Search Engines

Mahmoud M. Awali

@0xAwali

attacker

Cyberspace Engines Workflow

Functionalities

Words

Dashboards

attacker

My Methodology

Use These Words While Searching About

D a s h b o a r d s

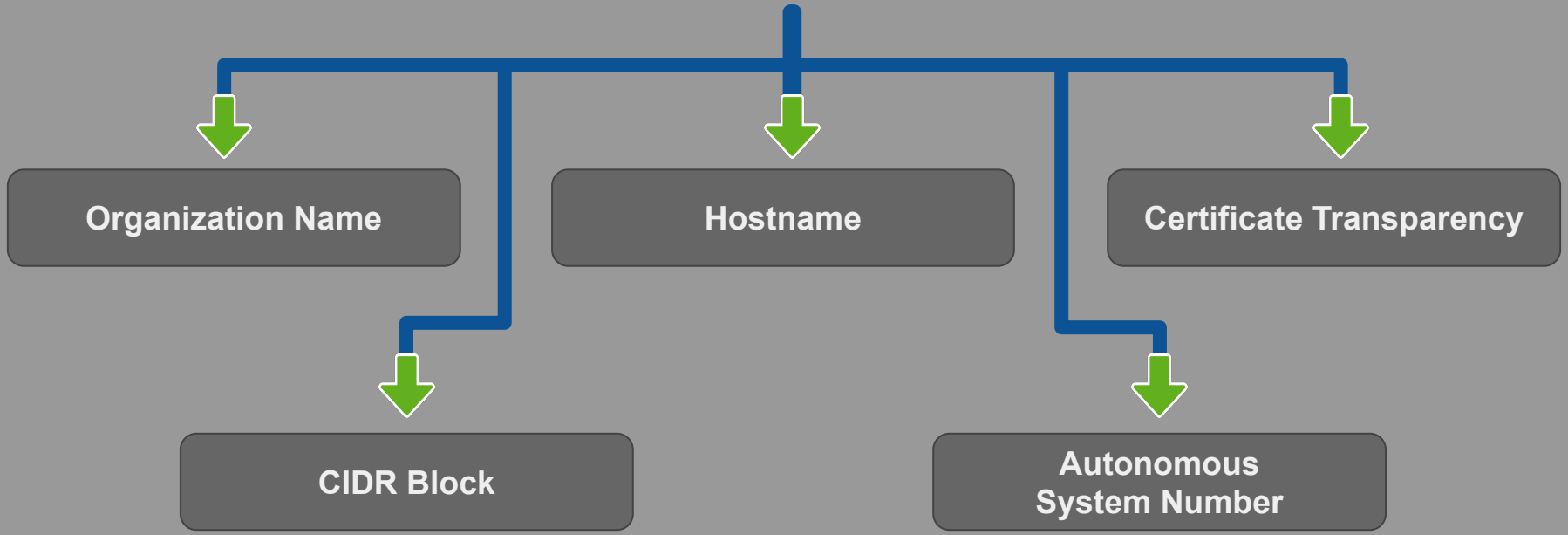
dashboard

"control panel"

admin

attacker

Dashboards Workflow



attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

D a s h b o a r d s

ssl.cert.subject.cn:"company.com" http.title:"dashboard"

ssl:"company.com" http.title:"dashboard"

FOFA cert="company.com" && title="dashboard"

FOFA cert.subject="company" && title="dashboard"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

D a s h b o a r d s

ssl.cert.subject.cn:"company.com" dashboard

ssl:"company.com" dashboard

FOFA cert="company.com" && body="dashboard"

FOFA cert.subject="company" && body="dashboard"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

D a s h b o a r d s

ssl:company.com +title:"dashboard"

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:dashboard

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

D a s h b o a r d s

ssl:company.com +dashboard

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

asn:ASN Number e.g. AS19551+http.title:"dashboard"

FOFA asn="Number e.g. 19551" && title="dashboard"

asn:Number e.g. 19551 +title:"dashboard"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

asn:ASN Number e.g. AS19551+dashboard

asn="Number e.g. 19551" && body="dashboard"

asn:Number e.g. 19551 +dashboard

IPv4

(autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

hostname:company.com http.title:dashboard

FOFA domain="company.com" && title="dashboard"

hostname:company.com +title:"dashboard"

Websites company.com AND 443.https.get.title:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

hostname:company.com dashboard

domain="company.com" && body="dashboard"

hostname:company.com +dashboard

Websites company.com AND 443.https.get.body:dashboard

attacker

My Methodology

Find Dashboard Pages With Google

site:*.company.com intitle:"dashboard"

Google Search

I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

net:"I.P.v.4/CIDR" http.title:dashboard

ip="I.P.v.4/CIDR" && title="dashboard"

cidr:I.P.v.4/CIDR +title:"dashboard"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

net:"I.P.v.4/CIDR" dashboard

FOFA ip="I.P.v.4/CIDR" && body="dashboard"

ZoomEye cidr:I.P.v.4/CIDR +dashboard

IPv4 I.P.v.4/CIDR AND 443.https.get.body:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

org:"Company Inc" http.title:dashboard

FOFA org="Company Name Inc." && title="dashboard"

organization:"Company" +title:"dashboard"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:dashboard

attacker

My Methodology

Use Cyberspace Engines To Discover

D a s h b o a r d s

org:"Company Inc" dashboard

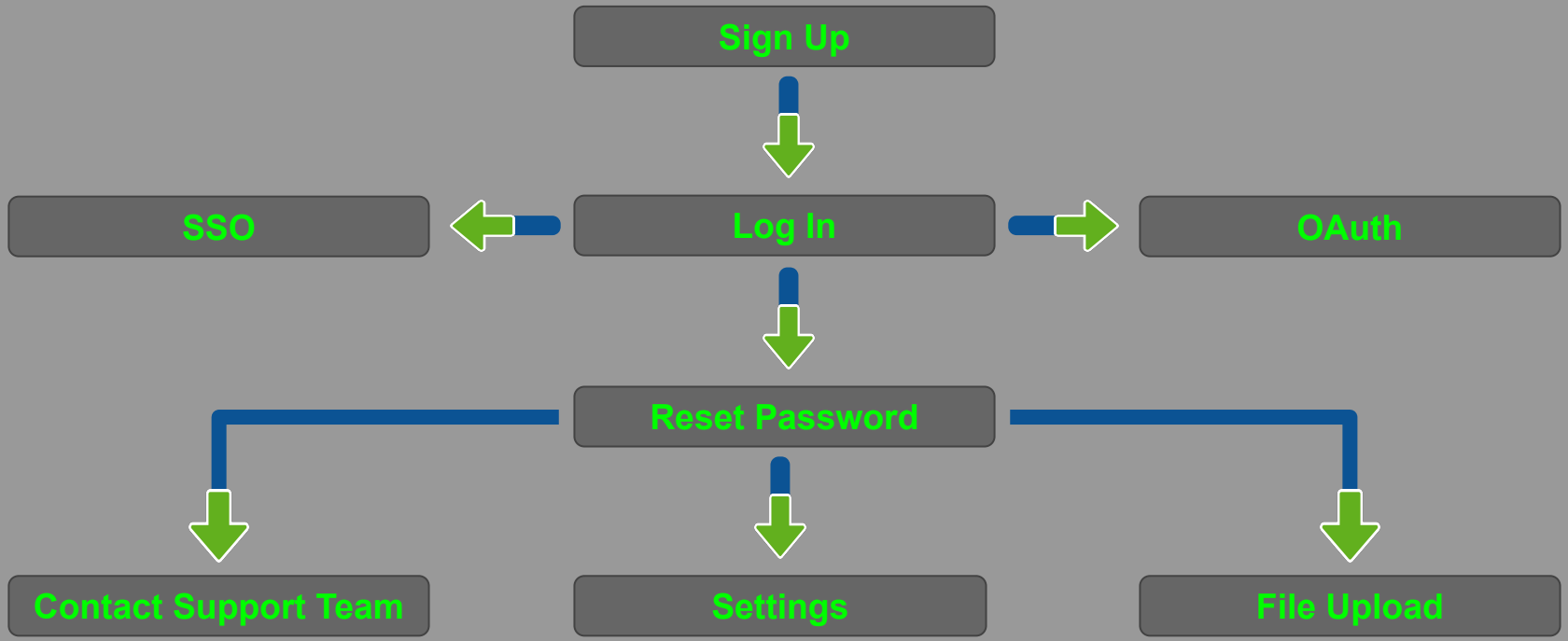
FOFA org="Company Name Inc." && body="dashboard"

organization:"Company" +dashboard

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:dashboard

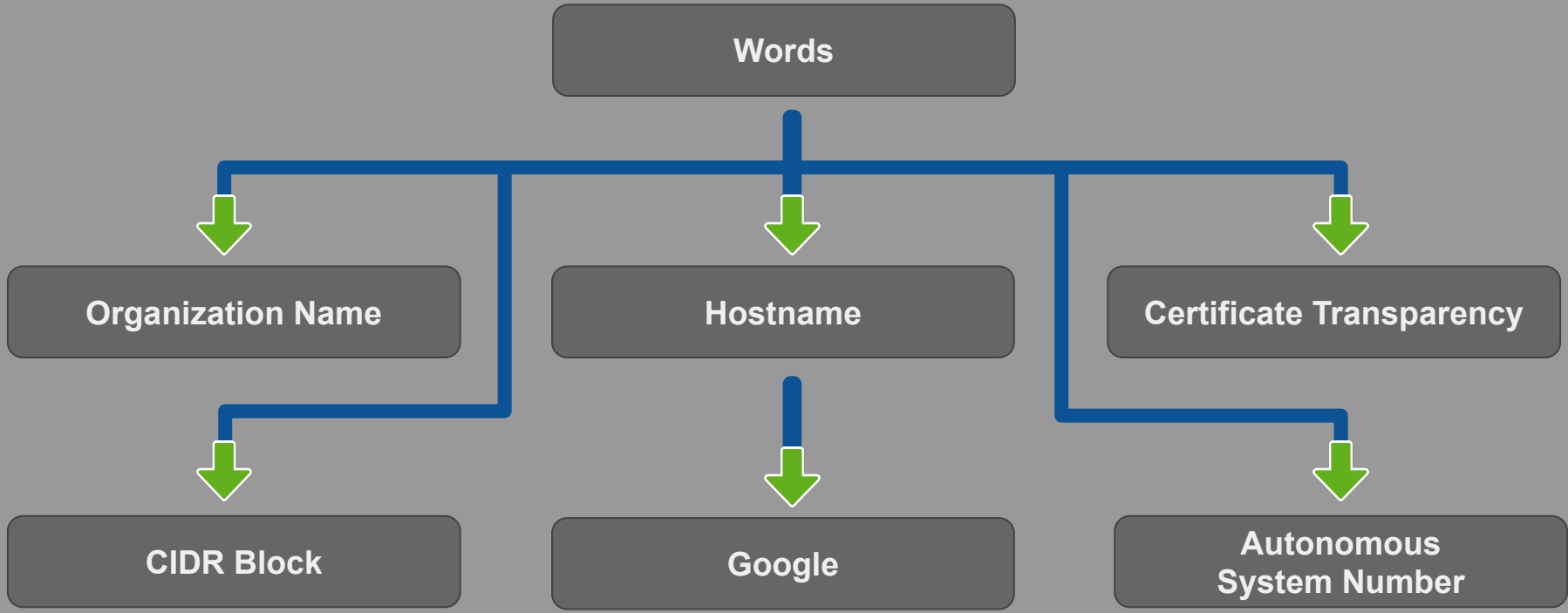
attacker

Functionalities Workflow



attacker

Sign Up Workflow



attacker

My Methodology

Use These Words While Searching About

Sign Up Pages

"sign up"

"new account"

registration

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Sign Up Pages

ssl.cert.subject.cn:"company.com" http.title:"sign up"

ssl:"company.com" http.title:"sign up"

FOFA cert="company.com" && title="sign up"

FOFA cert.subject="company" && title="sign up"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Sign Up Pages

- ssl.cert.subject.cn:"company.com" "sign up"
- ssl:"company.com" "sign up"
- cert="company.com" && body="sign up"
- cert.subject="company" && body"sign up"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Sign Up Pages

ssl:company.com +title:"sign up"

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"sign up"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Sign Up Pages

ssl:company.com +"sign up"

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

asn:ASN Number e.g. AS19551+http.title:"sign up"

FOFA

asn="Number e.g. 19551" && title="sign up"

asn:Number e.g. 19551 +title:"sign up"

IPv4

(autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

asn:ASN Number e.g. AS19551+"sign up"

FOFA asn="Number e.g. 19551" && body="sign up"

asn:Number e.g. 19551 +"sign up"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

hostname:company.com http.title:"sign up"

domain="company.com" && title="sign up"

hostname:company.com +title:"sign up"

Websites company.com AND 443.https.get.title:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

hostname:company.com "sign up"

FOFA domain="company.com" && body="sign up"

hostname:company.com +"sign up"

Websites company.com AND 443.https.get.body:"sign up"

attacker

My Methodology

Find Sign Up Pages With Google

site:*.company.com intitle:"sign up"

Google Search I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

net:"I.P.v.4/CIDR" http.title:"sign up"

FOFA

ip="I.P.v.4/CIDR" && title="sign up"

cidr:I.P.v.4/CIDR +title:"sign up"

IPv4

I.P.v.4/CIDR AND 443.https.get.title:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

	net:"I.P.v.4/CIDR" "sign up"
FOFA	ip="I.P.v.4/CIDR" && body="sign up"
	cidr:I.P.v.4/CIDR +"sign up"
 IPv4	I.P.v.4/CIDR AND 443.https.get.body:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

org:"Company Inc" http.title:"sign up"

org="Company Name Inc." && title="sign up"

organization:"Company" +title:"sign up"

IPv4

443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"sign up"

attacker

My Methodology

Use Cyberspace Engines To Discover

Sign Up Pages

org:"Company Inc" "sign up"

FOFA org="Company Name Inc." && body="sign up"

organization:"Company" +"sign up"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"sign up"

Sign Up

First Name

Last Name

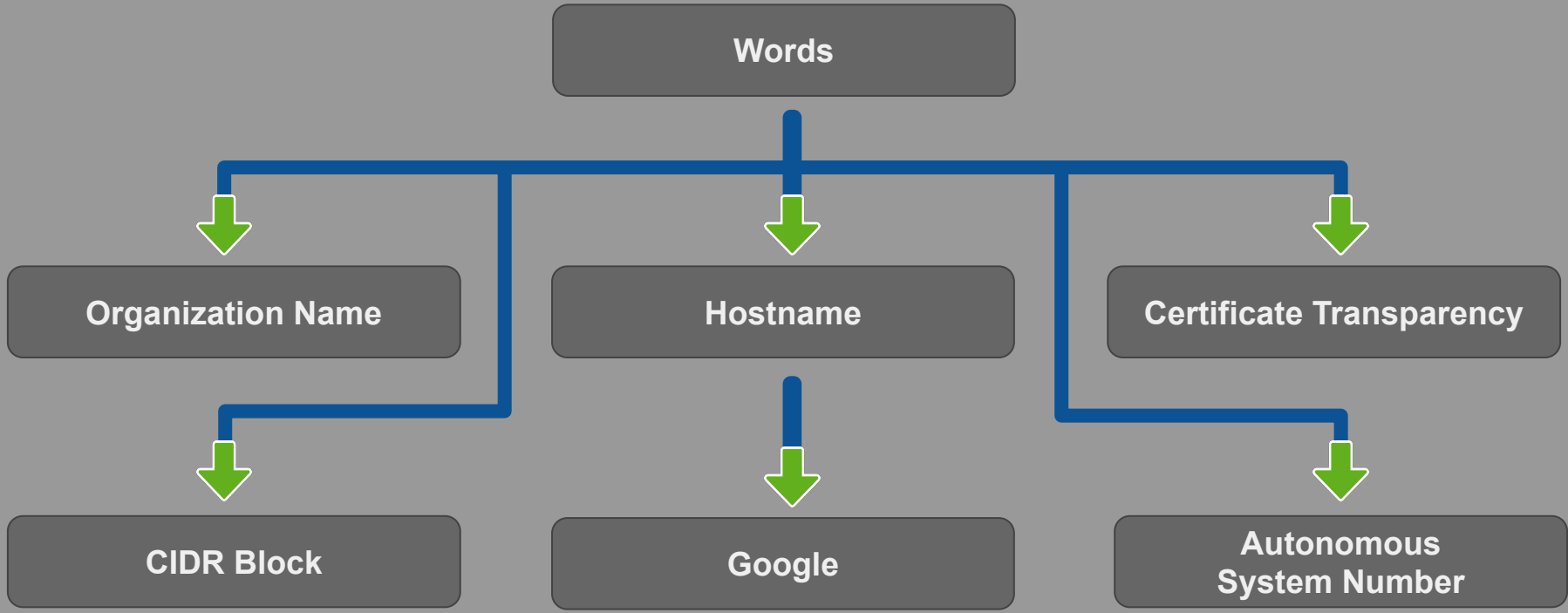
Email Address

Password

My Sign Up Checklist

attacker

Log In Workflow



attacker

My Methodology

Use These Words While Searching About

Log In Pages

"log in"

"sign in"

login

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Log In Pages

- ssl.cert.subject.cn:"company.com" http.title:"log in"
- ssl:"company.com" http.title:"log in"
- cert="company.com" && title="log in"
- cert.subject="company" && title="log in"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Log In Pages

- ssl.cert.subject.cn:"company.com" "log in"
- ssl:"company.com" "log in"
- cert="company.com" && body="log in"
- cert.subject="company" && body="log in"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Log In Pages

ssl:company.com +title:"log in"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"log in"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Log In Pages

ssl:company.com +"log in"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

asn:ASN Number e.g. AS19551+http.title:"log in"

FOFA asn="Number e.g. 19551" && title="log in"

ZoomEye asn:Number e.g. 19551 +title:"log in"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

asn:ASN Number e.g. AS19551+"log in"

FOFA asn="Number e.g. 19551" && body="log in"

asn:Number e.g. 19551 +"log in"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

hostname:company.com http.title:"log in"

domain="company.com" && title="log in"

hostname:company.com +title:"log in"

Websites company.com AND 443.https.get.title:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

hostname:company.com "log in"

FOFA domain="company.com" && body="log in"

ZoomEye hostname:company.com +"log in"

Websites company.com AND 443.https.get.body:"log in"

attacker

My Methodology

Find Log In Pages With Google

site:*.company.com intitle:"log in"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

net:"I.P.v.4/CIDR" http.title:"log in"

FOFA ip="I.P.v.4/CIDR" && title="log in"

ZoomEye cidr:I.P.v.4/CIDR +title:"log in"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

net:"I.P.v.4/CIDR" "log in"

FOFA ip="I.P.v.4/CIDR" && body="log in"

ZoomEye cidr:I.P.v.4/CIDR +"log in"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

	org:"Company Inc" http.title:"log in"
FOFA	org="Company Name Inc." && title="log in"
ZoomEye	organization:"Company" +title:"log in"
IPv4	443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"log in"

attacker

My Methodology

Use Cyberspace Engines To Discover

Log In Pages

org:"Company Inc" "log in"

org="Company Name Inc." && body="log in"

organization:"Company" +"log in"

IPv4

443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"log in"

Log In

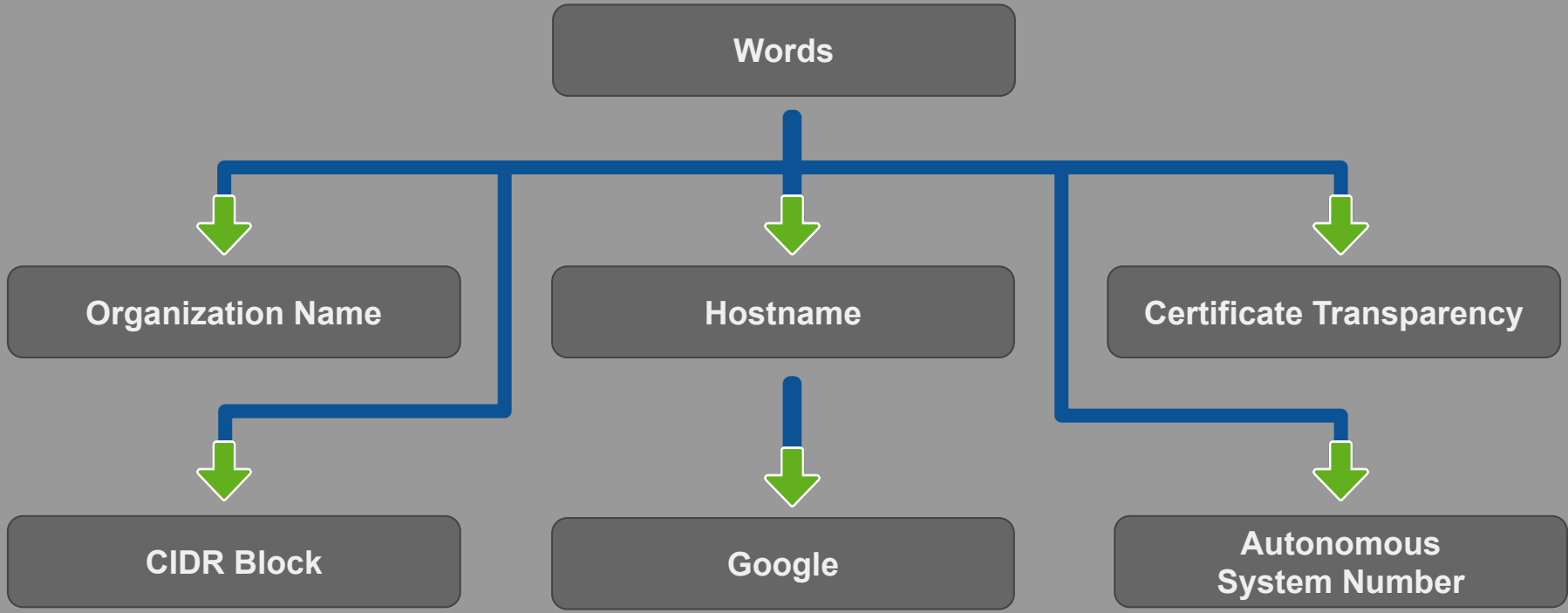
Email Address OR Mobile Number

Password

My Log In Checklist

attacker

OAuth Workflow



attacker

My Methodology

Use These Words While Searching About

OAuth Pages

"log in with"	"login with"
"sign up with"	"signup with"
"sign in with"	"signin with"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

OAuth Pages

ssl.cert.subject.cn:"company.com" http.title:"log in with"

ssl:"company.com" http.title:"log in with"

FOFA cert="company.com" && title="log in with"

FOFA cert.subject="company" && title="log in with"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

OAuth Pages

ssl.cert.subject.cn:"company.com" http.status:302 oauth

ssl:"company.com" http.status:302 oauth

FOFA cert="company.com" && status_code="302" && header="oauth"

FOFA cert.subject="company" && status_code="302" && header="oauth"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

OAuth Pages

ssl.cert.subject.cn:"company.com" oauth

ssl:"company.com" oauth

FOFA cert="company.com" && body="oauth"

FOFA cert.subject="company" && body="oauth"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

OAuth Pages

ZoomEye

ssl:company.com +title:"log in with"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"log in with"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

OAuth Pages

ssl:company.com +("302 Found" +"oauth")

IPv4

(443.https.tls.certificate.parsed.names:Company.com) AND 443.https.get.status_code:302 AND 443.https.get.body:oauth

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

OAuth Pages

ZoomEye

ssl:company.com +"log in with"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

asn:ASN Number e.g. AS19551+http.title:"log in with"

FOFA

asn="Number e.g. 19551" && title="log in with"

asn:Number e.g. 19551 +title:"log in with"

IPv4

(autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover OAuth Pages

asn:ASN Number e.g. AS19551 http.status:302 oauth

asn="Number" && status_code="302" && header="oauth"

asn:Number +("302 Found" +"oauth")

IPv4

(autonomous_system.asn:Number) AND 443.https.get.status_code:302 AND 443.https.get.body:oauth

attacker

My Methodology

Use Cyberspace Engines To Discover OAuth Pages

asn:ASN Number e.g. AS19551+"log in with"

asn="Number e.g. 19551" && body="log in with"

asn:Number e.g. 19551 +"log in with"

IPv4

(autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

hostname:company.com http.title:"log in with"

domain="company.com" && title="log in with"

hostname:company.com +title:"log in with"

Websites

company.com AND 443.https.get.title:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover OAuth Pages

hostname:company.com http.status:302 oauth

domain="company.com" && status_code="302" && header="oauth"

hostname:company.com +("302 Found" +"oauth")

Websites

company.com AND 443.https.get.status_code:302 AND 443.https.get.body:oauth

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

hostname:company.com "log in with"

domain="company.com" && body="log in with"

hostname:company.com +"log in with"

Websites

company.com AND 443.https.get.body:"log in with"

attacker

My Methodology

Find OAuth Pages With Google

site:*.company.com intitle:"log in with"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

net:"I.P.v.4/CIDR" http.title:"log in with"

FOFA ip="I.P.v.4/CIDR" && title="log log in"

ZoomEye cidr:I.P.v.4/CIDR +title:"log in with"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

net:"I.P.v.4/CIDR" http.status:302 oauth

FOFA ip="I.P.v.4/CIDR" && status_code="302" && header="oauth"

cidr:I.P.v.4/CIDR +("302 Found" +"oauth")

IPv4 (I.P.v.4/CIDR) AND 443.https.get.status_code:302 AND 443.https.get.body:oauth

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

net:"I.P.v.4/CIDR" "log in with"

ip="I.P.v.4/CIDR" && body="log in"

cidr:I.P.v.4/CIDR +"log in with"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

org:"Company Inc" http.title:"log in with"

FOFA org="Company Name Inc." && title="log in with"

organization:"Company" +title:"log in with"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"log in with"

attacker

My Methodology

Use Cyberspace Engines To Discover

OAuth Pages

org:"Company Inc" http.status:302 oauth

FOFA org="Company Name Inc." && status_code="302" && header="oauth"

organization:"Company" +("302 Found" +"oauth")

IPv4

443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND
443.https.get.status_code:302 AND 443.https.get.body:oauth

attacker

My Methodology

Use Cyberspace Engines To Discover OAuth Pages

org:"Company Inc" oauth

org="Company Name Inc." && body="oauth"

organization:"Company" +"oauth"

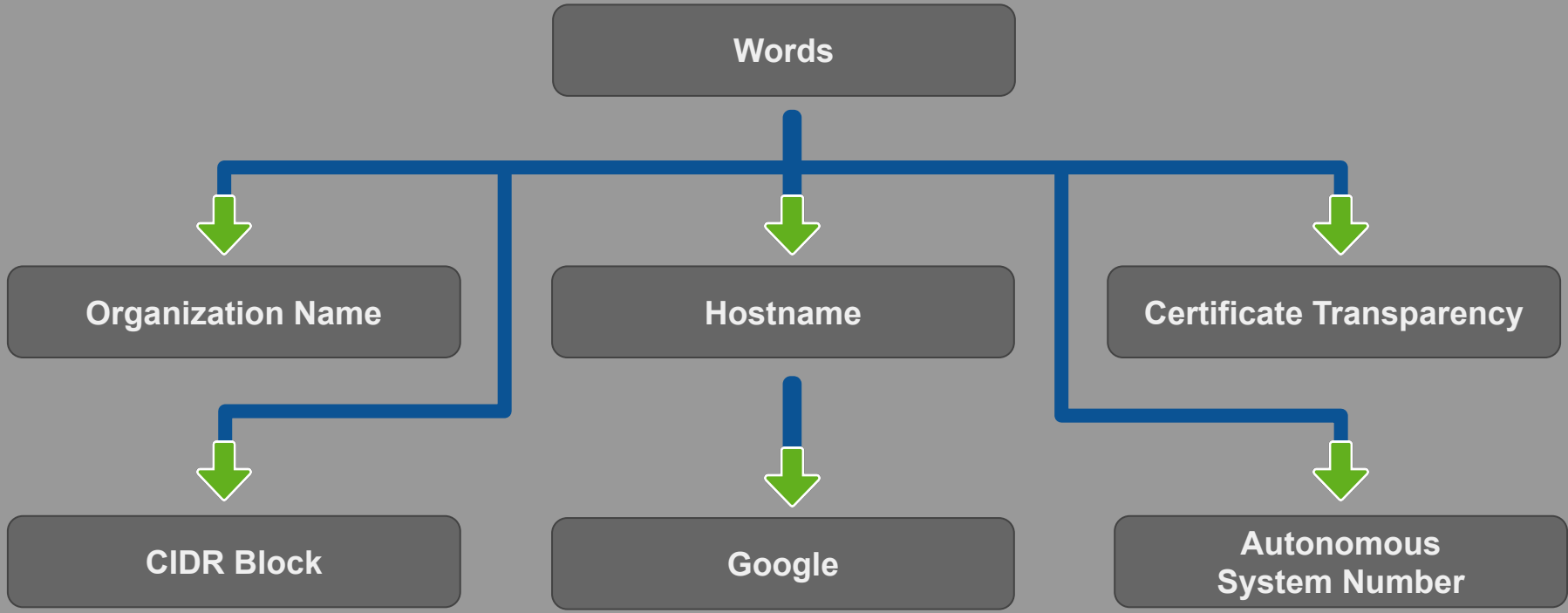
IPv4

443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:oauth


OAuth
Sign Up AND Log In
Sing Up With Google
Log In With Apple
My OAuth Checklist

attacker

SSO Workflow



attacker

My Methodology

Use These Words While Searching About

Single Sign-On Pages

"sso login"

"login with sso"

SAMLRequest

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Single Sign-On Pages

ssl.cert.subject.cn:"company.com" http.title:"login sso"

ssl:"company.com" http.title:"login sso"

FOFA cert="company.com" && title="login sso"

FOFA cert.subject="company" && title="login sso"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Single Sign-On Pages

ssl.cert.subject.cn:"company.com" http.status:302 sso

ssl:"company.com" http.status:302 sso

FOFA cert="company.com" && status_code="302" && header="sso"

FOFA cert.subject="company" && status_code="302" && header="sso"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Single Sign-On Pages

ssl.cert.subject.cn:"company.com" "login sso"

ssl:"company.com" "login sso"

FOFA cert="company.com" && body="login sso"

FOFA cert.subject="company" && body="login sso"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Single Sign-On Pages

ZoomEye

```
ssl:company.com +title:"sso"
```

IPv4

```
(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"sso"
```

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Single Sign-On Pages

ZoomEye

```
ssl:company.com +("302 Found" +"sso")
```

IPv4

```
(443.https.tls.certificate.parsed.names:Company.com) AND 443.https.get.status_code:302 AND 443.https.get.body:sso
```

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Single Sign-On Pages

ZoomEye ssl:company.com +sso

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

asn:ASN Number e.g. AS19551+http.title:"sso"

FOFA asn="Number e.g. 19551" && title="sso"

ZoomEye asn:Number e.g. 19551 +title:"sso"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

asn:ASN Number e.g. AS19551 http.status:302 sso

asn="Number" && status_code="302" && header="sso"

asn:Number +("302 Found" +"sso")

IPv4

(autonomous_system.asn:Number) AND 443.https.get.status_code:302 AND 443.https.get.body:sso

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

asn:ASN Number e.g. AS19551+sso

FOFA asn="Number e.g. 19551" && body="sso"

ZoomEye asn:Number e.g. 19551 +sso

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

hostname:company.com http.title:"sso"

FOFA domain="company.com" && title="sso"

hostname:company.com +title:"sso"

Websites company.com AND 443.https.get.title:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

hostname:company.com http.status:302 sso

domain="company.com" && status_code="302" && header="sso"

hostname:company.com +("302 Found" +"sso")

Websites

company.com AND 443.https.get.status_code:302 AND 443.https.get.body:sso

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

hostname:company.com sso

domain="company.com" && body="sso"

hostname:company.com +sso

Websites

company.com AND 443.https.get.body:"sso"

attacker

My Methodology

Find Single Sign-On Pages With Google

site:*.company.com intitle:"sso"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

net:"I.P.v.4/CIDR" http.title:"sso"

FOFA ip="I.P.v.4/CIDR" && title="sso"

cidr:I.P.v.4/CIDR +title:"sso"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

net:"I.P.v.4/CIDR" http.status:302 sso

FOFA ip="I.P.v.4/CIDR" && status_code="302" && header="sso"

cidr:I.P.v.4/CIDR +("302 Found" +"sso")

IPv4 (I.P.v.4/CIDR) AND 443.https.get.status_code:302 AND 443.https.get.body:sso

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

net:"I.P.v.4/CIDR" sso

ip="I.P.v.4/CIDR" && body="sso"

cidr:I.P.v.4/CIDR +sso

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"sso"

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

org:"Company Inc" http.title:"sso"

FOFA org="Company Name Inc." && title="sso"

organization:"Company" +title:"sso"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:sso

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

org:"Company Inc" http.status:302 sso

FOFA org="Company Name Inc." && status_code="302" && header="sso"

organization:"Company" +("302 Found" +"sso")

IPv4

443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND
443.https.get.status_code:302 AND 443.https.get.body:sso

attacker

My Methodology

Use Cyberspace Engines To Discover

Single Sign-On Pages

org:"Company Inc" sso

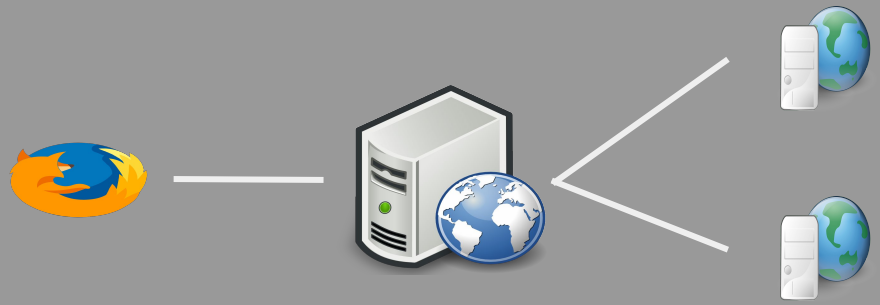
FOFA org="Company Name Inc." && body="sso"

organization:"Company" +sso

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:sso

SSO

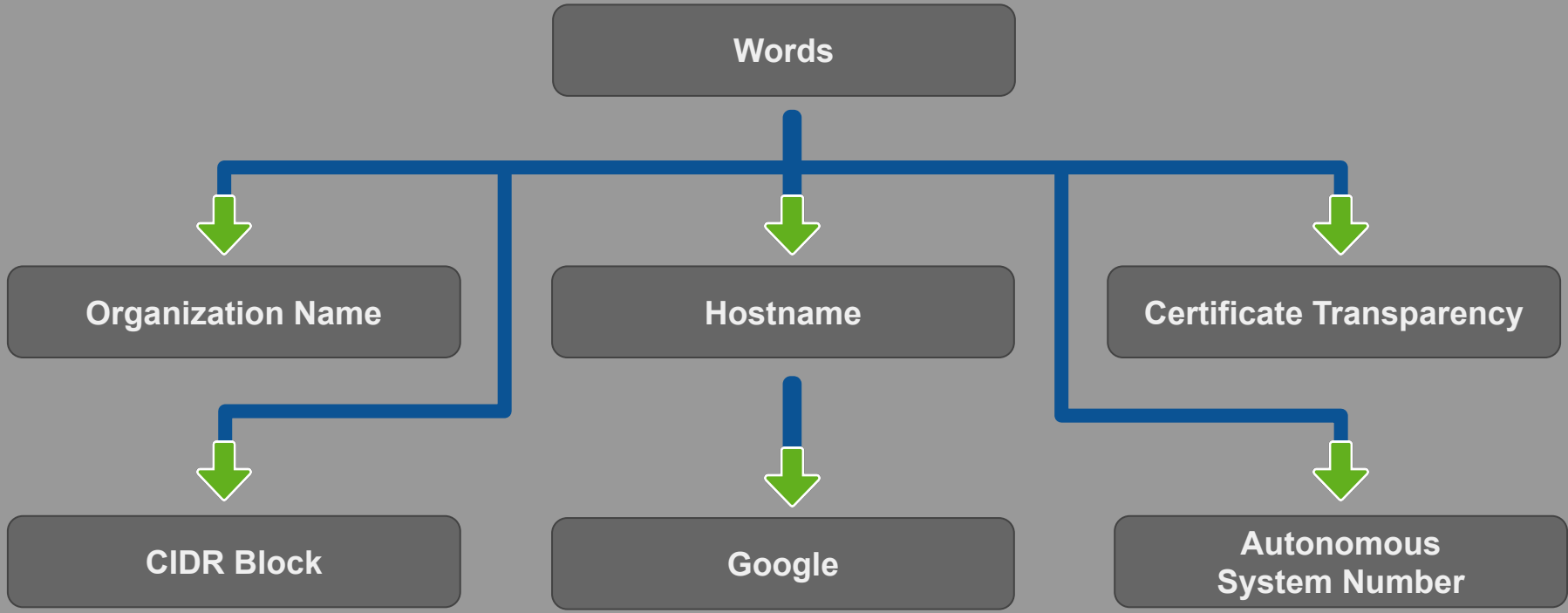
Single Sign-On



My SSO Checklist

attacker

Reset Password Workflow



attacker

My Methodology

Use These Words While Searching About

Reset Password Pages

- reset pass
- forget
- password

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Reset Password Pages

ssl.cert.subject.cn:"company.com" http.title:"password"

ssl:"company.com" http.title:"password"

FOFA cert="company.com" && title="password"

FOFA cert.subject="company" && title="password"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Reset Password Pages

ssl.cert.subject.cn:"company.com" "reset pass"

ssl:"company.com" "reset pass"

FOFA cert="company.com" && body="reset pass"

FOFA cert.subject="company" && body="reset pass"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Reset Password Pages

ZoomEye

ssl:company.com +title:"password"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"password"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Reset Password Pages

ZoomEye

ssl:company.com +"reset pass"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"reset pass"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

asn:ASN Number e.g. AS19551+http.title:"password"

asn="Number e.g. 19551" && title="password"

asn:Number e.g. 19551 +title:"password"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"password"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

asn:ASN Number e.g. AS19551+"reset pass"

FOFA asn="Number e.g. 19551" && body="reset pass"

asn:Number e.g. 19551 +"reset pass"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"reset pass"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

hostname:company.com http.title:"password"

FOFA domain="company.com" && title="password"

hostname:company.com +title:"password"

Websites company.com AND 443.https.get.title:"password"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

hostname:company.com "reset pass"

domain="company.com" && body="password"

hostname:company.com +"reset pass"

Websites

company.com AND 443.https.get.body:"reset pass"

attacker

My Methodology

Find Reset Password Pages With

Google

site:*.company.com intitle:"password"

Google Search

I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

net:"I.P.v.4/CIDR" http.title:"password"

FOFA ip="I.P.v.4/CIDR" && title="password"

ZoomEye cidr:I.P.v.4/CIDR +title:"password"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"password"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

net:"I.P.v.4/CIDR" "reset pass"

FOFA ip="I.P.v.4/CIDR" && body="reset pass"

ZoomEye cidr:I.P.v.4/CIDR +"reset pass"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"reset pass"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

org:"Company Inc" http.title:"password"

FOFA org="Company Name Inc." && title="password"

ZoomEye organization:"Company" +title:"password"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"reset pass"

attacker

My Methodology

Use Cyberspace Engines To Discover

Reset Password Pages

org:"Company Inc" "password"

FOFA org="Company Name Inc." && body="password"

organization:"Company" +"password"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"password"

A T O

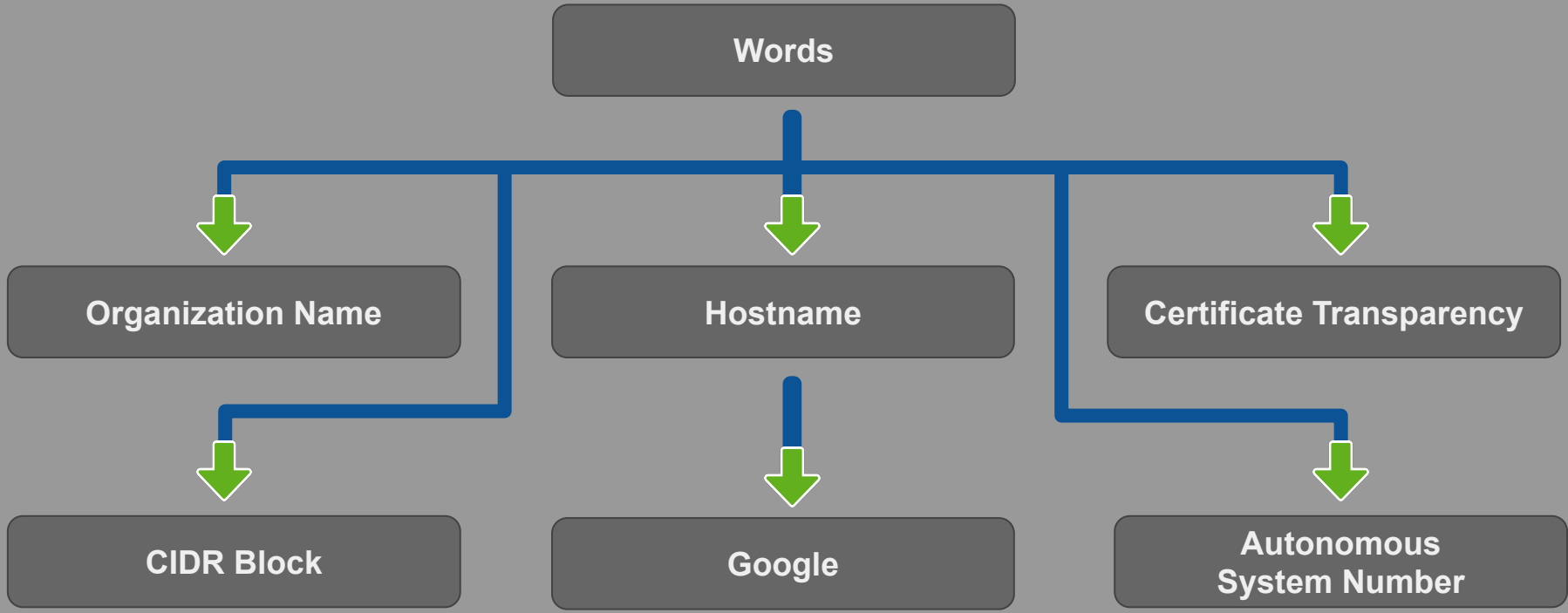
Reset Password

Email Address OR Mobile Number

My resetPASS Checklist

attacker

File Upload Workflow



attacker

My Methodology

Use These Words While Searching About

File Upload Pages

"file upload"

upload

uploading

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

File Upload Pages

ssl.cert.subject.cn:"company.com" http.title:"upload"

ssl:"company.com" http.title:"upload"

FOFA cert="company.com" && title="upload"

FOFA cert.subject="company" && title="upload"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

File Upload Pages

ssl.cert.subject.cn:"company.com" "upload"

ssl:"company.com" "upload"

FOFA cert="company.com" && body="upload"

FOFA cert.subject="company" && body="upload"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

File Upload Pages

ssl:company.com +title:"upload"

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"upload"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

File Upload Pages

ZoomEye

ssl:company.com +"upload"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

asn:ASN Number e.g. AS19551+http.title:"upload"

FOFA asn="Number e.g. 19551" && title="upload"

asn:Number e.g. 19551 +title:"upload"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

asn:ASN Number e.g. AS19551+"upload"

FOFA asn="Number e.g. 19551" && body="upload"

asn:Number e.g. 19551 +"upload"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

hostname:company.com http.title:"upload"

FOFA domain="company.com" && title="upload"

hostname:company.com +title:"upload"

Websites company.com AND 443.https.get.title:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

hostname:company.com "upload"

FOFA domain="company.com" && body="upload"

ZoomEye hostname:company.com +"upload"

Websites company.com AND 443.https.get.body:"upload"

attacker

My Methodology

Find File Upload Pages With Google

site:*.company.com intitle:"upload"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

net:"I.P.v.4/CIDR" http.title:"upload"

FOFA ip="I.P.v.4/CIDR" && title="upload"

ZoomEye cidr:I.P.v.4/CIDR +title:"upload"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

net:"I.P.v.4/CIDR" "upload"

FOFA ip="I.P.v.4/CIDR" && body="upload"

ZoomEye cidr:I.P.v.4/CIDR +"upload"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

org:"Company Inc" http.title:"upload"

FOFA org="Company Name Inc." && title="upload"

ZoomEye organization:"Company" +title:"upload"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"upload"

attacker

My Methodology

Use Cyberspace Engines To Discover

File Upload Pages

org:"Company Inc" "upload"

FOFA org="Company Name Inc." && body="upload"

ZoomEye organization:"Company" +"upload"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"upload"

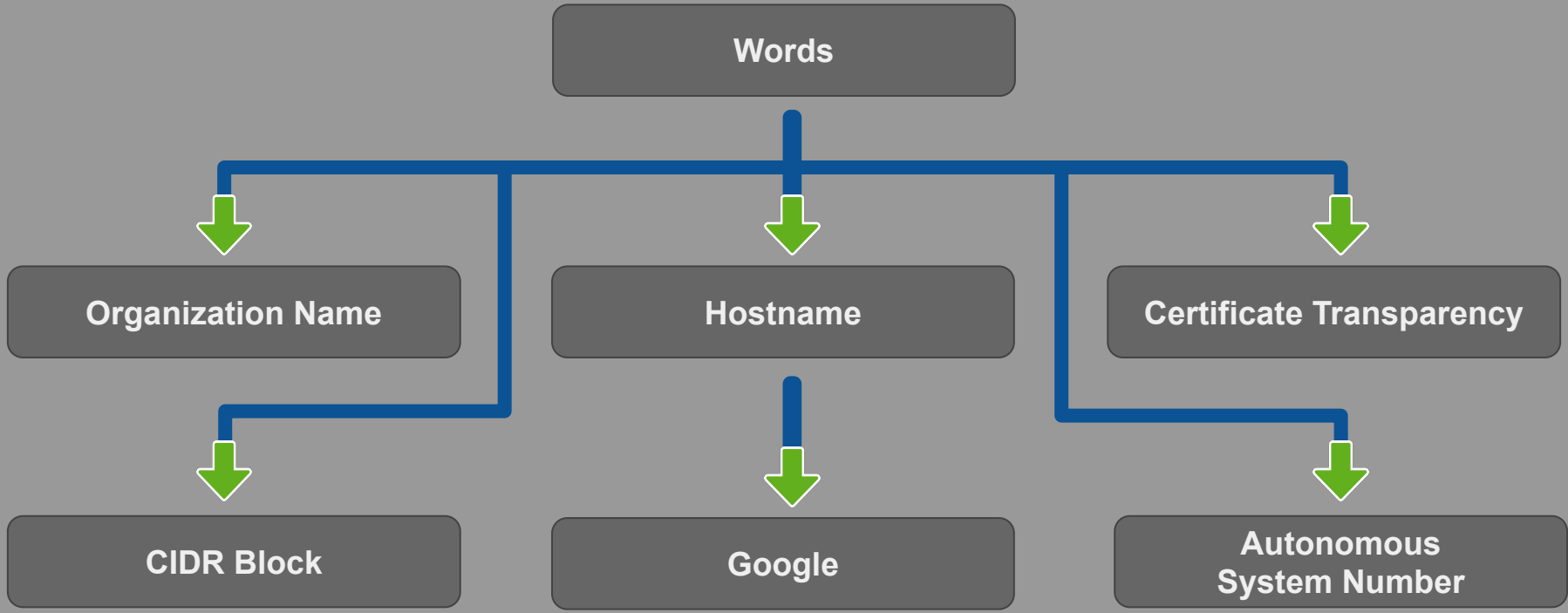
File Upload

Upload File From Your Computer

My File Upload Checklist

attacker

Settings Workflow



attacker

My Methodology

Use These Words While Searching About

Settings Pages

settings

"edit profile"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Settings Pages

ssl.cert.subject.cn:"company.com" http.title:"settings"

ssl:"company.com" http.title:"settings"

FOFA cert="company.com" && title="settings"

FOFA cert.subject="company" && title="settings"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Settings Pages

ssl.cert.subject.cn:"company.com" "settings"

ssl:"company.com" "settings"

FOFA cert="company.com" && body="settings"

FOFA cert.subject="company" && body="settings"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Settings Pages

ZoomEye

```
ssl:company.com +title:"settings"
```

IPv4

```
(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"settings"
```

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Settings Pages

ZoomEye

ssl:company.com +"settings"

IPv4

(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

asn:ASN Number e.g. AS19551+http.title:"settings"

FOFA asn="Number e.g. 19551" && title="settings"

asn:Number e.g. 19551 +title:"settings"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

asn:ASN Number e.g. AS19551+"settings"

FOFA asn="Number e.g. 19551" && body="settings"

ZoomEye asn:Number e.g. 19551 +"settings"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

hostname:company.com http.title:"settings"

domain="company.com" && title="settings"

hostname:company.com +title:"settings"

Websites company.com AND 443.https.get.title:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

hostname:company.com "settings"

domain="company.com" && body="settings"

hostname:company.com +"settings"

Websites

company.com AND 443.https.get.body:"settings"

attacker

My Methodology

Find Settings Pages With Google

site:*.company.com intitle:"settings"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

net:"I.P.v.4/CIDR" http.title:"settings"

FOFA ip="I.P.v.4/CIDR" && title="settings"

ZoomEye cidr:I.P.v.4/CIDR +title:"settings"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

net:"I.P.v.4/CIDR" "settings"

FOFA ip="I.P.v.4/CIDR" && body="settings"

ZoomEye cidr:I.P.v.4/CIDR +"settings"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

org:"Company Inc" http.title:"settings"

FOFA org="Company Name Inc." && title="settings"

ZoomEye organization:"Company" +title:"settings"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"settings"

attacker

My Methodology

Use Cyberspace Engines To Discover

Settings Pages

org:"Company Inc" "settings"

FOFA org="Company Name Inc." && body="settings"

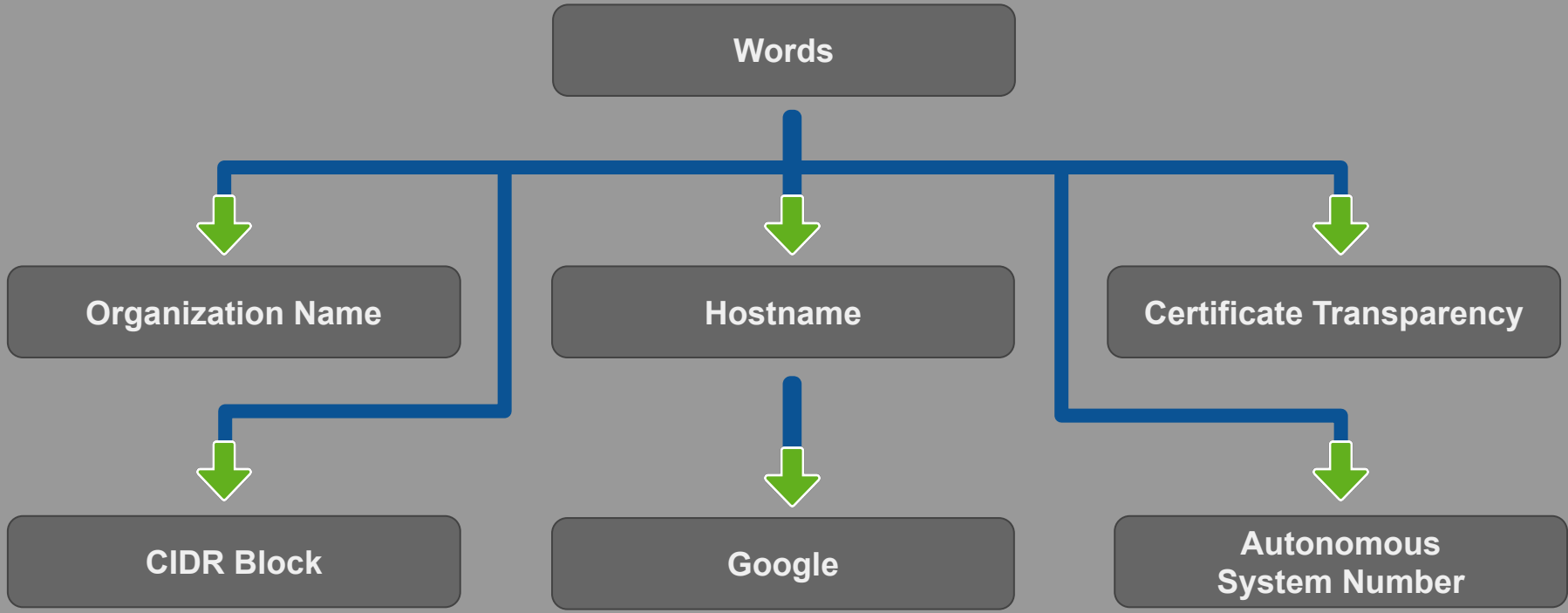
organization:"Company" +"settings"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"settings"


Settings
Edit - Add - Remove
Settings
User company.com/me Edit
Email me@gmail.com Edit
Password ********** Edit
Phone 01********** Add
Your Account Remove
My Settings Checklist

attacker

Contact Support Team Workflow



attacker

My Methodology

Use These Words While Searching About

Contact Support Pages

support

"contact us"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Contact Support Pages

ssl.cert.subject.cn:"company.com" http.title:"support"

ssl:"company.com" http.title:"support"

FOFA cert="company.com" && title="support"

FOFA cert.subject="company" && title="support"

attacker

My Methodology

Use Shodan AND Fofa Engines To Discover

Contact Support Pages

ssl.cert.subject.cn:"company.com" "support"

ssl:"company.com" "support"

FOFA cert="company.com" && body="support"

FOFA cert.subject="company" && body="support"

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Contact Support Pages

ZoomEye

`ssl:company.com +title:"support"`

IPv4

`(443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.title:"support"`

attacker

My Methodology

Use Zoomeye AND Censys Engines To Discover

Contact Support Pages

ZoomEye ssl:company.com +"support"

IPv4 (443.https.tls.certificate.parsed.names:company.com) AND 443.https.get.body:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

asn:ASN Number e.g. AS19551+http.title:"support"

FOFA asn="Number e.g. 19551" && title="support"

asn:Number e.g. 19551 +title:"support"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.title:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

asn:ASN Number e.g. AS19551+"support"

FOFA asn="Number e.g. 19551" && body="support"

ZoomEye asn:Number e.g. 19551 +"support"

IPv4 (autonomous_system.asn:Number e.g. 19551) AND 443.https.get.body:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

hostname:company.com http.title:"support"

FOFA domain="company.com" && title="support"

hostname:company.com +title:"support"

Websites company.com AND 443.https.get.title:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

hostname:company.com "support"

FOFA domain="company.com" && body="support"

hostname:company.com +"support"

Websites company.com AND 443.https.get.body:"support"

attacker

My Methodology

Find Contact Support Pages With Google

site:*.company.com intitle:"support"

Google Search | I'm Feeling Lucky

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

net:"I.P.v.4/CIDR" http.title:"support"

FOFA ip="I.P.v.4/CIDR" && title="support"

ZoomEye cidr:I.P.v.4/CIDR +title:"support"

IPv4 I.P.v.4/CIDR AND 443.https.get.title:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

net:"I.P.v.4/CIDR" "support"

FOFA ip="I.P.v.4/CIDR" && body="support"

ZoomEye cidr:I.P.v.4/CIDR +"support"

IPv4 I.P.v.4/CIDR AND 443.https.get.body:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

org:"Company Inc" http.title:"support"

FOFA org="Company Name Inc." && title="support"

organization:"Company" +title:"support"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.title:"support"

attacker

My Methodology

Use Cyberspace Engines To Discover

Contact Support Pages

org:"Company Inc" "support"

FOFA org="Company Name Inc." && body="support"

organization:"Company" +"support"

IPv4 443.https.tls.certificate.parsed.subject.organization:"Company Inc" AND 443.https.get.body:"support"

Contact

Support Of The Company

Email Address

Describe Your Issue

Message

My Contact Team Checklist

Thank You

Mahmoud M. Awali

@0xAwali