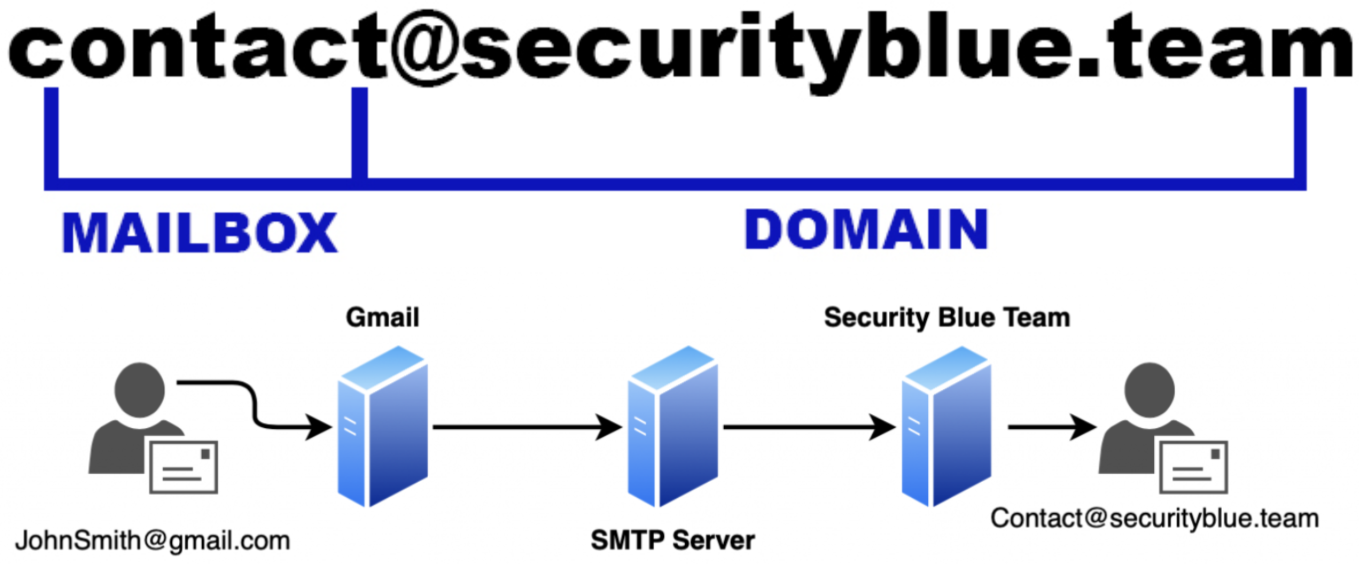
Phishing Analysis

Social Engineering

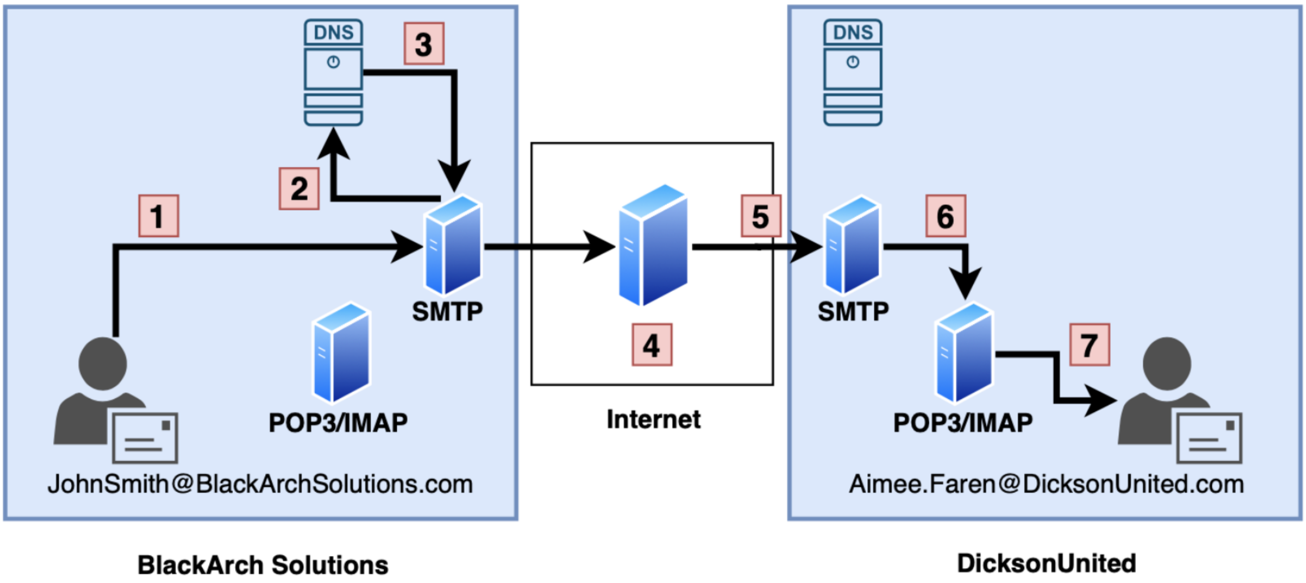
Social engineering is the practice of exploiting a human as opposed to a system, using psychological methods in order to get them to complete actions that they wouldn't normally do, such as disclosing confidential information, allowing someone into a restricted area without proper authorization, or transferring money to an unverified account.
Phishing is a social engineering attack.



Email Protocols

- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol 3 (POP3)

- Internet Mail Access Protocol (IMAP)



Webmail

Webmail allows users to access their emails as long as they have access to an Internet connection and a web browser.

Email anatomy

Email Header

Header fields

- **From**, showing the sender's email address
- **To**, showing the recipient's email address
- **Date**, showing the date when the email was sent

Optional header fields

- **Received**, showing various information about the intermediary servers and the date when the message was processed
- **Reply-To**, showing a reply address
- **subject** showing the message's subject
- **message-ID**, showing a unique identification for the message
- **message body**, containing the message, separated from the header by a line break

Email body

An email body is where the information written by the sender is displayed for the recipient. This can be purely text-based or it can include hyperlinks, images, and HTML styling.

Phising

Phishing is a type of email-based attack, where malicious actors are actually attacking humans instead of computer systems, in order to get them to do something they normally wouldn't. Examples include giving out their account credentials, downloading malware, transferring money, disclosing information, and more.

Reckon Emails

- Recon spam emails that contain nothing except random letters in the body text such as "adjdfkaweasda".
- Emails that use social-engineering techniques to try and get the recipient to respond.
- More complex emails use tracking pixels to see if the email has been viewed in an email client.

Credential Harvester

- Imitates commonly-used websites and services (such as Outlook, Amazon, HMRC, DHL, FedEx)
- Entices the recipient to enter credentials into a fake login portal.
- Uses social-engineering tactics including; creating a sense of urgency, and using false authority.
- URLs may be completely random or attempt to copy the legitimate domain name of the organization they are masquerading as.
- Often have small spelling or styling mistakes, something that is extremely rare with legitimate emails coming from big brands and organizations.

Smishing

Smishing is a kind of phishing attack, where the attack vector is through a text message or SMS.

Vishing

Similar to smishing, vishing is a kind of phishing attack, where the attack vector is through a phone call.

Whaling

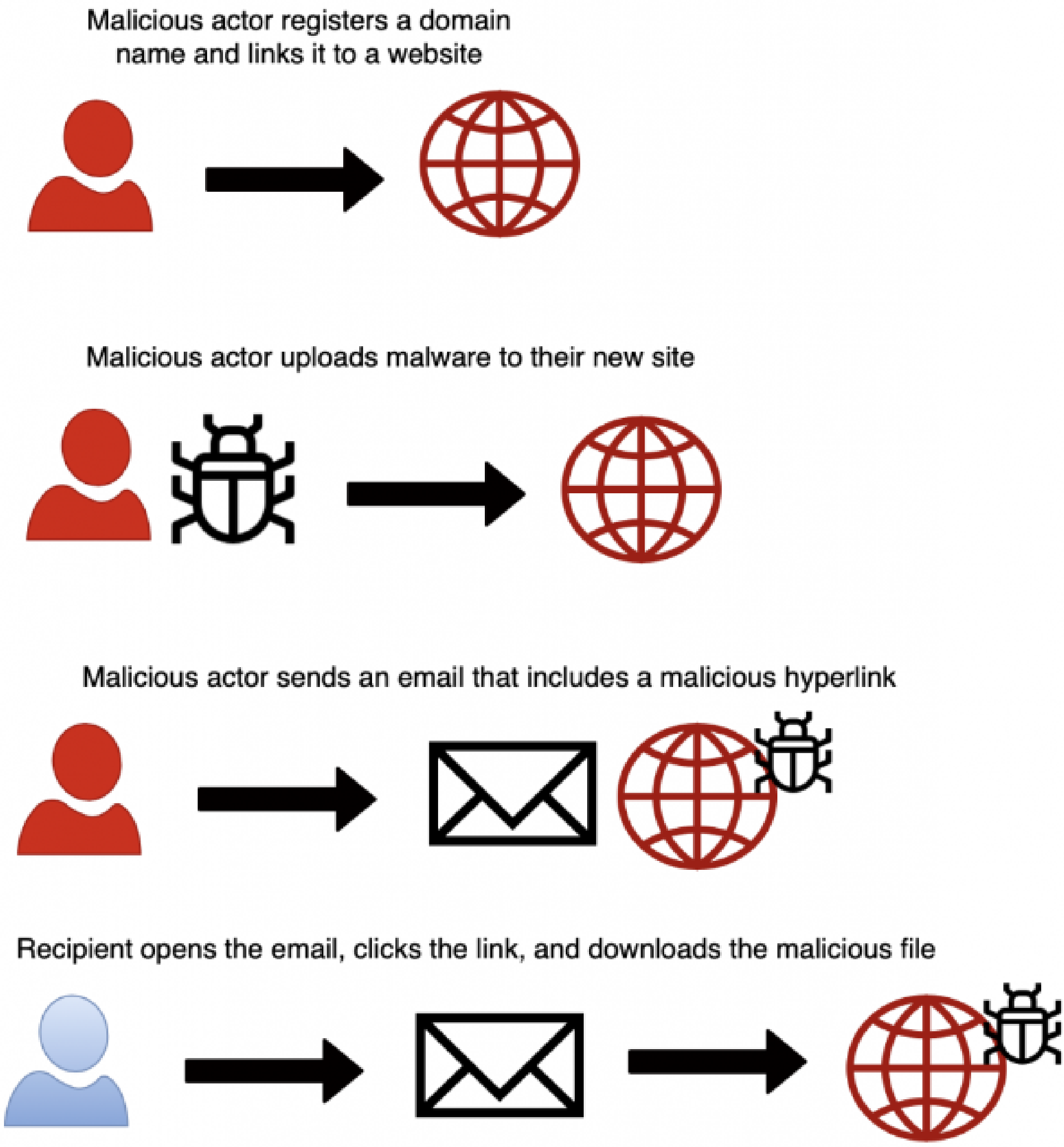
Whaling is a highly-targeted phishing attack that looks to target individuals within management positions in an organization, often C-level executives, due to the wealth of information they have access to.

Malicious Attachments

Microsoft Office Macros

Hosted Malware

- Malicious Domains



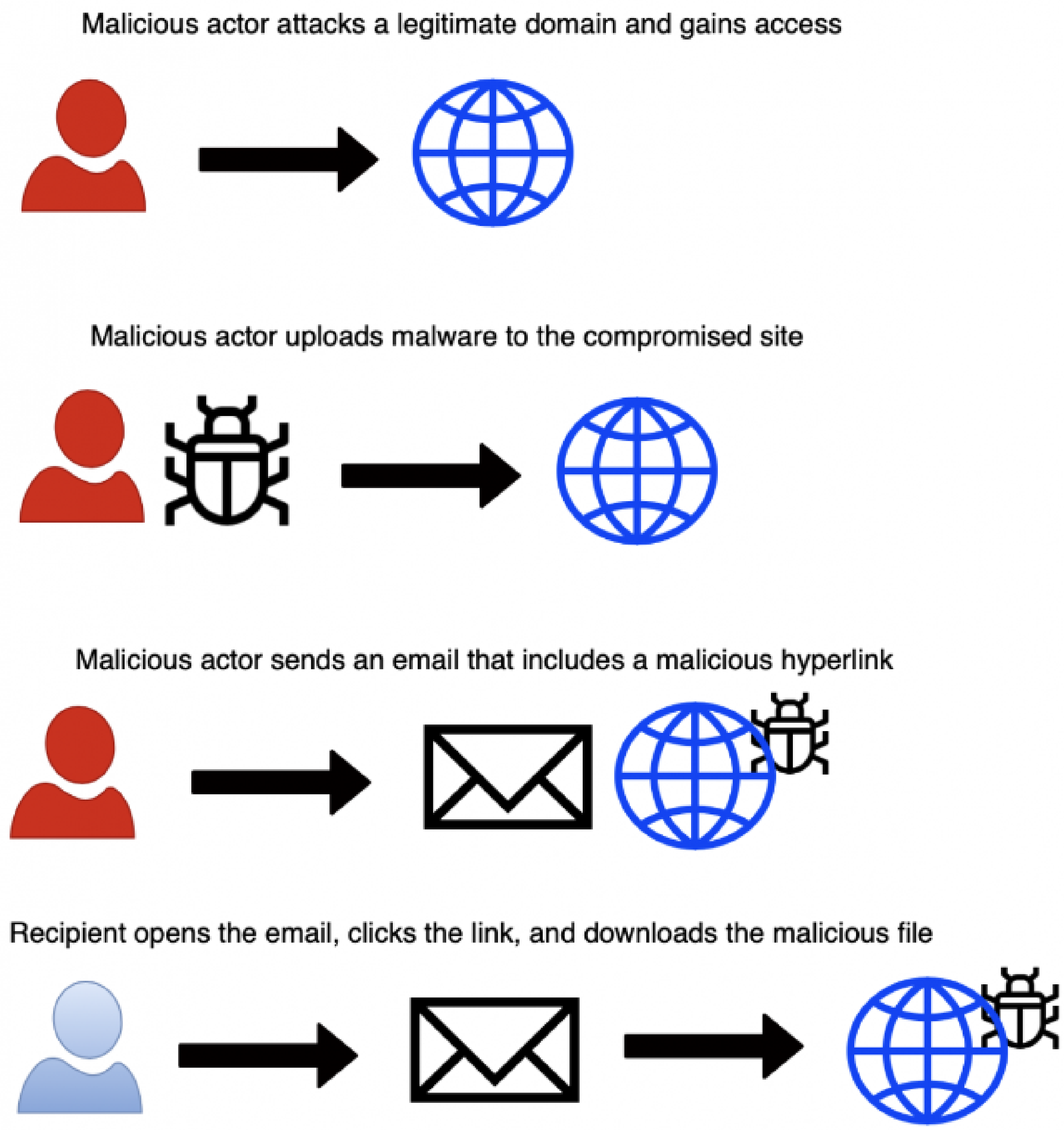
Malicious actor registers a domain name and links it to a website

Malicious actor uploads malware to their new site

Malicious actor sends an email that includes a malicious hyperlink

Recipient opens the email, clicks the link, and downloads the malicious file

- Compromised Domains



Malicious actor attacks a legitimate domain and gains access

Malicious actor uploads malware to the compromised site

Malicious actor sends an email that includes a malicious hyperlink

Recipient opens the email, clicks the link, and downloads the malicious file

Spam emails

Spam emails (also known as "junk mail") are messages that are unsolicited, unwanted, or unexpected but are not necessarily malicious in nature.

- Newsletters that the user has unknowingly signed up for
- Marketing emails trying to promote products and services
- Update announcements from companies and services the user has registered with

Spear Phising

Spear phishing is when a malicious actor spends time before the phishing attack to gather information about their specific target, to make the email more effective. By tailoring the email to the target, it makes it more convincing.

Business Email Compromise

A business email compromise is a phishing attack that can target any organization but focuses on those that are likely to transfer large amounts of money to either purchase goods or pay other parties such as vendors. The malicious actor will monitor their target over a period of time to determine which companies the organization pays, and when they have found a relationship between the company and a supplier, they will either compromise an email account belonging to a member of the executive board or a high-level employee, or spoof the address so it appears legitimate, and will instead direct the relevant employees to transfer the money to a different bank account that is under the malicious actor's control.

Tactics and techiques

Impersonation

Impersonation is the act of pretending to be somebody else. This can be used by malicious actors to trick their target into thinking they are someone they know, making them more likely to open and interact with a phishing email. A malicious actor could pose as a friend, a colleague, or even someone higher up within the organization, such as a manager, director, or even the CEO.

Typosquatting

Typo squatting is the act of impersonating a brand or domain name by misspelling it, such as missing letters or including additional ones.

Homographs

This attack exploits the fact that many different characters look exactly alike. These characters are called homographs, and the problem is with how the characters are encoded using Unicode.

Sender Spoofing

Sender spoofing is the process of making the sending address in an email look the same as a legitimate email to make the recipients believe it is coming from a genuine sender.

HTML Styling

HTML styling is where code and images are used to style an email. This is used by legitimate emails to provide a more visually attractive design, making the email appear more professional.

Attachments

- Non-malicious files that are used for social engineering.
- Non-malicious files that have malicious hyperlinks
- Malicious files

Hyperlinks

A hyperlink is a webpage URL that is embedded into text, a button, or an image. When clicked, it will open the recipient's default browser, and navigate to the webpage for them. Hyperlinks are used when the attacker wants to direct the target to web resources, such as a malicious file download, a page with a fake login portal acting as a credential harvester, or other content as part of their phishing attack.

URL-Shortening

A tactic for disguising malicious URLs, and preventing some aspects of automated security analysis, is the use of URL shortening services such as Bitly and Short URL. These services work by keeping a record of full URLs and generating short versions that simply redirect to the full URL.

Use of Legitimate Services

Phishers will make use of legitimate services such as free email providers, to bypass defensive measures that can be implemented by defenders. Whilst we will go into detail about email blocking in the Defensive Measures section of this domain, organizations will typically not block webmail domains, such as: Gmail.com, Outlook.com

---

Email Investigations

Artifacts

Artifacts are specific pieces of information we need to retrieve from emails that allow us to conduct further searches, share intelligence with other organizations, and take defensive measures.
Email Artifacts

- Sending Email Address
- Subject Line
- Recipient Email Addresses
- Reply-To Address
- Date & Time

File Artifacts

- Attachment Name
- SHA256 Hash Value

Web Artifacts

- Full URLs
- Root Domain

Collect hashes via Powershell
get-filehash -algorithm {hashtype} {filename}

Collect hash via Linux CLI

- sha256sum {file}
- sha1sum {file}
- md5sum {file}

Investigation tools

Visualization tool

- URL2PNG
- URLScan

URL Reputation tools

- Virustotal
- URLScan
- URLhaus
- PhishTank

File Reputation tools

- Virustotal
- Talos File Reputation

Interaction tools

- Sandboxes like Hybrid Analysis

Defensive Actions

Preventive

Marking external emails
Email security technology

- SPF
  This record is established to identify the hostnames or IP addresses that are allowed to send emails for your custom domain. When having an SPF record specified on your domain, helps prevent a malicious actor from spoofing your domain.
- DKIM
  Domain Keys Identified Mail (DKIM) is a method of email authentication that cryptographically verifies if an email has been sent by its trusted servers and hasn't been tampered with during transmission. The way that DKIM works is that when the mail server sends an email, an encrypted hash of the email contents is generated using a private key and then it adds this hash to the email header as a DKIM signature.
- DMARC
  This type of record allows the domain owner to specify what should happen if emails fail both SPF and DKIM checks. There are three basic options that the mail server can take: none, quarantine, and reject.

Spam filter

- Content filters
- Rule-based filters
- Bayesian filters

Attachment filtering
Attachment sandboxing
Emails that include file attachments are extracted and analyzed, and files are detonated (run) in a virtual

environment, where everything is monitored to actually see what happens when a file is executed.
Security awareness training

- Preferably during the onboarding process (where a new employee joins a company), users should be put through either an in-person or an online training course that teaches them how to spot phishing emails, and the actions they should take (generally reporting them to the security team).
- Simulated Phishing Attacks

Reactive

Blocking Email Artifacts
Blocking Web Artifacts
Blocking File Artifacts