DNS Threat Intelligence vs. AI Network Security

White Paper For Network Operators

CUJO AI

Vendors like Google, Amazon, and Microsoft dictate, how internet habits will evolve. Apple has already made the feature available for devices that are managed by MDM platforms and plans to roll it out to the general iPhone (iOS 11 and up) population at some point in the near future[1]. Having HTTPS everywhere and encrypted DNS are just a couple trends which will be adopted soon enough to introduce more privacy within home consumer space.

The pace at which cyber-attack patterns and malicious infrastructure developments are shifting conspire to keep security vendors one step behind in this race.

Signature-driven detects are no longer sufficient or effective due to their reactive nature. There are between 200k and 300k new malware samples released every day[2]. From an attacker's perspective, DNS blacklisting is effective within the Delivery or Actions on Objectives attack phases[3]. The focus is solely on blocking known bad destinations, rather than on proactively detecting cyber threats.

Broadband customers are bringing millions of new smart devices into their homes and these are becoming an increasingly essential part of the modern broadband home. These new devices are difficult to secure using traditional methods. DNS blacklisting is not effective against Internet of Things (IoT) hacking or hacker attempts to gain a foothold in the Network Operator's network. The latest innovative shift in technologies enables encryption to be implemented easily and it will become a key strategic direction to protect sensitive data generated by IoT devices.

While encryption enhancements introduce more security and privacy for broadband in homes and other consumer spaces, there is also a downside to this trend: *Network Operators face more challenges when it*

[1] https://dnsdisco.com/iOS-dns-proxy-post.html

[2] https://www.av-test.org/en/statistics/malware/

[3] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Copyright © 2018 CUJO LLC.

comes to protecting communication channels and identifying compromised devices/attacks.

On 25 May 2018, General Data Protection Regulation (GDPR) will come into effect. Essentially, it is going to protect the data of the citizens of the European Union member states. This also includes non-EU organizations that use the data of EU citizens. According to the regulation, all organizations will have to improve their security measures, including data assessment, high security standards, and privacy policies. This regulation will reform the overall cybersecurity landscape and require additional security controls.

Instead of relying on human analysts, CUJO AI uses behavioral analysis, machine learning (ML), and artificial intelligence (AI) algorithms to ensure network security for both browser enabled and Internet of Things (IoT) devices.

Why is DNS Blacklisting not the Best Security Control?

DNS firewalls can be sidestepped.

DNS blacklisting is reactive. With millions of new threats, it is practically impossible to effectively track all new malicious DNS addresses.

DNS blacklisting is irrelevant for many threat vectors like bots or camera hacks.

DNS is being encrypted on endpoints moving forward.

General Data Protection Regulation (GDPR) will dictate the adoption of much more privacy controls (i.e., DNS encryption).

Find out more about the service and get a full white paper at **cujo.com**
Contact our team for more information: **isp@getcujo.com**

Copyright © 2018 CUJO LLC.