SEQRITE

WHITE PAPER

EVOLUTION OF SPEAR-PHISHING ATTACK

CASE STUDIES AND HOW TO PREVENT

www.seqrite.com

AUTHORS

Shiv Mohan
Security Research Lead

Jatin Sharma
Data Analyst

Table of Content

Introduction

Phishing is a social engineering technique to steal sensitive data like credentials personal and financial details of a victim.

Spear phishing is a special Phishing attack that targets a particular individual or group within an organization or business. In this attack, the Attacker tracks and gathers some basic information about the target before sending the phishing payloads via various phishing techniques. A successful attempt at these attacks can cause organizations financial loss and brand damage.

Spear phishing attacks are very efficient and hard to detect by the traditional security defenses as the techniques used by attackers mimic trusted services. For example, attackers frequently target executives and employees by sending EMAIL that pretends to be from trusted sources with a sense of urgency & high importance or lure the victim into harvesting sensitive data. Once successfully exploited, the Attacker can gain unauthorized access to enter the organization and perform criminal activities such as sensitive data theft & trading the stolen data on the dark web, malware spread, ransomware attacks, financial scams, etc.

In Spear phishing, the Attacker gathers plenty of details about targeted victims to trick even the most alert tech-savvy individuals.

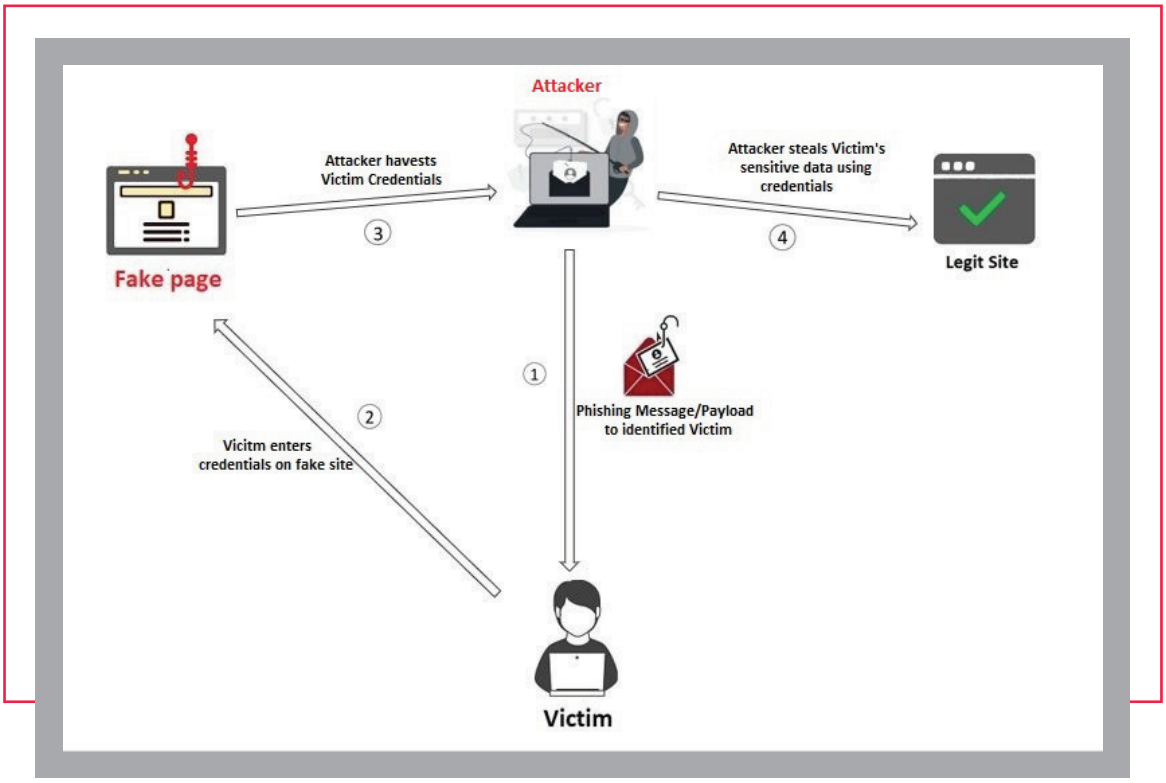


Fig-1 Spear-phishing attack chain

Spear-phishing is becoming the standard technique to gain Initial Access for advanced persistent threat (APT) attacks. The attackers use advanced malware and multi-stage operations to accomplish a particular objective, gaining long-term access to the organization's sensitive networks data and assets.

Phishing attacks are generalized attacks sent to a targeted large number of victims. In contrast, spear-phishing attack is more sophisticated, and targets are specific to victims for whom attackers gather the details to plan the attack. This makes it more challenging to identify spear-phishing attacks. A whaling attack, a type of spear-phishing attack, is a highly sophisticated and personalized attack where targets are high-value top-level executives like CEO, CTO, and VPs of organizations.

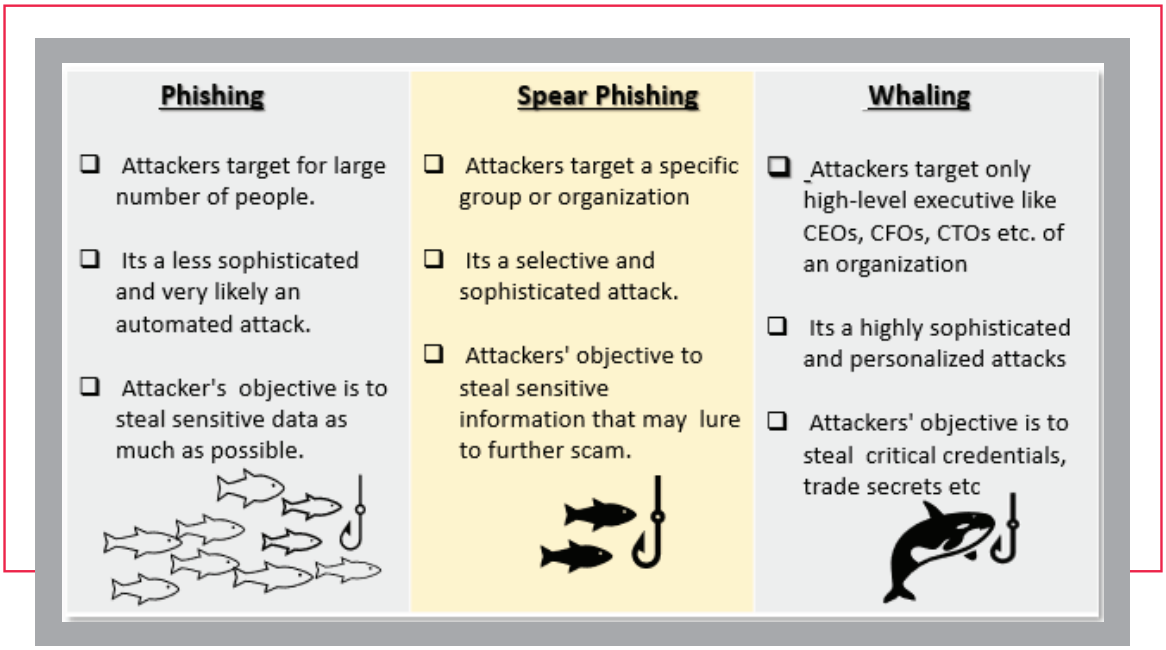


Fig-2 Phishing Vs Spear-Phishing Vs Whaling

Spear phishing techniques

01 Emails with Phishing attachments & embedded links: The attacker sends emails to targeted victims with attached documents or embedded shortened & dynamic URLs that spoof victims to land on a phishing site.

02 Messaging & calling services: The attacker shares phishing links to the target via messaging services like SMS (Smishing), WhatsApp, etc., Phone Calls (Vishing) to victims to lure them into accessing phishing URLs.

03 Social networking sites: Attackers target victims on networking sites like Facebook, LinkedIn, etc. and share a phishing link

03 Malware: The attacker manages to drop malware or scripts that land victims at phishing sites once executed.

05 Phishing as-a-service & Phish Kits: Attackers use Phishing services or kits for targeted users.

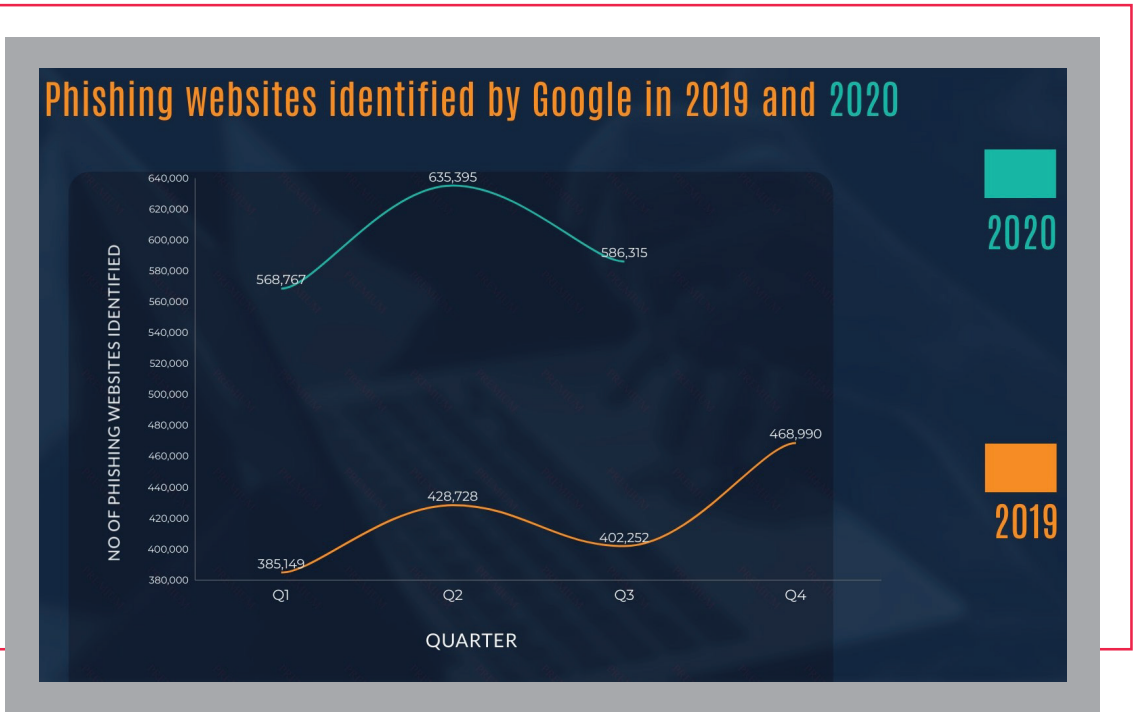
Characteristics of spear-phishing

- Sense of urgency, with research on target with social engineering, the Attacker shares phishing content with a sense of urgency, threat, high importance to spoof the target. For example, Fake emails from the IT department request the victims to change passwords urgently, but it is a victim to a fake website to harvest the credential.
- Spear phishing is sophisticated. Attackers pretend to be a trusted individual or group, but a closer examination may show typographical errors, incorrect jargon, and too formal or informal message content.
- Always ask for Sensitive information or money. Example: Fake messages declare you as a 'winner.' for a lottery or any contest winner lure targets to click and land on a phishing page to get 'Rewards' by submitting bank details or other sensitive credentials.

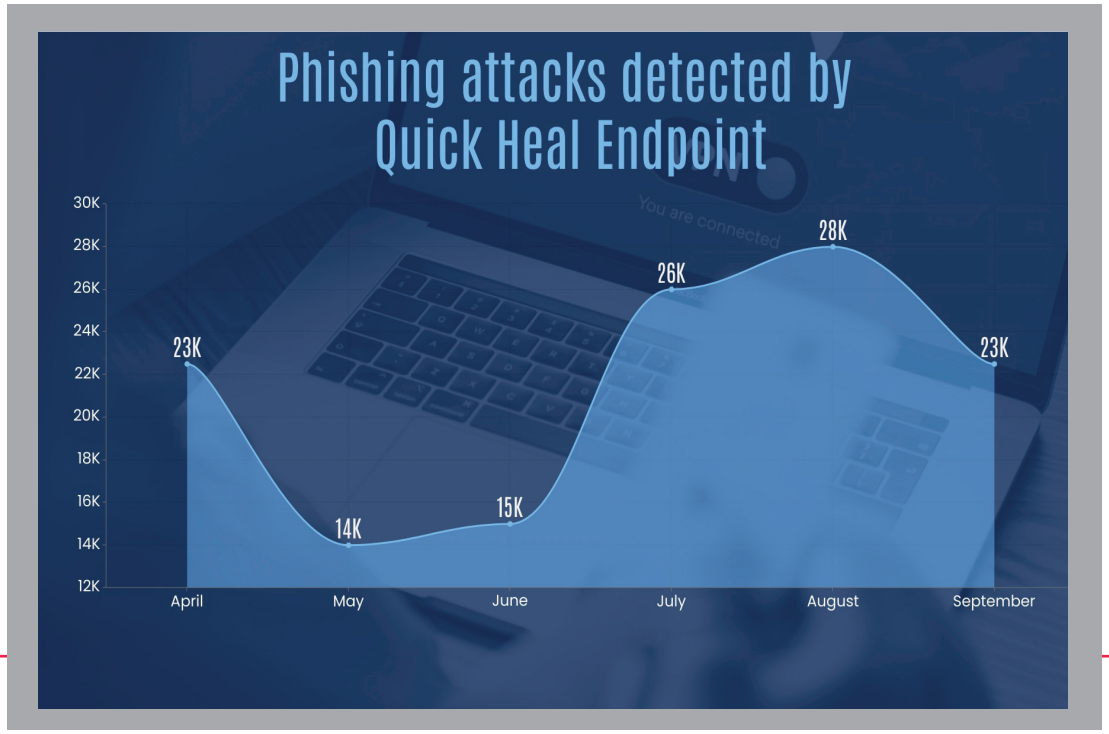
The UPSURGE OF SPEAR-PHISHING

In the last few years, there has been an upsurge in spear-phishing attacks targeting individuals in various sectors, including Healthcare, Technology, Social media, professional Services, finance, Manufacturing, Energy, etc. During the Covid pandemic, a spear-phishing attack surge was observed in Government sectors & other healthcare sectors. The Attackers attempt to phish victims by creating Covid19 related havoc, donation scam, fake vaccinations schemes to harvest sensitive data, or money scams.

According to Google, Gmail blocks more than 100 Million phishing emails every day. While a week during the covid-19 period, Google saw 18 million daily malware and phishing emails related to COVID-19. This is in addition to more than 240 million COVID-related daily spam messages.

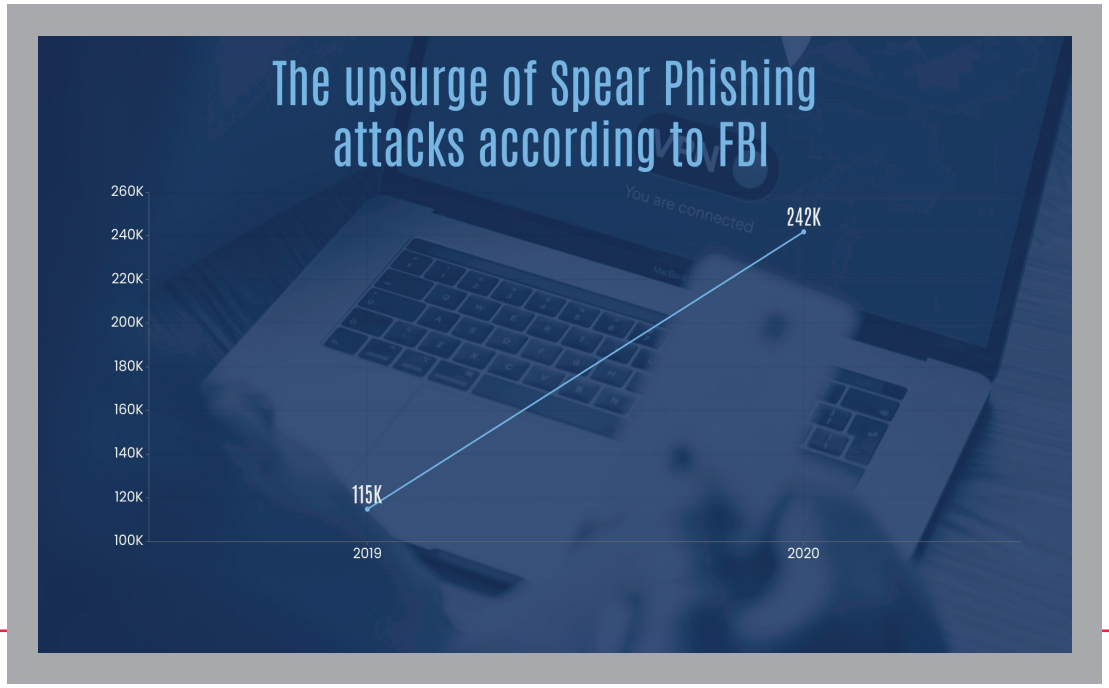


Quick heal endpoints had observed a massive surge in Phishing emails and covid-19 related phishing emails when the pandemic was at its peak in India during the second wave. The following graph shows the Phishing emails blocked by the Quick Heal endpoints.



More than 90% of Spear phishing attack payloads arrived by email, and few are carried out through malicious websites. It has been observed that attackers called or sent messages to the targets to land them on phishing websites.

According to the FBI report, phishing remained the most successful kind of cybercrime in the previous year. Phishing events nearly doubled in frequency in the USA from **114,702 incidents in 2019 to 241,324 incidents in 2020.**



So, the success of a spear-phishing campaign is based on:

- The so-called sender can pretend to be a trusted individual
- The data in the phishing email appears to be correct or something which the end-user is interested in
- The request may seem reasonable

Case Study 1: Email from IT department

An employee got a fake email from an attacker pretending to be from the Admin Desk of the IT department. This high-priority fake mail mentioned that employees would no longer be able to access their Email after 15th March 2021 as it will expire.

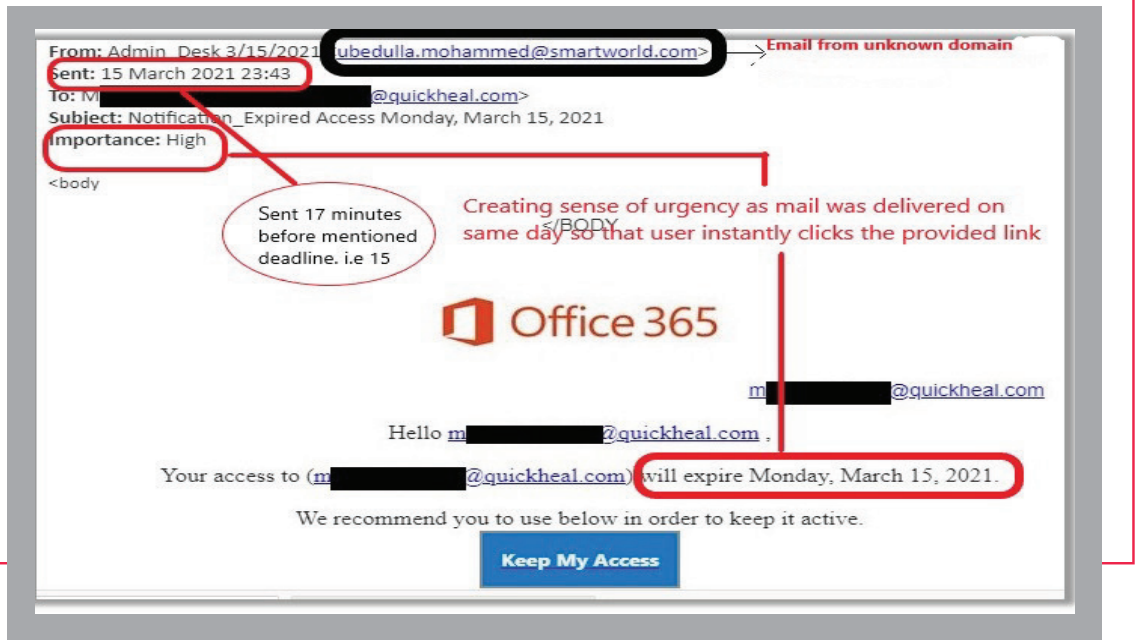


Fig-3 Example of Spear phishing EMAIL

The sender asks users to use the embedded link in "**Keep My Access**" to keep their email active. At first sight, this seems to be an email from a legitimate source, but in reality, if we check the sender's Email ID, this is a spear-phishing attack on the organization.

Analysis highlights:

1. The email is from a domain smartword.com that is unrelated to the Organization's Admin Desk.
2. The Email importance is set too high with eye catching subject and creates a sense of urgency to grab the user's attention to make mistakes in a hurry. A little time is given to a user to think and respond as the mail mentioned that the user would no longer be able to access the email after March 15, the only time of 17 Minutes. It creates a panic situation for a user.
3. When the user clicked the link and ended up compromising credentials by landing on the Fake Microsoft phishing page (hxxps://pixels-eg[.]com) and providing the gateway to scammers to enter into Organization.

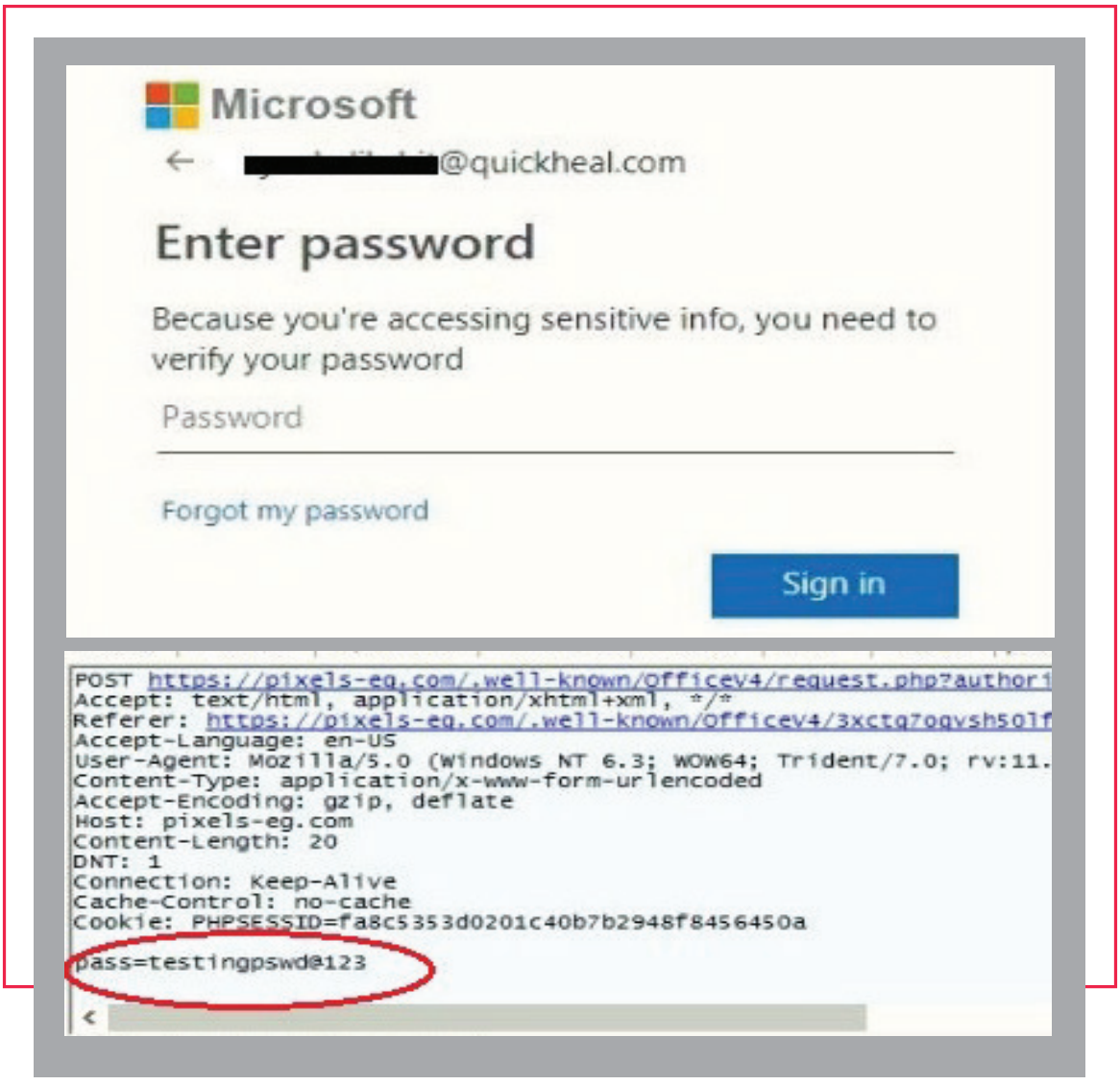
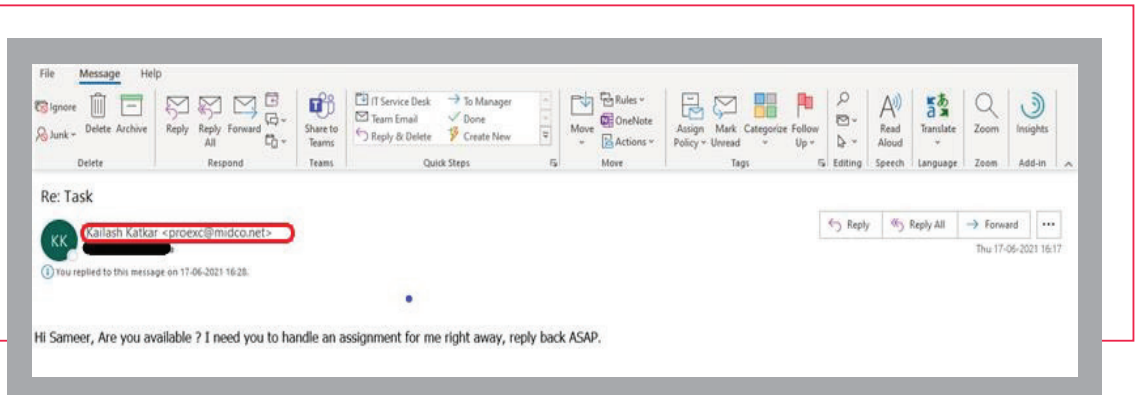


Fig-4 Analysis of Spear phishing EMAIL

Once the user submits the credentials on a fake look-alike mimic Microsoft page, the credential will be posted to a remote site managed by Attacker.

Case Study 2: CEO FRAUD

CEO Fraud is defined as a scam in which scammers spoof organization email accounts and represent a CEO



using spear-phishing to try to fool employees of a company (an employee in the finance or accounting department) by asking them to make unauthorized payments for the company, which later can be refunded to the employee.

Fig-5 Example of CEO fraud Spear phishing EMAIL

Here is some analysis:

1. The email is pretending to be from the CEO of the organization, asking for the availability of the employee to assign some assignment.
2. This mail is also from an unknown domain, i.e., Madco.net.
3. The above mail also seems suspicious as it landed in a junk mail folder.

After the employee replied to that mail scammers ask the employee to make a payment of INR 54000 and the money will be refunded as soon as possible.

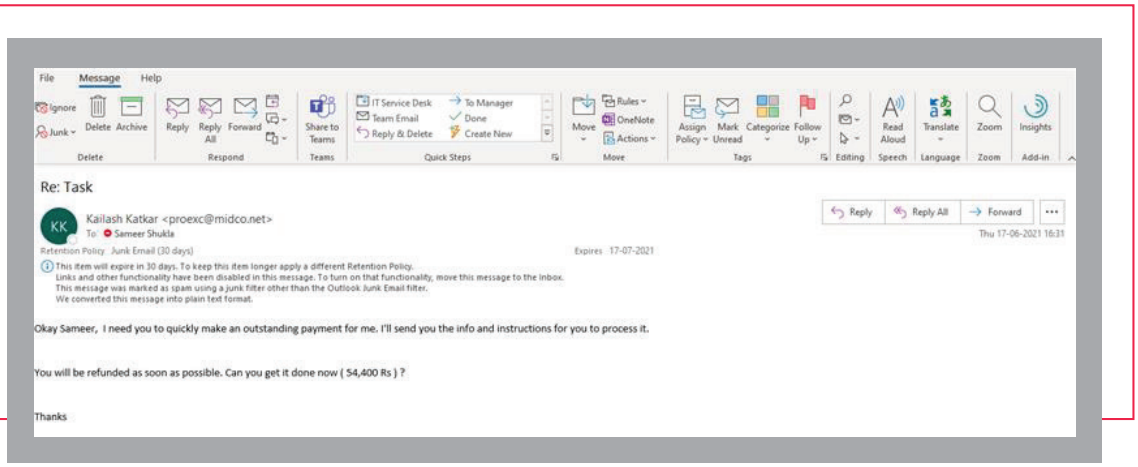


Fig-6 Example of CEO fraud Spear phishing EMAIL

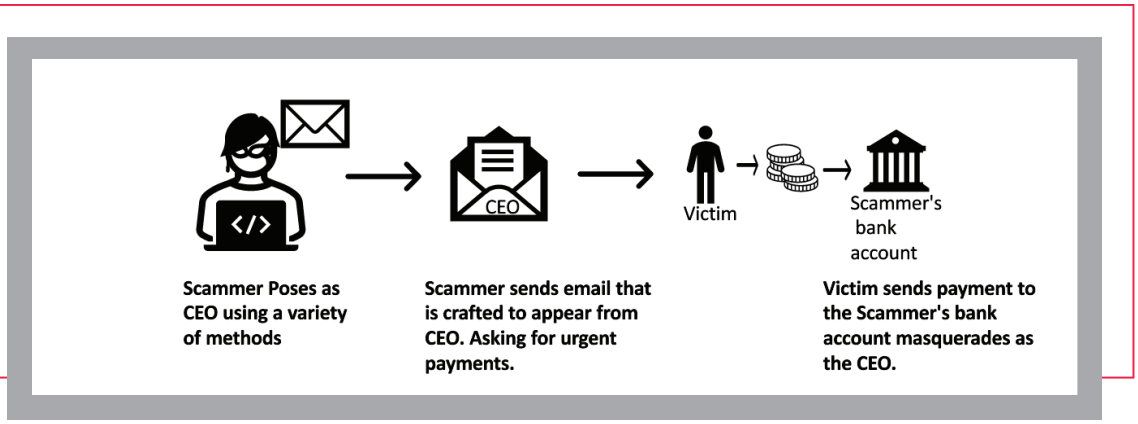


Fig-7 Flow of CEO fraud Spear phishing EMAIL

World-Wide case study

1. Anthem Medical Data Breach

In February 2015, USA-based Giant health insurance company, Anthem, Inc. revealed that scammers had broken into its servers and had initially stolen the Personal Identification Information (PII) data of more than 37.5 million people. Still, later, the stolen PII count increased to 78.8 million PII. The stolen data included PII containing name, Medical ID, DOB, Address, and social security number.

The attackers fetched PII data in compressed split archives and uploaded the compressed files to sell to Dark Web.

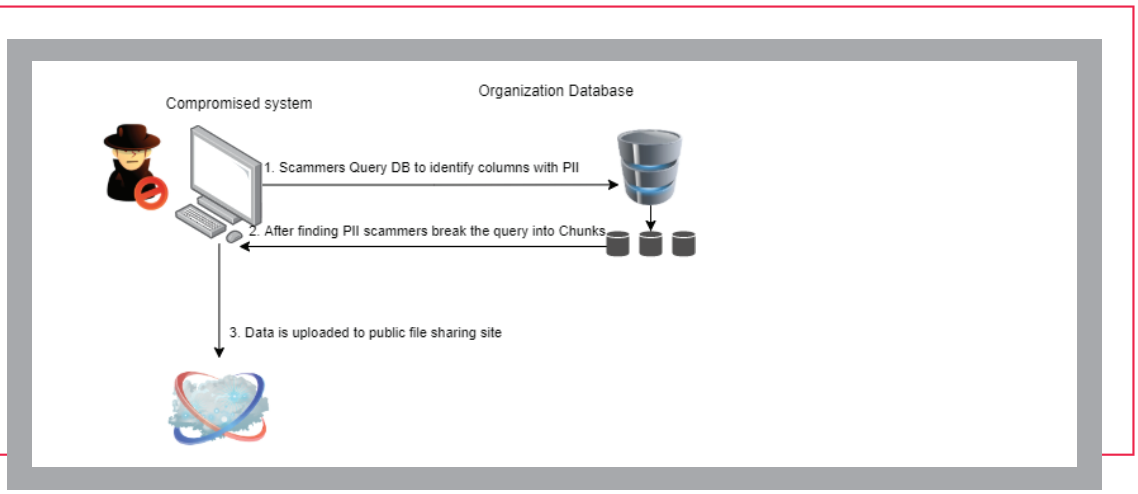


Fig-8 Flow of Anthem Medical Data Breach

Investigators suspected that Chinese government-affiliated groups had targeted employees of Anthem with pseudonyms such as “Deep Panda” and “Black Vine.”

Anthem faced numerous class actions. In 2017 class actions settlement cost Anthem $115 million. The

settlement document states that the company “has already incurred vital costs linked to the data breach. That includes $2.5 million to hire skillful experts, $115 million for implementing security developments, $31 million to provide initial notification to the public and affected individuals, and $112 million to provide credit protection to breach-impacted consumers. “Anthem has also agreed on additional safety improvements and other efforts to assist those affected by the breaches,” the document notes.

Analysis of attack

The research by the examination team and Anthem hired security firm Mandiant for a separate internal investigation, which concluded that the data breach started on 18th February 2014. Below are attacked chain highlights:

- The attackers started attacks by sending phishing emails linked to malicious fake websites to harvest credentials.
- A key employee's credentials were unintentionally compromised then the attacker tricked the employees into downloading and installing Malware in the victim's system.
- The Malware allowed attackers to obtain remote access to that computer and many other systems within the Anthem enterprise, including Anthem's data warehouse. The scammers were able to move alongside Anthem systems and increase privileges, getting more excellent ability to access data and make changes in Anthem's environment.
- The scammers used at least 50 accounts and compromised at least 90 systems within the Anthem network environment & data warehouse, a system where vast customers' PII is stored. Queries to that data resulted in a loss of approximately 78.8 million unique user personal records.

The investigation team found that Anthem had taken proper steps before the breach to guard its data and applied a remediation plan to respond to the breach once it was discovered effectively. The investigation team worked with Anthem to develop a plan to address their security vulnerabilities.

2. JP Morgan Chase and Co Data Breach

J.P. Morgan Chase & Co is one of the leading banks in the world with total assets of 3.39 lakh crores USD and the largest bank in the United States and the fourth-largest bank in the world in terms of total assets. The J.P. Morgan trademark is used by investment banking, asset management, treasury services, private wealth management, and divisions.

In 2014, one of the world's largest banks was the victim of a systematically planned cyberattack. The records of 76 million households and 7 million small businesses were compromised. A total of 83 million data containing Names, Addresses, Phone numbers, and Emails makes it one of the most significant data breaches in history.

The intrusion began on June-14 and continued until July-14. Reports of a suspected Data Breach surfaced in late August-14. According to security experts, the data breach was likely linked to a spear-phishing attack that had compromised one of the bank's employees.

Analysis of attack

- The attackers obtained a list of applications and programs used by the bank and created a plan to exploit vulnerabilities in the applications to enter the bank's systems. The Attackers used a zero-day vulnerability on one of the applications on J.P. Morgan's website, which is one of the characteristics of spear-phishing once the target is compromised.
- It is suspected that an employee probably fell to a spear-phishing attack and unintentionally clicked on the link with a malicious payload created by attackers sing social engineering techniques.
- It is reported that malware has infected an employee's personal computer, and from there, the scammers were able to advance further into the bank's network. Attackers broke through different complex security layers to breach the data and remove vast amounts of data.
- This data breach came into the spotlight just days after bank customers have faced a massive surge in phishing emails attempting to harvest banking credentials. Here victims were redirected to a fake login portal. The malware is created to look like a Java update after their username and password are entered into the form.

The scammers got high-level access into the bank's systems, but the bank could identify and prevent the scammers before they wiped customer accounts.

HOW TO **STAY SAFE** AGAINST SPEAR-PHISHING ATTACKS?

PHISHING AWARENESS & EDUCATION PROGRAMS

Organizations should conduct cyber security awareness and training programs to educate the employees on how to recognize phishing attacks, verify emails, and hover over Links, Messages and attachments before opening or clicking.

USE MULTI-FACTOR AUTHENTICATIONS

Multi-factor authentication (MFA) should be enforced for authentication activities to reduce the misuse of stolen credentials.

VERIFY THE SENDER DETAILS

Double-check the sender's identity using another communication platform to avoid any phishing trap.

AVOID SHARING PERSONAL DETAILS ON SOCIAL & NETWORKING SITES

To execute sophisticated attacks like Spear phishing attacks, Cybercriminals research to collect available information about targeted victims on social media & networking platforms that info used to spoof victims by maintaining legitimacy in attack techniques.

EFFECTIVE SECURITY SOLUTIONS

Deploy practical Real-time threat intelligence, online browser protection, email security, Anti Malware, firewall solutions, etc., to detect phishing attacks.

BE CAUTIOUS WHILE SHARING SENSITIVE INFORMATION

Always think and validate the links or websites before entering any credentials or financial details.

About **Quick Heal Security Labs** A leading source of threat research, threat intelligence, and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

References

- *https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/*
- *(https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)*
- *https://en.wikipedia.org/wiki/2014_JPMorgan_Chase_data_breach*
- *https://en.wikipedia.org/wiki/Anthem_medical_data_breach*
- *https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond*

Quick Heal Technologies Ltd.
Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune,
Maharashtra, India - 411014.
Phone: 1800 212 7377 | info@seqrite.com | www.seqrite.com