International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

DNS Data Exfiltration Detection

Deep Bhatt[1], Palak Furia[2], Mangesh Gupta[3], R.R.sedamkar[4]

[1]*Student, Dept. of Computer Engineering, Thakur College of Engineering and technology, Maharashtra, India*
[2]*Student, Dept. of Computer Engineering, Thakur College of Engineering and technology, Maharashtra, India*
[3]*Student, Dept. of Computer Engineering, Thakur College of Engineering and technology, Maharashtra, India*
[4]*Dean. of Thakur College of Engineering and technology, Maharashtra, India*

Abstract - DNS hasn't been modified a whole lot due to the fact that Paul Mockapetris invented it in 1983. Still, it meets precisely the identical necessities as mentioned in RFC 882. As packages span a couple of hosts, then networks, and ultimately the Internet, those packages additionally want to span a couple of administrations. . Limits and associated operational methods (protocol, statistics format, etc.). The quantity of sources (along with mailboxes), the quantity of aid locations, and the variety of these environments create a steady manner of relating to precise sources which are comparable however scattered in the course of the environment. If you want, you motivate a powerful problem. Dan Kaminsky, a famend DNS protection researcher, can think about it as a globally deployed routing and caching overlay community that connects each the private and non-private Internets. This reasons extreme problems. Is it secure enough? Are you susceptible to statistics breaches? The solution is that DNS may be exploited in lots of unconventional ways, making it an excellent backdoor for hackers seeking to steal touchy statistics. This paper describes the approaches hackers use to take advantage of DNS for DNS tunneling and statistics mining purposes.

Key Words: Data Exfiltration, Information, Stealing Data Gathering, Servers, Tunneling, IP networks, Malware, Monitoring, Measurement, Encoding.

1.INTRODUCTION

Stealing Data—Why and What Kind? DNS is more and more getting used as a pathway for fact exfiltration both via the means of malware-inflamed gadgets or via means of malicious insiders. According to a latest DNS safety survey, forty six percent of respondents used DNS exfiltration and forty five percent skilled DNS tunneling. DNS tunneling includes tunneling IP protocol site visitors thru DNS port 53—that is regularly now no longer even inspected via way of means of firewalls, even next-technology ones—maximum probable for functions of facts exfiltration. So what kinds of facts are being stolen? They range and can include: Personally identifiable statistics (PII) inclusive of social safety numbers.

Regulated facts associated with Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliance. Intellectual belongings that offer an agency an aggressive advantage. Other touchy statistics inclusive of credit score card numbers, corporation financials, payroll statistics, and emails Malicious insiders both set up a DNS tunnel from in the community or encrypt and embed chunks of the facts in DNS queries. Data may be decrypted at the alternative quit and positioned again collectively to get the treasured statistics. Motivations range from hacktivism and espionage to economic wrongdoing, wherein the facts may be without problems offered for a neat earnings withinside the underground market.

1.1 DNS as a Transport Protocol

Most organizations have a couple of protection mechanisms and protection technology in place, consisting of subsequent era firewalls, IDSs, and IPSs. So how can hackers use DNS to move statistics throughout a couple of layers of cautiously crafted protection mechanisms? The nature of the DNS protocol, which was invented more than 30 years ago, is such that it's miles trusted, but susceptible to hackers and malicious insiders. To absolutely recognize the vulnerability, it's vital to recognize the character of DNS messages. There are sorts of DNS messages, queries and replies, and they each have the same format. Each message includes a header and 4 sections: question, answer, authority, and additional. The header field “flags' 'controls the content material of those 4 sections, however the shape of all DNS messages is the equal.2 Various gadgets and parameters inside the DNS have length limits. The length limits are indexed below. Some may be without problems changed, at the same time as others are extra fundamental. What does this mean? Hackers have as a base 512 octets to “encode” statistics in UDP messages to keep away from detection. They also can embed signaling data or mild encoding in a number of the labels or names areas and break out with it. 1.2 Exfiltration

Data exfiltration thru DNS can contain setting a few cost string withinside the names section (as much as 255 octets) or the UDP messages section (as much as 512 octets), formatted as a question, after which sending it to a rogue DNS server that logs the question. Hackers install a call server with question logging enabled. This call server could be the “trap server” for the touchy records that are being stolen. It runs a primary set up of BIND and is on the market from the Internet. It may even conceal in the back of a cable modem, so long as port fifty three is exceeded to it.

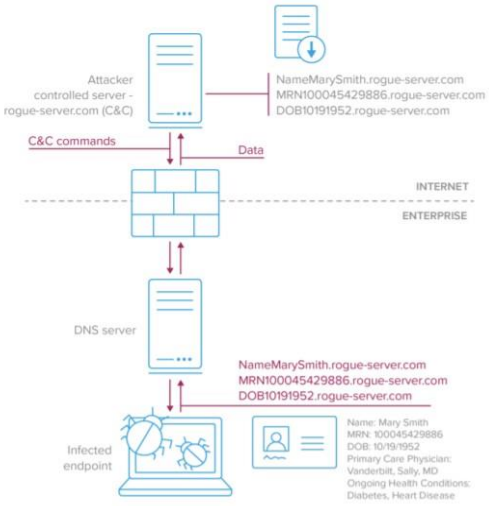

Figure 1. Data exfiltration via DNS queries

Of route different smart techniques may be hired with the aid of using cybercriminals, which includes ID tagging, series numbering, etc. This is specifically beneficial while tagging transactions (like credit score card purchases), wherein the series of activities would possibly inform us which bits are names, numbers, or card verification value (CVV) numbers. This is especially genuine of the FrameWorkPOS malware. With lots of capability DNS queries going out of a community as a part of an exfiltration attempt, it would appear like a trivial assignment to trap such a way of transport, however thieves are quite smart approximately keeping off detection. They use techniques which include sluggish drip, which sends queries at a managed slower tempo on the way to now no longer make the fee soar excessive and spark off alerts. Another approach they use is supply IP spoofing, wherein the supply IP is rewritten withinside the queries, in order that it looks like the queries are coming from many one-of-a-kind clients. Proper community protection needs to trap this on the transfer port, however you are probably amazed at how regularly the method works!

Infiltration

We've seen how information leakage can happen, but what use is DNS to transport information directly onto a network? Hackers can use DNS to transport a payload or to inject malicious code. It's simpler than you think. Similar to exfiltration, the hacker can take a binary file, assemble it to send encrypted (possibly as HEX), and then upload it to their rogue server in TXT data. and content filter? You can extract them from the command line or just write browser code to store it in a blob and then sell it to a file. You can also easily inject it into an organization's internal DNS server via dynamic DNS. , in which you can shoot down the code of browsers, mobile phone smartphone applications or phishing. When clicked or exploited, the code is downloaded from DNS and assembled via a client. Now that hackers can send and retrieve information through DNS, the idea of DNS as a covert forwarding protocol becomes clear.

Working with Data-loss Prevention Solutions

Most Data Loss Prevention (DLP) solutions protect against data leakage via email, web, FTP, and other vectors by monitoring data at rest, in transit, and in use. However, they do not discuss DNS-based exfiltration. Infoblox Threat Insight complements traditional DLP solutions by closing the gap and preventing DNS from being used as a backdoor for data theft. The most effective way to combat DNS-based data exfiltration is to build intelligent detection capabilities directly into DNS infrastructure.

3.1 Automating Threat Response through Integration

While detecting and blocking data exfiltration attempts is critical, it is also important to ensure rapid remediation of infected devices. This can be achieved through tighter integration between detection technologies and endpoint repair solutions. Infoblox integrates with leading endpoint solutions like Carbon Black to provide indicators of compromise when an endpoint attempts to exfiltrate data. With this intelligence, Carbon Black will automatically prevent malicious processes from running and connecting in the future, effectively isolating the infected endpoint and preventing data leakage even when the device is off-site. In addition, Infoblox shares valuable information about network and security events with the Cisco Identity Services Engine (ISE) to automate security response and timeliness. The information may be sent to the security architecture organization for quarantine. Finally, Infoblox automatically integrates with SIEM technologies or internally developed user behavior analysis solutions via APIs to provide comprehensive contextual data such as device operating system type, user information, and DHCP lease information without the need for endpoint agents.

CONCLUSION

Data theft is one of the biggest risks for any business. DNS is often used as a data mining route because it is not vetted for common security controls. Solutions proposed in this paper can protect against more complex data mining techniques.

REFERENCES

1) B. L. Josh Grunzweig and Mike Scott, New wekby attacks use dns requests as command and control mechanism, 2016, [online] Available: http://bit.ly/1TAYE8j.

2) Y. H. C. Sudeep Singh, Targeted attacks against banks in the middle east., 2016, [online] Available: http://bit.ly/22IwOCz.

3) S. Bromberger, "Dns as a covert channel within protected networks", National Electric Sectory Cybersecurity Organization, 2011.

4) G. Farnham and A. Atlasis, "Detecting dns tunneling", SANS Institute InfoSec Reading Room, pp. 1-32, 2013.

5) T. Fawcett, ExFILD: A tool for the detection of data exfiltration using entropy and encryption characteristics of network traffic, 2010.

6) J. Hind, "Catching dns tunnels with ai", Proceedings of DefCon, vol. 17, 2009.

7) Karasaridis, K. Meier-Hellstern and D. Hoeflin, "Nis04-2: Detection of dns anomalies using flow data analysis", Global Telecommunications Conference 2006. GLOBECOM'06. IEEE, pp. 1-6, 2006.

8) V. Paxson, M. Christodorescu, M. Javed, J. R. Rao, R. Sailer, D. L. Schales, et al., "Practical comprehensive bounds on surreptitious communication over dns", USENIX Security, pp. 17-32, 2013.

9) M. S. Sheridan and A. Keane, "Detection of dns based covert channels", ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015, pp. 267, 2015.

10) H. Binsalleeh, A. M. Kara, A. Youssef and M. Debbabi, "Characterization of covert channels in dns", New Technologies Mobilityand Security (NTMS) 2014 6th

11) International Conference on, pp. 1-5, 2014. J. Dietrich, C. Rossow, F. C. Freiling, H. Bos, M. Van Steen and N. Pohlmann, "On botnets that use dns for command and control", Computer Network Defense (EC2ND) 2011 Seventh European Conference on, pp. 9-16, 2011.

12) Y. Chen, M. Antonakakis, R. Perdisci, Y. Nadji, D. Dagon and W. Lee, "Dns noise: Measuring the pervasiveness of disposable domains in modern dns traffic", Dependable Systems and Networks (DSN) 2014 44th Annual IEEE/IFIP International Conference on, pp. 598-609, 2014.

13) Dnscat., 2004, [online] Available: http://bit.ly/lPhF8Qd. Show in Context Google Scholar

14) 14.E. Skoudis, "The six most dangerous new attack techniques and whats coming next", RSA Conference (RSA12), 2012.

15) Dns tunneling, 2006, [online] Available: http://bit.ly/2gJ3pDn.

16) Dns visualization, 2009, [online] Available: http://bit.ly/2gZfyCe.

17) K. Born, Dns tunnel detection using character frequency analysis, 2010.

18) P. Butler, K. Xu and D. D. Yao, "Quantitatively analyzing stealthy communication channels", International Conference on Applied Cryptography and Network Security, pp. 238-254, 2011.

19) C. Fry, Security monitoring proven methods for incident detection on enterprise networks. (p. 28), 2009. Show in Context Google Scholar

20) Bernhardpos-new pos malware discovered by morphick, 2015, [online] Available: http://bit.ly/2969q7w.

21) F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, et al., "Scikit-learn: Machine learning in Python", Journal of Machine Learning Research, vol. 12, pp. 2825-2830, 2011.

22) L. Buitinck, G. Louppe, M. Blondel, F. Pedregosa, A. Mueller, O. Grisel, et al., "API design for machine learning software: experiences from the scikit-learn project", ECML PKDD Workshop: Languages for Data Mining and Machine Learning, pp. 108-122, 2013.