MIA TEAM REPORT – Cyber security

Case Overview

The RSA Security division of the EMC Corporation said that it had suffered a sophisticated data breach, potentially compromising computer security products widely used by corporations and governments. The company, which pioneered an advanced cryptographic system during the 1980s, sells products that offer stronger computer security than simple password protection. Known as multifactor authentication, the technology is typically based on an electronic token carried by a user that repeatedly generates a time-based number that must be appended to a password when a user logs in to a computer system.

Newspaper extract regarding the occurrence says that “RSA, which is based in Bedford, Mass., posted an urgent message on its Web site on Thursday referring to an open letter from its chairman, Art Coviello. The letter acknowledged that the company had suffered from an intrusion Mr. Coviello described as an “advanced persistent threat. Mr. Coviello said that the company’s investigation had revealed that the intruder successfully stole digital information from the company that was related to RSA’s SecurID two-factor authentication products”. Furthermore Mr. Coviello added that “We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.” Actually the intruder could produce cards that duplicate the ones supplied by RSA, making it possible to gain access to corporate networks and computer systems.

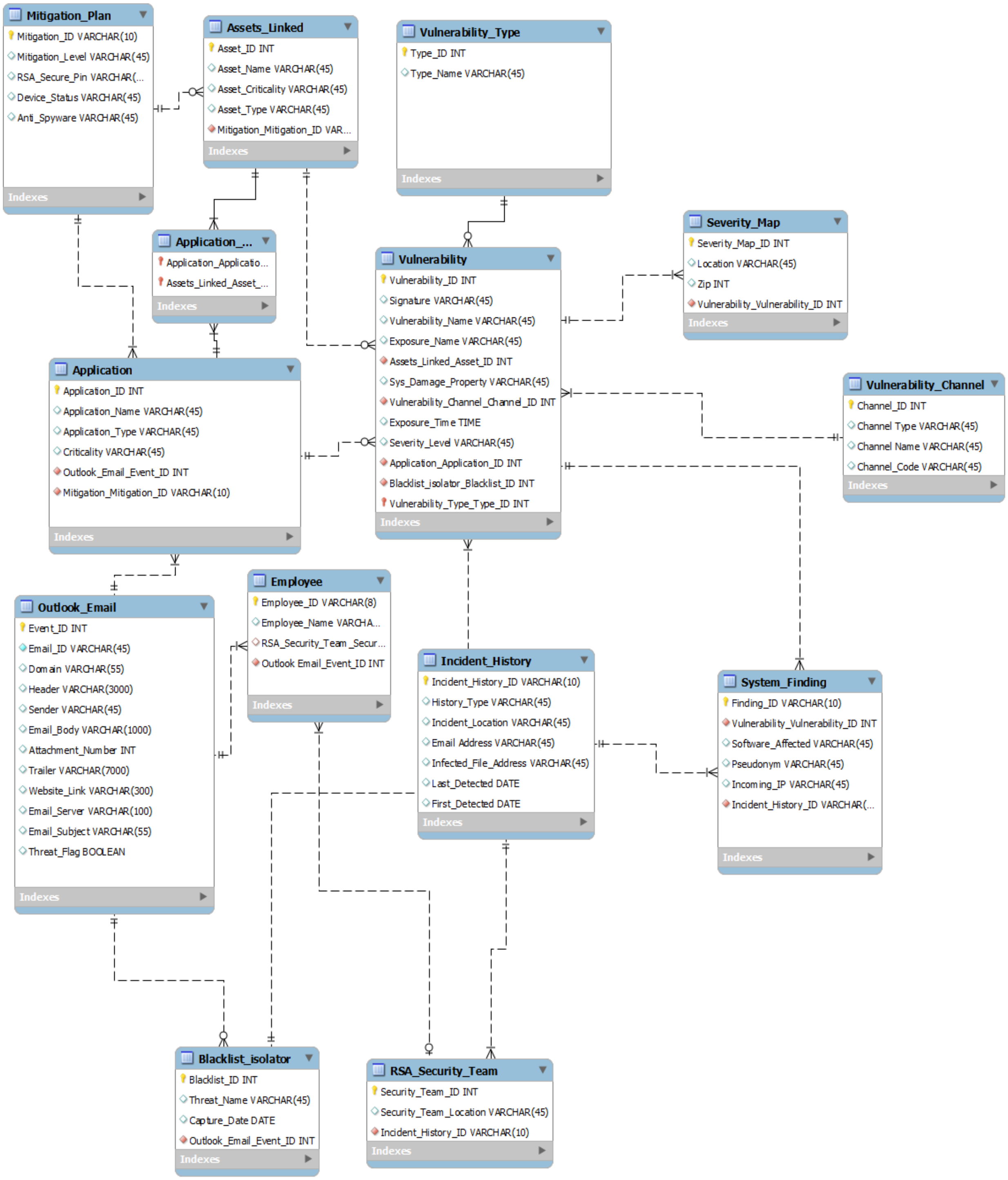
Problem:

A security division of EMC-RSA was infiltrated by an attacker that sent a phishing e-mail with an attached Microsoft Excel spreadsheet file to several RSA employees. The infected file contained malware that had the ability to steal passwords and sensitive data. This cyberattack was responsible for stealing the important and confidential company data.

Solution:

We are designing an efficient database design to tackle this issue in future. We will be having a history of all the attack related data. Example: The subject line of the e-mail, sender details etc. We will also have a Vulnerability table with the vulnerability details. Moreover, we are planning to create an alert system to track such harmful e-mails in future and protect the system. We will be dealing with System impact, Mitigation Methodology, Damage information and details about the threat.

ER Diagram Model



Explaining Few Entities of our ER Model

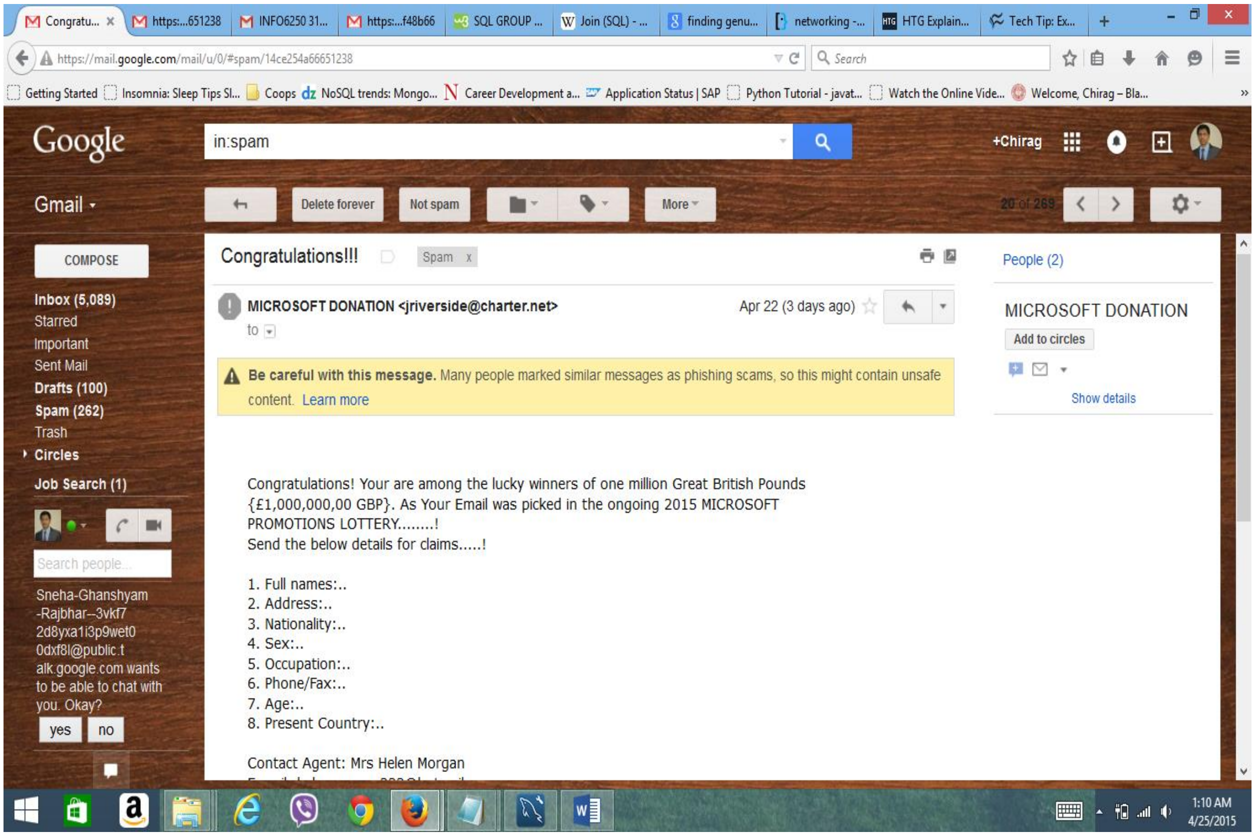
- Mitigation: The action of reducing the severity, seriousness, or painfulness of the threat.
- Vulnerability: Threat which is resolved into various other types.
- Severity: The state or quality of being severe. Basically, harshness or intensity of a threat.
- Assets: The property owned by a person or company on which threat may or may not attack.
- Blacklist Isolator: It will filter out the emails if it contains any threats or not.
- Incident history: Tracing out the history of a particular threat.
- System_Finding : System will give more details about Incoming threats IP Address, Pseudo name etc.

Entities	Relationship
Mitigation_Plan - Application	One-Many (Mandatory)
Application-Mitigation	Many-One (Mandatory)
Mitigation_Plan-Assets_Link	One-Many(Optional)
Assets_Link- Mitigation_Plan	Many-One (Mandatory)
Application-Vulnerability	One-Many(Optional)
Vulnerability-Application	Many-One(Mandatory)
Outlook_Email-Employee	One-Many(Mandatory)
Employee- Outlook_Email	Many-One(Mandatory)
Outlook_Email-Blacklist_Isolator	One-Many(Optional)
Blacklist_Isolator- Outlook_Email	Many-One(Mandatory)
Blacklist_Isolator-Vulnerability	One-Many (Mandatory)
Vulnerability- Blacklist_Isolator-	Many-One(Mandatory)
RSA_Security_Team-Employee	One-Many (Mandatory)
Employee- RSA_Security_Team	Many-One(Optional)
RSA_Security_Team-Incident_History	Many-One(Mandatory)
Incident_History- RSA_Security_Team-	One-Many(Mandatory)
Incident_History-System_Finding	One-Many (Mandatory)
System_Finding-Incident_History	Many-One(Mandatory)
System_Finding- Vulnerability	Many-One(Mandatory)
Vulnerability- System_Finding	One-Many (Mandatory)
Vulnerability- Vulnerability_Channel	Many-One(Mandatory)
Vulnerability_Channel- Vulnerability	One-Many (Mandatory)
Vulnerability-Severity_Map	One-Many (Mandatory)
Severity_Map- Vulnerability	Many-One(Mandatory)
Vulnerability- Vulnerability_Type	Many-One(Mandatory)

Vulnerability_Type- Vulnerability	**One-Many(Optional)**
Vulnerability-Assets_Link	**Many-One(Mandatory)**
Assets_Link- Vulnerability	**One-Many(Optional)**

1. **Phishing** is the illegal attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Example of Spam Email



Congratulations!!! Spam x

MICROSOFT DONATION <jriverside@charter.net>
to

Apr 22 (3 days ago)

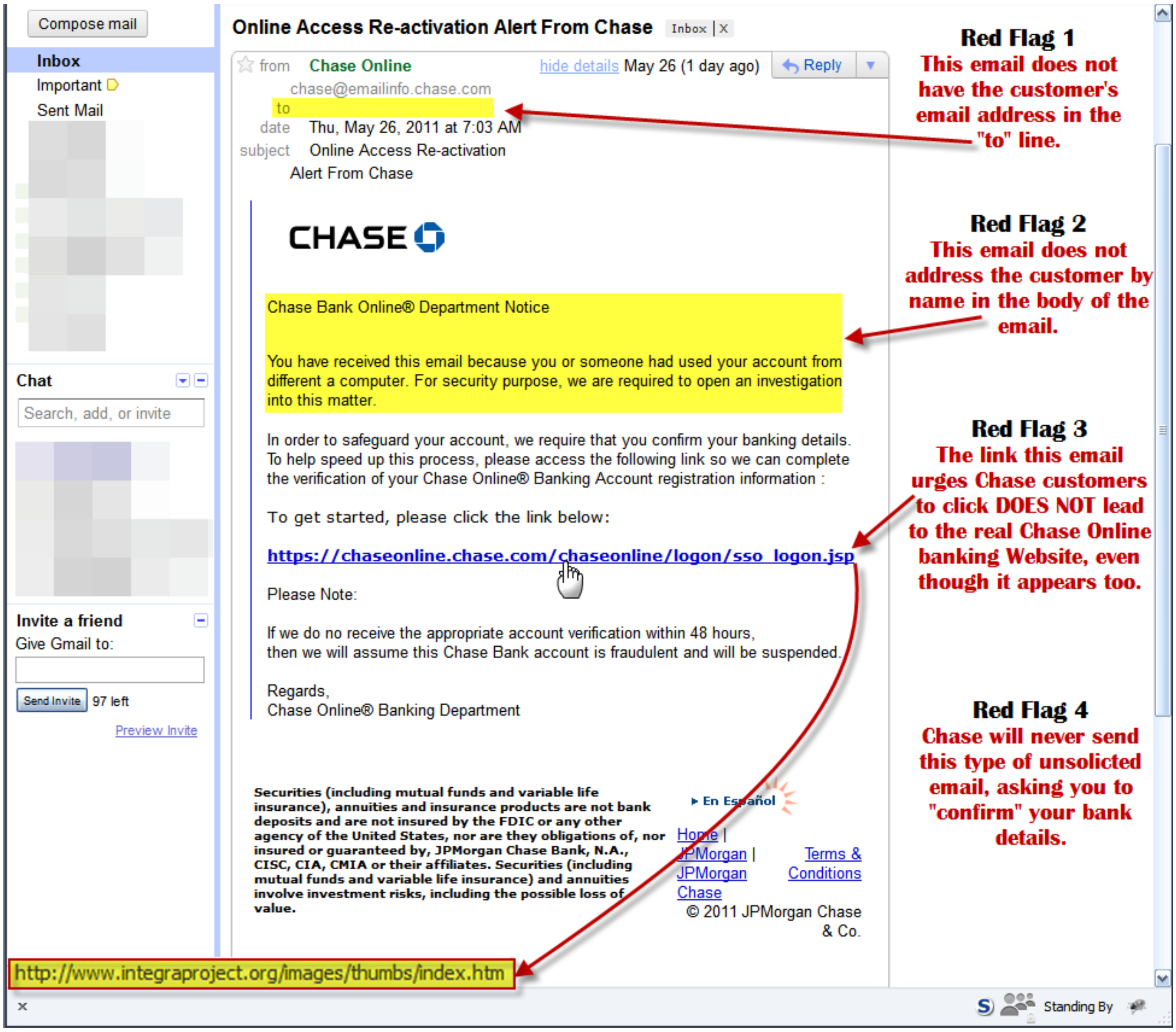
Be careful with this message. Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

Sneha-Ghanshyam-Rajbhar--3vkf72d8yxa1i3p9wet00dxf8l@public.talk.google.com wants to be able to chat with you. Okay?

Congratulations! Your are among the lucky winners of one million Great British Pounds {£1,000,000,00 GBP}. As Your Email was picked in the ongoing 2015 MICROSOFT PROMOTIONS LOTTERY........!
Send the below details for claims.....!

1. Full names:..
2. Address:..
3. Nationality:..
4. Sex:..
5. Occupation:..
6. Phone/Fax:..
7. Age:..
8. Present Country:..

Contact Agent: Mrs Helen Morgan



Online Access Re-activation Alert From Chase

from Chase Online
chase@emailinfo.chase.com
to
date Thu, May 26, 2011 at 7:03 AM
subject Online Access Re-activation Alert From Chase

May 26 (1 day ago)

CHASE

Chase Bank Online® Department Notice

You have received this email because you or someone had used your account from different a computer. For security purpose, we are required to open an investigation into this matter.

In order to safeguard your account, we require that you confirm your banking details. To help speed up this process, please access the following link so we can complete the verification of your Chase Online® Banking Account registration information :

To get started, please click the link below:

https://chaseonline.chase.com/chaseonline/logon/sso_logon.jsp

Please Note:

If we do no receive the appropriate account verification within 48 hours, then we will assume this Chase Bank account is fraudulent and will be suspended.

Regards,
Chase Online® Banking Department

Securities (including mutual funds and variable life insurance), annuities and insurance products are not bank deposits and are not insured by the FDIC or any other agency of the United States, nor are they obligations of, nor insured or guaranteed by, JPMorgan Chase Bank, N.A., CISC, CIA, CMIA or their affiliates. Securities (including mutual funds and variable life insurance) and annuities involve investment risks, including the possible loss of value.

▸ En Español

Home | JPMorgan | JPMorgan Chase   Terms & Conditions

© 2011 JPMorgan Chase & Co.

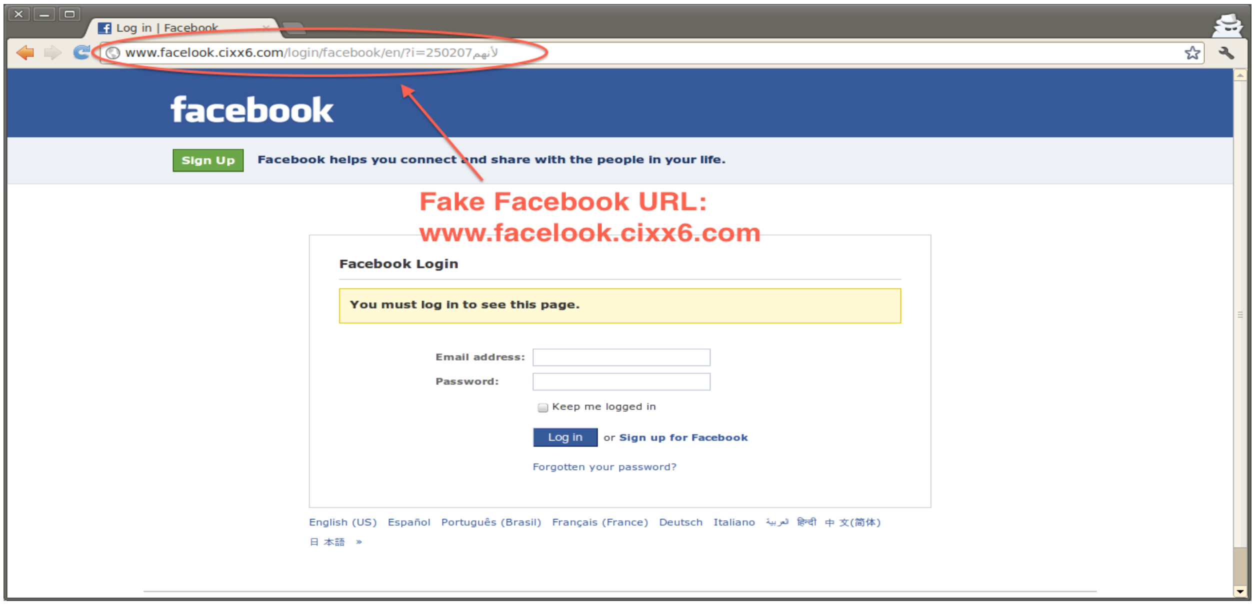
http://www.integraproject.org/images/thumbs/index.htm

Red Flag 1
This email does not have the customer's email address in the "to" line.

Red Flag 2
This email does not address the customer by name in the body of the email.

Red Flag 3
The link this email urges Chase customers to click DOES NOT lead to the real Chase Online banking Website, even though it appears too.

Red Flag 4
Chase will never send this type of unsolicted email, asking you to "confirm" your bank details.


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Log in
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »

Facebook helps you connect and share with the people in your life.

Fake Facebook URL:
www.facelook.cixx6.com

Facebook Login

You must log in to see this page.

Email address:

Password:

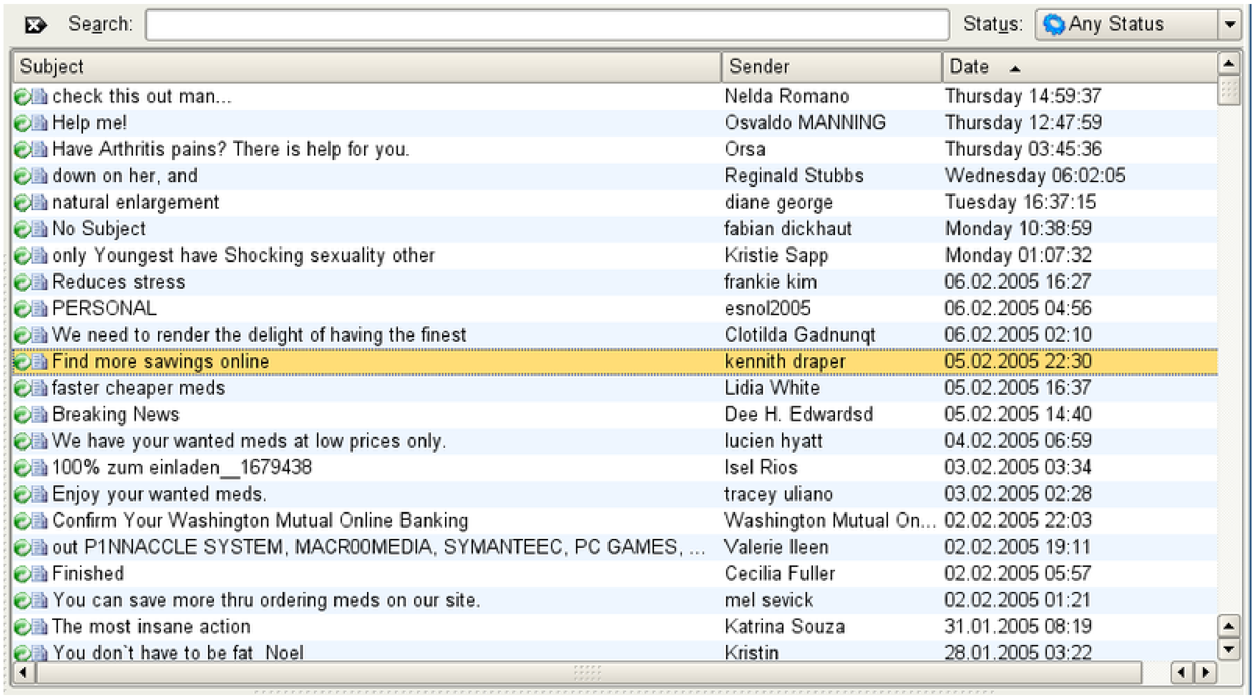
□ Keep me logged in

Log in or Sign up for Facebook

Forgotten your password?

2. Spamming

   Electronic spamming is the use of electronic messaging systems to send unsolicited messages (**spam**), especially advertising, as well as sending messages repeatedly on the same site. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam,online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social spam, television advertising and file sharing spam.



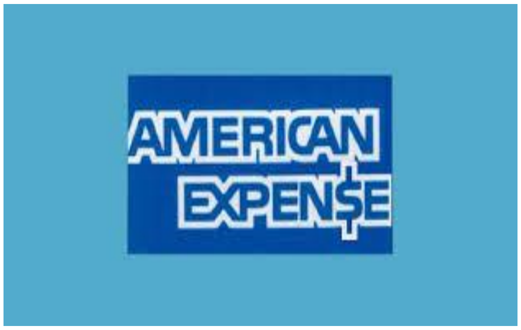
Search: Status: Any Status

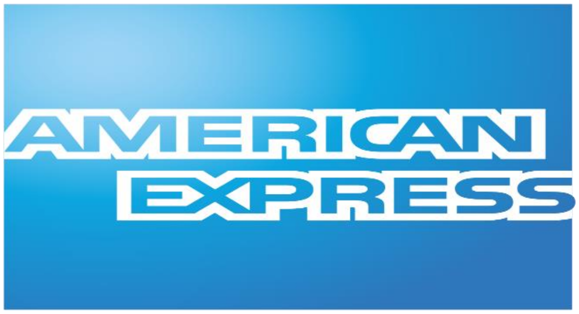
Subject	Sender	Date
check this out man...	Nelda Romano	Thursday 14:59:37
Help me!	Osvaldo MANNING	Thursday 12:47:59
Have Arthritis pains? There is help for you.	Orsa	Thursday 03:45:36
down on her, and	Reginald Stubbs	Wednesday 06:02:05
natural enlargement	diane george	Tuesday 16:37:15
No Subject	fabian dickhaut	Monday 10:38:59
only Youngest have Shocking sexuality other	Kristie Sapp	Monday 01:07:32
Reduces stress	frankie kim	06.02.2005 16:27
PERSONAL	esnol2005	06.02.2005 04:56
We need to render the delight of having the finest	Clotilda Gadnunqt	06.02.2005 02:10
Find more sawings online	kennith draper	05.02.2005 22:30
faster cheaper meds	Lidia White	05.02.2005 16:37
Breaking News	Dee H. Edwardsd	05.02.2005 14:40
We have your wanted meds at low prices only.	lucien hyatt	04.02.2005 06:59
100% zum einladen__1679438	Isel Rios	03.02.2005 03:34
Enjoy your wanted meds.	tracey uliano	03.02.2005 02:28
Confirm Your Washington Mutual Online Banking	Washington Mutual On...	02.02.2005 22:03
out P1NNACCLE SYSTEM, MACR00MEDIA, SYMANTEEC, PC GAMES, ...	Valerie Ileen	02.02.2005 19:11
Finished	Cecilia Fuller	02.02.2005 05:57
You can save more thru ordering meds on our site.	mel sevick	02.02.2005 01:21
The most insane action	Katrina Souza	31.01.2005 08:19
You don`t have to be fat Noel	Kristin	28.01.2005 03:22

Spoofing:

A spoofing attack **is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.** E-mail spoofing is the forgery of an e-mail header so that the message **appears to have originated from someone or somewhere other than** the actual source.

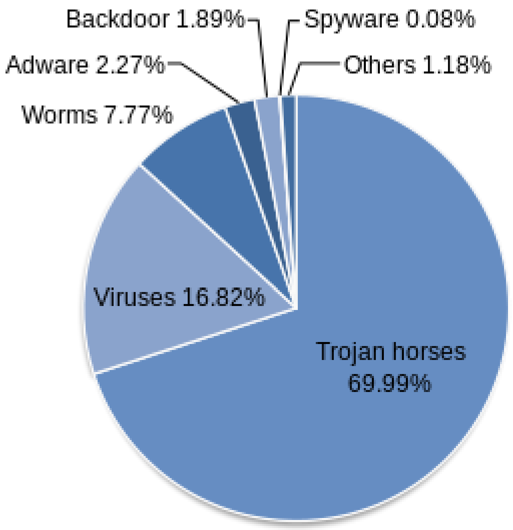
Spoofed Logo Actual Logo





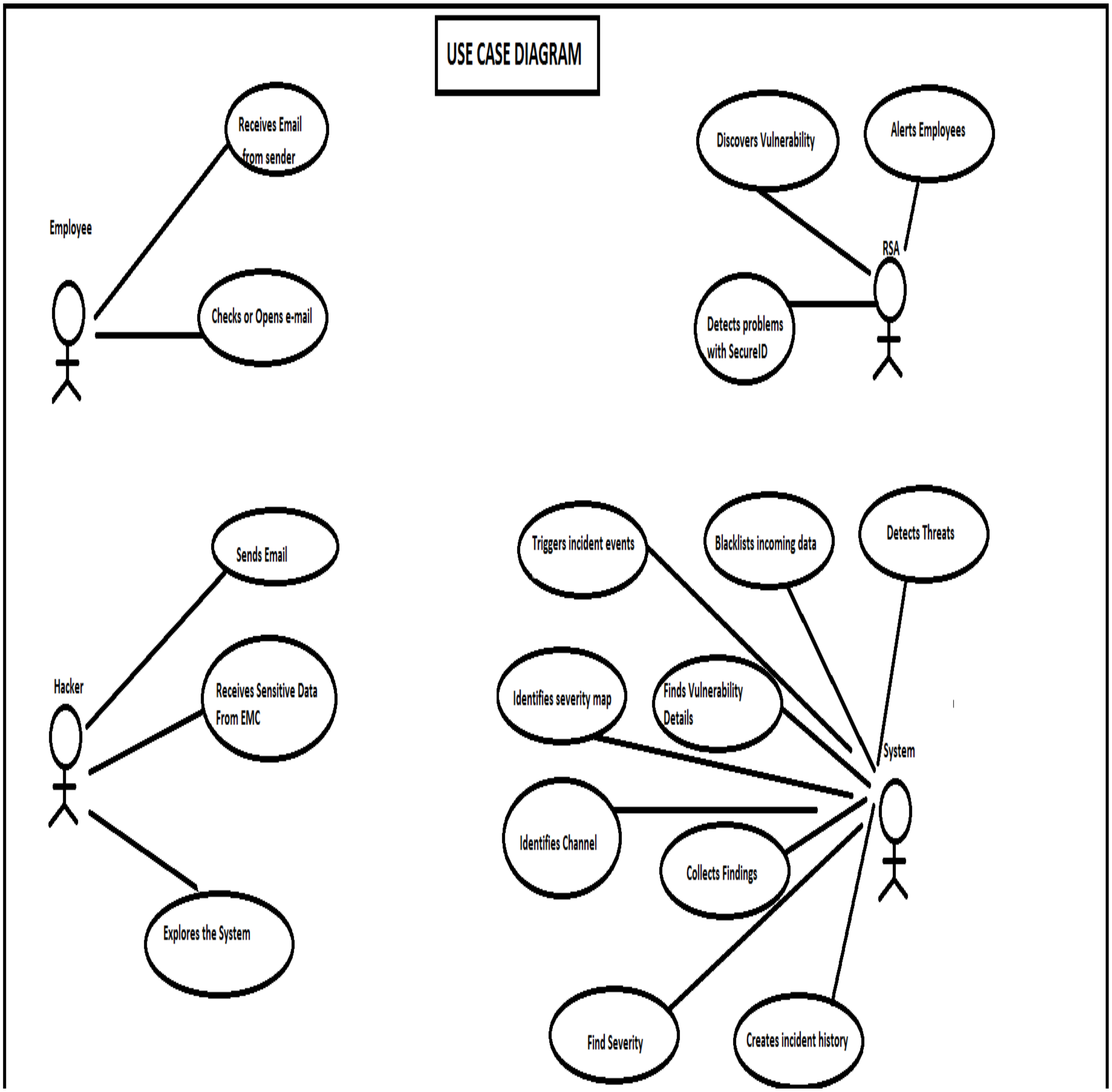
Malware

Malware is a category of malicious code that includes viruses, worms, and Trojan horses. **Malware**, short for **malicious software**, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.[1] Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.



Malware by categories March 16, 2011

Use Case

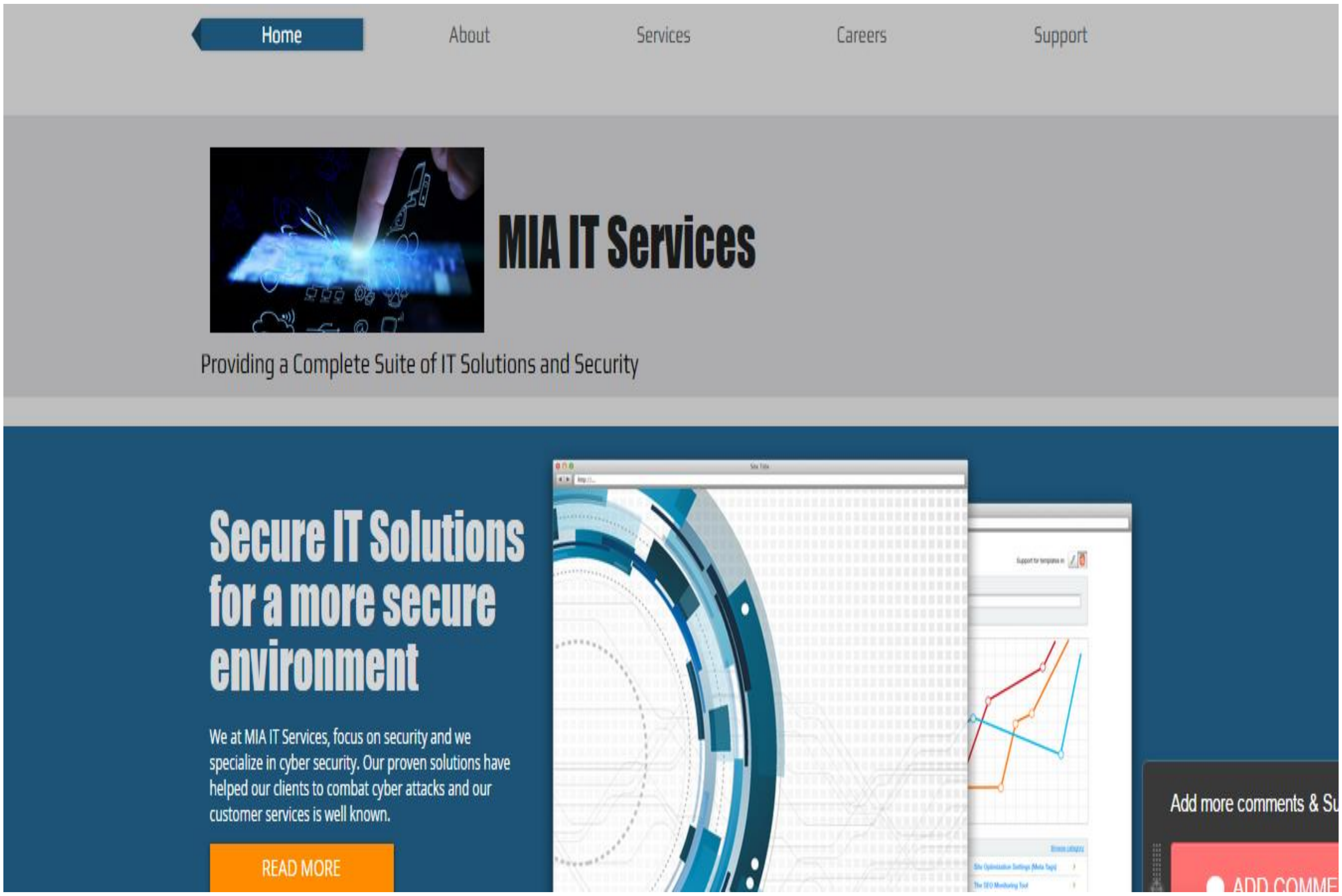

USE CASE DIAGRAM
Employee
Receives Email from sender
Checks or Opens e-mail
RSA
Discovers Vulnerability
Alerts Employees
Detects problems with SecureID
Hacker
Sends Email
Receives Sensitive Data From EMC
Explores the System
System
Triggers incident events
Blacklists incoming data
Detects Threats
Identifies severity map
Finds Vulnerability Details
Identifies Channel
Collects Findings
Find Severity
Creates incident history

User Interface

The link to our User Interface is as follows:-

http://bit.ly/1DUGRnY

Here are few Screen-shots from our User Interface

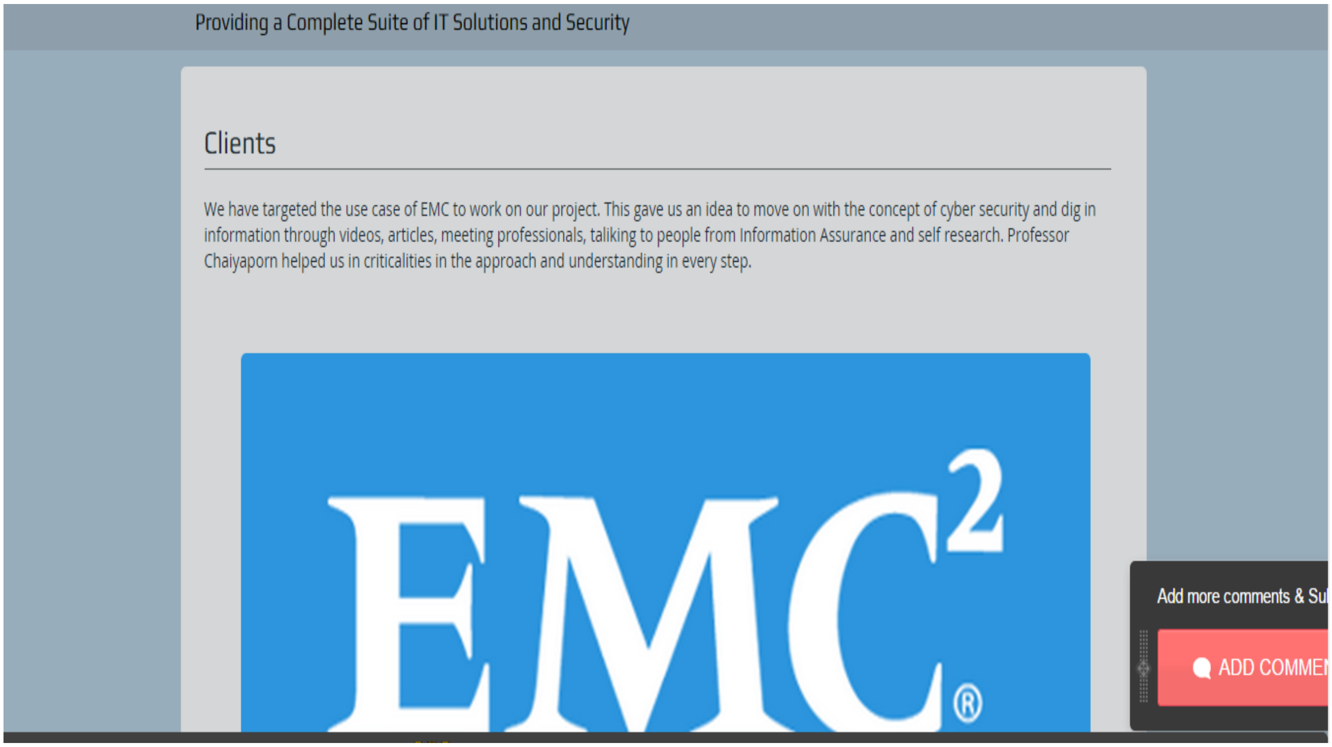


MIA IT Services

Providing a Complete Suite of IT Solutions and Security

Secure IT Solutions for a more secure environment

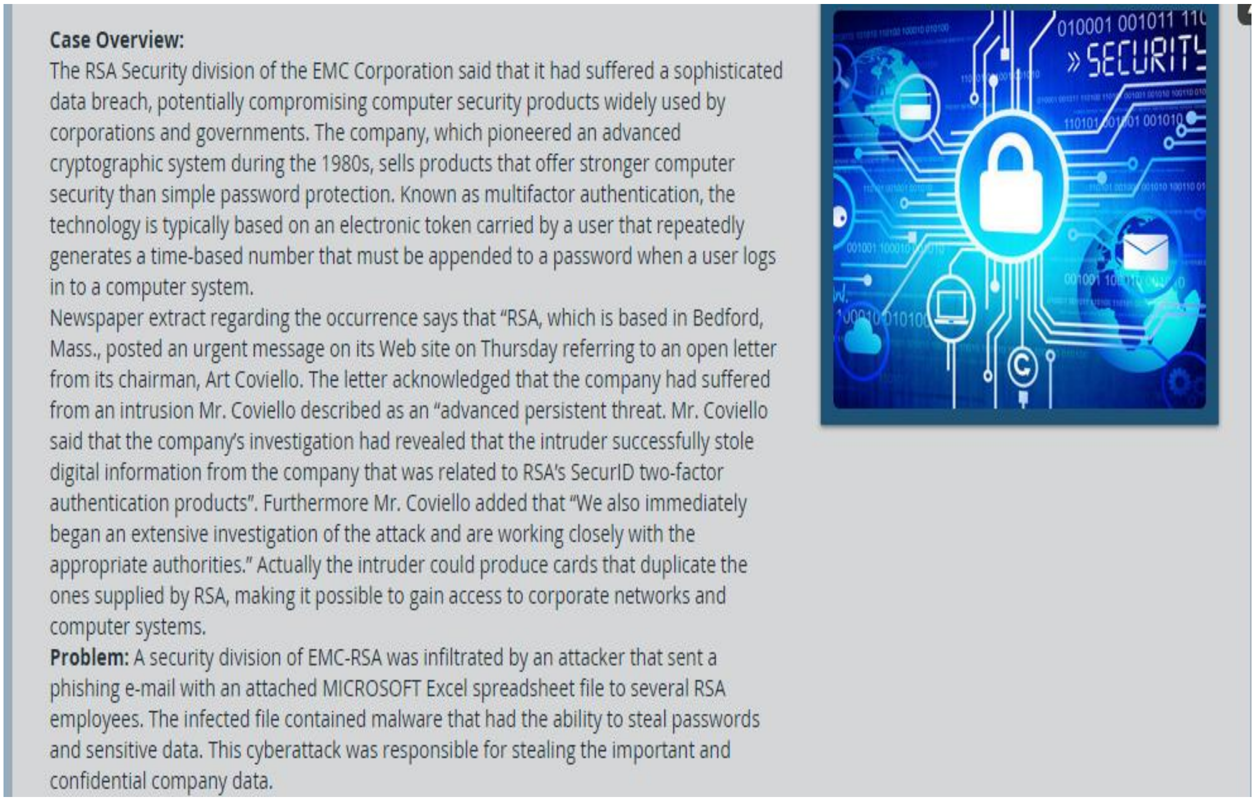
We at MIA IT Services, focus on security and we specialize in cyber security. Our proven solutions have helped our clients to combat cyber attacks and our customer services is well known.



Providing a Complete Suite of IT Solutions and Security

Clients

We have targeted the use case of EMC to work on our project. This gave us an idea to move on with the concept of cyber security and dig in information through videos, articles, meeting professionals, taliking to people from Information Assurance and self research. Professor Chaiyaporn helped us in criticalities in the approach and understanding in every step.



Case Overview:
The RSA Security division of the EMC Corporation said that it had suffered a sophisticated data breach, potentially compromising computer security products widely used by corporations and governments. The company, which pioneered an advanced cryptographic system during the 1980s, sells products that offer stronger computer security than simple password protection. Known as multifactor authentication, the technology is typically based on an electronic token carried by a user that repeatedly generates a time-based number that must be appended to a password when a user logs in to a computer system.
Newspaper extract regarding the occurrence says that "RSA, which is based in Bedford, Mass., posted an urgent message on its Web site on Thursday referring to an open letter from its chairman, Art Coviello. The letter acknowledged that the company had suffered from an intrusion Mr. Coviello described as an "advanced persistent threat. Mr. Coviello said that the company's investigation had revealed that the intruder successfully stole digital information from the company that was related to RSA's SecurID two-factor authentication products". Furthermore Mr. Coviello added that "We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities." Actually the intruder could produce cards that duplicate the ones supplied by RSA, making it possible to gain access to corporate networks and computer systems.
Problem: A security division of EMC-RSA was infiltrated by an attacker that sent a phishing e-mail with an attached MICROSOFT Excel spreadsheet file to several RSA employees. The infected file contained malware that had the ability to steal passwords and sensitive data. This cyberattack was responsible for stealing the important and confidential company data.

Span Header

```
Delivered-To: chirag91286@gmail.com
Received: by 10.170.95.197 with SMTP id m188csp40154yka;
        Sat, 7 Feb 2015 03:17:14 -0800 (PST)
X-Received: by 10.68.135.166 with SMTP id pt6mr1879544pbb.31.1423307834368;
        Sat, 07 Feb 2015 03:17:14 -0800 (PST)
Return-Path: <mwyatt2@liberty.edu>
Received: from na01-bn1-obe.outbound.protection.outlook.com (mail-
bn1bon0078.outbound.protection.outlook.com. [157.56.111.78])
        by mx.google.com with ESMTPS id fe2si13788695pab.97.2015.02.07.03.17.11
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
        Sat, 07 Feb 2015 03:17:14 -0800 (PST)
Received-SPF: pass (google.com: domain of mwyatt2@liberty.edu designates 157.56.111.78 as
permitted sender) client-ip=157.56.111.78;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of mwyatt2@liberty.edu designates 157.56.111.78 as
permitted sender) smtp.mail=mwyatt2@liberty.edu
Received: from BY2PR05MB952.namprd05.prod.outlook.com (10.141.220.153) by
 BY2PR05MB680.namprd05.prod.outlook.com (10.141.221.151) with Microsoft SMTP
 Server (TLS) id 15.1.75.20; Sat, 7 Feb 2015 11:17:08 +0000
SRVR:BY2PR05MB952;H:BY2PR05MB949.namprd05.prod.outlook.com;FPR:;SPF:None;ML
V:nov;PTR:InfoNoRecords;LANG:;
Content-Type: multipart/mixed; boundary="_004_142330781342985028libertyedu_"
MIME-Version: 1.0
X-MS-Exchange-CrossTenant-originalarrivaltime: 07 Feb 2015 11:17:06.0735
 (UTC)
X-MS-Exchange-CrossTenant-fromentityheader: Hosted
X-MS-Exchange-CrossTenant-id: baf8218e-b302-4465-a993-4a39c97251b2
```

```
<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Diso-8859-=
UEsDBBQABgAIAAAAIQAwWJrDuAEAAFwJAAATAAgCW0NvbnRlbnRfVHlwZXNdLnh
tbCCiBAIooAAC
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAADE
Vl1PwjAUfTfxPyx9NayAiTGG4YMfj0oi/oDS3kF1a5v2KvDvvdtgMQgbgSy+LGmae8655350
o/tV
nkXf4IO2JmGDuM8iMNIqbeYJe58+925ZFFAYJTJrIGFrCOx+fHkxmq4dhIiiTUjYAtHdcR7k
AnIR
YuvA0E1qfS6Qjn7OnZCfYg582O/fcGkNgsEeFhhsPHolAV4riCbC44vIiYcvrVc8tRaNRQgxw
bHo
oYorqBMmnMu0FEjC+bdRO6Q9m6ZagrLyKyequIBz3koIgVLLs7iGviqg+Xj0CKn4yjB6WpG
2yo4P
B/MdVp0XWZQX+2M8ZGEnpkXpxpqYIstswkK70KCq2YpNNgctrR1phjnB0Ro5F9ps9R/UE
XCddVHX
CreVHozqqLG2yE0SyKqJty5wao2zWxuKhlWgetTfDjxqqLvnsPuASHPQwVyFDXJT+vVsgx+
enf7e
yQZ/JP/1P/MP/o0faVcDL7/niyhhWi1fgFCdlLwCPpK/g5IfyZ/S+zUVswy6KPoGutWEJczeOpv
+
X+CtQirTzu+9PwugvRr1/pXWn1CM7YtdRO/Zurz8Nxr/AAAA//8DAFBLAwQUAAYACAA
AACEAHpEa
t/MAAABOAgAACwAIAl9yZWxzLy5yZWxzIKIEAiigAAIAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA

A Proper Header

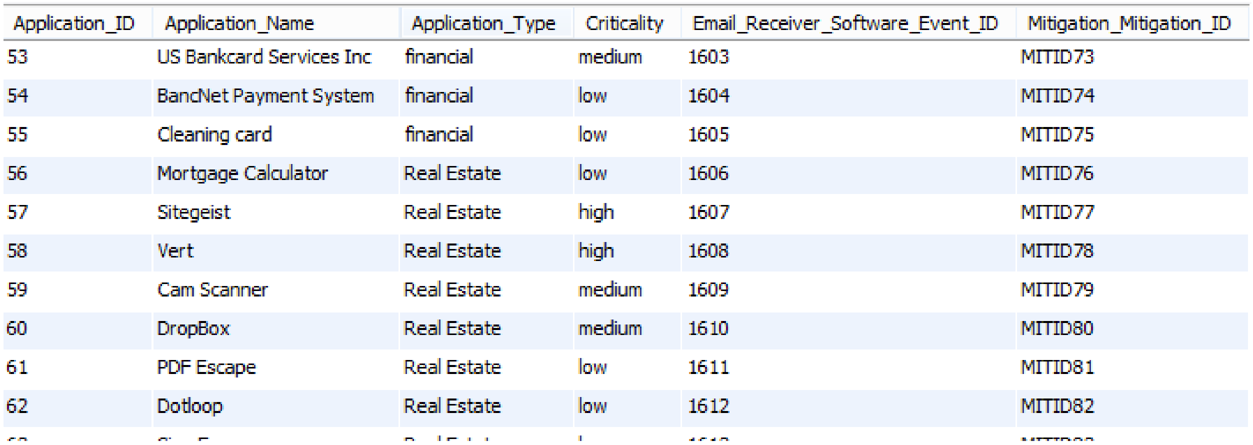
Delivered-To: gajiwala.c@husky.neu.edu Received: by 10.96.10.136 with SMTP id i8csp158362qdb; Fri, 24 Apr 2015 16:48:41 -0700 (PDT) X-Received: by 10.52.35.132 with SMTP id h4mr1515550vdj.65.1429919321760; Fri, 24 Apr 2015 16:48:41 -0700 (PDT) Return-Path: <do-not-reply@blackboard.com> Received: from mail-relay6-va2.blackboard.com (mail-relay6-va2.blackboard.com. [69.196.241.6]) by mx.google.com with ESMTPS id kk8si10888037vdb.31.2015.04.24.16.48.40 (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128); Fri, 24 Apr 2015 16:48:41 -0700 (PDT) Received-SPF: pass (google.com: domain of do-not-reply@blackboard.com designates 69.196.241.6 as permitted sender) Authentication-Results: mx.google.com; spf=pass (google.com: domain

of do-not-reply@blackboard.com designates 69.196.241.6 as permitted sender) smtp.mail=do-not-reply@blackboard.com; dkim=pass header.i=@blackboard.com Received: from fgprd-100802-9734-app001.mhint (fgprd-100802-9734-app001.mhint [10.5.7.0]) by mail-relay6-va2.blackboard.com (Sentrion-MTA-4.3.2/Sentrion-MTA-4.3.2) with ESMTP id t3ONma7M018700; Fri, 24 Apr 2015 23:48:36 GMT DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=blackboard.com; s=apr2011; t=1429919320; bh=9+MUtGJUdA4JD6eLMQxXnAO/4NgXxgrBvsv7evCbaNw=; h=Date:From:Reply-To:To:Subject;
b=AA2Arm03tUTt1Wwc9R2UV7i+jHN/8BsnuOd2Ig8Lnu6XapR7vtXOusexHhocjLRpz
xRhiJwDk9ciBPR7EaEb9nj1v/b7xeeRcPdYaveb/zbl5NrYhyTYRi0ncGUmfctmNAL
x0bitgTpsuqzRfGVBIXI3BXmsR805kPUNBS+ul0c= Date: Fri, 24 Apr 2015 19:48:36 -0400 (EDT) From: "Yusuf Ozbek - y.ozbek@neu.edu" <do-not-reply@blackboard.com> Reply-To: "Yusuf Ozbek -y.ozbek@neu.edu" <y.ozbek@neu.edu> To: "INFO6250.31767.201530":; Message-ID: <847807895.16818.1429919316197.JavaMail.bbuser@fgprd-100802-9734-app001.mhint> Subject: INFO6250 31767 Web Development Tools & Methds SEC 01 - Spring 2015 (INFO6250.31767.201530): MIDTERM PAPERS MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="----=_Part_16817_1988937105.1429919316180" ------=_Part_16817_1988937105.1429919316180 Content-Type: text/plain; charset=UTF-8 Content-Transfer-Encoding: 7bit
Hi all, I will be on campus sometime around noon. Please stop by if you have any doubts, or last minute questions about the Final Exam. I will bring the Midterm Exam papers if you want to come check out your exam papers as well. I don't the room and exact timings, but I will email to confirm the room and my availability when I come to the Campus. Good Luck with the Final Exam in case I don't see you tomorrow. Y. Ozbek ------=_Part_16817_1988937105.1429919316180 Content-Type: text/html; charset=UTF-8 Content-Transfer-Encoding: 7bit
<p>Hi all,</p><br><p>I will be on campus sometime around noon.</p><br><p>Please stop by if you have any doubts, or last minute questions about the Final Exam.</p><br><p>I will bring the Midterm Exam papers if you want to come check out your exam papers as well.</p>

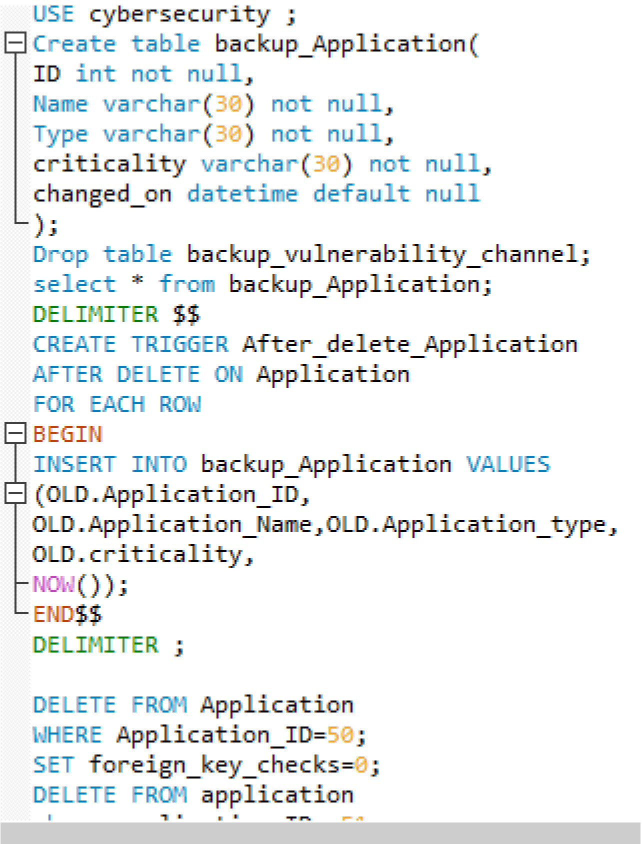
<br><p>I don't the room and exact timings, but I will email to confirm the room and my availability when I come to the Campus.</p><br><p>Good Luck with the Final Exam in case I don't see you tomorrow.</p><br><p>Y. Ozbek</p> ------=_Part_16817_1988937105.1429919316180-

Triggers

Delete Trigger

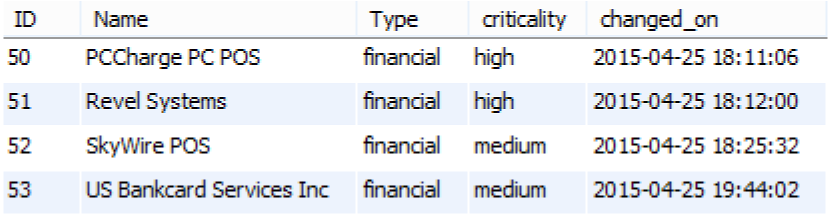


Application_ID	Application_Name	Application_Type	Criticality	Email_Receiver_Software_Event_ID	Mitigation_Mitigation_ID
53	US Bankcard Services Inc	financial	medium	1603	MITID73
54	BancNet Payment System	financial	low	1604	MITID74
55	Cleaning card	financial	low	1605	MITID75
56	Mortgage Calculator	Real Estate	low	1606	MITID76
57	Sitegeist	Real Estate	high	1607	MITID77
58	Vert	Real Estate	high	1608	MITID78
59	Cam Scanner	Real Estate	medium	1609	MITID79
60	DropBox	Real Estate	medium	1610	MITID80
61	PDF Escape	Real Estate	low	1611	MITID81
62	Dotloop	Real Estate	low	1612	MITID82



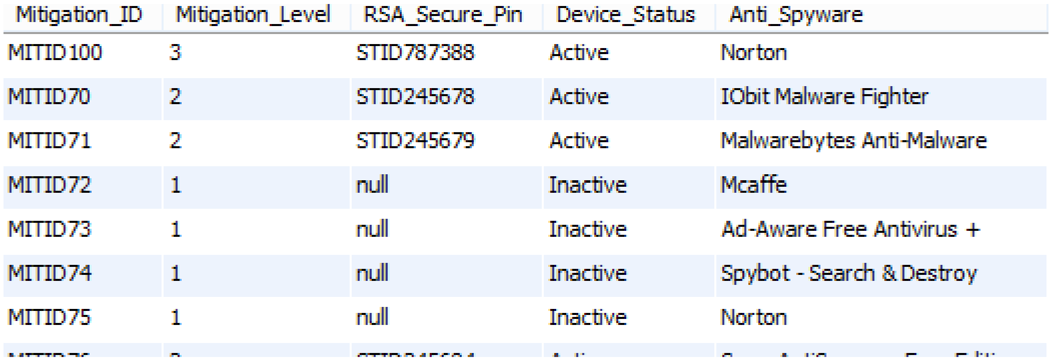
```
USE cybersecurity ;
Create table backup_Application(
ID int not null,
Name varchar(30) not null,
Type varchar(30) not null,
criticality varchar(30) not null,
changed_on datetime default null
);
Drop table backup_vulnerability_channel;
select * from backup_Application;
DELIMITER $$
CREATE TRIGGER After_delete_Application
AFTER DELETE ON Application
FOR EACH ROW
BEGIN
INSERT INTO backup_Application VALUES
(OLD.Application_ID,
OLD.Application_Name,OLD.Application_type,
OLD.criticality,
NOW());
END$$
DELIMITER ;

DELETE FROM Application
WHERE Application_ID=50;
SET foreign_key_checks=0;
DELETE FROM application
```

Output:

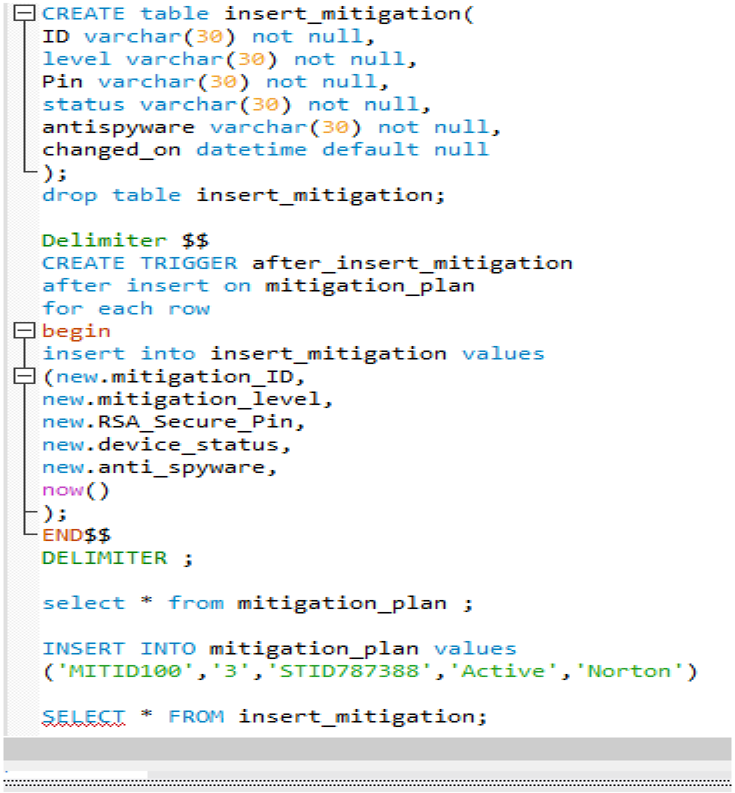


ID	Name	Type	criticality	changed_on
50	PCCharge PC POS	financial	high	2015-04-25 18:11:06
51	Revel Systems	financial	high	2015-04-25 18:12:00
52	SkyWire POS	financial	medium	2015-04-25 18:25:32
53	US Bankcard Services Inc	financial	medium	2015-04-25 19:44:02

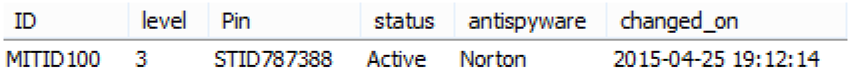
Insert Trigger



Mitigation_ID	Mitigation_Level	RSA_Secure_Pin	Device_Status	Anti_Spyware
MITID100	3	STID787388	Active	Norton
MITID70	2	STID245678	Active	IObit Malware Fighter
MITID71	2	STID245679	Active	Malwarebytes Anti-Malware
MITID72	1	null	Inactive	Mcaffe
MITID73	1	null	Inactive	Ad-Aware Free Antivirus +
MITID74	1	null	Inactive	Spybot - Search & Destroy
MITID75	1	null	Inactive	Norton

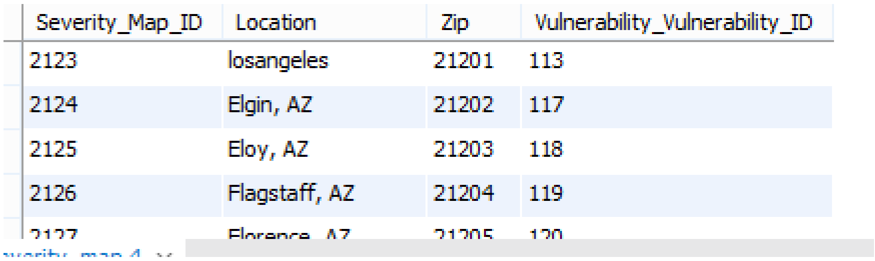


```
CREATE table insert_mitigation(
ID varchar(30) not null,
level varchar(30) not null,
Pin varchar(30) not null,
status varchar(30) not null,
antispyware varchar(30) not null,
changed_on datetime default null
);
drop table insert_mitigation;

Delimiter $$
CREATE TRIGGER after_insert_mitigation
after insert on mitigation_plan
for each row
begin
insert into insert_mitigation values
(new.mitigation_ID,
new.mitigation_level,
new.RSA_Secure_Pin,
new.device_status,
new.anti_spyware,
now()
);
END$$
DELIMITER ;

select * from mitigation_plan ;

INSERT INTO mitigation_plan values
('MITID100','3','STID787388','Active','Norton')

SELECT * FROM insert_mitigation;
```

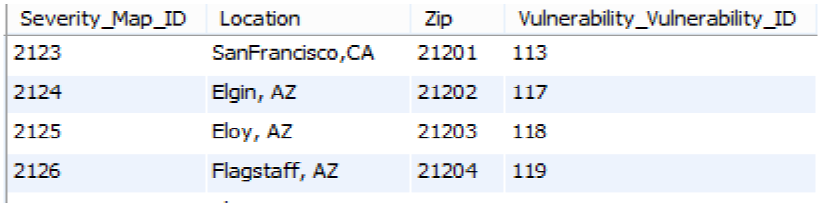


ID	level	Pin	status	antispyware	changed_on
MITID100	3	STID787388	Active	Norton	2015-04-25 19:12:14

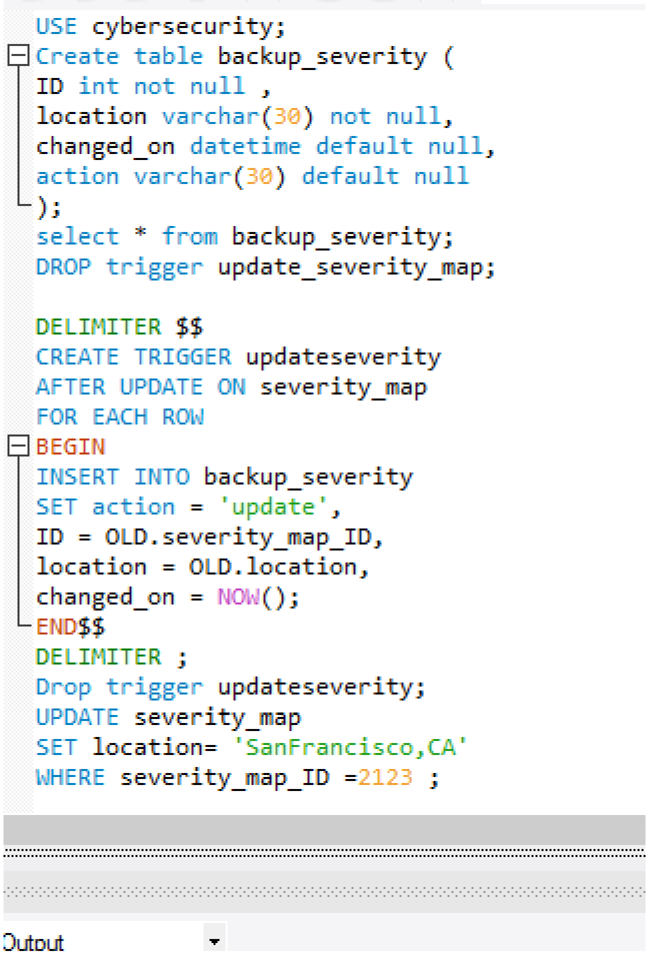
Update Trigger



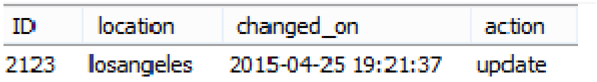
Severity_Map_ID	Location	Zip	Vulnerability_Vulnerability_ID
2123	losangeles	21201	113
2124	Elgin, AZ	21202	117
2125	Eloy, AZ	21203	118
2126	Flagstaff, AZ	21204	119
2127	Florence, AZ	21205	120



Severity_Map_ID	Location	Zip	Vulnerability_Vulnerability_ID
2123	SanFrancisco,CA	21201	113
2124	Elgin, AZ	21202	117
2125	Eloy, AZ	21203	118
2126	Flagstaff, AZ	21204	119

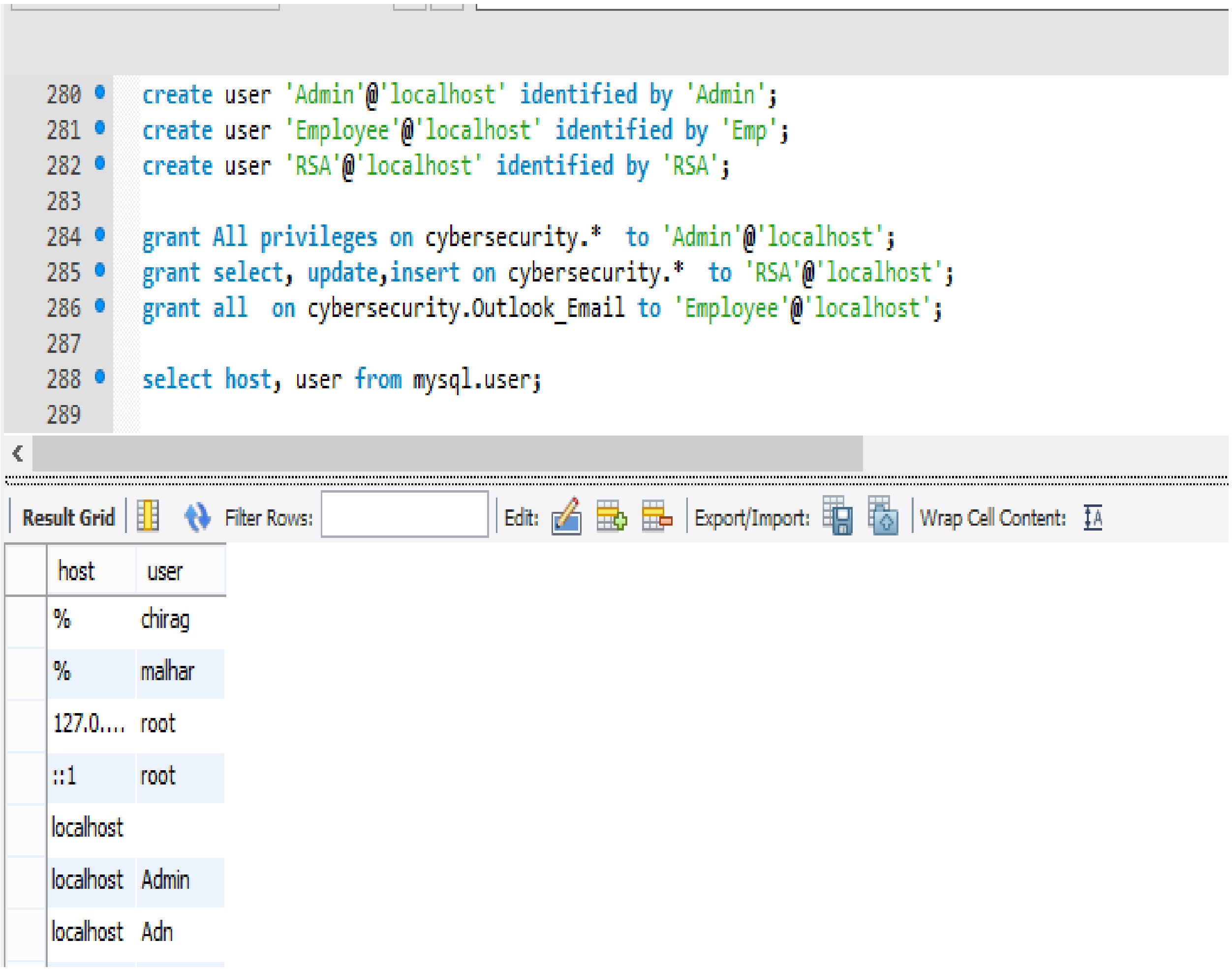


```
USE cybersecurity;
Create table backup_severity (
ID int not null ,
location varchar(30) not null,
changed_on datetime default null,
action varchar(30) default null
);
select * from backup_severity;
DROP trigger update_severity_map;

DELIMITER $$
CREATE TRIGGER updateseverity
AFTER UPDATE ON severity_map
FOR EACH ROW
BEGIN
INSERT INTO backup_severity
SET action = 'update',
ID = OLD.severity_map_ID,
location = OLD.location,
changed_on = NOW();
END$$
DELIMITER ;
Drop trigger updateseverity;
UPDATE severity_map
SET location= 'SanFrancisco,CA'
WHERE severity_map_ID =2123 ;
```



ID	location	changed_on	action
2123	losangeles	2015-04-25 19:21:37	update

User Priveleges

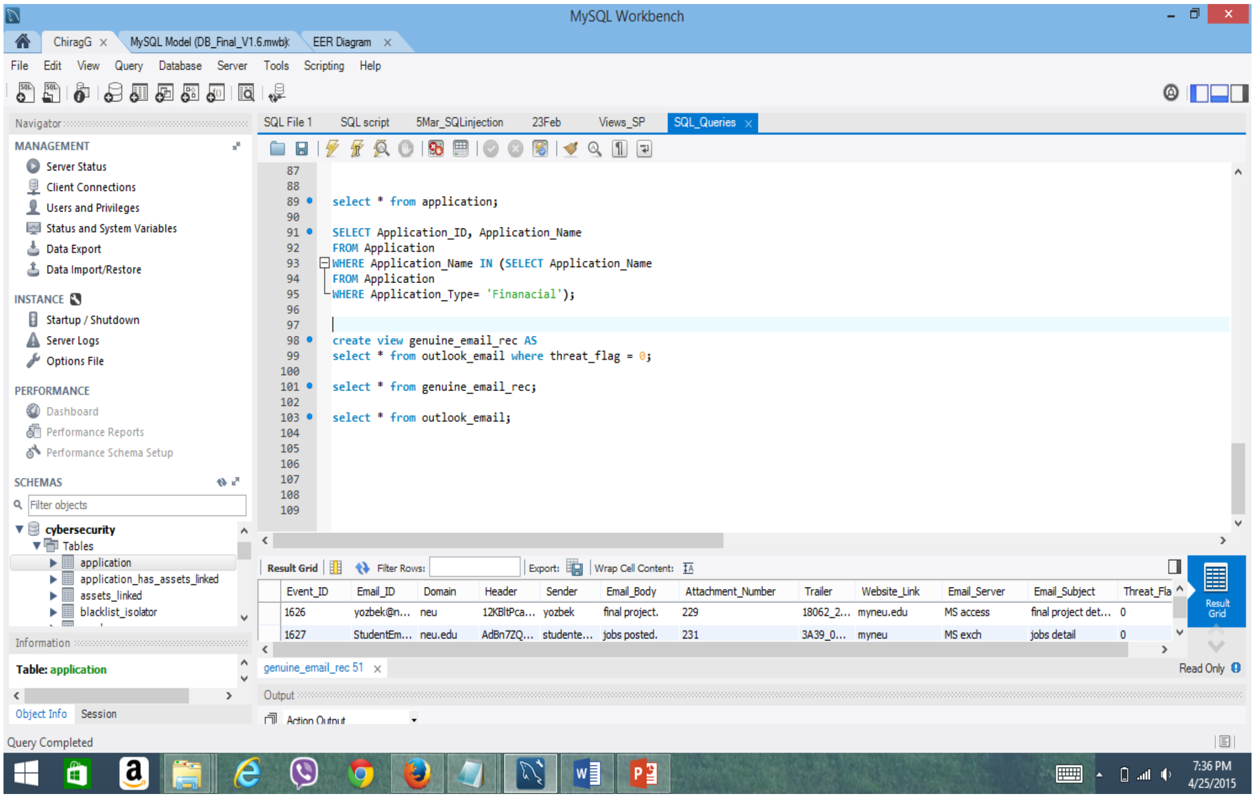


```
create user 'Admin'@'localhost' identified by 'Admin';
create user 'Employee'@'localhost' identified by 'Emp';
create user 'RSA'@'localhost' identified by 'RSA';

grant All privileges on cybersecurity.*  to 'Admin'@'localhost';
grant select, update,insert on cybersecurity.*  to 'RSA'@'localhost';
grant all  on cybersecurity.Outlook_Email to 'Employee'@'localhost';

select host, user from mysql.user;

```

host	user
%	chirag
%	malhar
127.0....	root
::1	root
localhost	
localhost	Admin
localhost	Adn

Views:

Genuene_email_record



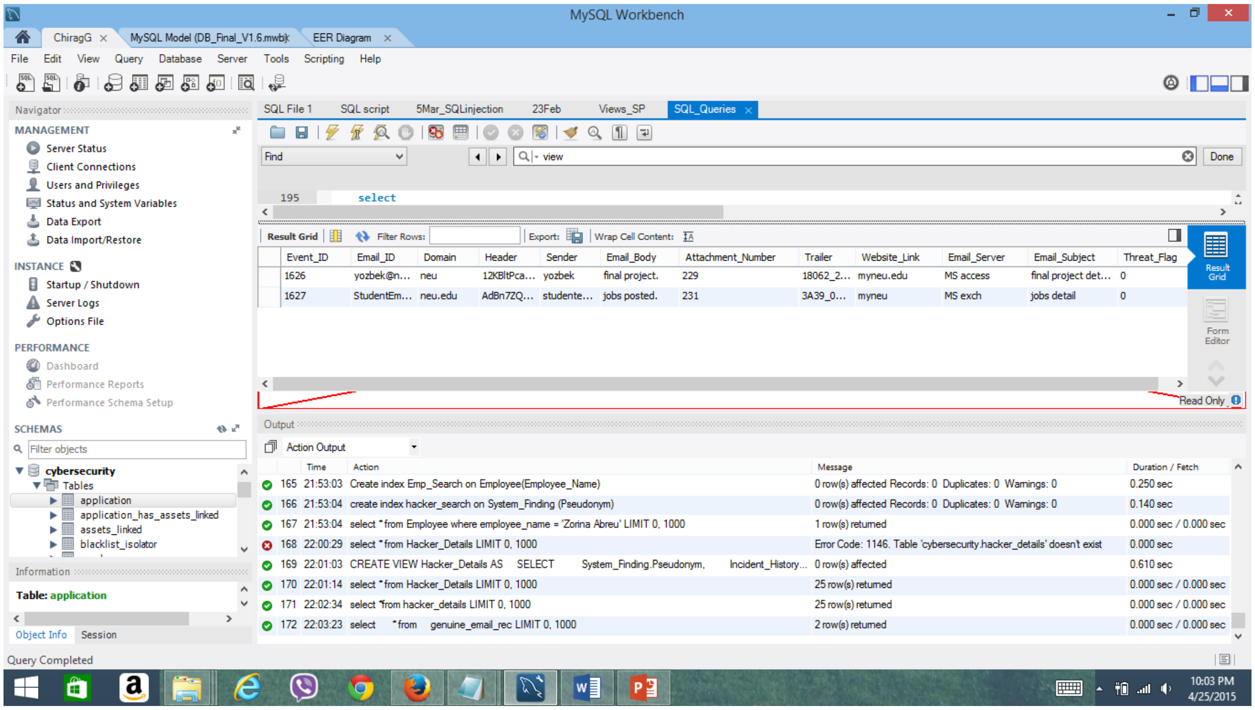
```
select * from application;

SELECT Application_ID, Application_Name
FROM Application
WHERE Application_Name IN (SELECT Application_Name
FROM Application
WHERE Application_Type= 'Finanacial');


create view genuine_email_rec AS
select * from outlook_email where threat_flag = 0;

select * from genuine_email_rec;

select * from outlook_email;
```

Event_ID	Email_ID	Domain	Header	Sender	Email_Body	Attachment_Number	Trailer	Website_Link	Email_Server	Email_Subject	Threat_Fla
1626	yozbek@n...	neu	12KBltPca...	yozbek	final project.	229	18062_2...	myneu.edu	MS access	final project det...	0
1627	StudentEm...	neu.edu	AdBn7ZQ...	studente...	jobs posted.	231	3A39_0...	myneu	MS exch	jobs detail	0

Hacker_Details Views

View 2.

```
create view genuine_email_rec AS select * from outlook_email where threat_flag = 0;

select * from genuine_email_rec;
```

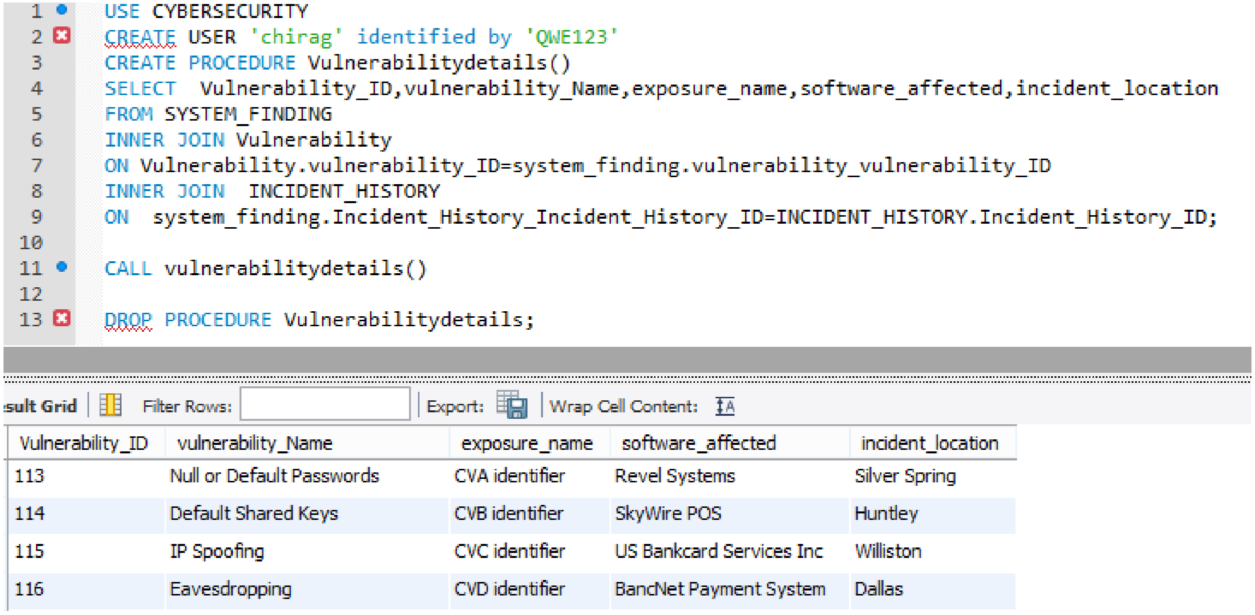


```
195        select
```

Event_ID	Email_ID	Domain	Header	Sender	Email_Body	Attachment_Number	Trailer	Website_Link	Email_Server	Email_Subject	Threat_Flag
1626	yozbek@n...	neu	12KBltPca...	yozbek	final project.	229	18062_2...	myneu.edu	MS access	final project det...	0
1627	StudentEm...	neu.edu	AdBn7ZQ...	studente...	jobs posted.	231	3A39_0...	myneu	MS exch	jobs detail	0

```
    Time      Action                                                                   Message                                                        Duration / Fetch
165 21:53:03  Create index Emp_Search on Employee(Employee_Name)                        0 row(s) affected Records: 0  Duplicates: 0  Wamings: 0         0.250 sec
166 21:53:04  create index hacker_search on System_Finding (Pseudonym)                  0 row(s) affected Records: 0  Duplicates: 0  Wamings: 0         0.140 sec
167 21:53:04  select *from Employee where employee_name = 'Zorina Abreu' LIMIT 0, 1000  1 row(s) returned                                               0.000 sec / 0.000 sec
168 22:00:29  select *from Hacker_Details LIMIT 0, 1000                                 Error Code: 1146. Table 'cybersecurity.hacker_details' doesn't exist  0.000 sec
169 22:01:03  CREATE VIEW Hacker_Details AS    SELECT    System_Finding.Pseudonym,    Incident_History...  0 row(s) affected                     0.610 sec
170 22:01:14  select *from Hacker_Details LIMIT 0, 1000                                 25 row(s) returned                                              0.000 sec / 0.000 sec
171 22:02:34  select *from hacker_details LIMIT 0, 1000                                 25 row(s) returned                                              0.000 sec / 0.000 sec
172 22:03:23  select    *from    genuine_email_rec LIMIT 0, 1000                        2 row(s) returned                                               0.000 sec / 0.000 sec
```

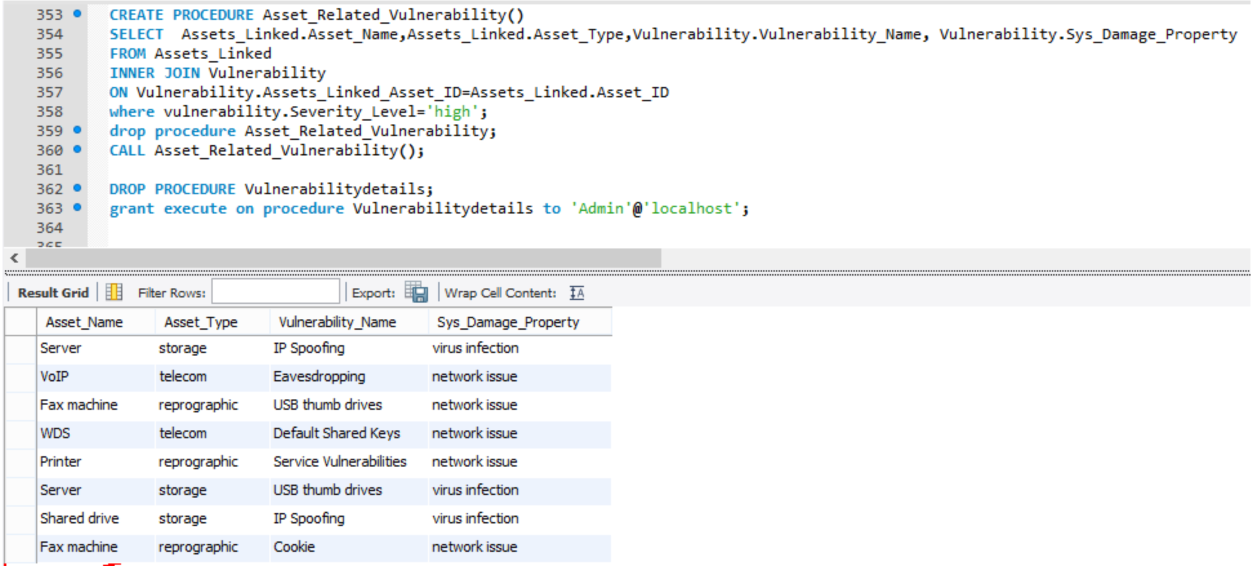
Stored Procedures 1



```sql
USE CYBERSECURITY
CREATE USER 'chirag' identified by 'QWE123'
CREATE PROCEDURE Vulnerabilitydetails()
SELECT  Vulnerability_ID,vulnerability_Name,exposure_name,software_affected,incident_location
FROM SYSTEM_FINDING
INNER JOIN Vulnerability
ON Vulnerability.vulnerability_ID=system_finding.vulnerability_vulnerability_ID
INNER JOIN  INCIDENT_HISTORY
ON  system_finding.Incident_History_Incident_History_ID=INCIDENT_HISTORY.Incident_History_ID;

CALL vulnerabilitydetails()

DROP PROCEDURE Vulnerabilitydetails;
```

Vulnerability_ID	vulnerability_Name	exposure_name	software_affected	incident_location
113	Null or Default Passwords	CVA identifier	Revel Systems	Silver Spring
114	Default Shared Keys	CVB identifier	SkyWire POS	Huntley
115	IP Spoofing	CVC identifier	US Bankcard Services Inc	Williston
116	Eavesdropping	CVD identifier	BancNet Payment System	Dallas

Stored Procedure 2



```sql
CREATE PROCEDURE Asset_Related_Vulnerability()
SELECT  Assets_Linked.Asset_Name,Assets_Linked.Asset_Type,Vulnerability.Vulnerability_Name, Vulnerability.Sys_Damage_Property
FROM Assets_Linked
INNER JOIN Vulnerability
ON Vulnerability.Assets_Linked_Asset_ID=Assets_Linked.Asset_ID
where vulnerability.Severity_Level='high';
drop procedure Asset_Related_Vulnerability;
CALL Asset_Related_Vulnerability();

DROP PROCEDURE Vulnerabilitydetails;
grant execute on procedure Vulnerabilitydetails to 'Admin'@'localhost';
```

Asset_Name	Asset_Type	Vulnerability_Name	Sys_Damage_Property
Server	storage	IP Spoofing	virus infection
VoIP	telecom	Eavesdropping	network issue
Fax machine	reprographic	USB thumb drives	network issue
WDS	telecom	Default Shared Keys	network issue
Printer	reprographic	Service Vulnerabilities	network issue
Server	storage	USB thumb drives	virus infection
Shared drive	storage	IP Spoofing	virus infection
Fax machine	reprographic	Cookie	network issue

Back-Up Strategy

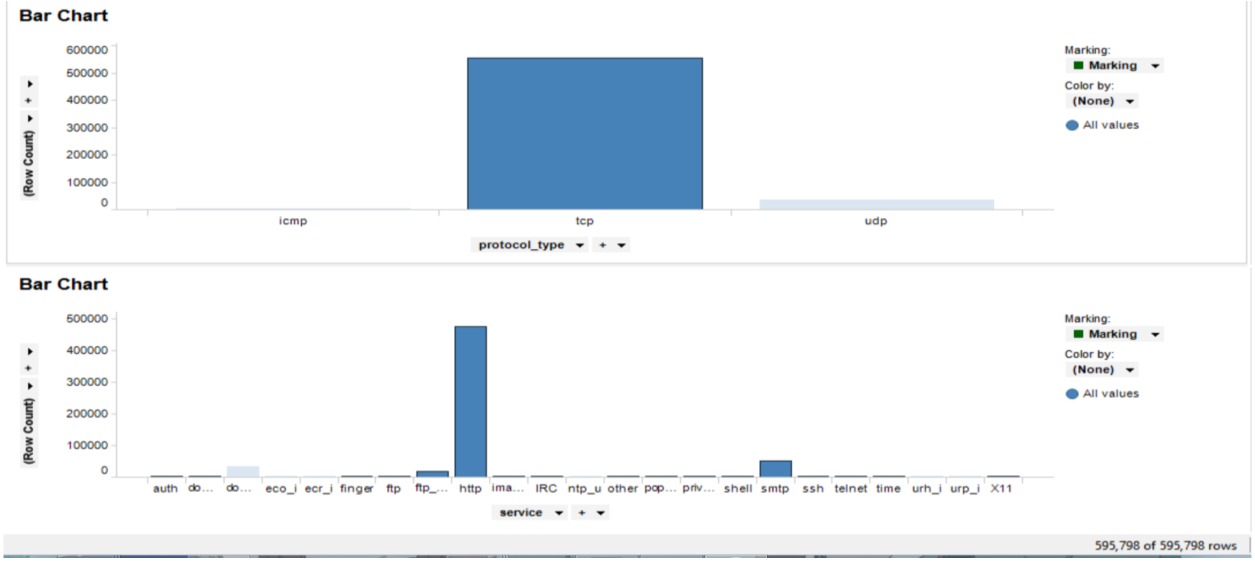
Days	**Mon**	**Tues**	**Wed**	**Thurs**	**Fri**	**Sat**	**Sun**
Back-up Strategy	**I**	**I**	**I**	**F**	**I**	**I**	**F**

I-Incremental Back-up

F-Full Back-up

Statistical analysis using Tableau:

The KDD-99 held in 1999 by the US Army gathered the data in a simulated environment, where the data connections from multiple host was being analyzed, showing 40% off the connection as phishing.



The statistical analysis of which services based on protocol are most vulnerable to attacks

INTERESTING FACTS RELATED TO OUR PROJECT:

* The subject Line of the E-mail received by the group of employees at the EMC that attracted their attention to open the infected e-mail was:

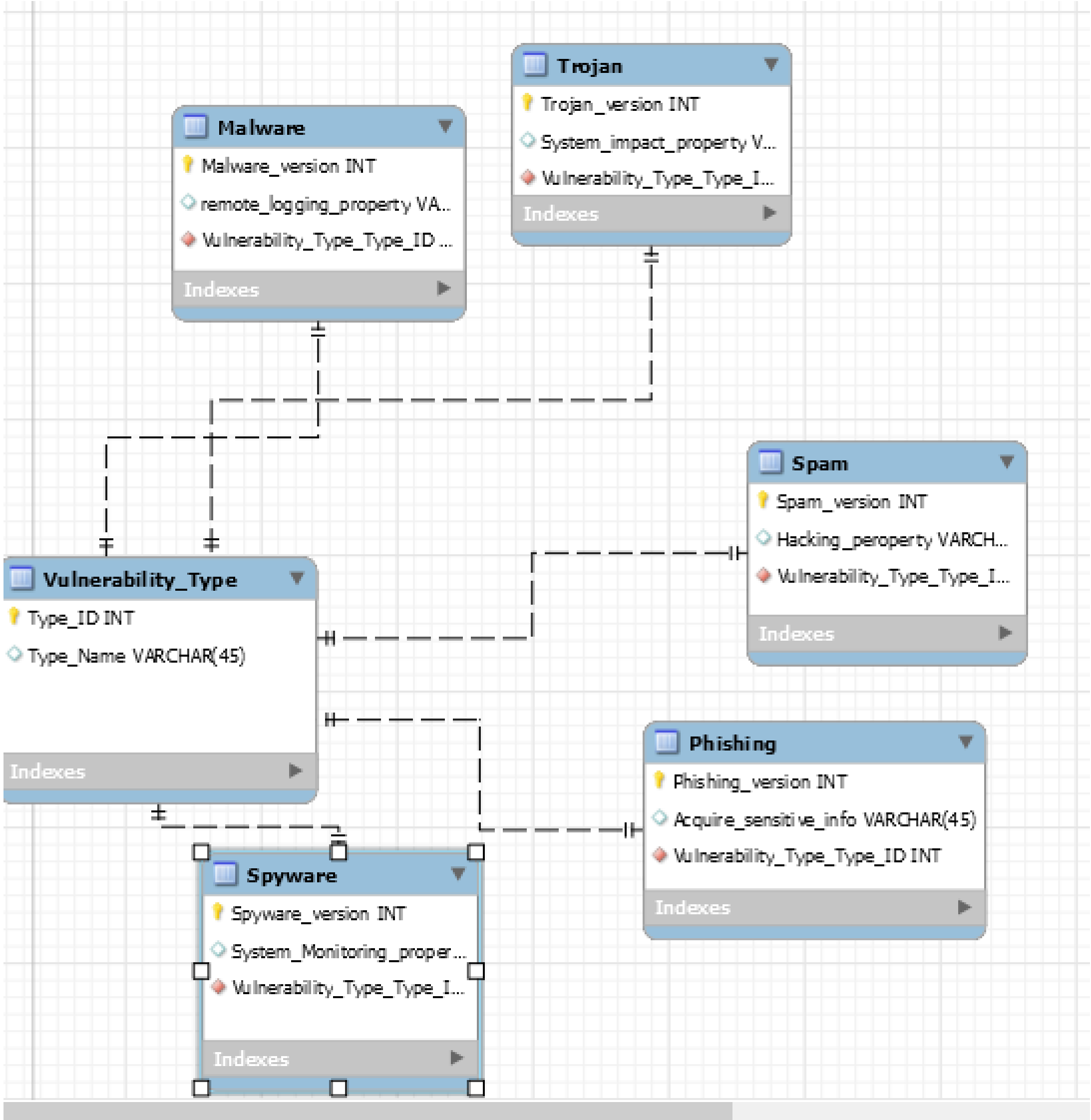
Subject: 2011 Recruitment Plan

* To handle the security breach experienced by the EMC in March 2011, it purchased a company named NetWitness Corp., security company that makes the NextGen visibility monitoring system to detect electronic threats and malware based attacks. It operates as a part of RSA.

* Link to an interesting article named Anatomy of an attack

https://blogs.rsa.com/anatomy-of-an-attack/

Specialization for Vulnerability_Type:


Trojan
Trojan_version INT
System_impact_property V...
Vulnerability_Type_Type_I...
Indexes
Malware
Malware_version INT
remote_logging_property VA...
Vulnerability_Type_Type_ID ...
Indexes
Spam
Spam_version INT
Hacking_peroperty VARCH...
Vulnerability_Type_Type_I...
Indexes
Vulnerability_Type
Type_ID INT
Type_Name VARCHAR(45)
Indexes
Phishing
Phishing_version INT
Acquire_sensitive_info VARCHAR(45)
Vulnerability_Type_Type_ID INT
Indexes
Spyware
Spyware_version INT
System_Monitoring_proper...
Vulnerability_Type_Type_I...
Indexes