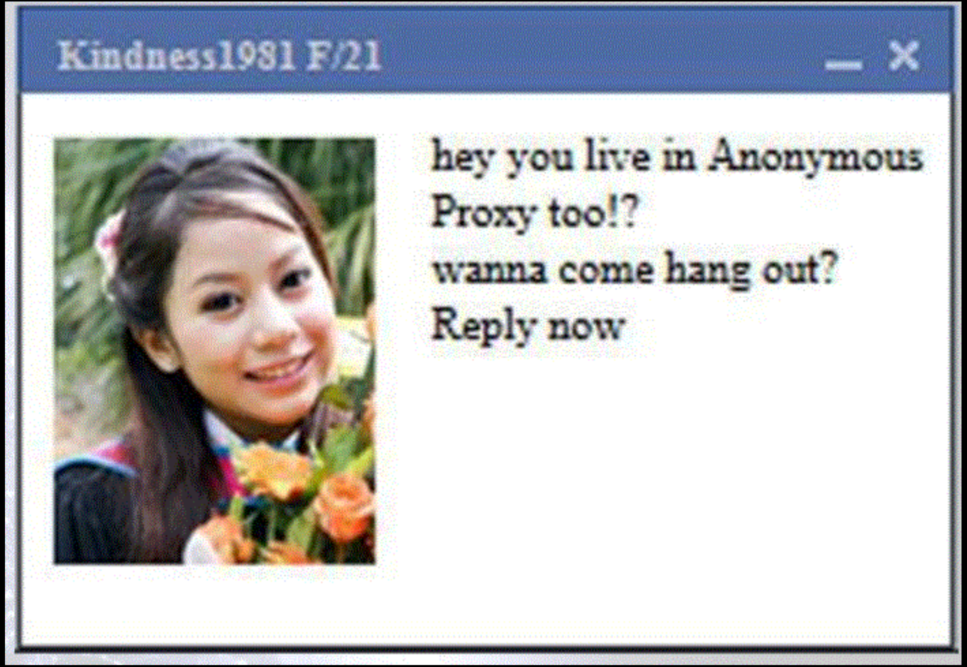
Dissecting Advanced Initial Access Techniques - Spear Phishing

Josu Barrientos
@bulw4rk
29/10/2021

About Me

- Josu Barrientos (@bulw4rk)
  - Head of Offensive Security @ ITS by Ibermatica
  - Telecomunication Engineer
  - Enjoy writing stuff that bypasses others’ stuff
  - Paid for writing reports



hey you live in Anonymous Proxy too!?
wanna come hang out?
Reply now

Notes

- Much misinformation about its execution and real complexity (much more than Gophish)

- Advanced technical and procedural content (not entry level)

- Short in time, so won’t go deep

- All the content focuses on full-fledge Red Team Engagements (Adv. Sim/Emul)

Spear Phishing

Introduction

Introduction

- A targeted e-mail based phishing: Individuals, or dept./company/industry level.
- One of the main Initial Access Techniques in mature environments during Adversary Simulation/Emulation engagements.
- IDd T1566 in MITRE ATT&CK.
- Targeting both people (Social Engineering) and security technologies in place.

Introduction | Types

- T1566.001: Spear Phishing Attachment.
    - E.g. Office Macros

- T1566.002: Spearphishing Link
    - E.g. Credential Harvesting

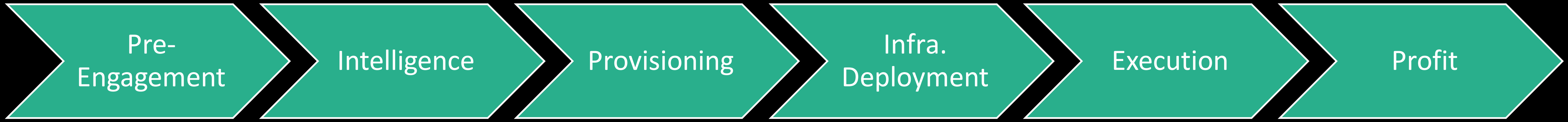
- T1566.003: Spearphishing via Service
    - E.g. Links on LinkedIn

Introduction | What do we face?

- User awareness

- Security Product Deployment:
  - Email Security GW
  - Web Proxies
  - FWs
  - AVs
  - EDRs
  - SIEM/SOC
  - Etc.

Introduction | Methodology



Pre-Engagement

Intelligence

Provisioning

Infra. Deployment

Execution

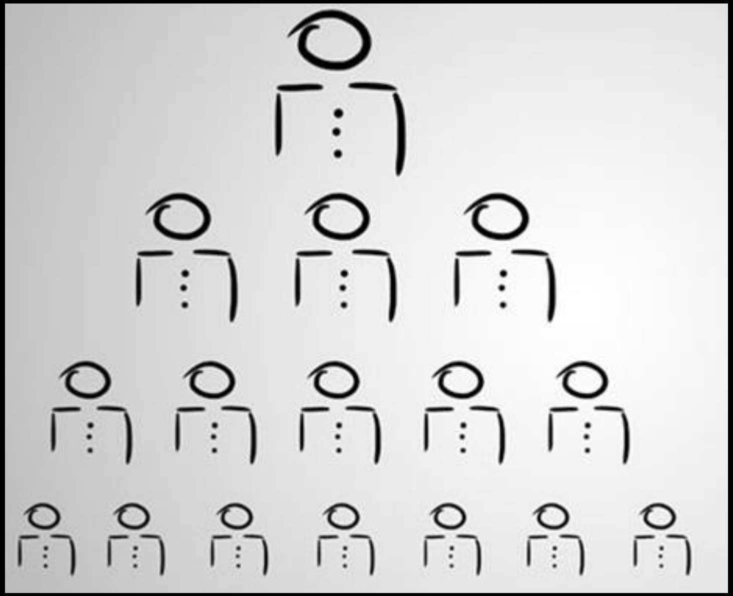
Profit

Spear Phishing

Intelligence

Intelligence | Org. Recon

- Necessary to create good pretexts, we are looking for:
  - Group/Company Structure
  - Sector
  - Physical Locations
  - Competitors
  - Third parties / providers
  - News



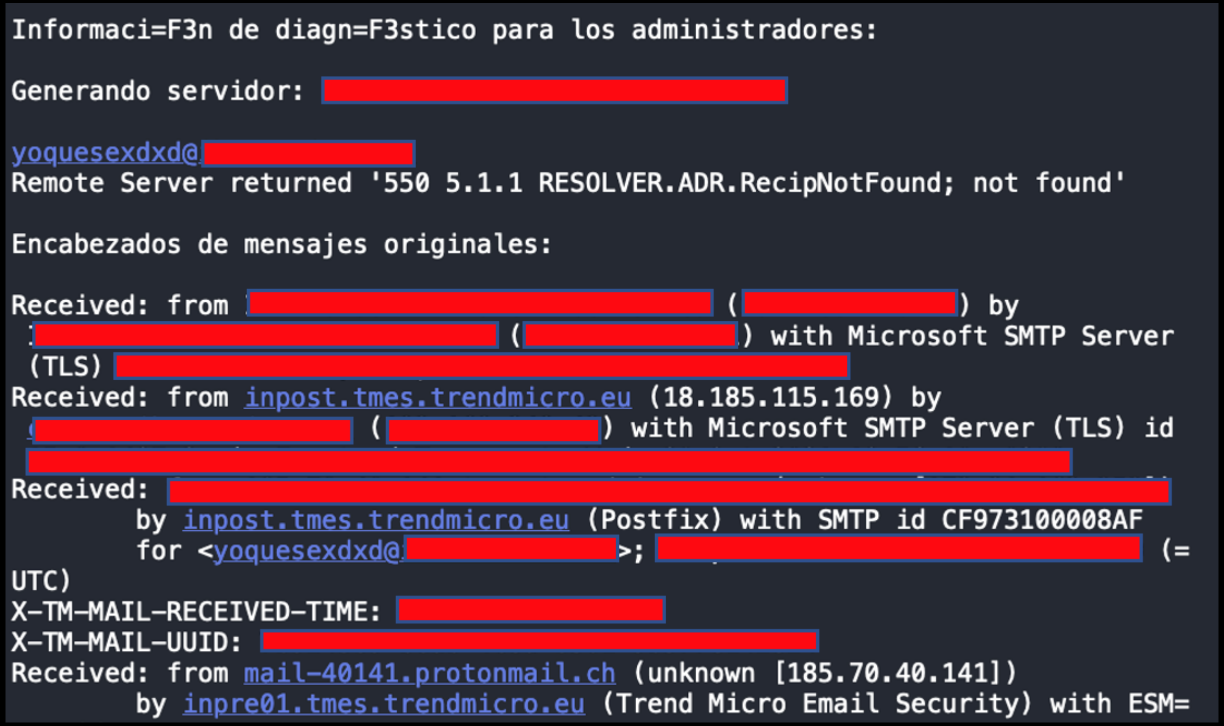
Intelligence | Users & Roles

- Employee information:
  - Name & Surname
  - Job/Department
  - E-mail addresses

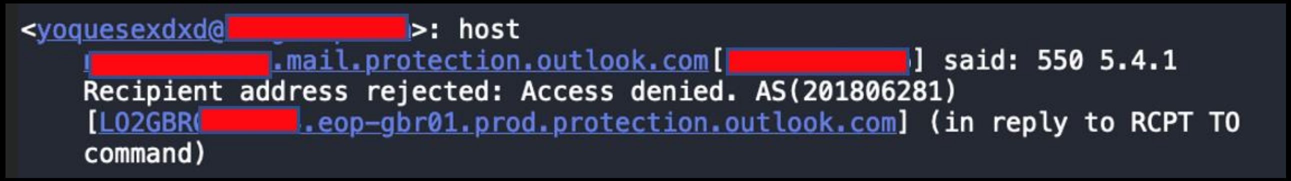
- Sources/Tools:
  - Browser/Web page
  - LinkedIn
  - Pastebins
  - Credential Dumps
  - Etc.

Intelligence | Security Products (I)

- Security products in place to be bypassed:
  - **Anti-Spam 🡐**
  - Web Proxies
  - FWs
  - DNS Resolvers
  - AV/EDR
  - SIEM



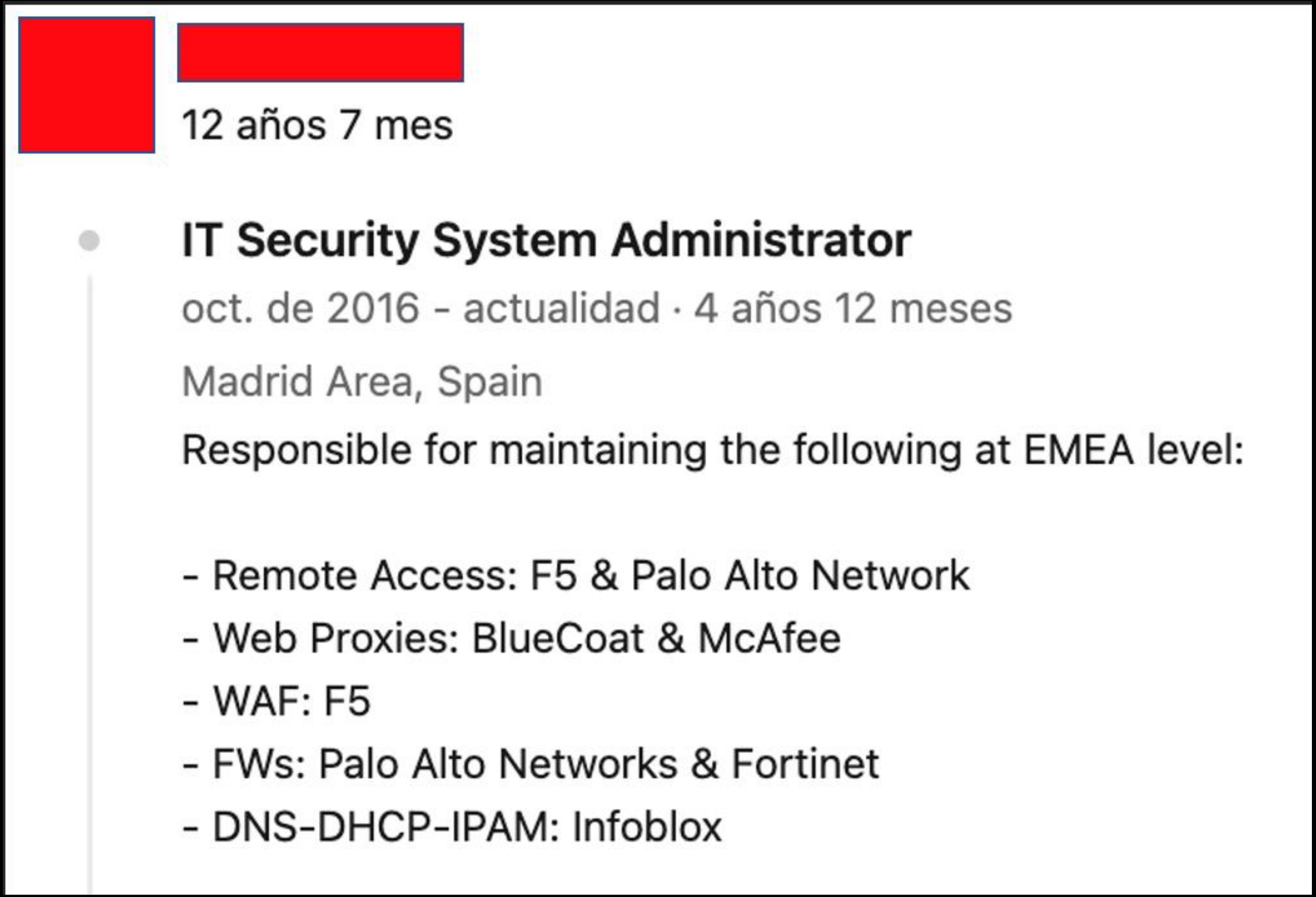
```
Informaci=F3n de diagn=F3stico para los administradores:

Generando servidor: [redacted]

yoquesexdxd@[redacted]
Remote Server returned '550 5.1.1 RESOLVER.ADR.RecipNotFound; not found'

Encabezados de mensajes originales:

Received: from [redacted] ([redacted]) by
 [redacted] ([redacted]) with Microsoft SMTP Server
 (TLS) [redacted]
Received: from inpost.tmes.trendmicro.eu (18.185.115.169) by
 [redacted] ([redacted]) with Microsoft SMTP Server (TLS) id
 [redacted]
Received: [redacted]
        by inpost.tmes.trendmicro.eu (Postfix) with SMTP id CF973100008AF
        for <yoquesexdxd@[redacted]>; [redacted] (=
UTC)
X-TM-MAIL-RECEIVED-TIME: [redacted]
X-TM-MAIL-UUID: [redacted]
Received: from mail-40141.protonmail.ch (unknown [185.70.40.141])
        by inpre01.tmes.trendmicro.eu (Trend Micro Email Security) with ESM=
```



```
<yoquesexdxd@[redacted]>: host
    [redacted].mail.protection.outlook.com[[redacted]] said: 550 5.4.1
    Recipient address rejected: Access denied. AS(201806281)
    [LO2GBR[redacted].eop-gbr01.prod.protection.outlook.com] (in reply to RCPT TO
    command)
```

Intelligence | Security Products (II)

- Security products in place to be bypassed:
  - Anti-Spam
  - **Web Proxies ←**
  - **FWs ←**
  - **DNS Resolvers ←**
  - AV/EDR
  - SIEM



[redacted] [redacted]

12 años 7 mes

IT Security System Administrator

oct. de 2016 - actualidad · 4 años 12 meses

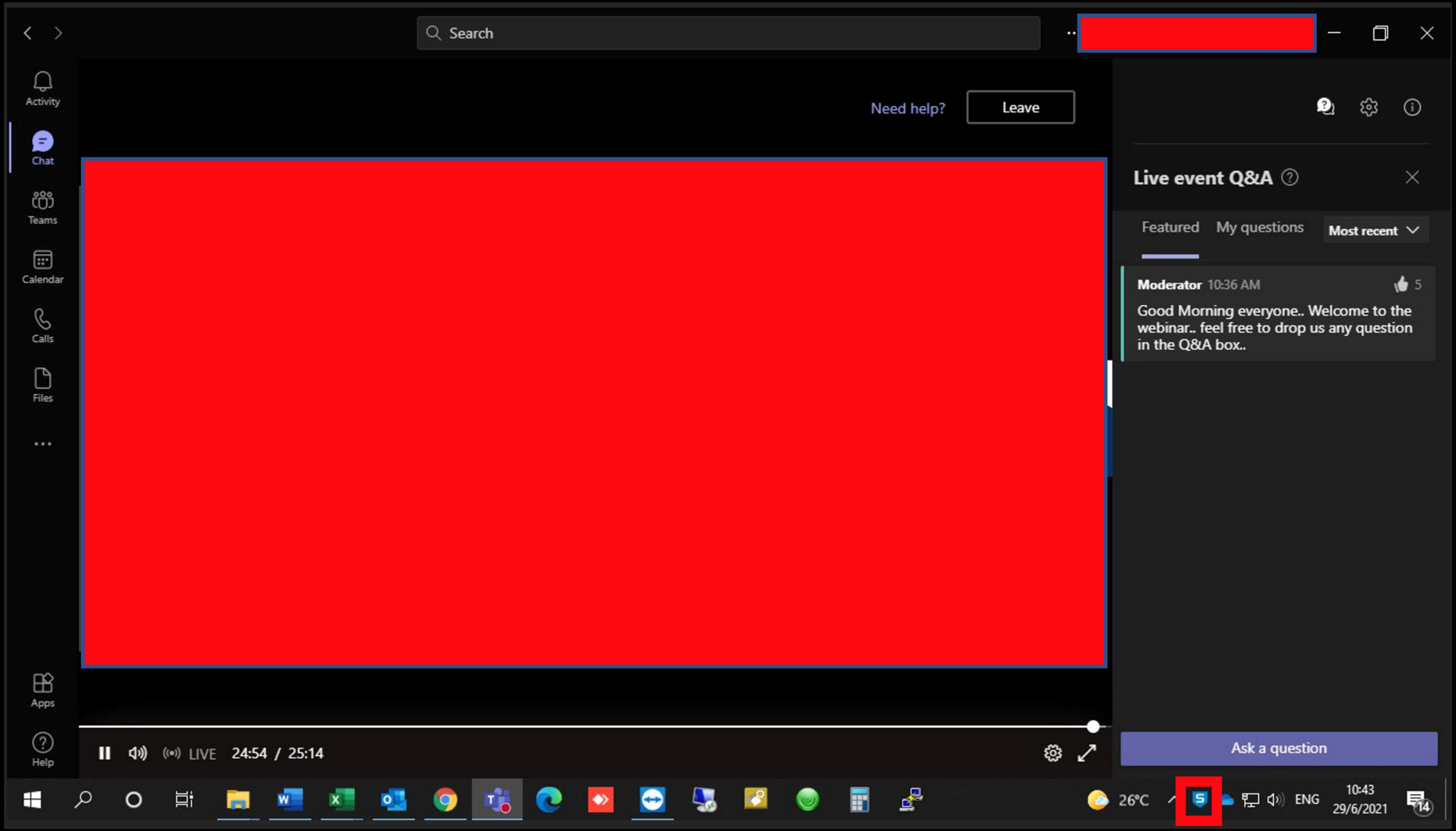
Madrid Area, Spain

Responsible for maintaining the following at EMEA level:

- Remote Access: F5 & Palo Alto Network
- Web Proxies: BlueCoat & McAfee
- WAF: F5
- FWs: Palo Alto Networks & Fortinet
- DNS-DHCP-IPAM: Infoblox

Intelligence | Security Products (III)

- Security products in place to be bypassed:
  - Anti-Spam
  - Web Proxies
  - FWs
  - DNS Resolvers
  - **AV/EDR ←**
  - SIEM



[redacted]

[redacted]

Live event Q&A

Moderator 10:36 AM

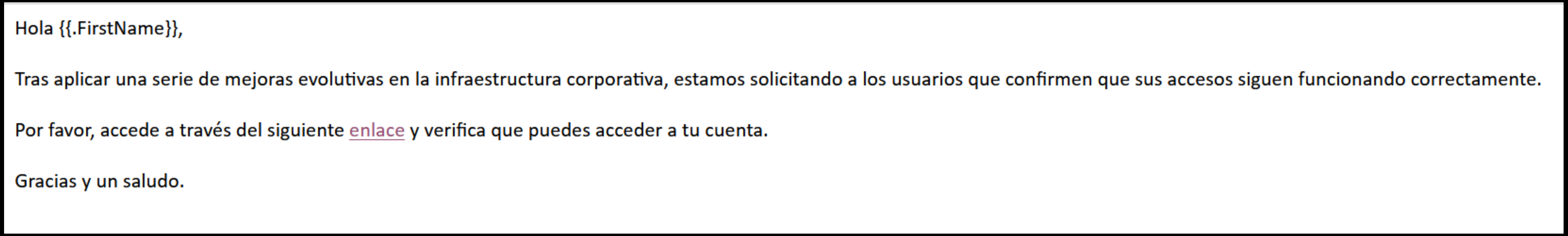
Good Morning everyone.. Welcome to the webinar.. feel free to drop us any question in the Q&A box..

From some guy on twitter

Intelligence | Pretexting

- Time to create the pretext and lures for the Spear Phishing:
  - Topic
  - Keep it simple and clean
  - Target individuals or small groups, distributed in different locations &/OR time zone

  - FROM: sistemas.<empresa>@<domain>



Hola {{.FirstName}},

Tras aplicar una serie de mejoras evolutivas en la infraestructura corporativa, estamos solicitando a los usuarios que confirmen que sus accesos siguen funcionando correctamente.

Por favor, accede a través del siguiente enlace y verifica que puedes acceder a tu cuenta.

Gracias y un saludo.

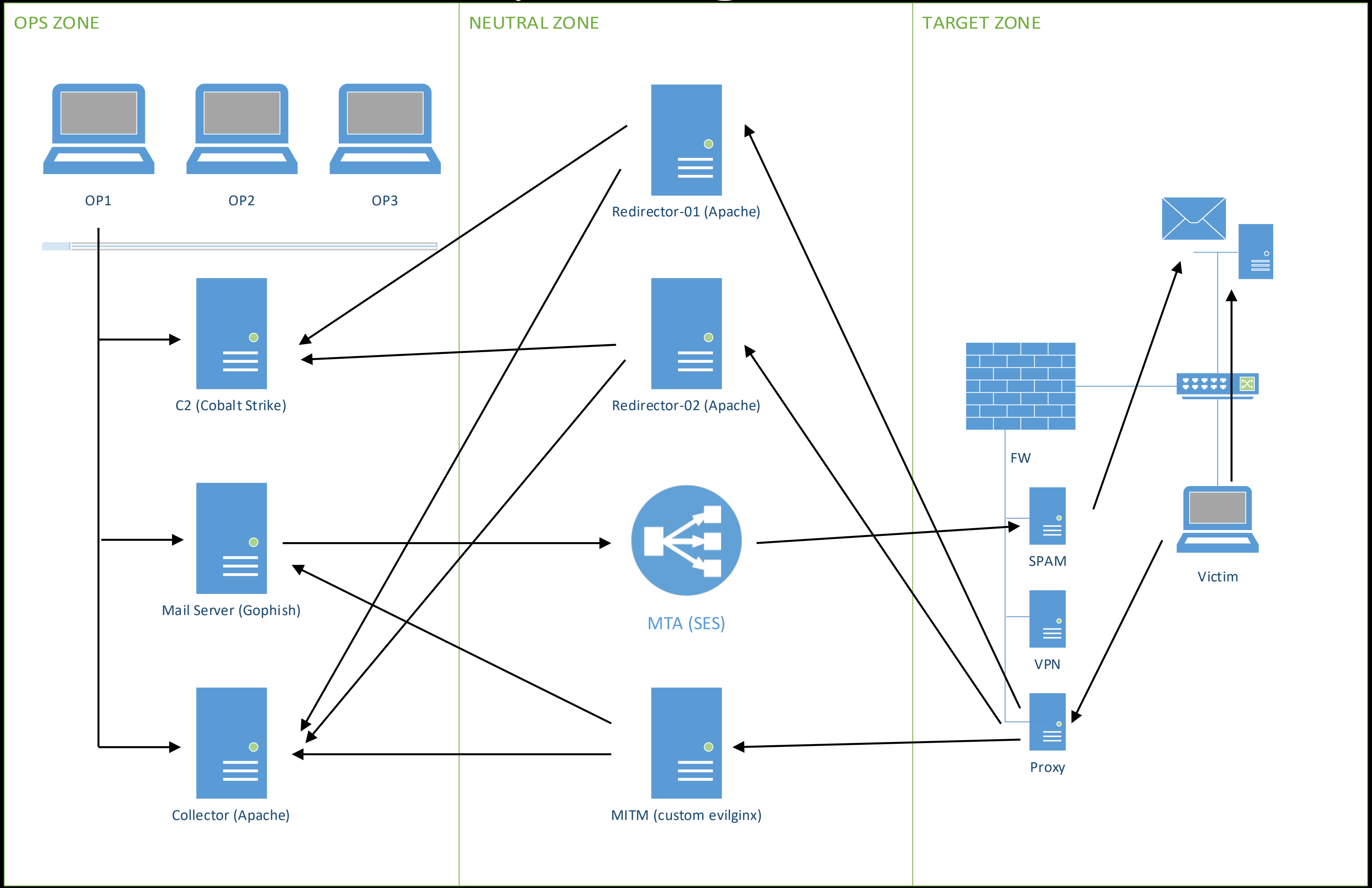
Spear Phishing

Provisioning & Infra. Deployment

Prov. & Infra. | Things we need

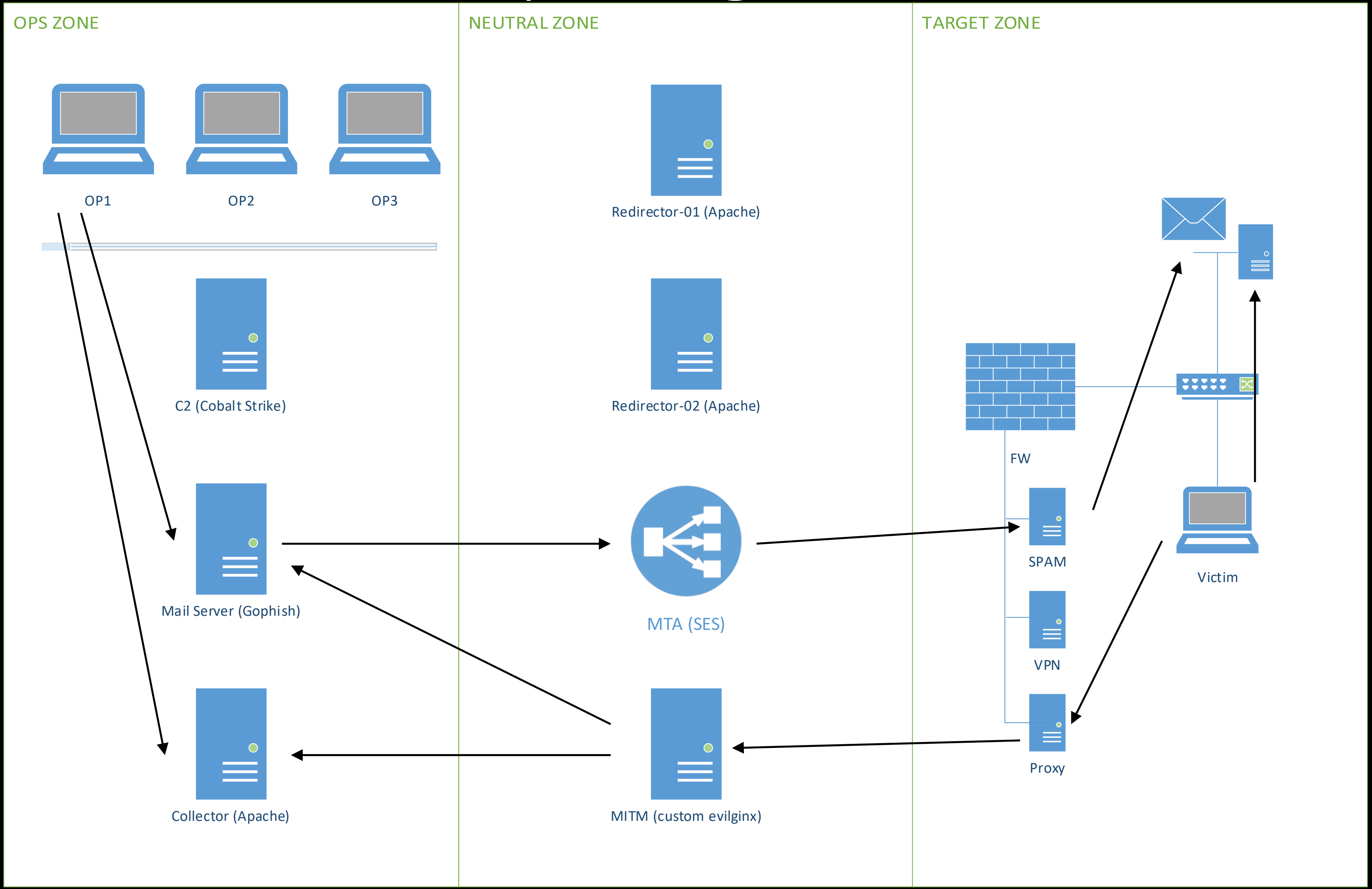
- Shopping list (options):
  - Hosting: Linode, AWS, Azure, etc.
  - C2s: Cobalt Strike, Covenant, etc.
  - Redirectors: Apache, Nginx, etc.
  - MitM: evilginx2
  - MTAs (aaS or ad-hoc): Amazon SES, Mailchimp, Mailjet, Postfix, etc.
  - Mail Server: Gophish, Cobalt Strike, etc.
  - Domains: Reputation & Categotization & (privacy ON)
  - DNS management: Cloudfare

Prov. & Infra. | Design & Comms. (I)



- Simple and repeatable
- Separating the design in zones helps in automation, access control and filtering, and securing engagement data
- Baseline ad-hoc customization

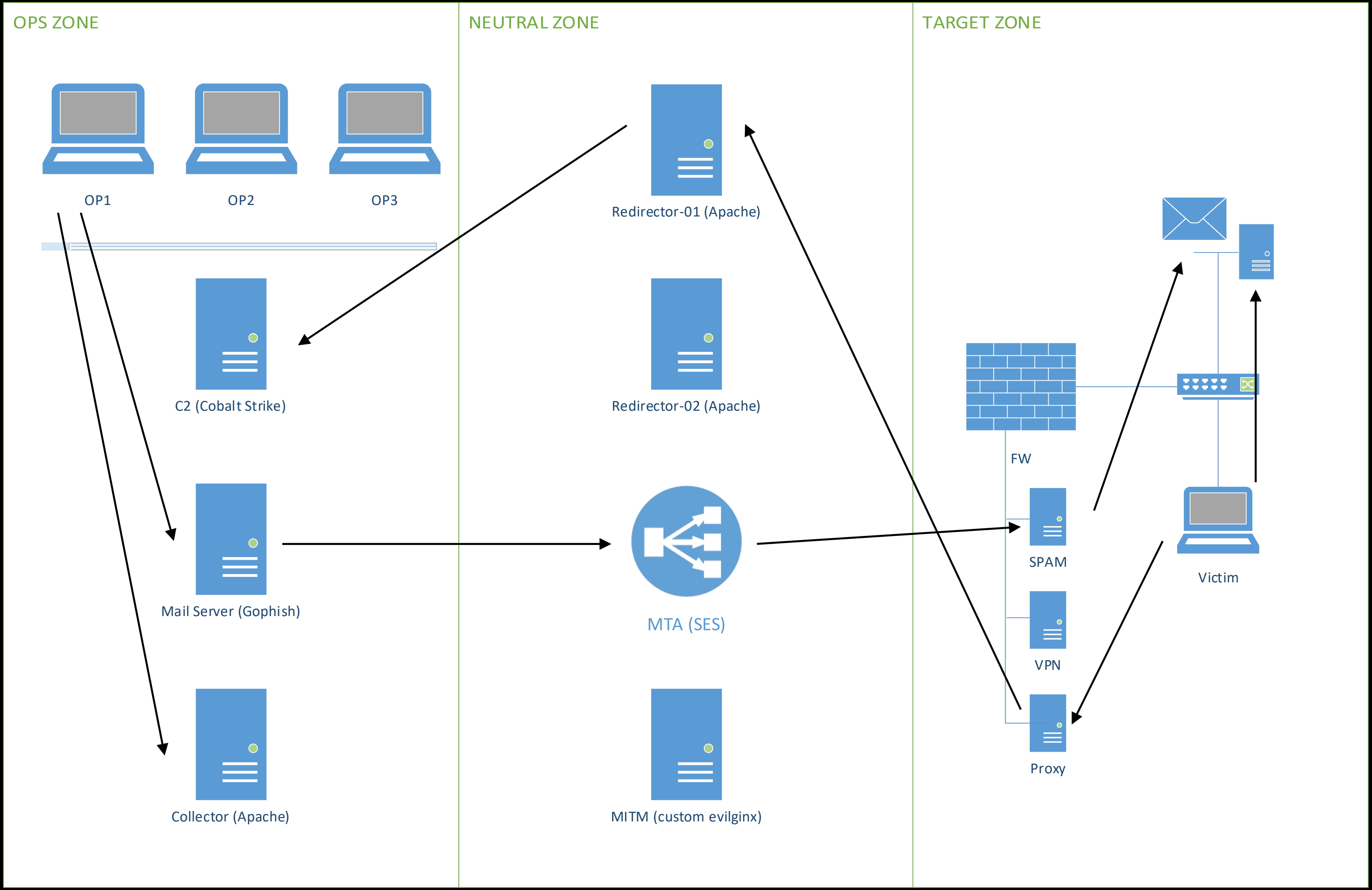
Prov. & Infra. | Design & Comms. (II)



Credential Harvesting

- No execution on client
- Just Email GW and Proxy interfering
- Provides Domain Level Valid credentials
- In case of 2FA, limited to the exploited service

Prov. & Infra. | Design & Comms. (III)



Attachment base code execution → E.g. Beacon implant

- Execution of malicious code in the client
- Email GW, Proxy, AV/EDR, SIEM, etc., interfering
- Provides authenticated user level access on the domain
- Remote control through C2 channels

Prov. & Infra. | Domains (I)

- Depending on the usage:
  - Sending Mail: Senders Good reputation
  - C2 or Harvesters: Good categorization (needed to fight egress-filtering)
    - Financial & Health good options

- Resources
  - Expired-domains: Domain preselection

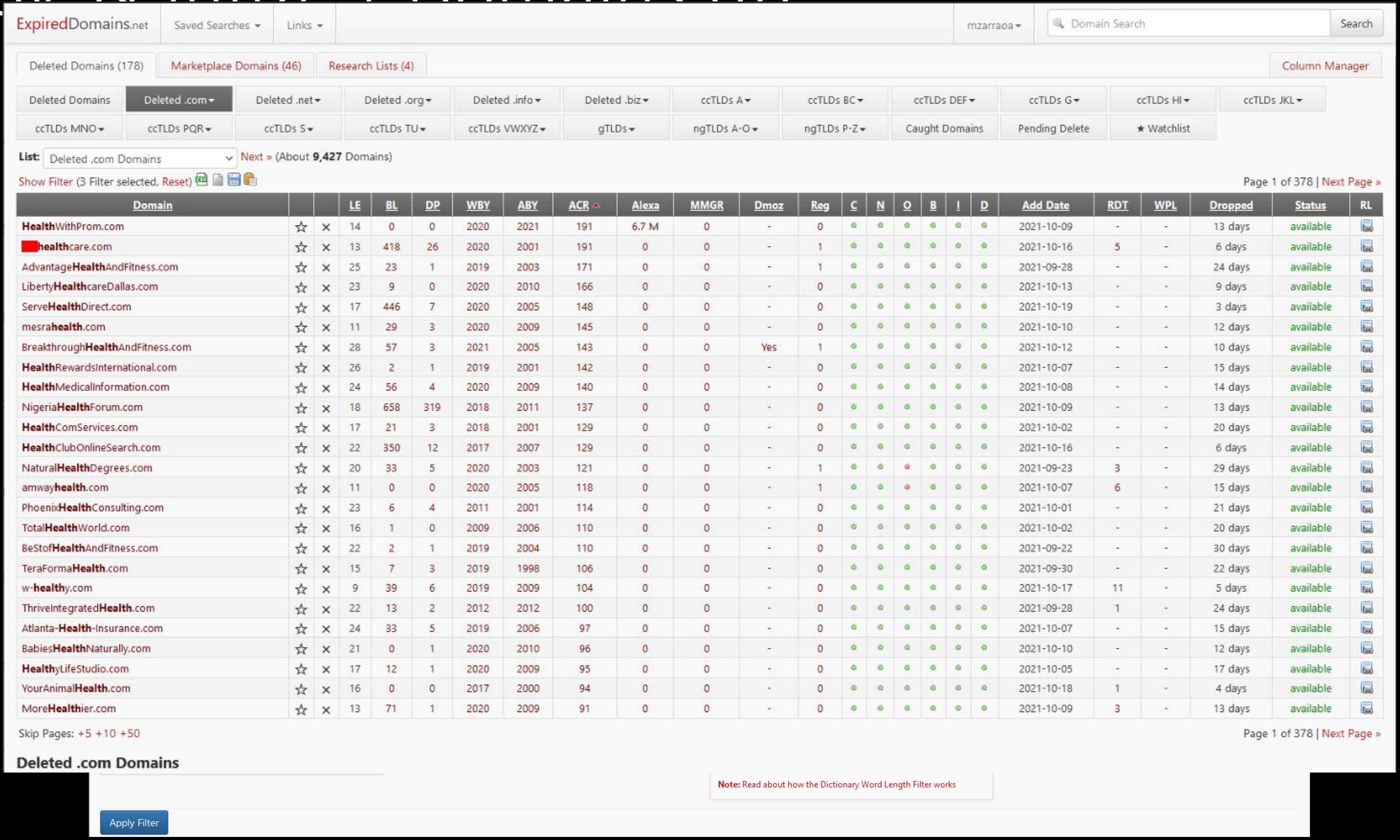
Categorization Checking Sites:

McAfee
FortiGuard
Bluecoat/Symantec
Checkpoint
Palo Alto Wildfire
Trend Micro Site Safety Center
Cisco Talos Intelligence Group
Forcepoint
IBM X-Force Exchange
Etc.

Reputation Checking Sites:

MultiRBL.valli.org
MXTOOLBOX - Email Blacklist Check

Prov. & Infra. | Domains (II)



List: Deleted .com Domains Next » (About **9,427** Domains)

Show Filter (3 Filter selected, Reset)

Page 1 of 378 | Next Page »

Domain			LE	BL	DP	WBY	ABY	ACR	Alexa	MMGR	Dmoz	Reg	C	N	O	B	I	D	Add Date	RDT	WPL	Dropped	Status	RL
HealthWithProm.com	☆	×	14	0	0	2020	2021	191	6.7 M	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-09	-	-	13 days	available	
[redacted]**health**care.com	☆	×	13	418	26	2020	2001	191	0	0	-	1	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-16	5	-	6 days	available	
Advantage**Health**AndFitness.com	☆	×	25	23	1	2019	2003	171	0	0	-	1	🟢	🟢	🟢	🟢	🟢	🟢	2021-09-28	-	-	24 days	available	
Liberty**Health**careDallas.com	☆	×	23	9	0	2020	2010	166	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-13	-	-	9 days	available	
Serve**Health**Direct.com	☆	×	17	446	7	2020	2005	148	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-19	-	-	3 days	available	
mesra**health**.com	☆	×	11	29	3	2020	2009	145	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-10	-	-	12 days	available	
Breakthrough**Health**AndFitness.com	☆	×	28	57	3	2021	2005	143	0	0	Yes	1	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-12	-	-	10 days	available	
HealthRewardsInternational.com	☆	×	26	2	1	2019	2001	142	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-07	-	-	15 days	available	
HealthMedicalInformation.com	☆	×	24	56	4	2020	2009	140	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-08	-	-	14 days	available	
Nigeria**Health**Forum.com	☆	×	18	658	319	2018	2011	137	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-09	-	-	13 days	available	
HealthComServices.com	☆	×	17	21	3	2018	2001	129	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-02	-	-	20 days	available	
HealthClubOnlineSearch.com	☆	×	22	350	12	2017	2007	129	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-16	-	-	6 days	available	
Natural**Health**Degrees.com	☆	×	20	33	5	2020	2003	121	0	0	-	1	🟢	🟢	🔴	🟢	🟢	🟢	2021-09-23	3	-	29 days	available	
amway**health**.com	☆	×	11	0	0	2020	2005	118	0	0	-	1	🟢	🟢	🔴	🟢	🟢	🟢	2021-10-07	6	-	15 days	available	
Phoenix**Health**Consulting.com	☆	×	23	6	4	2011	2001	114	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-01	-	-	21 days	available	
Total**Health**World.com	☆	×	16	1	0	2009	2006	110	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-02	-	-	20 days	available	
BeStof**Health**AndFitness.com	☆	×	22	2	1	2019	2004	110	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-09-22	-	-	30 days	available	
TeraForma**Health**.com	☆	×	15	7	3	2019	1998	106	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-09-30	-	-	22 days	available	
w-**health**y.com	☆	×	9	39	6	2019	2009	104	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-17	11	-	5 days	available	
ThriveIntegrated**Health**.com	☆	×	22	13	2	2012	2012	100	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-09-28	1	-	24 days	available	
Atlanta-**Health**-Insurance.com	☆	×	24	33	5	2019	2006	97	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-07	-	-	15 days	available	
Babies**Health**Naturally.com	☆	×	21	0	1	2020	2010	96	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-10	-	-	12 days	available	
HealthyLifeStudio.com	☆	×	17	12	1	2020	2009	95	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-05	-	-	17 days	available	
YourAnimal**Health**.com	☆	×	16	0	0	2017	2000	94	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-18	1	-	4 days	available	
More**Health**ier.com	☆	×	13	71	1	2020	2009	91	0	0	-	0	🟢	🟢	🟢	🟢	🟢	🟢	2021-10-09	3	-	13 days	available	

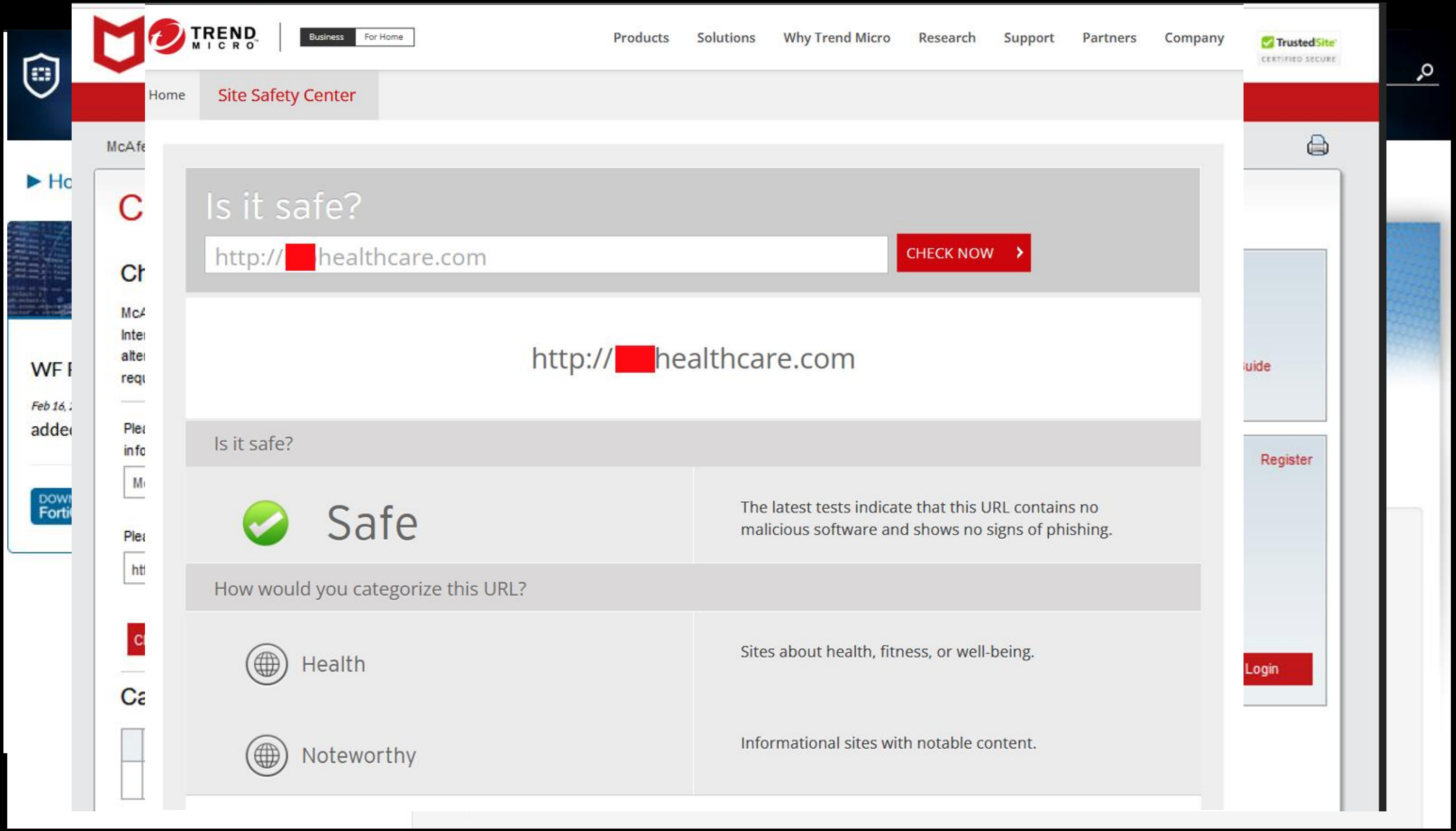
Skip Pages: +5 +10 +50

Page 1 of 378 | Next Page »

Deleted .com Domains

Note: Read about how the Dictionary Word Length Filter works

Prov. & Infra. | Domains (III)



Is it safe?

http://[redacted]healthcare.com

http://[redacted]healthcare.com

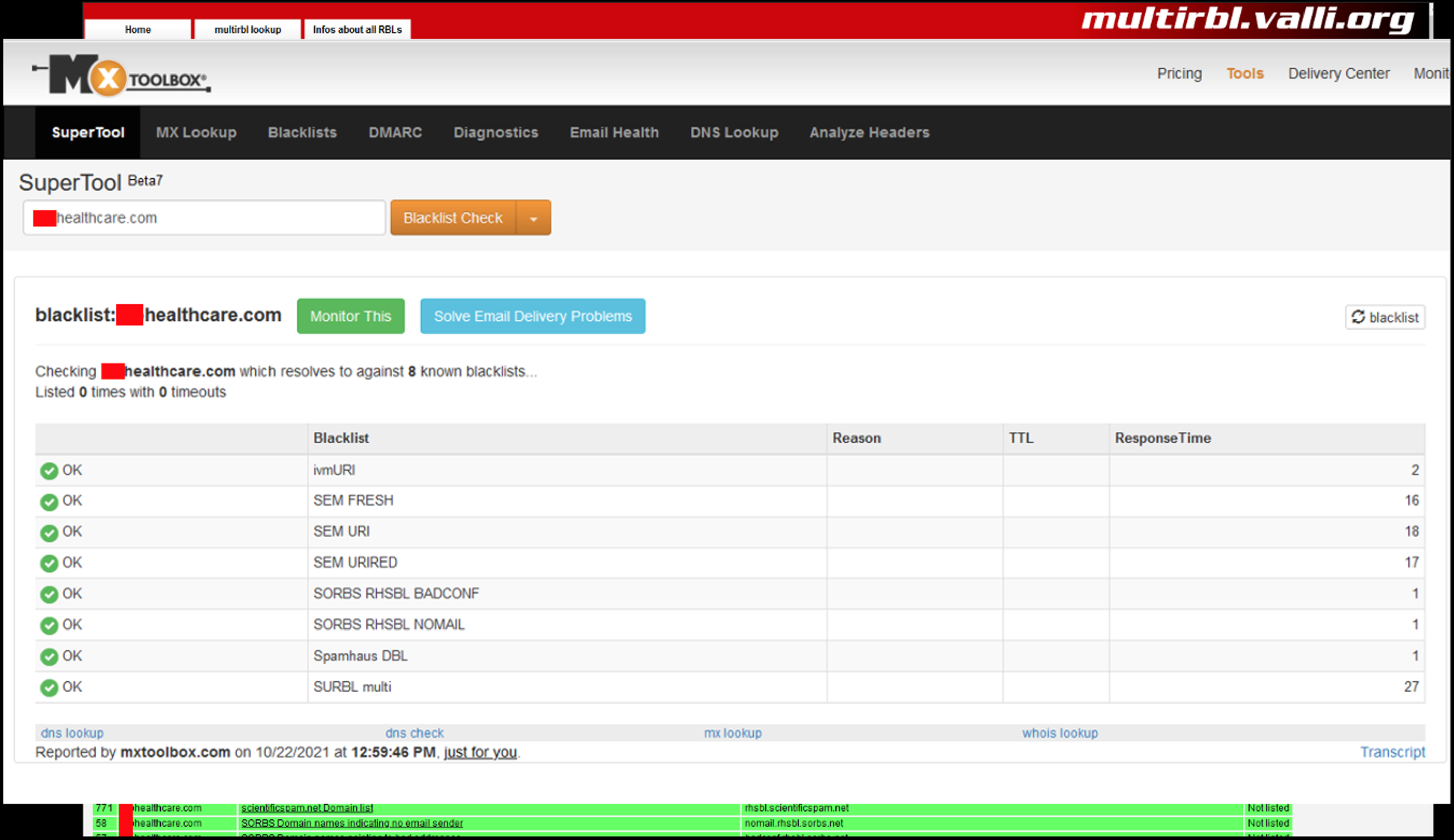
Is it safe?

✓ Safe	The latest tests indicate that this URL contains no malicious software and shows no signs of phishing.

How would you categorize this URL?

Health	Sites about health, fitness, or well-being.
Noteworthy	Informational sites with notable content.

Prov. & Infra. | Domains (IV)



SuperTool Beta7

[redacted]healthcare.com

blacklist:[redacted]healthcare.com

Checking [redacted]**healthcare.com** which resolves to against **8** known blacklists...
Listed **0** times with **0** timeouts

	Blacklist	Reason	TTL	ResponseTime
✓ OK	ivmURI			2
✓ OK	SEM FRESH			16
✓ OK	SEM URI			18
✓ OK	SEM URIRED			17
✓ OK	SORBS RHSBL BADCONF			1
✓ OK	SORBS RHSBL NOMAIL			1
✓ OK	Spamhaus DBL			1
✓ OK	SURBL multi			27

dns lookup dns check mx lookup whois lookup

Reported by **mxtoolbox.com** on 10/22/2021 at **12:59:46 PM**, just for you. Transcript

771	[redacted]healthcare.com	scientificspam.net Domain list	rhsbl.scientificspam.net	Not listed
58	[redacted]healthcare.com	SORBS Domain names indicating no email sender	nomail.rhsbl.sorbs.net	Not listed
57	[redacted]healthcare.com	SORBS Domain names pointing to bad addresses	badconf.rhsbl.sorbs.net	Not listed

Prov. & Infra. | Hosting

- We just need some cheap machines, but on a hosting which provides, at least:
  - Automatic Deployment
  - Template based machines
  - APIs
  - FWs granularity

aws

linode

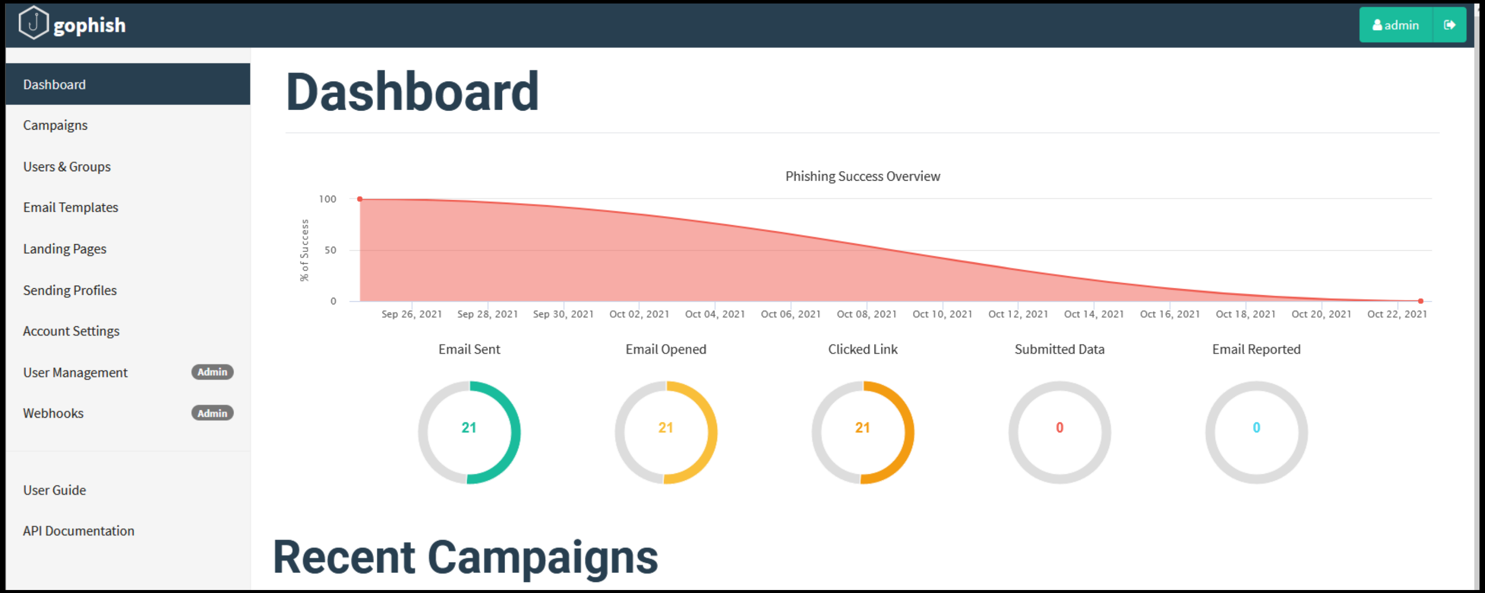
DigitalOcean

Prov. & Infra. | MTAs

- We can go full “aaS” or deploy our own MTA
- “aaS” option: Sender reputation falls in the provider, easy start up, good results in general.
- “ad-hoc” option: Deploy our own MTA, with e.g. postfix. Requires tuning, hardening and configuration. The IP addresses may not have good reputation.
- Do not forget: SPF, DKIM & DMARC
- Ask the “aaS” provider for permission

Prov. & Infra. | Mail Server

- Several options: Gophish, Cobalt Strike, SET, etc. (even CLI)
- Gophish does pretty good job
  - Easy to deploy and automate
  - Can be customed: Webhooks, code customization, hiding fingerprints, etc.
  - Can handle multiple pretexts at the same time (and centralized for multiples engagements)

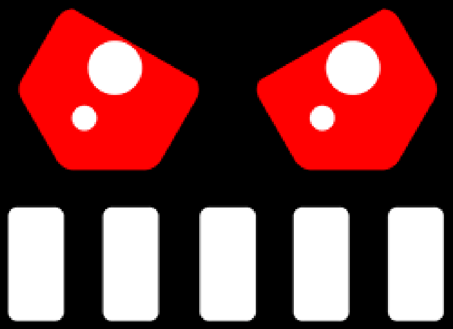


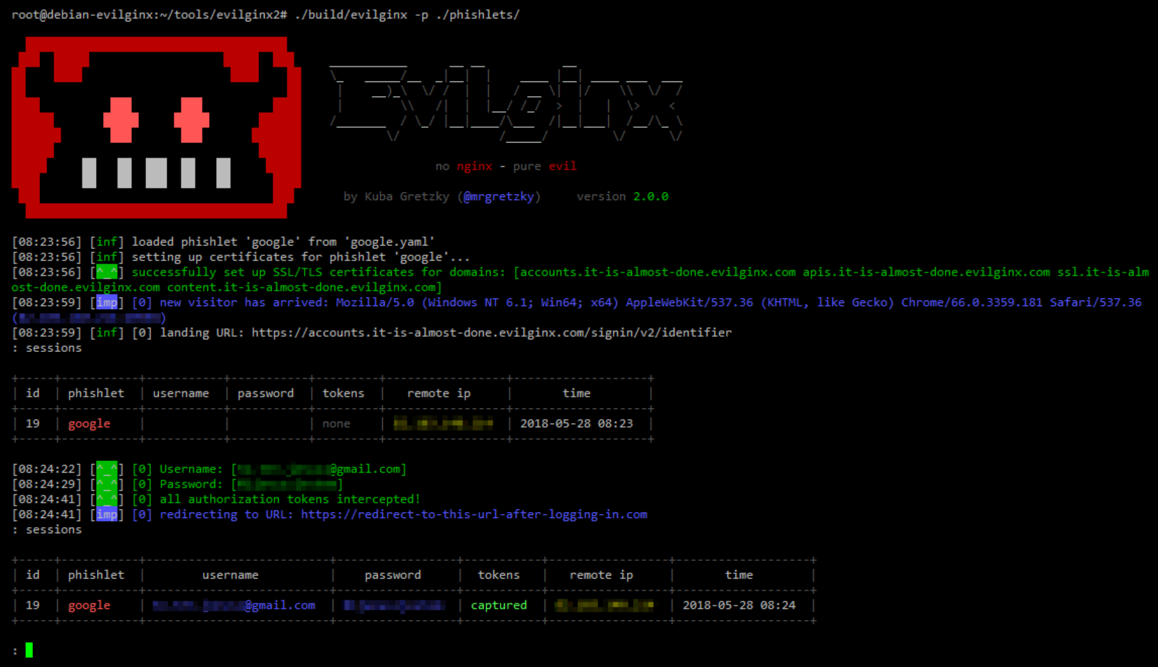
Prov. & Infra. | Redirectors

- Just a reverse proxy
- Used to hide our operations
  - Expendables
  - Can be burned with minimum impact to the OPS in redundant deployments
  - With SSL Certs, looks pretty legitimate
  - Can be deployed mechanisms to stop scans, fool email security gateways, etc.
- Alternatives
  - Port forwarding: Easy, but not powerful
  - Virtual hosting: best alternative, allows us to play with the requests (malleable profiles)

Prov. & Infra. | MITM

- New method heir to the famous harvesting landing pages (no need to clone anything)
- By proxifying the traffic, credentials and sesión cookies are extracted
- Easy 2FA defeat
- De facto: evilginx (https://github.com/kgretzky/evilginx2)
- Important: evilginx directly from Github is not a production tool, but a lab toy, requires some powerups:
  - Hooks to notify operatos
  - Augment registering capabilities
  - Phishlet continuous patching and creation
  - Phishlet customization to avoid INTEL harvesters
  - Bug patching
  - Etc.





```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                         no nginx - pure evil

              by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+----+----------+----------+----------+--------+---------------+------------------+
| id | phishlet | username | password | tokens |   remote ip   |       time       |
+----+----------+----------+----------+--------+---------------+------------------+
| 19 | google   |          |          | none   | [redacted]    | 2018-05-28 08:23 |
+----+----------+----------+----------+--------+---------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+----+----------+-------------------------+---------------+----------+---------------+------------------+
| id | phishlet |        username         |   password    |  tokens  |   remote ip   |       time       |
+----+----------+-------------------------+---------------+----------+---------------+------------------+
| 19 | google   | [redacted]@gmail.com    | [redacted]    | captured | [redacted]    | 2018-05-28 08:24 |
+----+----------+-------------------------+---------------+----------+---------------+------------------+

: 
```

Prov. & Infra. | Final Tips

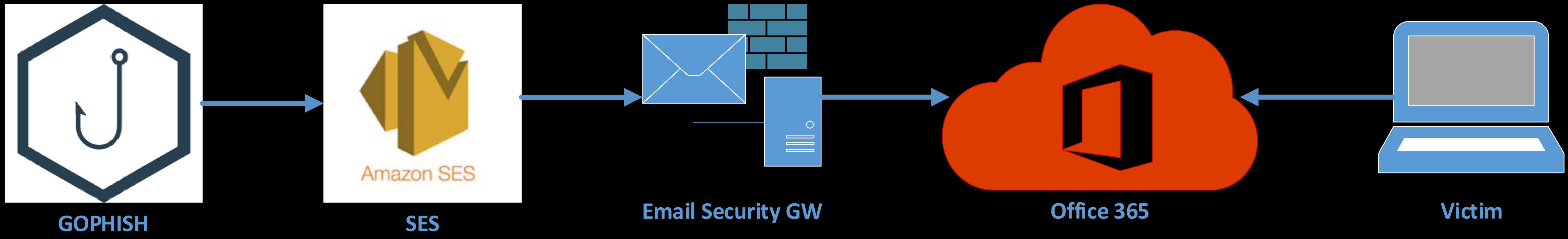
- Do not rely on single provider: Diversify
- Time consuming, automate: E.g. manual << scripting < Ansible < Terraform
- Read providers TOS and ask for permission
- Do not re-use infra
- Execute both unitary and integration tests, to ensure all works as expected
- Do not send overtest the infrastructure and the pretexts

Spear Phishing

Execution

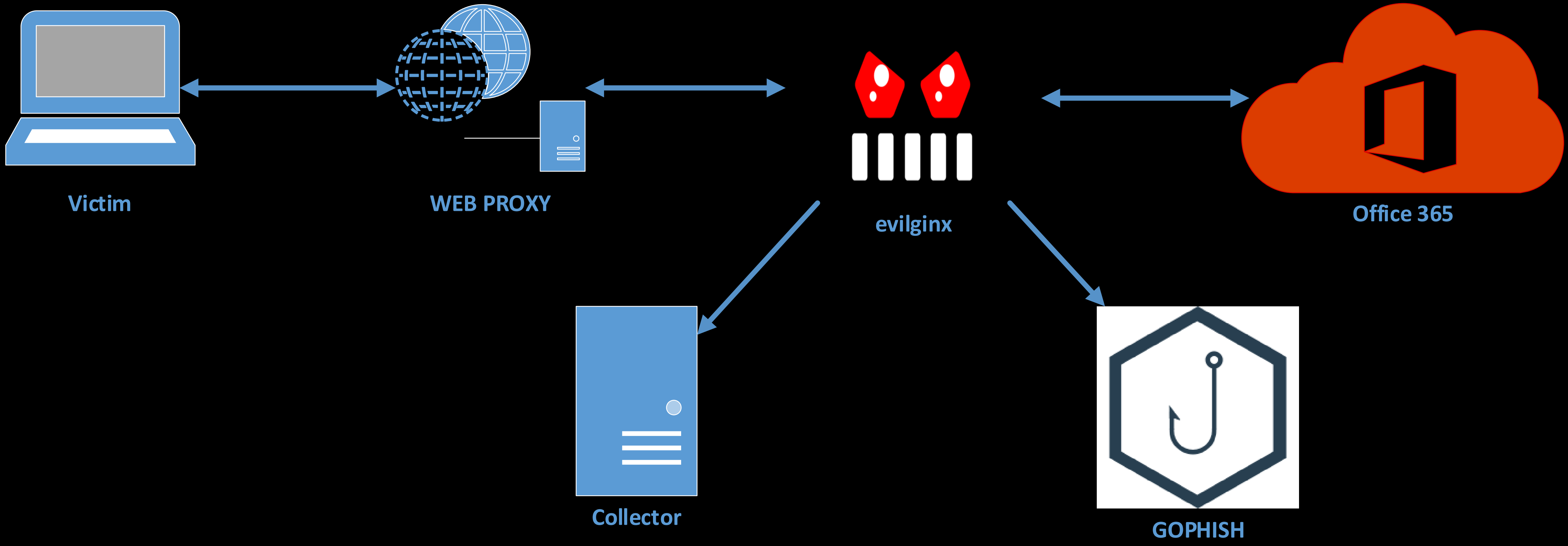
Execution | Credential Harvesting

1. Sending the phishing e-mails



Execution | Credential Harvesting

2. Interacting with the lure



Spear Phishing

Defensive Considerations

Defensive Considerations

- Start with human awareness (first line/filter)

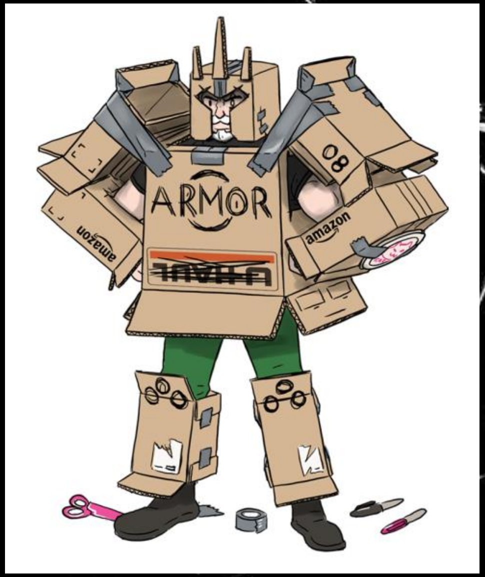
- Subscribe to intelligence feeds

- Evasion of 2FA capture is done by using U2F (Universal 2nd Factor)

- JS Injection: Bypasseable

- Blue Team needs to understand and follow Red Team tradecraft to implement state of the art mitigations

Q&A



Josu Barrientos
@bulw4rk