Philippine’s CyberSecurity Strategy

Gen Macalinao
CyberSecurity Bureau

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

RECENT CYBER THREATS

JAN

$534 million is stolen from Japan's largest digital currency exchange.

Coincheck

FEB

AdultSwine, a mobile malware infecting children's game apps with adware, is downloaded by up to 7 million users.

MAR

The City of Atlanta suffers an attack that locks down city systems for over a week.

APR

Saks Fifth Avenue

Saks 5th Avenue and Lord & Taylor have five million customers' credit card details stolen.

MAY

Users of Copenhagen's city bikes are denied access due to the system being hacked.

CITY OF COPENHAGEN

JUN

EXACTIS

340 million records of Americans and business are leaked from the Florida-based marketing firm.

JUL

Singapore suffers its biggest cyber attack with the theft of 1.5 million patient records, including the Prime Minister's.

SingHealth

AUG

BRITISH AIRWAYS

Hackers attack British Airways' mobile app and steal credit card details of almost 400,000 customers.

SEP

30 million Facebook users' phone numbers and personal details are exposed in a major breach of privacy.

facebook

OCT

ONWASA

Onslow Water and Sewer Authority suffers a ransomware attack impeding efforts to provide services.

NOV

Hackers steal the personal details of 500 million Marriott owned Starwood Hotel customers.

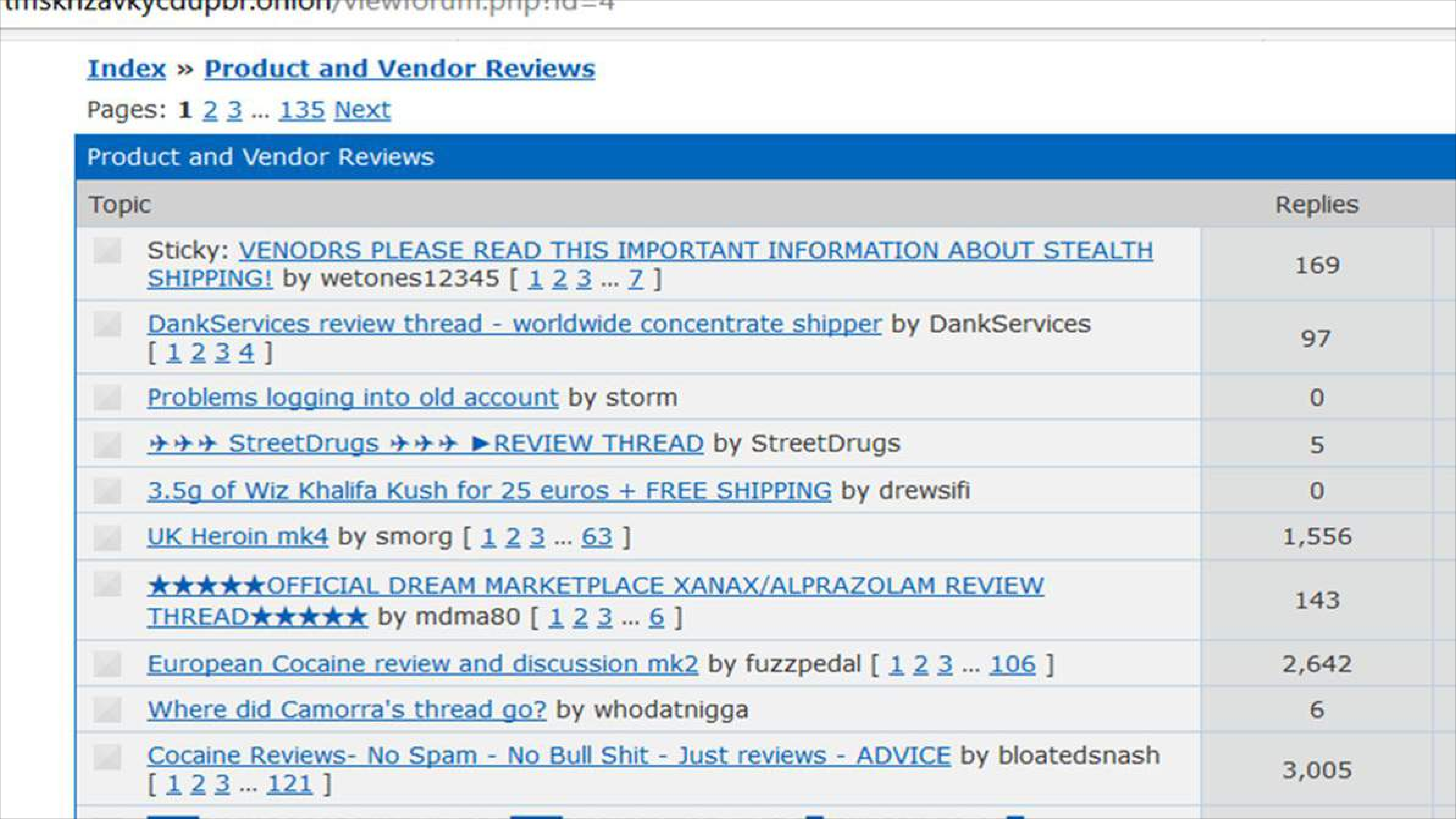
Marriott
HOTELS · RESORTS · SUITES

DEC

THE WALL STREET JOURNAL.

Ransomware causes printing and delivery disruptions to the LA Times, WSJ and NYT newspapers.

The Dark Web



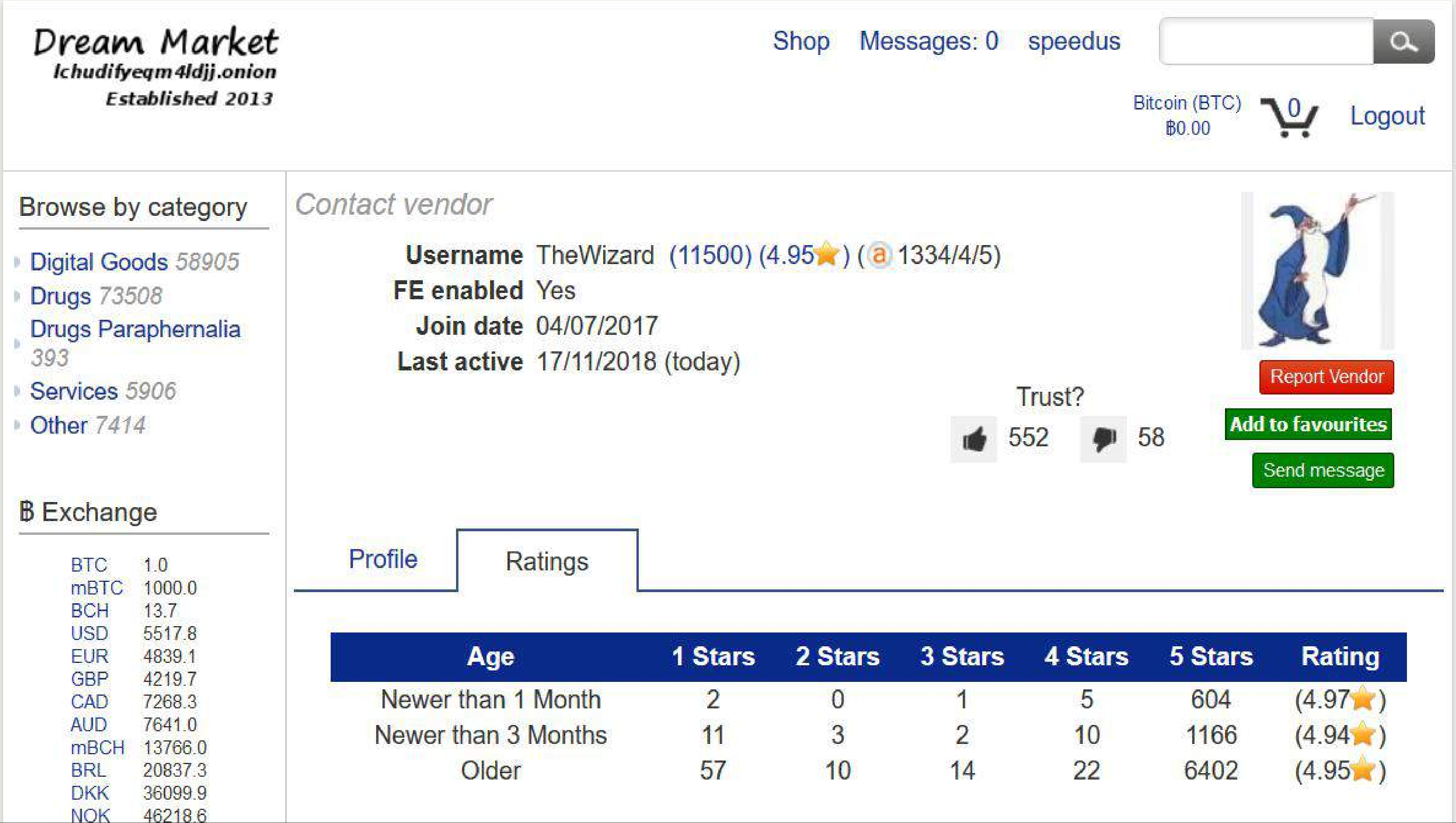
tmskhzavkycdupbr.onion/viewforum.php?id=4

Index » Product and Vendor Reviews

Pages: 1 2 3 ... 135 Next

Product and Vendor Reviews

Topic	Replies
Sticky: VENODRS PLEASE READ THIS IMPORTANT INFORMATION ABOUT STEALTH SHIPPING! by wetones12345 [1 2 3 ... 7]	169
DankServices review thread - worldwide concentrate shipper by DankServices [1 2 3 4]	97
Problems logging into old account by storm	0
✈✈✈ StreetDrugs ✈✈✈ ►REVIEW THREAD by StreetDrugs	5
3.5g of Wiz Khalifa Kush for 25 euros + FREE SHIPPING by drewsifi	0
UK Heroin mk4 by smorg [1 2 3 ... 63]	1,556
★★★★★OFFICIAL DREAM MARKETPLACE XANAX/ALPRAZOLAM REVIEW THREAD★★★★★ by mdma80 [1 2 3 ... 6]	143
European Cocaine review and discussion mk2 by fuzzpedal [1 2 3 ... 106]	2,642
Where did Camorra's thread go? by whodatnigga	6
Cocaine Reviews- No Spam - No Bull Shit - Just reviews - ADVICE by bloatedsnash [1 2 3 ... 121]	3,005



Dream Market
lchudifyeqm4ldjj.onion
Established 2013

Shop Messages: 0 speedus

Bitcoin (BTC)
฿0.00

0

Logout

Browse by category

- Digital Goods *58905*
- Drugs *73508*
- Drugs Paraphernalia *393*
- Services *5906*
- Other *7414*

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	13.7
USD	5517.8
EUR	4839.1
GBP	4219.7
CAD	7268.3
AUD	7641.0
mBCH	13766.0
BRL	20837.3
DKK	36099.9
NOK	46218.6

Contact vendor

Username	TheWizard (11500) (4.95★) (ⓐ 1334/4/5)
FE enabled	Yes
Join date	04/07/2017
Last active	17/11/2018 (today)

Trust?

👍 552 👎 58

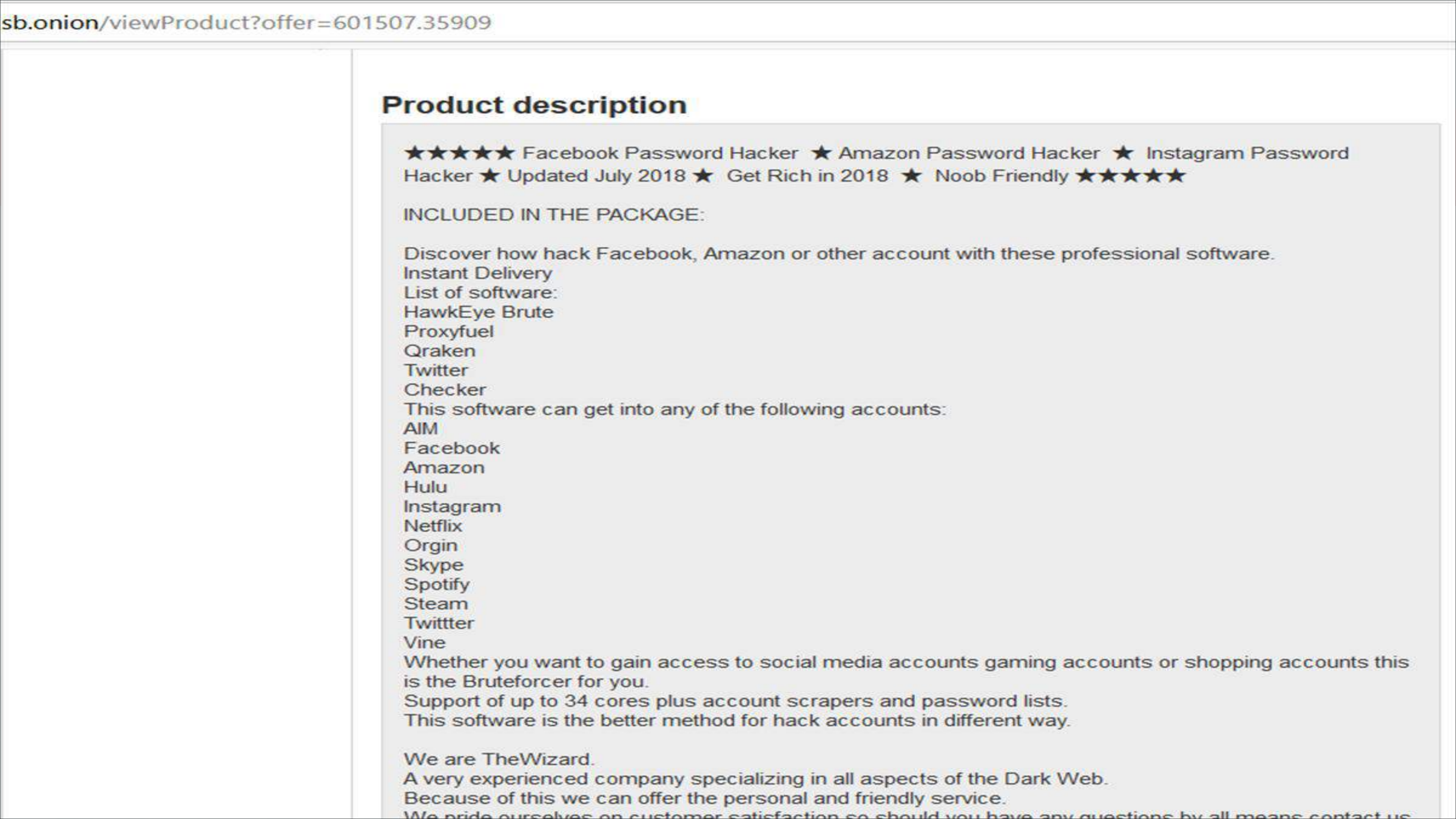
Report Vendor

Add to favourites

Send message

Profile Ratings

Age	1 Stars	2 Stars	3 Stars	4 Stars	5 Stars	Rating
Newer than 1 Month	2	0	1	5	604	(4.97★)
Newer than 3 Months	11	3	2	10	1166	(4.94★)
Older	57	10	14	22	6402	(4.95★)



sb.onion/viewProduct?offer=601507.35909

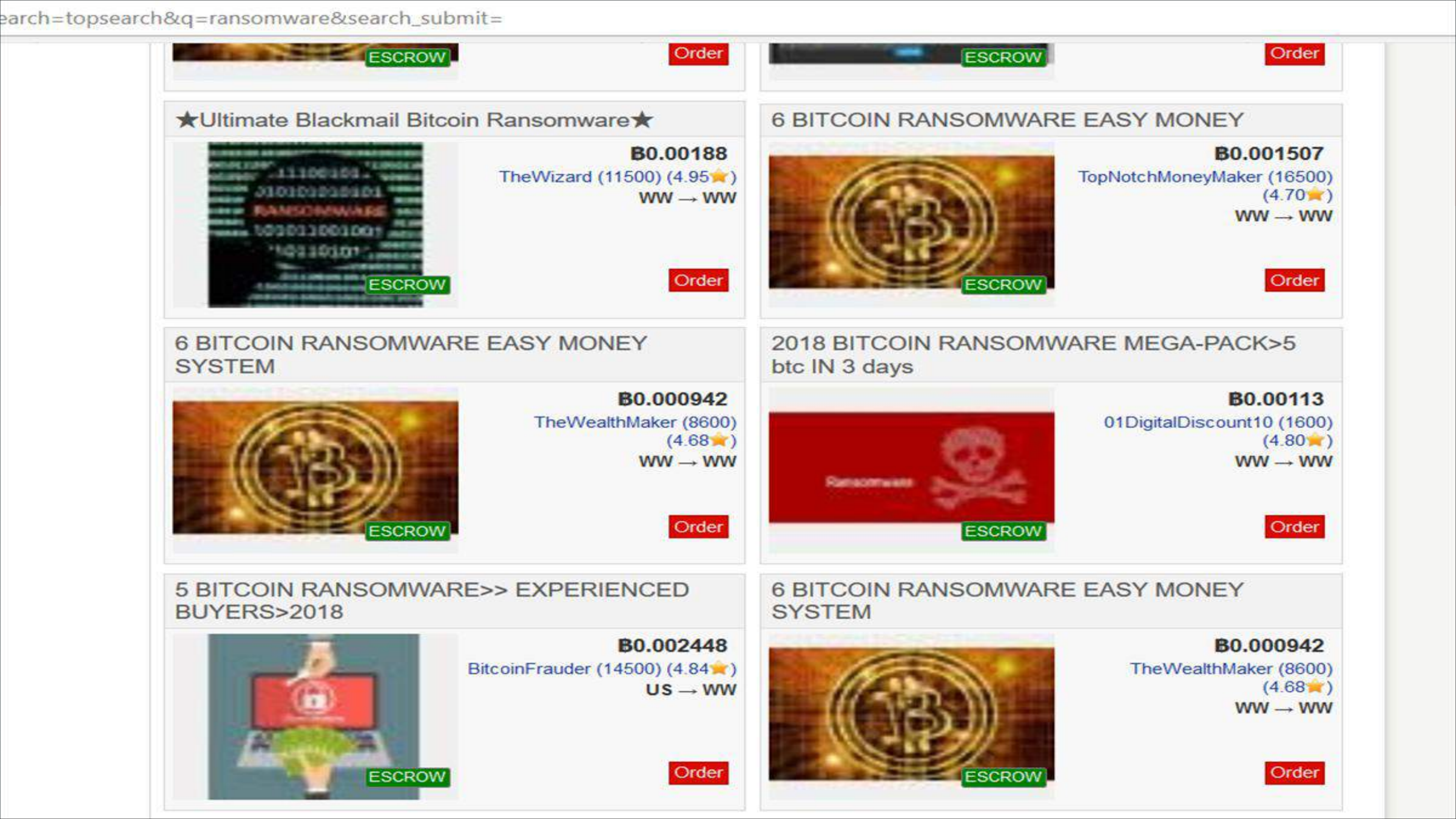
Product description

★★★★★ Facebook Password Hacker ★ Amazon Password Hacker ★ Instagram Password Hacker ★ Updated July 2018 ★ Get Rich in 2018 ★ Noob Friendly ★★★★★

INCLUDED IN THE PACKAGE:

Discover how hack Facebook, Amazon or other account with these professional software.
Instant Delivery
List of software:
HawkEye Brute
Proxyfuel
Qraken
Twitter
Checker
This software can get into any of the following accounts:
AIM
Facebook
Amazon
Hulu
Instagram
Netflix
Orgin
Skype
Spotify
Steam
Twittter
Vine
Whether you want to gain access to social media accounts gaming accounts or shopping accounts this is the Bruteforcer for you.
Support of up to 34 cores plus account scrapers and password lists.
This software is the better method for hack accounts in different way.

We are TheWizard.
A very experienced company specializing in all aspects of the Dark Web.
Because of this we can offer the personal and friendly service.
We pride ourselves on customer satisfaction so should you have any questions by all means contact us



earch=topsearch&q=ransomware&search_submit=

ESCROW Order

ESCROW Order

★Ultimate Blackmail Bitcoin Ransomware★

Ƀ0.00188
TheWizard (11500) (4.95★)
WW → WW

ESCROW Order

6 BITCOIN RANSOMWARE EASY MONEY

Ƀ0.001507
TopNotchMoneyMaker (16500) (4.70★)
WW → WW

ESCROW Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM

Ƀ0.000942
TheWealthMaker (8600) (4.68★)
WW → WW

ESCROW Order

2018 BITCOIN RANSOMWARE MEGA-PACK>5 btc IN 3 days

Ƀ0.00113
01DigitalDiscount10 (1600) (4.80★)
WW → WW

ESCROW Order

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018

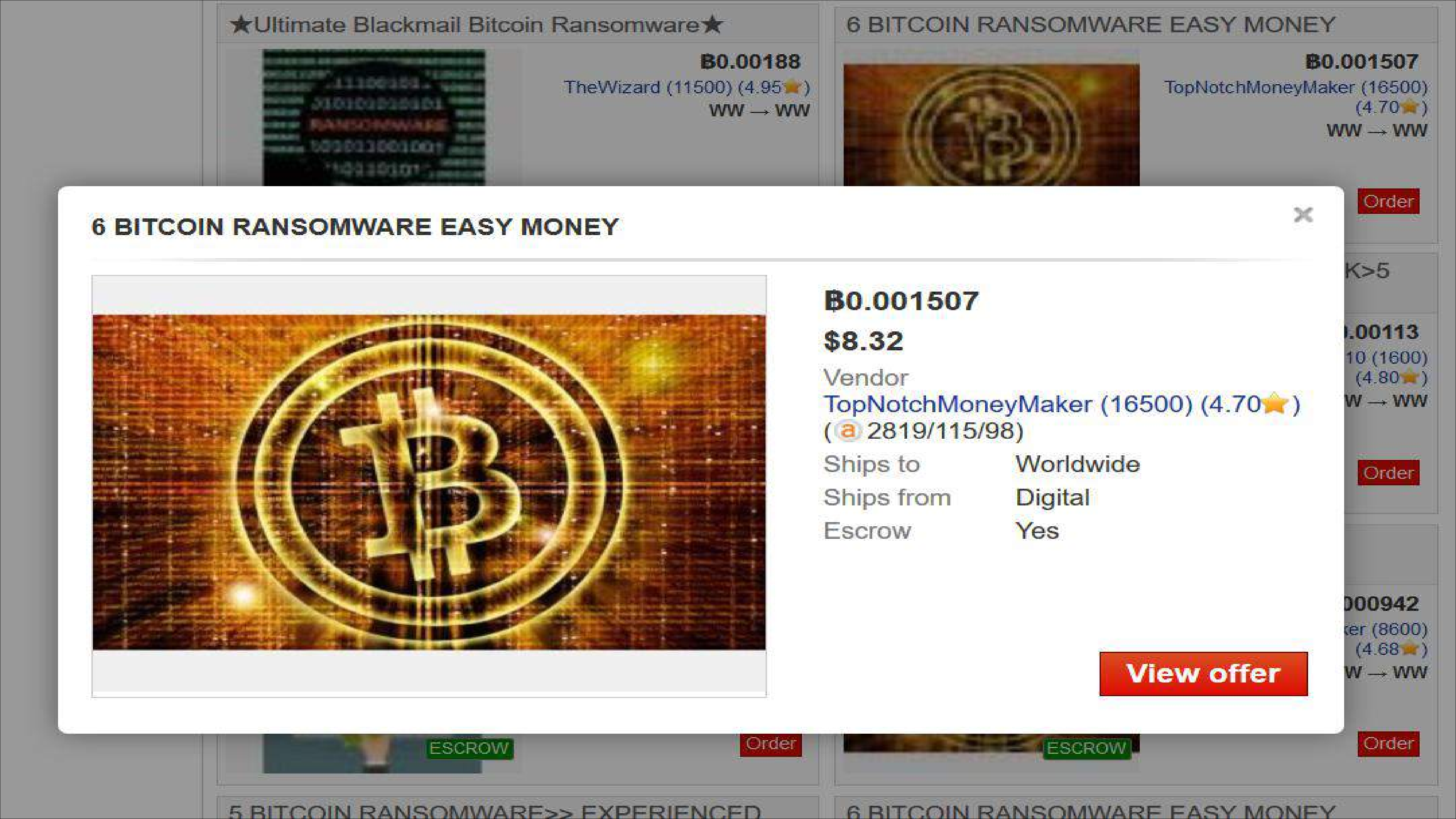
Ƀ0.002448
BitcoinFrauder (14500) (4.84★)
US → WW

ESCROW Order

6 BITCOIN RANSOMWARE EASY MONEY SYSTEM

Ƀ0.000942
TheWealthMaker (8600) (4.68★)
WW → WW

ESCROW Order



★Ultimate Blackmail Bitcoin Ransomware★

Ƀ0.00188

TheWizard (11500) (4.95★)

WW → WW

6 BITCOIN RANSOMWARE EASY MONEY

Ƀ0.001507

TopNotchMoneyMaker (16500) (4.70★)

WW → WW

Order

6 BITCOIN RANSOMWARE EASY MONEY

Ƀ0.001507

$8.32

Vendor
TopNotchMoneyMaker (16500) (4.70★)
(ⓐ 2819/115/98)

Ships to	Worldwide
Ships from	Digital
Escrow	Yes

View offer

K>5

.00113

10 (1600)

(4.80★)

W → WW

Order

000942

ker (8600)

(4.68★)

W → WW

ESCROW

Order

ESCROW

Order

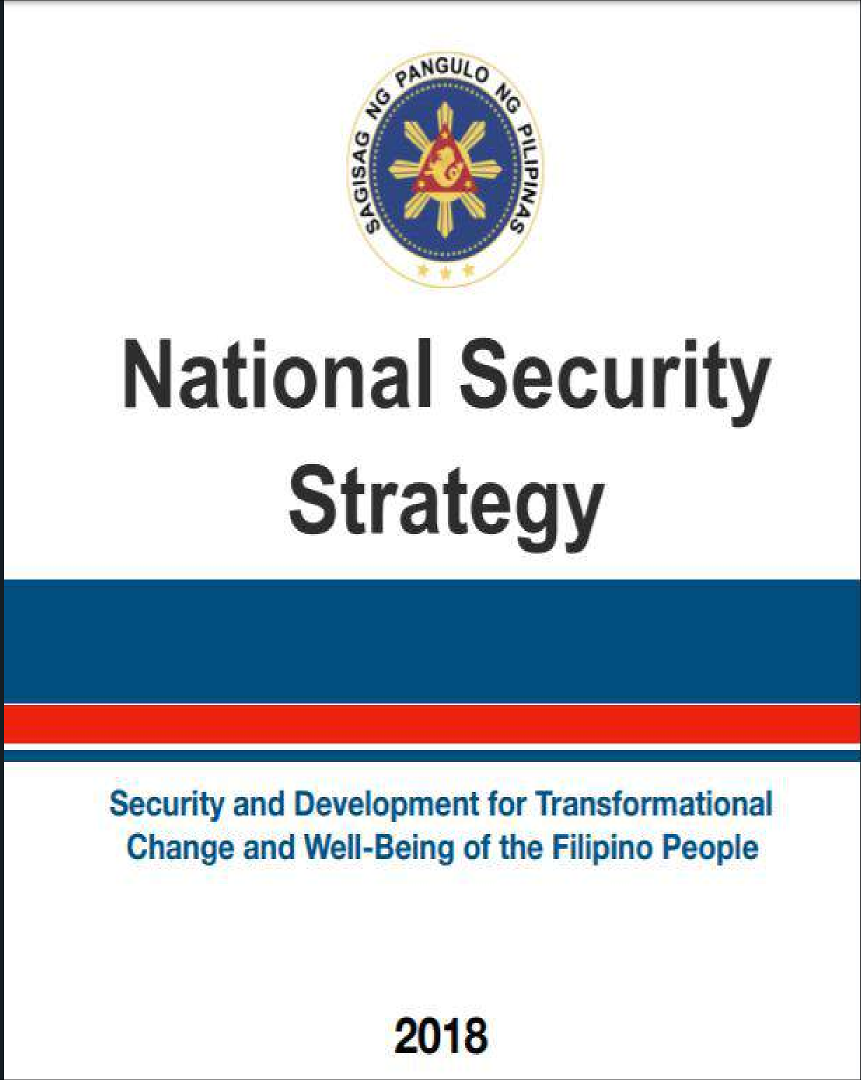
5 BITCOIN RANSOMWARE>> EXPERIENCED

6 BITCOIN RANSOMWARE EASY MONEY

Attacks to CII	**B**ank Heist, **N**avigation Systems Manipulation, **C**ontrol of Electronic Medical Equipment and Records, **O**verride of Oil and Gas Systems
Attacks to Government Infostructure	**H**acking resulting in Data breach **D**efacement of PH Government Agencies Websites
Sophistication of Cyber Attacks	**A**PT, **D**DoS, **S**PAM, **S**pear Phishing, **S**ocial Engineering

12-pt National Security Goals

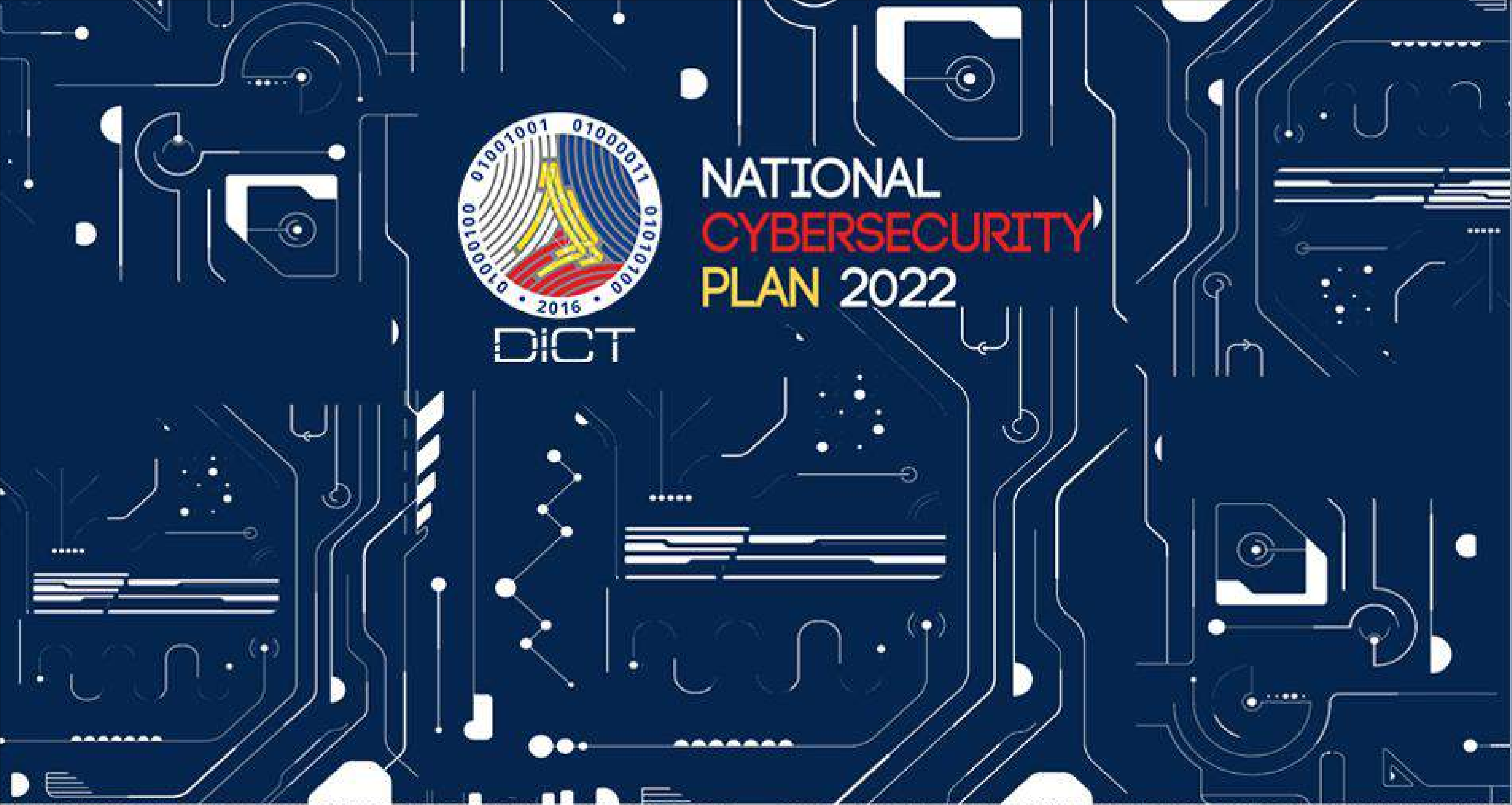
- Guarantee public safety and achieve good governance
- Mitigate the impact of health related threats
- Develop a dynamic, inclusive, and sustainable economy
- Achieve food and water security
- Safeguard and preserve national sovereignty and territorial integrity
- Heighten consciousness and pride on Filipino heritage, culture and values
- Promote human and ecological security
- Achieve energy security
- Ensure maritime and airspace security
- Strengthen international relations
- PROVIDE STRONG CYBER INFRASTRUCTURE AND CYBER SECURITY
- Improve vital transportation infrastructure and port security



National Security Strategy

Security and Development for Transformational Change and Well-Being of the Filipino People

2018

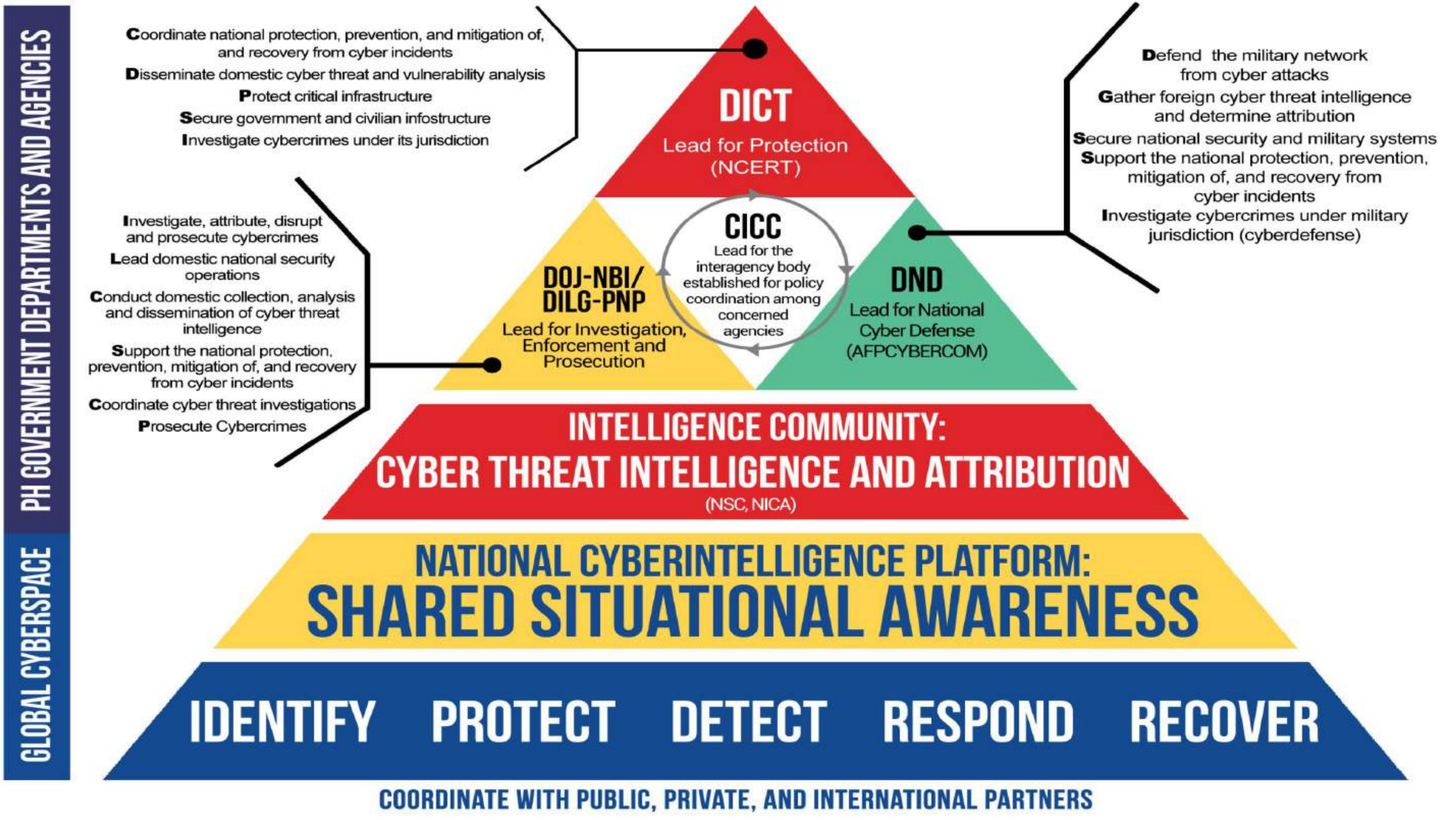


DICT

NATIONAL CYBERSECURITY PLAN 2022

01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 01010000 01101100 01100001 01101110
01000011 01111001 01100010 01100101 01110010 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

01001110 01100001 01110100 01101001 01101111 01101110 01100001 01101100 01010000 01101100 01100001 01101110
01000011 01111001 01100010 01100101 01110010 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001



PH GOVERNMENT DEPARTMENTS AND AGENCIES

GLOBAL CYBERSPACE

Coordinate national protection, prevention, and mitigation of, and recovery from cyber incidents

Disseminate domestic cyber threat and vulnerability analysis

Protect critical infrastructure

Secure government and civilian infostructure

Investigate cybercrimes under its jurisdiction

DICT

Lead for Protection (NCERT)

Defend the military network from cyber attacks

Gather foreign cyber threat intelligence and determine attribution

Secure national security and military systems

Support the national protection, prevention, mitigation of, and recovery from cyber incidents

Investigate cybercrimes under military jurisdiction (cyberdefense)

Investigate, attribute, disrupt and prosecute cybercrimes

Lead domestic national security operations

Conduct domestic collection, analysis and dissemination of cyber threat intelligence

Support the national protection, prevention, mitigation of, and recovery from cyber incidents

Coordinate cyber threat investigations

Prosecute Cybercrimes

DOJ-NBI/ DILG-PNP

Lead for Investigation, Enforcement and Prosecution

CICC

Lead for the interagency body established for policy coordination among concerned agencies

DND

Lead for National Cyber Defense (AFPCYBERCOM)

INTELLIGENCE COMMUNITY: CYBER THREAT INTELLIGENCE AND ATTRIBUTION

(NSC, NICA)

NATIONAL CYBERINTELLIGENCE PLATFORM: SHARED SITUATIONAL AWARENESS

IDENTIFY PROTECT DETECT RESPOND RECOVER

COORDINATE WITH PUBLIC, PRIVATE, AND INTERNATIONAL PARTNERS

Key Strategic Imperatives

Protection of Critical Infostructure (CII)

CyberSecurity Assessment and Compliance Programs

Protection of Government Networks (Public and Military)

Public Networks thru establishment of CERTs

Military Networks thru establishment of Cyber Defense Centers (DND, NSC, AFP)

Protection of Businesses and Supply Chains

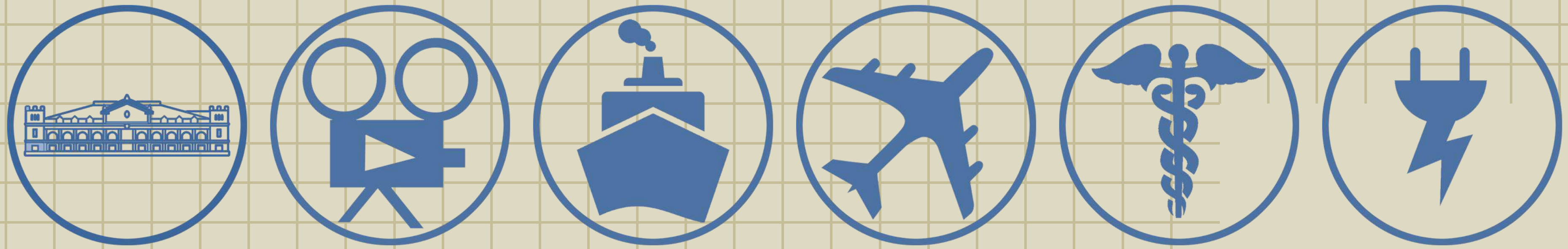
National Common Criteria Evaluation and Certification Program

Protection of Individuals

CyberSecurity Education Campaign Program

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Critical Infostructure



DICT
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

National CyberSecurity Plan Implementation Milestones

Memorandum Circulars 005 to 007, s2017

Issuance of Memorandum Circulars (MC) on the following:

- **Protection of Critical Infostructure (DICT-MC 005);**
- **Protection of Government Agencies (DICT-MC 006; and**
- **Protection of Individuals (DICT-MC 007)**

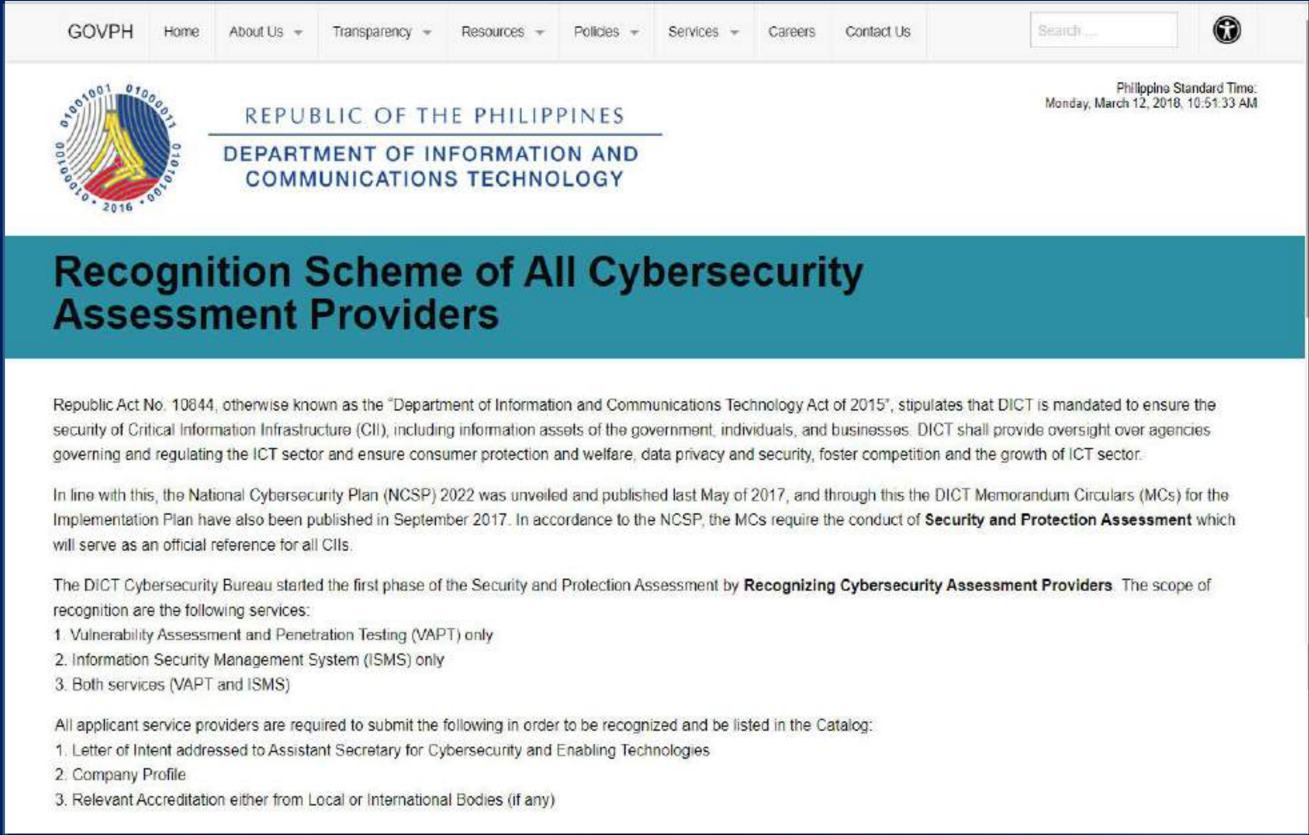
•The MCs state the general policies of the state in cybersecurity and directs relevant agencies and companies to comply

•The MCs can be downloaded at www.dict.gov.ph

DICT Security Assessment Recognition Scheme

- DICT CyberSecurity Bureau Conducts VAPT for government Agencies

- For government agencies and other CIIs who prefer private companies to do the VAPT, the Bureau has a Recognition Scheme for all Cybersecurity Assessment Providers


GOVPH
Home
About Us
Transparency
Resources
Policies
Services
Careers
Contact Us
Search ...
REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
Philippine Standard Time:
Monday, March 12, 2018, 10:51:33 AM

Recognition Scheme of All Cybersecurity Assessment Providers

Republic Act No. 10844, otherwise known as the "Department of Information and Communications Technology Act of 2015", stipulates that DICT is mandated to ensure the security of Critical Information Infrastructure (CII), including information assets of the government, individuals, and businesses. DICT shall provide oversight over agencies governing and regulating the ICT sector and ensure consumer protection and welfare, data privacy and security, foster competition and the growth of ICT sector.

In line with this, the National Cybersecurity Plan (NCSP) 2022 was unveiled and published last May of 2017, and through this the DICT Memorandum Circulars (MCs) for the Implementation Plan have also been published in September 2017. In accordance to the NCSP, the MCs require the conduct of **Security and Protection Assessment** which will serve as an official reference for all CIIs.

The DICT Cybersecurity Bureau started the first phase of the Security and Protection Assessment by **Recognizing Cybersecurity Assessment Providers**. The scope of recognition are the following services:

1. Vulnerability Assessment and Penetration Testing (VAPT) only
2. Information Security Management System (ISMS) only
3. Both services (VAPT and ISMS)

All applicant service providers are required to submit the following in order to be recognized and be listed in the Catalog:

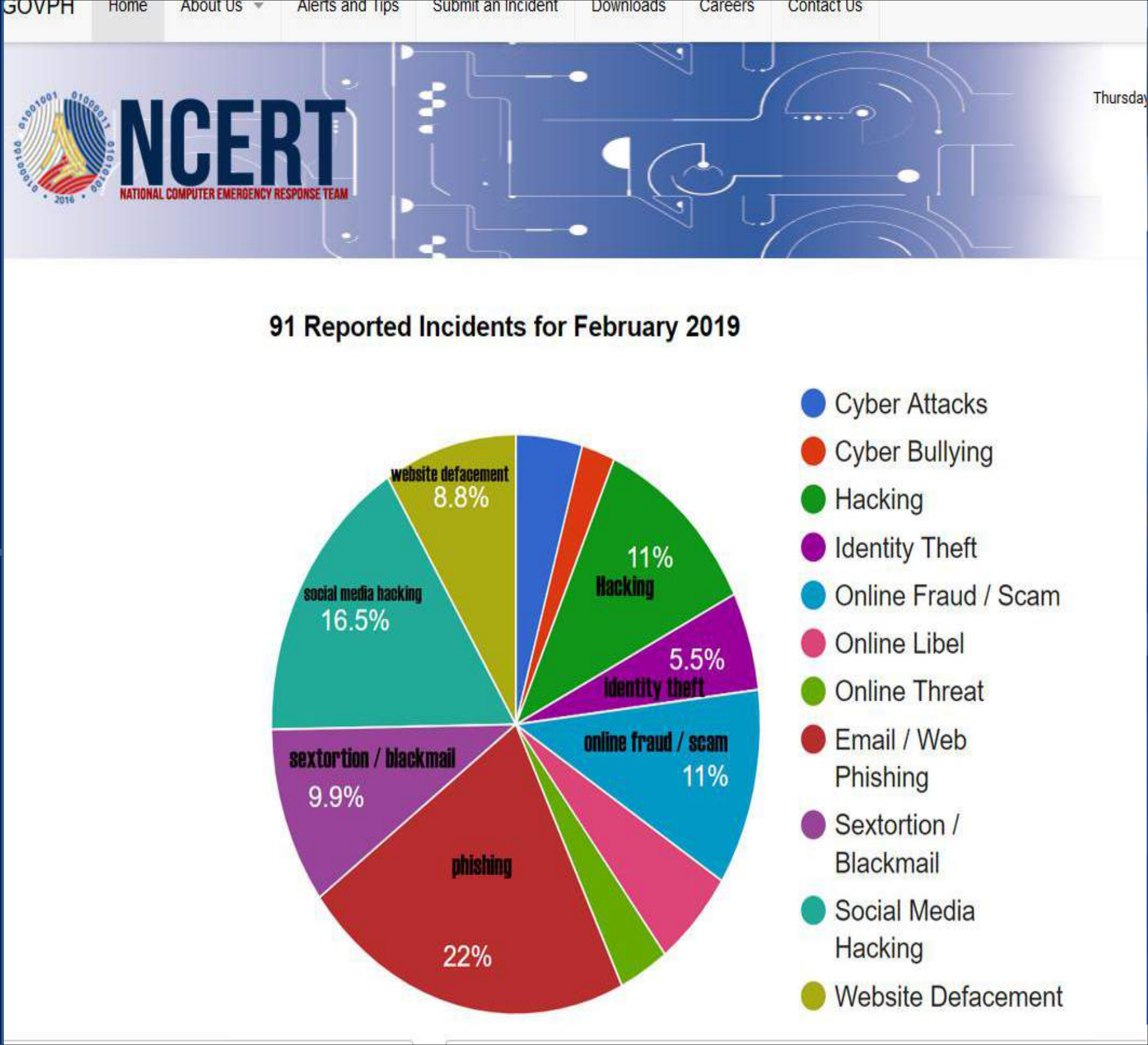
1. Letter of Intent addressed to Assistant Secretary for Cybersecurity and Enabling Technologies
2. Company Profile
3. Relevant Accreditation either from Local or International Bodies (if any)

National Computer Emergency Response Team Website (NCERT Website)

- Status: Launched at the Philippine Cybersecurity Conference 2018
- This is an informative website focusing on threat and vulnerability warnings and alerts
- It has an embedded Helpdesk Ticketing System that shareholders can use in reporting cyber attacks and cybercrimes

Incident Report Statistics System

- Status: 100% working
- It is a web application that is used to collect data and transform information and incidents reported to CERT-PH into usable statistics



91 Reported Incidents for February 2019

Critical Infostructure FGDs

Computer Emergency Response Team (CERT) Manual

- The draft of the Computer Emergency Response Team (CERT) Manual has been disseminated to CIIs and government agencies for inputs.

Engagements with Government and CIIs on the creation of Government and Sectoral CERTs

- FGD with the Energy Sector representatives – Oct. 23, 2017
- Meeting with the Military Sector/AFP – Nov. 8, 2017
- FGD with Energy Sector - April 18, 2018
- FGD with Banking and Finance Sector - May 21, 2018
- DOE Cybersecurity Policy Writeshop – June 13-14, 2018
- FGD with BPO and Health Sectors- June 26, 2018
- FGD with transportation, Water, Utilities, and Emergency Services Sectors – August 3, 2018

Capacity Building Initiatives

CERT Training

Course 001: CERT Training – May 22-23, 2018

- 45 Participants (DICT Clusters and IT officers of Priority Agencies)

Course 001: CERT Training – August 31, 2018

- 50 Participants (IT and Policy officers of Priority Different Agencies)

Energy Sectoral CERT

What has been done?

- FGD with the Energy Sector resulting in identification of the Department of Energy (DOE) as lead for the Energy Sectoral CERT
- CyberSecurity Policy Writeshop with DOE
- CERT Training for DOE IT personnel

What's next?

- Establishment of the National Energy Cybersecurity Governance Framework
- National CyberSecurity Strategy for the Energy Sector
- DOE's Cyber Resilience Network Infrastructure (CRNI)

Cybersecurity Caravans

- The main cybersecurity awareness program of the DICT is the CyberSecurity Caravan conducted in various schools nationwide.

- Thirteen (13) cybersecurity caravans have been conducted so far with the following number of attendees:

Universidad de Zamboanga (Zamboanga City) – 1,200 participants

Ateneo De Davao University (Davao City) – 800 participants

Laguna State Polytechnic University (San Pablo City) – 2,000 participants

University of San Carlos (Cebu) – 250 participants

Taytay, Rizal – 2,000 participants

Catanduanes State University (Catanduanes) – 700 participants

Ateneo De Naga (Naga City) – 500 participants

AMA Computer University (Quezon City) – 1,300 participants

University of Science and Technology of Southern Philippines (CDO) – 3,000

Siliman University (Dumaguete City) – 1,200 participants

Bataan Peninsula State University (Bataan) – 1,000 participants

Olongapo City – 700 participants

Bicol University (Legazpi City) – 2,200 participants

Integration of Cybersecurity in the Academe

Campaign to integrate CyberSecurity into the Philippine education system

- Partnership with the Commission on Higher Education to develop a cybersecurity curriculum tailor-fit for the Philippines
- Meeting with school administrators all over the country
- Through this advocacy, the following have pioneered the offering of the following in their respective universities:

**AMA Computer Universit
y**

Bachelor of Science in CyberSecurity

Holy Angel University (Pampanga)

**Professional Science Ma
sters
(PSM) in CyberSecurity**

FIRST
AND ONLY ONE IN THE PHILIPPINES!
PROFESSIONAL SCIENCE MASTER'S (PSM) IN
CYBERSECURITY
HOLY ANGEL UNIVERSITY GRADUATE SCHOOL

National Cyber Intelligence Platform

CyberSecurity Management Systems Project (CMSP)

- Request for Information (RFI) Meeting – March 19, 2018
- Posting of Biddings Docs on Philippine Star and PHILGEPS website – May 30, 2018
- Pre-Bidding Conference – June 7, 2018
- Bid Opening – August 6, 2018
- Awarding of Contract – December 2018

Protection of the most vulnerable sector of the society

Child Online Protection

- Anti- Cyberbullying
- Anti- Online Sexual Exploitation of Children
- Digital Parenting

- Launch of the Anti-Cyberbullying video competition for high school & college students | Jul 9, 2018
- FGD on Digital Parenting | August 5, 2018
- Focus Group Discussion on Anti-Online Sexual Exploitation of Children | Aug 8, 2018
- Digital Parenting Conference for DICT | Aug 25, 2018
- Child Online Protection Stakeholders Consultation | September 28, 2018

Rule on Cybercrime Warrants

DICT CyberSecurity Bureau served as Subject Matter Expert (SME) in the development of the RCW which took effect August 15, 2018.

International Cooperation

The Philippines became the 57th party to the Budapest Convention after the Senate unanimously concurred on the signing of the instrument of accession in February 2018.

The Philippines endorsed the Paris Call for Trust and Security in Cyberspace in November 2018.

The Philippines actively and strongly supports ASEAN initiatives towards norms and legal frameworks in the region.

DICT Memorandum Circulars 005, 006, 007, s2017

01001001 01000011 01010100 01000100 • 2016 •

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

SingHealth data breach findings:

- Tardiness in raising the alarm : Poor incident response system
- Weak administrative passwords
- Unpatched workstation

GENERAL POLICIES for CRITICAL INFOSTRUCTURE

- **Adoption of PNS ISO/IEC 27000 Family of Standards and other relevant International Standards for Mandatory Compliance**
- **Conduct of Annual Risk and Vulnerability Assessment**
- **Conduct of Security Assessment**
- **Creation of CERT**
- **Certificate of Cybersecurity Compliance**
- **Telecommunications Cyber Hygiene**
- **Seal of Cybersecurity**
- **Preparation of the Disaster Recovery and Business Continuity Plans**
- **Conduct of National Cyber Drills and Exercises**
- **Privacy of Personal Data**
- **Monitoring and Evaluation of Compliance to the NCSP 2022**

http://www.dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-005.pdf

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

GENERAL POLICIES for GOVERNMENT AGENCIES

- Establishment of Government Computer Emergency Response Teams (GCERT)
- Collaboration with Local and International Linkages
- Privacy of Personal Data
- Responsibility of Agency Heads
- Monitoring and Evaluation of Compliance to the NCSP 2022
- Organizational Membership

http://www.dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-006.pdf

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

GENERAL POLICIES for the Protection of Individuals

- #PRInt (Paper, Radio, Internet (Social Media) and Television
- Observation of Cybersecurity Awareness Week
- Philippine Government Websites
- Responsibility of Agency Heads
- Monitoring and Evaluation of Compliance to the NCSP 2022
- Organizational Membership

http://www.dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-007.pdf

Creation of CERT

- All identified CIIs shall create its own CERT
- DICT Cybersecurity Bureau shall handle the Philippines National CERT (CERT-PH) which will serve as the central authority for all CERTs in the country
- Information sharing shall be done with the use of established communication protocol – Traffic Light Protocol (TLP)

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

TRAFFIC LIGHT PROTOCOL

- Red : not for disclosure, restricted to participants only.
- Amber : limited disclosure, restricted to participants’ organizations.
- Green : limited disclosure, restricted to the community.
- White : disclosure is not limited.

Creation of Sectoral CERT

- All CIIs shall create a Sectoral CERT to be headed by a Chairman and elected among member organizations

- The Chairman shall then report to the DICT on a periodic basis

DICT
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

DICT

NATIONAL CYBERSECURITY PLAN 2022

The END

THANK YOU!