protiviti®
Face the Future with Confidence

IT and Industrial Cyber Security

February 2020

Presented by
Vaibhav Koul,
Director, Protiviti, India

Table of Contents

1. Current Trends

protiviti

1. Current Trends

Some Cyber breaches since Jan 2020 (illustrative)

Public healthcare cluster NHG fined $6,000 for not securing personal data

Albany Airport falls victim to cyber attack

Wawa Breach: Hackers Put 30 Million Stolen Payment Card Details for Sale

EDITORS' PICK | 6,498 views | Jan 30, 2020, 04:35am

United Nations Confirms 'Serious' Cyberattack With 42 Core Servers Compromised

Adventist Health Identifies Data Breach

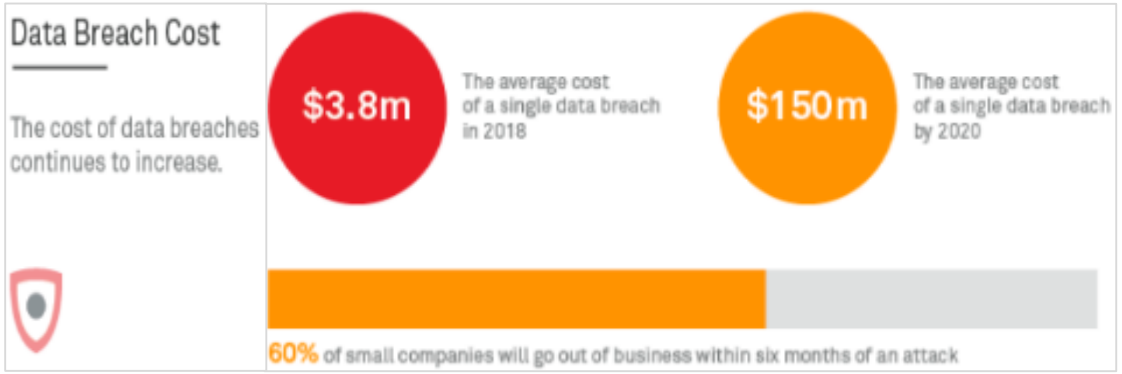
Man jailed for using data breach info leaks to claim over $12 million in IRS tax refunds

Information leaked due to data breaches was used to file fraudulent tax returns.

Coronavirus Outbreak: Hackers Use Fear To Spread Malware

1. Current Trends : IT and OT Breaches

Cost of data breaches is increasing exponentially



A recent survey of more than 30 Power and Utility companies found:

- **More than 60 percent** of companies have suffered a security compromise in the past year
- **Two-thirds of companies** believe risks to OT systems have increased substantially in recent years
- Only **one-third of companies** report that OT and IT are fully aligned in their organizations
- Just **35 percent** rate their readiness to address cyber threats as high

By 2021, cybercrime is likely to cost the world $6 trillion annually – more than the combined GDP of the UK and France.

Source: Juniper / Symantec research

Source: Protiviti | ESI ToughtLabs https://www.protiviti.com/IN-en/insights/cybersecurity-imperative
https://www.thesslstore.com/blog/2018-cybercrime-statistics/

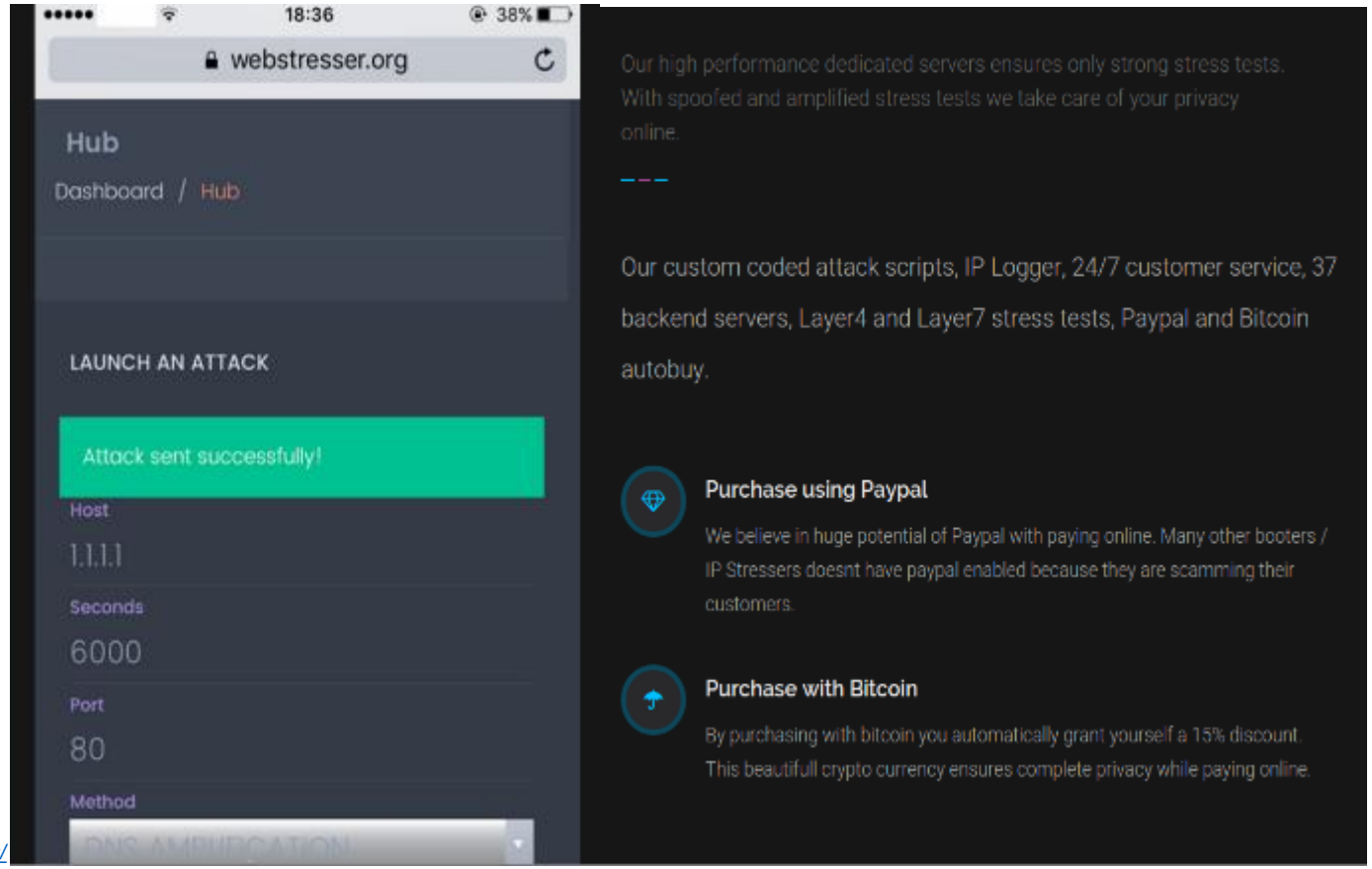
1. Insights into Cybercrime

Attackers no longer need to be skilled and sophisticated to launch attacks

Cybercrime as a Service

Cybercrime Product or Service	Price (in US Dollars)
SMS Spoofing	$20/month
Custom Spyware	$200
Hacker-for-Hire	$200+
Malware Exploit Kit	$200-$700
Blackhole Exploit Kit	$700/month or $1,500/year
Zero-Day Adobe Exploit	$30,000
Zero-Day iOS Exploit	$250,000

Snippet of a recently taken down DOS-as-a-service provider



Source : *https://krebsonsecurity.com/tag/webstresser-org/*
https://www.thesslstore.com/blog/2018-cybercrime-statistics/

2. Real world cyber attacks

protiviti

2. Real world cyber attacks

Attacker objectives

Attackers Objective

Operations Disruption

Attack Targets

Operational Technology (OT)

Targeted Attacks

IT targeted Attacks

Attackers Objective

Business Disruption, Financial Loss, data theft

2. Real world cyber attacks

Case A: ICS Cyber Attack on Steel facility

Targeted malware attack on the blast furnace of a steel plant

Attacker uses spear phishing for target corporate users

Corporate user clicks open the email and opens the pdf attachment which executes the malware

Malware infects the corporate user machine

Lateral movement through trusted zones between corporate and plant network

Reached the furnace controllers and updated the temperature thresholds

2. Real world cyber attacks

Case B: Power Grid Cyberattack

Attack
Electricity distribution control centers

Damage
Power Outage and Reputational Loss

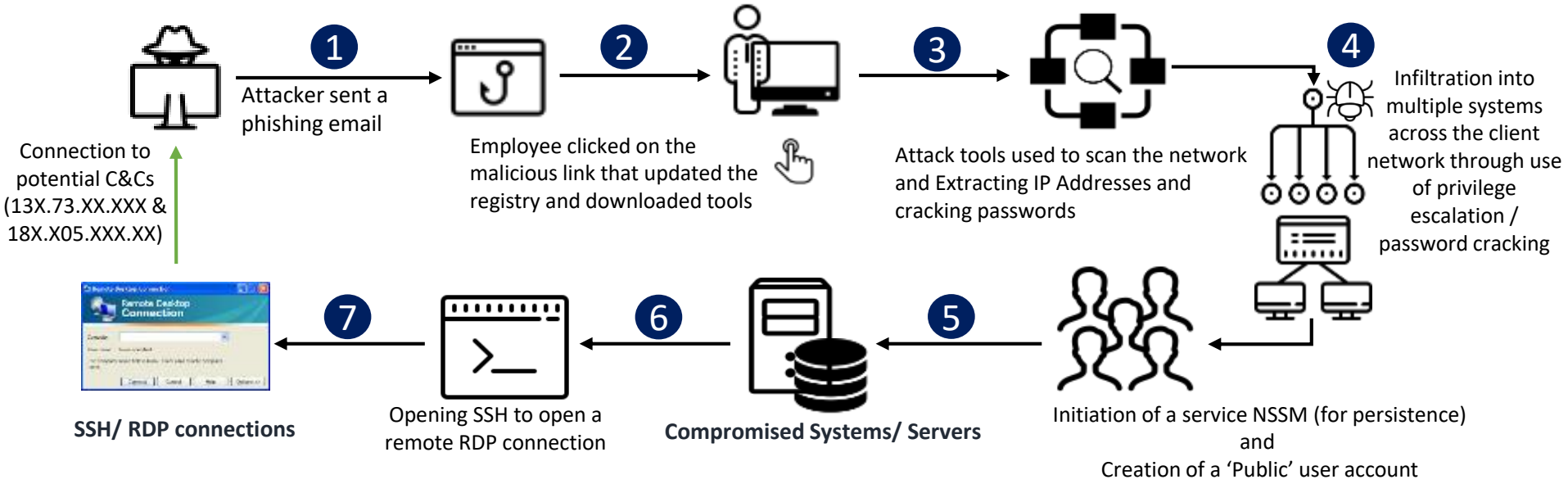
Impact
30 substations were switched off, and about 230 thousand people were affected

Power Grid Cyberattack

- A **cyberattack** penetrated electricity distribution control centers using **software vulnerabilities, stolen credentials and sophisticated malware**.
- The attackers were able to **open dozens of circuit breakers** and **shut off power to more than 200,000** customers for several hours. That attack also **cut off electricity service**, though to a much smaller geographic area, and for about an hour.

2. Real world cyber attacks

Case C : Living off the land / use of dual purpose tools



Attackers used methods to gain and download data from the compromised systems and servers.

1. The attacker sent a phishing email to an employee with a malicious link / file with macros.
2. After clicking the link, the attack tools were downloaded.
3. The downloaded tools were used to enumerate the victim's internal network and
4. Tools were used to crack passwords of the identified systems and cracked user credentials were used for infiltrating into multiple systems, launching malicious service
5. The malicious services and users were used to open a remote connection through SSH / remote desktop to gain remote access to the identified systems.
6. The malicious services were used to keep the connectivity and access persistent (to allow access even if the user credentials were changed)

2. Real world cyber attacks

Case D : Ransom Scare

Spoofed email

Actual password of the user

From: Romeo@acme.com
Sent: 10 October 2018 13:55
To: rome580 <Romeo@acme.com
Subject: Your password is rome580

I am aware rome580 is your password. Lets get straight to point. You don't know me and you are probably wondering why you're getting this mail? There is no one who has compensated me to investigate you. Actually, I setup a software on the streaming website and guess what, you visited this website to have fun while you were in office. While you were viewing videos, your browser started working as a Remote control Desktop that has a keylogger which provided me with access to your screen as well as web cam. after that, my software gathered all of your contacts from your Messenger, FB, and e-mail . And then I created a video. First part shows the video you were watching, and next part shows the view of your cam, yeah it is you.

You do have 2 alternatives. Why dont we go through each of these options in details:

Very first choice is to disregard this email. In this situation, I most certainly will send out your actual video recording to almost all of your superiors. Just consider concerning the disgrace you experience. how it is going to affect your growth and standing in the organization?

Next solution should be to compensate me $250. Let us name it as a donation. In this scenario, I will asap discard your video footage. You could go on everyday life like this never took place and you will not ever hear back again from me.
You'll make the payment by Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

Illustrative

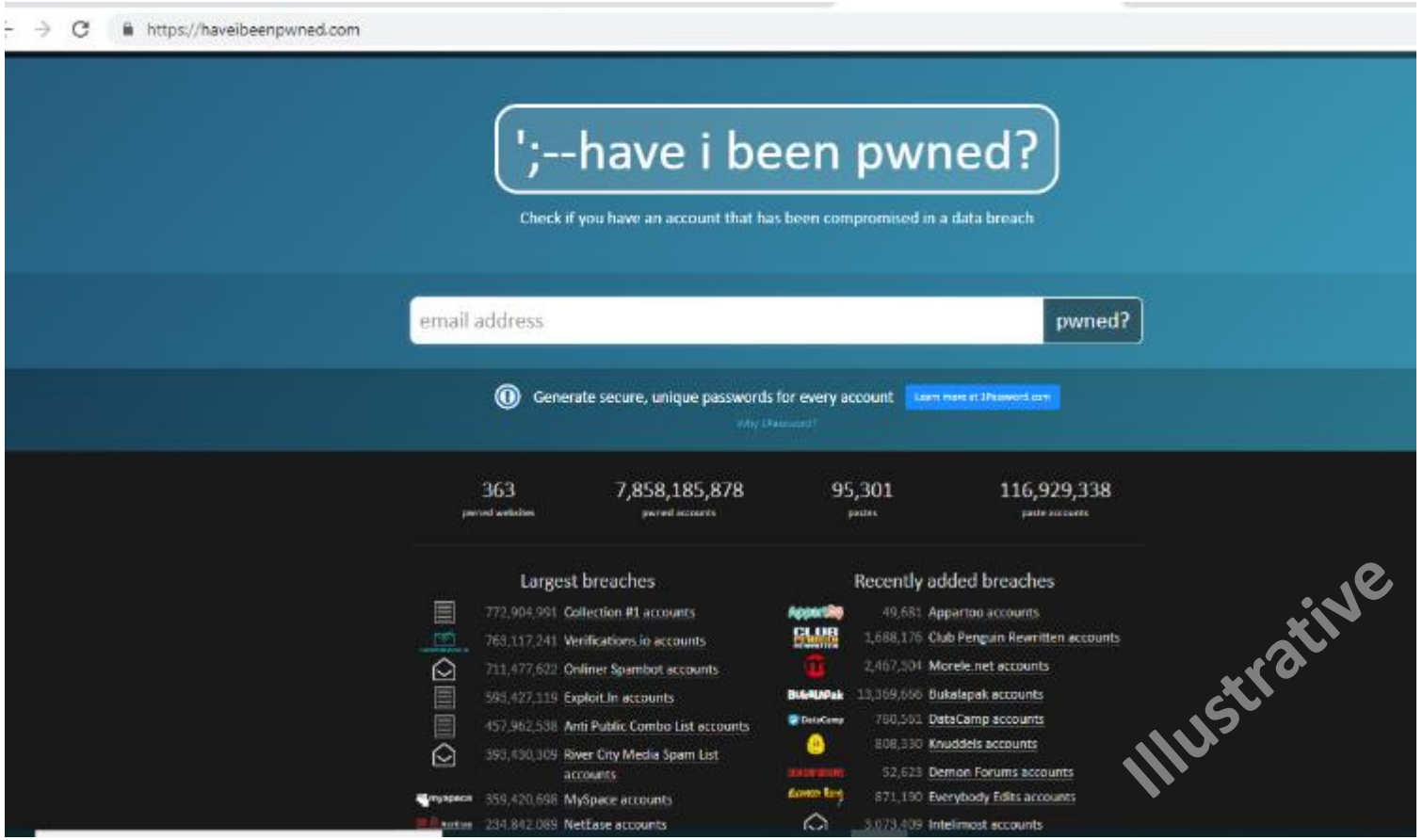
BTC Address to send to: 1D7r8uiC9bx2udQA7hGuvDmcAw37CxJaxK
[CASE-sensitive, copy & paste it]
If you have been thinking about going to the cops, very well, this e-mail cannot be traced back to me. I have taken care of my moves. I am also not looking to ask you for a lot, I just want to be paid.

You have one day to make the payment. I have a unique pixel in this e mail, and now I know that you have read through this email. If I do not get the BitCoins, I will, no doubt send your video to all of your contacts including superiors, colleagues, and so on. Nevertheless, if I receive the payment, I will erase the recording right away. If you need proof, reply Yea! then I definitely will send your video to your superiors. This is the non-negotiable offer and so don't waste my time & yours by responding to this e-mail.

2. Real world cyber attacks

Case D : Ransom Scare

https://haveibeenpwned.com/

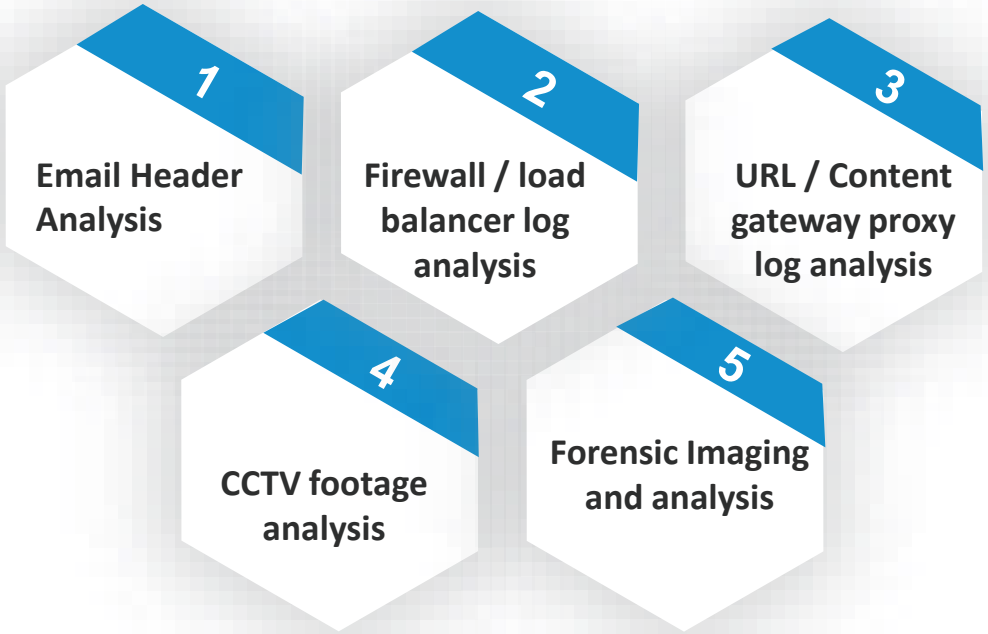


2. Real world cyber attacks

Case E: Fraudulent allegations

Case background: The client is a leading services MNC. The clients key customer had received an anonymous incriminating email from a yahoo email address alleging that specific client employee was selling customer data on the dark net. The investigation on this matter was completed and the allegation was noted to be false. The client wanted to now identify the sender of the fraudulent email. The anonymous email was from yahoo.com domain and was received at 12:25 pm on 11 February. The content of the email indicated that the suspect may have been an internal employee from company. Internal investigation was initiated to identify the employee involved in this.

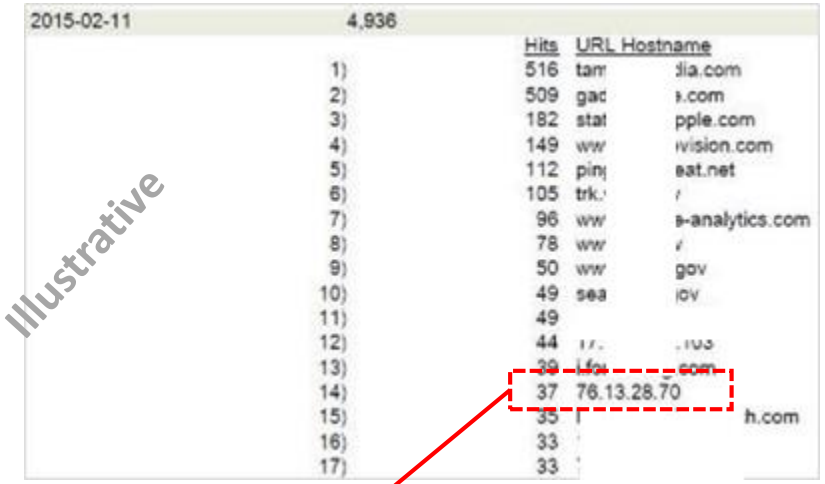
Attempt to identify the sender of the incriminating email by performing the following procedures



2. Real world cyber attacks

Case E: Fraudulent allegations

Case background: Internet browsing log analysis Suspicious employee had initiated 37 sessions to yahoo.com domain on 11th February. Out of these one of the sessions was initiated on 12:04:16. (The incriminating email was received at 12:25 pm on 11 February).



There were 37 hits to the IP address 76.13.28.70 on 11th February. This IP address is associated with the domain - yahoo.com

Sessions indicating access to the yahoo domain

2. Real world cyber attacks

Case E: Fraudulent allegations

CCTV and Access log correlation - Below artifacts indicate that 'Suspect' was in the work area at the time of the receipt of the incriminating email (i.e. 11 February, 12:25 pm).

Access Card System Log

Log indicates 'Suspect' was inside the work area on 11 February, 12:25 pm and then left at work area by 12.27 PM

Date	Transaction	Reader	Denied reason	Last nam	Badge	Number	Department
11-02-2015 08:14:00	Access Granted	Rdr02					
11-02-2015 08:14:00	Access Granted	Rdr02					
11-02-2015 12:27:00	Access Denied	Rdr02	- Anti Pass Back				
11-02-2015 12:27:00	Access Granted	Rdr02					

Illustrative

2. Real world cyber attacks

Case E: Fraudulent allegations

CCTV and Access log correlation - Below artifacts indicate that suspect was in the work area at the time of the receipt of the incriminating email (i.e. 11 February, 12:25 pm).

CCTV Footages

Footage indicates 'Suspect' was at his desk on 11 February, **12:25 pm** and left briefly from the facility after that at ~ **12:27 pm**

2. Real world cyber attacks

Case E: Fraudulent allegations

Analysis of Internet searches The potential suspect had searched on google to determine- how many servers of yahoo are running in India. This search was performed on 9 February (i.e. 2 days prior to the receipt of the email with the allegations)

Last Visited Date/Time - (UTC+5:30) (dd-MM-yyyy)	09-02-2015 15:42:16
URL	https://www.google.com/?gws_rd=ssl#q=how+many+servers+is+running+is+india+for+yahoo+company
Title	how many servers is running is india for yahoo company - Google Search
Visit Count	1
Typed Count	0
Source	INS-C003-D1.E01 - Partition 1 (Microsoft NTFS, 465.76 GB) OSDisk (Unallocated Clusters)
Located At	Physical Sector 496837835
Evidence Number	INS-C003-D1

Illustrative

Last Visited Date/Time - (UTC+5:30) (dd-MM-yyyy)	09-02-2015 15:42:19
URL	https://www.google.com/search?q=how+many+servers+is+running+is+india+for+yahoo+company&biw=1366&bih=667&source=lnms&tbm=isch&sa=X&ei=_ofYVJ3cNoG5ggTMy4HAAQ&ve
Title	how many servers is running is india for yahoo company - Google Search
Visit Count	1
Typed Count	0
Source	INS-C003-D1.E01 - Partition 1 (Microsoft NTFS, 465.76 GB) OSDisk (Unallocated Clusters)
Located At	Physical Sector 496837834
Evidence Number	INS-C003-D1
Bookmark Comment	

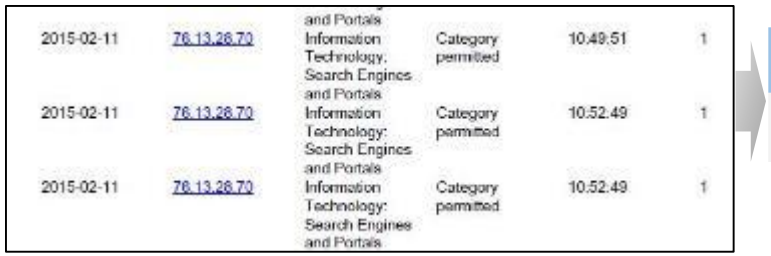
2. Real world cyber attacks

Case E: Fraudulent allegations

Detailed analysis of websense logs and desktop activity logs Specific instances of access to yahoo correlating to the websense logs were not noted from the hard disk analysis. However, we noted that the user was connected to the Citrix environment before each instance of access to yahoo. This indicated the possibility that access to yahoo may have been performed through the Citrix environment. (Hence no traces were noted on the local desktop).

Websense Logs

Corresponding Internet Activity Log from the desktop image

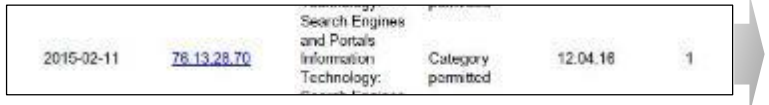


2015-02-11	76.13.28.70	and Portals Information Technology: Search Engines and Portals	Category permitted	10:49:51	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	10:52:49	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	10:52:49	1

11 Feb 2015		
Time	source	Description
10:47:46 AM	Internet Explorer Cache	URL: https://www. l.com/corp-ir/media_files/iro
10:49:00 AM	Internet Explorer Cache	URL: https://www. l.com/corp-ir/media_files/iro

2015-02-11	76.13.28.70	and Portals Information Technology: Search Engines and Portals	Category permitted	10:53:04	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	11:12:18	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	11:12:18	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	11:12:33	1
2015-02-11	76.13.28.70	Information Technology: Search Engines and Portals	Category permitted	11:12:33	1

11 Feb 2015		
Time	source	Description
10:52:50 AM	Internet Explorer Cache	URL: https://www. com/corp-ir/media_files/irol/83/83420
11:09:00 AM	Internet Explorer Cache	URL: https://www. com/corp-ir/media_files/irol/83/83420



2015-02-11	76.13.28.70	Search Engines and Portals Information Technology:	Category permitted	12:04:16	1

11 Feb 2015		
Time	source	Description
11:59:01 AM	Internet Explorer Cache	URL: https://www. media_files/irol/83/83420
11:59:01 AM	Internet Explorer Cache	URL: https://www. media_files/irol/83/83420
12:04:01 PM	Internet Explorer Cache	URL: https://www. media_files/irol/83/83420
12:04:03 PM	Internet Explorer Cache	URL: https://www. media_files/irol/83/83420

4. Cyber Defenses – What should be on ground ?

protiviti

3. Cyber defenses: what should be on ground?

Typical areas of Cyber Readiness

CYBER DEFENCE MODEL

Prevent

- Cyber Strategy
- Cyber Policies & Processes
- Cyber Defense Architecture
- IT/OT Security Defenses
- Perimeter Defenses
- Network Defenses
- End Point Defenses
- Application Defenses
- Database Defenses

Detect

- Cyber Security Programs
- Threat Hunting
- Security Monitoring
- Threat & Vulnerability
- Cyber Assurance Programs

Respond

- Cyber Incident Response

3. Cyber defenses: what should be on ground?

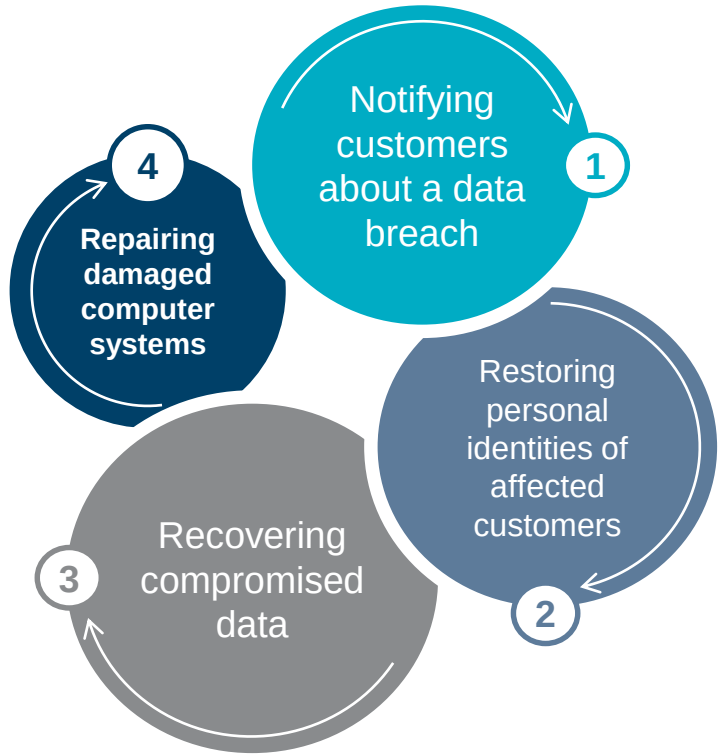
What is Cyber Insurance?

Case for Cyber Insurance

- A cyber insurance policy, also referred to as **cyber risk insurance** is designed to help an organization mitigate risk exposure by **offsetting costs** involved with recovery after a **cyber-related security breach** or similar event.
- With its roots in errors and omissions (E&O) insurance, cyber insurance began catching on in 2005, with the total value of premiums forecasted to reach **$7.5 billion by 2020**.
- According our survey in 2018, about **one-third of U.S. companies** currently purchase some type of cyber insurance. Different **cyber insurance policies** offer different types of coverage, limits of coverage, and premium/deductible rates.
- There are a number of **immediate and ongoing costs** to a business that are directly related to a cyberattack. There are **different types of cyber insurance** designed to cover those costs and to **supply funds to mitigate** the consequences of an attack.

What does cyber insurance cover?

Besides legal fees and expenses, cyber insurance typically helps with:



3. Cyber defenses: what should be on ground?

Critical success factors for a cyber defense program…

Cyber Defense is not just one time activity

Senior management commitment

Cyber security infused work culture

Board & leadership focus

Critical success factors

Right sized technology

Investment ear marking

Right fit people

It's a continuous process

Thank You……

Vaibhav Koul
Director

Face the Future with Confidence

protiviti®