

Forum:[Hack Forums](#)

Thread: [Question: What's BEC & How to become BEC successful Phisher and Earn Huge Bag](#)

hakme_xsscat - July 17, 2024, 5:46 pm

Hello HF's Member's Good day..

I am a skilled IT Technician and Ethical Grey hat Hacker. I used to be a member of sky-fraud.ru and an IRC hacking group. My expertise includes web hacking, hardware networking, password cracking, and professional social engineering attacks like BEC, Bank, CC: spear phishing, Pretexting, Baiting, Tailgating, and Scareware. I have been a Linux administrator since 2009 and have knowledge of scripting languages like bash, Python, and Perl. I have also learned HTML, CSS, and JavaScript to enhance my hacking and IT security skills as a penetration tester. Although I am not an elite JavaScript programmer, I strive to improve. To learn more and currently learning Golang.

<!--!-----!>

Here is my first thread Tutorial for HF's member's

What's BEC?

Business email compromise (BEC) is another scam that relies heavily on social engineering techniques. In a BEC attack, a scammer impersonates a trusted company executive, civil engineering contractor or third-party vendor's to initiate financial invoice transfers to an account they own. This can be done from office365 mailbox or any business emails like GoDaddy, Alibaba cloud business webmail, ETC.

For example, they may pretend to be a security vendor updating your cloud business emails instructions. The hacker would send a detailed email from an address that appears legitimate to the person within the organization who typically makes payments in mailbox. If the recipient of the email follows the instructions, the money they send will end up in the scammer's bank account. I won't go into detail here, as there are threads on BEC from the (Microsoft security team that you can read to gain a deeper understanding of how BEC works). Some members are looking to profit from BEC, as BEC spammers can make more money than bank or credit card spammers. However, BEC spamming requires a lot of time, patience, and knowledge to successfully cash out. You'll need to monitor the hacked BEC logs in your mailbox for several days or weeks. Once you see an invoice payment initiated in your mailbox logs, you'll need to create a clone email address ID. I personally used a Proton Plus account to set up my hosting webmail for the clone mailbox address ID with Office365. I then configured email forwarding in the victim's mailbox settings. It's important to be cautious with your activities in the victim's mailbox, as any suspicious behavior could prompt them to change their passwords. (Here is a recently screenshot of a BEC Office365 hacked log mailbox.) Is good to understand Social engineering cyber attacks can involve baiting, spear phishing, pretexting, and more.

WHAT DO I NEED TO BE SUCESSFUL BEC SPAMMER?

Here is the things you need to be successful spammer and got results.

1- Your brain

2- Dedicated time

3- Patience needed: because you might fail first spamming attempt do not allow any spammer fool you that you will get bulks results in their first setup for you as beginner. many companies this days has security Intelligence that guide them before they proceed any activities in their mailbox.

Here: is basic Tools You needs.

?????Fresh Html Letter coded + scan code qr with obfuscator.

?????Html Attachment offline login file.html example(offline html attachment proof)

?????You need strong obfuscator system (To OBF your html,js,css against window antivirus system and Microsoft outlook-0365-protection to avoid warning victim downloading file.html as phishing harmful file.)

?????Quality leads validated with debounce checker mailbox

?????Google cloud free account (To make perfect inbox link bypass against spam-filter or smtp isp bot filtering).

?????Open redirect url handling can be found on awstrack. or (use GitHub tool to find open redirect url to hide your link)

?????Office365 Validator Script 90% or 99% real userid valid.

?????Bulletproof VPS to make your hosting panel. Never use hacked shell or hacked cpanel. i dont use them or make your choice??.

?????Smart-Link(API-BOT) fake host machine blocker, web root blocker, bot url visitor blocker. to manage your url this good because you can replace ban domain from spamhaus. without make new spamming and continue getting more results. never use antibot.pw they are useless.

?????Mailer Script that support spoof. like Python MSS or node.js MSS

?????CDN-DNS to backend your domain and vps IP. check my thread here how to setup host with CDN-DNS(####)

?????Spam words checker use this tool>(spam-words-checker)

?????Subject encoded user this tool>(Subject Encoded)

?????Email-AI writer also good, it help use this tool>(Email-AI-free tool)

?????Trusted Anonymous DNS provider's (custom domain is cool, but setup subdomain from management)

?????You can also spam box to box: if you have hacked office365 log with good contacts to do box to box spamming with your phishing attachment offline file.html. you need outlook extention tool for this aspect with your brain. however i can't post details about this here due to security researchers on forum.

<!-----!>

Here is free new tutorial video.2024 how to spam inbox and setup mailer for both sms and email spamming

(video email inbox [ask me])

(video sms[ask me])

<!-----!>

some spammer don't really know their enemies when they are about spamming office-365 BEC. let me list your enemies for you.

??Outlook protection spf record scan

??Outlook protection IP address scan

??Outlook protection blacklisted check scan

??Outlook protection safelink scan

??Outlook protection spam filtering scan

??Outlook protection smtp server scan (Microsoft security didn't support any smtp sender with mail.shffhr.com?)

Once you grasp the Microsoft security rules and have a basic understanding of how email delivery works, you won't encounter any issues with your inbox. However, if you neglect email security rules, you might compromise your setup and your SMTP. Some people have a good SMTP but lack the necessary knowledge, leading to failure and blaming the seller of their tools. Sometimes, even with a good SMTP, using the wrong words and having a blacklist setup can trigger security alerts, as Microsoft Outlook will detect you as a spammer and send a return email to your SMTP server, triggering spamhaus security.

To stay safe: Make sure to check out this thread to learn how to safeguard your organization from cybercriminals using tactics like baiting, spear phishing, pretexting, and more.

Big thanks you to all HF's member's happy phishing and hacking...!

Problind - August 19, 2024, 1:32 pm

(Jul 17, 2024 05:46 PM)hakme_xsscat Wrote: [\[CITE\]](#) Hello HF's Member's Good day..

I am a skilled IT Technician and Ethical Grey hat Hacker. I used to be a member of sky-fraud.ru and an IRC hacking group. My expertise includes web hacking, hardware networking, password cracking, and professional social engineering attacks like BEC, Bank, CC: spear phishing, Pretexting, Baiting, Tailgating, and Scareware. I have been a Linux administrator since 2009 and have knowledge of scripting languages like bash, Python, and Perl. I have also learned HTML, CSS, and JavaScript to enhance my hacking and IT security skills as a penetration tester. Although I am not an elite JavaScript programmer, I strive to improve. To learn more and currently learning Golang.

[b]<!--[/b]-----!>

Here is my first thread Tutorial for HF's member's

What's BEC?

Business email compromise (BEC) is another scam that relies heavily on social engineering techniques. In a BEC attack, a scammer impersonates a trusted company executive, civil engineering contractor or third-party vendor's to initiate financial invoice transfers to an account they own. This can be done from office365 mailbox or any business emails like GoDaddy, Alibaba cloud business webmail, ETC.

For example, they may pretend to be a security vendor updating your cloud business emails instructions. The hacker would send a detailed email from an address that appears legitimate to the person within the organization who typically makes payments in mailbox. If the recipient of the email follows the instructions, the money they send will end up in the scammer's bank account. I won't go into detail here, as there are threads on BEC from the (Microsoft security team that you can read to gain a deeper understanding of how BEC works). Some members are looking to profit from BEC, as BEC spammers can make more money than bank or credit card spammers. However, BEC spamming requires a lot of time, patience, and knowledge to successfully cash out. You'll need to monitor the hacked BEC logs in your mailbox for several days or weeks. Once you see an invoice payment initiated in your mailbox logs, you'll need to create a clone email address ID. I personally

used a Proton Plus account to set up my hosting webmail for the clone mailbox address ID with Office365. I then configured email forwarding in the victim's mailbox settings. It's important to be cautious with your activities in the victim's mailbox, as any suspicious behavior could prompt them to change their passwords. (Here is a recently screenshot of a BEC Office365 hacked log mailbox.) Is good to understand Social engineering cyber attacks can involve baiting, spear phishing, pretexting, and more.

WHAT DO I NEED TO BE SUCESSFUL BEC SPAMMER?

Here is the things you need to be successful spammer and got results.

- 1- Your brain
- 2- Dedicated time
- 3- Patience needed: because you might fail first spamming attempt do not allow any spammer fool you that you will get bulks results in their first setup for you as beginner. many companies this days has security Intelligence that guide them before they proceed any activities in their mailbox.

Here: is basic Tools You needs.

?????Fresh Html Letter coded + scan code qr with obfuscator.

?????Html Attachment offline login file.html example(offline html attachment proof)

?????You need strong obfuscator system (To OBF your html,js,css against window antivirus system and Microsoft outlook-0365-protection to avoid warning victim downloading file.html as phishing harmful file.)

?????Quality leads validated with debounce checker mailbox

?????Google cloud free account (To make perfect inbox link bypass against spam-filter or smtp isp bot filtering).

?????Open redirect url handling can be found on awstrack. or (use GitHub tool to find open redirect url to hide your link)

?????Office365 Validator Script 90% or 99% real userid valid.

?????Bulletproof VPS to make your hosting panel. Never use hacked shell or hacked cpanel. i dont use them or make your choice??.

?????Smart-Link(API-BOT) fake host machine blocker, web root blocker, bot url visitor blocker. to manage your url this good because you can replace ban domain from spamhaus. without make new spamming and continue getting more results. never use antibot.pw they are useless.

?????Mailer Script that support spoof. like Python MSS or node.js MSS

?????CDN-DNS to backend your domain and vps IP. check my thread here how to setup host with CDN-DNS(####)

?????Spam words checker use this tool>(spam-words-checker)

?????Subject encoded user this tool>(Subject Encoded)

?????Email-AI writer also good, it help use this tool>(Email-AI-free tool)

?????Trusted Anonymous DNS provider's (custom domain is cool, but setup subdomain from management)

?????You can also spam box to box: if you have hacked office365 log with good contacts to do box to box spamming with your phishing attachment offline file.html. you need outlook extention tool for this aspect with your brain. however i can't post details about this here due to security researchers on forum.

[b]<!--[/b]-----!>

Here is free new tutorial video.2024 how to spam inbox and setup mailer for both sms and email spamming

(video email inbox [ask me])

(video sms[ask me])

[b]<!--[b]-----!>

some spammer don't really know their enemies when they are about spamming office-365 BEC. let me list your enemies for you.

??Outlook protection spf record scan

??Outlook protection IP address scan

??Outlook protection blacklisted check scan

??Outlook protection safelink scan

??Outlook protection spam filtering scan

??Outlook protection smtp server scan (Microsoft security didn't support any smtp sender with mail.shffhr.com?)

Once you grasp the Microsoft security rules and have a basic understanding of how email delivery works, you won't encounter any issues with your inbox. However, if you neglect email security rules, you might compromise your setup and your SMTP. Some people have a good SMTP but lack the necessary knowledge, leading to failure and blaming the seller of their tools. Sometimes, even with a good SMTP, using the wrong words and having a blacklist setup can trigger security alerts, as Microsoft Outlook will detect you as a spammer and send a return email to your SMTP server, triggering spamhaus security.

To stay safe: Make sure to check out this thread to learn how to safeguard your organization from cybercriminals using tactics like baiting, spear phishing, pretexting, and more.

Big thanks you to all HF's member's happy phishing and hacking...!This is a quite solid post , what's your tg or dcord. For a follow up

Y2J_007 - October 14, 2025, 1:20 pm

Top tier....any follow up platform?