Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Prepared for: National Telecommunications and Information Administration
Prepared by: Donal Kerr, COO, 4Securitas, Dublin, Ireland.
7 Feb 2018

Summary: While we agree that coordinated international efforts are required due to the multi jurisdictional nature of this problem we suggest that United States public bodies should be more specific and vocal in outlining exactly what coordinated actions should take place, when and by which parties.

To this end we propose a logical and pragmatic solution which builds on data analysis in combination with a simple accompanying reporting and communication and blacklisting process using a database of Botnet attacks.

To effectively tackle Botnets we first need to neutralise compromised devices and then work back to the source. Rather than engage in a series of loosely-defined international meetings and rapprochement over many years we propose that a better approach would be for the US to start with primary data alongside a communication strategy aiming to reach consumer, enterprise and also government and political actors around the world.

What we propose is a sort of internet hygiene, not dissimilar form that way that infectious diseases are dealt with - deal with the patients and the sources of infection. This would be a much more effective way to tackle botnets and their proliferation.

ISP's would need to bear more responsibility for endpoint hygiene, and simply not allow interoperability with devices that do not provide adequate security, the sorts of IOT devices that botnets seek to compromise.

By refusing to work with these devices, ISPs and others would use the power of the market to slowly force better compliance. This is better than policy makers complaining about insecure devices, creating layers of new regulations and policy standards but doing little about the underlying technical issues.

The market incentive would manifest automatically without the need to draft laws, regulations and treaties - although these could complement this initiative.

Disclaimer: I am co founder of a security company and part of a delegation from Ireland which will travel to the Boston College in March this year. My company is producing a database that already tracks botnets, we have direct personal experience of this phenomenon.

Detailed Comment:

Page 3
1. Automated, distributed attacks are a global problem. The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners.

While we agree that coordinated international efforts are required due to the multi jurisdictional nature of this problem we suggest that the US should be more specific and vocal in outlining what coordinated actions should take place, when and by which parties.

2. Effective tools exist, but are not widely used. The tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.

We do not fully agree that effective tools are widely available. Many enterprise tools are developed with the wrong incentives in mind (as is referenced later in the paper).

Education and awareness is needed. Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient.

Education that is not vendor driven or defined is crucial. Gartner estimates that by 2020 there will be nearly 2 million vacancies globally in security and it is essential that these future professionals learn security fundamentals, not just how to use a few enterprise products.

As an analogy, learning to use Facebook does not make one a 'social media expert' no more than using a port scanner renders one a security professional. In our work we have met numerous graduates of University level security courses how despite having impressive credentials do not know that basics of infrastructure, computing or fundamental protocols such as TCP/IP upon which the modern internet is built.

5. Market incentives are misaligned. Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.

This is an accurate observation. There is a lot of money to be made in selling complex and expensive solutions. Many vendors are part of the problem in mis-selling solutions.

Automated, distributed attacks are an ecosystem-wide challenge. No single stakeholder community can address the problem in isolation.

This is an accurate observation, however we believe that the US government is in a unique position to take the lead. The 13 DNS root servers are in the United States and given this , the US is in a prime position to take the lead and act as a gatekeeper in this regard.

Page 7

1. Automated, distributed attacks are a global problem. The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners.

This is an accurate observation, however we believe that the US government should start a project to analyse data and get the facts and then more toward multilateral political and regulatory solutions.

In our opinion the ideal initiative would be to create and populate a sort of Database containing all compromised devices that are connected to the public network - globally.

This sounds like a big project, and it is. It would involve collection of public device data from ISPs, individuals and enterprises. One that has been populated to a reasonable extent, the next step would be to interrogate the device owners - using the line of least resistance to trace back the true controller.

For instance if a home router in OHIO is launching brute force attacks on a University database in New York then the local ISP can be informed. They can take action to remove the device from their sub net. Furthermore, using basic security techniques they can trace back the controller of that device and report to the ISP and the Database whether this was in the same jurisdiction.

With that information, then multilateral action becomes much clearer and informed - policy makers can easily point to server and log data and focus their efforts on the small number of malicious actors who are exploiting vulnerabilities.

The US is a global leader in many fields. Before beginning a lengthy consultation with international partners we suggest that the US takes the lead and establishes a Database that is a trusted reference and source of truth regarding security data, in particular around compromised devices - by geo, vertical, device type, software layer etc.

In other sectors such as healthcare, US public bodies are trusted internationally - for example the Centers for Disease and Control (CDC)

2. Effective tools exist, but are not widely used. The tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.

We do not fully agree. Many enterprise software products require highly experienced security staff to successfully deploy and operate them. Many products complicate security rather than making it more accessible. Many products are over specified and have too many configurations. Many network security applications severely interfere with business operations, require huge resources and are prohibitively expensive.

For security practices to become more central to the development of software, there needs to be legislation in place that mandates companies and organizations to take this seriously.
The EU has taken the lead in this space with GDPR - see the 72 hour breach notification provision as an example.
The US could follow suit and help create standards that enterprise software vendors will have to adhere to.

Education and awareness is needed. Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient.
In particular, customer-friendly mechanisms to identify more secure choices analogous to the Energy Star program 17 or National Highway Traffic Safety Administration (NHTSA) 5- Star Safety Ratings 18 are needed to inform buying decisions.

We agree that education is necessary at consumer and enterprise level, however much needs to be done and the US government could help create supportive mechanisms that would naturally lead to better security awareness.

Market incentives are misaligned. Perceived market incentives do not align with the goal of “dramatically reducing threats perpetrated by automated and distributed attacks.” Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.

We agree that this is one of the roots of the problem - be it a Chinese OEM developing whitelabel home monitoring devices or a large Enterprise vendor selling complex and expensive solutions. A back to basics approach would be of benefit to everyone concerned.

Responding in a timely fashion requires preparation and knowledge. Given the large set of security controls needed in the modern Internet, not all staff at smaller ISPs or key enterprises are aware of the benefits of filtering and other tools. Many ISPs offer warnings about compromises and ongoing attacks, but if enterprises ignore those notices and warnings, then the ISP is less likely to diligently follow up with further notifications. Victims often struggle when encountering their first substantial attack without a response plan in place, because they depend on the very network under attack to understand it and contact service providers for aid.

We agree that this is one of the roots of the problem - ISPs and other key gatekeepers should operate under more stringent reporting control given their key role in maintaining 'hygiene' in the online environment. There is a wide variability in the extent to which national ISPs vet / scrutinize customer and how they manage their properties of subdomains. Some are very secure and responsive, others very lax and do not take their responsibilities seriously. Given its size and power, the US is in a good position to nudge international ISPs to basic minimal compliance standards which would benefit enterprise and consumer all over the world

Infrastructure providers across the board must develop a broad understanding of the benefits of shared defense approaches, and communities should work together to drive best practice adoption. This work includes ubiquitous adoption of filtering at the interface with customer networks, including multi-tenant infrastructures such as cloud providers. Ideally, infrastructure providers should understand the current levels of attacks, maintain sufficient capacity to absorb realistically expected levels of malicious traffic, and communicate those capabilities to their customers. Infrastructure-provider services for DDoS mitigation should integrate with customers' existing network solutions, regardless of the level of service a customer has chosen. An increasingly smart network can segment different types of traffic automatically, to isolate or mitigate applications or devices that are sources of attacks. Enterprises are increasingly able to address application-level attacks with appropriate tools, and the vendors of these tools should work with both customers and the relevant application vendors to make security decisions easier and more efficient. As new products and tools become available, players across the ecosystem should understand how their behavior can help-or hinder-their efficacy.

The modern internet should not have to be filtered through some sort of global Fortinet that screens all traffic and slows everything down. It would be more efficient to police for botnets and malicious activity and both end point and network level, with a core guiding principal being the non-interference with business operations so that normal activity is not buffered.
One of the main reasons that security controls are often circumvented is because they interfere with business or create too many false positive and alerts.

Working with ISPs, OEMs, equipment makers, retailers and designers will be a better approach than filtering all traffic.

While enterprises typically have professional information technology (IT) operations staff, cybersecurity-specific expertise is often lacking. This challenge is often compounded by a similar lack of awareness among organizations' decision makers, who are responsible for resourcing IT operations within their organizations or for overseeing the IT operations. IT operations teams are often unaware of the risks of open resolvers and other sources of attack amplification, or the importance of ingress and egress filtering. When ISPs report potential compromise to customers, they often find that the enterprise cannot identify or locate the compromised devices, and even if the enterprise can identify the devices, it may not have the tools or expertise to recover to a secure state. Enterprises may struggle to work collaboratively with service providers when under attack. Failure to implement basic backup procedures places enterprises at greater risk from ransomware attacks.

There need to be more supports in place at an ISP level. If a ISP tenant cannot identify a compromised device then there need to be supports available further up in the hierarchy to deal with the problem, otherwise the problem will continue to fester.

Devices are a diverse and growing technical domain of the ecosystem. The Internet simultaneously supports multi-user computing systems, personal computing and mobile devices, and operational technology (e.g., supervisory control and data acquisition [SCADA] in industrial/manufacturing settings), and IoT in homes and offices. As a general rule, edge devices play two diametrically opposed roles with respect to distributed threats: malicious actors compromise edge devices to create distributed threats, and edge devices may also be the target of the threat (e.g., ransomware attacks). Poorly secured endpoints can be both the source and victim of attacks.

There needs to be debate about the unintended consequences of connecting all electronic devices to the public internet. There is no cost to connecting yet another endpoint to the public internet.

Edge devices may be vulnerable to compromise for a variety of reasons:
- Often, devices were not designed with security in mind. Developers are either unaware of good security design practices, assume that the device will be inaccessible (e.g., on a local network air gapped from the Internet), or want to avoid security solutions that impose additional cost or increase time to market. The resulting design choices, such as hard-coded administrative passwords, create inherently insecure devices. In other cases, appropriate security controls are present but usability/user interfaces result in less-secure configurations.

There needs to be debate about the unintended consequences of connecting all electronic devices to the public internet. There is no cost to connecting yet another endpoint to the public internet. (e.g. Linux password.conf file which contains enforced password policies, this is contain in most modern devices)

Thanks to linux and its embedded kernel that is used in the many of IoT devices, this issue can be addressed. All of these devices can be re-designed with simple patch deployments via creation of repositories. Once we know where those devices are and what kind of device they are, this is feasible.

Our Qualifications:

Our team has decades of business and technical experience from globally scaling startups like Twitter to large projects building and managed infrastructure and security for Fortune 500 companies and government departments.

Founder 1 Stefan Uygur - CTO and Product Architect: Phd, Infrastructure and systems expert. More than 2 decades experience with Linux Systems Administration, Penetration Testing, Vulnerability Analysis, Management and Assessment. Founder of Hacklab Italy and co creator of BackBox Linux. Previous senior tech roles at Sun Microsystems, Amaya and First Derivatives.

Founder 2 Donal Kerr - COO : Lawyer and business builder adept at providing strategic and regulatory counsel and issues management on a cross-company level. Previously Trust & Safety, Legal at Twitter. Previously held variety of business and operational roles in Financial Services at Citi, BNYM, RBCD. Recently Completed Enterprise Irelands New Frontiers Entrepreneur Development programs

IC4 The Irish Centre for Cloud Computing & Commerce

https://www.4securitas.com/
CRO: 598914

4Securitas @ Startlab,
Bank of Ireland
88 - 90 Camden St. Lower
Dublin D02 PY23