CONSORTIUM

Research Brief

FUTURE LANDSCAPE OF INTELIGENT DNS

Shahzad Mahmood Khan

Project manager, BlueCat Networks, Suite 502, 4101 Yonge Street, Toronto, Ontario Canada.

Keywords: DNS security, cyber security threats, data security.

History:
Received: June 13, 2016
Accepted: July 18, 2016
Published: August 3, 2016
Collection year: 2016
Status: Published

Identifiers and Pagination:
Year: 2016
Volume: 1
First Page: 1
Last Page: 3
Publisher ID:
10.21065.AdvEngTech.1-1
DOI:http://dx.doi.org/10.21065/AdvEngTech.1.1

Corresponding author:
Shahzad Mahmood Khan. Project manager, BlueCat Networks, Suite 502, 4101 Yonge Street, Toronto, Ontario Canada.
T.: +1 (416) 821-8685
E.: shahzadkhan15nov@gmail.com

Citation:
Shahzad Mahmood Khan. Future landscape of intelligent DNS. Adv Eng Tech 2016 [1]. 1-3

Sorry but your transactoin is denied

You're at Starbucks trying to make a purchase of your favourite hot-drink and your card is denied. How embarrassing. But wait - You've paid your balance every month without fail. What gives?

What likely could have happened is that some intelligant software at your financial institution detected a purchase anomaly and took action to prevent the fraud. Today, these tools are incredibly powerful, scanning through terabytes of data to detect even slight deviations in behavioral models like a sequence of small charges at online vendors or sudden spending pattern on new product categories. These are common signs of fraud that can raise red flags.

Cyber threats are growning

Cyber attacks are growning and recenlty some attackers stole 40 million credit cards from retail giant Target using an HVAC vendor's credentials.

Even Twitter, Netflix, Reddit and other websites suffered outages when millions of consumer wireless routers, digital cameras and DVR players infected with malware orchestrated a DDoS attack at DNS hosting provider Dyn.

Imagine that a university was locked out of critical systems after it was attacked by its own malware soda machines and other IoT devices.

No, not another attack?

We live in a digital world. But the promise of innovative consumer and business services that connectivity will unlock comes with a portentous reality: it's only a matter of time before your devices, intellectual property, and mission critical applications will come under attack.

The culprit facilitator

Last few years, the speed of malware attacks, their complexity, and their frequency have increased at an astounding rate. According to industry research, 91% of these attacks leverage DNS - a technology that is fundamental to how devices connect to networks. This is how compromised devices receive instructions, exfiltrate data and reverse engineer the network to find other systems to attack.

Funding:
The authors received no direct funding for this research.

Competing Interests:
The authors declare no competing interests

Additional information is available at the end of the article.

How fast can you react?

By the time all the relevant data is pulled together and properly analyzed by the network adminstrators, it's already out dated to result in any meaningful actions. When cyber attacks are flowing through a DNS infrastructure, most network administrators are egaged identifying anomalies in real time. The adminis have little insight into the spread of cyber attacks on networks with the absence of single source of data which can both pull DNS data together and analyze it against historical patterns.

Threat awareness

No process or technology, aimed for the benefit of a wide audience, is sucessfully carried out or implemented in the shadows without proper communication. In too many instances, serucirty artifacts become shelf-ware because they are developed and executed in a vacuum. For this reason, awreness efforts around threat modeling should take place before, during, and after the threat modeling process.

DNS Data Security

As a network service, DNS services run on a physical or virtual DNS server. Hence, securing physical server acedss, the operating system, and the DNS server implementation are critical considerations for DNS Data protection.

We need intelligent DNS

Network experts have long recognized the value of DNS as a critical element of network control, compliance and service delivery. Advances in automation, integration and the cloud are allowing modern IT organizations to rapidly deliver DNS to business users so they can access information and data across the enterprise.
What is needed are sophisticated tools that can interpret exactly what the information is saying so you can improve threat detection, prevention and response. It's time to look at DNS data in a new light and take advantage of this huge untapped resource.

Time for smart DNS to show off

- Show me who's on my network
- What's happening on my network
- Please trace the activities to it's source
- Close the gaps after identifying them
- Block the obvious threats
- Show my network efficiency

References

1. Lei Zhang, Qianhong Wu, Josep Domingo-Ferrer, Bo Qin, Peng Zeng, "Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security", Information Sciences, Vol.272, pp.223-237, 2014.
2. B. Zdrnja, "Security monitoring of DNS traffic," May 2006.
3. John Pescatore, "Securing DNS Against Emerging Threats: A Hybrid Approach", SANS Institute InfoSec Reading Room, pp. 4-9, 2015.

4. Joao Afonso and Pedro Veiga, “Improving DNS Security Using Active Firewalling with Network Probes”, International Journal of Distributed Sensor Networks, Vol. 2012, pp. 1-7.
5. Hyungjin Im, Jungho Kang, and Jong Hyuk Park, “Certificateless based Public Key Infrastructure using a DNSSEC”, Journal of Convergence, Vol. 6 [3], pp. 26-30, 2015.