ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA

Scuola di Ingegneria e Architettura
Corso di Laurea Magistrale in Ingegneria Informatica

Report del corso di Cybersecurity

L'IMPORTANZA DELLA CYBERSECURITY NEI CONFLITTI INTERNAZIONALI:
GUERRA INFORMATICA RUSSO-UCRAINA

Autore
Antonio Sarchione
0001093353

ANNO ACCADEMICO 2024-2025

1. Introduzione

La componente informatica nello scontro tra Russia e Ucraina ha acquisito nel tempo un ruolo sempre più centrale.

La dissoluzione dell'Unione Sovietica fu un evento che segnò profondamente la Russia e tutti i paesi che ne furono membri, fra cui l'Ucraina. Infatti, queste due nazioni si presentarono agli albori del nuovo millennio come due nazioni decisamente obsolete sotto vari aspetti e profondamente in crisi. Nonostante ciò, entrambe seppero sfruttare le potenzialità che offriva l'evoluzione della rete; in particolar modo, dal 2014 in poi si ebbe una crescita esponenziale del numero degli utenti che iniziarono ad utilizzare internet in modo consapevole[1].

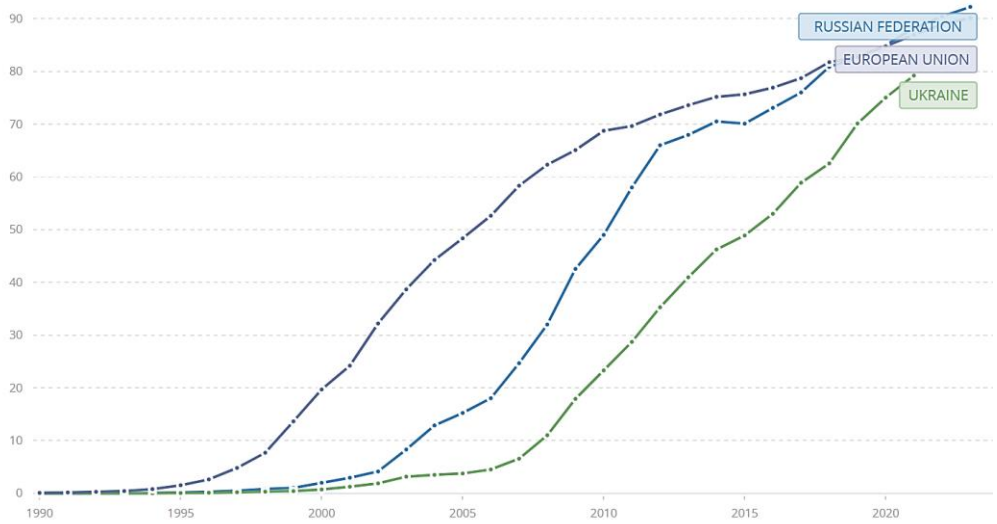


Figura 1: confronto in percentuale della popolazione che utilizza internet tra Russia, Ucraina e UE

Tra le due nazioni fu sicuramente la Russia quella che ebbe la piena consapevolezza della potenza di internet, tanto che la Russia fu uno dei primi paesi a sfruttare il le tecnologie più avanzate per la realizzazione di attacchi informatici e per la manipolazione dell'opinione pubblica tramite propaganda e disinformazione.

I primi utilizzi di armi informatiche risalgono al 2013-2014, durante il periodo della Rivoluzione della Dignità, ovvero un movimento di protesta democratico che portò alla rimozione dall'incarico dell'allora presidente ucraino Viktor Yanukovych[1], la quale venne descritta dalla propaganda russa come un colpo di stato e che venne utilizzato come pretesto per occupare e annettere la penisola di Crimea, alimentando proteste separatiste filo-russe e innescando la conseguente guerra del Donbass[2][3].

[1] Il presidente ucraino decise di non firmare un accordo di associazione politica e di libero scambio con l'Unione Europea, ma, piegato dalle forti pressioni del governo russo, scelse di stringere un legame con l'Unione doganale eurasiatica, composta da Russia, Bielorussia e Kazakistan

L'ingresso illegale delle truppe russe in Crimea e degli scontri nel Donbass hanno dimostrato che gli esperti militari russi ritenessero già nel 2014 che la guerra informatica potesse rappresentare la spina dorsale della guerra del futuro. Infatti, durante l'avanzata, le connessioni tra la penisola e l'Ucraina furono interrotti, tramite avanzati sistemi di jamming e di soppressione elettronica, i principali siti del governo ucraino e i siti notiziari furono presi di mira da attacchi DDoS e i cellulari di molti parlamentari ucraini vennero hackerati.
Fu qui che gli esperti ucraini dichiararono l'inizio di una guerra informatica con la Russia[4].

Da quel momento in poi furono numerosi gli attacchi informatici russi nei confronti dell'Ucraina. Infatti, l'idea di sfruttare le tecnologie digitali per fini meno nobili e quindi di essere utilizzate come un'arma prevalse quella di impiegare armi militari e tattiche di battaglia, rendendo così il conflitto una guerra non convenzionale.

Tuttavia, con l'invasione dell'Ucraina nel febbraio 2022, questo schema di una guerra non convenzionale venne meno, andando incontro all'applicazione della "Dottrina Gerasimov"[2], la quale sottolinea l'importanza del controllo dello spazio informativo e secondo la quale le armi militari debbano essere utilizzate solo in casi estremi[5].
Nonostante la predisposizione russa a voler sopraffare l'avversario grazie agli armamenti bellici terrestri, prima dell'invasione e durante la stessa, l'utilizzo di armi informatiche ricoprì un ruolo da protagonista, sia per quanto riguarda l'offensiva russa, ma soprattutto, per quanto riguarda la difesa ucraina.

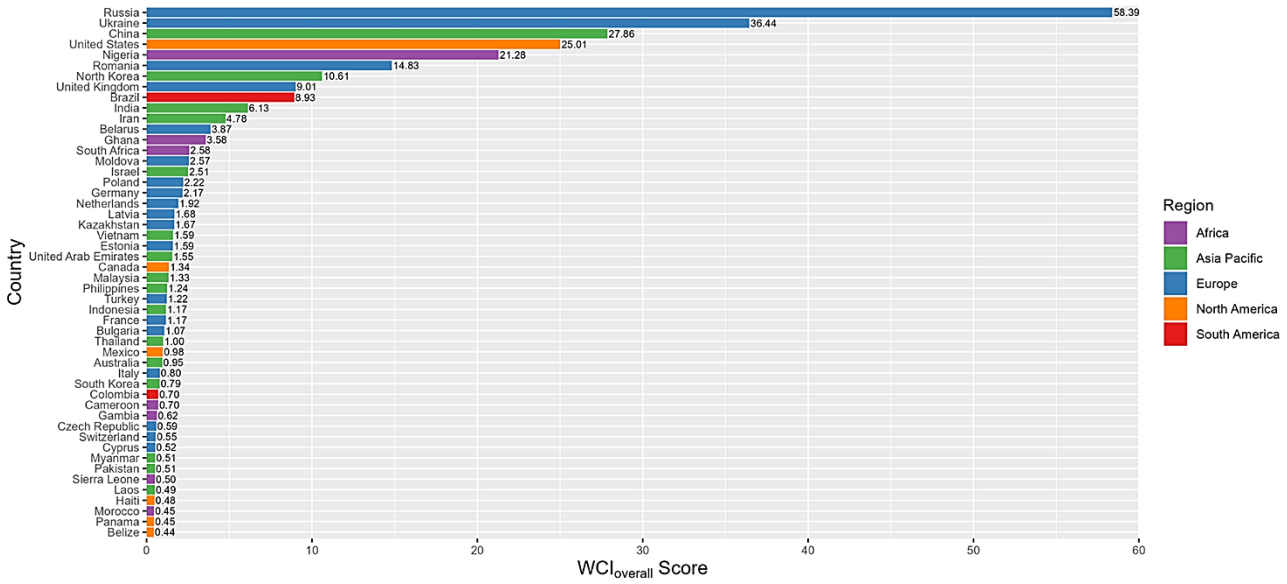


Figura 2: World Cybercrime Index[3]

[2] Valerij Vasil'evič Gerasimov è il capo di stato maggiore generale delle Forze armate russe
[3] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312

2. CyberWar

In questo nuovo tipo di guerra, definita "ibrida", le forze in campo non sono più rappresentate solo da soldati ordinari e forze speciali sul terreno, ma soprattutto da figure come hacker, spie e attori APT[4] che operano attacchi in ambito informatico all'interno del cyberspazio, con il fine di ottenere informazioni preziose o danneggiare strutture e infrastrutture fisiche. Dunque, la guerra informatica non si limita al solo ambito informatico, ma ha come obiettivo quello di destabilizzare tutti i servizi di un paese, che al giorno d'oggi risultano essere praticamente tutti informatizzati.

Quindi, si può affermare che la stessa evoluzione umana ha portato alla creazione di questa nuova tipologia di guerra dove le armi tradizionali sono affiancate da armi innovative, le quali hanno portato alla rielaborazione del concetto di conflitto. Gli scontri non avvengono più solo sul suolo fisico, un campo ritenuto troppo ridotto per le armi odierne, ma avvengono anche sul campo informatico, spostando la quasi totalità dell'attenzione sugli strumenti tecnologici messi a disposizione di stati o anche singoli individui per attaccare digitalmente all'interno del cyberspazio.

Il cyberspazio indica l'ambiente globale, interconnesso e digitale in cui le informazioni circolano e sono accessibili tramite infrastrutture tecnologiche e con il tempo è diventato l'elemento chiave nel contesto della guerra moderna, soprattutto in quella cibernetica. Al giorno d'oggi, la sua importanza è tale da essere definito come il *quinto dominio*[6], dopo terra, acqua, aria e spazio. A differenza degli altri domini, il cyberspazio è stato costruito dall'uomo e la sua caratteristica principale risiede nel fatto che è incorporato in tutti gli altri e le operazioni effettuate al suo interno generano conseguenze su tutti gli altri.

Per questo motivo, il cyberspazio non va inteso come un mero spazio di comunicazione e scambio di informazioni, piuttosto va inteso come un dominio operativo, il cui ruolo focale nei conflitti informatici è dato da alcune delle sue caratteristiche distintive[7]:

- **assenza di confini**: non esistono confini dipendenti dalla morfologia del terreno o da eserciti schierati che possano impedire attacchi al di fuori dei confini nazionali
- **anonimato**: l'identificazione precisa di un attore responsabile di un attacco risulta molto più difficile e questo elevato livello di anonimato crea una zona grigia in cui attacchi informatici possono essere lanciati senza una dichiarazione formale di guerra[8]
- **interconnessione**: la quasi totalità della infrastrutture critiche di ciascuna nazione è strettamente legata al cyberspazio e questo le rende vulnerabili ad attacchi e interferenze esterne
- **asimmetria**: all'interno del cyberspazio anche attori con risorse limitate dal punto di vista economico possono rendersi protagonisti di attacchi significativi a grandi potenze

A tal proposito, un'affermazione lecita è quella di poter definire la guerra cibernetica come una realtà del XXI secolo che, combinando la tecnologia avanzata, le strategie politiche e le dinamiche globali, ha influito e continua ad influire sull'operato di stati e organizzazioni sovranazionali, imponendo loro di sviluppare sia capacità offensive che difensive per gestire al meglio un panorama in continua evoluzione.

[4] Advanced Persistent Threat

In quest'ottica, nel corso del conflitto iniziato nel febbraio del 2022, la Russia sfruttò a pieno le potenzialità offerte da questa nuova tipologia di guerra, sia per indebolire la manovra difensiva ucraina, tramite attacchi al cyberspazio ucraino e quindi a tutte le infrastrutture ad esso collegato e siti web, principalmente governativi, bancari e notiziari[9], e sia per effettuare operazioni di propaganda interna col fine di manipolare l'opinione pubblica e di reclutare nuovi soldati filoputiniani.

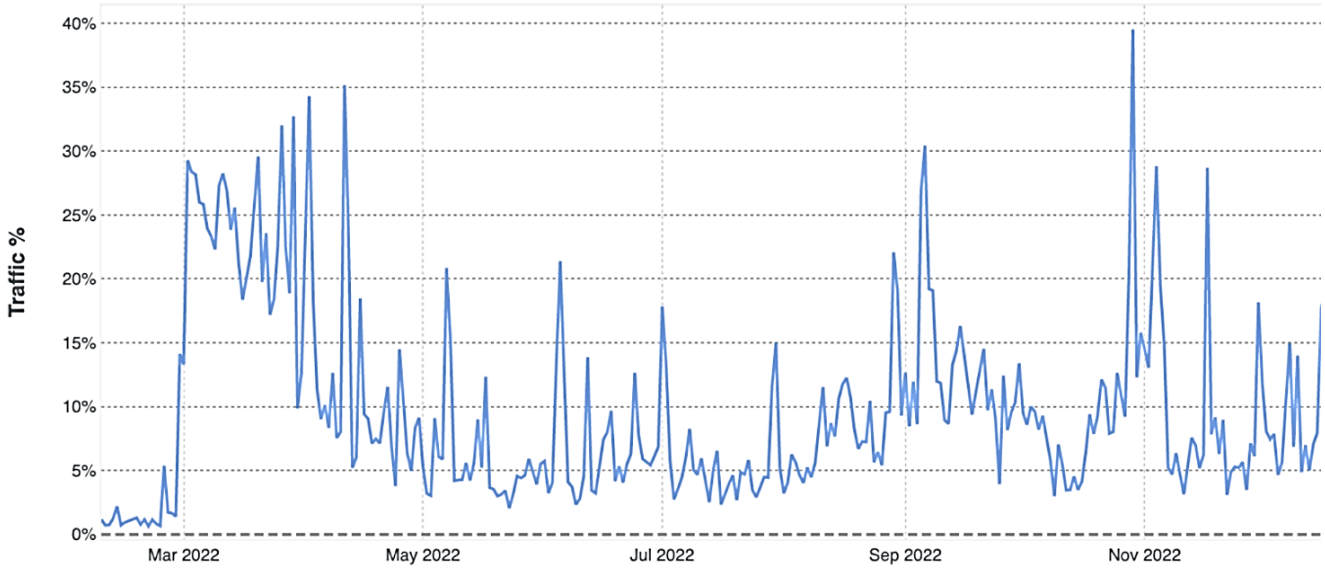


Figura 3: percentuale giornaliera di traffico a livello applicativo verso l'Ucraina

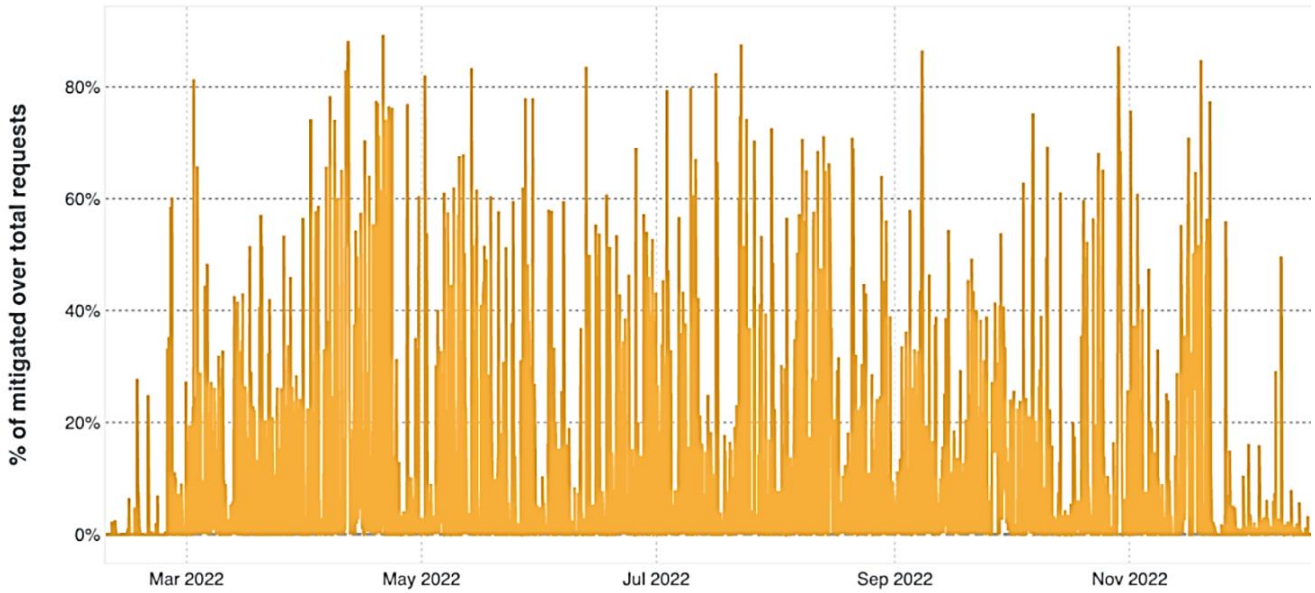


Figura 4: percentuale giornaliera del traffico di attacchi DDoS verso i siti sul dominio di primo livello ".ua"

3. Offensiva Russa

L'invasione dell'Ucraina da parte delle armate russe, avvenuta nel febbraio 2022, ha segnato un momento cruciale nella moderna guerra ibrida ed esemplifica chiaramente l'intersezione di strategie militari informatiche e convenzionali[10].

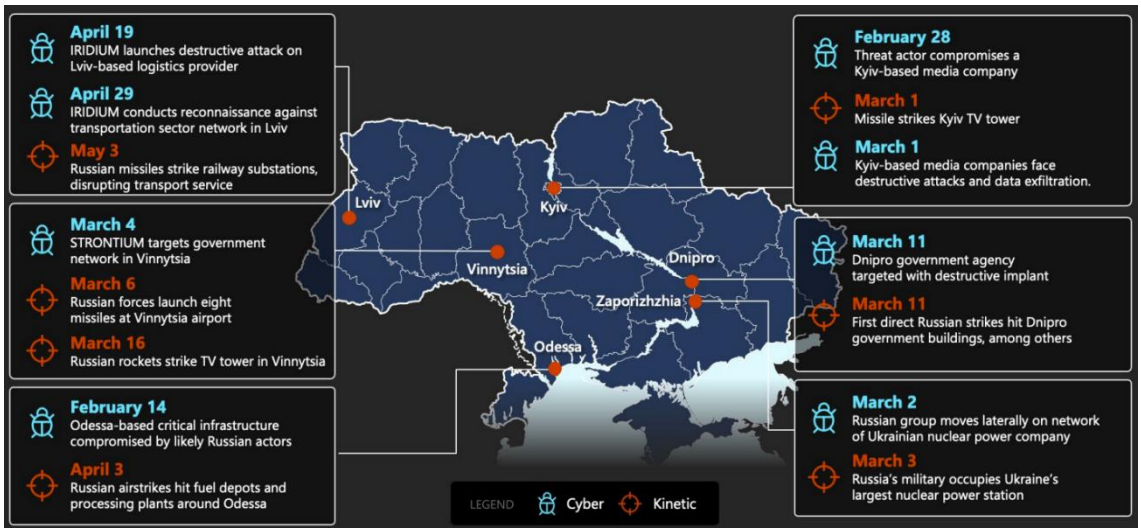


Figura 5: Operazioni militari e informatiche russe coordinate in Ucraina

Essa ebbe inizio il 24 febbraio 2022, ma le operazioni informatiche russe per garantire loro dei vantaggi ebbero inizio già nel mese precedente. Gli attacchi furono molteplici durante l'intero scontro e restano ancora oggi materia di interesse per le due nazioni coinvolte, ma anche per tutti i paesi del mondo.

Di seguito, verranno esaminati i principali attacchi e le principali operazioni informatiche russe che hanno caratterizzato lo scontro e rappresentato degli eventi chiave nel conflitto tra Russia e Ucraina.

DDoS Attacks

Nella settimana precedente l'invasione, venne registrata un'impennata di attacchi DDoS nel cyberspazio ucraino fino al raggiungimento dell'attacco combinato avvenuto nel pomeriggio del 23 febbraio 2024. Tali attacchi ebbero come obiettivo la sopraffazione dei siti web del governo e dell'esercito ucraino, l'inaccessibilità dei principali servizi delle istituzioni finanziarie, come PrivatBank e Oschadbank, e dei maggiori organi di informazione[13]. Dunque, il fine ultimo fu l'inibizione delle capacità del governo ucraino nel coordinare efficacemente delle risposte, generando una forte destabilizzazione tramite attacchi ripetuti alla quotidianità dei servizi civili e governativi.

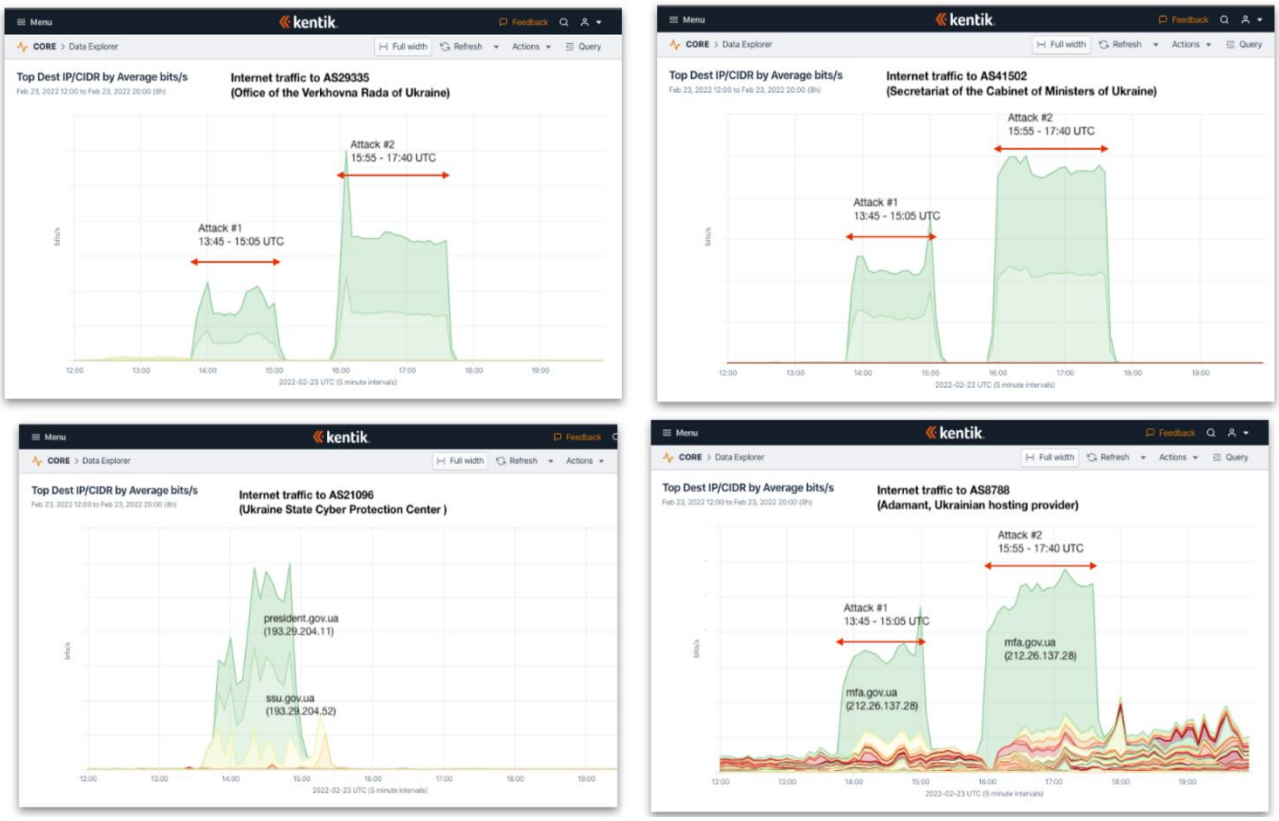


Figura 6: traffico internet sui siti di interesse ucraini durante gli attacchi DDoS

Per la realizzazione di queste operazioni venne sfruttata una botnet, ovvero una rete di dispositivi compromessi, controllati da remoto e utilizzati per generare enormi volumi di traffico per rendere inaccessibili i server di destinazione. Il modello di botnet realizzato fu un modello centralizzato, la cui attività fu orchestrata tramite dei server C2[5] situati in posizioni geograficamente diverse, oscurandone l'attribuzione.

Tuttavia, dopo approfondite ricerche, i servizi di sicurezza nazionale di Stati Uniti e Regno Unito attribuirono questi attacchi all'Unità GRU[6] e al Killnet, un collettivo di hacker filo-russi che già prima di allora si assunse la responsabilità di molteplici campagne DDoS.

HermeticWiper

HermeticWiper, il cui nome deriva dall'appropriazione indebita di un certificato digitale di una società cipriota chiamata Hermetica Digital Ltd, è un malware wiper che colpì diverse infrastrutture governative e critiche in tutta l'Ucraina e che venne identificato dal MSTIC[7] il giorno precedente l'invasione.

[5] Command and Control
[6] Glavnoje Razvedyvatel'noje Upravlenije, ovvero il Direttorato Principale per l'Intelligence
[7] Microsoft Threat Intelligence Center, una soluzione di intelligence che protegge le organizzazioni dalle minacce informatiche

Questo malware si presentò come un eseguibile contenente quattro driver legittimi del software EaseUS[8] che implementano operazioni su disco di basso livello. Una volta lanciato, in base al sistema operativo, uno di questi driver veniva caricato creando un servizio che procedeva prima a disabilitare il VSS[9] del computer e poi a sovrascrivere il proprio file con byte casuali, impedendo l'analisi del wiper[11].

Successivamente, il malware sovrascriveva con byte casuali, avvalendosi della funzione API di Windows CryptoGenRandom, le seguenti aree:

- Master Boot Record (MBR)
- Master File Table (MFT)
- $LogFile e $Bitmap su tutte le unità
- Il file NTUSER.dat, contenente tutte le chiavi di registro
- Tutti gli Event Logger del computer

Dopo aver fatto ciò, si occupava della cancellazione ricorsiva dei file e delle cartelle presenti nel disco fisso, tramite il codice di controllo FSCTL_MOVE_FILE, e quindi della conseguente frammentazione dello stesso[11][12], rendendo ancor più difficile l'estrazione dell'immagine grezza del disco per una successiva ricostruzione.

Questo malware colpì centinaia di macchine soprattutto grazie ad un worm sviluppato in C++, chiamato *HermeticWizard*, che, avvalendosi di due diffusori crittografati, uno responsabile della diffusione tramite WMI e l'altro della diffusione tramite SMB, si occupava del recupero degli indirizzi IP locali e per ogni indirizzo del tentativo di apertura di una connessione TCP sulle varie porte in ordine casuale e dell'esecuzione del wiper sulle macchine raggiungibili[11].

Viasat Hack

Un altro attacco informatico di particolare rilevanza per questo conflitto fu quello del 24 febbraio 2024 a Viasat, una società americana che fornisce servizi di comunicazione a banda larga, e in particolare alla sua rete satellitare KA-SAT. L'attacco venne messo in atto su più fasi[14]:

1. **Riconoscimento**: gli aggressori identificarono le vulnerabilità dell'infrastruttura KA-SAT tramite una scansione attiva dei sistemi accessibili al pubblico e tra queste fu fatidica una appliance VPN Fortinet non configurata correttamente rappresentò il punto di ingresso per per accedere al sistema
2. **Accesso**: gli aggressori sfruttarono un furto di credenziali avvenuto nella rete terrestre da parte di un utente malintenzionato per ottenere l'accesso remoto e una patch non implementata nel segmento di gestione dell'operatore Skylogic per passare attraverso la zona demilitarizzata

[8] EaseUS Partition Master, un gestore di partizioni del disco che consente agli utenti di gestire dischi rigidi su server Windows a 32 o 64 bit
[9] Volume Shadow Copy Service, servizio che coordina le azioni necessarie per creare uno snapshot dei dati di cui si desidera eseguire il backup

3. **Movimento laterale**: una volta all'interno, gli aggressori utilizzarono strumenti amministrativi legittimi per muoversi lateralmente attraverso la rete e per aumentare loro i privilegi necessari per ottenere il pieno controllo sulla rete operativa
4. **Targeting**: gli aggressori selezionarono specifiche celle geografiche di KA-SAT su cui impartire le operazioni di sovrascrittura dei dati critici dei modem, rendendo inaccessibile la rete internet per diverse migliaia di utenti in Ucraina e in Europa, evitando, comunque, di compromettere i servizi governativi e di mobilità per ridurre al minimo i danni collaterali ai servizi di alto valore
5. **Distribuzione**: sui modem delle aree selezionate fu installato un file .elf, chiamato AcidRain, il quale operò come un wiper, progettato per cancellare in modo irreversibile i dati chiave del modem, prendendo di mira un numero elevato di sistemi embedded

Grazie alla sua precisione e alla sua tempistica, questo attacco causò un'enorme perdita di comunicazioni e di informazioni all'inizio della guerra e agevolò l'avanzata russa sul territorio ucraino, sottolineando l'importanza e la crescente integrazioni degli attacchi digitali con le operazioni cinetiche.

Troll Farm

Durante il conflitto Russo-Ucraino, ricoprì un ruolo di rilevanza assoluta anche la figura della *Troll Farm*, ossia un gruppo istituzionalizzato di troll che, tramite la pubblicazione di messaggi sulle piattaforme digitali, cercò di manipolare l'opinione pubblica, mirando all'amplificazione di un sentimento filo-russo, sia dal punto di vista politico che militare, e alla destabilizzazione del sostegno pubblico nei confronti dell'Ucraina.

Questa rete a favore dei russi comprendeva svariati account sui principali social network, come Twitter, TikTok e Instagram, che riuscirono a raggiungere milioni di visualizzazioni e consensi, pubblicando dei post che promuovevano le dichiarazioni del governo russo e condividendo falsi video di fact-checking russi. Inoltre, gli account in questione lavorarono concretamente per aumentare l'engagement utilizzando retweet e hastag coordinati, creando un'illusione di supporto diffuso[15]. Questo fu evidente durante le prime fasi dell'invasione, poiché le reti di troll incrementarono notevolmente la loro presenza sui social promuovendo giustificazioni a favore della guerra e screditando le atrocità dell'operato russo.

La realizzazione di questa campagna di disinformazione fu attribuita all'IRA[10], nonostante alcune piattaforme digitali si rifiutarono di fornire maggiori dettagli sugli account colpevoli di questo attacco. Si presume che il motivo di questo rifiuto fu dovuto al fatto che le piattaforme non volessero attribuire queste attività malevole all'IRA perché i troll utilizzarono spesso VPN, falsificando le loro posizioni e complicando la loro reale attribuzione[15][16].

[10] Internet Research Agency, una società privata di proprietà della figura nota come "chef di Putin" che opera negli interessi del Cremlino

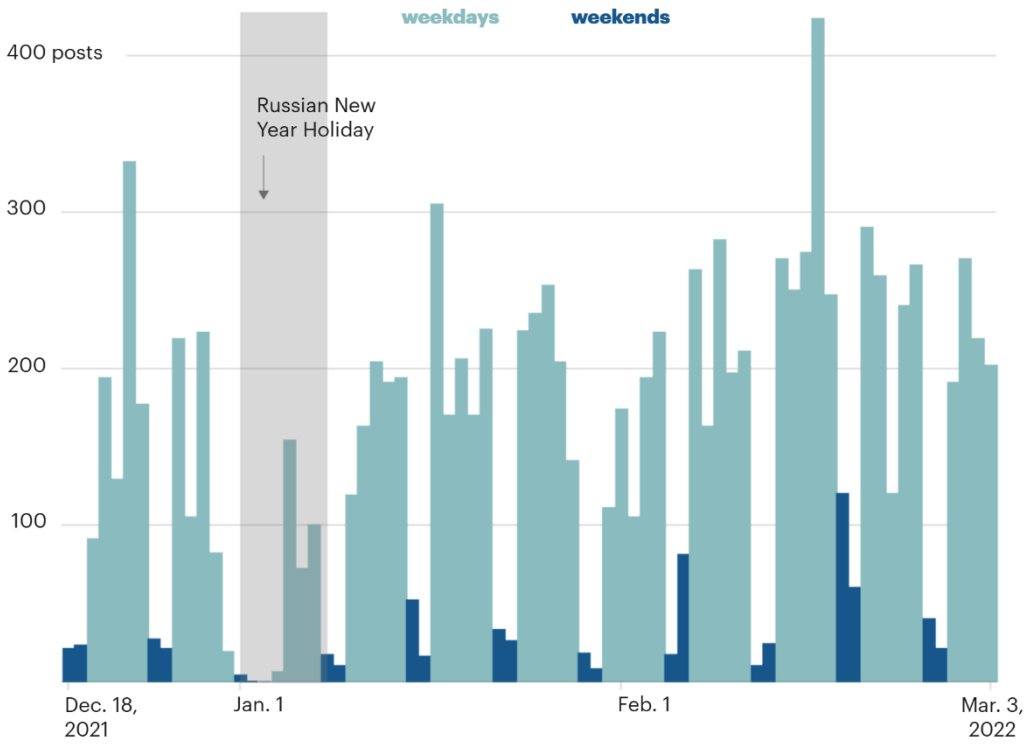


Figura 7: numero dei post giornalieri su Twitter di 28 account identificati come aventi un comportamento coordinato o simile a un bot

4. Resilienza Ucraina

Le dimensioni del cyber conflitto Russo-Ucraino hanno evidenziato l'evoluzione della difesa informatica come parte integrante della guerra moderna[17].
Prima dell'invasione russa, analisti militari e politici globali prevedevano che la potenza militare russa, caratterizzata da formidabili unità corazzate e da una tecnologia missilistica avanzata, avrebbe rapidamente sopraffatto le difese ucraine e che le loro operazioni informatiche avrebbero paralizzato le infrastrutture critiche e interrotto i sistemi di comando e di controllo; quindi, si prevedeva che la componente informatica avrebbe particolarmente avvantaggiato l'avanzata russa, piuttosto che la difesa ucraina. Contrariamente a queste previsioni, l'invasione ha avuto uno svolgimento ben diverso, dimostrando come le forze ucraine abbiano sfruttato al meglio le loro abilità informatiche a loro vantaggio, durante l'intero conflitto[17][18].

Nonostante le varie affermazioni del governo russo, è evidente come gli attacchi informatici russi fallirono in gran parte nel produrre risultati degni di nota. Tali fallimenti non furono dovuti solo alle solide competenze ucraine in materia di cyber difesa, furono principalmente il risultato dell'efficace resilienza informatica dell'Ucraina stessa. In merito a questa affermazione, di seguito, in contrapposizione con il capitolo precedente, verranno esposte le manovre difensive nello scontro cibernetico che hanno permesso all'Ucraina di sopperire ai vari attacchi informatici russi.

DDoS Attacks

La risposta dell'Ucraina agli attacchi DDoS russi rappresento un ottimo esempio di mitigazione rapida e reattiva delle minacce. L'SSCIP[11] ucraina implementò prontamente una soluzione WAF[12], ovvero un firewall per applicazioni web che monitora, filtra, reindirizza e blocca, se necessario, il traffico HTTP/S in ingresso, progettato per fornire rilevamenti basati sul comportamento di eventuali attacchi al livello applicativo (L7) e di rete (L3-L4). Tale soluzione, sfruttando i centri di scrubbing CDN[13] dislocati in tutto il mondo, quindi anche in prossimità dell'origine dell'attacco, fornì una capacità di mitigazione pari a 10 Tbps, capace di mantenere per lo più stabile le infrastrutture di comunicazione ucraine[19].

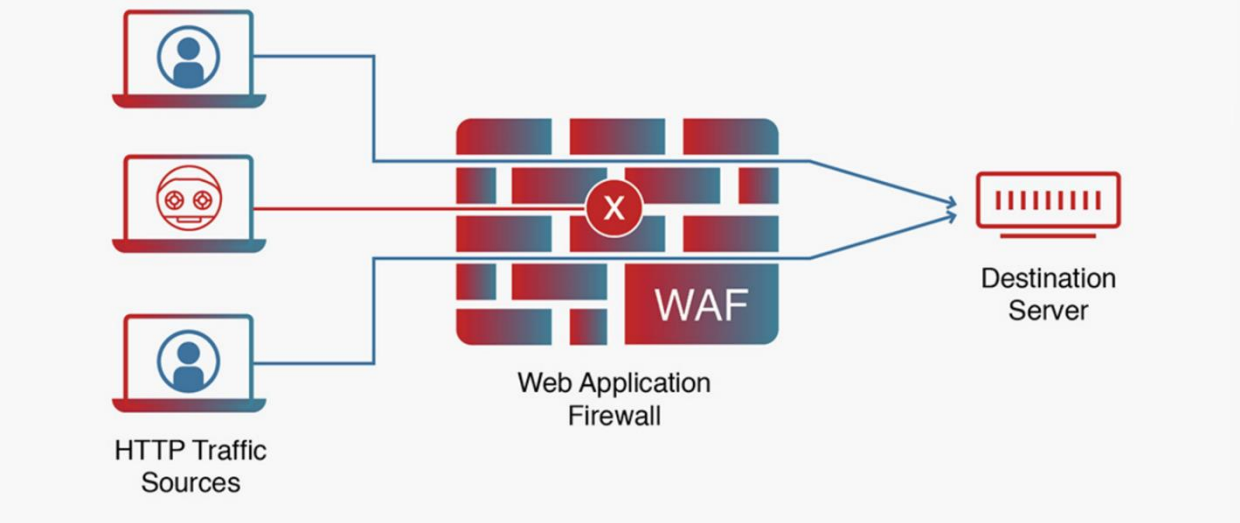


Figura 8: Architettura WAF di base

La soluzione adottata risultò particolarmente efficace contro gli attacchi DDoS soprattutto grazie alla scelta del CERT-UA[14] di sfruttare alcune piattaforme di monitoraggio e condivisione in tempo reale, come la MISP[15] della NATO oppure la rete CDN di Akamai[16], per condividere e ricevere informazioni sulle minacce emergenti. In questo modo, gli indirizzi IP delle fonti di traffico dannose venivano condivise poco dopo ogni tentativo di attacco, permettendo di aggiornare continuamente le regole del firewall e di instaurare un meccanismo di geo-blocking sempre attivo per impedire l'accesso da regioni fortemente associate ai traffici botnet coordinati, in particolare in Russia e nelle reti proxy.

La difesa dell'Ucraina contro gli attacchi DDoS russi è stata caratterizzata da agilità, collaborazione internazionale e soluzioni tecniche solide. Queste misure non solo hanno garantito la continuità

[11] State Service of Special Communications and Information Protection
[12] Web Application Firewall
[13] Content Delivery Network
[14] Computer Emergency Response Team of Ukraine, un'unità strutturale specializzata nella protezione informatica dei servizi statali
[15] Malware Information Sharing Platform, una piattaforma per la condivisione di informazioni sui malware all'interno di una comunità fidata
[16] Azienda statunitense che fornisce una piattaforma per la distribuzione di contenuti via Internet

operativa, ma hanno anche stabilito un punto di riferimento per le strategie anti-DDoS in tempo di guerra.

HermeticWiper

I malware wiper utilizzati durante questo conflitto mirarono alla distruzione dei dati critici e all'interruzione dei servizi essenziali. Tuttavia, la risposta dell'Ucraina a questa tipologia di attacchi dimostrò un approccio stratificato alla sicurezza informatica, capace di coinvolgere difese tecniche e meccanismi di risposta agli incidenti, grazie anche alla collaborazione con alleati internazionali e aziende tecnologiche private.

La controffensiva ucraina a questa tipologia di attacco si stratificò in più fasi[20]:

1. **Preparazione preventiva**: le agenzie ucraine per la sicurezza informatica collaborarono insieme a partner globali con il fine di prevenire la diffusione del malware e le misure proattive adottate consistettero nella diffusione degli IoC[17], contenenti anche hash di file, nell'aggiornamento dei sistemi operativi per mitigare lo sfruttamento delle vulnerabilità note utilizzate da HermeticWizard e nella distribuzione di sistemi avanzati di protezione degli endpoint per rilevare comportamenti anomali, come l'installazione di driver non autorizzati
2. **Rilevamento e contenimento**: per rilevare la presenza del malware HermeticWiper all'interno dei computer furono utilizzati degli strumenti EDR[18], per identificarne la firma univoca; invece, per isolare i sistemi infetti e per impedire il movimento laterale, sfruttato da HermeticWizard, venne bloccato il traffico SMB e disattivata la comunicazione WMI all'interno dei segmenti critici e furono analizzati i crash dump, disabilitati dal wiper, per identificarne la metodologia di distribuzione[21]
3. **Mitigazione**: nonostante HermeticWiper disabilitò le copie shadow, per limitare i danni, alle organizzazioni fu consigliato di utilizzare soluzioni di backup air-gapped, in cui i dati vengono storati su supporti offline, non accessibili da internet; inoltre, furono utilizzati strumenti specializzati in NTFS[19] recovery per recuperare i dati parzialmente danneggiati
4. **Recupero e resilienza**: le strategie di recupero attuate dopo l'incidente consistettero nel reimaging per i sistemi gravemente compromessi, per ripristinarne rapidamente le capacità operative, e nel implementazione di controlli di accesso più rigorosi, di una segmentazione di rete migliore e di autenticazioni MFA[20] nei sistemi critici

Per una buona difesa, quindi, furono fondamentali anche gli sforzi collaborativi internazionali dei privati, come ESET, che fornì un'analisi iniziale dei HermeticWiper e HermeticWizard, inclusa la reverse engineering del malware per rivelarne i meccanismi operativi, come MISC, che aiutò le istituzioni ucraine ad implementare difese anti-malware avanzate in tempo reale, come CrowdStrike

[17] Indicators of Compromise, indicatori che costituiscono la prova dell'attacco e permettono di scoprire gli strumenti utilizzati per sferrare l'attacco
[18] Endpoint Detection and Response
[19] New Technology File System, file system utilizzato da Microsoft, la cui struttura è basata su di una Master File Table
[20] Multi-Factor Authentication

e SentinelOne che condivisero gli approfondimenti sulle tattiche avversare e gli IoC sulle reti europee.

Viasat Hack

Il cyberattacco alla rete di comunicazione satellitare KA-SAT di VIASAT illustrò chiaramente la natura in evoluzione della guerra informatica, in cui gli attacchi alle infrastrutture critiche, come quelle delle comunicazioni, possono avere implicazioni strategiche significative. Simultaneamente, le misure difensive adottate dall'Ucraina evidenziarono il valore dell'analisi forense coordinata e l'importanza delle capacità di risposta in tempo reale per contrastare minacce informatiche così sofisticate.

La risposta difensiva dell'Ucraina a questo attacco fu un'operazione avvenuta in più fasi:

1. **Analisi**: nella fase iniziale la difesa ucraina consistette in una fase di analisi forense, in cui furono estratti i dump di memoria dai dispositivi compromessi per identificare il comportamento del malware AcidRain, per poterne simulare il comportamento in ambiente di laboratorio e per poter risalire alle firme dello stesso e alle sequenze di chiamate di sistema utilizzate, tramite reverse engineering[23]
2. **Segmentazione e contenimento**: in questa fase furono identificati i modem compromessi e messi in quarantena i segmenti interessati per limitare la propagazione degli aggiornamenti corrotti; poi, VIASAT aggiornò il firmware dei modem non ancora colpiti per renderli in grado di rifiutare i comandi OTA[21] non autorizzati
3. **Condivisione**: la complessità dell'attacco richiese anche un'intensa cooperazione internazionale, infatti i team del CERT-UA collaborarono con agenzie governative, come NSA[22] e GCHQ[23], e aziende private, come SentinelOne o Mandiant, per analizzare le tattiche, le tecniche e le procedure dell'attacco e tale condivisione di informazioni consentì un rapido sviluppo di patch difensive applicabili a sistemi simili in tutto il mondo[22][23]
4. **Monitoraggio avanzato e igiene informatica**: i sistemi di monitoraggio sfruttarono i dati storici per identificare le deviazioni dell'attività normale dei modem e per consentire un rapido rilevamento delle anomalie causate dal malware AcidRain; inoltre, poiché i modem satellitari rientrano nella categoria dei dispositivi IoT, furono fondamentali per la creazione di una resilienza futura anche le pratiche di igiene informatica attuate con l'aggiornamento del firmware, come la rimozione della password predefinita e la crittografia delle comunicazioni OTA, ed una revisione dettagliata dell'architettura della rete KA-SAT che portò a controlli di accesso più rigorosi e ad autenticazione multifattoriali[23]

[21] Over-The-Air
[22] National Security Agency, ente governativo statunitense responsabile della sicurezza nazionale
[23] Government Communications Headquarters, ente governativo britannico che si occupa della sicurezza, dello spionaggio e del controspionaggio nell'ambito delle comunicazioni

Troll Farm

Il conflitto digitale tra Russia e Ucraina è stato caratterizzato da uno sforzo senza precedenti da parte delle forze ucraine nel contrastare, oltre alle operazioni belliche e agli attacchi informatici, anche le operazioni di disinformazione russe e in particolar modo le attività delle Troll Farm. L'individuazione di tali attività richiese metodi analitici avanzati, costituiti dall'unione di algoritmi di Machine Learning o AI-Driven, utilizzati per identificare gli account sospetti e per analizzare le loro attività e il loro linguaggio, ad analisti umani, impegnati nell'incrociare i dati con gli eventi del mondo reale[24].

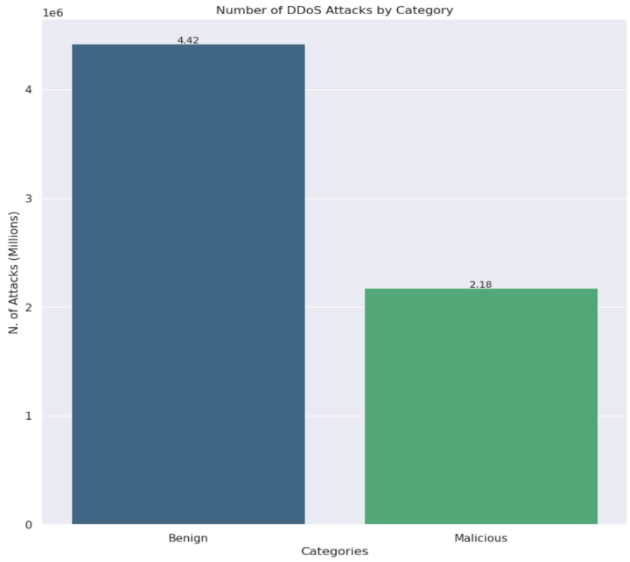
Un ruolo cruciale nella lotta contro le campagne di disinformazione dei troll russi è da attribuire anche a piattaforme di monitoraggio collaborative, come StopFake e CyberHub, in cui dei volontari pubblicano ancora oggi i contenuti sospetti, i quali vengono poi valutati ed esaminati degli analisti e diffusi attraverso i canali governativi ufficiali e i media indipendenti.

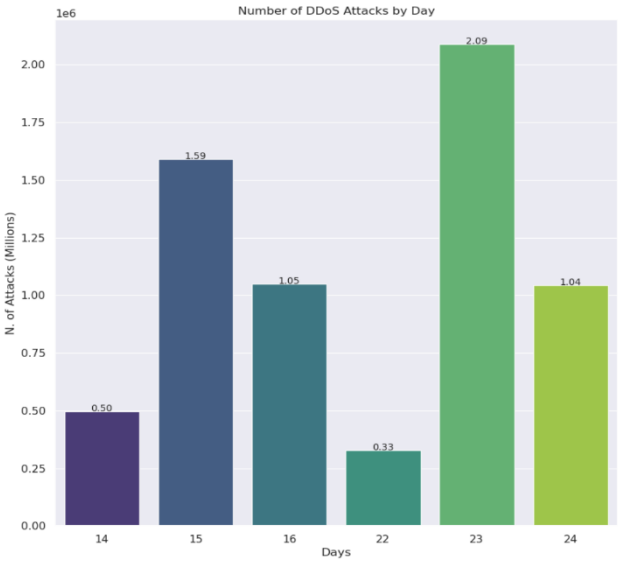
Inoltre, come meccanismo di difesa informatica, il Ministero Ucraino della Trasformazione Digitale, guidato dal vice primo ministro Mykhailo Federov, mobilitò migliaia di specialisti IT per creare un vero e proprio esercito attivo ancora oggi che prese il nome di "IT Army of Ukraine"[25]. I principali compiti vengono distribuiti tramite dei canali Telegram crittografati e spaziano dall'identificazione di malintenzionati al lancio di attacchi su siti web russi, con l'obiettivo di diffondere disinformazione e seminare sfiducia tra gli avversari. Questa mobilitazione rappresentò un caso senza precedenti, poiché mai prima d'ora un numero così elevato di volontari prestò le proprie conoscenze informatiche per creare un esercito digitale in difesa della propria nazione[25].

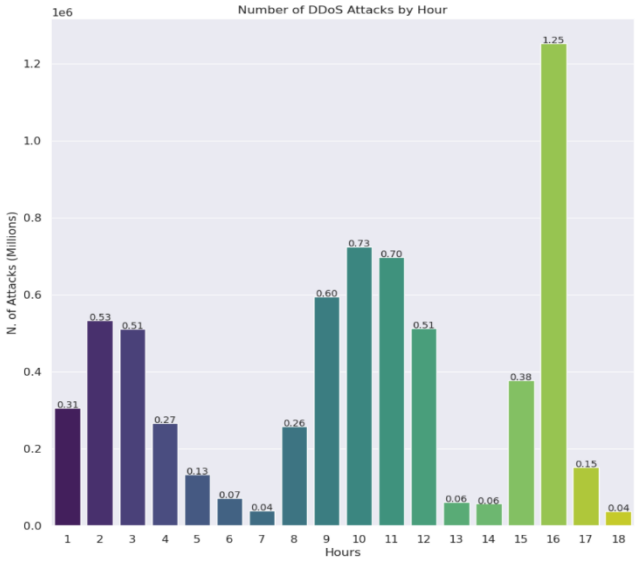
5. DDoS Attacks Detector

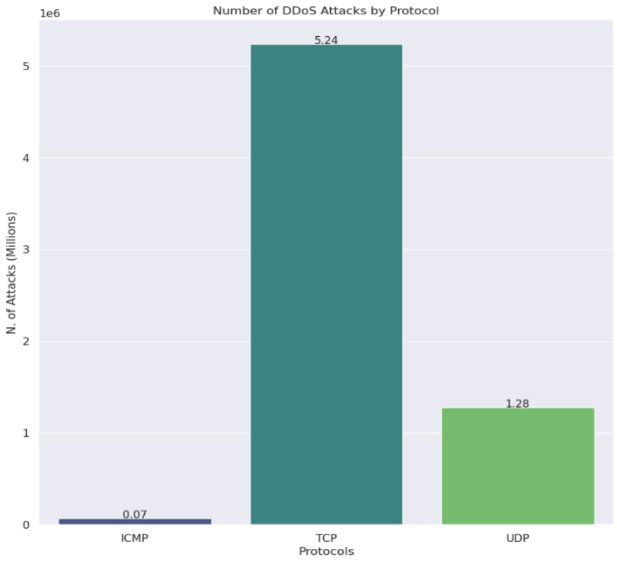
Per la parte tecnica, si è deciso di realizzare una rete neurale in grado di rilevare e classificare con accuratezza piuttosto elevata gli attacchi DDoS nelle reti SDN utilizzando il Machine Learning. Per la realizzazione del dataset di partenza sono stati recuperati e modificati secondo le necessità dei dataset, ispirati a quelli recuperabili dal CSE-CIC-IDS2018[24] e dal CIC-DOS2019[25].

Nella prima parte, i dati ottenuti sono stati ripuliti per poter effettuare un'analisi della distribuzione del traffico internet e quindi degli attacchi. La classificazione del traffico è stata effettuata per categoria, per giorno del mese, per ora del giorno e, infine, per tipologia di protocollo.









[24] https://www.unb.ca/cic/datasets/ids-2018.html
[25] https://www.unb.ca/cic/datasets/ddos-2019.html

Successivamente all'analisi dei dati ricavati, è stata effettuata un'analisi comparativa dettagliata di quattro algoritmi di ML e di uno di DL:

- **Decision Tree:** un algoritmo di apprendimento supervisionato non parametrico che viene utilizzato sia per le attività di classificazione che di regressione. Presenta una struttura gerarchica ad albero che consiste in un nodo radice, rami, nodi interni e nodi foglia

```
st = time.time()
#%%time
#-----------FIT MODEL DT---------------#
dt_model = DecisionTreeClassifier(max_depth=3, splitter="random")
dt_model.fit(X_train, y_train)
y_pred=dt_model.predict(X_test)
accuracy = metrics.accuracy_score(y_test, y_pred)
print('Accuracy of Decision Tree Classifier : %.2f' % (accuracy*100))
print(classification_report(y_test, y_pred, target_names = labels))
et = time.time() - st
class_acc.append(accuracy*100)
class_time.append(et)
```

```
Accuracy of Decision Tree Classifier : 87.43
              precision    recall  f1-score   support

      benign       0.92      0.89      0.90    442269
   malicious       0.79      0.84      0.81    217338

    accuracy                           0.87    659607
   macro avg       0.86      0.87      0.86    659607
weighted avg       0.88      0.87      0.88    659607
```

- **Quadratic Discriminant Analysis:** un algoritmo in cui ogni classe segue una distribuzione gaussiana; esso è generativo ed è molto simile a quella dell'analisi discriminante lineare, con l'eccezione che la covarianza e la media di tutte le classi sono uguali

```
st = time.time()
#%%time
#-----------FIT MODEL QDA---------------#
qda_model = QuadraticDiscriminantAnalysis()
qda_model.fit(X_train, y_train)
y_pred=qda_model.predict(X_test)
accuracy = metrics.accuracy_score(y_test, y_pred)
print('Accuracy of Quadratic Discriminant Analysis Classifier : %.2f' % (accuracy*100))
print(classification_report(y_test, y_pred, target_names = labels))
et = time.time() - st
class_acc.append(accuracy*100)
class_time.append(et)
```

```
Accuracy of Quadratic Discriminant Analysis Classifier : 55.53
              precision    recall  f1-score   support

      benign       0.98      0.34      0.51    442269
   malicious       0.42      0.99      0.59    217338

    accuracy                           0.56    659607
   macro avg       0.70      0.67      0.55    659607
weighted avg       0.80      0.56      0.54    659607
```

- **Logistic Regression:** un algoritmo di apprendimento automatico supervisionato che esegue attività di classificazione binaria prevedendo la probabilità di un risultato e fornendo un risultato limitato a due possibili risultati: sì/no, 0/1 o vero/falso; essa analizza la relazione tra una tra una o più variabili indipendenti e classifica i dati in classi discrete

```
st = time.time()
#%%time
#-----------FIT MODEL LR---------------#
lr_model = LogisticRegression()
lr_model.fit(X_train, y_train)
y_pred=lr_model.predict(X_test)
accuracy = metrics.accuracy_score(y_test, y_pred)
print('Accuracy of Logistic Regression Classifier : %.2f' % (accuracy*100))
print(classification_report(y_test, y_pred, target_names = labels))
et = time.time() - st
class_acc.append(accuracy*100)
class_time.append(et)
```

```
Accuracy of Logistic Regression Classifier : 95.15
              precision    recall  f1-score   support

      benign       0.95      0.98      0.96    442269
   malicious       0.96      0.89      0.92    217338

    accuracy                           0.95    659607
   macro avg       0.95      0.94      0.94    659607
weighted avg       0.95      0.95      0.95    659607
```

- **Stochastic Gradient Descent:** un algoritmo iterativo che ricerca il valore ottimale di una funzione obiettivo (Minimo/Massimo) e per farlo, invece di utilizzare l'intero set di dati per ogni iterazione, seleziona un singolo esempio di training casuale per calcolare il gradiente e aggiornare i parametri del modello; il suo vantaggio è la sua efficienza computazionale, specialmente nel caso di grandi set di dati

```
st = time.time()
#%%time
#-----------FIT MODEL SGD--------------#
sgd_model = SGDClassifier(loss="hinge", penalty="l2")
sgd_model.fit(X_train, y_train)
y_pred=sgd_model.predict(X_test)
accuracy = metrics.accuracy_score(y_test, y_pred)
print('Accuracy of Stochastic Gradient Classifier : %.2f' % (accuracy*100))
print(classification_report(y_test, y_pred, target_names = labels))
et = time.time() - st
class_acc.append(accuracy*100)
class_time.append(et)
```

```
Accuracy of Stochastic Gradient Classifier : 95.48
              precision    recall  f1-score   support

      benign       0.95      0.98      0.97    442269
   malicious       0.97      0.89      0.93    217338

    accuracy                           0.95    659607
   macro avg       0.96      0.94      0.95    659607
weighted avg       0.96      0.95      0.95    659607
```

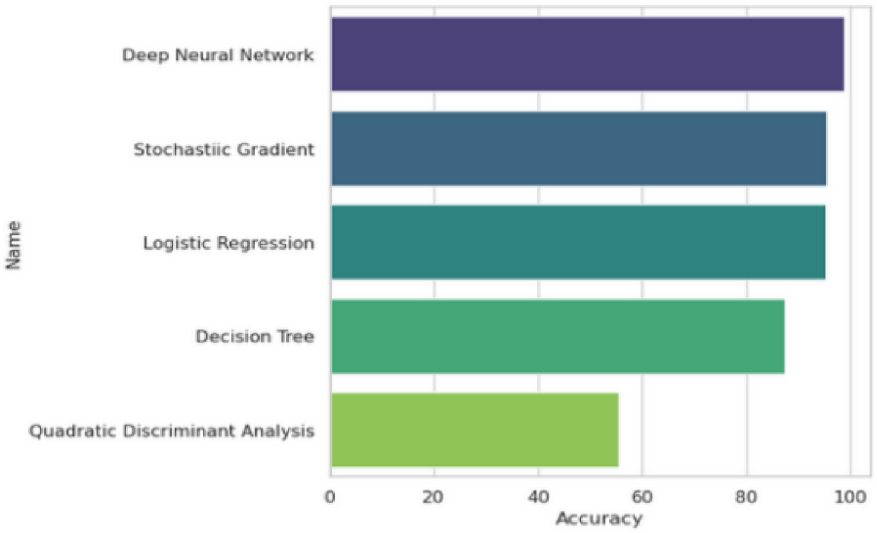
- **Deep Neural Network:** una rete composta da diversi strati, di cui almeno tre strati di nodi, ovvero strato di input, strato nascosto e strato di output che sono interconnessi tra loro; in questo caso, la rete utilizza la retropropagazione dell'errore come algoritmo di addestramento, tramite ReLU (Rectified Linear Unit), e la funzione di attivazione sigmoidea per il processo di classificazione. Inoltre, è stato deciso di utilizzare l'ottimizzatore Adam per la rete, il quale è perfetto nel caso di grandi dataset poiché rappresentando una combinazione di due algoritmi, ossia "Gradient Descent With Momentum" e " Root Mean Square Propagation (RMSP)", eredita i punti di forza e sfrutta gli attributi di questi due metodi per garantire una discesa del gradiente più ottimizzata

```
#-----------DEFINE MODEL WITH ADAM ALGORITHM--------------#
model = keras.Sequential()
model.add(Dense(24 , input_shape=(X_train.shape[1],) , activation="relu" , name="Layer1"))
model.add(Dense(10 , activation="relu" , name="Layer2"))
model.add(Dense(1 , activation="sigmoid" , name="OutLayer"))
opt = keras.optimizers.Adam(learning_rate=0.01)
model.compile( optimizer=opt, loss="binary_crossentropy", metrics=['accuracy', tf.keras.metrics.AUC()])
model.summary()
```

```
#-----------FIT MODEL DNN--------------#
st = time.time()
history_org = model.fit(
    X_train,
    y_train,
    batch_size=1024*N_CSV,
    epochs=10, verbose=2,
    callbacks=[model_ckp, reduce_lr],
    validation_data=(X_test,y_test),
    shuffle=True,
    class_weight=None,
    sample_weight=None,
    initial_epoch=0)
et = time.time() - st
loss, accuracy, *check = model.evaluate(X_test, y_test)
print('Accuracy of Deep neural Network : %.2f' % (accuracy*100))
class_acc.append(accuracy*100)
class_time.append(et)
```

```
Epoch 7/10
829/829 - 9s - 11ms/step - accuracy: 0.9884 - auc: 0.9931 - loss: 0.0491 - val_accuracy: 0.9888 - val_auc: 0.9929 - val_loss: 0.0486 - learni
ng_rate: 0.0100
Epoch 8/10
829/829 - 9s - 10ms/step - accuracy: 0.9884 - auc: 0.9931 - loss: 0.0489 - val_accuracy: 0.9884 - val_auc: 0.9932 - val_loss: 0.0483 - learni
ng_rate: 0.0100
Epoch 9/10
829/829 - 10s - 12ms/step - accuracy: 0.9885 - auc: 0.9932 - loss: 0.0487 - val_accuracy: 0.9888 - val_auc: 0.9928 - val_loss: 0.0494 - learn
ing_rate: 0.0100
Epoch 10/10
829/829 - 8s - 10ms/step - accuracy: 0.9885 - auc: 0.9933 - loss: 0.0487 - val_accuracy: 0.9888 - val_auc: 0.9935 - val_loss: 0.0475 - learni
ng_rate: 0.0100
20613/20613 ━━━━━━━━━━━━━━━━━━━━ 55s 3ms/step - accuracy: 0.9889 - auc: 0.9936 - loss: 0.0473
Accuracy of Deep neural Network : 98.88
```

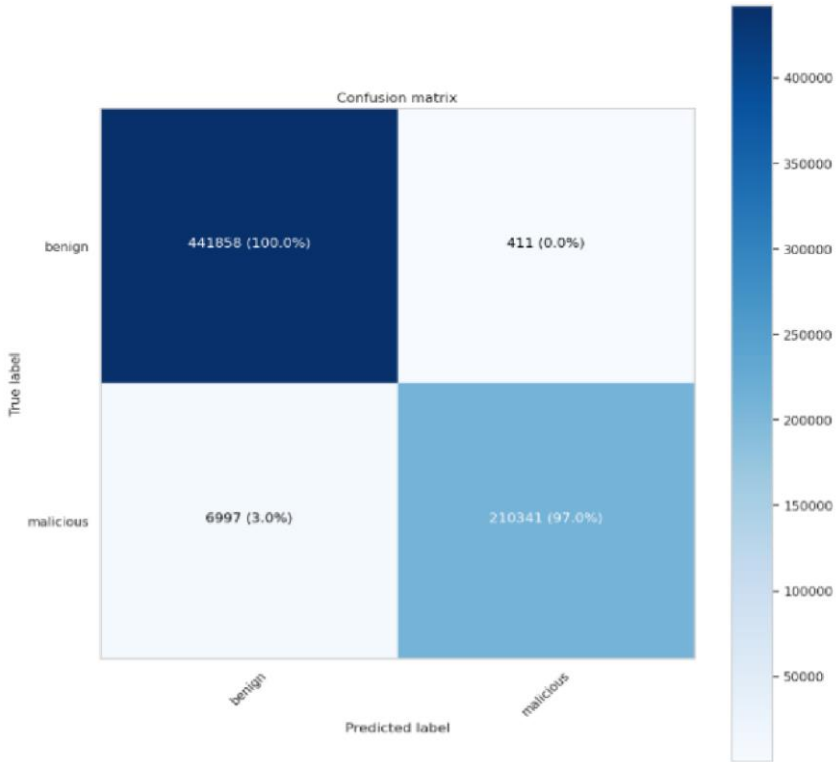
Una volta terminato l'apprendimento dei vari modelli, si può osservare che l'efficacia del modello proposto tramite Deep Neural Network è superiore a quella dei classificatori di base.



	Accuracy	Execution Time
Deep Neural Network	98.876905	101.496034
Stochastiic Gradient	95.480491	31.556996
Logistic Regression	95.148172	168.175483
Decision Tree	87.434791	35.084984
Quadratic Discriminant Analysis	55.534432	339.321120

L'accuratezza del modello che sfrutta la DNN è risultata pari al 98,88%, ovvero circa il 3,4% in più rispetto al miglior modello successivo Stochastic Gradient Descent, la cui accuratezza è del 95,48%. Invece, per quanto riguarda il tempo di esecuzione abbiamo una differenza di circa 70 secondi a fronte di un dataset contenente un numero di righe superiore a 6,5 milioni.

A tal proposito, è stata realizzata la matrice di confusione per il modello DNN in modo da restituire una chiara rappresentazione dell'accuratezza di classificazione statistica e anche un modo per valutare quali sono i risultati i punti deboli del modello ottenuto.



6. Conclusione

Da questo conflitto si può chiaramente evincere che l'obiettivo principale della Russia è stato quello di destabilizzare le infrastrutture di un paese avversario tramite una guerra non convenzionale, cercando di porre delle solite basi per poter sferrare un conseguente attacco militare terrestre. Questa nuova tipologia di guerra rappresenta un chiaro esempio della direzione che si sta decidendo di intraprendere per quanto riguarda i conflitti internazionali e non. Tuttavia, bisogna sottolineare che la Russia non rappresenta l'unico protagonista della guerra cibernetica, anzi, al giorno d'oggi, ci sono diverse nazioni, tra le quali soprattutto Stati Uniti e Cina, che utilizzano già da tempo iniziative informatiche con lo scopo di sopraffare i propri avversari.

L'utilizzo dell'evoluzione informatica e delle proprie conoscenze come arma per fini meno nobili rappresenta una realtà alla quale occorre dare il giusto peso e che non bisogna prendere più sottogamba. È facile pensare che questo tipo di avvenimenti accadano sempre e solo lontano dal suolo italiano o dalle nostre abitazioni, ma la verità è ben diversa, Infatti, basti pensare che l'Italia ha registrato un incremento di cyberattacchi del +65% nel 2023 e di un ulteriore +23% nel corso del primo semestre del 2024, secondo il rapporto Clusit 2024[26]. Per far fronte a questi attacchi rivolti a civili e ad aziende, innanzitutto, occorrerebbe rafforzare la consapevolezza informatica per rendere i cittadini più autonomi nel riconoscere fonti false e nell'aumentare il livello di attenzione da mantenere durante la navigazione web.

Invece, per quanto riguarda la difesa verso le infrastrutture critiche di un ecosistema nazionale, come per l'Ucraina, la rapida intensificazione del conflitto in ambito informatico ha dimostrato quanto bisogni essere preparati nel distribuire operazioni digitali all'interno e all'esterno dei propri confini nazionali ma anche nello sfruttare al meglio i recenti progressi sull'individuazione e sulla protezione delle minacce informatiche. Come descritto nel report, l'Ucraina, forte anche della memoria storica sui precedenti attacchi subiti e della collaborazione dei privati, ha dimostrato di saper impiegare al meglio tutto ciò per difendere sia i confini territoriali che i "confini" del proprio cyberspazio.

Tuttavia, l'unico dubbio che rimane riguarda la continua evoluzione delle minacce informatiche che corre di pari passo con quella delle operazioni difensive: riusciranno mai le operazioni di difesa informatica a rendere completamente immuni i sistemi da queste continue minacce?

Riferimenti bibliografici

[1] data.worldbank.org, *Data for Russian Federation, Ukraine, European Union*, https://data.worldbank.org/?locations=RU-UA-EU

[2] A. Makuch, I. Stebelsky, *The Maidan protest movement*, https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine , 2024

[3] Y. Bahid, O. Kutsenko, N. Rodríguez, D. White, *The statistical and dynamic modeling of the first part of the 2013-2014 Euromaidan protests in Ukraine: The Revolution of Dignity and preceding times*, https://doi.org/10.1371/journal.pone.0301639 , 2024

[4] S. Sukhankin, *Russian Electronic Warfare in Ukraine: Between Real and Imaginable, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/* , 2017

[5] M. Galeotti, *The "gerasimov doctrine" and russian nonlinear war*, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ , 2014

[6] Gen. L. D. Welch, *CYBERSPACE – THE FIFTH OPERATIONAL DOMAIN*, https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx , 2011

[7] R. A. Clarke, R. K. Klarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 2010

[8] J. Jordan, *International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict*, https://www.jstor.org/stable/26999974?seq=1 , 2020

[9] K. Berdan, D. Belson, J. Tomé, One year of war in Ukraine: Internet trends, attacks, and resilience, https://blog.cloudflare.com/one-year-of-war-in-ukraine/ , 2023

[10] B. Smith, *Defending Ukraine: Early Lessons from the Cyber War,* https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ , 2022

[11] ESET Research, *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine*, https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/ ,2022

[12] Hasherezade, A. Saini, R. Santos, *HermeticWiper: A detailed analysis of the destructive malware that targeted Ukraine*, https://www.threatdown.com/blog/hermeticwiper-a-detailed-analysis-of-the-destructive-malware-that-targeted-ukraine/ , 2022

[13] C. Doman, *Technical Analysis of the DDoS Attacks against Ukrainian Websites*, https://www.cadosecurity.com/blog/technical-analysis-of-the-ddos-attacks-against-ukrainian-websites , 2022

[14] F. Quiquet, *An analysis of the Viasat cyber attack with the MITRE ATT&CK® framework*, https://www.spacesecurity.info/an-analysis-of-the-viasat-cyber-attack-with-the-mitre-attck-framework/ , 2023

[15] C. Silvermann, J. Kao, *Infamous Russian Troll Farm Appears to Be Source of Anti-Ukraine Propaganda*, https://www.propublica.org/article/infamous-russian-troll-farm-appears-to-be-source-of-anti-ukraine-propaganda , 2022

[16] G. Alieva, I. Kloo, K. M. Carley, *Analyzing Russia's propaganda tactics on Twitter using mixed methods network analysis and natural language processing: a case study of the 2022 invasion of Ukraine*, https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-024-00479-w , 2024

[17] S. Duguin, P. Pavlova, *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf , 2023

[18] A. Kott, G. Dubynskyi, A. Paziuk, S. E. Galaitsi, B. D. Trump, I. Linkov, *Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security*, https://arxiv.org/pdf/2408.14667 , 2024

[19] J. Igorevna, *Ukraine's Response to Cyber Threats a Model in DDoS Prevention*, https://www.radware.com/blog/ddos-protection/2022/11/ukraines-response-to-cyber-threats-a-model-in-ddos-prevention/ , 2022

[20] CISA, FBI, *Destructive Malware Targeting Organizations in Ukraine*, https://www.cisa.gov/sites/default/files/publications/AA22-057A_Destructive_Malware_Targeting_Organizations_in_Ukraine.pdf , 2022

[21] P. Tavares, HermeticWiper malware used against Ukraine, https://www.infosecinstitute.com/resources/malware-analysis/hermeticwiper-malware-used-against-ukraine/ , 2022

[22] S. Cohen, *AcidRain Malware and Viasat Network Downtime in Ukraine: Assessing the Cyber War Threat*, https://www.justsecurity.org/83021/acidrain-malware-and-viasat-network-downtime-in-ukraine-assessing-the-cyber-war-threat/ , 2022

[23] N. Saunders, M. Colaluca, *DEF CON 31 Conference - Defending KA-SAT: The Detailed Story of the Response*, https://www.youtube.com/watch?v=qI_ICtX3Gm8 , 2023

[24] F. Ezzeddine, O. Ayoub, S. Giordano, G. Nogara, I. Sbeity, E. Ferrara, L. Luceri, *Exposing influence campaigns in the age of LLMs: a behavioral-based AI approach to detecting state-sponsored trolls*, https://doi.org/10.1140/epjds/s13688-023-00423-4 , 2023

[25] V. Karagiannopoulos, *Ukraine's IT army is a world first: here's why it is an important part of the war*, https://theconversation.com/ukraines-it-army-is-a-world-first-heres-why-it-is-an-important-part-of-the-war-212745, 2023

[26] Clusit, Rapporto Clusit sulla sulla sicurezza ICT in Italia, https://clusit.it/rapporto-clusit/ , 2024