

Cheap'n'Easy Phishing Against Mature Organization (That actually works)

Phishing Pas Cher et Facile contre
une organisation mature (Ca
fonctionne vraiment)

JON GAINES

SO WHO ARE YOU



ANYWAY????

- ▶ Jon Gaines
- ▶ ~8 Years as an Offensive Security Consultant; >14 for fun
- ▶ Senior Security Consultant by Day; Run GainSec by Night
- ▶ 20 CVEs, a single expired cert, BS + AS in Cyber, Speaker/Lecturer, Published articles
- ▶ Love Blackbox Externals, Web App, Red Teams and OSINT
- ▶ Perform all the * pen tests (minus K8s, GCP, Azure)
- ▶ HATE phishing campaigns (vishing is ok)

SO WHO ARE YOU



ANYWAY????

- ▶ Jon Gaines
- ▶ ~8 ans comme Consultant en cybersécurité offensive; >14 ans pour le fun
- ▶ cybersécurité offensive (senior) la journée; dirige GainSec la nuit
- ▶ 20 CVEs, une seule certification expirée, Deux diplômes de la université en cyber, Orateur, Articles publiés
- ▶ Aime Blackbox Externes, applications Web, Red Team et OSINT
- ▶ Soccupe de toutes les sortes de test de penetration (sauf K8s, GCP, Azure)
- ▶ DETESTE les campagnes de phishing (vishing est ok)

TF is Phishing?

- ▶ " Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving information to criminals that they shouldn't have access to. In a phishing scam, you might receive an email that appears to be from a legitimate business and is asking you to update or verify your personal information by replying to the email or visiting a website. The web address might look similar to one you've used before. The email may be convincing enough to get you to take the action requested." – FBI - [Source](#)
- ▶ It's how every 17-year-old gets into your organization (looking at you Uber)
- ▶ C'est comment chaque adolescent de 17 ans rentre dans votre organisation (Uber)

Possible Targets

Important Monetary Distinctions

- ▶ \leq \$10 Million
- ▶ Fortune 500
- ▶ Fortune 300
- ▶ Fortune 10

Important Type Distinctions

- ▶ Financial
- ▶ Healthcare
- ▶ Software Development
- ▶ Gov't

Cibles Possibles

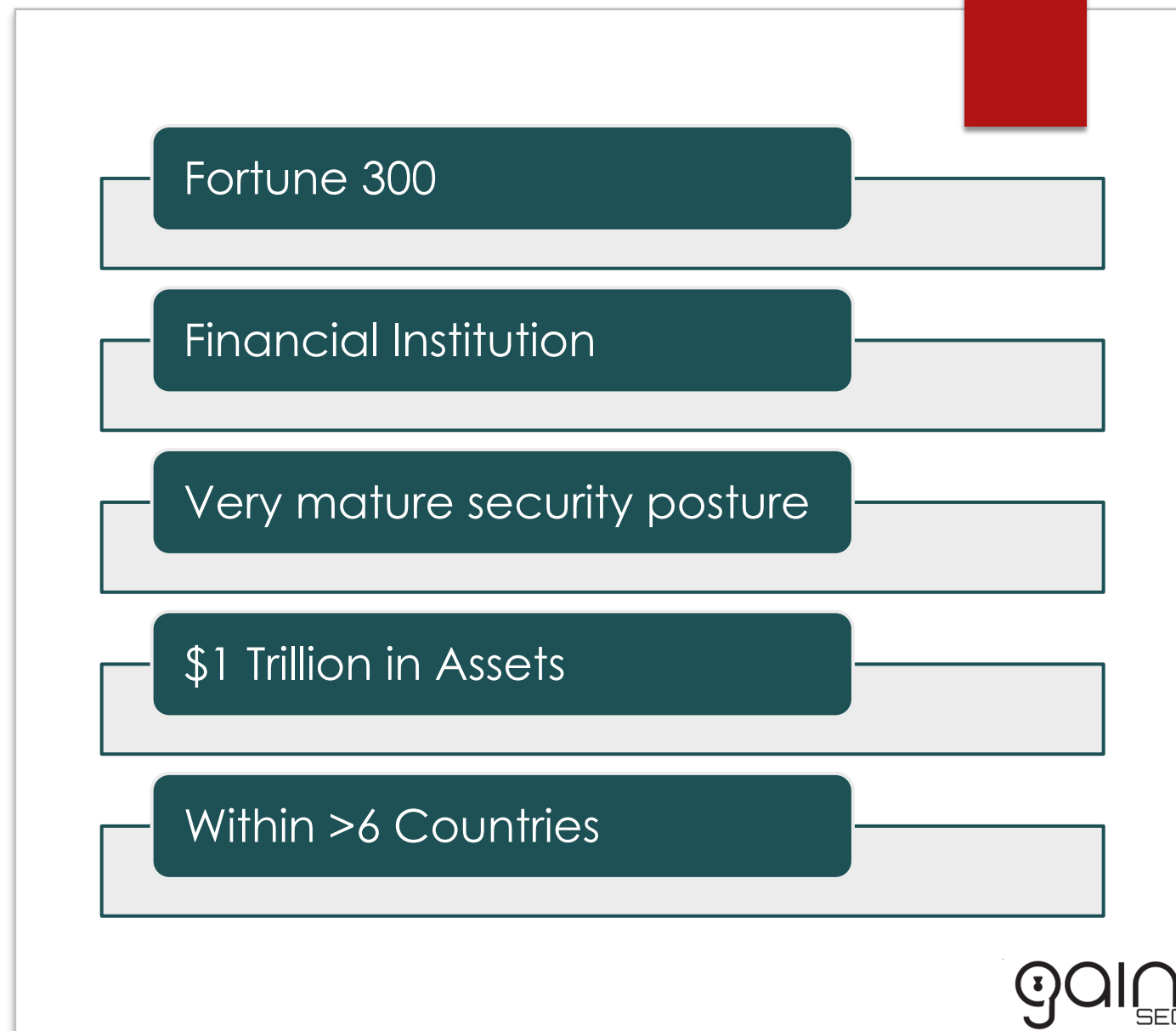
Distinctions Monetaires Importantes

- ▶ \leq \$10 Millions
- ▶ Fortune 500
- ▶ Fortune 300
- ▶ Fortune 10

Types de Distinctions Importantes

- ▶ Finance
- ▶ Sante
- ▶ Développement de logiciel
- ▶ Gouvernement

Our Target



Notre Cible

Fortune 300

Institution Financiere

Securite Tres Efficace

\$1 Trillion en Actifs

Dans plus de 6 pays

Goals – Phishing Campaigns apart of a Red Team

- ▶ Harvest User/Pass/2FA/Session Cookies
- ▶ Collect a list of possible targets for spear-phishing
- ▶ Have the employees execute a C2 stager, giving us control of one(or multiple) assets (boxes or computers) that the organization owns. → Gain persistence → STOP
- ▶ Find holes in their email filtering

Objectifs - Campagne de Phishing faisant partie de une Red Team

- ▶ Remplir Nom de utilisateur/Mot de passe/2FA(code securite)/Session Cookie
- ▶ Collecter une liste de cibles possibles pour le Spear-phishing
- ▶ Piéger les employes pour qu'ils ouvrent un C2 stager, nous donnant acces a leurs ordinateurs → Gain persistence → STOP
- ▶ Find holes in their email filtering
- ▶ Trouver des failles dans la filtration d' e-mail

OSINT OSINT OSINT

- ▶ Discovering a list of emails
- ▶ Discovering a list of used 3rd party services
- ▶ Determining other "mainstream" 3rd party services that are acceptable

What that actually means:

- ▶ Phonebook.cz, Infoga, RocketMail, Search Engine Dorking, Data Breaches/Leaks
- ▶ Search Engine Dorking, Manual Testing, Data Breaches/Leaks
- ▶ Experience...

OSINT OSINT OSINT

- ▶ Découvrir une liste d' e-mail
- ▶ Découvrir une liste d' utilisation de services tiers
- ▶ Découvrir une liste de services tiers
<<mainstream>>

Ce que cela veut vraiment dire:

- ▶ Phonebook.cz, Infoga, RocketMail, Search Engine Dorking, Data Breaches/Leaks
- ▶ Search Engine Dorking, Test Manuel, Data Breaches/Leaks
- ▶ Experience...

info@journal-officiel.gouv.fr
jean-marc.franc@intradef.gouv.fr
lionel.khimeche@dga.defense.gouv.fr
jose.ruiz@dga.defense.gouv.fr
dominique.berthet@dga.defense.gouv.fr
courrier.fae-sai@diplomatie.gouv.fr
entraide-civile-internationale@justice.gouv.fr
xavier.leprete@education.gouv.fr
clement.lazarus@sante.gouv.fr
jacques.sauret@sante.gouv.fr
patrick.tyburn@martinique.pref.gouv.fr
denis.lopez@martinique.pref.gouv.fr
philippe.sarron@interieur.gouv.fr
frederique.martini@developpement-durable.gouv.fr
helene.sekutowicz@diplomatie.gouv.fr
bernard.frontero@diplomatie.gouv.fr
elie.jarmache@pm.gouv.fr
rene.feunteun@ecologie.gouv.fr
pierre.tribon@agriculture.gouv.fr
jerome.sautier@diplomatic.gouv.fr
nicolas.gorodetska@agriculture.gouv.fr
infomusee.archivesnationales@culture.gouv.fr
jean-baptiste.auzel@culture.gouv.fr
anom.aix@culture.gouv.fr
corsen.mrcc@equipement.gouv.fr
ministere@developpement-durable.gouv.fr
contact.cgeiet@finances.gouv.fr
anissa.belgacem@interieur.gouv.fr
thibaud.kurtz@diplomatie.gouv.fr
jean.carsignol@equipement.gouv.fr
guy.desire@equipement.gouv.fr
thierry.kretz@developpement-durable.gouv.fr
joel.raoul@developpement-durable.gouv.fr

Emails

Emails 2



inbody:"@gouv.fr" filetype:docx

[https://s3.amazonaws.com › khudes › embennell2](https://s3.amazonaws.com/khudes/embennell2) DOC ⋮

ifg (hong kong) limited - Amazon S3

dana.purcarescu@diplomatie.gouv.fr, Pete Sepp <pressguy@ntu.org>, ... SEE IMPORTANT ATTACHMENTS LOTS OF INFO IN BODY OF E-MAIL This effects each and ...

3rd Party Services (Services Tiers)

inurl:yvelines -gouv.fr -yrvelines.fr

<https://yvelines.us5.list-manage.com> › ... · [Translate this page](#) ⋮

78-92.fr

Les Présidents et les élus des Départements des Yvelines et des Hauts-de-Seine ont engagé une réflexion commune sur le devenir de leur territoire et de ...



3rd Party Services 2 Services Tiers 2

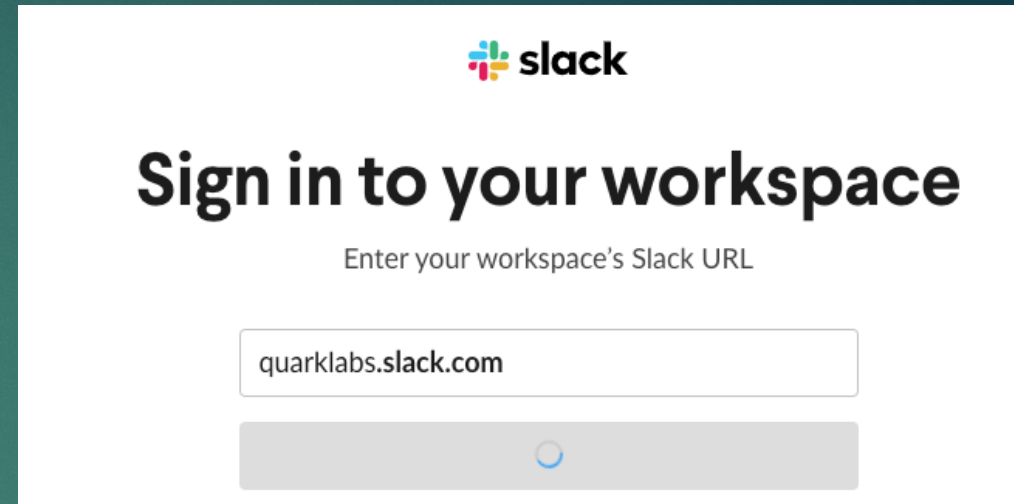
- ▶ Remember to include Links!
- ▶ Se rappeler d'inclure les liens!

Technology/Service	Description	Source/Too
Eightfold.ai	AI Talent Management	SearchDNS
REDACTED.de	Employee Benefits	Google
Betterteam.com	Job Listings	Google
YouConnect	Appraisers	Google
cumul	Customer Analytics	Google
Learn.Com	Employee Training?	Google
Smarsh Socialite	Compliance and Engagement?	Google
Global Meet - MyConference	Conference Meetings	Google
		Google
		Google
Adobe Connect	?	Google
Voya	Record Keeping	Google
Swoogo	Event Management Platform	Google
SupplierGateway	Suppliers Platform	Google
Taleo	Job Listings	Google
SurveyMonkey	Surveys	Google
GitHub	Code	SwissCows
		SwissCows
		SwissCows
cvent	Event RSVP/Register	SwissCows
Invision	Workflow	Netlas
		Netlas
		Netlas
		Netlas
		Netlas
Cumul	Customer Analytics API	Netlas
Security Compass	Threat modeling	Netlas
		Netlas
Demdex	Adobe	

Mainstream 3rd Party Services 3

- ▶ With experience comes insight...
- ▶ Avec l'expérience vient la connaissance...

- ▶ DocuSign
- ▶ ShareDrive
- ▶ Slack
- ▶ WebEx
- ▶ Confluence
- ▶ Etc



The image shows a Slack login page. At the top is the Slack logo. Below it is the heading "Sign in to your workspace". Underneath is the instruction "Enter your workspace's Slack URL". There is a text input field containing "quarklabs.slack.com". Below the input field is a grey button with a blue circular loading spinner.

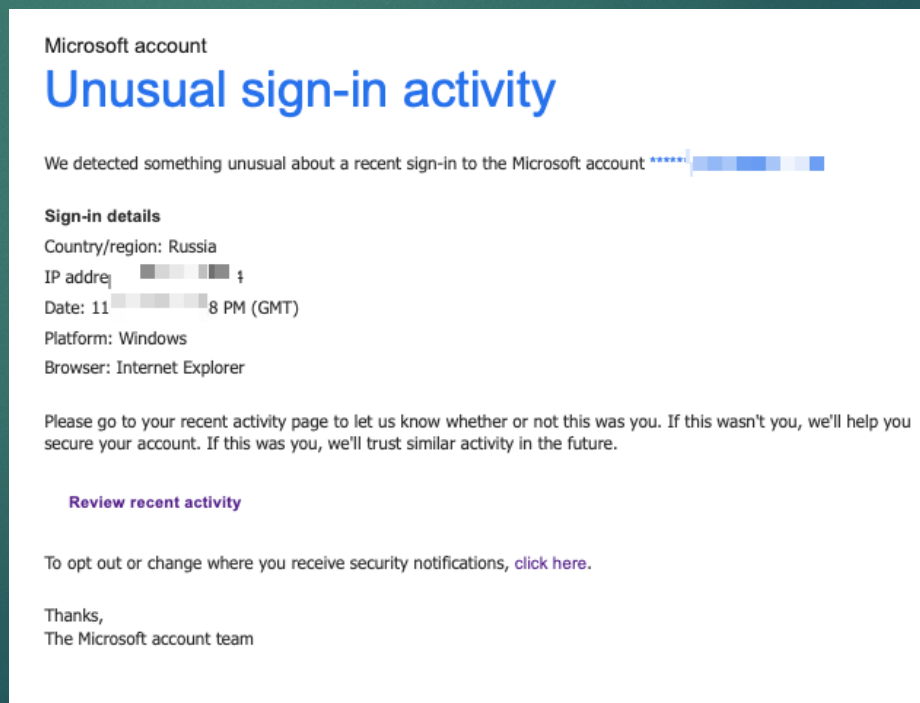


User/Pass/Session Harvest

Total \$ Spent: \$10*

*Per Domain

- ▶ Evilnginx2 is GREAT for this!
- ▶ Leveraging Outlook based off their DNS records (TXT Record)
- ▶ Quick Recorded demo!

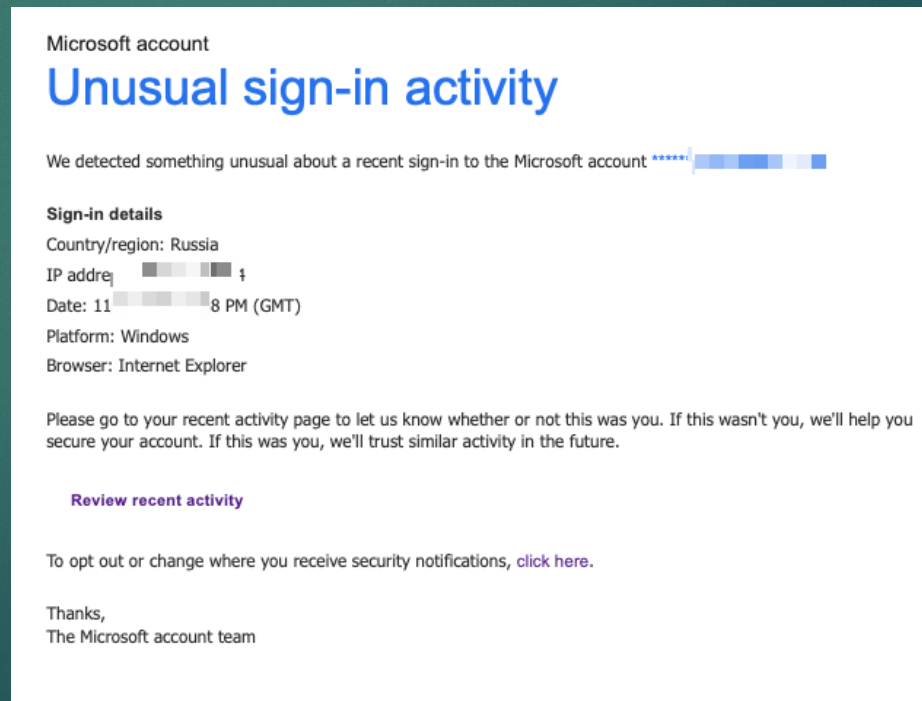


Remplir Nom de utilisateur/Mot de passe/2FA(code securite)/Session

Total \$ Depense: \$10*

*Par Domaine

- ▶ Evilnginx2 est SUPER pour ca!
- ▶ Utiliser Outlook base sur leur DNS records (TXT Record)
- ▶ Rapide demo video!



Spear-Phishing Harvest

Total \$ Spent: \$ 70

SurveyMonkey

Surveys

Google

Remote Work Employee Feedback

This MANDATORY survey is being used for our leaders to gain insight to their employees perspective about working remotely. If your position is approved you will receive further communication about when this switch will occur.

1. Are you able to complete the tasks assigned to you from a remote working environment?

- ☐ Yes
- ☐ No
- ☐ Not Sure

6. What is your first and last name?

7. What is your job title?

8. What is your email address?

9. What is your work phone number?

Done

Spear-Phishing Remplissage

Total \$ Depense : \$ 70

SurveyMonkey

Surveys

Google

Remote Work Employee Feedback

This MANDATORY survey is being used for our leaders to gain insight to their employees perspective about working remotely. If your position is approved you will receive further communication about when this switch will occur.

1. Are you able to complete the tasks assigned to you from a remote working environment?

- ☐ Yes
- ☐ No
- ☐ Not Sure

6. What is your first and last name?

7. What is your job title?

8. What is your email address?

9. What is your work phone number?

Done

Mainstream 3rd Party Services

Mainstream Services Tier

Total \$ Spent: \$ 130
Total \$ Depense : \$ 130

EMERGENCY PASSWORD CHANGE FORM

You have received this form due to an imminent threat
against your account.

It is important to act quickly.

Please fill out the following information

Current Password:

New Password:

Name:

Signature:

Date:

Time:

You should receive a confirmation follow-up call within one
hour from the IT team.

If you do not receive this follow-up or have any questions or
concerns, please email info@nvisium.com or call
888-888-8888

C2 Stager Execution

Total \$ Spent: \$ 140

*Per Domain

The hardest

Use what is easiest;
You cannot use
MailChimp +
GoPhish, they will
filter

O365 FTW

One Month free trial!
(Allows custom
domains + aliases!

Use what you
already have

AWS s3 Bucket (12
hours temporary
access w/ specific
URL)

Open Source/Latest
Greatest/Ear to the
Tracks > Cobalt Strike
(Without a dev team
or specialization)

C2 Stager Execution

Total \$ Depense: \$ 140

*Par Domaine

Le plus difficile

Utilise le plus facile;
Tu ne peux pas
utiliser MailChamp +
GoPhish; ils filtreront

O365 fonctionne

Un mois d'essai
gratuit! (Permet
domaines + aliases
personnalisés)!

Utilise ce que tu as
déjà

AWS s3 Bucket (12
heures d'accès
temporaire avec un
URL spécifique)

Open Source/Le
nouveau/Le mieux
> Cobalt Strike (sans
une équipe de
développement)

C2 Stager Execution 2

Total \$ Spent: \$ 140
Total \$ Depense: \$ 140

*Per Domain
*Par Domaine

Deployments made easy with Linode's One-Click App Marketplace

Hello,

Are you looking for a faster, simpler way to deploy? Check out [Linode's One-Click App Marketplace](#), where you can choose from dozens of popular applications like WordPress, OpenVPN and cPanel.

The [Linode](#) Marketplace makes it easy to get your project started without having to jump right into the command line. Simply [choose your app](#), customize it, and run it the way you want.

Ready to get started? Learn how to quickly deploy new services from our apps with our guide, "[How to Use Linode's One-Click Apps](#)". For help with specific apps like Minecraft, Plesk, Gitlab and more, [check out this section of our docs](#).

Lastly, are you looking for an app that you don't see in our Marketplace? We're always looking for new ones to add. Let us know what you'd like to see next by emailing us at feedback@linode.com.

Sincerely,
The [Linode](#) team

Copyright © 2022 [Linode](#), LLC, 249 Arch Street, Philadelphia, PA, 19106. All rights reserved.
855-4-[LINODE](#) (855-454-6633) Intl.: +1 609-380-7100 [Email us](#)

You have received this email because you indicated that you'd like to receive updates and tips about your [Linode](#) account. To unsubscribe or change your email preferences: [Subscription Center](#)

[Support](#) | [Community](#) | [Product Docs](#) | [Guides](#)

Enterprise Password Shield Installation

Password Shield

To: J



Password Shield© Installation

Your employer has recently subscribed to Password Shield©!

Our software protects your computer in real time by ensuring your passwords are never saved insecurely. We also monitor any data breaches and data leaks and will notify you if your password is compromised!

There is only one step you need to take to start your protection!

Please install the software using the attached file.

If for some reason the file is not appearing you can download a new installer [HERE](#).

















Sincerely,
Password Shield Customer Success Team

[Quoted text hidden]

C2 Stager Execution 3

Total \$ Spent: \$ 140

*Per Domain

	27c11522		r		Windows 10	Pass...Shield...	3624	x64	
	4d3a280a		r		Windows 10	Pass...Shield...	3624	x64	
	53adcdec		r		Windows 10	Pass...Shield...	3624	x64	
	1998541e		or		Windows 10	Pass...Shield...	3828	x64	

Lessons Learned

Total \$ Spent: \$ 140

*Per Domain

3rd Party Services are KING

Newly registered domains will be flagged

Leverage legit services in anyway possible

Don't go crazy

LOGS (AWS Cloudtrail, o365 Message Trace, Apache/HTTP Logs)

Warstories

A Retenir

Total \$ Depense: \$ 140

*Par Domaine

Services Tiers sont ROIS

Nouveaux domaines enregistres seront signales

Utilise des services tiers legaux des que possible

Reste raisonnable

LOGS (AWS Cloudtrail, o365 Message Trace, Apache/HTTP Logs)

Warstories