DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

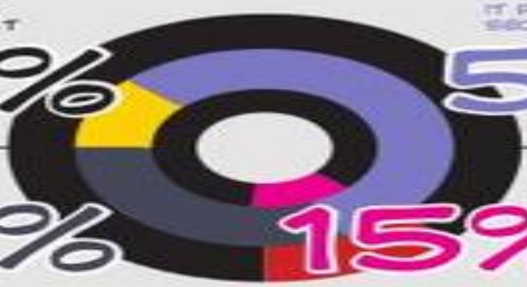
INCIDENT HANDLING

Darryle Justin M. Caparas

UNEDUCATED EMPLOYEES

THE TOP CAUSE OF ORGANIZATIONAL DATA BREACHES: "NEGLIGENT INSIDERS"

TODAY'S ORGANIZATIONS EXPERIENCE AN AVERAGE OF *14.4 INCIDENTS/YEAR* OF UNINTENTIONAL DATA LOSS THROUGH EMPLOYEE NEGLIGENCE



87% BUSINESSES BREACHED THAT *DID NOT* HAVE SECURITY POLICIES IN PLACE THAT INCLUDED SECURITY AWARENESS EDUCATION

56% IT PROFESSIONALS THAT REPORT SECURITY POLICIES ARE COMMUNICATED TO NEW HIRES DURING ORIENTATION

32% EMPLOYEES THAT SAY THEY WERE EDUCATED ON SECURITY POLICIES

15% PUBLICLY REPORTED INSIDER BREACHES THAT ARE EXECUTED WITH MALICIOUS INTENT

AND THEIR 7 DEADLY SINS

#1: PATHETIC PASSWORDS

15% IN APPROXIMATELY 15% OF PHYSICAL SECURITY TESTS PERFORMED AT CLIENT SITES IN 2011 WRITTEN PASSWORDS WERE FOUND ON AND AROUND USER WORKSTATIONS

THE MOST COMMON CORPORATE PASSWORD IS Password1 BECAUSE IT JUST BARELY MEETS THE MINIMUM COMPLEXITY REQUIREMENTS OF ACTIVE DIRECTORY FOR LENGTH, CAPITALIZATION AND NUMERICAL FIGURES

#2: PEEPING ROM

71% WORKERS SURVEYED THAT SAY THEY HAVE BEEN ABLE TO SNEAK A PEEK AT A CO-WORKER'S OR STRANGER'S WORK STATION IN THE WORKPLACE OR A PUBLIC PLACE

ONE IN THREE WORKERS LEAVE THEIR COMPUTERS LOGGED ON TO NETWORK RESOURCES AND UNLOCKED WHEN THEY ARE AWAY FROM THEIR DESK

26.4% OF *MALWARE* IS KEY LOGGER OR APPLICATION-SPECIFIC — WHICH OFTEN REQUIRES DETAILED KNOWLEDGE OF OR PHYSICAL ACCESS TO A TARGETED SYSTEM

#3: USB STICK UP

60% OF USERS WHO FIND RANDOM USB STICKS IN A PARKING LOT WILL PLUG THEM INTO THEIR COMPUTERS

ADD THE COMPANY LOGO, AND THAT NUMBER INCREASES TO 90%

35% OF USERS REPORT HAVING EXPERIENCED A VIRUS INFECTION THROUGH A USB DEVICE

#4: PHISH BITING

69% OF IT SECURITY PROS SAY THEY COME ACROSS PHISHING MESSAGES THAT GET PAST SPAM FILTERS

27% OF IT ORGANIZATIONS HAVE TOP EXECUTIVES OR PRIVILEGED USERS WHO HAVE FALLEN FOR MALICIOUS EMAIL ATTACKS

USERS TRAINED IN AVOIDING PHISHING AND SCAM EMAILS FELL FOR THESE MALICIOUS EMAILS *42% LESS* THAN THOSE WITHOUT TRAINING

#5: RECKLESS ABANDON

70% OF USERS DO NOT PASSWORD PROTECT THEIR SMARTPHONES

89% OF PEOPLE WHO FIND LOST CELL PHONES RUMMAGE THROUGH THE DIGITAL CONTENTS TO LOOK AT SENSITIVE INFORMATION

#6: HOOKING UP WITH ANOTHER MAN'S WI-FI

BY 2015, THE NUMBER OF WI-FI HOTSPOT DEPLOYMENTS WILL INCREASE BY 350%

18% ONLY 18 PERCENT OF USERS USE A VPN TOOL WHEN ACCESSING PUBLIC WI-FI

FBI THE FBI RECENTLY RELEASED AN ALERT TO TRAVELERS WARNING AGAINST AN UPTICK IN MALWARE PASSED OFF AS SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

#7: A LITTLE TOO SOCIAL

67% OF YOUNG WORKERS THINK CORPORATE SOCIAL MEDIA POLICIES ARE OUTDATED

70% REGULARLY IGNORE IT POLICIES

52% OF ENTERPRISES HAVE SEEN AN INCREASE OF MALWARE INFECTIONS DUE TO EMPLOYEES' USE OF SOCIAL MEDIA

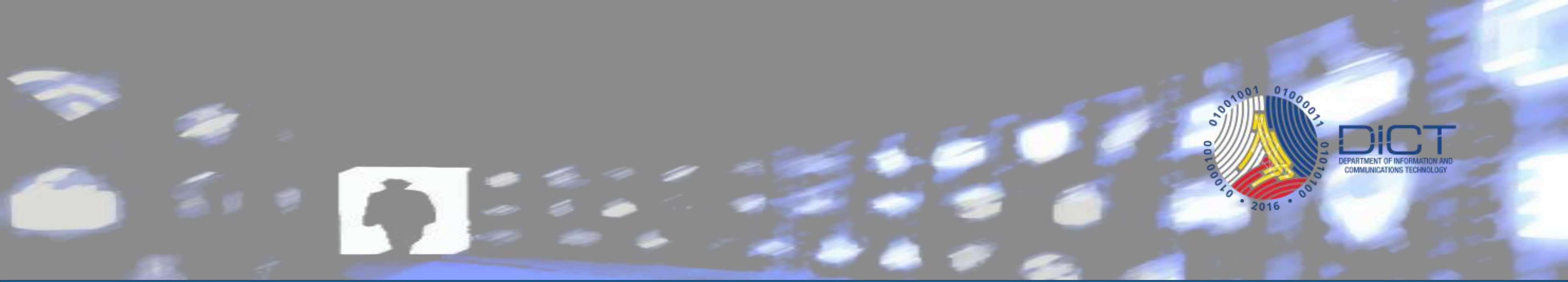
DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

OBJECTIVES

- To be familiarize with the CERT escalation procedure.

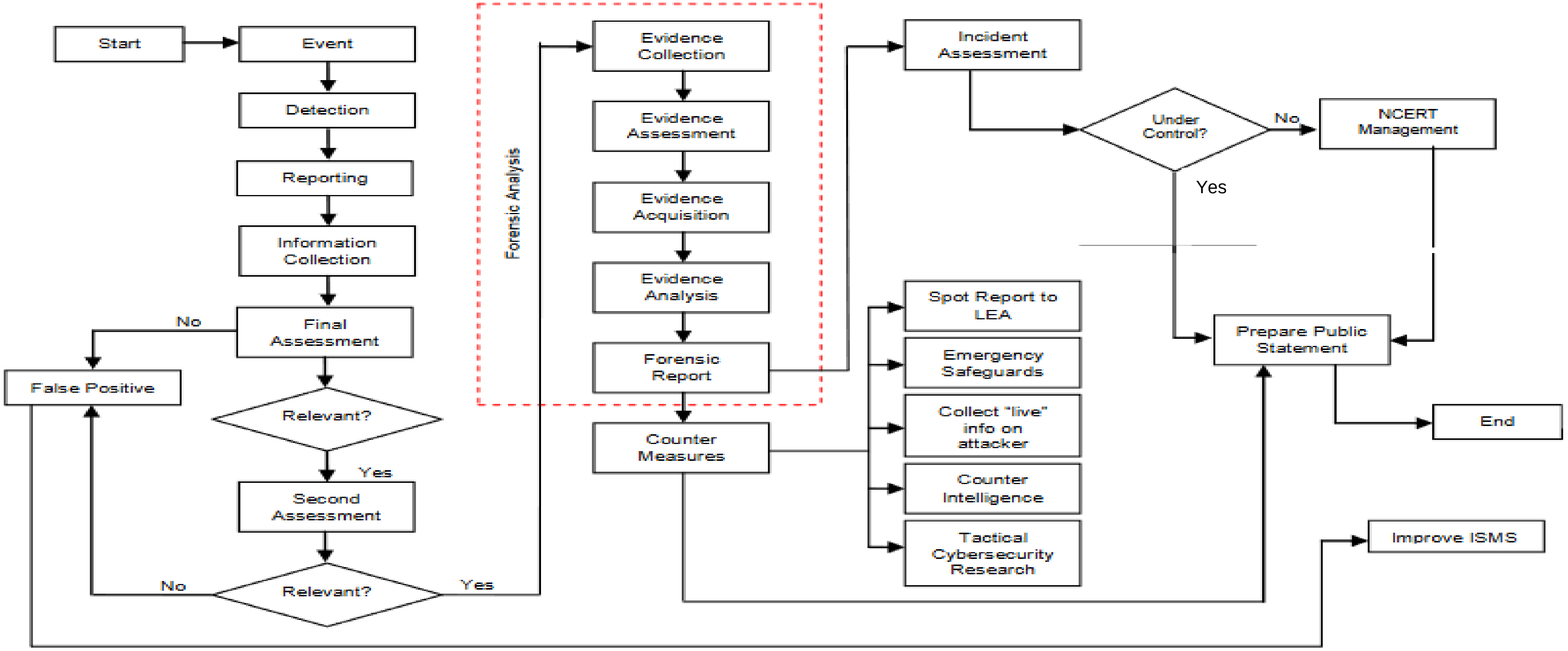
- Enable us to respond and act on the cyber incident that is within your responsibility.

- Utilization of the free tools available online.



Escalation Procedure

Incident Handling Flowchart

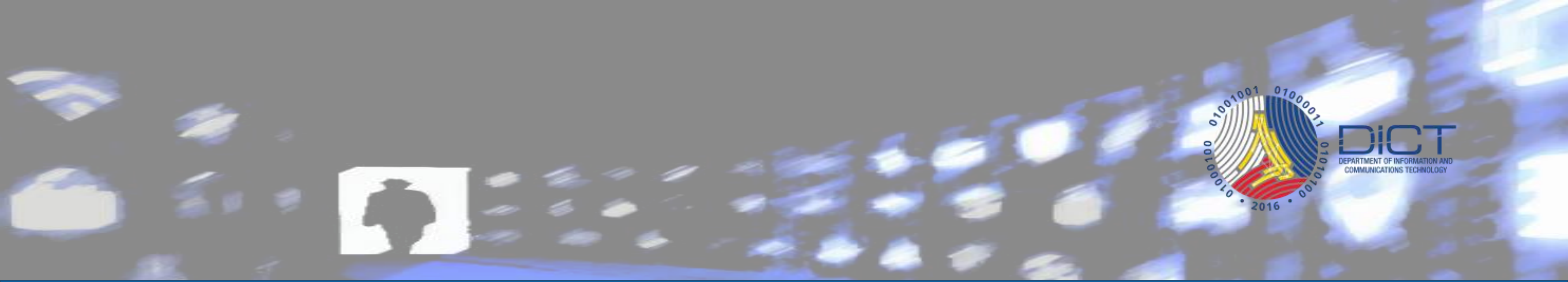


Factors to Consider for Escalation

- When results of the evaluation is determined to have an impact on the national security
- When the results of the evaluation have severe or catastrophic adverse impact to the organization
- When the results of the evaluation will is classified as critical and will severely affect the information system level of the organization
- When major issues become evident at the early stages of reporting
- When information security incident report is a recurring incident after it has been previously resolved

What are included in the Escalation Request?

- The type of event and when it happened
- Degree of severity or adverse impact
- The name of the person requesting for escalation and the official time stamp and date when escalation requests was made
- The case number assigned to the information security incident report.



Information Gathering & Incident Handling

Internet Abuse

This refers to the improper way of using the internet.

Common types of internet abuse:

- Website defacement
- Phishing
- Malware

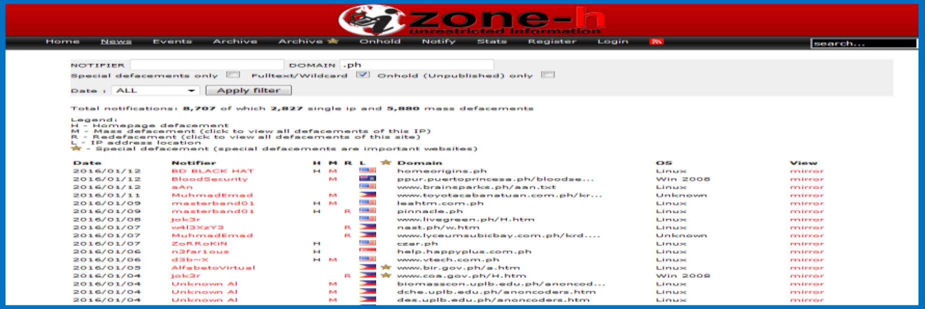
Public Feeds

Example of sites that provide free data feed on reported Internet abuse incidents:

- Defacement
  - http://www.zone-h.org/
  - https://google.com/
- Real-time Blacklist Mails
  - https://mxtoolbox.com/blacklists.aspx
- Phishing
  - https://www.phishtank.com/asn_search.php
- Malware - Botnet
  - https://zeustracker.abuse.ch/monitor.php

Public Feeds

- Web defacement
  http://www.zone-h.org



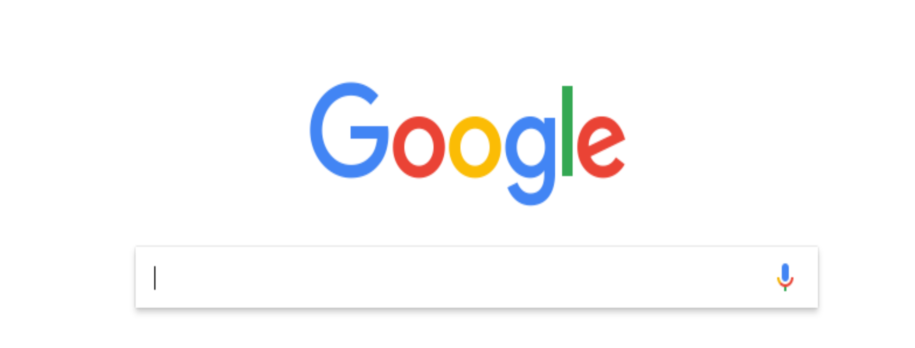
NOTIFIER DOMAIN .ph
Special defacements only □ Fulltext/Wildcard ☑ Onhold (Unpublished) only □
Date : ALL Apply filter

Total notifications: **8,707** of which **2,827** single ip and **5,880** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2016/01/12	BD BLACK HAT	H	M				homeorigins.ph	Linux	mirror
2016/01/12	BloodSecurity		M				ppur.puertoprincesa.ph/bloodse...	Win 2008	mirror
2016/01/12	aAn						www.brainsparks.ph/aan.txt	Linux	mirror
2016/01/11	MuhmadEmad		M				www.toyotacabanatuan.com.ph/kr...	Unknown	mirror
2016/01/09	masterband01	H	M				leahtm.com.ph	Linux	mirror
2016/01/09	masterband01	H		R			pinnacle.ph	Linux	mirror
2016/01/08	jok3r						www.livegreen.ph/H.htm	Linux	mirror
2016/01/07	w4l3XzY3			R			nast.ph/w.htm	Linux	mirror
2016/01/07	MuhmadEmad			R			www.lyceumsubicbay.com.ph/krd....	Unknown	mirror
2016/01/07	ZoRRoKiN	H					czar.ph	Linux	mirror
2016/01/06	n3farious	H					help.happyplus.com.ph	Linux	mirror
2016/01/06	d3b~X	H	M				www.vtech.com.ph	Linux	mirror
2016/01/05	AlfabetoVirtual					★	www.bir.gov.ph/a.htm	Linux	mirror
2016/01/04	jok3r			R		★	www.coa.gov.ph/H.htm	Win 2008	mirror
2016/01/04	Unknown Al		M				biomasscon.uplb.edu.ph/anoncod...	Linux	mirror
2016/01/04	Unknown Al		M				dche.uplb.edu.ph/anoncoders.htm	Linux	mirror
2016/01/04	Unknown Al		M				des.uplb.edu.ph/anoncoders.htm	Linux	mirror

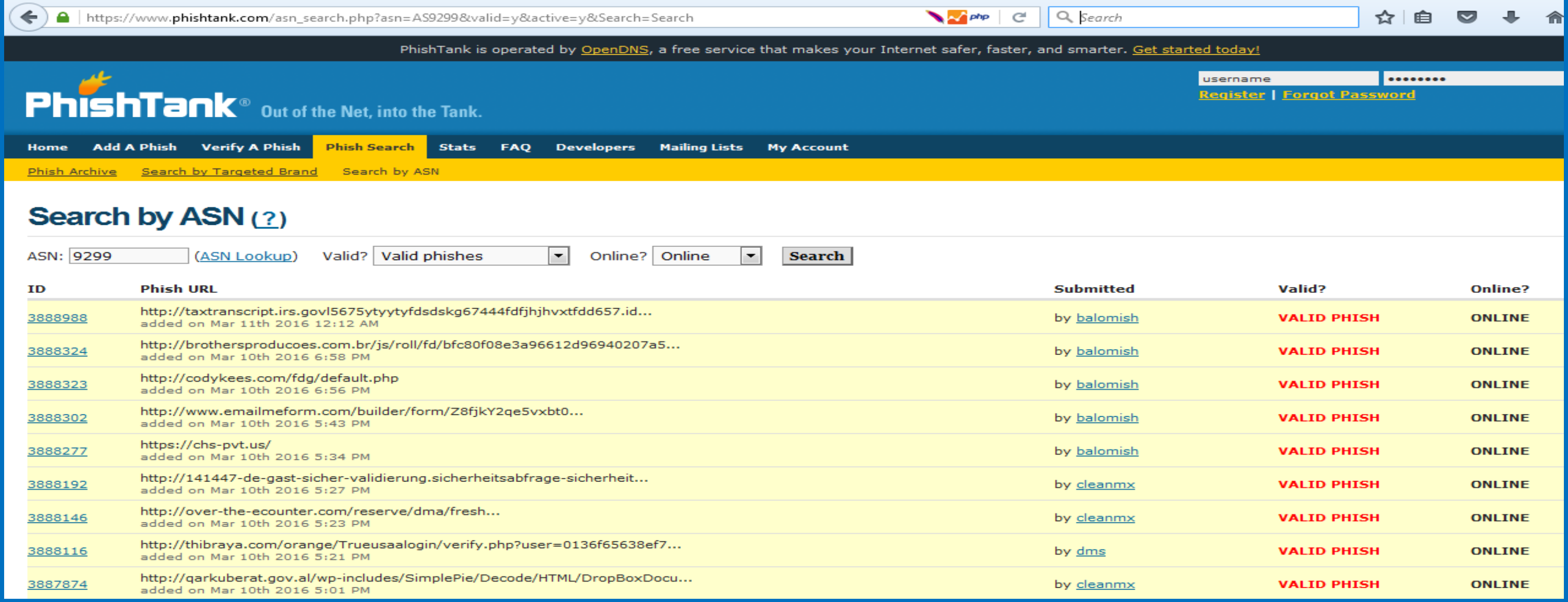
http://google.com



Public Feeds

Phishing

https://www.phishtank.com/asn_search.php



https://www.phishtank.com/asn_search.php?asn=AS9299&valid=y&active=y&Search=Search

PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank® Out of the Net, into the Tank.

username | •••••••••

Register | Forgot Password

Home | Add A Phish | Verify A Phish | Phish Search | Stats | FAQ | Developers | Mailing Lists | My Account

Phish Archive | Search by Targeted Brand | Search by ASN

Search by ASN (?)

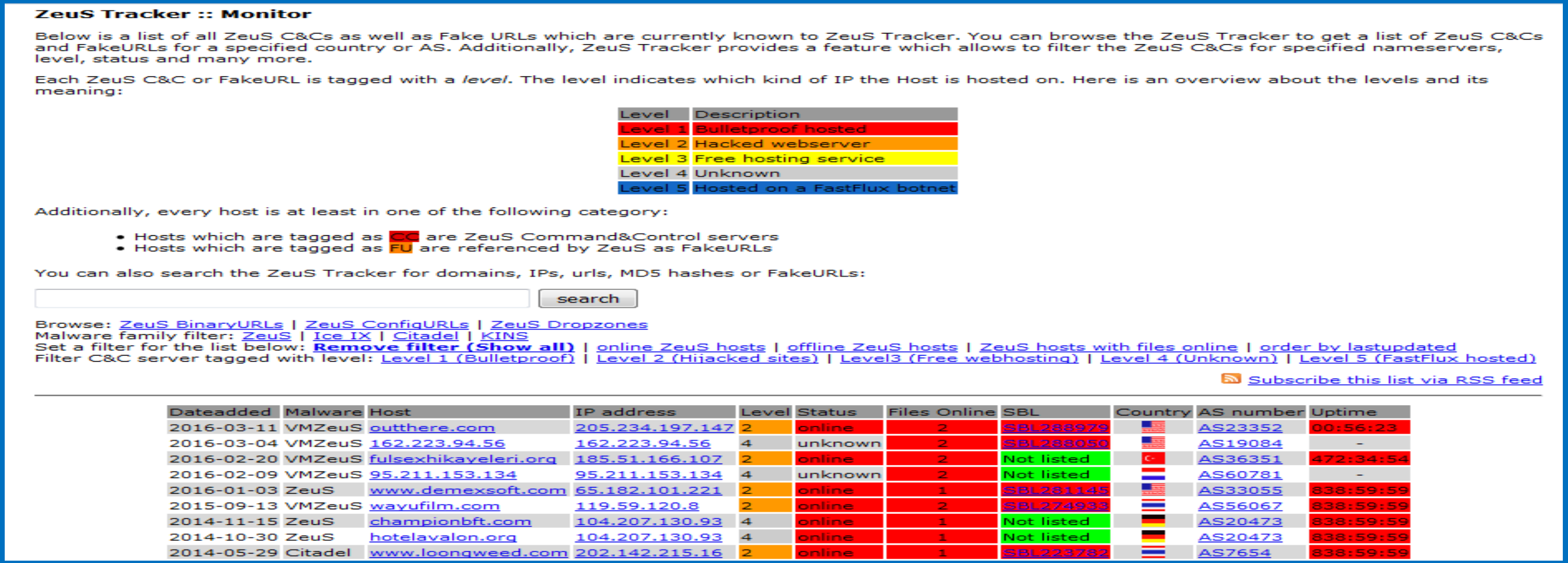
ASN: 9299 (ASN Lookup) Valid? Valid phishes Online? Online Search

ID	Phish URL	Submitted	Valid?	Online?
3888988	http://taxtranscript.irs.govl5675ytyytyfdsdskg67444fdfjhjhvxtfdd657.id... added on Mar 11th 2016 12:12 AM	by balomish	VALID PHISH	ONLINE
3888324	http://brothersproducoes.com.br/js/roll/fd/bfc80f08e3a96612d96940207a5... added on Mar 10th 2016 6:58 PM	by balomish	VALID PHISH	ONLINE
3888323	http://codykees.com/fdg/default.php added on Mar 10th 2016 6:56 PM	by balomish	VALID PHISH	ONLINE
3888302	http://www.emailmeform.com/builder/form/Z8fjkY2qe5vxbt0... added on Mar 10th 2016 5:43 PM	by balomish	VALID PHISH	ONLINE
3888277	https://chs-pvt.us/ added on Mar 10th 2016 5:34 PM	by balomish	VALID PHISH	ONLINE
3888192	http://141447-de-gast-sicher-validierung.sicherheitsabfrage-sicherheit... added on Mar 10th 2016 5:27 PM	by cleanmx	VALID PHISH	ONLINE
3888146	http://over-the-ecounter.com/reserve/dma/fresh... added on Mar 10th 2016 5:23 PM	by cleanmx	VALID PHISH	ONLINE
3888116	http://thibraya.com/orange/Trueusaalogin/verify.php?user=0136f65638ef7... added on Mar 10th 2016 5:21 PM	by dms	VALID PHISH	ONLINE
3887874	http://qarkuberat.gov.al/wp-includes/SimplePie/Decode/HTML/DropBoxDocu... added on Mar 10th 2016 5:01 PM	by cleanmx	VALID PHISH	ONLINE

Public Feeds

Malware - Botnet

https://zeustracker.abuse.ch/monitor.php



ZeuS Tracker :: Monitor

Below is a list of all ZeuS C&Cs as well as Fake URLs which are currently known to ZeuS Tracker. You can browse the ZeuS Tracker to get a list of ZeuS C&Cs and FakeURLs for a specified country or AS. Additionally, ZeuS Tracker provides a feature which allows to filter the ZeuS C&Cs for specified nameservers, level, status and many more.

Each ZeuS C&C or FakeURL is tagged with a *level*. The level indicates which kind of IP the Host is hosted on. Here is an overview about the levels and its meaning:

Level	Description
Level 1	Bulletproof hosted
Level 2	Hacked webserver
Level 3	Free hosting service
Level 4	Unknown
Level 5	Hosted on a FastFlux botnet

Additionally, every host is at least in one of the following category:

- Hosts which are tagged as CC are ZeuS Command&Control servers
- Hosts which are tagged as FU are referenced by ZeuS as FakeURLs

You can also search the ZeuS Tracker for domains, IPs, urls, MD5 hashes or FakeURLs:

search

Browse: ZeuS BinaryURLs | ZeuS ConfigURLs | ZeuS Dropzones
Malware family filter: ZeuS | Ice IX | Citadel | KINS
Set a filter for the list below: **Remove filter (Show all)** | online ZeuS hosts | offline ZeuS hosts | ZeuS hosts with files online | order by lastupdated
Filter C&C server tagged with level: Level 1 (Bulletproof) | Level 2 (Hijacked sites) | Level3 (Free webhosting) | Level 4 (Unknown) | Level 5 (FastFlux hosted)

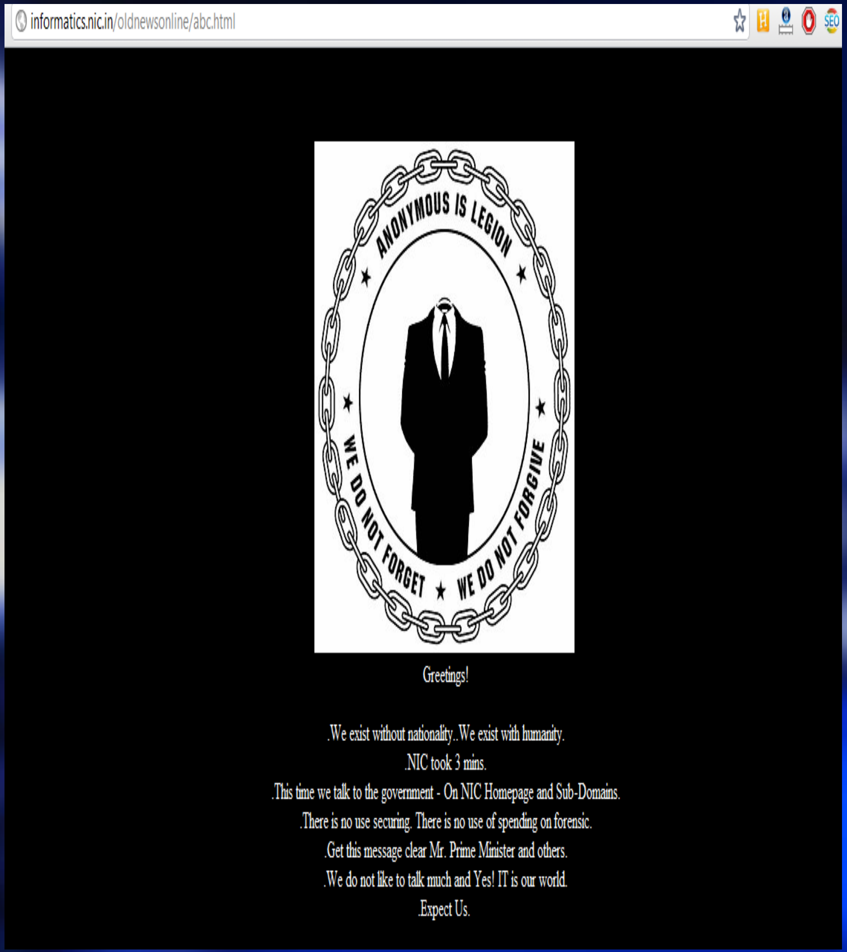
Subscribe this list via RSS feed

Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Uptime
2016-03-11	VMZeuS	outthere.com	205.234.197.147	2	online	2	SBL288979	🇺🇸	AS23352	00:56:23
2016-03-04	VMZeuS	162.223.94.56	162.223.94.56	4	unknown	2	SBL288050	🇺🇸	AS19084	-
2016-02-20	VMZeuS	fulsexhikayeleri.org	185.51.166.107	2	online	2	Not listed	🇹🇷	AS36351	472:34:54
2016-02-09	VMZeuS	95.211.153.134	95.211.153.134	4	unknown	2	Not listed	🇳🇱	AS60781	-
2016-01-03	ZeuS	www.demexsoft.com	65.182.101.221	2	online	1	SBL281145	🇺🇸	AS33055	838:59:59
2015-09-13	VMZeuS	wayufilm.com	119.59.120.8	2	online	2	SBL274933	🇹🇭	AS56067	838:59:59
2014-11-15	ZeuS	championbft.com	104.207.130.93	4	online	1	Not listed	🇩🇪	AS20473	838:59:59
2014-10-30	ZeuS	hotelavalon.org	104.207.130.93	4	online	1	Not listed	🇩🇪	AS20473	838:59:59
2014-05-29	Citadel	www.loongweed.com	202.142.215.16	2	online	1	SBL223782	🇹🇭	AS7654	838:59:59

Incident Handling

Process in incident handling:

- Identification
- Containment
- Eradication
- Recovery
- Documentation



Greetings!

.We exist without nationality..We exist with humanity.
.NIC took 3 mins.
.This time we talk to the government - On NIC Homepage and Sub-Domains.
.There is no use securing. There is no use of spending on forensic.
.Get this message clear Mr. Prime Minister and others.
.We do not like to talk much and Yes! IT is our world.
.Expect Us.

Web defacement

an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of defacers, who break into a web server and replace the hosted website with one of their own.

Incident Handling for Web Defacement

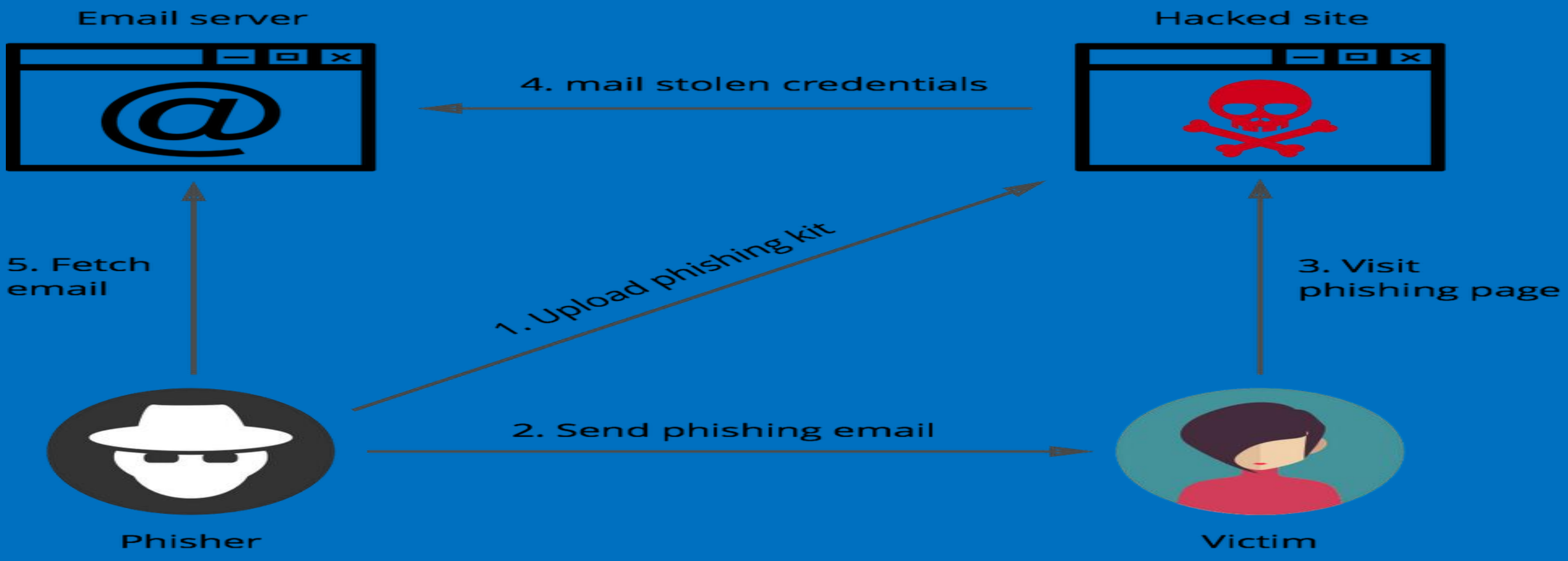
- Check if your website or online system is reported compromised.
  - Zone-h
  - Google Hacks
  - Social Media
- Check and analyze the reported incident.
- Temporarily remove the server from the network.
- Examine your server for files uploaded by the hacker.
- Remove the uploaded files by the hacker.
- Restore your services.
- Document all of the actions you have done for future reference.

Phishing

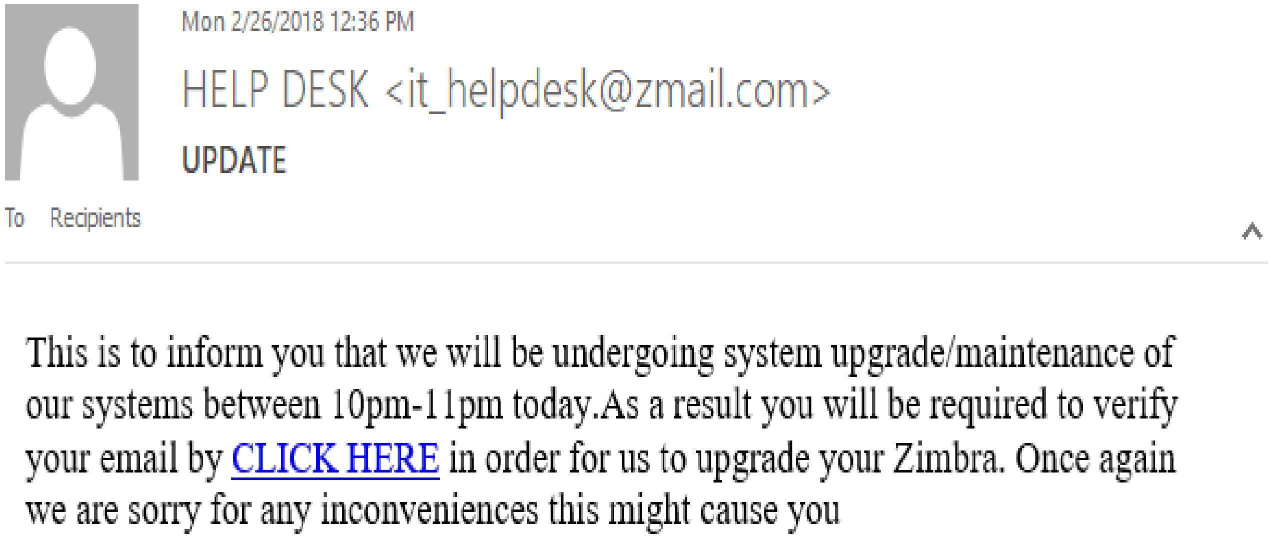
Attempt to fraudulently acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

- *Authentication information.*
- *Social Security Numbers.*
- *Stealing personal information.*
- *Account numbers*

Phishing


Email server
Hacked site
4. mail stolen credentials
5. Fetch email
1. Upload phishing kit
3. Visit phishing page
2. Send phishing email
Phisher
Victim

Sample Phishing



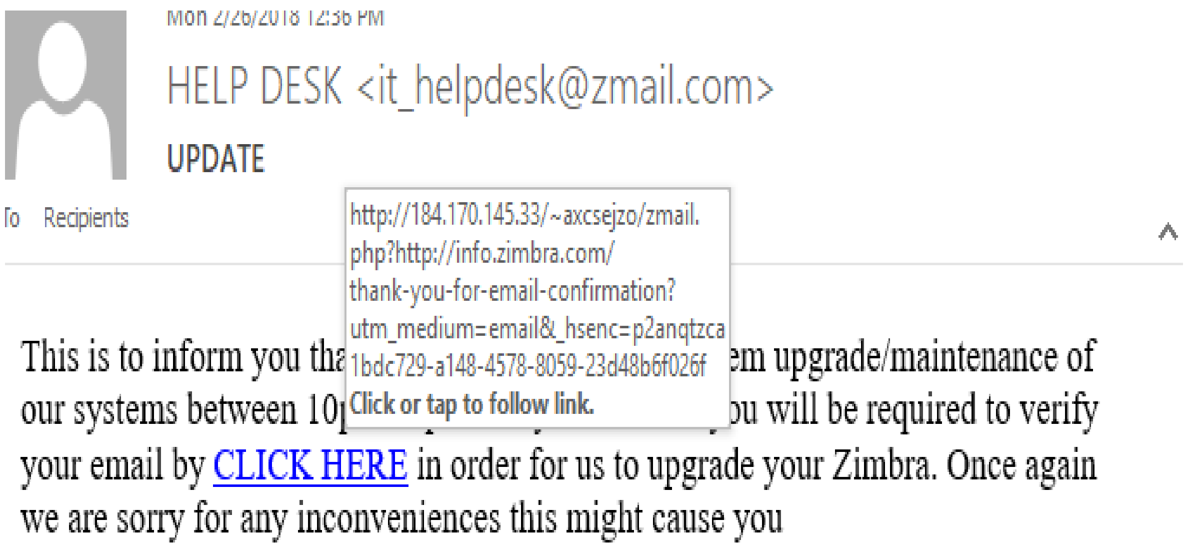
Mon 2/26/2018 12:36 PM

HELP DESK <it_helpdesk@zmail.com>

UPDATE

To Recipients

This is to inform you that we will be undergoing system upgrade/maintenance of our systems between 10pm-11pm today.As a result you will be required to verify your email by CLICK HERE in order for us to upgrade your Zimbra. Once again we are sorry for any inconveniences this might cause you



Mon 2/26/2018 12:36 PM

HELP DESK <it_helpdesk@zmail.com>

UPDATE

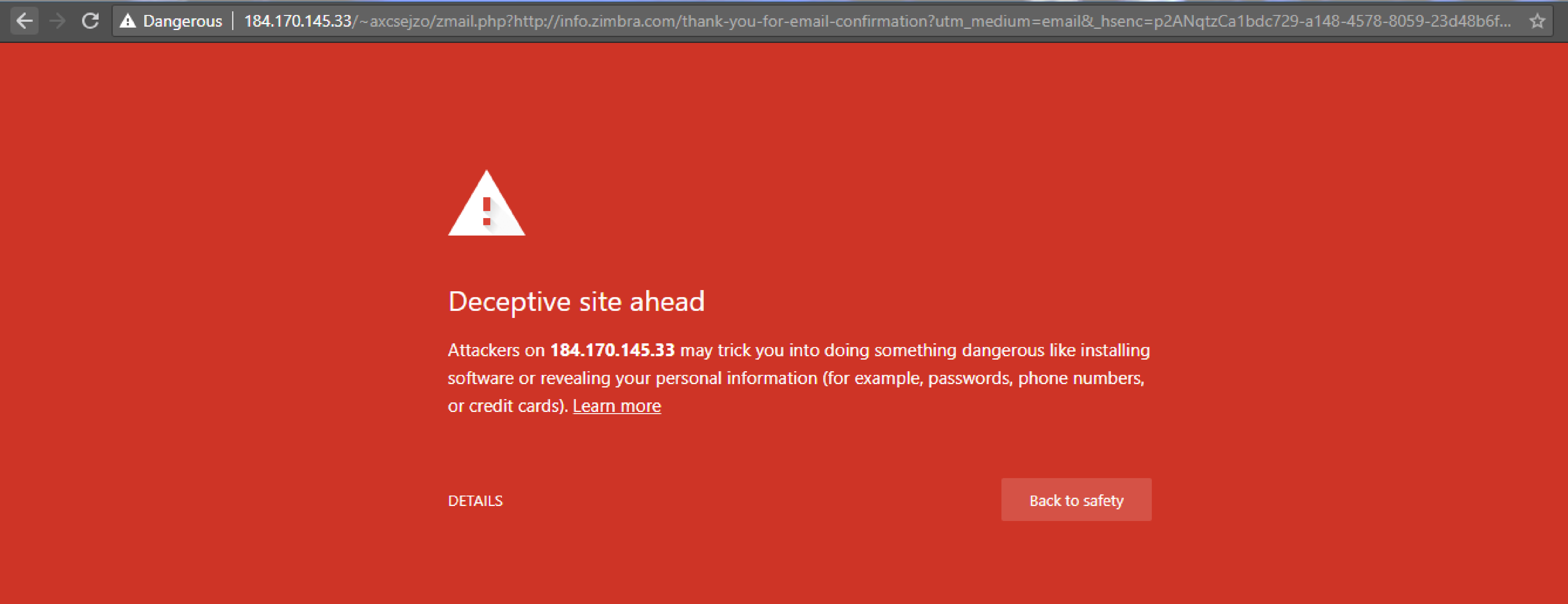
To Recipients

http://184.170.145.33/~axcsejzo/zmail.php?http://info.zimbra.com/thank-you-for-email-confirmation?utm_medium=email&_hsenc=p2anqtzca1bdc729-a148-4578-8059-23d48b6f026f

Click or tap to follow link.

This is to inform you tha em upgrade/maintenance of our systems between 10p ou will be required to verify your email by CLICK HERE in order for us to upgrade your Zimbra. Once again we are sorry for any inconveniences this might cause you

Sample Phishing



184.170.145.33/~axcsejzo/zmail.php?http://info.zimbra.com/thank-you-for-email-confirmation?utm_medium=email&_hsenc=p2ANqtzCa1bdc729-a148-4578-8059-23d48b6f...

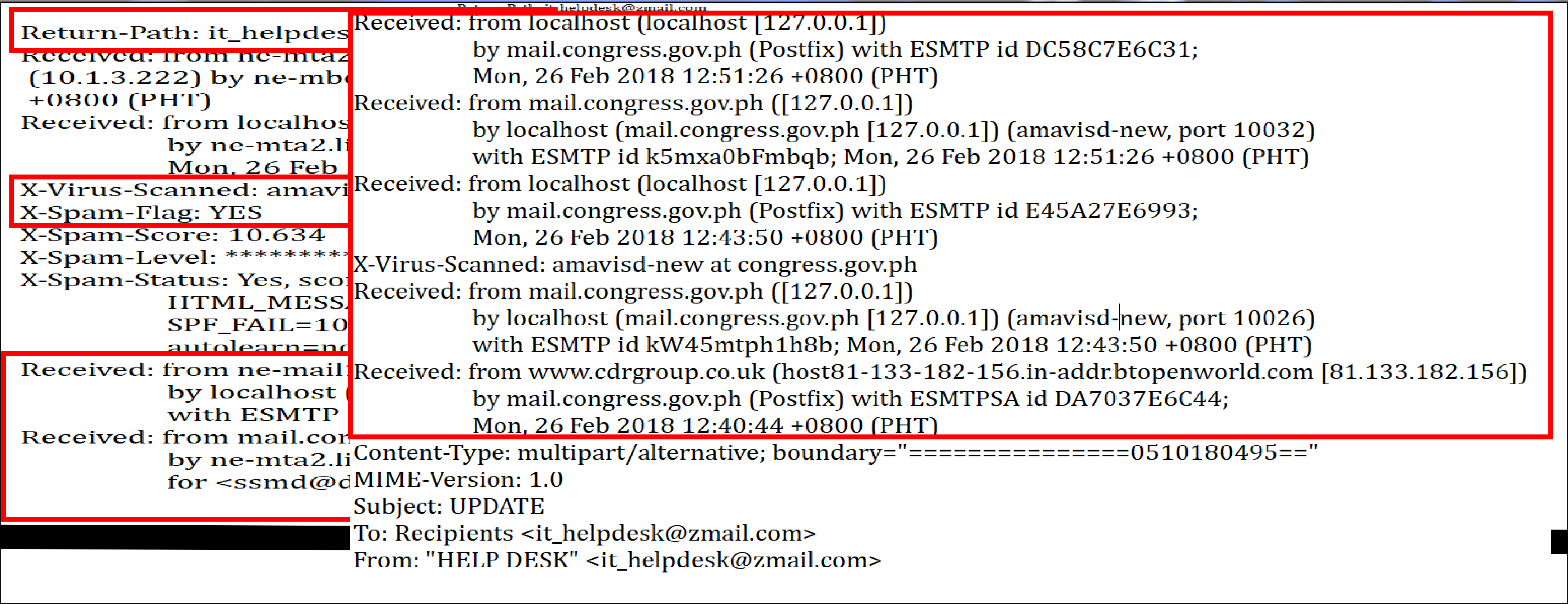
Deceptive site ahead

Attackers on **184.170.145.33** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

Incident Handling for Phishing

- Immediate changing of password.
- Check email header.
- Forward the email to the email administrator or postmaster.
- Check the domain of the email involved if it is listed as phishing or spam email on any RBL websites.
  - https://mxtoolbox.com/
  - https://www.ultratools.com/tools/spamDBLookup

Incident Handling for Phishing



```
Return-Path: it_helpdes
Received: from ne-mta2
 (10.1.3.222) by ne-mb
 +0800 (PHT)
Received: from localhos
          by ne-mta2.li
          Mon, 26 Feb
X-Virus-Scanned: amavi
X-Spam-Flag: YES
X-Spam-Score: 10.634
X-Spam-Level: *********
X-Spam-Status: Yes, sco
          HTML_MESS
          SPF_FAIL=10
          autolearn=no
Received: from ne-mail
          by localhost (
          with ESMTP
Received: from mail.con
          by ne-mta2.li
          for <ssmd@c
```

```
Return-Path: it_helpdesk@zmail.com
Received: from localhost (localhost [127.0.0.1])
        by mail.congress.gov.ph (Postfix) with ESMTP id DC58C7E6C31;
        Mon, 26 Feb 2018 12:51:26 +0800 (PHT)
Received: from mail.congress.gov.ph ([127.0.0.1])
        by localhost (mail.congress.gov.ph [127.0.0.1]) (amavisd-new, port 10032)
        with ESMTP id k5mxa0bFmbqb; Mon, 26 Feb 2018 12:51:26 +0800 (PHT)
Received: from localhost (localhost [127.0.0.1])
        by mail.congress.gov.ph (Postfix) with ESMTP id E45A27E6993;
        Mon, 26 Feb 2018 12:43:50 +0800 (PHT)
X-Virus-Scanned: amavisd-new at congress.gov.ph
Received: from mail.congress.gov.ph ([127.0.0.1])
        by localhost (mail.congress.gov.ph [127.0.0.1]) (amavisd-new, port 10026)
        with ESMTP id kW45mtph1h8b; Mon, 26 Feb 2018 12:43:50 +0800 (PHT)
Received: from www.cdrgroup.co.uk (host81-133-182-156.in-addr.btopenworld.com [81.133.182.156])
        by mail.congress.gov.ph (Postfix) with ESMTPSA id DA7037E6C44;
        Mon, 26 Feb 2018 12:40:44 +0800 (PHT)
Content-Type: multipart/alternative; boundary="===============0510180495=="
MIME-Version: 1.0
Subject: UPDATE
To: Recipients <it_helpdesk@zmail.com>
From: "HELP DESK" <it_helpdesk@zmail.com>
```

• If you have doubts on the email

- Ask directly the sender if the email came from him using another media.
- If there is an attachment on the email.
  - ➢ Check the attachment.
  - ➢ Download the attachment but do not run/execute.
  - ➢ Check the attachment using VirusTotal.

    https://virustotal.com/

Malware

Trojan

Virus

Botnet

Worm

Rootkits

Spyware

Ransomware

Adware

- Malware is software which interferes with the normal operation of a computer system.
- It is software that performs unauthorized functions causing the normal operation of the computer system to be abnormal.

Symptoms of Infection

- Unusual increase in CPU usage.
- Slow computer or web browser speeds.
- Problems connecting to networks.
- Freezing or crashing.
- Modified or deleted files.
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves
- Strange computer behaviour.
- Emails/messages being sent automatically and without user’s knowledge

Incident Handling Malware Infection

- Identify all the infected workstation.
- Remove the infected workstation from the network.
- Ask the employees that is held reliable on the infected workstation.
- Run a thorough investigation on the malware that infected the workstations.

  Manual Malware Analysis.

  - ➢ Use a virtual machine.
  - ➢ Record/document the initial running process of the virtual machine.
  - ➢ Run the malware file.
  - ➢ Record/document the running process of the virtual machine and compare it to the initial.
  - ➢ Check the network traffic of the virtual machine by installing a network analyzer tool.
  - ➢ Document all the IP address and Domain where the workstation is communicating with.

Incident Handling Malware Infection

- Remove the malware that has infected the workstations.
  - You may use the tools below which are free:

HiJackThis

https://sourceforge.net/projects/hjt/

Windows Sysinternals

https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

Windows Defender

- Block the IP address and domain where the test virtual machine communicates.
- Document all actions performed and improve end-user policy.

QUESTIONS?

darryle.caparas@dict.gov.ph

END OF PRESENTATION