LiveAction®

How ETA Works

Encrypted Traffic Analysis

Andrew Fast, Ph.D. | Chief Data Scientist

ThreatEye®

LiveAction®

How ETA Works

Encrypted Traffic Analysis

Andrew Fast, Ph.D. | Chief Data Scientist

Introduction

As of 2019, over 70% of all network traffic is being encrypted, hiding critical information from network defenders[1]. Previously, defenders had access to both the content and server information of email and webpages. Now, the widespread adoption of HTTPS and recent introduction of new encrypted protocols such as DNS over HTTPS and TLS 1.3 threaten to dramatically reduce visibility into server identity and content. Once these sources of security information are removed, the next frontier for network defenders is applying cryptanalysis techniques and machine learning for traffic analysis. CounterFlow's ThreatEye Platform combines these two techniques to provide visibility into "hidden" patterns within the communication itself.

[1] https://www.nsslabs.com/press/2019/7/17/nss-labs-announces-2019-ngfw-group-test-results/

ThreatEye®

Cryptanalysis

Derived from two Greek root words, "Cryptanalysis" (CRYPT – hidden, ANALYSIS – loosen) is the investigation of the hidden aspects of communication systems. Historically, there are two kinds of cryptanalysis: breaking the encryption itself and side-channel analysis of potential information "leaks". Encrypted traffic analysis is a type of side-channel analysis that allows network defenders to do their jobs while maintaining the privacy and network integrity provided by a fully encrypted system. ThreatEye provides three levels of Encrypted Traffic Analysis:

Traffic Analysis

LEVEL 1

Information available in the network transaction (ip address, ports, protocol, and timing)

Certificate Analysis

LEVEL 2

Looking at the particulars of the encryption being used (cipher suites and extensions etc.)

Deep Packet Dynamics

LEVEL 3

Looking at patterns in the sequence of packet lengths and times

EXAMPLE 1

Encrypted Traffic Analysis to Uncover Command & Control (C2) Activity

Malicious threat actors and malware system operators communicate with infected target systems using a set of techniques called Command and Control (C2). To avoid detection, C2 techniques are designed to mimic normal, benign traffic using common ports[2] and standard encryption protocols[3]. Despite these precautions, Encrypted Traffic Analysis with machine learning is effective at uncovering different types of C2 activity.

[2] MITRE ATT&CK Commonly Used Port - https://attack.mitre.org/techniques/T1043/

[3] MITRE ATT&CK Standard Cryptographic Protocol - https://attack.mitre.org/techniques/T1032/

LEVEL 1

Defends Against: Beaconing

Beaconing is used by an infected system to reestablish contact with the control infrastructure. This activity is characterized by sending identical messages at a specified interval. When repeated messages surface, Level 1 ETA recognizes potential beaconing activity by capturing patterns within both the communication intervals and the byte totals in both directions.

LEVEL 2

Defends Against: TLS Fingerprinting

The encryption software libraries used by malware often differ from the encryption libraries used by browser, apps, and other legitimate software. When beaconing activity identifies a suitable command host, an encrypted C2 protocol initiates a secure connection using these same libraries. These events create a distinctive signature that can be identified on the network.[4]

LEVEL 3

Defends Against: Sequence of Packet Lengths

Once a secure connection is made, communication between the C2 infrastructure and the infected target begins. Due to the specific nature of the C2 commands, the number and size of the packets being exchanged over this connection often have characteristic signatures that distinguish them from typical web traffic.[5] Here, real-time analysis of packet traits like these can yield signature deviations that point to C2 activity.

> "In summary, ETA combined with machine learning techniques effectively identifies malicious C2 activity on the network. Despite having no visibility into the content of the exchange, ETA tells us a great deal about encrypted traffic and provides valuable insights to aid network defenders."

[4] Hiding in Plain Sight: Malware's Use of TLS and Encryption, Blake Anderson, Cisco, January 2016

[5] Detect Malicious Communications Even Under TLS, Anton Tyurin, Positive Technologies, November 2018

EXAMPLE 2

Defending Against Exfiltration with Encrypted Traffic Analysis

Once a threat actor has identified information of value, he or she must find a way to transport that data back to home base. Because bulk transfers of large amounts of data are readily detectable, attackers use other, less detectible techniques to exfiltrate data.

LEVEL 1

Defends Against: "Low and Slow"

Rather than exfiltrating the data in a single transfer, threat actors can choose to release small amounts of data over time[6]. Basic traffic analysis recognizes this "low and slow" technique by tracking byte totals over time.

LEVEL 2

Defends Against: Tunneling

Tunneling encapsulates one protocol—or layer—of encryption within another one. This type of traffic has a different packet dynamic profile compared with standard traffic on that port. ThreatEye's parsing capabilities can even detect nested layers of encryption[7]. Some forms of tunneling, such as DNS tunneling, are also detectable by analyzing the ratio of bytes being transferred in each direction during a connection.

LEVEL 3

Defends Against: Cloud Service

Each cloud application has a highly recognizable packet dynamics fingerprint tied to its typical usage. Because exfiltration to a cloud-based account requires extensive data transfer, profiling typical usage for that user or IP[8] can highlight whether or not a certain exfiltration is from the enterprise's normal activities or the work of a possible threat actor.

> "Here again, Encrypted Traffic Analysis, coupled with machine learning capabilities, evaluates complex data patterns over time and highlights which activities grade as normal (potentially benign) or abnormal (potentially malicious)—all without access to the content of the data being transferred."

[6] MITRE ATT&CK Data Transfer Size Limits https://attack.mitre.org/techniques/T1030/

[7] MITRE ATT&CK Multilayer Encryption https://attack.mitre.org/techniques/T1079/

[8] MITRE ATT&CK Transfer Data to Cloud Account https://attack.mitre.org/techniques/T1537/

Cryptanalysis Techniques for Encrypted Traffic Analysis

We group cryptanalysis techniques for ETA into three main categories:

FINGERPRINT

Unique identification of network entities such as devices, domains, IPs, users, and connections.

MAP

Identify meaningful relationships between network entities on the globe, in the network, and with similar features.

PROFILE

Observe changing behavior of network entities over time with comparisons to established baselines.

TABLE 1

Example ETA Techniques

		FINGERPRINT	MAP	PROFILE
LEVEL 1	Traffic Analysis	Protocol Fingerprint – each machine has a protocol fingerprint based on the services it utilizes or provides	Shared IP or ASN – often multi-tenant servers host multiple malicious sites in the same location	Pattern of life/time of day – traffic at odd hours of the day or night can indicate malicious traffic
LEVEL 2	Certificate Analysis	TLS Fingerprinting – unique combinations of cipher suites and extensions	Malware use of TLS – identify malware propensity with specific fingerprints	Novel Fingerprints – the emergence of new fingerprints can indicate the presence of malware or other unwanted software on the network
LEVEL 3	Deep Packet Dynamics	OS Fingerprinting – identify host and IoT device types from "instinctive" packet header details	Application ID – characterize applications based on similar byte patterns of typical usage	Interactive Sessions – detect usage of Remote Access Toolkits (RATs) by identifying the characteristic patterns of transmission of individual keystrokes

Deep Packet Dynamics vs Deep Packet Inspection

Deep Packet Dynamic (DPD) data supplied by ThreatEye's probe software provide reliable security information that is useful for evaluating both encrypted and unencrypted traffic. In contrast, legacy visibility solutions identify relevant data using Deep Packet Inspection (DPI) which only works for unencrypted or clear text protocols such as HTTP. For encrypted traffic, DPI requires a decryption proxy, or middle box, to be deployed. Middleboxes can be costly, introduce performance bottlenecks and create additional security concerns.

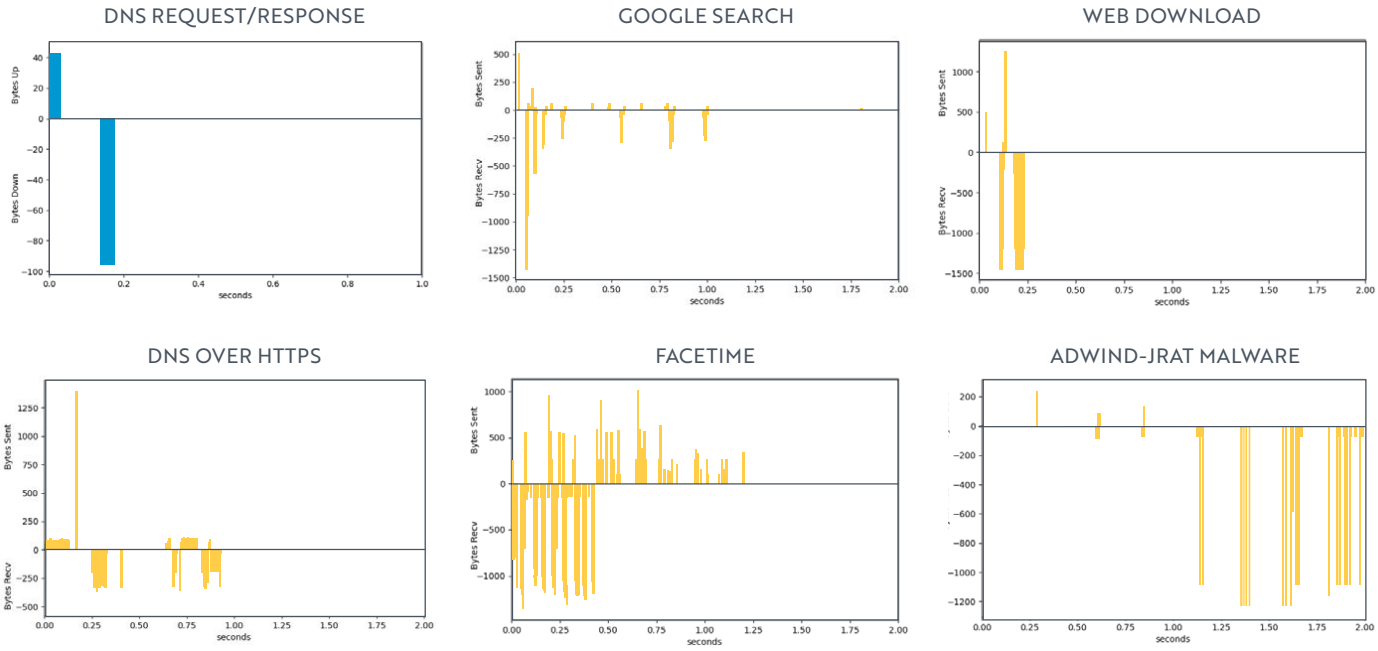
The need to transition from DPI to DPD is underscored by the recent, rapid adoption of the HTTPS standard for the majority of Internet traffic. Previously, security practitioners would apply DPI techniques to unencrypted HTTP traffic to identify critical session details such as browser user agent, presence of a network cookie, or parameters of an HTTP POST. As web traffic moves from HTTP to encrypted HTTPS, network defenders are losing visibility into those details. Deep packet dynamic data (such as SPLT[9]) provides similar insights without the need for payload inspection. By relying on intra-flow visibility with full packet accounting, Encrypted Traffic Analysis can identify characteristics of HTTP flows and distinguish between malicious and benign traffic without decryption.

Analyzing deep packet dynamics both increases the amount of data produced for each flow and makes it more difficult to separate important network signals from noise. To address this challenge, ThreatEye includes a proprietary machine learning engine to apply statistical and machine learning models at the point of collection, allowing it to identify complex intra-flow patterns as the data are arriving. ThreatEye analyzes data across multiple flows and seamlessly integrates this data with its machine learning engine. This combination—streaming ML + rich DPD features—is unlocking visibility for network defenders at a time when legacy techniques offer fewer and few insights into encrypted traffic.

TABLE 2

DPD Illustrated

Similar to a conversation between two people, DPD (here, SPL) capture the back and forth between two Internet hosts, giving us important clues about the encrypted communication.



[9] Sequence of Packet Length and Time.

Above: Sequence of Packet Lengths (SPL) highlighting Packet Dynamics of popular web applications.

The Future of Deep Packet Dynamics

Network visibility is eroding as adoption of encrypted protocols increases. Encrypted Traffic Analysis addresses the loss of visibility by providing alternative techniques for network defenders to gain insight into network behavior despite the encryption, while protecting user privacy. Combining Deep Packet Dynamics with machine learning is the latest advance in ETA. This combination is revitalizing classic approaches to cryptanalysis by applying powerful algorithms to identify patterns in network data and can scale to address the continued growth in network traffic and the increased adoption of encrypted protocols.

LiveAction®

960 San Antonio Rd, Suite 200, Palo Alto, CA 94303
+1 (888) 881-1116

About LiveAction

LiveAction provides end-to-end visibility of network and application performance from a single pane of glass. This gives enterprises confidence that the network is meeting business objectives offers IT administrators full visibility for better decision making and reduces the overall cost of operations. By unifying and simplifying the collection, correlation and presentation of application and network data, LiveAction empowers network professionals to proactively and quickly identify, troubleshoot and resolve issues across increasingly large and complex networks. To learn more and see how LiveAction delivers unmatched network visibility, **visit www.liveaction.com.**