Title:

Real-time DNS-Based Data Loss Prevention using eBPF, deep learning and threats event streaming: A security framework to safeguard enterprises from emerging threats.

Abstract:

DNS is often considered most vulnerable protocol and primary target to exfiltrate data from enterprise networks due to its business significance and inherit security flaws. DNS-based data exfiltration through Command-and-Control (C2) channels and DNS tunneling techniques poses critical cybersecurity challenges, particularly in large-scale distributed environments. Emerging threats against DNS involve attackers to exploit DNS vulnerabilities by establishing covert channels, exfiltrate sensitive data, and maintain persistent control over compromised systems. Traditional defenses often fail to address these sophisticated and evolving threats, leading to delayed detection, substantial data loss, and widespread network compromise. This workshop presents a scalable security framework designed to fully prevent DNS data exfiltration in real-time using Linux kernel eBPF programs and deep learning following endpoint security approach. Operating directly within the kernel network stack, the solution leverages eBPF over kernel traffic control (tc) and Netfilter for Deep Packet Inspection (DPI) and real-time lexical analysis of DNS traffic. Additionally, it adapts to evolving obfuscation techniques in DNS protocols, effectively neutralizing sophisticated threats. The framework also provides robust support for destroying C2 channels within seconds of creation, exposing C2 implants processes, and preventing exfiltration over arbitrary transport ports. Moreover, due to threat streaming, and event stream analytics over centralized message brokers, it supports dynamic domain blacklisting at the enterprise DNS recursors, hence safeguarding all nodes in the enterprise environment.

Key Features of the Framework:

Deep Packet Inspection inside Linux Kernel: Utilizes eBPF programs over TC, Netfilter, and raw parsing of kernel socket buffers for advanced lexical analysis of DNS packets.

Dynamic eBPF Filter Injection: Detects and blocks encapsulated exfiltration attempts through virtual network interfaces using kernel probes.

Enhanced Observability: Delivers granular metrics and insights via eBPF maps and ring buffers, enhancing threat visibility.

Adaptive Obfuscation Detection: Employs deep learning models to counter evolving DNS exfiltration obfuscation techniques.

Transport Protocol Port Agnostic Protection: Ensures comprehensive safeguards against DNS exfiltration over arbitrary UDP ports.

Real-Time Mitigation: Integrates dynamic domain blacklisting and event stream processing for enterprise-scale DNS topologies.

The framework ensures minimal data loss while providing real-time prevention of DNS tunneling and C2 channels. It offers robust protection against all forms of DNS data exfiltration, enhances observability through comprehensive metrics, and ensures resilience against dynamically evolving threats, making it a significant advancement in building modern data loss prevention solutions to stop breaches over DNS.

Technical Innovation:

- First solution combining eBPF kernel-level DPI with Deep Learning for DNS security.
- Novel approach to real-time prevention without traffic mirroring to remote nodes, with real-time thwarting exfiltration directly at the endpoint.
- Advanced packet analysis across to exfiltration via DNS done over any random port.

Audience Takeaways:

1. Advanced kernel-level techniques for DNS security using eBPF, including deep packet inspection via SKB parsing for Layer 7 protocols.
2. Integration of machine learning with kernel operations for real-time threat detection and prevention
3. Use of eBPF and kernel network stack hook points to build robust data loss prevention solutions.
4. Strategies for Managing Encapsulated Traffic and Virtual Interfaces in Distributed Environments: Leveraging Kernel Probes for Dynamic Injection of DPI eBPF Programs into the Kernel Network Stack.
5. Optimization techniques for high-performance packet processing and analysis in Linux networking stack, with use of AF_XDP / AF_PACKET sockets for fast egress packet delivery completely bypassing Linux kernel network stack.
6. Scalable architecture design for enterprise-level DNS security across diverse network topologies
7. Innovative Approaches to fully prevent sophisticated DNS-Based Exfiltration Tunnels and real-rime by the disruption of C2 Communications.
8. Demonstrating how eBPF combined with the kernel's syscall layer can effectively terminate C2 implants at the endpoint, enhancing endpoint defense in real.

Source Code:
https://github.com/Synarcs/Data-Exfiltration-Security-Framework