Combating IoT-Based Botnets

DISTRIBUTED BOTNET DETECTION AND MITIGATION AT THE ENTERPRISE AND CARRIER MONITORING NEXUS

Brian Quinn
GIGAMON | 3300 OLCOTT STREET, SANTA CLARA, CA 95054

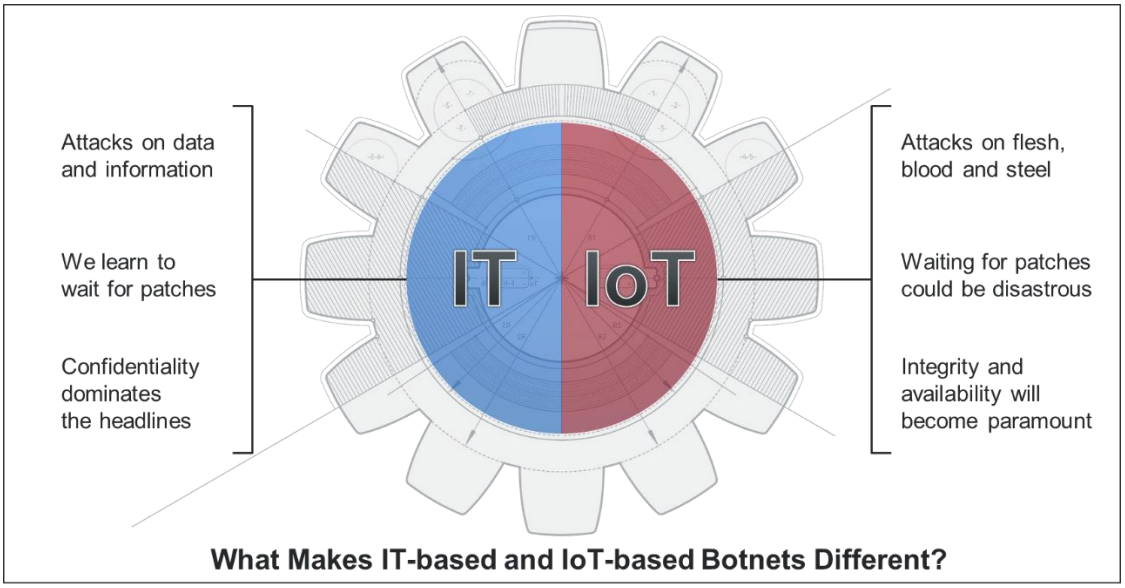
Gigamon appreciates the opportunity to provide comments to National Telecommunications and Information Administration's **Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats**. These comments are informed by Gigamon's experience in providing pervasive visibility to physical, virtual, and cloud environments to organizations in financial services, healthcare, high tech, and public sectors.

Executive Summary

Visibility is the key to monitoring for IoT-based botnets on the enterprise and carrier networks, and is foundational for providing an effective and efficient distributed defense system against IoT-based botnets. Establishing a network monitoring nexus at the enterprise and carrier level provides monitoring and analysis tools with visibility from across the complex, distributed and virtualized networks. As the number of enterprise and carrier networks capable of monitoring and alerting on botnet activity grows, and as the data is exchanged with threat sharing services, the faster and more decisive the collective and distributed response becomes against the IoT-based botnet threat.

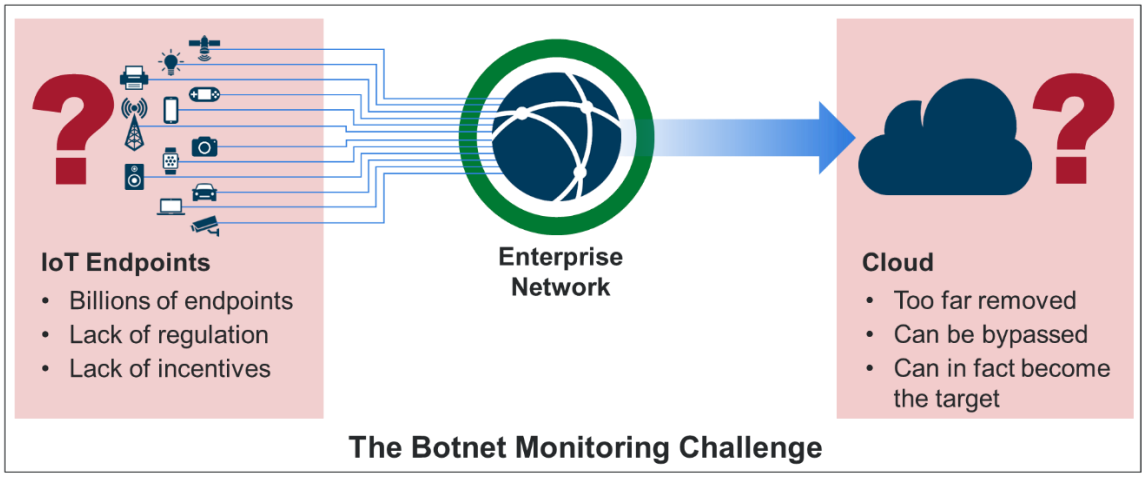
The Systemic Gaps in Botnet Defense

Botnets have the potential to turn Internet- or network-connected devices into a destructive army as infected devices connect and communicate. IoT-based botnets are of particular concern. Whereas typical hacking attacks target information, botnets that utilize IoT devices can affect the availability of services that impact life and limb.



What Makes IT-based and IoT-based Botnets Different?

Strategies that attempt to mitigate the spread of botnets at the IoT device level are ineffective. The largest botnets are built using IoT devices that have little or no security and can be compromised easily. Billons of IoT devices lack mechanisms to be patched, while many consumers lack the incentives to maintain patches or upgrade to neutralize even known vulnerabilities. As an example of the scope of IoT vulnerability, the Mirai botnet quickly coopted enough IoT devices to marshal DDoS attacks ranging from 500Gbs to 1Tbs in scale.

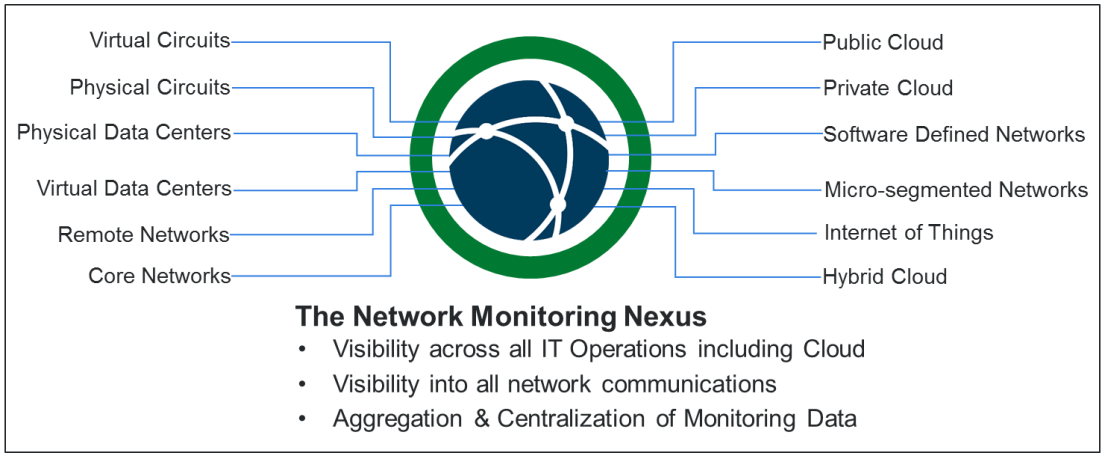


At the same time, putting security controls in the Cloud for IoT devices is perhaps not a feasible near or mid-term solution. The cloud based controls would be too far removed from the end devices, providing multiple opportunities to hijack and gain remote access to these IoT devices, and in many cases would still require some change at the device level for strong authentication and authorization.

Any solution that attempts to address these challenges needs to work through a medium that can be easily leveraged, without requiring billions of end-points to be upgraded, and needs to be as close to the end device as possible.

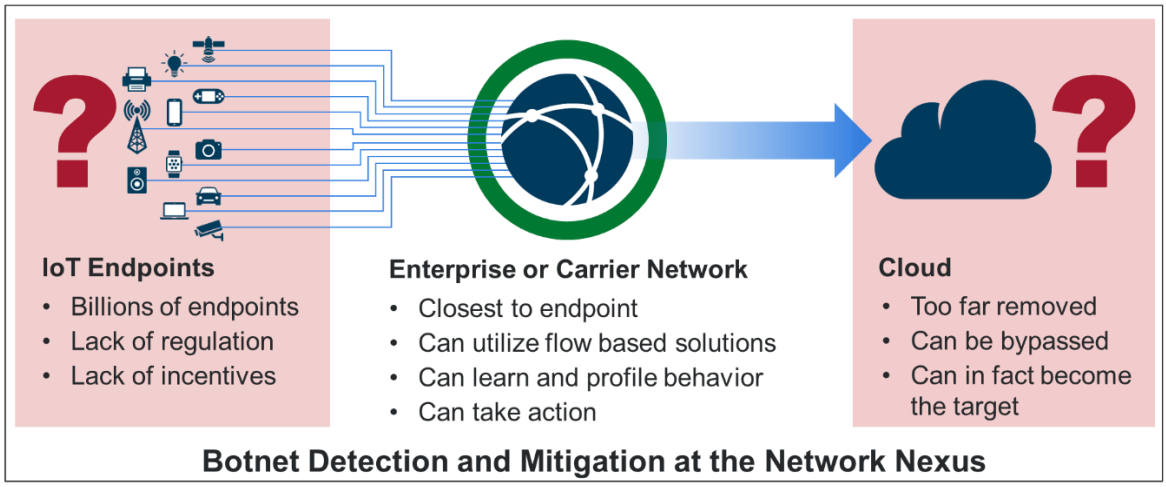
A New Paradigm for Botnet Detection and Mitigation using the Network Monitoring Nexus
A new approach, combining new technologies with existing cyber defense capabilities and best practices, has the potential to combat the spread of botnets by leveraging enterprise and carrier networks in a distributed defense model.

This approach centers on monitoring of IoT communication as it crosses the "network monitoring nexus". The network monitoring nexus is the monitoring "center" of the enterprise or carrier network, at which all network monitoring data is aggregated, with visibility extending across the complex, distributed and virtualized network including Cloud operations. From a control perspective, the network is closest to, and in fact touches, every connected IoT device that can be utilized by a large botnet or compromised by a remote access toolkit (RAT). This proximity provides the ability to fingerprint the device, as well as control any activity associated with the device.



Visibility is the key element in this approach, or what Gartner Group refers to as "Continuous Visibility", which is at the center of the **Twelve Security Capabilities of the Gartner Adaptive Security Architecture**.

Monitoring at the network nexus allows for detection and classification of IoT traffic whenever the IoT device communicates across the distributed enterprise network or utilizes network resources. Focusing efforts at the nexus provides an affordable and manageable approach to detecting the spread of botnets, as opposed to the alternatives of monitoring for botnets at the IoT device level or trying to corral botnets in the vast and growing Cloud infrastructure.



Establishing and utilizing a monitoring nexus to combat the spread of botnets provides key advantages:

1. An enterprise can profile and detect traffic associated with the spread of botnets at relatively low cost, using many existing cyber tools
2. New monitoring and detection tools can be rapidly deployed with no effect on current network cyber monitoring or operations.
3. Provides a central point to take action to block the spread at the network level, while enabling integration with evolving automated network defense capabilities

4. Provides a point for integration with threat sharing services. An army of properly configured enterprise networks connected to a threat services infrastructure provides a strong, distributed and cost-effective defense system. **Every enhancement to the monitoring and detection capability at the local enterprise level benefits the combined distributed defense system.**
5. Provides enterprise-wide traffic visibility required for the effective use of Cybersecurity Shared Services and Cybersecurity as a Service (CaaS).
6. Does not require billions of end devices to be upgraded.[1]
7. Provides a point of control and mitigation as close to the end device as possible. This is very important. The further you move away from an end device, the larger the amplification power of the botnet, with maximum intensity experienced at the intended target. The cumulation of attacks from large numbers of devices can overwhelm the ability of any target to directly mitigate the effects. By controlling activity close to the end devices, the impact of large scale DDoS attacks can be significantly minimized. **This is applicable to enterprise networks, but especially relevant for carrier networks as the control mechanism.**

The model can be extended to carrier networks through the implementation of subscriber aware visibility. Subscriber aware visibility provides a combination of high-throughput sampling with real-time analysis and user/device/control correlation, enabling this new approach to scale for carriers, and bringing the carrier networks into the distributed defense system.

Technologies for IoT-based Botnet Detection at the Enterprise Monitoring Nexus
A monitoring nexus on the enterprise network requires visibility across all IT operations – physical networks and data centers, virtual networks and data centers, remote locations, software defined networks, private cloud, and public cloud. Visibility enables aggregation of monitoring data from across the network at the nexus, where it is in intelligently processed, with custom data sets forwarded to cyber monitoring and analysis tools in real-time.

The use of a monitoring nexus allows for a distributed deployment of botnet detection tools as dictated by the requirements of the enterprise. The botnet monitoring suite can be a combination of physical and virtual tools deployed at the enterprise core and edge, along with virtual tool stacks deployed within a Cloud instantiation. The network monitoring nexus provides visibility for all of the tools and enables coordination among these distributed tools, such that all tools can utilize the secure tool orchestration services provided by the nexus.

To attain maximum visibility at a monitoring nexus for the detection of IoT-based botnet communications, a network traffic visibility solution is required that provides:

[1] Gigamon recognizes and supports NTIA's multi-stakeholder efforts in the area of Internet of Things security upgradability and patching and welcomes the progress being made up to date. Gigamon however recognizes the difficult issues of scalability and economics in IoT upgradability and patching and urges the NTIA to consider solutions to securing IoT that do not solely rely on upgradability and patching.

- The ability to extend real-time network traffic visibility across all IT operations, including public cloud deployments, with the ability to enable monitoring of network traffic at line rates and aggregation of all monitoring data without dropped packets.
- The ability to provide SSL Decryption of monitoring data without adding to throughput latency, enabling detection of botnet communications that utilize SSL/TLS encrypted web traffic without effecting network operations.
- The ability to enable device- and application-awareness for monitoring tools.
- The ability to provide a reliable source of flow-based traffic (i.e. NetFlow), with context-aware metadata.

A monitoring nexus is the foundation for IoT device discovery and enumeration. The ability to extract useful metadata from IoT traffic flows enables IoT device behavior fingerprinting and activity profiling, and detection of botnet communications using anomaly analysis.

Once the monitoring nexus is established, cyber monitoring and analysis tools specifically designed to identify botnet communications, and utilizing the enterprise-level visibility provided by the nexus, should be deployed. Examples include new solutions such as the ZingBox tool, but also include established cyber tools such as next generation firewalls. With access to visibility from across all IT operations, and working off customized monitoring data sets, the botnet monitoring and analysis solutions work with optimized effectiveness.

The nexus can be used to enable action, in concert with cybersecurity tools, to mitigate the botnet spread by blocking device communications and isolating any infected device on the network. When integrated with automated network cyber defense capabilities, these solutions allow for rapid and automated interdiction of botnet communications at the network level.

Also required is a solution component that can interface with threat services to inform all other participating networks of detected botnet activity, and to utilize information provided by the threat sharing services to enhance enterprise monitoring and defense.

Technologies for Botnet Monitoring at the Carrier Monitoring Nexus

As the main point of defense against IoT-based botnets that exploit consumer IoT devices, which may not connect to enterprise networks, a different approach is required for creating a carrier network monitoring nexus. With the very high traffic levels of carrier networks, whose volume is growing quickly due IoT traffic and because of applications such as Big Data and AR/VR, it is impossible to affordably sample every packet and single out IoT communications for effective analysis. The carrier network requires a network traffic visibility solution that supports subscriber-aware visibility.

Subscriber-aware visibility provides high-bandwidth sampling to enable effective detection of botnet traffic from very large data sets of mixed traffic, combined with GTP Correlation that enables correlation of user data and control sessions on the carrier backbone. This correlation is critical for the detection of anomalies related to IoT botnet activity.

To provide for maximum effectiveness at a carrier monitoring nexus for the detection of IoT-based botnet communications, the carrier network traffic visibility solution requires:

- The ability to extend network traffic visibility across all IT operation, including carrier private cloud services and public cloud services, with the ability to enable monitoring of network traffic at very high line rates while providing very high volumes of aggregated data.
- Support for subscriber-aware visibility.
- The ability to provide SSL Decryption of monitoring data, enabling detection of botnet communications that utilize SSL/TLS encrypted web traffic.
- The ability to enable device- and application-awareness for monitoring tools.
- The ability to provide a reliable source of flow-based traffic (i.e. NetFlow) and context-aware metadata.

As with enterprise networks, carrier networks can deploy cyber tools specifically designed to monitor for botnet communications. The use of subscriber-aware visibility at the monitoring nexus enables the carrier to deploy these tools in a cost-effective way as traffic volumes continue to increase. Carriers can also deploy cybersecurity tools that have the ability to automatically isolate and block traffic if it contains botnet communications.

And as with the enterprise networks, the carriers will need to exchange threat information with threat sharing services in order to increase the size of the distributed botnet defense system.

Conclusion

Visibility is the key to monitoring for IoT-based botnets on the enterprise and carrier networks, and is foundational for providing an effective and efficient distributed defense system against IoT-based botnets. Establishing a network monitoring nexus at the enterprise and carrier level provides monitoring and analysis tools with visibility from across the complex, distributed, and high bandwidth networks. As the number of enterprise and carrier networks capable of monitoring and alerting on botnet activity grows, and as the data is exchanged with threat sharing services, the faster and more decisive the collective and distributed response becomes against the IoT-based botnet threat.