Overview

I applaud the work that went into this report from across government and private sector. The conditions that lead to "Automated Distributed Threats" are a critical, systemic, and under-addressed issue that markets, for all their beneficial characteristics, have yet to address. There are a large class of issues, of which botnets used for DDoS are only one. We have more options with some of these threats than with others. Looking across the entire lifecycle of devices provides a greater range of available tools for all classes of threats, whether automated and distributed, or otherwise.

For instance, DDoS botnets are multi-stage threats, and each stage presents an opportunity to head off. They must be vulnerable and exposed; exploited to join the Botnet; directed to act in concert with bot peers. Harm typically comes from resource exhaustion, such as bandwidth, server processing capabilities, etc. Harm can be amplified by focusing on a single point of failure, such as a single DNS provider, serving as the sole provider for a large number of organizations.

On the other hand, automated distributed threats such as WannaCry and NotPetya have a much shorter "kill chain" than DDoS botnets, which give fewer options. These two threats caused harm at the point of exploitation by disabling systems that were both vulnerable and exposed, while spreading to other vulnerable, exposed systems at the speed of the network. Fortunately, subsets of approaches that work to staunch this type of threat also work against other types.

It may be instructional to give an example from the science fiction genre that some in government find illustrative.[1] When zombies[2] start appearing, building high walls is one approach to protect against them. Yet this fails to defend from fast-moving, high-jumping, intelligent, flash-mobbing zombies who can get over walls.[3] Halting the infection of new zombies, however, protects against the corny zombies as well as the scary ones. And perhaps most importantly, those who can't get into the defensive perimeters have much greater survivability.

The most effective and efficient approaches concentrate effort on the greatest impact with the least effort. The best approaches would look to align incentives, for all stakeholders, at points of greatest leverage throughout the supply chain and chain of operations.

- Design and manufacture gives capabilities to equip defenders.
- Network providers can form a gating function to the shared resource of the Internet.
- Avoiding single points of failure in architecture, design, and operations.
- Organizational procurement, government oversight, and ex-post remedies provide the most advantageous leverage points.

Current State of the Ecosystem and Vision for the Future

I'm very pleased to see that Section II accurately and succinctly characterizes the current state of the ecosystem. In particular, the recognition that known effective practices are underused by consumers and organizations, as well as the use of legacy and other systems that cannot be secured without

[1] Zombie Preparedness, CDC, https://www.cdc.gov/phpr/zombie/index.htm

[2] An earlier term for botnets and bots was zombies, because of the similarity between the biological and computing process of zombification.

[3] *World War Z*, directed by Marc Forster, 2013, Plan B Films. Based on the excellent book: Max Brooks, *World War Z*, 2006, Crown Books.

considerable effort. Further, the document as a whole recognizes that harm can accrue to multiple parties, that victims may propagate harm, and that no single approach can solve all of the issues.

The report highlights efforts and desire for greater standardization for security. While standards are good, they tend to be brittle, backward-looking, and take many years to develop and implement across the market. On the other hand, frameworks can enumerate classes of capabilities, objectives, and drivers in a way that is more flexible and evergreen. I've been fortunate enough to contribute to such frameworks as the NIST Cybersecurity Framework,[4] an excellent example for operations, as well as I Am The Cavalry's Automotive 5-Star Cyber Safety Framework[5] and Hippocratic Oath for Connected Medical Devices[6] which guide IoT design. These latter two frameworks encourage manufacturers to favor patterns that work, and avoid those that are known to fail.

Transparency and awareness reduces information asymmetry and allows market availability to more closely meet buyer expectations. These mechanisms enable a voluntary mechanism for manufacturers to highlight security capabilities and buyer considerations. Buyers can better distinguish products based on their security capabilities, and more fully account for cost and risk in their decision-making. NTIA has done some excellent work in this field, with its multi-stakeholder processes.

Education and awareness for individuals and small or medium businesses would be welcomed, though it's not clear that this alone will improve effectiveness of securing IoT devices against botnets. Awareness is probably most effective at time of purchase, to better equip buyers' decision-making. To that end, retailers can be a key ally in improving the security of new devices coming online. Simple, understandable comparisons can help buyers decide which security models best fit their expectation for their and others' role in maintaining a secure Internet environment.

An example given by a telecommunications industry lobbyist was that of a connected dog collar, used for tracking and retrieving lost pets. The individual suggested that in the event the collar became part of a botnet or was vulnerable to known botnet attacks, it could be shut off from the mobile carrier network, thus alleviating risk to other Internet devices. The owner then could purchase a new collar, free of the particular defect that facilitated its participation in a botnet. Another manufacturer may choose to take alternate measures to ensure the owner could locate their pet. In this circumstance, awareness and education would play a key role in informing buyers of a) potential failure modes and consequences; b) responsibility to identify failure in a timely manner; c) obligation to replace the device, at their cost; d) ensure new devices are free of the same defect.

Governments have a central role to play in securing the Internet of Things through governance, policy, and coordination. Governments tend to have the best vantage point to look across multiple industry sectors and segments, as well as internationally, and balance objectives of all societal stakeholders. Where international stakeholders share common markets, supply chains, threats, and harms, international cooperation and collaboration aligns stakeholders' interests. While optimal solutions may not be identical across all societies, Governments can coordinate policies that are more compatible, or at least attempt to avoid contradictory ones.

[4] *Cybersecurity Framework*, National Institute of Standards and Technology, https://www.nist.gov/cyberframework

[5] *Automotive 5-Star Cyber Safety Framework*, I Am The Cavalry, August 8, 2014. https://iamthecavalry.org/5star

[6] *Hippocratic Oath for Connected Medical Devices*, I Am The Cavalry, January 19, 2016. https://iamthecavalry.org/oath

The report should be clear, when discussing risk-based decision-making, to identify risk: to whom; from who/what; by which means. Too often, government and industry differ on stakeholders, types of impact, and whether something is a harm or a remedy. For instance, a regulatory fine is a financial risk to shareholders, but may remunerate consumers whose data has been stolen.

The government needs to lead a conversation about accountability, liability, and responsibility throughout the supply chain and chain of operations. Roles and risk decisions are too often assumed, so downstream buyers are unable to evaluate risk decisions made by upstream suppliers. Buyers may compensate by under- or over-treating residual risk, which is either wasteful or risks security failure – liability for both outcomes is borne by the buyer. Governments can adjust this liability placement by imposing ex-ante market-gating mechanisms and ex-post liability regimes, or by facilitating information exchange to permit stakeholders to define and understand their role and risk.

Goals

1.1 Consensus opinion is a poor approximation for empirical evidence of failures and failure modes. Existing databases, such as Common Weakness Enumeration (CWE) and Common Vulnerabilities Exposure (CVE), identify well-known poor practices as well as specific software defects. These can serve as baselines for designing, implementing, and maintaining a higher degree of security than consensus-driven standards. Their advantage is that the lists keep pace with newly discovered issues, whereas standards are "point-in-time", get stale quickly, and tend to be more fragile. Favor the former, more objective, observable factors in a standard of care.

1.2 New and innovative approaches are necessary to ensure knowledge keeps pace with adversary capabilities. Manufacturer Usage Descriptions (MUD) is an excellent example of a capability that can greatly improve security of IoT devices. However, new research should not come at the cost of, nor delay implementation of, practices we already know are sound and effective, such as patching, avoiding known defects, adversarial resilience modeling, and coordinated vulnerability disclosure. Ensure these two approaches are not seen as tradeoffs.

1.3 William Gibson once observed that "the future is already here, it's just not very evenly distributed." Promulgation and adoption of existing known effective practices should be at the forefront of approaches to cybersecurity.

3.2 Awareness and education is necessary but insufficient for a more secure Internet ecosystem. This is particularly true where "bits and bytes meet flesh and blood" such as automotive, medical devices, aviation, trains, etc. Advanced knowledge of cybersecurity practices must not be a prerequisite to safe operation of IoT devices. There is too much at stake to rely solely on subject matter expertise of IoT owners – even for those who are relative experts. This Goal is a good one.

5.1-2 Labels and information about security can be a key part of improving operational security. Labels in particular can increase trust among buyers. However, highly subjective and overly simplified labeling and scoring can increase cost without substantially improving security or market confidence. Assessment/audit regimes for labeling creates a class of services for overcoming standards, and often leads to incentives that are at odds with the objectives. Instead, favoring objective, observable criteria which can be independently verified allows for less expensive validation regimes and reduces incidence of gaming the system.

5.3 Software vulnerabilities are a byproduct of the software development process. When the software development lifecycle is informed by defensive coding, Rugged Manifesto,[7] OWASP Top 10 Risks,[8] and other security practices, the resulting products are higher quality, with fewer defects. The majority of developers today have never had secure coding training, and many have never been through a formal academic software development curriculum. Creation of curricula, graduation requirements, and other steps to improve security of academic programs would be welcomed.

Conclusion

The Botnet report is clearly the culmination of countless hours from many stakeholders, addressing a clear and present threat to Internet stability and resilience. It’s great to see such work, and I sincerely hope that most of the Actions are taken. There’s a tremendous amount of work to do, and also a tremendous amount to gain from making the Internet safer, sooner, together.

Beau Woods
@beauwoods
Cyber Safety Innovation Fellow, Atlantic Council
Cyber Safety Volunteer, I Am The Cavalry
Founder/CEO, Stratigos Security

[7] The Rugged Software Manifesto. https://www.ruggedsoftware.org/

[8] OWASP Top 10 Risks. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project