Open Source Intelligence

Raphael Karger & Mike Antoniades

Summary

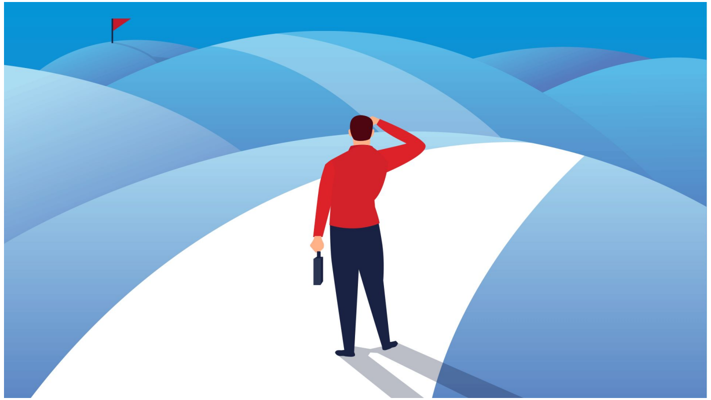
- What is OSINT?
- Goals
- Assets and Scoping
- Sensitive Information Discovery
- Identifying Social Engineering Targets
- Ethics

What is Open Source Intelligence?

- Open Source Intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context

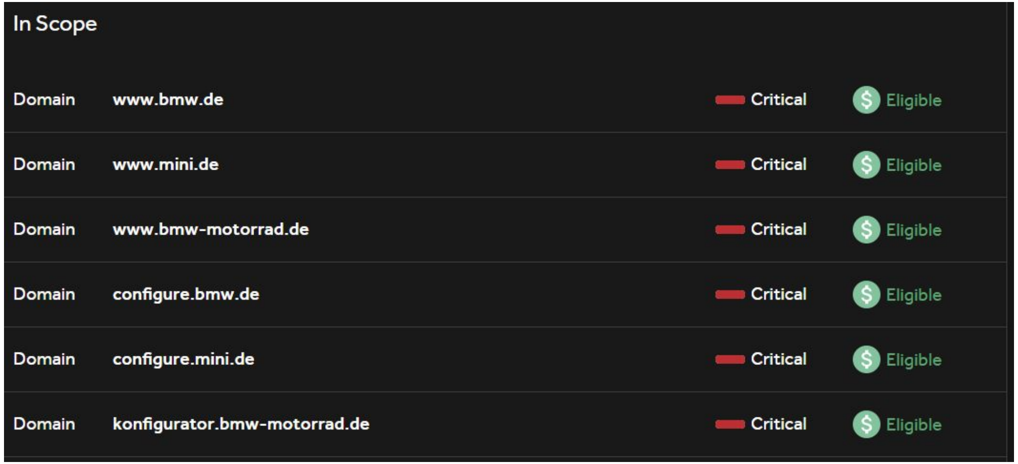
Goals

- Disclose sensitive information
- Widen scope
- Find assets
- Discover internal workings of company



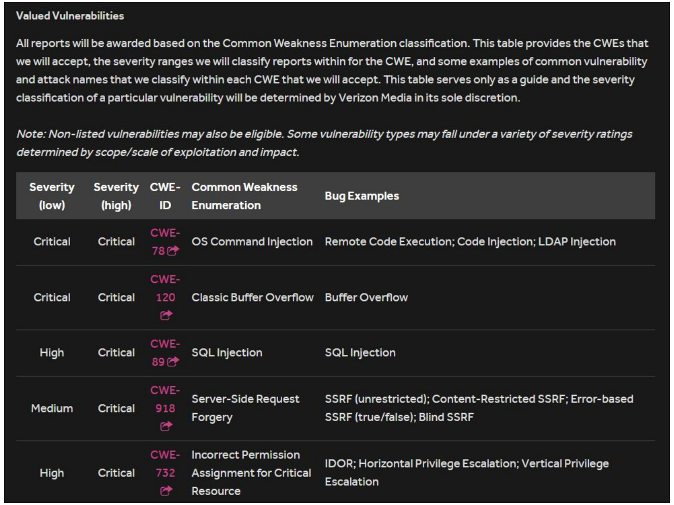
Assets and Scoping

- Asset - any data, device, or other component of the environment that supports information-related activities
- Scoping - Assets you are allowed to test and what type of testing is permitted



In Scope

Domain	www.bmw.de	Critical	$ Eligible
Domain	www.mini.de	Critical	$ Eligible
Domain	www.bmw-motorrad.de	Critical	$ Eligible
Domain	configure.bmw.de	Critical	$ Eligible
Domain	configure.mini.de	Critical	$ Eligible
Domain	konfigurator.bmw-motorrad.de	Critical	$ Eligible



Valued Vulnerabilities

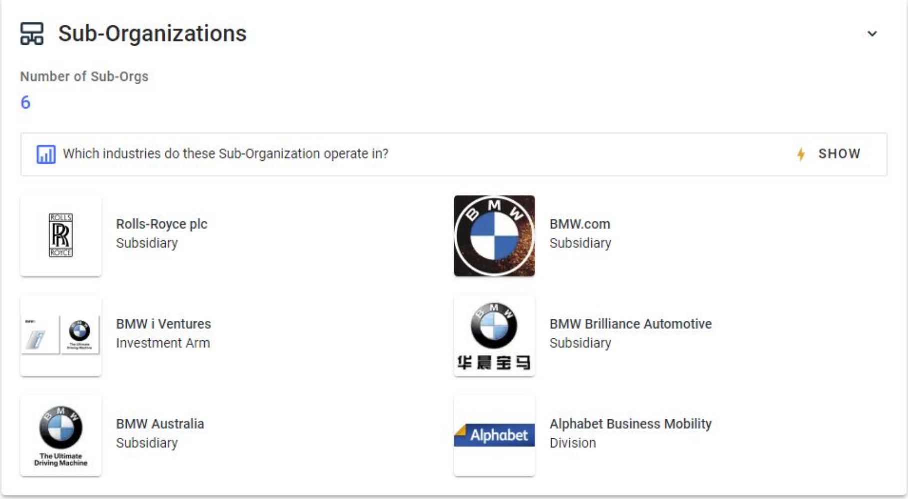
All reports will be awarded based on the Common Weakness Enumeration classification. This table provides the CWEs that we will accept, the severity ranges we will classify reports within for the CWE, and some examples of common vulnerability and attack names that we classify within each CWE that we will accept. This table serves only as a guide and the severity classification of a particular vulnerability will be determined by Verizon Media in its sole discretion.

Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

Severity (low)	Severity (high)	CWE-ID	Common Weakness Enumeration	Bug Examples
Critical	Critical	CWE-78	OS Command Injection	Remote Code Execution; Code Injection; LDAP Injection
Critical	Critical	CWE-120	Classic Buffer Overflow	Buffer Overflow
High	Critical	CWE-89	SQL Injection	SQL Injection
Medium	Critical	CWE-918	Server-Side Request Forgery	SSRF (unrestricted); Content-Restricted SSRF; Error-based SSRF (true/false); Blind SSRF
High	Critical	CWE-732	Incorrect Permission Assignment for Critical Resource	IDOR; Horizontal Privilege Escalation; Vertical Privilege Escalation

Locate Subsidiaries

- When conducting a large scale penetration test identifying subsidiaries allows for a significantly larger attack surface
- Useful Sites:
  - https://www.crunchbase.com/organization/companyName



Sub-Organizations

Number of Sub-Orgs

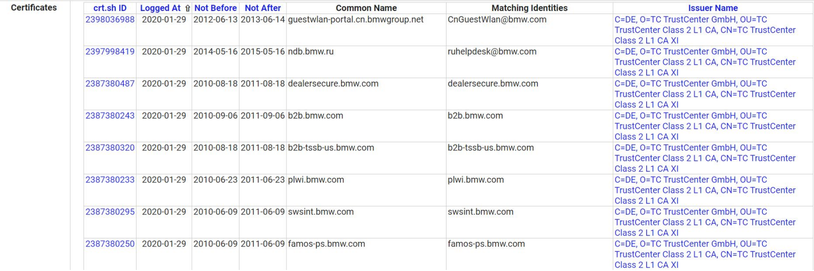
6

Which industries do these Sub-Organization operate in?

Rolls-Royce plc Subsidiary	BMW.com Subsidiary
BMW i Ventures Investment Arm	BMW Brilliance Automotive Subsidiary
BMW Australia Subsidiary	Alphabet Business Mobility Division

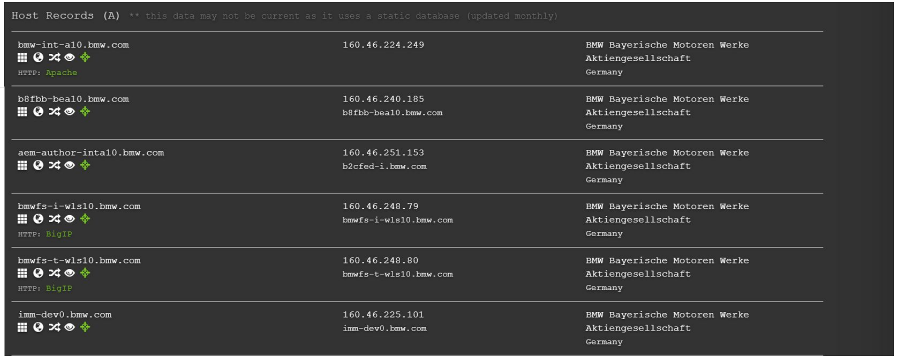
Subdomain Enumeration

- Subdomain - simply a domain that is a part of another domain
  - Examples: mail.google.com, portal.itsli.albany.edu, ast.pdp.albany.edu
- Often host unique (and possibly vulnerable) services
- Useful Sites:
  - https://talosintelligence.com/
  - https://dnsdumpster.com/
  - https://crt.sh/?q=domain.tld



Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
2398036988	2020-01-29	2012-06-13	2013-06-14	guestwlan-portal.cn.bmwgroup.net	CnGuestWlan@bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2397998419	2020-01-29	2014-05-16	2015-05-16	ndb.bmw.ru	ruhelpdesk@bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380487	2020-01-29	2010-08-18	2011-08-18	dealersecure.bmw.com	dealersecure.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380243	2020-01-29	2010-09-06	2011-09-06	b2b.bmw.com	b2b.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380320	2020-01-29	2010-08-18	2011-08-18	b2b-tssb-us.bmw.com	b2b-tssb-us.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380233	2020-01-29	2010-06-23	2011-06-23	plwi.bmw.com	plwi.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380295	2020-01-29	2010-06-09	2011-06-09	swsint.bmw.com	swsint.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI
2387380250	2020-01-29	2010-06-09	2011-06-09	famos-ps.bmw.com	famos-ps.bmw.com	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 L1 CA, CN=TC TrustCenter Class 2 L1 CA XI

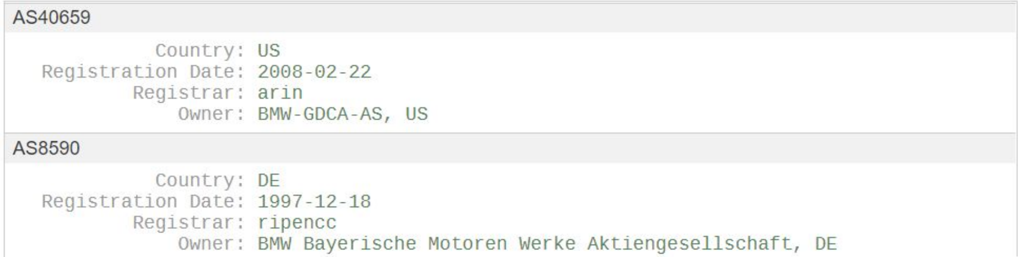


Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

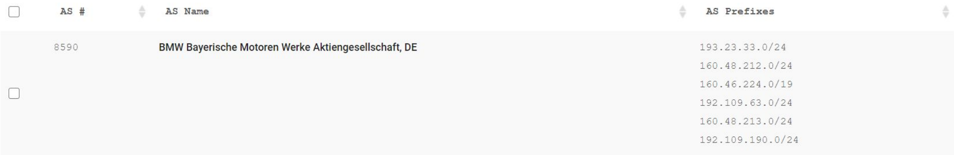
bmw-int-a10.bmw.com HTTP: Apache	160.46.224.249	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
b8fbb-bea10.bmw.com	160.46.240.185 b8fbb-bea10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
aem-author-inta10.bmw.com	160.46.251.153 b2cfed-i.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
bmwfs-i-wls10.bmw.com HTTP: BigIP	160.46.248.79 bmwfs-i-wls10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
bmwfs-t-wls10.bmw.com HTTP: BigIP	160.46.248.80 bmwfs-t-wls10.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany
imm-dev0.bmw.com	160.46.225.101 imm-dev0.bmw.com	BMW Bayerische Motoren Werke Aktiengesellschaft Germany

Autonomous System Number (ASN)

- ASN - Put simply, is a set of ip ranges under control of an organization
- Useful Sites:
  - Find an ASN: https://www.ultratools.com/tools/asnInfo
  - ASN to CIDR Range(IP range): https://hackertarget.com/as-ip-lookup/



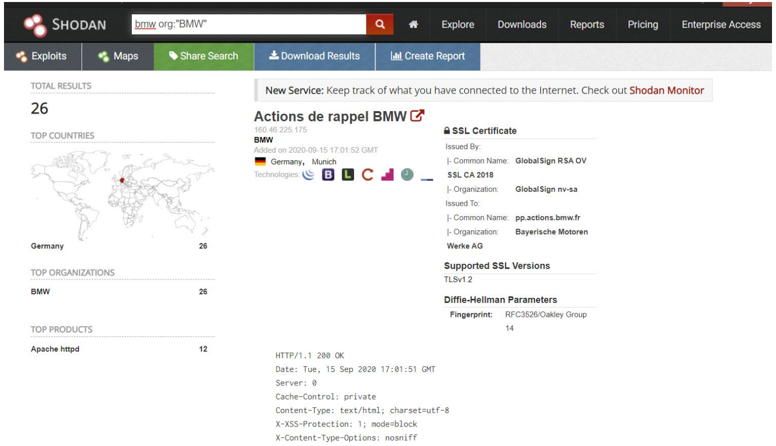
```
AS40659
              Country: US
    Registration Date: 2008-02-22
            Registrar: arin
                Owner: BMW-GDCA-AS, US
AS8590
              Country: DE
    Registration Date: 1997-12-18
            Registrar: ripencc
                Owner: BMW Bayerische Motoren Werke Aktiengesellschaft, DE
```



□	AS #	AS Name	AS Prefixes
□	8590	BMW Bayerische Motoren Werke Aktiengesellschaft, DE	193.23.33.0/24 160.48.212.0/24 160.46.224.0/19 192.109.63.0/24 160.48.213.0/24 192.109.190.0/24

Service Discovery

- Websites such as Shodan index most of the public internet. They can be used to identify what's running on assets quickly.
- Useful Sites:
  - https://shodan.io/
  - https://censys.io/



TOTAL RESULTS

26

TOP COUNTRIES

Germany	26

TOP ORGANIZATIONS

BMW	26

TOP PRODUCTS

Apache httpd	12

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Actions de rappel BMW

160.46.225.175
BMW
Added on 2020-09-15 17:01:52 GMT
Germany, Munich
Technologies:

SSL Certificate

Issued By:
|- Common Name: GlobalSign RSA OV SSL CA 2018
|- Organization: GlobalSign nv-sa
Issued To:
|- Common Name: pp.actions.bmw.fr
|- Organization: Bayerische Motoren Werke AG

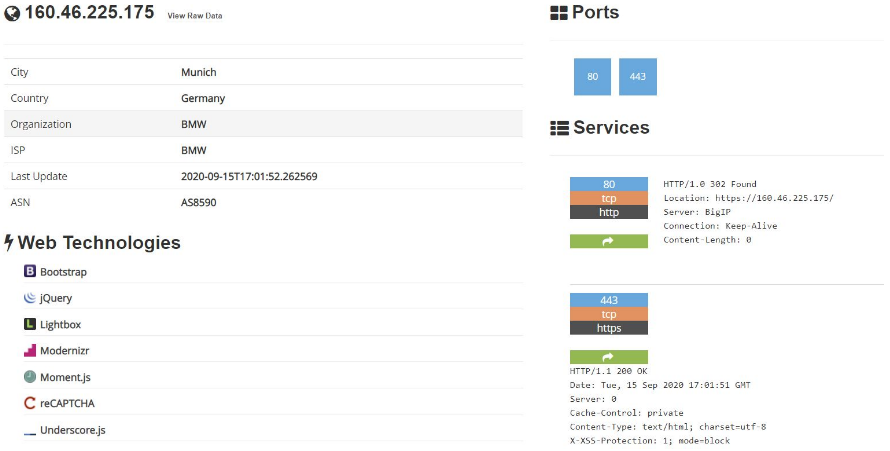
Supported SSL Versions

TLSv1.2

Diffie-Hellman Parameters

Fingerprint: RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Tue, 15 Sep 2020 17:01:51 GMT
Server: 0
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
```



160.46.225.175

City	Munich
Country	Germany
Organization	BMW
ISP	BMW
Last Update	2020-09-15T17:01:52.262569
ASN	AS8590

Web Technologies

- Bootstrap
- jQuery
- Lightbox
- Modernizr
- Moment.js
- reCAPTCHA
- Underscore.js

Ports

80 443

Services

80 tcp http

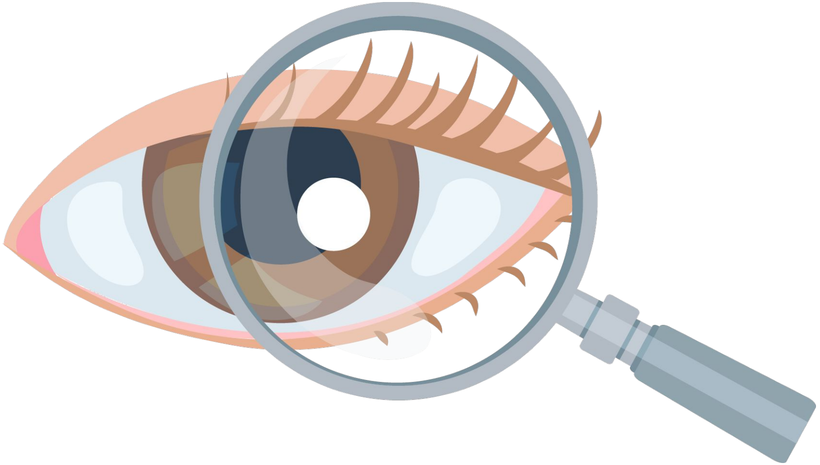
```
HTTP/1.0 302 Found
Location: https://160.46.225.175/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
```

443 tcp https

```
HTTP/1.1 200 OK
Date: Tue, 15 Sep 2020 17:01:51 GMT
Server: 0
Cache-Control: private
Content-Type: text/html; charset=utf-8
X-XSS-Protection: 1; mode=block
```

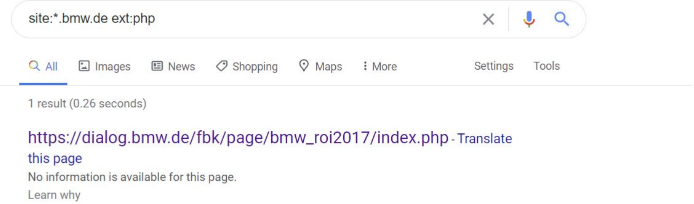
Sensitive Information Discovery

- Sensitive Information - access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others
- Google can help us find some interesting things ;)



Google Dorking

- Using Google's (or any other search engine) indexing capability to find information that should not be found
- Syntax:
  - AND is always implied.
  - OR: Escobar (Narcotics OR Cocaine)
  - "-" = NOT: Escobar -Pablo
  - "+" = MUST: Escobar +Roberto
  - Use quotes for exact phrase matching: “Cocaine is Bad”
- Example Dorks: mail/u/0 filetype:pdf, site:*.domain.tld ext:txt
- Useful Sites:
  - https://www.exploit-db.com/google-hacking-database


site:*.bmw.de ext:php

1 result (0.26 seconds)

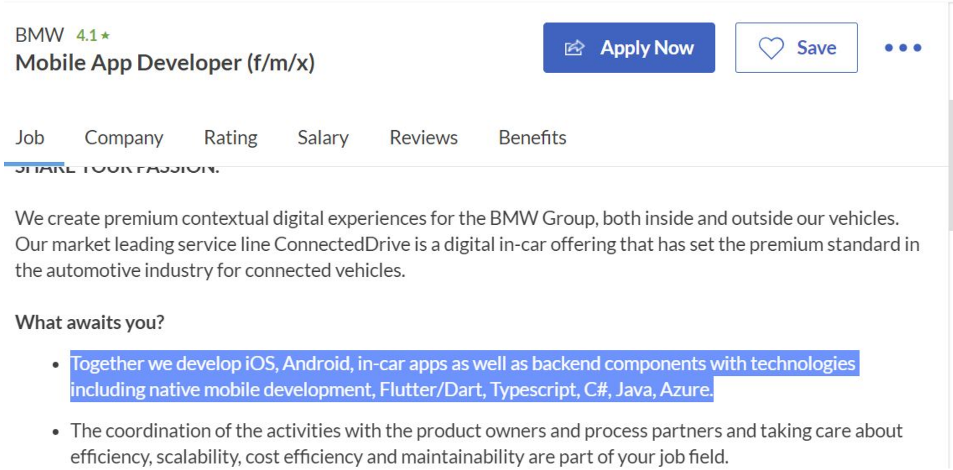
https://dialog.bmw.de/fbk/page/bmw_roi2017/index.php - Translate this page

No information is available for this page.

Learn why

Job Postings

- Company job listings are a great way to find what technologies the company uses
- Useful Sites:
  - ○ https://www.linkedin.com/jobs
  - ○ https://glassdoor.com
  - ○ https://indeed.com



Mobile App Developer (f/m/x)

SHARE YOUR PASSION:

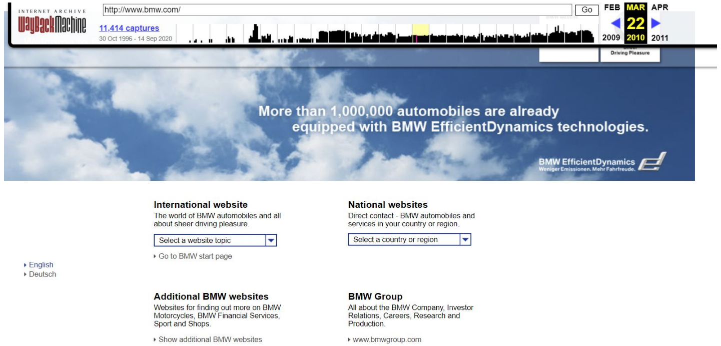
We create premium contextual digital experiences for the BMW Group, both inside and outside our vehicles. Our market leading service line ConnectedDrive is a digital in-car offering that has set the premium standard in the automotive industry for connected vehicles.

What awaits you?

- Together we develop iOS, Android, in-car apps as well as backend components with technologies including native mobile development, Flutter/Dart, Typescript, C#, Java, Azure.
- The coordination of the activities with the product owners and process partners and taking care about efficiency, scalability, cost efficiency and maintainability are part of your job field.

Archiving Services

- Archiving services enable an attacker to find out dated information and endpoints
- Outdated endpoints are some times vulnerable to web attacks such as SQL Injection
- Useful sites:
  - https://archive.org
  - https://waybackmachine.com



More than 1,000,000 automobiles are already equipped with BMW EfficientDynamics technologies.

International website

The world of BMW automobiles and all about sheer driving pleasure.

Go to BMW start page

National websites

Direct contact - BMW automobiles and services in your country or region.

Additional BMW websites

Websites for finding out more on BMW Motorcycles, BMW Financial Services, Sport and Shops.

Show additional BMW websites

BMW Group

All about the BMW Company, Investor Relations, Careers, Research and Production.

www.bmwgroup.com

The Art of Social Engineering

“the psychological manipulation of people into performing actions or divulging confidential information”

- Common applications:
  - Spear Phishing - the fraudulent practice of sending emails ostensibly **from a known or trusted sender** in order to induce targeted individuals **to reveal confidential information/perform certain actions**.
  - Voice
  - Physical/oral

Kevin Mitnick

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W72144602I).

NAME: ....MITNICK, KEVIN DAVID

AKA(S): ....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex:....................MALE
Race:....................WHITE
Place of Birth:....................VAN NUYS, CALIFORNIA
Date(s) of Birth:....................08/06/63; 10/18/70
Height:....................5'11"
Weight:....................190
Eyes:....................BLUE
Hair:....................BROWN
Skintone:....................LIGHT
Scars, Marks, Tattoos:....................NONE KNOWN
Social Security Number (s):....................550-39-5495
NCIC Fingerprint Classification:....................DOPMDOPM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9212-1112-0154-C

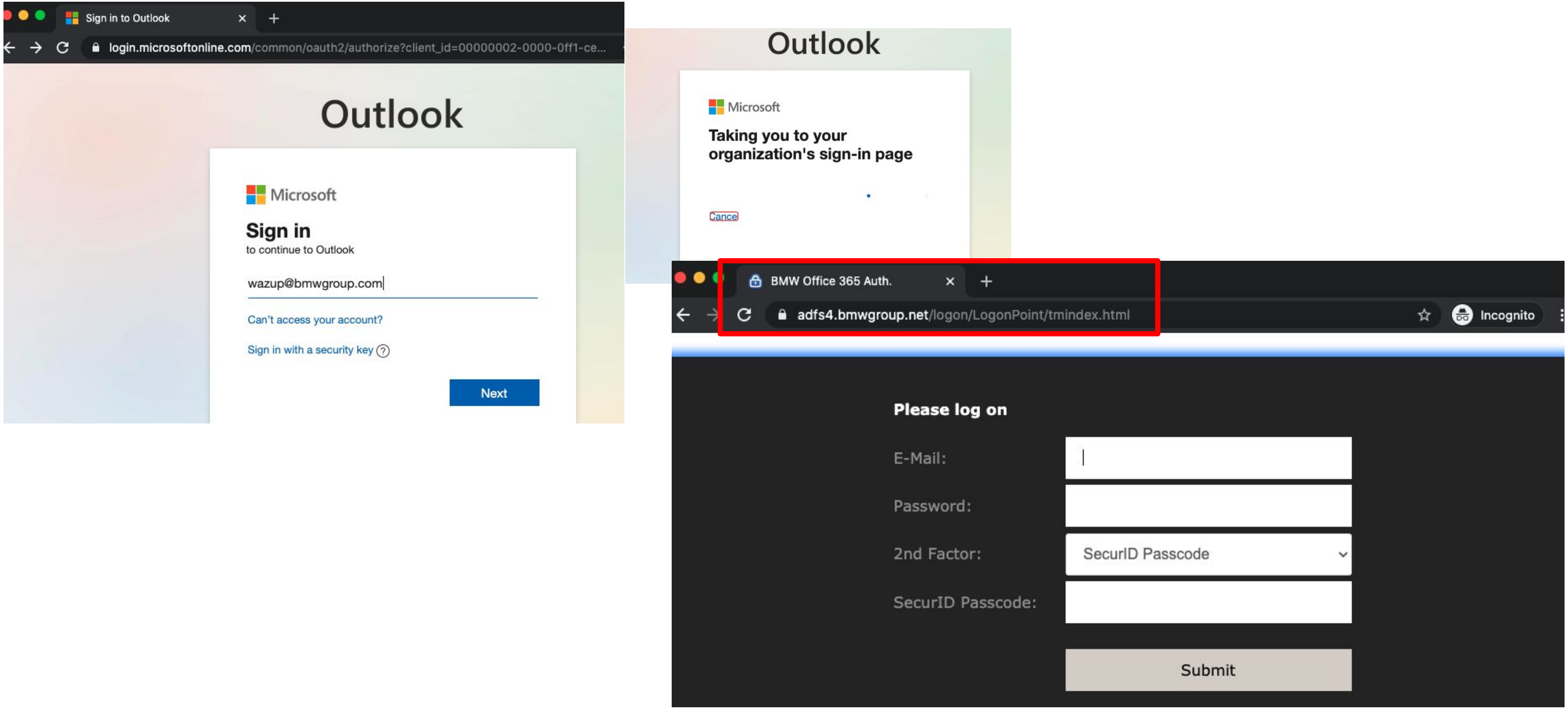
DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

Identifying Targets

- Identifying employees and associated titles
- Identifying email services (eg. Office365)
- Identifying email address format (eg. John Doe = jdoe@ecorp.com)
- Google Dorks:
  - site:facebook.com intext:" works at BMW Group"
  - site:linkedin.com intext:" works at BMW Group"
  - intext:"@bmwgroup.com"
- Useful Sites & Tools:
  - Rocketreach.co
  - theHarvester
  - ReconNG
  - Skrapp.io (addon for chrome)
  - Linkedin.com

Identifying Email Services



Sign in to Outlook

login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce...

Outlook

Microsoft

Sign in

to continue to Outlook

wazup@bmwgroup.com

Can't access your account?

Sign in with a security key ?

Next

Outlook

Microsoft

Taking you to your organization's sign-in page

Cancel

BMW Office 365 Auth.

adfs4.bmwgroup.net/logon/LogonPoint/tmindex.html

Incognito

Please log on

E-Mail:

Password:

2nd Factor: SecurID Passcode

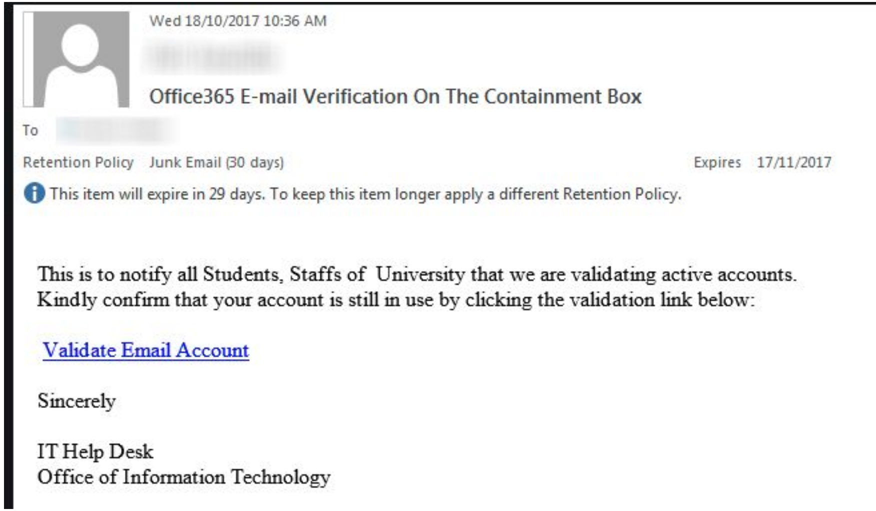
SecurID Passcode:

Submit

Crafting a Scenario

- Using previous recon to craft a believable scenario
  - Eg. What email/management system is your target using? Office 365?
  - Can you impersonate an email service internal upgrade?
- What domain will you be using to sent the email?
  - Is it relatable to the target domain or to your scenario? (eg. bmw.it.internal.com)
- Identify email logos and fonts to increase believability
  - Involves active reconnaissance
- Common domain tricks
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

Spear-Phishing Examples



Wed 18/10/2017 10:36 AM

[redacted]

Office365 E-mail Verification On The Containment Box

To [redacted]

Retention Policy Junk Email (30 days) Expires 17/11/2017

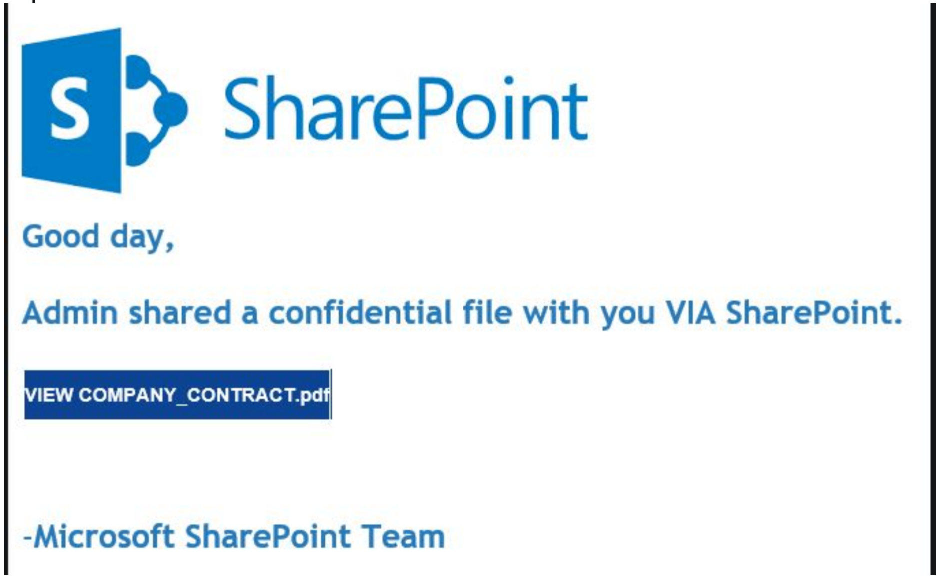
ⓘ This item will expire in 29 days. To keep this item longer apply a different Retention Policy.

This is to notify all Students, Staffs of University that we are validating active accounts. Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

IT Help Desk
Office of Information Technology



SharePoint

Good day,

Admin shared a confidential file with you VIA SharePoint.

VIEW COMPANY_CONTRACT.pdf

-Microsoft SharePoint Team

Ethics

- Adhere to scope outlined in the worksheet. If any vulnerabilities are found report it to the corresponding company.
- Members are obligated to act accordingly with laws and school rules. Any indication that a member is doing something unethical may lead to the individual being removed from the team or banned from meetings
- We do not condone any form of illegal activity.

Q&A

Activity

- Worksheet - shorturl.at/uJ057