CERT-PH
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

Annual **Report**

cert-ph@dict.gov.ph
8920-0101 local 1708 | 2378
www.ncert.gov.ph

ABOUT US

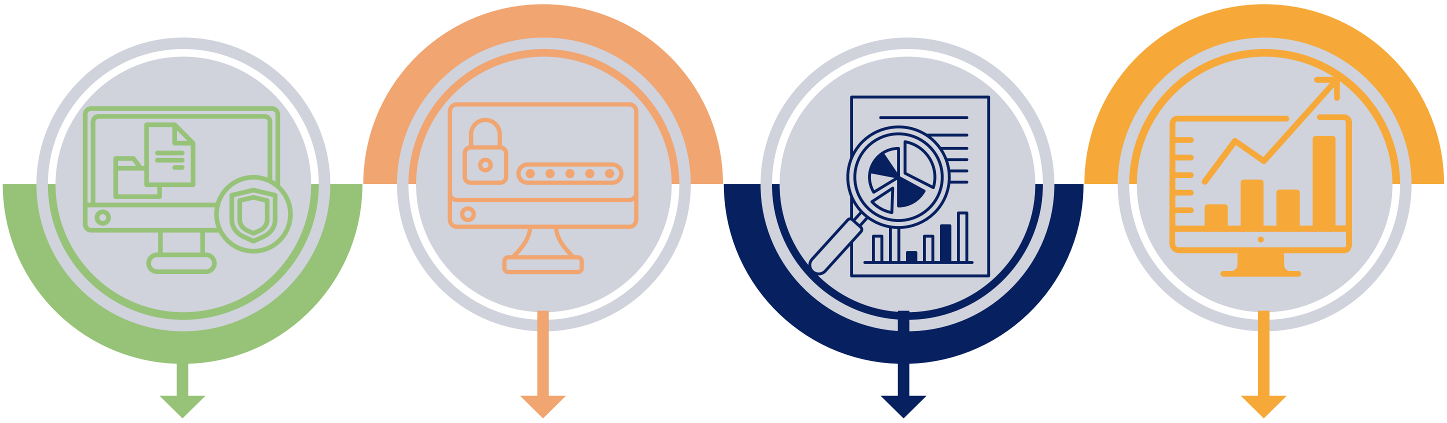
INTRODUCTION

The National Computer Emergency Response Team (NCERT) Division under the Cybersecurity Bureau, Department of Information and Communications Technology (DICT) is responsible for receiving, reviewing, and responding to computer security incident reports and activities.

CERT-PH also monitors the implementation of the information security incident response plan to ensure that detected and reported cybersecurity incidents and events are given appropriate and immediate response.

The CERT-PH is the highest body for cybersecurity related activities. All CERTs, Government CERTS, Sectoral (or Private) CERTs, as well as organizational CERTs shall coordinate and report incidents to the National CERT.

CERT-PH CORE FUNCTIONS



INCIDENT RESPONSE

- Responds to Cybersecurity incidents reported to the Bureau (internal and external to the Department);
- Monitors the implementation of the Information Security Incident Response Plan to ensure that detected, and reported incidents are given appropriate immediate action;
- Develops well-structured processes for handling and managing information security events and enabling tools, methodologies, and practices.

SECURITY OPERATIONS CENTER

- Administers the operations of the Cybersecurity Management System Project (CMSP);
- Conducts regular network monitoring security testing, source code analysis, vulnerability and risk management, and escalation and resolution of cybersecurity-related incidents;
- Monitors the system for possible information security threats and injects countermeasures and remedies.

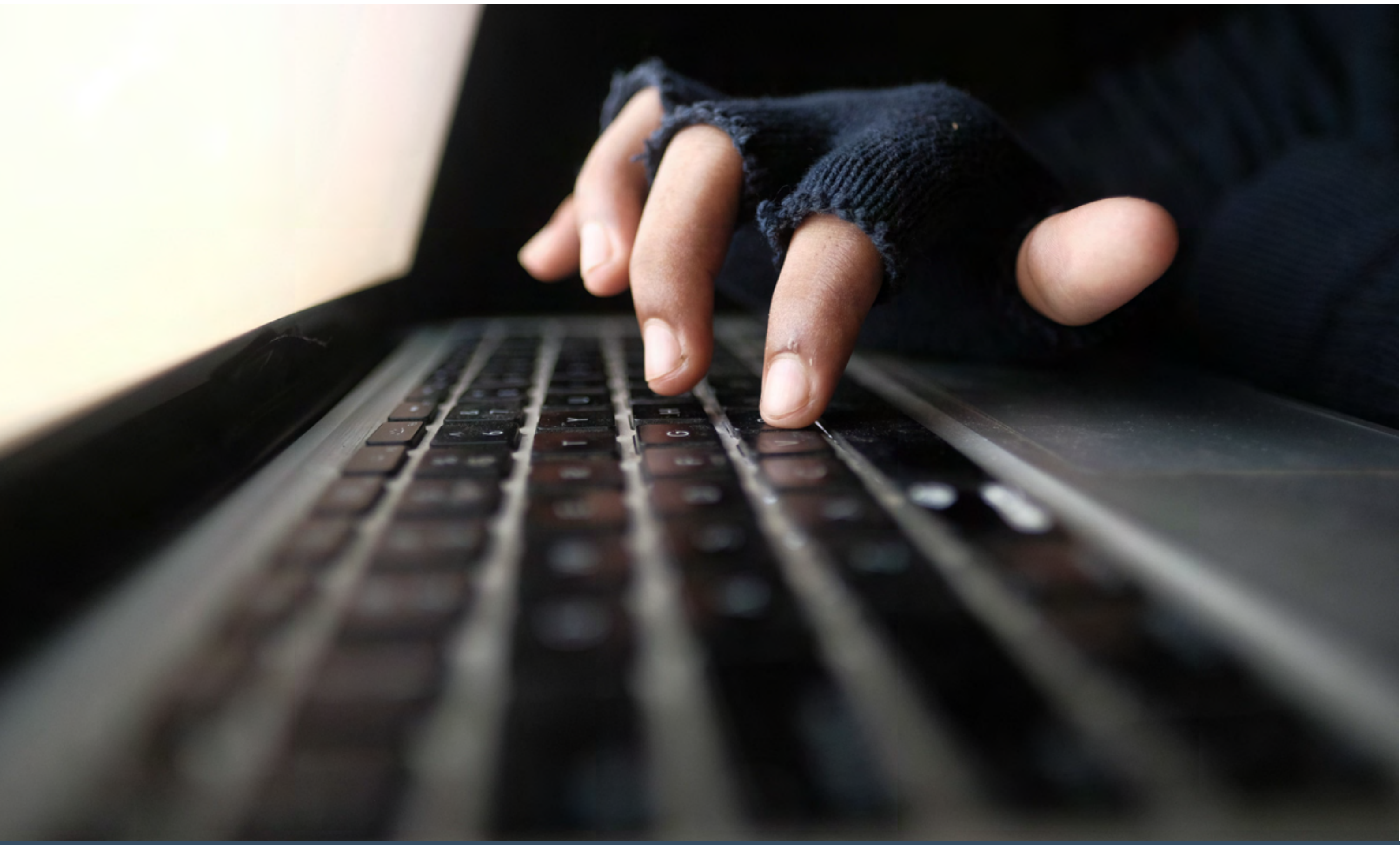
VULNERABILITY AND PENETRATION TESTING

- Conducts Vulnerability Assessment and penetration testing to Government Agencies;
- Provides technical details and analysis of discovered vulnerabilities and criticality to systems owner;
- Examines and evaluates web and network assets to identify security deficiencies

CYBER THREAT MONITORING

- Collects and analyzes data from publicly available sources and feeds regarding cyber threats;
- Collaborates with international and local communities and organizations on existing and new threats in cyberspace;
- Develops an effective implementation approach to monitoring and information sharing of cyber security incidents.

INCIDENT RESPONSE SECTION



INCIDENT RESPONSE

At the end of December 2022, the National Computer Emergency Response Team (CERT-PH) Incident Response (IR) section was able to handle a total of 1,129 cybersecurity-related incidents. This includes incidents caused by various attack vectors.

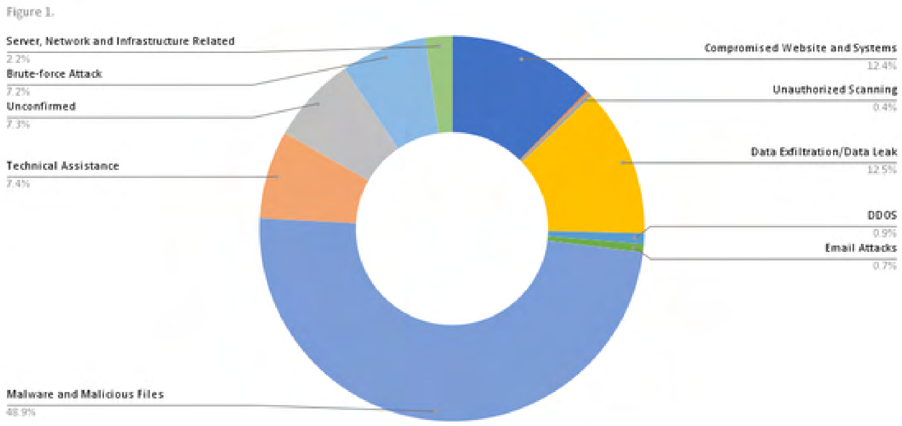
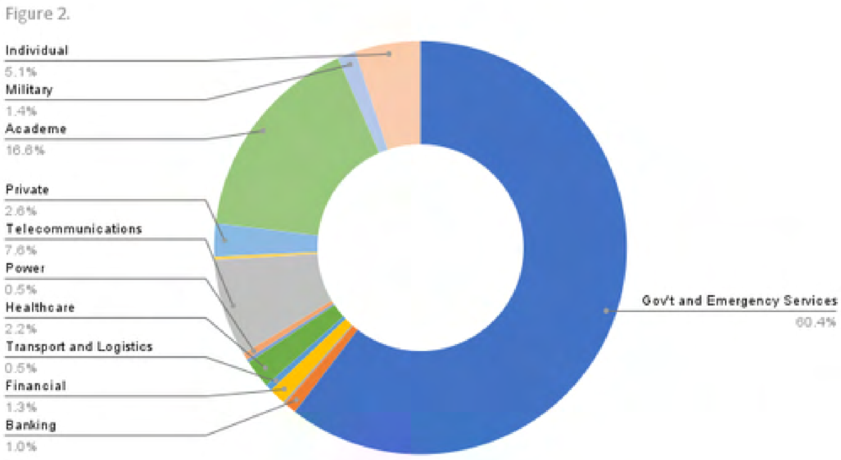


Figure 1. Incidents per Attack Category
This data represents the percentage of all recorded attack vectors that were monitored by CERT-PH during the year 2022. In this year, cases involving malware and malicious files were the most common types of incidents handled.

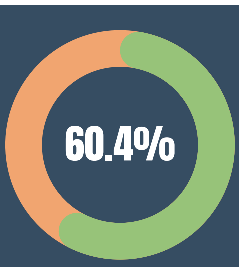
ATTACK VECTORS 2022
Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server. This year, CERT-PH was able to record a total of 549 incidents of malware and malicious files. This covers around 48.9% of the total incidents handled by the team this year. Attacks under this category includes backdoors, bot and botnets, malicious script, malicious infection, malicious IP and ransomware attacks.

Figure 2. Incidents per Sector
This graph displays the sectoral distribution of all attacked monitored and handled by the CERT-PH. As shown in the figure, agencies under the Government and Emergency Services sector has been the most popular target of cyberattacks.



1092

TICKETS CLOSED FOR 2022



GOVERNMENT-TARGETTED ATTACKS

997

INCIDENTS CLASSIFIED WITH MODERATE IMPACT

INCIDENT RESPONSE

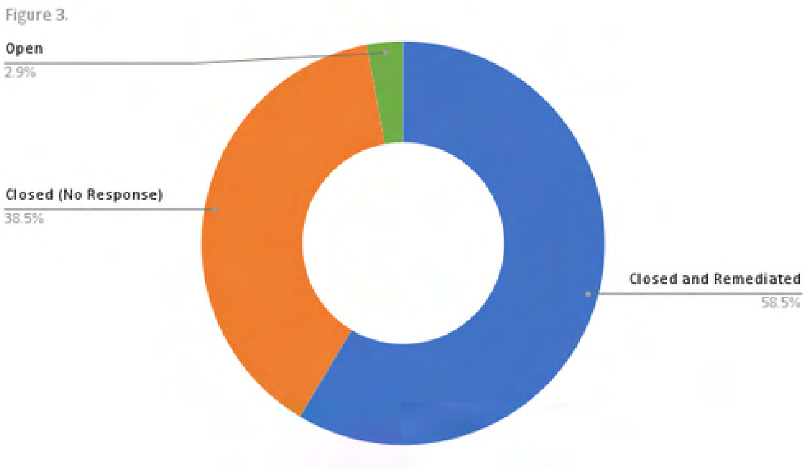


Figure 3. Incident Status as of December 31, 2022

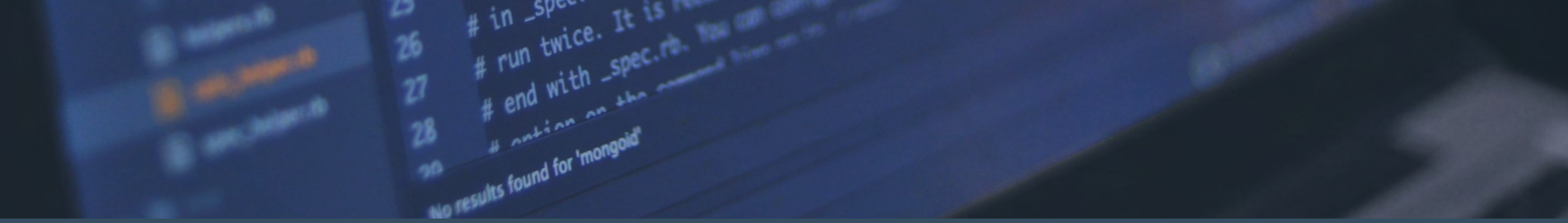
This figure covers the percentage of all the reported attack vectors that the CERT-PH received for the year 2022.

It can be noted that majority of the ticketed incidents were closed which means the case were already solved or dismissed. However, it can also be noticed that a significant percentage was closed due reason that no response has been received from the affected agency or organization.

All impacted clients received remedial procedures from CERT-PH, which also made recommendations on how to take the right measures to preserve their organization' enhanced security posture.

Meanwhile, the team is still getting in touch with the organizations that have been impacted by recent and continuing incidents.

As part of its post-incident activity, CERT-PH is currently updating its methodologies and techniques for guiding all stakeholders on how to properly defend and protect their IT infrastructure and environment against the rapidly evolving cybersecurity vectors. This is done in light of the incidents that were reported in 2022.



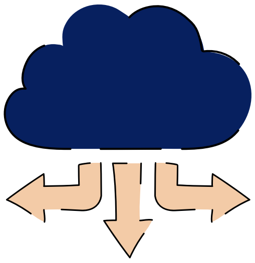
2022 MOST COMMON ATTACK VECTORS

BASED ON CERT-PH RECORDED INCIDENTS

1

PHISHING

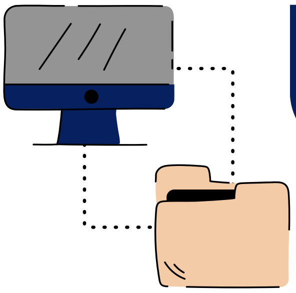
Phishing, a type of social engineering attack, remains one of the key methods used by attackers to compromise their targets, both individuals and organizations. It works as it is done on a large scale where threat actors send massive waves of emails purporting to be legitimate companies or personalities to promote fake pages or infect users with malicious attachments. The end goal of a phishing attack is to steal credentials, particularly confidential government, and login information, or worse to compromise an entire organization.



2

OUTDATED AND MISCONFIGURED SERVERS AND WEBSITE APPLICATIONS

It is very important to not dismiss the security updates when being notified to update. Servers and web applications that are not up-to-date or publicly accessible leaves an open door to vulnerabilities which can be exploited by adversaries.



3

ATTRITION

This attack vector focuses on the partial or total disruption of some component within the network. In this category, we find brute-force attacks to gain unauthorized access, forcing credentials, CAPTCHAs, or others. These attacks can also target the integrity of the network with denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks.

TOP THREAT ACTORS IN THE PHILIPPINES IN 2022

BASED ON CERT-PH RECORDED INCIDENTS

LOCKBIT

LockBit uses a ransomware-as-a-service (RaaS) model and consistently conceived new ways to stay ahead of its competitors. Its double extortion methods also add more pressure on victims, raising the stakes of their campaigns. One of its notable tactics was the creation and use of the malware StealBit, which automates data exfiltration. This tool was seen with the release of LockBit 2.0, which has been touted by its creators for having the fastest and most efficient encryption among its competition.

BLACKCAT

BlackCat was first observed in mid-November 2021 by researchers from the MalwareHunterTeam, BlackCat (aka AlphaVM, AlphaV, or ALPHV) swiftly gained notoriety for being the first major professional ransomware family to be written in Rust, a cross-platform language that enables malicious actors to customize malware with ease for different operating systems like Windows and Linux, thus affording a wide range of enterprise environments.

TAG-22

An APT (Advanced Persistent Threat) group named TAG-22 (Threat Activity Group 22) is a Chinese State-Sponsored organization known to be targeting the Philippines this year specifically the Department of Information and Communications Technology. CERT-PH investigated the DICT's network by conducting deep scanning from a compromised endpoint. The use of tools such as Network Forensic Module and Endpoint Forensic Module for Threat Protection System (TPS) concluded that some devices appear to be communicating to the APT's list vector which has been verified listed as a malicious indicator. TAG-22 uses compromised GlassFish servers and Cobalt Strike in initial access operations before switching to the bespoke Winnti, ShadowPad, and Spyder backdoors for long-term access using dedicated actor-provisioned command and control infrastructure.

CRITICAL INCIDENTS HANDLED IN 2022

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

Telecommunications Sector

TICKET #4173

DATA BREACH

Government and Emergency Sector

TICKET #4072

RANSOMWARE

Health Sector

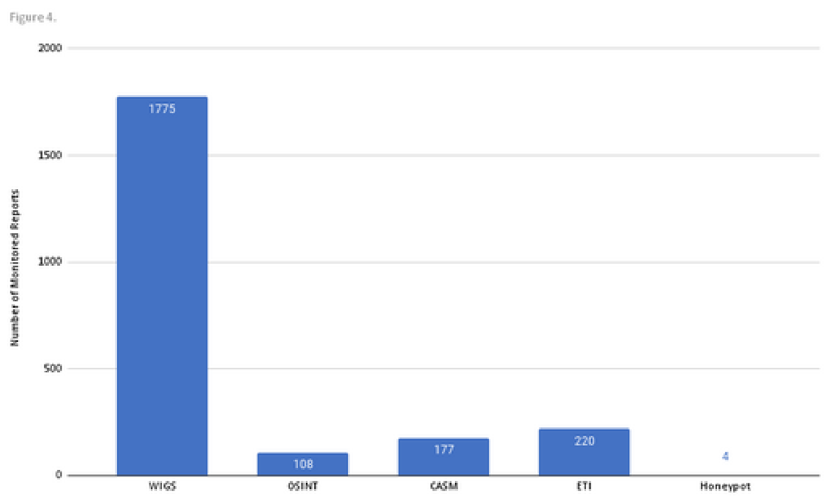
TICKET #3302

CYBER THREAT MONITORING

CYBER THREAT MONITORING

Figure 4. Monitored Threats

From January to December 2022, a total of 2,284 Monitored Threats were created. CERT-PH through the Web Information Gathering System (WIGS) has monitored 1,775 threats, while the External Threat Intelligence System (ETI) has 220 monitored threats. Those monitored through Open Sources account for 108 monitored threats.



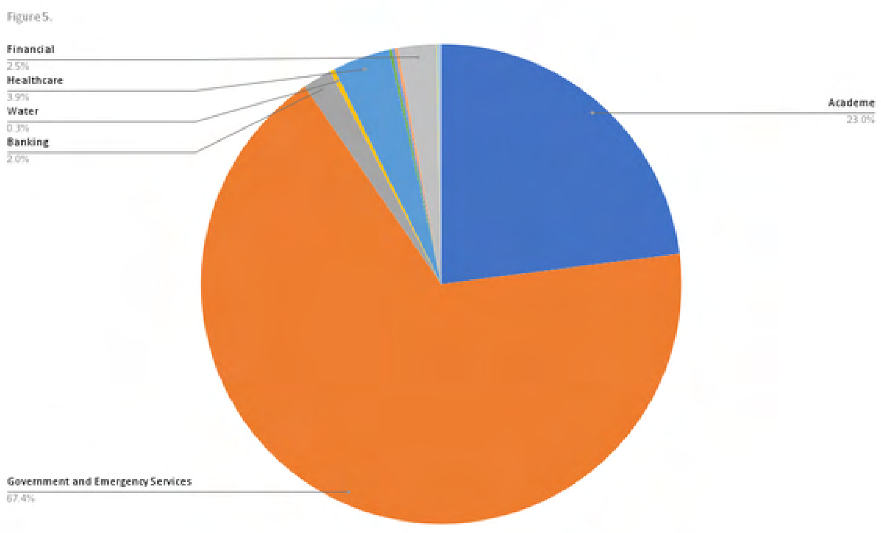
Recently the CERT-PH monitoring team has initiated the operation of its Honeypot monitoring which shows how attackers work and examines different types of threats the reports accounted for was 4.

Lastly monitored threats within DICT and attached agencies monitored by the Cyber Attack Surface Management have 177 reports.

Figure 05. Monitored Threats per Sector

Based on CERT-PH Monitoring Systems the Government and Emergency Services which includes NGAs, LGUs GOCCs, and instrumentalities have a large number of monitored threats which accounted for 67.4%. Various monitored threats reported such as vulnerabilities, malware, alleged data leaks, and website defacement were either reported or escalated to the Incident Response Section.

Cyber threat feeds and advisories are issued on a regular basis. Reports and information about the latest cyber threat news, topics, and articles from the web that may impact the Philippine government and cyberspace are gathered and analyzed to provide timely, actionable advice to our stakeholders so they can protect themselves online.



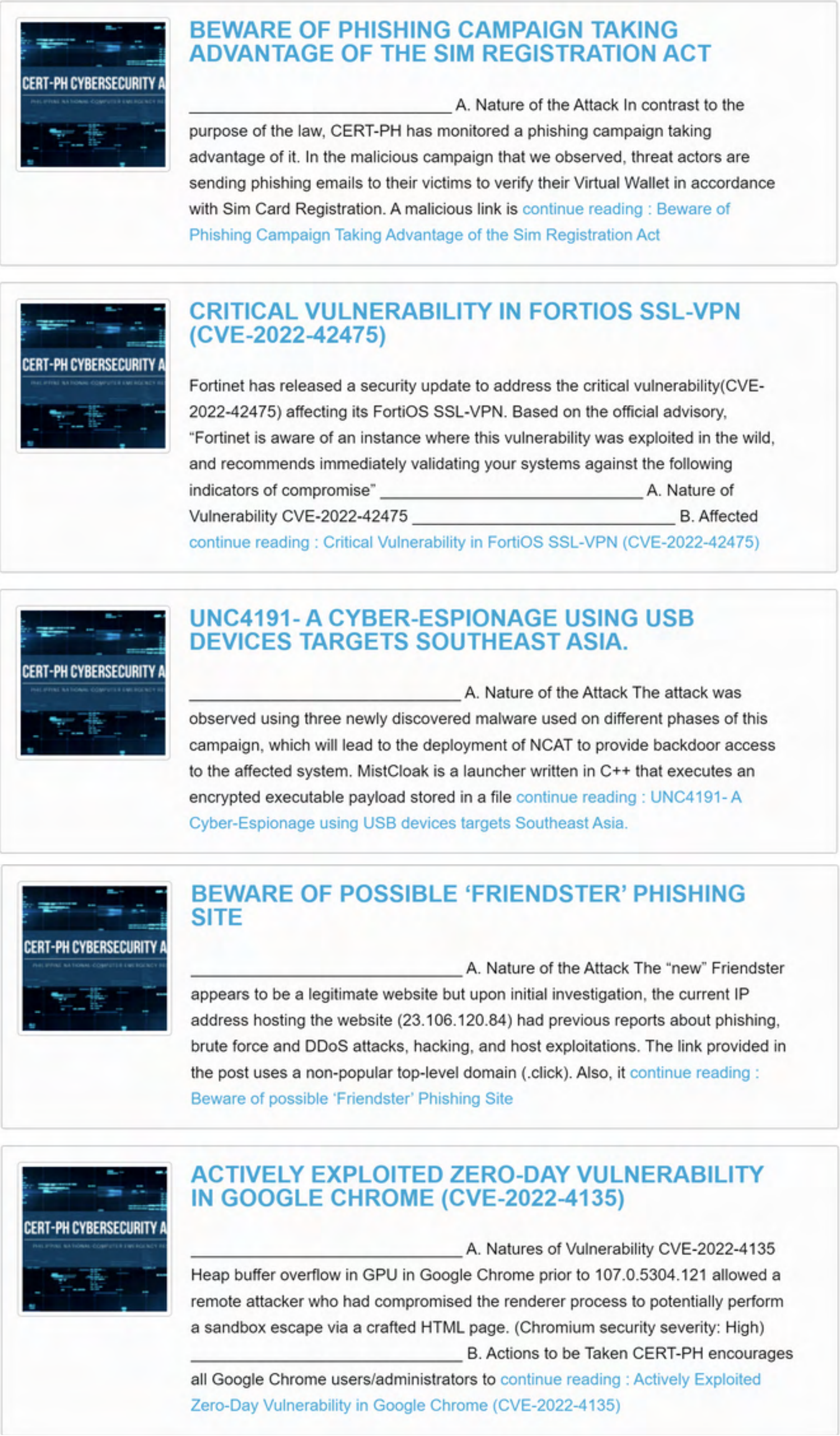
230

CYBER THREAT FEEDS ISSUED

37

SECURITY ADVISORIES FOR PUBLIC

ISSUED CERT-PH SECURITY ADVISORIES IN 2022



BEWARE OF PHISHING CAMPAIGN TAKING ADVANTAGE OF THE SIM REGISTRATION ACT

______________________________ A. Nature of the Attack In contrast to the purpose of the law, CERT-PH has monitored a phishing campaign taking advantage of it. In the malicious campaign that we observed, threat actors are sending phishing emails to their victims to verify their Virtual Wallet in accordance with Sim Card Registration. A malicious link is continue reading : Beware of Phishing Campaign Taking Advantage of the Sim Registration Act

CRITICAL VULNERABILITY IN FORTIOS SSL-VPN (CVE-2022-42475)

Fortinet has released a security update to address the critical vulnerability(CVE-2022-42475) affecting its FortiOS SSL-VPN. Based on the official advisory, “Fortinet is aware of an instance where this vulnerability was exploited in the wild, and recommends immediately validating your systems against the following indicators of compromise” ______________________________ A. Nature of Vulnerability CVE-2022-42475 ______________________________ B. Affected continue reading : Critical Vulnerability in FortiOS SSL-VPN (CVE-2022-42475)

UNC4191- A CYBER-ESPIONAGE USING USB DEVICES TARGETS SOUTHEAST ASIA.

______________________________ A. Nature of the Attack The attack was observed using three newly discovered malware used on different phases of this campaign, which will lead to the deployment of NCAT to provide backdoor access to the affected system. MistCloak is a launcher written in C++ that executes an encrypted executable payload stored in a file continue reading : UNC4191- A Cyber-Espionage using USB devices targets Southeast Asia.

BEWARE OF POSSIBLE ‘FRIENDSTER’ PHISHING SITE

______________________________ A. Nature of the Attack The “new” Friendster appears to be a legitimate website but upon initial investigation, the current IP address hosting the website (23.106.120.84) had previous reports about phishing, brute force and DDoS attacks, hacking, and host exploitations. The link provided in the post uses a non-popular top-level domain (.click). Also, it continue reading : Beware of possible ‘Friendster’ Phishing Site

ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY IN GOOGLE CHROME (CVE-2022-4135)

______________________________ A. Natures of Vulnerability CVE-2022-4135 Heap buffer overflow in GPU in Google Chrome prior to 107.0.5304.121 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High) ______________________________ B. Actions to be Taken CERT-PH encourages all Google Chrome users/administrators to continue reading : Actively Exploited Zero-Day Vulnerability in Google Chrome (CVE-2022-4135)

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

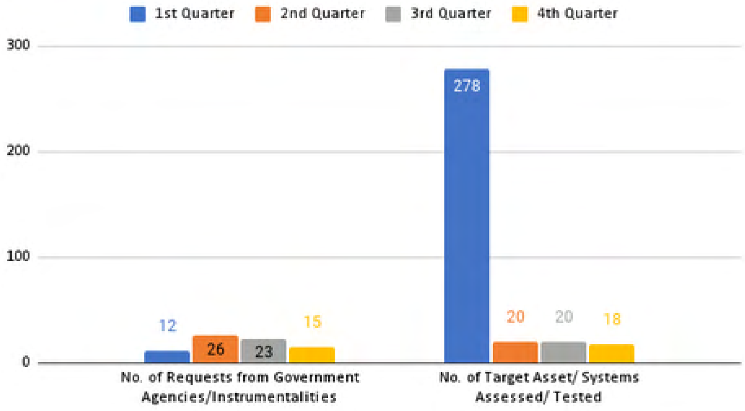
VULNERABILITY ASSESSMENT AND PENETRATION TESTING

The table below shows the number of requests for assessments or tests from government agencies or instrumentalities during each quarter of the year, as well as the total number of target assets or systems that were assessed or tested. This figure includes the total number of requests and assessments/tests across all four quarters.

	1ST QTR	2ND QTR	3RD QTR	4TH QTR	TOTAL
No. of Requests from GovernmentAgencies/Instrumentalities	12	26	23	15	76
No. of Target Asset/ SystemsAssessed/ Tested	278	20	20	18	336

For the year 2022 (January-December), the CERT-PH has received and accommodated a total number of 76 requests from different Government Agencies and Instrumentalities.

Figure 6.



Of these requests, vulnerability assessment and penetration testing services were conducted to a total of 336 web applications, network and mobile apps to discover any existing attack vectors that could be used by adversaries for potentially compromising the overall security, privacy, and operations of the Government and other Cybersecurity Bureau stakeholders. This also includes proactive engagements with various stakeholders.