WHITEPAPER

Bitdefender

OEM

Antispam Software Development Kit

A TECHNOLOGY BREAKDOWN

www.bitdefender.com

Contents

Spam usually refers to junk or unsolicited emails, but the vast majority of it is anything but benign. Cybercriminals have been using email as a preferred attack vector, as it confers a certain legitimacy to the message, it can be credible if properly formatted and worded, and it's sometimes not considered malicious per se if it has no malicious attachments. Relying more on social engineering to dupe victims into performing various actions, some estimate that four to six out of every 10 emails sent globally are actually spam.

Perhaps one of the oldest scams successfully adopted in the internet age is the Spanish Prisoner scam, commonly known as the Nigerian Prince Scam. It goes back to the 18th century and involves promising the victim a large sum of money in return for a small payment, usually taxes or legal fees. If the victim actually pays, the scammer continues asking the victim for additional payments, invoking transaction failures or other lies.

While not all spam emails are actually scams, it's becoming increasingly difficult for the average user to differentiate between legitimate and illegitimate emails, especially as cybercriminals have adopted new tactics to maximize the success of their campaigns.

Bitdefender has specifically developed and patented technologies that keep up with the evolving nature of spam messages, by balancing accurate detection with performance to swiftly flag any potential threat before it impacts users or organizations.

Antispam SDK (Software Development Kit) Overview

- Full cloud email security solution via our RTDA (Real Time Data Analysis) antispam service
- Wide range of independent filters for a complete inspection of the scanned email (blacklists and content filtering technologies)
- Our cloud databases are updated every second and detection is replicated around the world in a couple of seconds
- Very quick reaction when dealing with FPs/FNs (false positives/false negatives)
- No need for signature updates, as all detection is completed in the cloud
- Small footprint - information is extracted from the email and queried to the cloud - one query for all incorporated cloud filters
- The spam detection technologies are not language-dependent
- Proprietary technologies – patented algorithms and detection methods
- Enables security vendors, telecom companies and email service providers to secure the email flow against email threats

Award-Winning Technology

The Bitdefender Security for Mail Servers solution, powered by the antispam technology, is the only product to have received 24 consecutives VBSpam+ awards, the highest certification awarded in the VBSpam Tests performed by Virus Bulletin.

The performance of our technology translates into a constant detection rate over 99.9% with no false positives. It is the only antispam solution to have achieved VBSpam certification in all 61 Virus Bulletin Antispam comparative tests ever performed.

Bitdefender has been participating in Virus Bulletin's VBSpam testing program since its outset in 2009 and has achieved a pass in every published test it has taken part in. The September 2020 VBSpam test report saw Bitdefender ranked first when compared by the Final Score and continues their solid performance with a 24th consecutive VBSpam+ award, which is the highevst-level certification in the program, thus reflecting the product's ability to correctly block malicious and phishing emails combined with a quick response when filtering legitimate emails.
Ionuţ Răileanu, VBSpam Test Lead - Virus Bulletin

Privacy and Assessment

One of the biggest aspects of email security is privacy. Bitdefender has been focusing on analyzing email content and specific elements without infringing on privacy, by developing detection filters and working with hashes and anonymized information that allow for full privacy while letting our cloud antispam technologies correctly tag the email as legitimate or not.

The Bitdefender Antispam SDK has a local component designed to ensure email and content privacy by extracting only relevant information that helps assess the topic of emails. Also, a series of machine learning classification models and hundreds of heuristics combine with the detection filters to classify/tag analyzed emails as one of five categories (malware, phishing, extortion, scam or marketing). While these tags describe the email's overall category or topic, over a dozen sub-tags are also available to achieve finer granularity for each category.

The sub-tags further narrow down the type of scam under analysis. For example, scams can relate to employment, investment, financial, pharma, and even education, while phishing can be financial or business email compromise/ spear phishing-related.

To ensure full privacy, the technologies behind this initial validation of the email run on the client's machine, with minimum impact on performance. The final validation of whether the received email is indeed spam is performed by the cloud-based component, which receives this initial assessment – along with other proprietary information – to issue the final verdict back to the client.

While the Antispam SDK is fully cloud-based, the local extraction of various components, features, topics, and other anonymized information helps Bitdefender cloud-based antispam technologies assess the status of the analyzed email.

Technologies Description

Fingerprinting

Email fingerprinting is based on patented machine learning algorithms, which are tasked with extracting and analyzing email content, specifically from the subject and email body as well as metadata. These algorithms are designed to withstand poisoning attempts. For example, some spam campaigns embed garbage text, such as quotes, that's either written with a really small font or has the same text color as the background color. While this text may or may not be visible to the user, it can poison fingerprinting algorithms. Using these algorithms to scrub the email's body of any poisoning text is vital to obtain a generic fingerprint that can detect a specific spam wave. In addition, this capability is combined with character visual normalization features that help us detect a spam wave which employs obfuscating techniques, using a generic fingerprint.

An additional algorithm is tasked with extracting an email fingerprint based on the HTML's tree structure. This is particularly useful and reliable when fingerprinting email campaigns that have similar formatting and HTML structure. For instance, some spam waves rely on the same template, with only minor edits to URLs or text used to poison the email's content.

Malicious attachment detection

This technology focuses on identifying malicious aspects of the email, classifying various degrees of threat. It analyses the email's file hashes and URLs and compares it with Bitdefender database of confirmed malicious file hashed and URLs. For example, a malicious file may be included either as attachment, part of an archive or directly linked in the email, triggering the alarm.

Spam image detection

Spammers often include the text as an image in an email to avoid traditional antispam filters based on text-related content. To mitigate this workaround, Bitdefender developed a patented technology that extracts metadata from images in the email. The metadata is analyzed using Bitdefender proprietary machine learning algorithms and is confirmed as spam or legit content.

At the same time, we employ additional filters, including for body parts exposure that, based on a scoring system, confirms if the imagine contains nudity. For example, if in an email contains an image with specific human elements and properties that qualify as nudity, the image will trigger the spam detection.

Other computer vision technologies, like OCR (optical character recognition), face detection and card detection, help us analyze the content from the images attached or linked in the spam messages.

Email address blacklist

We use proprietary email address blacklisting technology to filter out known spamming email addresses. The email addresses are extracted from the body of the message and from the headers. The MD5 hashes are queried to the

cloud. Initially created for Nigerian and lottery scams, this is now very useful in detecting other kind of spam too: fake sales, spear phishing, dating, employment, loan etc.

Using machine learning models, heuristics and clustering methods, these spam waves are identified and the proper email addresses blacklisted.

For example, exploited free webmail domains are gmail.com, yahoo.com, yandex.com, qq.com, hotmail.com.

Phone number filters

According to our observations, telephone numbers are used mostly in Russian, Asian and US spam that focuses on dating, scam & fraud campaigns.

This proprietary technology employs a blacklist of such phone numbers that are present in an extremely obfuscated form in an attempt to avoid detection. Using special extraction methods and visual normalization features, we build detection mechanisms and successfully target these spam waves.

Proactive detection technology

The proactive detection is our most complex antispam filter combining:

- spam & phishing message patterns
- hundreds of heuristic checks
- headers and body analysis
- machine learning models for email classification
- URL threat data and categories

These filters are used to generate proactive detection and prevent real-time spam outbreaks.

Domain & URL reputation

URLs are among the most efficient ways for spammers to capitalize on their illicit work, because it's very easy for users to access them.

Domain detection allows us to block entire list of URLs associated with a specific domain used in spam waves.

We use a complex system that can analyze a list of features for any domain and identify the likelihood of it being used in spam attacks. We look at data such as HTML page structure and various other characteristics.

This allows us to identify previously unknown spammy domains, by comparing them to clusters of known malicious domains, allowing for zero-day spam detection.

URL detection is used in cases when legit domains are exploited, hacked or infected and we want to add a controlled detection. This lets us identify malicious URLs even when they are located on legit domains, such as shortening, free hosting and file-sharing domains.

Cryptocurrencies

The technology targets extortion scams and detects multiple obfuscated cryptocurrency wallet addresses used in scam emails. It covers cryptocurrencies such as bitcoin (BTC), litecoin (LTC), dashcoin (DSH) and etherium, with support for others.

Outbreak detection

We use email threat intelligence data, feeding our internal systems to help us enhance real-time outbreak detection and target spam campaigns.

At the core of our detection capabilities, we employ machine learning technologies and various clustering algorithms to identify the malicious email components. To ensure a high level of efficiency, we combine these capabilities with the previously mentioned filters.

Conclusions

Spam is becoming an increasingly common attack vector and one of hackers' preferred channels for reaching their victims. The spam campaigns are also becoming more targeted than ever, and it is extremely important for antispam technologies to be able to address campaigns in any language.

The antispam technologies need to constantly evolve to keep up with the newest and most innovative spam strategies trying to bypass them.

Machine learning algorithms are a key component in the next-gen antispam technology, giving security professionals the tools to combat all types of spam, such as phishing, spear phishing-BEC, malspam, extorsion, fraud and scams.

Antispam SDK (Software Development Kit) Overview

- Stellar ratings from independent testing organizations
- Cloud-based detection, very low false positive rates, and fast response time
- Proprietary technology with patented algorithms and detection methods
- Privacy-oriented: when developing detection filters protecting end users' privacy is our priority
- Phishing and fraud email detection
- Language-independent
- Leveraged by multiple OEM partners to enhance antispam detection

Partnering with Bitdefender provided us the technology needed to support our customers with exceptional products and services. In addition, we benefit from Bitdefender's timely and customized support throughout the integration process.

Director of Engineering, Global 500 Computer Services Company
Source: TechValidate. TVID: 78B-55B-B67

Bitdefender Technology Licensing Program

Bitdefender's Technology Licensing program allows its partners to grow their business and customer base with comprehensive security technologies. The program is unique in its ability to meet specific business objectives, combining advanced technology with unprecedented flexibility in terms of business and licensing models.

OEM partners add Bitdefender security technology to strengthen an existing offering, integrate it into a solution or service to expand capabilities, promote attractive value propositions to new or existing customers, secure additional revenue, increase customer satisfaction and differentiate in the market.

Learn more about Bitdefender's Technology Licensing solutions: https://www.bitdefender.com/oem/

WHY BITDEFENDER?

You're not alone. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology. We've become the provider of choice for leading Independent Software Vendors (ISVs), hardware vendors and service providers looking to integrate security technologies into their products and services. Today, Bitdefender technology is found in over 38% of the world's security solutions and has over 150 technology licensing partners worldwide.

PROVEN SOLUTIONS

Independent tests conducted by third-party industry organizations like AV Comparatives and AV-Test consistently prove that Bitdefender solutions have some of the best detection and performance rates in the industry.

ADVANCED TECHNOLOGY

Bitdefender takes a layered approach to cybersecurity, utilizing artificial intelligence, deep learning, and anomaly-based detection to provide proactive protection for unknown threats before they can infiltrate the user's system. Over one hundred patents were issued for core technologies in the past three years alone, 230 more are currently filed for examination, and 10% of our patents pertain to machine-learning algorithms.

EASE OF INTEGRATION

Bitdefender technologies can easily integrate with existing hardware and software solutions or services – significantly reducing the burden on your development resources. Bitdefender also supplies comprehensive documentation, including step-by-step "how-to" guides and descriptive examples of all SDKs, to support the process.

PROTECTION FOR ALL ENVIRONMENTS

Bitdefender SDKs and APIs work across major operating systems – Windows, Mac, and Linux – as well as all major hardware platforms such as Intel x86, ARM, MIPS and PowerPC. Built from the ground up with portability in mind, they can easily be integrated into additional platforms with minimal programming effort.

STRATEGIC SERVICES AND SUPPORT

All Bitdefender Technology Licensing agreements are backed by strategic technical support services with extensive Service Level Agreements (SLAs). This helps you focus on providing an extraordinary level of service to your customers and spending more time on your business goals and execution.

ENGAGED PARTNERS:

KONICA MINOLTA · JUNIPER NETWORKS · FIREEYE · WatchGuard · NETGEAR · Acronis · TitanHQ · adaptivemobile · LogMeIn · GFI Software · KERIO

INDUSTRY RECOGNITION

AV comparatives CERTIFIED · AV comparatives Product of the Year 2019 · FORRESTER WAVE LEADER 2019 Cloud Workload Security · BITDEFENDER ADVANCED ENDPOINT PROTECTION NSS Labs RECOMMENDED

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win — a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a **luminous Dragon-Wolf** on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.

Bitdefender-OEM-WhitePaper-AntispamSDK-creat4969-en_EN
12/18/19November 18, 2020 2:53 pm17/18/20