Threat Profile:
Credential Harvesting Attacks Using Spear-Phishing

May 1, 2020

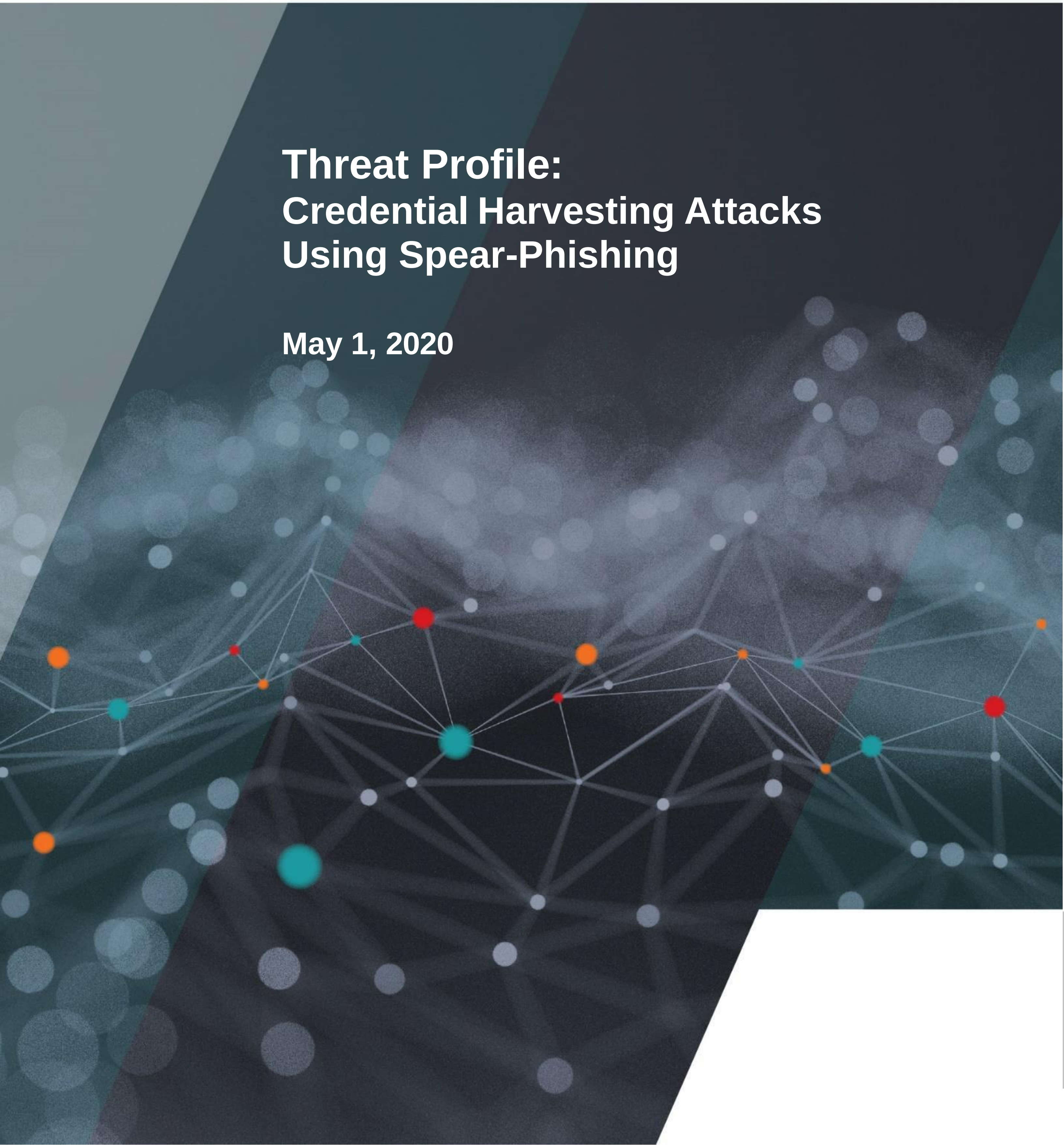


Table of Contents

1 EXECUTIVE SUMMARY

Credentials harvesting is a type of cyber-attack where the threat actors' goal is to steal the targeted users' credentials. The stolen credentials can then be sold by hackers on the dark web or used directly to commit fraud, identity theft and industrial espionage. Malicious hackers use several techniques to trick users to give away their access credentials. One technique that stands out is spear phishing.

According to the Verizon's 2019 Data Breach Investigation Report, email is the primary attack vector responsible for delivering around 90% of all cyber-attacks detected by the participants of the study, while 32% of the breaches involved phishing attacks and 29% involved stolen credentials.

The report also indicates that cyber-attacks are mostly financially motivated (71%) or aim at industrial espionage (25%).

While phishing attacks target a large group with the hope that one of them will bite the bait, spear phishing attacks are more focused, targeting a particular organization and/or specific individuals. Prior to launching spear phishing attacks, attackers typically dedicate significant time and resources to researching their targets. The objective is to identify high value targets and identify how to attract them with specially crafted and targeted emails or text messages that will lure them to malicious websites or convince them to open malicious attachments.

These malicious websites are usually crafted to mimic the look and feel of other websites that the targeted victim usually visits. The victim is presented with a login screen in which he/she inputs their login credentials, unknowingly handing them over on to the attackers.

In other instances, the emails contain attachments the contain malware specifically designed to gather login credentials and send them over to the attackers' command and control centers.

During the past few months, we have observed an increase in credential harvesting attacks targeting our clients using spear-phishing.

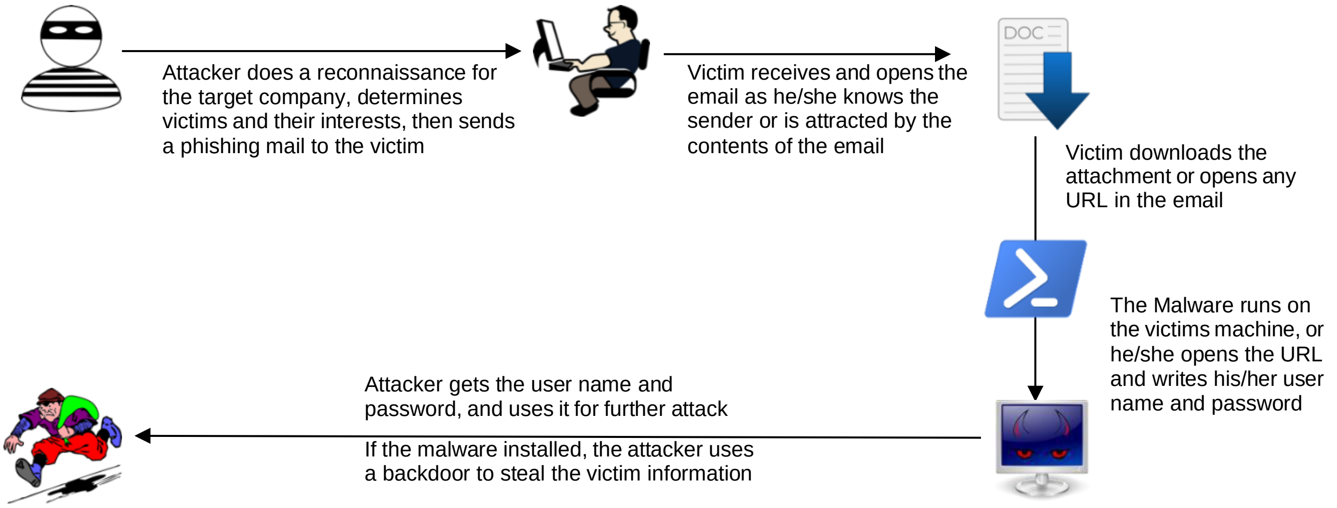
This report provides an analysis of the techniques used by attackers to craft spear phishing attacks to steal user credentials, and the most effective ways to detect them and prevent them.

2 ANATOMY OF A SPEAR PHISHING ATTACK

Whether to reuse stolen credentials to access information systems at later attack stages or to monetize them by selling combos on the darknet, threat actors, varying from script kiddies to state sponsored groups, tend to use spear phishing because of its effectiveness, low cost and because of the availability of professional phishing kits, and sophisticated malwares.

Spear phishing attacks have three major stages:

1. Researching the Target
2. Crafting the Message
3. Harvesting the Credentials



Attacker does a reconnaissance for the target company, determines victims and their interests, then sends a phishing mail to the victim

Victim receives and opens the email as he/she knows the sender or is attracted by the contents of the email

Victim downloads the attachment or opens any URL in the email

The Malware runs on the victims machine, or he/she opens the URL and writes his/her user name and password

Attacker gets the user name and password, and uses it for further attack

If the malware installed, the attacker uses a backdoor to steal the victim information

2.1 Phase 1 – Researching the Target

Spear-phishing is the act of sending a specially crafted scam email to a specific individual, organization, industry or users over an electronic communication channel. Although email is the primarily used channel, other channels like SMS and Instant Messaging are used as well. The key distinction between spear phishing and regular phishing is the amount of research involved that allows the attacker to pick a target and personalize a message specific to the intended recipient.

Attackers pick a target, whether that be an organization or an individual, and analyzes their online footprint to understand corporate structures, reporting lines, personal relationships and personal interests. Attackers analyze social media platforms such as LinkedIn, Facebook and Twitter to better understand their target and formulate a strategy of attack.

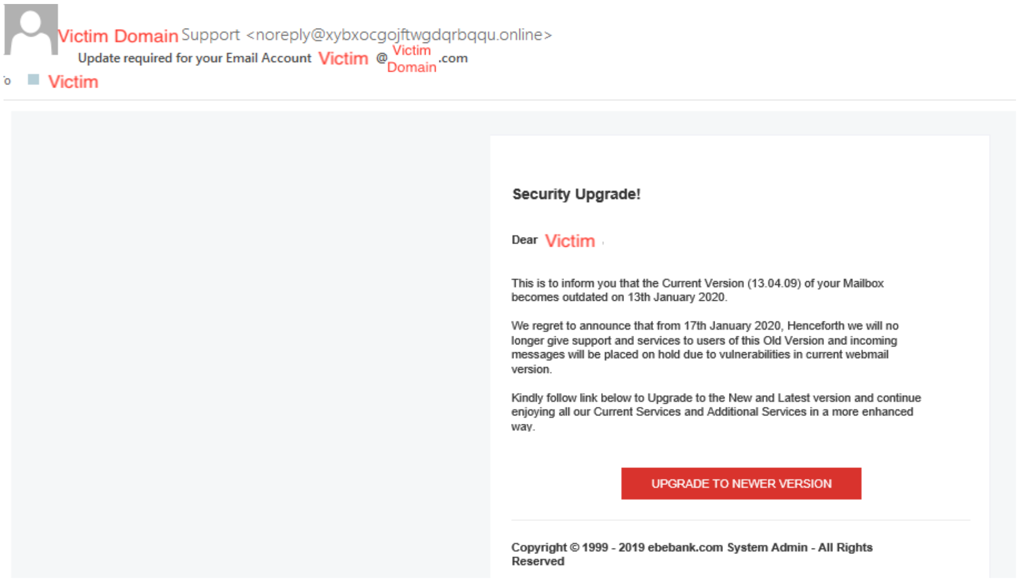
2.2 Phase 2 – Crafting the Message

Once a target is defined and profiled, the attackers start by personalizing a message to deliver over email, SMS or an Instant Messaging platform with content that they know will be of interest to the victim.

Attackers send phishing mails with clever tactics to get the victims attention with a subject and/or body email that is addressed to the recipient. Victims are prompted to open a malicious attachment and/or click on a link that takes them to a spoofed website where they are asked to provide passwords, account numbers, PINs, etc. This spoofed website is usually designed to mimic the look and feel of a website familiar to the victim.

Most recently, we have noticed a spike in phishing and spear phishing campaigns pretending to originate from the World Health Organization (WHO) asking people to open malicious attachments that they claim to contain important information about the Covid-19 pandemic.

The example below shows a classic hacker trick in which an email is sent to lure recipients to open a phishing URL by pretending to be the victim’s organization’s technical support. They’re asked to upgrade their Mailbox version in order to maintain access.



Victim Domain Support <noreply@xybxocgojftwgdqrbqqu.online>

Update required for your Email Account Victim @Victim Domain .com

o Victim

Security Upgrade!

Dear Victim ,

This is to inform you that the Current Version (13.04.09) of your Mailbox becomes outdated on 13th January 2020.

We regret to announce that from 17th January 2020, Henceforth we will no longer give support and services to users of this Old Version and incoming messages will be placed on hold due to vulnerabilities in current webmail version.

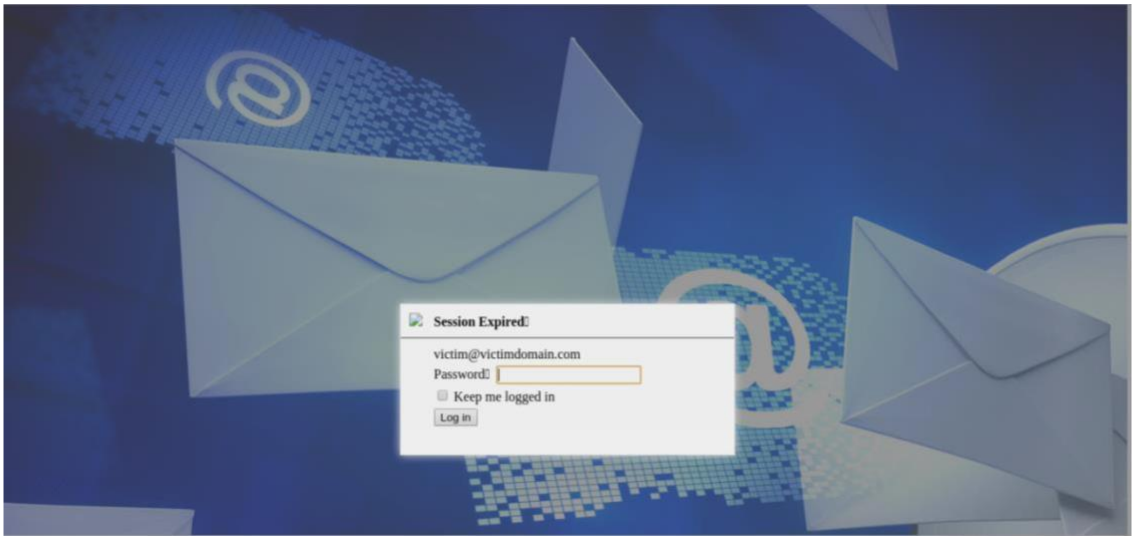
Kindly follow link below to Upgrade to the New and Latest version and continue enjoying all our Current Services and Additional Services in a more enhanced way.

Copyright © 1999 - 2019 ebebank.com System Admin - All Rights Reserved

2.3 Phase 3 – Harvesting the Credentials

The unsuspecting victim clicks the phishing URL and/or attachments, which directs them to a login page that seems it is a legitimate website, in an attempt to steal their credentials.

All that they need from them is a user name/email and password.



Session Expired

victim@victimdomain.com

Password:

□ Keep me logged in

3 MITIGATION

3.1 Preventive Controls

3.1.1 USING MULTI-FACTOR AUTHENTICATION

Multi-factor authentication relies on more factors than just the password to authenticate users. These factors include something you know (a password), something you have (a one-time password generating token) and something you are (fingerprint). By combining more than one factor, an organization adds a layer of protection by requesting additional proof of user identity.

While multi-factor authentication, does not prevent spear phishing, it nullifies its impact, because the stolen passwords can no longer be used on their own to compromise a user account or organizations.

3.1.2 PATCHING OF END USER PRODUCTIVITY TOOLS

By regularly patching end-user productivity tools such as MS-Office and Adobe Acrobat Reader, organizations can minimize the exposure to weaponized attachments that include malicious code exploits an unpatched vulnerability to cause damage.

3.1.3 DISABLING MACROS

A macro is a series of commands that a user can use to automate a repeated task. Attackers use macro documents to simulate attacks on the victim's machine. A macro virus uses a macro language such as VBScript as a means of propagating, so whenever possible disabling macros may prevent viruses from running.

3.1.4 USER AWARENESS

Users are the prime targets of spear phishing campaigns, hence any effective prevention must involve training users on how to spot spear phishing emails and messages when they receive them, and how to report them through the appropriate channels to the relevant incident response teams.

3.1.5 LEAST PRIVILEGE PRINCIPLE

Only the minimum necessary privileges should be assigned to a user that requests access to a resource, and should be in effect for the shortest duration necessary.

Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. Therefore, careful delegation of access rights can limit attackers from damaging a system

3.2 Detective Controls

3.2.1 EMAIL SECURITY

Email security is a set of measures used to secure an organization’s email service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts.

As a result of its ubiquity and inherent vulnerabilities, email is a popular vector for cyber-attacks including malware, spam, and phishing.

Well configured and updated email security may detect phishing mails that contain malicious attachments and/or malicious URLs or domains, and may even block it before it is received.

3.2.2 ANTIVIRUS

Antivirus software is designed to detect and destroy threats such as viruses, malware, ransomware and spyware.

It is mandatory that every organization adds this security layer in case of any malware attack that can affect its internal network. Regularly updated antivirus software may keep you safe from a malware/phishing attack when it happens.

In many cases, phishing mails contain malicious attachments that spread malware to the victims’ machine when clicked/downloaded. Well-configured and updated Antivirus may detect or even prevent this malware before running and being spread.

3.2.3. THREAT HUNTING FOR IOCS

The term “threat hunting” means being proactive and searching for any attack symptoms in your network, using indicators of compromise (IOC), which consist of IPs, hashes, URLs and domains.

If we can combine the above two factors we can detect the attack early, and mitigate it accordingly.

In section 4 (**DETECTION**) we will explain how we can use threat hunting and related IOCs to detect such attacks.

3.3 Reactive Controls

3.3.1 QUICKLY CHANGING PASSWORDS

Organizations must develop detailed incident response procedures that involve the resetting of the passwords of the users who have received spear phishing emails or might have clicked on the links they contain.

The effective implementation of this incident response procedure requires educating the users on how to report spear phishing emails and having the means to identify other users who might have received the malicious email and interacted with it in any way.

4 DETECTION

- Monitor URL requests that contain *@[yourdomain]* in URL Path AND target Domain Name does not contain [*yourdomain*].
- Monitor Web requests that > first seen, newly registered and DGA domains.
- Monitor received emails from > first seen and newly registered domains.
- Monitor for suspicious authentication activity on published services > from unexpected Geo-Locations.
- Gathering more IOCs related to latest spear phishing attacks and try to block it at your different security controls like (Firewall, proxy, email security, Antivirus, etc...), as well as monitor its activities, below at section 5 (**INDICATORS OF COMPROMISE**) will help you to get more information for such IOCs.

5 REFERENCES

- https://www.us-cert.gov/ncas/alerts/TA18-201A
- https://attack.mitre.org/techniques/T1193/
- https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- https://exchange.xforce.ibmcloud.com/
- https://www.phishlabs.com/covid-19-threat-intelligence/
- https://www.pivotpointsecurity.com/blog/credential-harvesting-more-than-password-phishing/
- https://enterprise.verizon.com/resources/reports/dbir