Quantitative Security

Colorado State University
Yashwant K Malaiya

CS 559
L8: Distance Presentations

CSU Cybersecurity Center
Computer Science Dep

Quick Project Presentations

- Presentations Sept 15, 17 coming week
  - Schedule will be on Canvas discussions
- 12-15 min presentations for each person, 12 slides
  - Need time for discussions
  - When two persons have the same topic, they must collaborate, to minimize overlap. The presentations will be scheduled one after the other.
  - Post slides/abstract 24 hours in advance Canvas Discussions in Quick Research Abstract and presentation forum
  - Everyone should preview upcoming presentations
  - Online section: Submit abstract, presentation and a link to your video by Tuesday 5 PM.
    - Slides: Video: same limits
- On-campus: 5-10 minutes discussion for each presentation
- Everyone must view all presentations, comment/questions on at least half of the presentations
- Provide feedback using the Peer Review form due 9/19 Sat. Also do a detailed review of two assigned reports.

Peer Review form

- Will be available soon in Canvas. Due Sept 19, Sat.
- Evaluate each category using 10-point scale.
  - 10: top 25%, 9: next 25%, 8: next 25%, 7: bottom 25%.
  - 25% is about 7 students.
  - Overall score should be average of the other 4 scores.

Mercenary Mobile Surveillance

An analysis of endpoint compromises, Telephony Interception and Industry Pipeline

Presenter: Brian Alexander
CS 599 – Fall 2026
Instructor: Prof Yashwant K. Malaiya

- Shift in methodologies away from traditional phishing and social engineering to zero-click exploits
- Focus: Analysis of NSO Group (Pegasus), Crytox (Predator) and Circles Platform
- Scope of Research: Mechanics behind the exploits, CVSS Mathematical Modeling, Commercial Pipeline and current defensive countermeasures.

Abstract

- Examines commercial mercenary mobile surveillance and the evolution from traditional mobile spyware.
- Evaluation of the technical mechanics of these surveillance systems, focusing primarily on NSO Group's Pegasus but also looking into methodologies of Cytrox's Predator and Circles platform.
- Analyzes NSO Group's BLASTPASS exploit chain for initiating Pegasus is analyzed showing how it bypasses sandboxing and assessing the CVSS mathematical framework to show the threat levels of zero-click spyware.
- Reviews forensic reverse-engineering discoveries, corporate talent pipelines via the European Parliament's PEGA Committee findings, and countermeasures such as Apple's Lockdown Mode and memory-safe language adoption.

Current Evolution of Mobile Exploitations

- Traditional Approach: Phishing which depended on user interaction, at least one-click. Relied on social engineering, malicious links and user error.
- Zero-Click Exploitations: Can compromise mobile devices with no user interaction, no visible alerts and no forensic data for users to see.
- Shift of methodology of the attacks are moving away from browsers and are now targeting low-level background systems daemons.

NSO Group's Pegasus Execution and Vulnerabilities

- Operates in memory, without on-disk persistence evading mobile OS file system audits.
- Root/Kernel privileges are gained allowing access to live microphone and camera streams, GPS tracking and contacts. The diagram outlines all access granted.
- Captures input directly from application memory prior to any encryption during sending.

Diagram from purported NSO Group Pegasus documentation

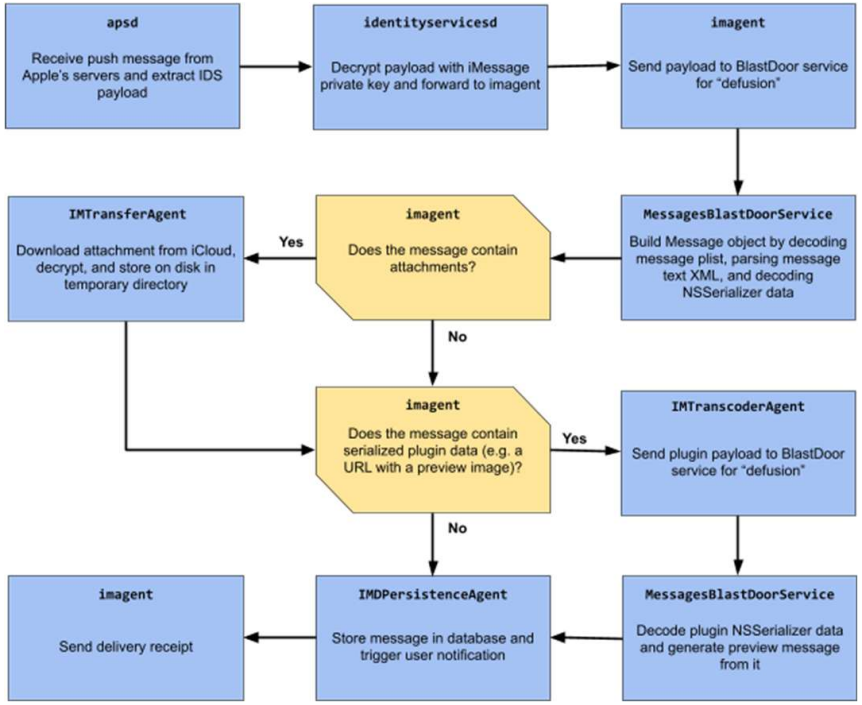
[2] B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak, and R. Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep. No. 113, Sep. 2018. [Online]. Available: https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[5] Amnesty International Security Lab, "Forensic Methodology Report: How to Catch NSO Group's Pegasus," Amnesty International, Tech. Rep., Jul. 2021.

Functionality of one Pegasus zero-click exploit: BLASTPASS

- Targeted Apple iOS devices running out of date media parsers.
- Apple's BlastDoor sandbox was created specifically to isolate untrusted media; BLASTPASS bypassed it entirely by packaging WebP images inside PassKit (.pkpass) Wallet attachments.
- The exploit utilized automatic system daemon parsing immediately upon receiving and forcing a heap buffer overflow from malicious code planted inside. This overflow corrupted memory pointers and allowed code execution.
- Upon receiving the Apple Push Notification packet the OS signals to download and unpack the attachment. The overflow triggers before attachment processing is completed aborting the process before IMDPersistenceAgent triggers alerts or logs.

[1] B. Marczak, J. Scott-Railton, R. Deibert, and S. Anstis, "BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep., Sep. 2023.
[6] I. Beer, "Blasting Past Webp: An analysis of the NSO BLASTPASS iMessage exploit," Google Project Zero, Tech. Rep., Mar. 2025. [Online]. Available: https://projectzero.google/2025/03/blasting-past-webp.html



Heap buffer overflow & code execution happens here aborting notifications

Quantitative Comparison of Documented Exploits

- Note all exploits have a ranking of high, we shall see later the calculations are done with User Interaction as necessary, since they are not it should be even higher.
- Size of known Pegasus Network

Exploit Chain	Target Component / Parser	Target Daemons / Processes	CVE Identifier	Base Score (CVSS v3.1)	Zero-Click Vector	Source
FORCEDENTRY	CoreGraphics / JBIG2 Engine	IMTranscoderAgent	CVE-2021-30860	8.8 (High)	iMessage .gif (disguised PDF/JBIG2)	[2], [4]
BLASTPASS (1)	ImageIO / WebP Decoding	PassKit, Wallet	CVE-2023-41064	8.8 (High)	Malicious .pkpass Wallet attachment	[1], [6]
BLASTPASS (2)	Apple Wallet Framework	SpringBoard, Wallet	CVE-2023-41061	8.8 (High)	Malicious .pkpass Wallet attachment	[1], [6]
Pegasus C2 Mapping	Global Command & Control	Anonymizing Proxy Networks	N/A	36 Clusters / 45 Nations	Over-The-Air DNS fingerprinting	[2]

[1] B. Marczak, J. Scott-Railton, R. Deibert, and S. Anstis, "BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep., Sep. 2023.
[4] I. Beer and S. Groß, "FORCEDENTRY: Zero-Click, Zero-Day Exploit Chained with CoreGraphics Parsing Engine," *Google Project Zero Technical Disclosures*, Dec. 15, 2021.

CVSS Exploitability Metric: Risk Modeling

- Key Terms: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI); Confidentiality, Integrity and Availability (C.I.A)
- Common Vulnerability Scoring System, CVSS created to score exploits with a base score. Utilizing standard metrics for the levels of these interactions.
  - Exploitability = 8.22 x AV x AC x PR x UI
- With PR and UI requiring No interaction and AV being over network will yield an Exploitability of:
  - Exploitability = 8.22 x 0.85 x 0.77 x 0.85 x 0.85 = 3.89
- Then impact is calculated as:
  - Impact = 6.42 x (1- (1-C) x (1 – I) x (1-A))
- With root/kernel access and the other applications these are all considered high so 0.56.
  - Impact = $6.42 \times (1 - (1-0.56)^3) = 5.87$
- BaseScore = RoundUp(Impact + Exploitability)
  - RoundUp(3.89 + 5.87) = 9.8 (Critical)

Isolated assessments assigned these exploits as 8.8 (High) assuming user interaction was necessary for media files. Weaponized zero-click exploits change UI: Required (0.62) to UI: None (0.85), leading to a Critical Score.

[13] FIRST, "Common Vulnerability Scoring System v3.1: Specification Document," Forum of Incident Response and Security Teams (FIRST), Standard Spec., 2019. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

Endpoint Exploitation vs. Cullular Core Interception

- NSO Group's Pegasus installed via BlastPass or other exploits utilizes Endpoint Exploitation to direct install in memory on mobile OS.
- Circles Platform is another zero-click exploit directly to telecom protocols at the carrier routing level.
  - Signal System No. 7 (SS7) commands are utilized to gain zero-touch access to the devices geolocation.
  - Accomplished with zero installation of software onto the device.

[3] B. Marczak, J. Scott-Railton, S. P. Rao, S. Anstis, and R. Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep. No. 133, Dec. 2020. [Online]. Available: https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[7] P1 Security Telecom Labs, "SS7, Diameter, GTP, IMS & 5G Vulnerabilities: Legacy and Modern Protocols at Risk," P1 Security Research, White Paper, Aug. 2025.

Uncovering In-The-Wild Exploits

- Citizen Labs, from The University of Toronto is one of the leading watchdog organizations to research these exploits and work with the carriers.
  - Work with civil society orgs to analyze crash logs, network dumps and incoming attachments.
- Utilize reverse-engineering techniques to disassemble binaries using debuggers and IDA Pro mapping out sequences.
- Pivot off any IP addresses or URLs using open-source data sources like virus total or reverse DNS to link Indicators of Comopromise (IOCs) and malware samples to known groups, campaigns.

[5] Amnesty International Security Lab, "Forensic Methodology Report: How to Catch NSO Group's Pegasus," Amnesty International, Tech. Rep., Jul. 2021.
[9] G. Alexander (Security Engineer, Google; former Research Fellow, The Citizen Lab), Private Communication, Sep. 2026.

Israeli Military Pipeline to Corporate Enterprise

- Israeli Defense Force's IDF Unity 8200 is an elite taskforce for cyberwarfare, counterintelligence and surveillance.
- Elite veterans from this force have became the founding members of the commercial spyware enterprises that have been discussed: NSO Group, Circle Platform and Crytox.
- These organizations hold facilities across Isreal, Cyprus and Greece to circumvent export restrictions and the U.S. Entity List.

[10] B. Marczak, J. Scott-Railton, Q. Gallagher, et al., "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware," The Citizen Lab, Res. Rep. No. 150, Dec. 2021.
[12] European Parliament, "Report of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA)," European Parliament, Doc. A9-0189/2023, May 2023.

Modern Defense and Mitigation

- Google and Apple are transitioning OS system components from C/C++ to memory-safe languages like Rust.
- Apple has introduced Lockdown Mode a feature that will block ambient attachment processing, and untrusted WebP parsers, this has been proven to mitigate the BlastPass exploit discussed.
- Groups like Citizen Lab help with independent academic reporting and coordination of blacklisting commercial vendors.

[8] Google Security Team, "Memory Safety in Android: Shifting to Rust to Eliminate Vulnerabilities," Google Open Source Blog, Technical Report, 2023.

Research Authorities

- Citizen Lab's detailed reports of exploits were the most definitive authorities after reverse engineering them.
  - Citizen Lab's *BLASTPASS Report* (Marczak et al., 2023) & Citizen Lab's *Running in Circles Report* (Marczak et al., 2020)
- European Parliament PEGA Committee Inquiry Report (2023)
  - First government verification of independent research.
  - Driving force for increase in policy and sanctions for commercial spyware.

[1] B. Marczak, J. Scott-Railton, R. Deibert, and S. Anstis, "BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep., Sep. 2023.
[3] B. Marczak, J. Scott-Railton, S. P. Rao, S. Anstis, and R. Deibert, "Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles," The Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, Res. Rep. No. 133, Dec. 2020. [Online]. Available: https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
[12] European Parliament, "Report of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA)," European Parliament, Doc. A9-0189/2023, May 2023.

Closing Remarks

- As endpoint sandbox architecture becomes more common, mercenary spyware has continued to adapt.
- Multi-component exploit chains and carrier level exploitation has led to increased threat with zero User Interaction spyware being able to be deployed on mobile devices.
- Increased sanctions and policy are needed now more than ever to protect the privacy and safety of all phone users.

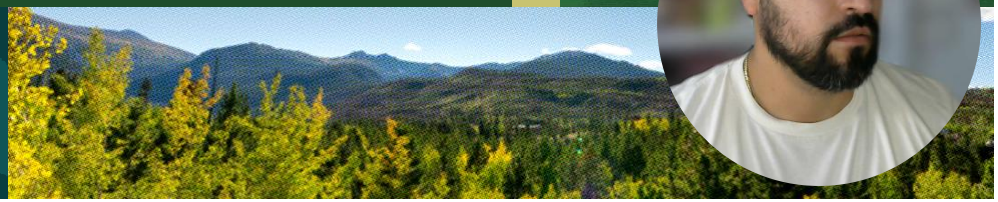
COLORADO STATE UNIVERSITY

Quantifying the Relationship Between Security Investment Achieved Security

Jose Flores

CS559 Quantitative Security – Fall 2026

Instructor: Prof. Yashwant Malaiya



Abstract

- Organizations invest in cybersecurity but cannot directly measure the return on investment.
- Gordon and Loeb's 2002 economic model shows that optimal spending falls well below the expected loss from a breach.
- Later research shows that when organizations are connected, they may either under or over invest, although evidence shows underinvestment.
- Commercial Cyber Risk Quantification tools now assign a dollar value to a security risk, helping organizations measure risk directly.

Current Status

- Organizations spend to make their information less vulnerable but cannot directly measure the return.
    - It is difficult for organizations to tell whether each dollar buy proportional security, or whether returns diminish past a point
- Studied since 2002, when Gordon and Loeb published an economic model of optimal security investment [1]
- Other work: How one company's security choices affect connected companies and their spending [2]
- Most recently: Cyber Risk Quantification tools that set a dollar amount to security risk [3]

The Gordon-Loeb Model

- **Scope:** A single organization over a single time period.
- **Three inputs:** Probability of a threat, Vulnerability, Potential Loss
- **Key assumption:** investment t reduces vulnerability, but cannot reduce the threat
- **S(z,v)** = chance of breach after investing **z**, with no spending, that chance is simply the vulnerability
    - Each additional dollar produces a smaller reduction than the one before it
    - No set amount of money make the information perfectly secure

Citation [1]

Expected Benefit and Net Benefit

- **Benefit of spending:** the reduction in expected loss
  - **EBIS(z) = [v – S(z,v)]L**
- **Net benefit:** subtracts what was spent
  - **ENBIS(z) = [v – S(z,v)]L – z**
- **Goal:** maximize the net benefit, where the gap between benefit and cost is the greatest
  - **$-S_z(z^*,v)L = 1$**

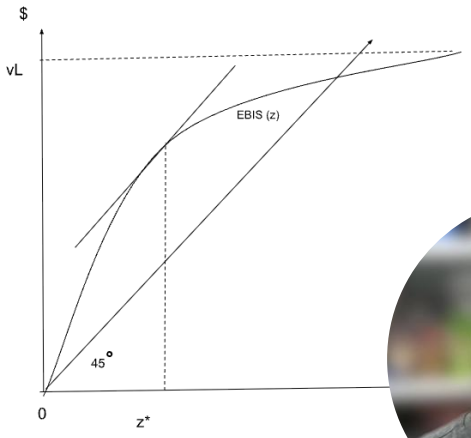


Fig. 1. Expected benefit and cost of security investment, adapte

Citation [1]

The 37% Limit

- Optimal Spending: Always ≤ 37% of the expected loss without any investment
  - **$Z^*(v) \leq (1/e)vL$**
- This is a limit, not a recommendation
- Depending on assumption, the limit can be as low as 25%

Citation [1]

Second Finding: Vulnerability is Not Priority

- Organizations should not automatically spend more because information is more vulnerable
- When information is very vulnerable, a set amount of spending slightly lowers expected loss
    - Moderately vulnerable information may be the better investment
- Instead, what matters is how much the investment reduces expected loss, not how vulnerable the information is.

Citation [1]

Limitations of the Model

- Single time period only
- Assumes money can be spent in small amounts
- Assumes losses stay within a certain size, not disasters or publics assets
- No procedure to determine threat or vulnerability probabilities
- Does not cover how one company's security decision affects others

Citation [1]

Recent Developments: Connections Between Companies

- Gordon and Loeb's model didn't cover one company's security affecting another, but later research addressed this
- Two ways a company's spending is affected by other companies:
    - **Technical**
        - Organizations linked through shared networks rely on each others security and underinvest
    - **Competitive markets**
        - If a company overinvest, attackers are more likely to target less protected competitors

Citation [1], [2]

Recent Developments: Companies Underinvest

- Companies spend too little and can measure the return, so they wait and see
- ~90% know cyberattacks are a high risk but awareness alone doesn't lead them to spend
- €4,530/ year average security spend(Italian company survey), about 15% of one worker's yearly pay
- Companies that have already been attacked are more likely to invest in prevention

Citation [2]

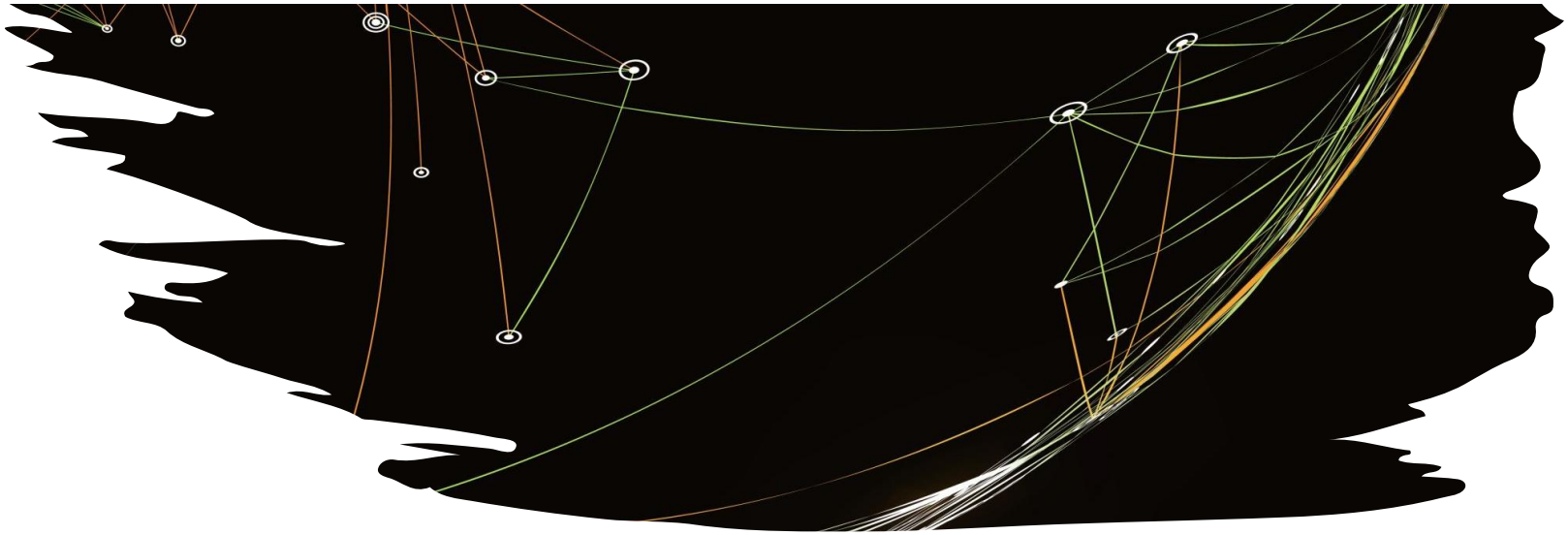
Current Products: Cyber Risk Quantification

- **CRQ** tools measure cyber risk in dollars
- Forrester 2025 top ranked tools: Safe Security, Axio, KPMG
- Capability shift: basic risk modeling in 2023 and automated recommendation and trend analysis in 2025
- Dollar amount instead of a score: helps companies make better investment decisions
- Analyst prediction: fully automated by 2027, with no user-estimated losses or attack probabilities

Citation [3]

Organizations, Key Documents, Conclusions

- **Three influential organizations**
  - **UMD, Robert H. Smith School of Business**: where the foundational model was developed
  - **Forrester Research**: ranks CRQ tools, tracked positions shifts since 2023
  - **Safe Security**: industry leader, first in the Forrester's 2025 rankings
- **Three key documents**
  - [1] Gordon & Loeb (2002): foundational paper, the model and the 37% limit
  - [2]Abrardi, Comino & Grassini(2026): connections between companies and evidence of underinvestment
  - [3]Novinson(2025): Forrrester's ranking and how tools evolved since 2023
- **Conclusion**
  - More spending is no directly proportional to more security
  - There is a point where spending is no longer worth it
  - Connected companies can under or over invest. Evidence shows, they spend too little because they can't measure return
  - CRQ tools set a dollar value on risk so companies can decide better



Botnets, Formation, Progression and Detection Controls

SHANKARA NARAYANAN

Abstract

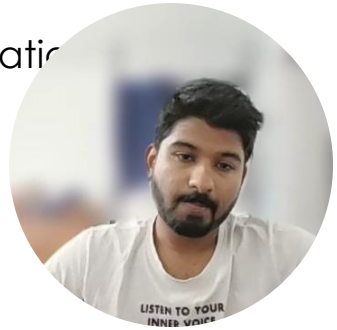
- Botnets represent a major threat to DDoS attacks, crypto mining and credential harvesting.
- In this presentation we focus more on its effects on Internet of Things environments.
- We will evaluate the quantitative mathematical models and describe how these infections spread across networks.
- We will conclude by reviewing the main defense me used to mitigate threats.

Current State of Technology

- Botnets are a major threat in cyberspace primarily because attackers actively target IoT endpoints.
- Targeted endpoints include IP cameras, home routers, and other vulnerable edge devices.
- These devices are easily compromised and for automated attacks due to default passwords, or outdated firmware.
- Modern botnet designs are actively moving away from traditional centralized control.
- Instead, attackers use decentralized approaches to make the botnets significantly harder to down.

Recent Development Hyper Volumetric Scale

- The scale of DDoS attacks has increased significantly.
- This growth requires mitigation systems capable of handling much higher volumes of traffic than in previous years.
- In recent incidents, attack thresholds have easily surpassed multi-terabit levels.
- Some of the largest volumetric attacks have reached staggering peaks of over 30 terabits per second.
- These assaults often combine high packet-per-second floods with application-layer request saturati



Recent Development – Cloud Nodes & C2

- **Exploitation of Cloud Nodes:** Attackers are now compromising misconfigured cloud instances and container environments alongside IoT devices.
- Bots operating from cloud infrastructure can generate much higher throughput per infected node compared to traditional, low-bandwidth IoT-based bots.
- **Decentralized C2 Topologies:** There has been a major shift in command and control (C2) architectures.
- Botnets have transitioned from single-server models to decentralized, peer-to-peer (P2P) structures.
- In these newer architectures, instructions are validated using cryptographic methods and seamlessly routed between neighboring peers.

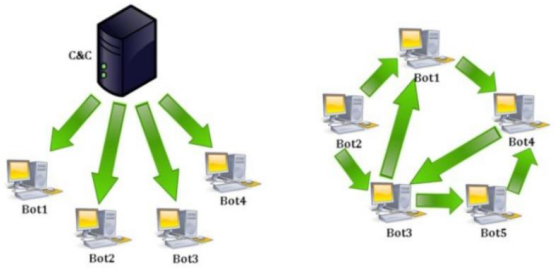


Figure 1: Comparison of Botnet Command and Control (C2) Topologies

Quantitative Modeling (The RCS Model)

- **The Baseline Model:** We can quantitatively model how botnets spread across vulnerable networks using the Random Constant Spread (RCS) model.
- **The Equation:** $\frac{da}{dt} = K \cdot a(1 - a)$
- **Variable Breakdown:**
  - a: Proportion of vulnerable machines currently infected (0 to 1).
  - K: Initial compromise rate (how efficiently the botnet scans/infects).
  - $(1 - a)$: Remaining proportion of uninfected vulnerable hosts.
- **Application:** This model describes t rapid early growth of an infecti during the critical window wh patches are unavailable.

Infection Dynamics

- The RCS differential equation produces a classic logistic "S-curve".
- During the initial scanning phase, the botnet grows exponentially as more compromised nodes join the swarm and begin scanning.
- The curve eventually flattens out and reaches saturation as the available pool of uninfected vulnerable targets is depleted.

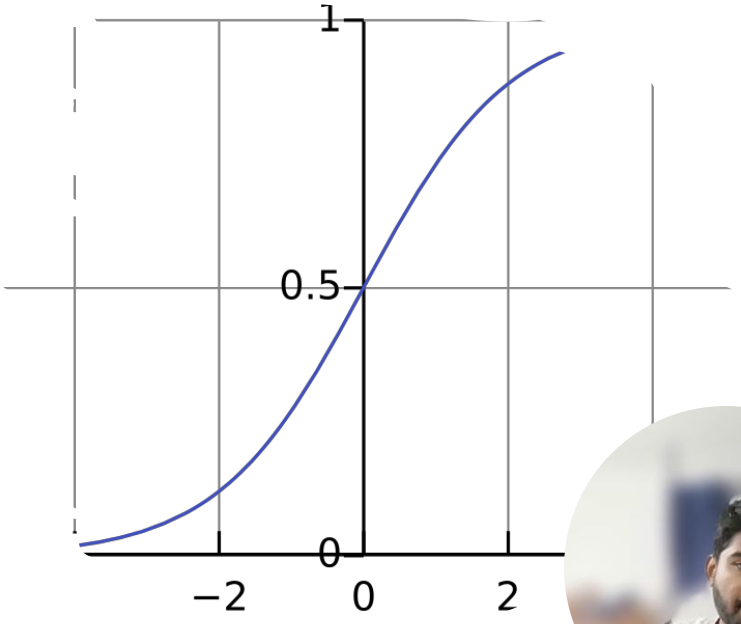


Figure 2: Random Constant Spread (RCS) Logistic Infection Curve

A Bar Chart of the Data (Hyper-Volumetric Trends)

- Recent data highlights the exponential growth predicted by infection models.
- In Q4 of 2024, a Mirai-Variant botnet reached a peak scale of 5.6 Tbps utilizing L3/L4 UDP Floods.
- In May 2025, the Mantis botnet (and other HTTPS botnets) reached 7.3 Tbps leveraging HTTPS Requests/sec.
- In Q4 of 2025, an unnamed variant reached an unprecedented 31.4 Tbps utilizing L3/L4 Multi-Vector attacks.

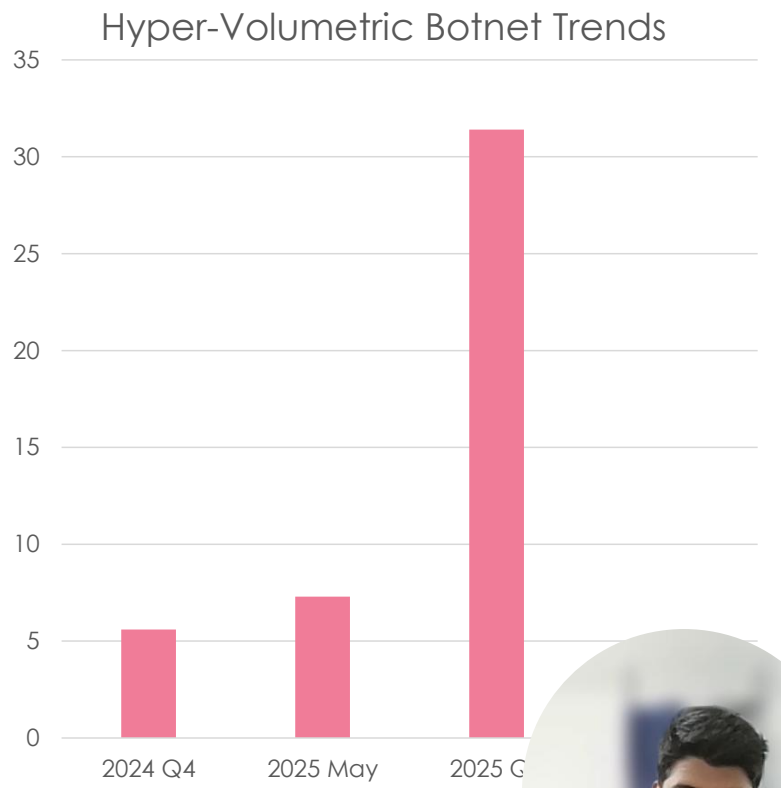


Figure 3: Peak Hyper-Volumetric DDoS (2024–2025)

Mature Technologies - Edge Scrubbing & Routing

- To successfully address multi-terabit attacks, it is essential to utilize automated edge-based mitigation strategies.
- **BGP Anycast Routing:** This technology distributes inbound volumetric attack traffic.
- Traffic is geographically distributed across globally distributed points of presence.
- This specific approach dissipates the impact and energy of the attack before it can reach the origin servers.

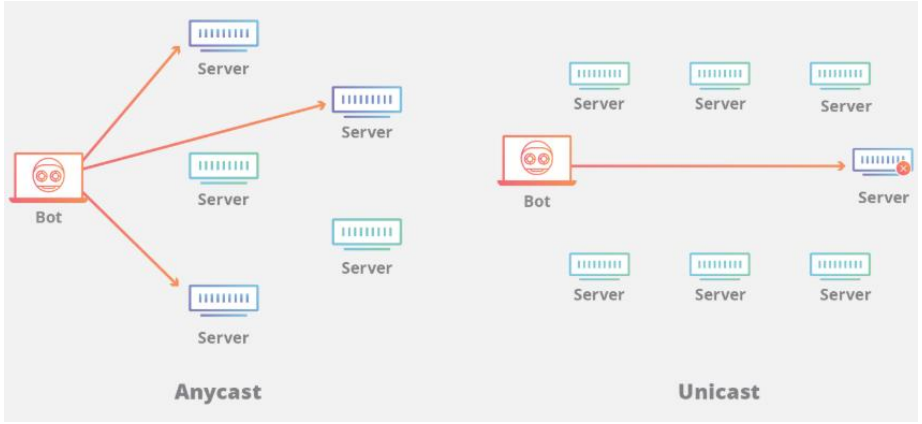


Figure 4: BGP Anycast vs. Unicast Volumetric DD

Mature Technologies - WAFs & Commercial Solutions

- **Edge Web Application Firewalls (WAF):** These firewalls perform inline inspection to detect anomalies in layer-7 protocols.
- WAFs evaluate layer-7 protocol anomalies and enforce dynamic rate limiting to control abusive traffic originating from autonomous systems.
- **Commercial Solutions:** Platforms such as Cloudflare Magic Transit and Akamai Prolexic are industry standards.
- These platforms provide mature, widely adopted techno for traffic scrubbing and real-time perimeter protection.

Influential Organizations

- **Cloudflare:** Leads the industry in global Anycast threat scrubbing and publishes frequent telemetry on volumetric DDoS shifts.
- **Akamai Technologies:** Pioneered the use of large-scale edge distribution networks and produces critical threat intelligence tracking application-layer botnet behaviors.
- **CISA:** Coordinates systemic vulnerability remediation across public and private critical infrastructure.
- CISA is also responsible for issuing CVE notices and activ managing botnet takedown efforts.