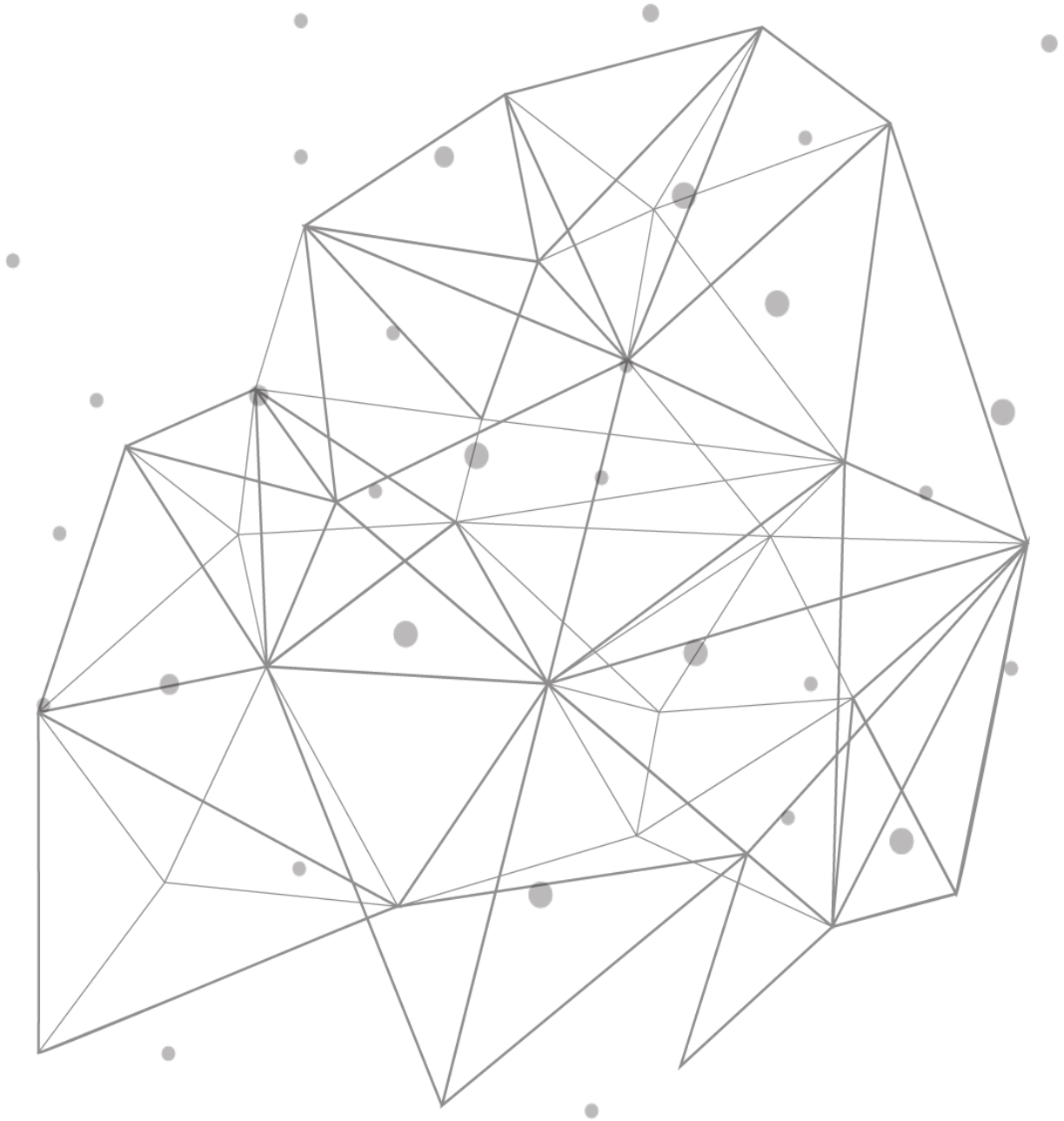
TCPWave DDI - Atlantis Model



Introduction

The cyber threat landscape drives enterprises to constantly track and correlate millions of external and internal data across the infrastructure, and it's impractical to deploy efficient security technology without relying on machine learning techniques. At the same time, it's impractical to effectively build machine learning techniques without a thorough, rich, and comprehensive dataset. Machine Learning (ML) techniques enhance security procedures and practices and simplify network security analysts to quickly identify, prioritize, and remediate new attacks.

TCPWave's DNS TITAN solution provides to combat and safeguards the DNS from the attacks. It uses In-House built tunnel detection Machine Learning (ML) algorithms trained using massive ~3.3M records and varied DNS data, thereby learning and detecting the malicious DNS traffic flowing through the DNS pathways in the enterprises.

Atlantis Model

It is a hybrid model whose deep learning architecture is designed using Convolution Neural Networks (CNN) layer and a Long- and Short-Term Memory (LSTM) layer in parallel. A single layer of Artificial Neural Networks (ANN) aggregates the outputs of these to optimize features learned in prior layers. The CNN layer examines local relationships between the characters and learns higher representational features automatically by treating domain names as one-dimensional grids. The LSTM learns the features shared across the characters of domains by processing the entire query sequence without treating each character independently and retaining long-term character dependencies of the queries.

About - Dataset

As the saying goes, data is the new oil in the modern era of ML and AI. For ML algorithms to work, it is imperative to lay a firm foundation with relevant data. A collection of instances is a dataset; the dataset fed into the ML algorithm is the training dataset. The dataset used to validate the model's accuracy is the test dataset or the validation dataset. TCPWave used a dataset of non-malicious domains and malicious domains. In the case of malicious domains, 51 DGA family queries and an additional 8000 domains were generated by well-known DNS tunneling tools under laboratory conditions: iodine, dnscat2, and dnsexfiltrator.

Model Evaluation

One of the most significant concepts of algorithms is Evaluation. It is the core part of building an effective ML model. Some of the evaluation metrics are accuracy, prediction, recall, etc.

Metrics	Description	Percentage (%)
Accuracy	It represents the number of correctly classified data points over the total number of data points.	97.90
Precision	It is the ratio of true positives to the sum of true positives and false positives.	98.67
Recall	It is the ratio of true positives to the sum of true positives and false negatives.	97.99
F1 score	It is the harmonic mean of precision and recall.	98.33

Performance on DGA families

We have validated the model performance on different DGA families, and the following are the Accuracy and False Negative ratio metrics.

DGA_class	Description	Accuracy (%)
bamital	It is a family of malware/DGA that intercepts web app traffic and blocks access to certain security-related websites by altering the variants.	100
banjori	It is a DGA family that targets the banking system and steals personal information, such as user names and passwords. It sends the information to a malicious hacker.	99.77
chinad	It comes from a family of adware – used to define potentially unwanted programs that often tend to penetrate users with the help of software application packing.	100
cryptolocker	It is a malware threat that infects the computer and searches for files to encrypt.	99
dircrypt	The malware infects a computer and starts encrypting its file system.	98.96
dyre	It is a DGA family that targets the banking system and steals personal information, such as user names and passwords.	100

DGA_class	Description	Accuracy (%)
emotet	It primarily originated as a DGA family that targets the banking system to steal a user's personal information. Later it was spread via phishing email attachments and links.	99.68
enviserv	It is malware that arrives on a system as a file dropped by other malware.	99.8
feodo	A DGA family targets the banking system to steal sensitive information from the victim's computers such as credit card information.	100
flubot	This malware/DGA targeting android users through fraudulent messages or notifications.	99.62
fobber_v1	It is a DGA family that targets banking system to steal the passwords of the users, and the data is encrypted and sent to the Command & Control servers.	100
fobber_v2	It is a DGA family that targets banking systems to steal the users' passwords, and the data is encrypted and sent to the Command & Control servers.	98.66
gameover	It is one of the most powerful malwares that steal bank credentials.	100
locky	It is malware that encrypts the files on the system, making them inaccessible to the users. The hackers demand a ransom for the same.	96.72
murofet	It acts as a virus by infecting executable files and attempts to download malicious files from various domains into the infected system.	99.79
mydoom	It is one of the most fast-spreading viruses affecting the windows operating system.	94.2
necro	This malware attempts to spread itself via email.	98.71
necurs	It is one of the most disruptive forces on the internet. It has harnessed more than nine million computers unwittingly under its control to send spam, distribute ransomware, and attack financial institutions.	97.84
padcrypt	It is ransomware distributed via spam emails.	97.02
pykspa_v1	A DGA-based malware spreads via skype by sending messages to other skype users with links.	97.48
pykspa_v2_fake	DGA-based malware spreads via skype by sending messages to other skype users with links. In this version, the number of domains generated	94

DGA_class	Description	Accuracy (%)
	may vary.	
pykspa_v2_real	It is a worm that spreads via skype by sending messages to other skype users with links.	93.43
qadars	A DGA family targets the banking system to steal the banking credentials.	97.5
ramnit	This type of malware can exfiltrate sensitive data such as user credentials and personal data.	98.33
ranbyus	It is malware that arrives on a system as a file dropped by other malware when visiting malicious sites.	99.58
rovnix	It is malware that usually arrives as an attachment on spam mail.	99.97
shifu	A DGA family targets the banking system to steal user credentials.	91.08
shiotob	A DGA family targets the banking system often spreads in email attachments, and is used to steal banking credentials and personal data.	98.93
simda	It is a large family of malware that, once installed on a machine, is remotely controlled by a malicious attacker to perform various actions, most commonly stealing personal information or system data.	97.84
symmi	It is malware that arrives on a system as a file dropped by other malware when visiting malicious sites.	99.51
tempedreve	It is malware that arrives on a system as a file dropped by other malware when visiting malicious sites.	91.19
tinba	It infects end-user devices, attempts to compromise financial accounts, and steals funds.	99.63

Note: Ignored the metrics of the DGA families for domains less than 100. Click here to learn more about DGA.

Conclusion

Armed with one of the best performing models - Atlantis, the TCPWave Product Engineering team works continuously to integrate the best, latest ML and AI techniques to safeguard the DNS appliances from various attacks such as the DGA, DNS Tunnelling, DNS Exfiltration, etc. to improvise the operational efficiencies of an organization. For a quick demo, contact the TCPWave Sales Team.

References

We thank DataHub for its service in providing the dataset.