

10th Information Security Conference
Athens, February 2023

Spyware Technologies 2023+



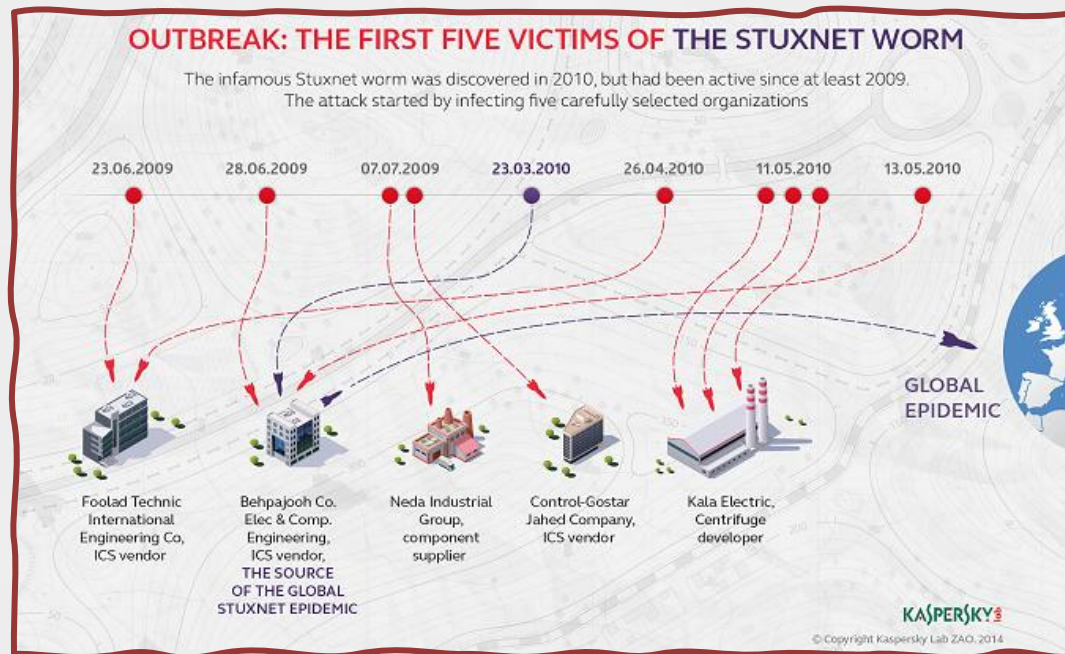
Dimitris A. Gritzalis, Professor of Cybersecurity
Director, MSc Programme on Information Systems Security & Development
Dept. of Informatics, Athens University of Economics & Business

The *zero-day* concept: From Defenders & Attackers...

Zero-Day Vulnerability: An unknown security vulnerability or software flaw that a threat actor can target with malicious code.

Zero-Day Exploit: The technique or tactic a malicious actor uses to leverage the vulnerability to attack a system.

Zero-Day Attack: It occurs when an attacker releases malware to exploit the software vulnerability before the flaw is fixed by software developers.

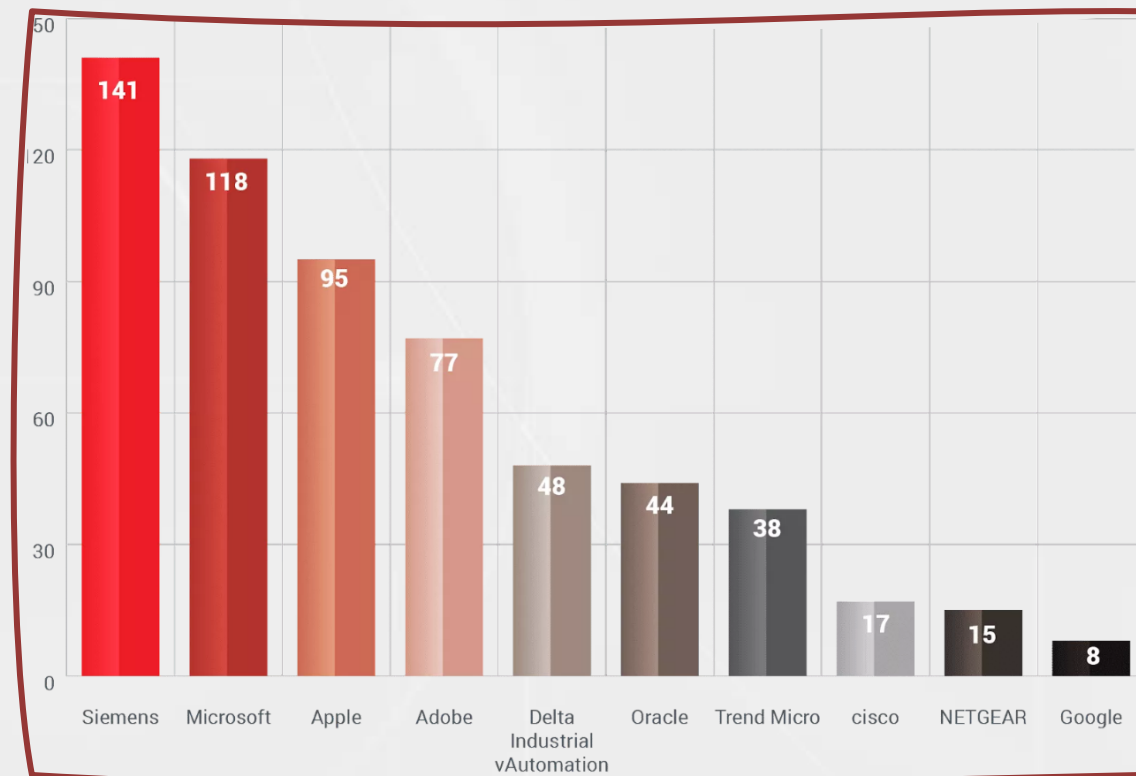


The *zero-day* concept: ...to Brokers & Market

Zero-Day Brokers: People who make or sell malware that's sold to people who will use that malware to exploit people.

Zero-Day Market: It refers to the commercial activity that happens around the trafficking of software exploits.

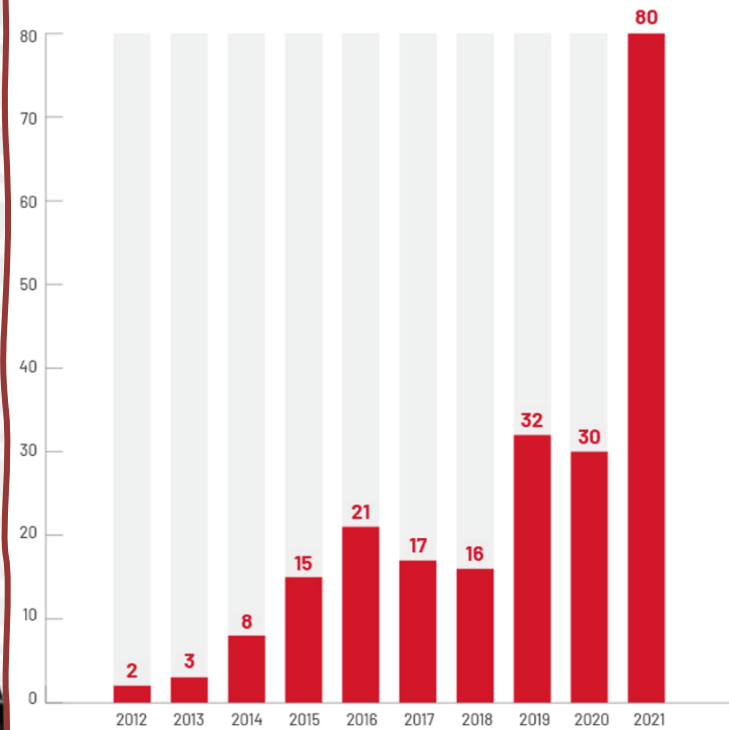
SIRP, Most zero-days observed, 2021.



The zero-day concept: ...to Commercial & State Espionage

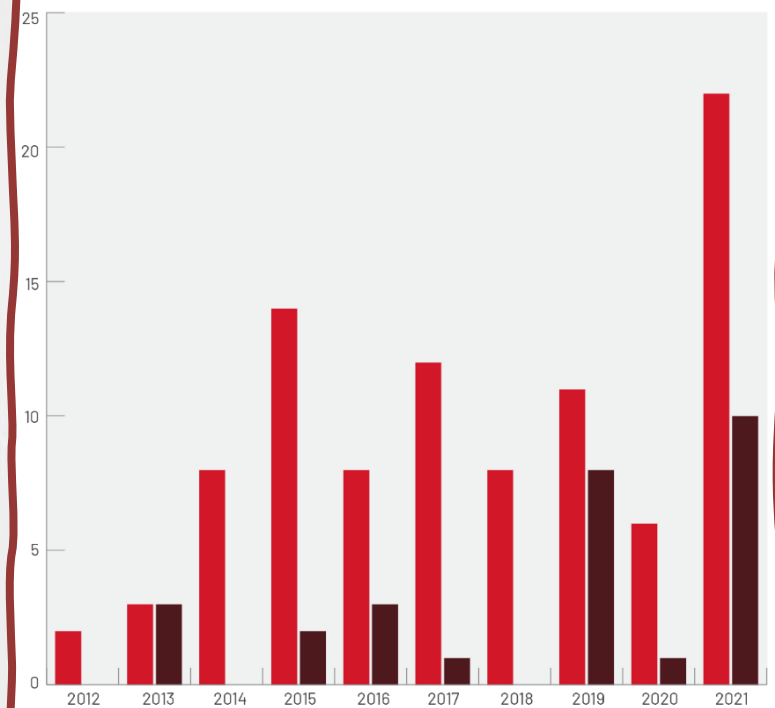
The rise of the Million Dollar Zero-Day Market
and the share of **Espionage/Spyware** and **State-actors**

Zero-Days Exploited
2012-2021



MANDIANT

Espionage Actors Lead Growth
in Zero-Day Exploitation



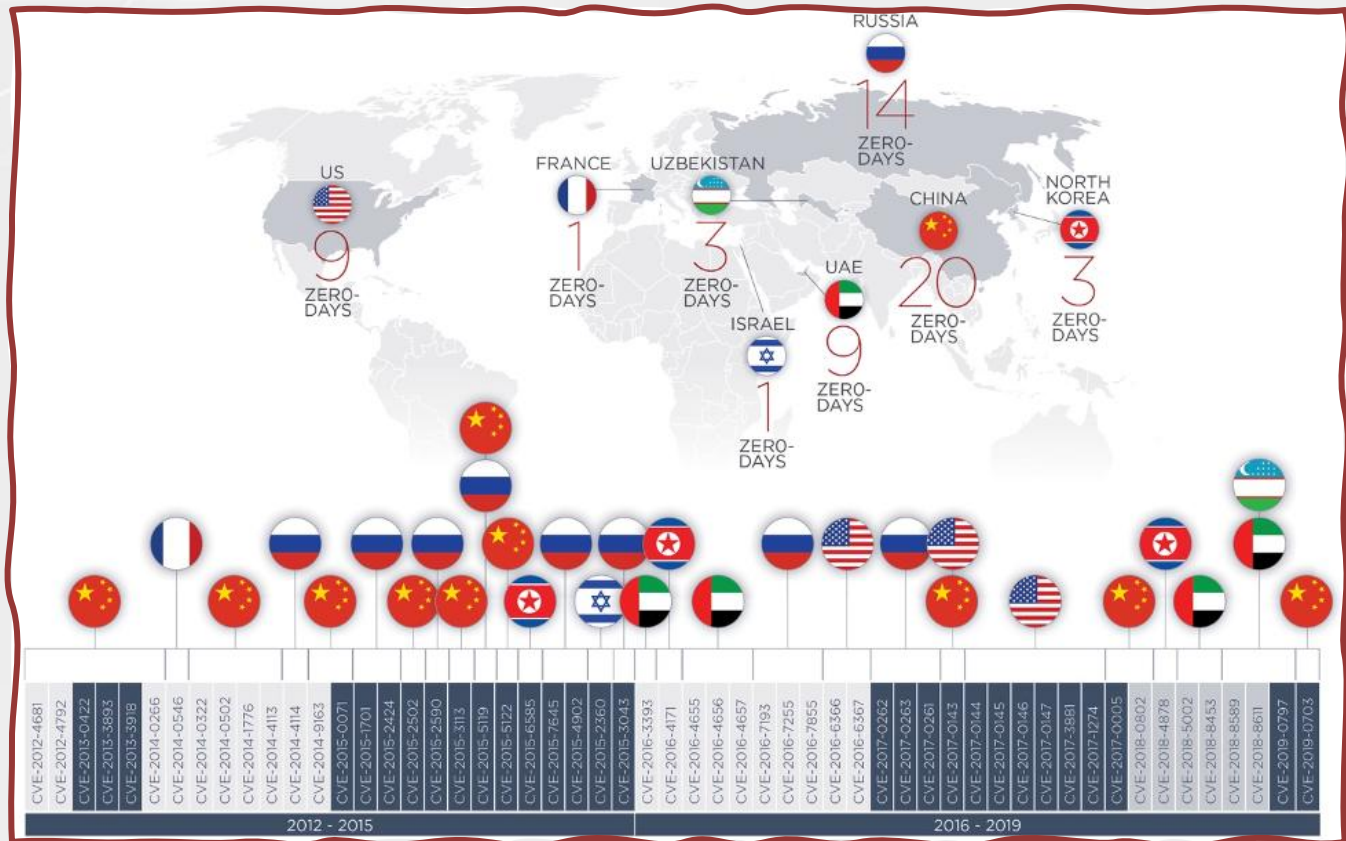
■ Espionage
■ Financial

MANDIANT



The zero-day concept: A geographical view of customers

Zero-day exploits leveraged by groups known or suspected to be **customers of private companies** that **supply offensive cyber tools** and services (MANDIANT)

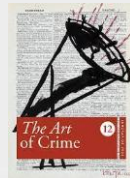


Spyware: A 2-edges sword

Spyware is a type of malicious software that enables someone to obtain, without proper authorization, information about a user smart digital device's activities by covertly transmitting data.

Lecturing about spyware is beneficial for both, spyware **developers**, as well as spyware **defenders**. **Indicators** that refer to spyware detection are usually protected.

Technologies that prevent/detect/neutralize spyware are - for the time being – **not openly disclosed**.



Spyware is a two-edges sword!



ZERODIUM Payouts for Mobiles*



ZERODIUM (2015+): >2K co-operated actors, >15K submitted exploits, >100M\$ paid.



Zerodium reviews and validates all submissions within one week or less. Payments are made in one or multiple installments by bank transfer or cryptocurrencies (e.g. Bitcoin, Monero, Zcash). The first payment is sent within one week or less (<https://zerodium.com>, visited Feb. 1, 2023).



Current Temporary Bounties

Target	Mozilla Thunderbird	Mozilla Thunderbird RCE We are looking for zero-click exploits affecting Thunderbird and leading to remote code execution when receiving/downloading emails, without requiring any user interaction, such as reading the malicious email message or opening an attachment. Exploits relying on opening/reading an email may be acquired for a lower reward.
Bounty	up to \$200,000	
Start Date	27 January 2022	
End Date	TBD	



Brokers bounties: Lessons learnt, so far!

- Exploit-as-a-service:** Zero-day exploits development options is **commercially available** and **financially attractive**.
- Focus:** Interest focuses mainly on exploiting **applications** and **protocols** vulnerabilities.
- Smartphones:** **Android** exploits appear financially more attractive than iOS ones (major geographic deviations exist).
- Messaging & Contact:** There is an interest for popular **message exchange** apps (WhatsApp, iMessage, WeChat, Telegram) and communication **protocols** (SMS, email).
- Operating Systems:** Much better prices offered for **zero-click** exploits (i.e., those needing no communication with the target).
- Locking:** Exploiting **legendary locking** applications (passcode, touch ID) appears more attractive that modern ones (face/finger-print recognition)



A pro-Civic Society & Democracy Evangelist*: My own 2 cents...

- ✓ State-of-the-art surveillance & panoptic technologies remain **away from the public sphere**. Exceptions occur - once in a blue moon.
- ✓ **Spyware** has been exploited by state actors for a while and is **here to stay** - for various reasons.
 - ✓ Spyware is a **two-edges sword**, similar to other edge technologies (e.g. nuclear, etc.).
 - ✓ State Actors (almost only) refer to the **one side** of the spyware potential. Media not always follow.
- ✓ Our **mindset** - as scientists and citizens/civic society members - should be built upon a **holistic view of Cybersecurity**.



* Δ. Γκριτζαλη, *Ασφάλεια και Πολιτική Ανυπακοή στον Κυβερνοχώρο, Εκδόσεις Νέων Τεχνολογιών (2^η έκδοση), Αθήνα, 2020.*

Ελλάδα - Spyware 2023+: Υπάρχουν Δικαστές, Ανεξάρτητες Αρχές, Επιστήμονες!

Η χρήση **προηγμένης τεχνολογίας** για την προάσπιση της εθνικής ανεξαρτησίας και της λαϊκής κυριαρχίας είναι **επιβεβλημένη** και **επαινετέα**.

Η **πανοπτική** παρακολούθηση μέσω προηγμένων τεχνολογιών για την εξυπηρέτηση **αλλότριου συμφέροντος** αποτελεί **αθλιότητα** που στρέφεται κατά της Δημοκρατίας και κάθε Πολίτη.

Το δικαίωμα στο **απόρρητο των επικοινωνιών** είναι το μόνο συνταγματικά **απολύτως απαραβίαστο** ατομικό δικαίωμα (πλην λόγων εθνικής ασφάλειας και σοβαρών εγκλημάτων).

Η ΑΔΑΕ αποτελεί **δικλείδα προάσπισης** των δικαιωμάτων των πολιτών και η ανεξαρτησία της πρέπει να είναι **εγγυημένη** και **απαρβίαστη**.

Η ΑΔΑΕ **δεν μπορεί να αντιτάξει το απόρρητο** ενώπιον του Κοινοβουλίου - του εκφραστή της υπέρτατης συνταγματικής αρχής της λαϊκής κυριαρχίας.

Ο **φόβος** είναι ανθρώπινος, αλλά **ασύμβατος με τη Δημοκρατία** και δεν αποτελεί λόγο υποκρισίας, υπεκφυγής, αποσιώπησης ή απραξίας.

Στη χώρα υπάρχουν άξιοι **Δικαστές**, αξιέπαινες **Ανεξάρτητες Αρχές** και νουνεχείς **Επιστήμονες**! Ελπίζω και αυτοκαθοριζόμενα **ΜΜΕ**.

κυρίως, όμως...
12



Ελλάδα - Spyware 2023+: ...κυρίως όμως υπάρχει η Λαϊκή Κυριαρχία!

...η λαϊκή κυριαρχία επιτάσσει, **θεσμικά**, ότι:

*«Ἡ τήρησις τοῦ Συντάγματος
ἀφιερῶται εἰς τὸν πατριωτισμὸν τῶν Ἑλλήνων»*

Σύνταγμα της Ελλάδας (άρ. 114, 1952)

...η λαϊκή κυριαρχία υπενθυμίζει, **ακτιβιστικά**, ότι:

*«Εμείς άλλον εχθρό δεν έχουμε
παρά μονάχα κείνον που δε σέβεται τον Άνθρωπο»*

Γ. Ρίτσος (1974)

