White Paper

The different types of spoofing attacks

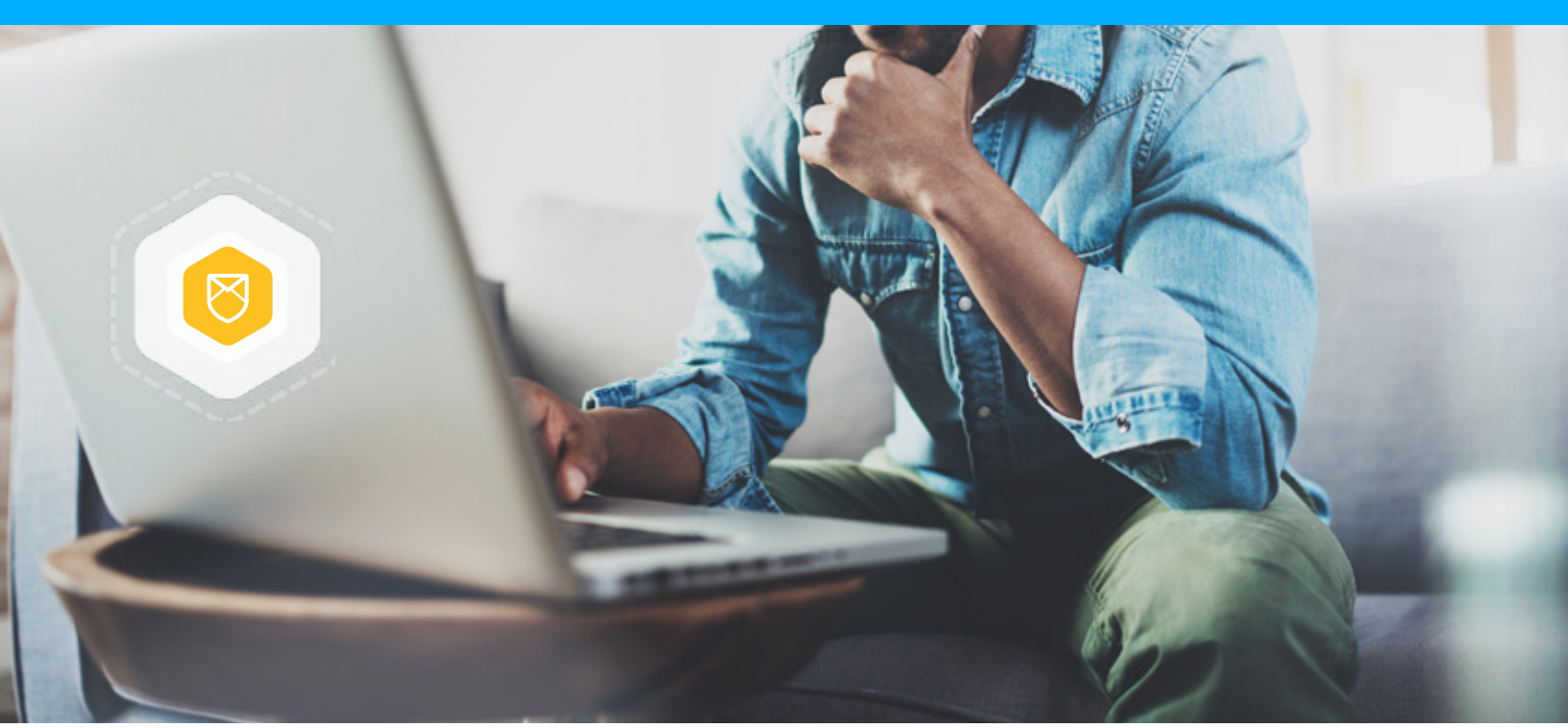
IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Introduction

Cybercrime will cost enterprises $5.2 trillion within the next five years. Over time, hackers have gotten more and more sophisticated and targeted with their attacks, confronting some of the largest businesses in the world. But large enterprises aren't their only victims. 43% of attacks are directed at small businesses, yet only 14% feel prepared to defend themselves.

And one of the most nefarious, abundant types of cybercrime—regardless of company size—is spoofing. In this article, we'll review six ways hackers circumvent standard security tools with spoofing and how you can best protect your company against spoofing attacks.



Contents

What is Spoofing

Spoofing occurs when a criminal poses as another person, entity, or organization to gain access to credentials, IP, or money. Hackers use a broad range of strategies to make their spoofing look legitimate, with spoofed websites, email addresses, phone numbers, IP addresses, and even Domain Name Servers. Any of these spoofing techniques can have devastating ripple effects on your company and clients.

Today, security teams typically only use three main protocols to protect against spoofing: Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC).

While SPF can protect against some forms of spoofing, authentication only happens on the specific mail from domain, not the From address that users see. Additionally, SPF doesn't work on forwarded emails and requires constant updates to its domain list.

DKIM takes this protection up a notch. Unlike SPF, DKIM can confirm that messages weren't tampered with in transit, and can therefore survive forwarding.

Along with SPF, DKIM set the stage for DMARC, a method of managing unauthorized use of email domains. With DMARC, security teams set up policies to monitor email traffic, send unauthorized emails to spam folders, and/or reject incoming emails altogether. DMARC is a useful way to block at least some spoofing attacks, but ironically, greater adoption has led attackers to launch more impersonation attacks that DMARC cannot detect.

So while all three methods are a helpful starting point, they are not a comprehensive solution. Below, we define six types of spoofing that can get around most companies' existing protocols, the vulnerabilities they exploit, and how SOC and security teams can combat them.

Types of Spoofing

- Email Spoofing
- IP Spoofing
- ARP Spoofing
- DNS / DNS Cache
- Domain Spoofing
- Caller ID Spoofing

Email Spoofing

Email spoofing is perhaps the most common form of spoofing. Hackers send over 300 billion spoofing emails per day, and the FBI reported over $26 billion in losses from email account compromise between 2016 and 2019. This costly and dangerous problem starts when a scammer sends an email with a forged sender address. Due to the security limitations of email protocols like SMTP, it is up to the email provider and other third party software systems to try to determine when an email has been spoofed. The four major types of email spoofing are:

1

Exact sender name impersonation.

This is the most common type of email spoofing and involves the forged sender address resembling that of a close colleague or friend.

Example: **JeffBezos@technologybusiness123.com**

2

Similar sender name impersonation.

The forged email appears to come from a trusted source with minor errors that can easily be overlooked.

Example: **JeffBezos@technologybusiness123.com**

3

Lookalike/cousin domain spoofing.

Significantly less common than the first two types of spoofing, this requires scammers to register the domain to set the right authentication records in the DNS.

Example: **JeffBezos@amaz0n.com**

4

Exact domain spoofs.

This is the rarest type of email spoofing technique used, but not impossible to encounter. The forged email domain exactly matches the spoofed domain.

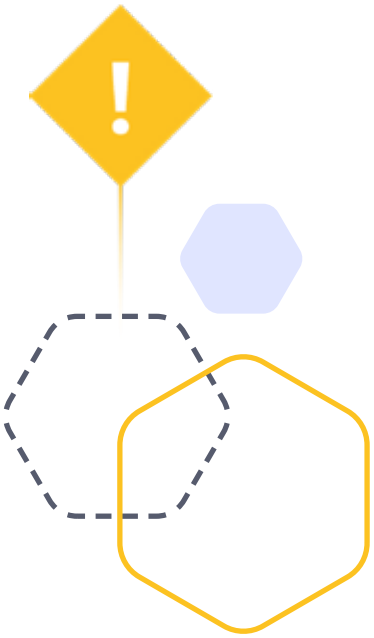
Example: **JeffBezos@technologybusiness123.com**

Besides setting up SPF, DKIM, and DMARC protocols, companies need a mailbox-level anomaly detection platform that combines machine learning, human behavior, and business insights. This extra level of security can flag impersonation attempts and lookalike spoofing that would normally slip through the DMARC and gate way level cracks.

IP Spoofing

According to the Center for Applied Internet Data Analysis, 21 million attacks were mounted on 6.3 million unique internet protocol addresses within just two years. These numbers are steadily mounting because of the ease with which attackers spoof IP addresses and trick computers into thinking a message is coming from a known source. IP spoofing is difficult to pinpoint because it occurs at the network level, leaving no trace of tampering. Hackers often use IP spoofing to initiate Man-in-the-Middle (MITM) and Denial-of-Service (DoS) attacks on specific devices and their associated infrastructure. These forms of attack overwhelm networks with high traffic all while disguising the traffic source.

Spoofed IPs can bypass security scripts and aren't always included in blacklisted IP records. Worse, IP spoofing can spread over multiple regions, hitting tens of thousands of computers at once. While IP spoofing isn't easy to spot, there are ways you can avoid it. Overall, you need a network monitoring system that is constantly looking for IP packet inconsistencies and presenting threats to your security team. It's a good idea to get a network attack blocker and put some computing resources behind a firewall as well. IP spoofing is also harder on sites that have migrated to IPv6, the newest Internet Protocol, so make sure your web designers are aware and have made the update.



ARP Spoofing

Address Resolution Protocol (ARP) spoofing, sometimes referred to as "ARP poisoning," is a type of attack in which a hacker sends fake ARP messages over a local network. In doing so, the attacker links his address to the IP address of a legitimate server or computer on the network to manipulate or "listen" to traffic. Besides obtaining confidential information, ARP spoofing can be used in DoS and MITM attacks or enable session hijacking, in which attackers steal session IDs that give them permission to access restricted systems or data.

There are several approaches to hindering ARP spoofing attacks:

- The first, very manual way is to map all the MAC addresses in your network to IP addresses. Although this is highly effective, it's a huge burden on your security team because any network changes will require an update to ARP tables across all hosts.
- Instead, most companies require their employees to use VPN. To log into a company's main systems, like Salesforce, Gmail, etc., employees have to log onto the organization's specific network and typically perform two-factor authentication.
- Physical security is an important element of ARP spoofing prevention as well. One safeguard is implementing ethernet switch security. This guarantees the validity of ARP messages and identifies anything suspicious. Pay attention to your network signals as well. They can sometimes extend to a parking lot or street corner, so ensure that only managed devices can connect to it.
- Lastly, make sure the sites your employees visit have SSL and TLS encryption. This won't preclude attacks from happening but can lessen the damage of an attack by muddling login credentials.

DNS/DNS Cache Poisoning

You DNS attacks are also on the rise. One such example was a spoof of WikiLeaks in 2017. A group of hackers called OurMine used DNS cache poisoning techniques to thwart traffic from the real WikiLeaks site and push it to their own page. While this attack resulted in great embarrassment, there have been other, much larger, and more severe examples of DNS poisoning. In 2018, a DNS spoofing attack was launched on AWS, rerouting traffic from several hosted domains to other sites. One of those sites was MyEtherWallet. Hackers made a spoofed version of the site to collect user credentials and ended up stealing $17 million worth of Ethereum. Other notable DNS hacks have harmed Facebook, Malaysia Airlines, and even domestic and international government agencies.

In Domain Server spoofing (DNS), otherwise known as "DNS cache poisoning," hackers alter DNS records to reroute traffic to a fraudulent website. Every time an employee tries to go to a specific site, they'll be redirected to a fake one that's under the attacker's control. Some of these sites may look fairly similar to the site the employee was attempting to visit, making it easy for hackers to procure usernames, passwords, or other sensitive material.

The most basic way to protect against DNS attacks is with DNS filtering. Blocking your DNS servers from answering Internet DNS queries can drastically reduce the potential for DNS spoofing. Beyond that, consider using DNS spoofing detection tools, domain name system security extensions, and end-to-end encryption. Encourage your employees to use VPN when accessing company systems, instruct them not to click on links they don't recognize, and teach them how to scan their computer for malware.

Domain Spoofing

Domain spoofing occurs when an attacker appears to use a company domain to impersonate an employee in an email or make a malicious website seem safe. Attackers are clever and use the same or similar branding, logos, and taglines of the real business, or even co-opt employees' email signatures. These disguises make people feel comfortable clicking on links, downloading files, wiring money, or submitting credentials. And with the rise of bots, domain spoofing has become even easier and more prolific. Over the past few years, domain spoofing has doubled, causing $1.3 billion in losses.

Domain spoofing, as you might guess, is near-impossible to detect. Hackers can create fake emails and websites that are slightly different from the real page without anyone ever knowing. Training employees to pick up on domain spoofing clues is a good idea, but they can't and won't catch everything. You need advanced methods of early detection to block tainted emails from ever reaching an employee's inbox. State-of-the-art email platforms can recognize impersonated email addresses and spoofed embedded links, stopping domain spoofing in its tracks.

Caller ID Spoofing

If you haven't received a phone call with a spoofed caller ID lately, you are one of the many few. At the end of 2019, over 80% of scam calls in the US used local area codes to get victims to pick up. And in 2020, the Federal Communications Commission reported that US consumers received nearly 4 billion robocalls per month. Although caller ID spoofing is often presented in the context of employees' private lives, it can affect their professional life as well. Many organizations provide their employees with company phones, and those are just as vulnerable to caller ID attacks.

Caller ID spoofing is just what it sounds like–hackers manipulating the telephone network to pretend that a phone call is coming from a certain area code, usually one the recipient is familiar with. To accomplish this, most attackers use Voice over Internet Protocol (VoIP) services that transmit calls over the internet. Train your employees to let these calls go to voicemail and alert the security staff if the calls continue. Place phone numbers on the Do Not Call Registry and talk to the enterprise phone carrier about their filtering services.

No matter which tactic attackers use, their main goal is to obtain sensitive information, install malware, or download dangerous attachments. As we've seen with above examples, each spoofing technique can have detrimental consequences for organizations and their customers. You need a cutting edge platform that can keep spoofing attacks at bay, and legacy security technologies aren't going to cut it.

Protect Yourself from Email Spoofing with IRONSCALES

IRONSCALES is a self-learning email security platform that can anticipate, identify, and react to targeted threats. Not only can the IRONSCALES platform help prevent email spoofing, its services reach beyond that to provide a secure and comprehensive experience for any company. Every time an email reaches your server, IRONSCALES looks for anomalies that could indicate impersonation, credential harvesting attempts, and known malware. IRONSCALES also has built-in natural language processing capabilities to pick up on fraud, and can cross-check emails against a log of emails other companies or employees have flagged.

With IRONSCALES advanced protection, you can avoid the adverse effects of spoofing and ensure a safe experience for employees and clients alike. Learn more about what IRONSCALES has to offer by scheduling a demo today.

Gartner peerinsights™

★★★★★

Great anti-phishing platform

-CISO in the Services Industry

Great anti-phishing platform that really gives added value for attacks a mail relay can't detect properly. Also help with forensic investigation of email incidents. Awareness program is nice and the reporting add-on can be implemented on many platforms (Outlook desktop/phone app, OWA).

Awards

2021 GLOBEE AWARDS GOLD WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

2021 GLOBEE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

2021 GLOBEE AWARDS BRONZE WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

Best Security Awareness Training 2021

Best Email Security Provider 2021

Best Phishing Protection 2021

Best Post-Delivery Protection 2021

IRONSCALES SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP CYBER RISK SOLUTIONS

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security andAnti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com