps well, because **everything valuable is defended**.
But castles rarely fall through the main gate.
In fact, one day, someone finds out a **hidden weakness** in the wall that *nobody has noticed* yet: a stone is set a little too loosely. Neither who built it nor the lord imagines its existence. But it's a crack that widened by a hair each winter. A seam that looks perfectly normal unless you know exactly where to press.
From a distance, **the wall is still looking solid**. Same shadows, same strength, same confidence. Yet the right hands can find that tired stone, push gently, and feel it shift. No siege towers. No battering ram. Just a quiet entry where nobody thought an entry was possible.
And the worst part is its **silence**. Welcome, to the *Zero-day land*.

1 INTRODUCTION

Inspired by the seminar held by *Dr. Selene Giupponi* on 1st April 2025, in particular by the video that has been shown about the possible outcomes of a targeted zero-day attack, I've decided to inspect and analyse the theme of **Zero-Day vulnerabilities**.
In addition, the Netflix series *"Zero-Day"* makes me think about whether the audience was effectively aware of how certain scenarios can really show up, and what is behind them in the real world.
Therefore, the primary goal of this report is to provide a comprehensive, technical, and defense-focused analysis of Zero-Day vulnerabilities and the Zero-Day market, emphasizing their implications in the field of **Digital Forensics** and **Cyber Threat Intelligence**.
We know that a vulnerability is an intrinsic weakness in an asset, but in this case, we will need a more accurate definition.
Note that **Figure 1** is referenced throughout to frame this "*window of vulnerability*" during which attackers can operate before detection and patching.

1.1 Project's aim

Along with this report, the themes of **zero-day market**, and in particular white, gray, and black markets, **vulnerabilities equities process**, and **transparency**, as well as some **historical case studies**, will be analyzed, with a focus on how these attacks represented different threat actors and consequences. The central role of proactive and reactive cyber defense will be discussed. Finally, some defense strategies and tools will be presented, as building blocks of an updated notion of "*security*" premised on layered controls and inter-team collaboration.

2 DEFINITIONS AND EXPLOITATION

Let's start with the definition: zero-day vulnerabilities are **security flaws** that are **unknown to the software vendor or the public** at the time of their discovery. In practical terms, this means that no official patch or fix has been released for the flaw, giving defenders "*zero days*" of advance warning to protect against an exploit.
Because, as we just stated, no patch exists initially, any attack exploiting such a vulnerability is by definition a **zero-day exploit**.
Exploits against such flaws often evade signature-based tools and can compromise even fully patched systems. The point is: intrusion detection rules for them do not yet exist. From a defender's perspective, zero-days are among the most dangerous threats.
What about the actual period they can lurk unnoticed? Many studies [1, 2] have found that zero-day flaws have a **surprisingly long average lifespan** in the wild – one study in particular, of real-world data, found an average life expectancy of 6.9 years for a zero-day vulnerability before discovery. [1]
In fact, after one year of a zero-day being privately used, there is only about a 5.7% chance that someone else (e.g., another researcher or adversary) will have independently discovered and disclosed that same flaw. [1]

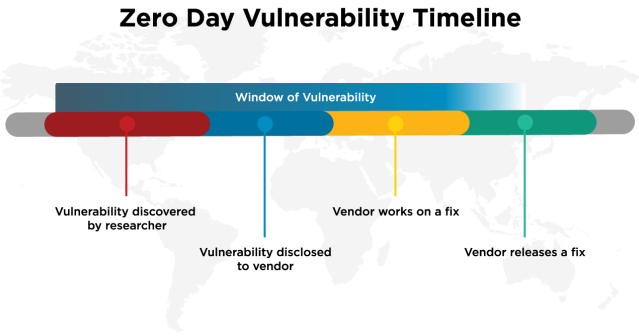


Figure 1: Window of vulnerability overview

This longevity under the radar underscores why these flaws are so prized by attackers.
Once an exploitable zero-day is found, developing a reliable exploit can be relatively quick (median of 22 days of development work according to the mentioned studies), meaning attackers can weaponize a new vulnerability in a matter of weeks. **Figure 2** expands to the vulnerability lifecycle, mapping discovery, private use, disclosure, and patching.
Zero-day exploits typically take advantage of severe weaknesses – for example, a memory corruption bug that allows arbitrary code execution or a logic flaw that bypasses authentication. Attackers deploy zero-day exploits through various vectors: a spear-phishing email with a malicious attachment, a drive-by download on a compromised website, a rogue document or application, or even via plug-in devices.
Since **no patches or signatures exist**, such attacks often succeed undetected, at least initially. For instance, the infamous **Operation Aurora** attack in 2009 [Section 4.2] leveraged an unknown hole in

Microsoft's Internet Explorer – a true zero-day at the time – to infiltrate Google and other companies, stealing intellectual property. Only after **Google publicly revealed the breach** did Microsoft rush to issue a security advisory and patch for that IE vulnerability, which the attackers had been exploiting in secret.

2.1 Criminal Exploitation

As briefly introduced with the previous operation, zero-days are not an exclusive tool of nation-states; **criminal groups and APT** (*Advanced Persistent Threat*) **groups** may also use zero-days when it's profitable or strategically useful. To make another example, the LockBit ransomware group – one of the most prolific cybercrime organizations – has historically obtained access to victims using a variety of methods, including purchased credentials, unpatched known flaws, and even zero-day exploits. [Figure 5]

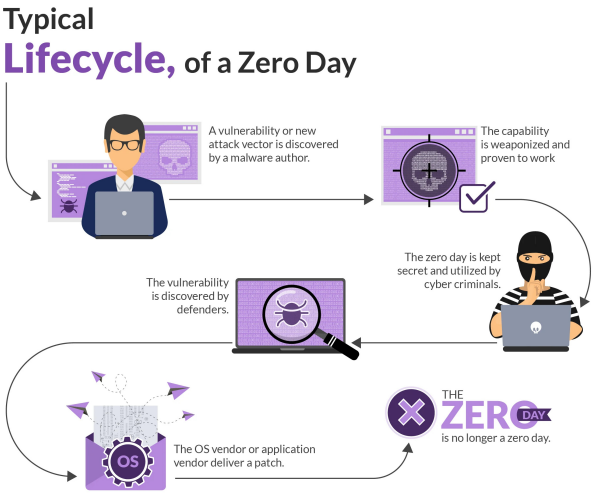


Figure 2: Lifecycle of a zero-day vulnerability

In other words, if a defensive weakness exists, whether known or unknown to the vendor, sophisticated attackers will exploit whichever path is available. This makes **comprehensive defense challenging**: organizations must not only patch known vulnerabilities promptly, but also assume that unknown vulnerabilities may already be in play and adopt a security posture of vigilant monitoring and response.

It should be noted that zero-day attacks, while dangerous, are relatively rare compared to attacks on known issues – **but they are increasing** [7]. **Google's Threat Analysis Group** reported that it tracked 97 zero-day exploits used in the wild in 2023 alone, many of them deployed by commercial spyware vendors and brokers (responsible for 75% of the zero-days targeting Google and Android platforms).

This illustrates that well-resourced threat actors are actively discovering and weaponizing new flaws. Once a zero-day becomes known (e.g., through public disclosure or detected use), it is, of course, no longer a "zero-day" – vendors will issue patches (turning it into an "N-day" vulnerability), and defenders can update protections. However, the **window of exposure before disclosure can be devastating**, which is why zero-days are often used in the earliest stages of high-impact breaches or espionage campaigns.

3 THE ZERO-DAY MARKET

Since zero-day exploits confer such a strategic advantage, I think it should not surprise that a clandestine economy has emerged to trade in these vulnerabilities. In particular, the zero-day market can be thought of as a three-segment iceberg:

- the **white market** (legal channels like bug bounty programs)
- the **gray market** (brokers and private companies buying exploits, often to resell to governments)
- the **black market** (illicit underground forums where criminals trade exploits)

This market exists in a digital space where not only technology and money, but also geopolitics intersect, and it is fueled by the high price zero-days demand and the anonymity of online transactions (often via cryptocurrencies like Bitcoin and Ethereum).

White Market (Responsible Disclosure)

On the legitimate end of the spectrum, many technology companies run bug bounty programs that **reward researchers for responsibly disclosing vulnerabilities**.

- ◇ Firms like Google, Microsoft, and Apple may easily pay from a few hundred to hundreds of thousands of dollars for critical bugs. These programs aim to incentivize hackers to report flaws to vendors so they can be fixed, **rather than exploiting or selling them**.
- ◇ For example, Apple's bug bounty offers up to $1 million for certain iOS zero-click vulnerabilities – a huge sum, yet often still below what the black market might pay.

Gray Market (Exploit Brokers)

A significant slice of zero-day trafficking is conducted by exploit broker companies that operate in a legal gray area.

- ◇ Firms like Zerodium and Crowdfense **openly buy zero-day vulnerabilities** from researchers and then sell or license the exploits to clients (usually government agencies or defense contractors, see Figure 3 for a real reference).
- ◇ Unlike bug bounty programs, gray-market brokers **do not disclose the bugs to the software makers**; instead, the findings are kept secret and provided to government customers. This means the vendor and public remain **unaware of the vulnerability** – it persists as a zero-day that governments might use for espionage or cyber operations.

Black Market (Underground Exploit Trade)

In the criminal underground, zero-days (and exploits for them) are bought and sold in dark web forums and private networks. This true black market is **harder to quantify** but certainly exists.

- ◇ Zero-days are extremely valuable for cybercriminals because they can break into targets that are otherwise hard to compromise (e.g., a new exploit to penetrate a fully patched server).
- ◇ However, for most criminals, it's often cheaper and simpler to use known exploits (for which patches might not be applied universally) than to develop or purchase a fresh zero-day.

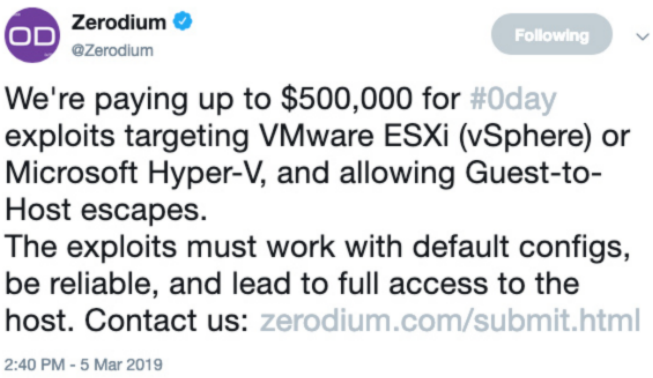


Figure 3: Zerodium's real offer example

That's why the zero-day market is mostly aimed at top-tier buyers: well-funded criminal groups and covert nation-state operators.

- The biggest payouts tend to involve flaws that open doors into critical infrastructure (industrial systems, telecom networks, government databases), and with crypto payments and encrypted chat platforms, these trades can happen more anonymously, making them very hard to trace or shut down.

3.1 The "equities" dilemma

One could say this is a particular economics of vulnerabilities: a severe zero-day in a widely used product is a time-sensitive commodity. Once it's revealed or patched, its value drops dramatically, so both sellers and buyers are **incentivized to use it quickly or keep it secret**. Governments face a classic dilemma here, often termed the "equities" problem:

> "*Should they disclose a discovered zero-day to protect the public (but lose its offensive value), or hoard it for intelligence and warfare purposes?*"

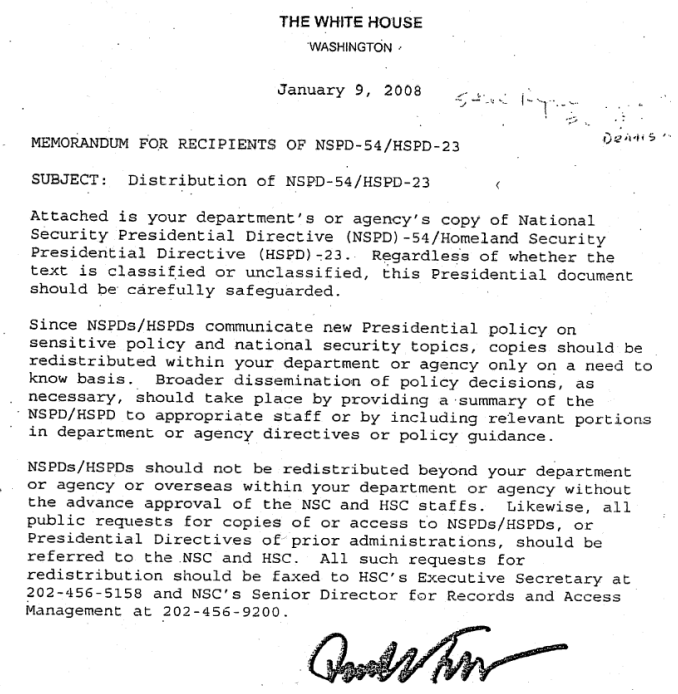
This conflict of interest has led to many policy debates. In the U.S., for example, there is a formal **Vulnerabilities Equities Process** (*VEP*) – an interagency policy that weighs the pros and cons of disclosing vs. retaining a zero-day held by the government.

The *VEP*, which was created in accordance with the *National Security Policy Directive-54/Homeland Security Policy Directive-23* [Figure 4], brings together agencies like the NSA, DHS, FBI, and others to **decide whether a given zero-day should be reported to the vendor** (to patch and improve overall security) **or kept secret** for national security use.
While this process adds some structure, it is largely opaque and ultimately a judgment call balancing public risk against intelligence value.

3.2 Transparency, norms and regulation

The zero-day market is largely **unregulated internationally**, and this raises ethical and security concerns. As noted in one official analysis [8, 11], it's a "complex and unregulated space, where the lines between legality and morality are often blurred."
There is an **increasing call** in the cybersecurity community for transparency and norms around zero-day use – some argue it should be treated like an arms trade (since exploits can be seen as digital weapons) and be subject to international law or agreements.

So far, consensus is hard to reach: nations are reluctant to give up the **strategic advantage that zero-days provide**, even as those same vulnerabilities could be turned against their own citizens by adversaries (e.g., the WannaCry case, Section 4.3). This status quo means the zero-day trade will likely continue to thrive in the shadows, with white-hat researchers, profiteering brokers, and black-hat hackers all vying to discover the next big flaw.



THE WHITE HOUSE
WASHINGTON

January 9, 2008

MEMORANDUM FOR RECIPIENTS OF NSPD-54/HSPD-23

SUBJECT: Distribution of NSPD-54/HSPD-23

Attached is your department's or agency's copy of National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23. Regardless of whether the text is classified or unclassified, this Presidential document should be carefully safeguarded.

Since NSPDs/HSPDs communicate new Presidential policy on sensitive policy and national security topics, copies should be redistributed within your department or agency only on a need to know basis. Broader dissemination of policy decisions, as necessary, should take place by providing a summary of the NSPD/HSPD to appropriate staff or by including relevant portions in department or agency directives or policy guidance.

NSPDs/HSPDs should not be redistributed beyond your department or agency or overseas within your department or agency without the advance approval of the NSC and HSC staffs. Likewise, all public requests for copies of or access to NSPDs/HSPDs, or Presidential Directives of prior administrations, should be referred to the NSC and HSC. All such requests for redistribution should be faxed to HSC's Executive Secretary at 202-456-5158 and NSC's Senior Director for Records and Access Management at 202-456-9200.

Figure 4: First page of the NSPD-54/HSPD-23

4 HISTORICAL INSIGHTS

I think anybody can't really understand the real impact of a phenomenon without real-world examples. Talking in theory is just half the way to comprehend **the whole spectrum of these kinds of vulnerabilities**. Since the video shown by Prof. Selene Giupponi, as well as the Netflix mini-series mentioned in Section 1, might be regarded as "excessive" or "overstated", I've decided to include a few notable historical cases where such exploits were used, and not so long ago, with dramatic results.

4.1 Stuxnet (2010)

Perhaps the most famous one, Stuxnet was a covert state-developed worm (widely attributed to a US-Israeli operation) designed to sabotage Iran's nuclear program. It exploited four separate zero-day vulnerabilities in Windows systems and Siemens industrial control software.

⇒ **Estimated damage**: Between US $243 billion and US $1 trillion in immediate and ripple economic losses. [9]

4.2 Operation Aurora (2009)

In a series of attacks believed to originate from China, hackers targeted Google, Adobe, and other U.S. companies. The attackers used a **then-unknown vulnerability in Internet Explorer 6/7** as a zero-day exploit to penetrate corporate networks.

By luring company employees to a malicious website (likely via spear-phishing), they triggered the IE zero-day to install malware, which opened backdoors and stole intellectual property (including Google source code).

⇒ **Estimated damage**: into the tens to hundreds of millions of dollars, given the scale of the victims and subsequent security overhauls. [5, 6, 10]

4.3 EternalBlue and WannaCry (2017)

EternalBlue is the name of a potent exploit for a zero-day in Microsoft's SMB (Server Message Block) protocol that was originally developed by the U.S. NSA.

The NSA kept this Windows vulnerability **secret for at least five years**, intending to use it for intelligence operations.
However, in 2017, a hacker group known as the Shadow Brokers stole and leaked the EternalBlue exploit, after an attempted auction on the black market failed.
Microsoft had been tipped off and released a patch (MS17-010) in March 2017, **but many systems remained unpatched**. In May 2017, the leaked exploit was integrated into WannaCry, a ransomware worm that spread globally and caused widespread disruption – encrypting files in over 200,000 systems (from UK hospitals to international businesses) within a day.

⇒ **Estimated damage**: About US $4 billion in global damage. [3]

4.4 Pegasus Spyware and iPhone Zero-Days (2016–2021)

Pegasus is a sophisticated mobile spyware suite sold by the Israeli company **NSO Group**, and it has been used by various governments to target journalists, dissidents, and activists. In August 2016, researchers at Citizen Lab exposed an attack on UAE human rights defender Ahmed Mansoor, who had received a suspicious text message. The link led to a chain of three iOS zero-day exploits (dubbed the *Trident exploit chain*) that would have remotely jailbroken his up-to-date iPhone and installed Pegasus.
Apple was alerted and pushed out an emergency patch (iOS 9.3.5) to close those vulnerabilities.

⇒ **Estimated damage**: While the full economic damage of Pegasus remains difficult to quantify, the legal case brought by Meta resulted in a US $168 million punitive damages award against NSO Group for compromising approximately 1,400 WhatsApp accounts. [4, 13]

4.5 LockBit Ransomware Group Breach (2025)

Zero-day exploits can cut both ways – even cybercriminals can fall victim. LockBit is a notorious ransomware-as-a-service gang known to use zero-days in their attacks.

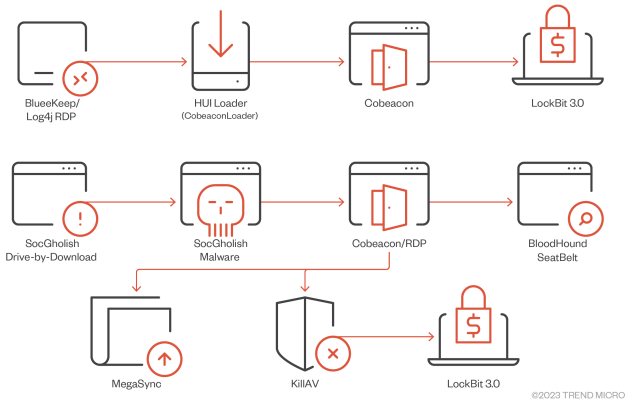


Figure 5: LockBit 3.0 attack flow

In a twist, LockBit's own infrastructure was reportedly breached and defaced in May 2025, with an internal data dump (including wallet addresses, chat logs, and affiliate details) leaked publicly.

⇒ **Estimated damage**: No reliable public financial estimate has been published; the impact is best described as operational and reputational harm (loss of trust, exposure of internal data useful to defenders and law enforcement). [12, 14]

5 DEFENCE AND BEST PRACTICES

Defending against zero-day threats presents a unique challenge due to the inherent nature of these vulnerabilities; as we explained, by definition, they are unknown to both vendors and defenders at the time of exploitation.
Traditional security tools, in particular those based on known signatures, are **largely ineffective in these scenarios**. So, what could we do? **Endpoint Detection and Response** (*EDR*) solutions, combined with anomaly-based detection and **User and Entity Behavior Analytics** (*UEBA*), can play a critical role in identifying suspicious patterns that deviate from baseline activity (such as privilege escalations or anomalous process executions), and therefore they may represent a solid groundwork to start with.

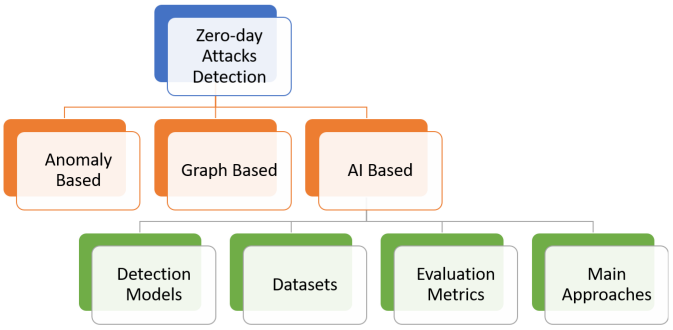


Figure 6: Zero-day detection strategies

While patching cannot defend against zero-days directly, **maintaining strong patch hygiene** reduces reliance on outdated software and prevents adversaries from falling back on known vulnerabilities. In parallel, system hardening measures—such as **enabling**

memory protections like *DEP*, *ASLR*, and **Control Flow Guard** —can frustrate exploit development by increasing the technical complexity required to achieve reliable code execution.

Furthermore, **sandboxing technologies** may be another layer of defence, providing an effective containment strategy by executing potentially malicious files in isolated virtual environments, allowing defenders to safely observe exploit behavior without risk to production systems. However, it may not always be possible, and it would be costly to cover a full "honeypot" system. Complementing this, **system isolation** through the use of virtual machines or containers can prevent zero-day payloads from moving beyond their initial point of entry, but again with similar limitations.

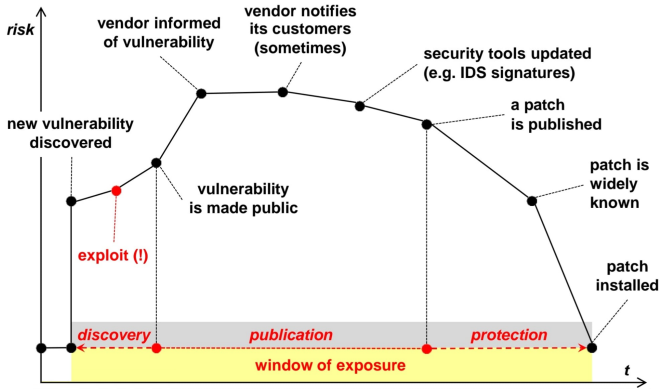


Figure 7: Window of Exposure

We must mention **Cyber threat intelligence** too, which is another cornerstone of zero-day defense. Monitoring emerging threat indicators, including **activity in dark web marketplaces** and disclosure feeds, allows organizations to anticipate and prepare for exploits before they reach critical systems.
When paired with active threat hunting, this intelligence enables teams to detect new attack vectors through forensic analysis of telemetry and logs.

Finally, in addition to technical controls, **user awareness** plays a complementary crucial role. We have seen in the historical insights that **social engineering remains a common vector** for zero-day delivery, particularly via spear-phishing (e.g., in the Operation Aurora, Section 4.2). Educating users on identifying malicious emails and enforcing strict policies around privilege separation, web browsing, and email usage reduces the likelihood of human-facilitated compromise.

6 CONCLUSION

To sum up, defending against zero-days is all about resilience: to quote a master in this field, *"Security is a process, not a product"* (Bruce Schneier).
We have to assume that some attacks will get in undetected; we can focus on limiting their impact, catching them as quickly as possible, and recovering swiftly. Moreover, the importance of **cross-collaboration** cannot be overstated: the Window of exposure detailed in Figure 7 clearly points out the most critical phases to work on, for the vendor as well as the customers. Of course, **prevention** should be the very first line of defence (e.g, disabling unnecessary services/systems, enforcing a security-first culture).
Considering also the human factor, but **assuming no perfect socio-technical system**, we can just ensure that the attackers' "zero-day" advantage is as short-lived as possible.

7 BIBLIOGRAPHY

[1] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay. 2017. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits.* Technical Report RR-1751. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

[2] Leyla Bilge and Tudor Dumitraş. 2012. Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12).* 833–844. https://doi.org/10.1145/2382196.2382284

[3] CBS News. 2017. WannaCry ransomware attack losses could reach $4 billion. (2017). https://www.cbsnews.com/news/wannacry-ransomware-cyence-estimates-4-billion-losses/

[4] Courthouse News Service. 2025. Meta wins $168 million in damages from Israeli cyberintel firm in WhatsApp spyware scandal. (2025). https://www.courthousenews.com/meta-wins-168-million-in-damages-from-israeli-cyberintel-firm-in-whatsapp-spyware-scandal/

[5] M. B. Gazula. 2017. *Cyber Warfare Conflict Analysis and Case Studies.* Ph.D. Dissertation. Massachusetts Institute of Technology. https://dspace.mit.edu/bitstream/handle/1721.1/112518/1012611628-MIT.pdf

[6] Google. 2010. A new approach to China. (2010). https://publicpolicy.googleblog.com/2010/01/new-approach-to-china.html

[7] Google Threat Analysis Group. 2024. 0-day exploitation in the wild in 2023. (2024). https://storage.googleapis.com/gweb-research2024-media/pubtools/pdf/0_day_exploitation_in_the_wild_in_2023.pdf Accessed 2026-02-11.

[8] Jay P. Kesan and Carol M. Hayes. 2016. Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities. *Arizona Law Review* 58 (2016), 753–830. https://arizonalawreview.org/pdf/58-3/58arizlrev753.pdf

[9] Lloyd's and Cambridge Centre for Risk Studies. 2015. Business Blackout: The insurance implications of a cyber attack on the U.S. power grid. (2015). https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout

[10] McAfee Labs. 2010. More Details on "Operation Aurora". (2010). https://www.mcafee.com/blogs/other-blogs/mcafee-labs/more-details-on-operation-aurora/

[11] Taiwo A. Oriola. 2011. Bugs for Sale: Legal and Ethical Proprieties of the Market in Software Vulnerabilities. *John Marshall Journal of Computer & Information Law* 28, 4 (2011), 451–522. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1694&context=jitpl

[12] Reuters. 2025. Ransomware group Lockbit appears to have been hacked, analysts say. (2025). https://www.reuters.com/technology/ransomware-group-lockbit-appears-have-been-hacked-analysts-say-2025-05-08/

[13] The Verge. 2025. Meta awarded $167.25 million over Pegasus spyware attack. (2025). https://www.theverge.com/news/662242/meta-nso-group-pegasus-whatsapp-hack-damages

[14] Trellix. 2025. Inside LockBit's Admin Panel Leak: Affiliates, Victims, and Millions in Crypto. (2025). https://www.trellix.com/blogs/research/inside-the-lockbits-admin-panel-leak-affiliates-victims-and-millions-in-crypto/