Gli attacchi informatici contro obiettivi italiani nel contesto della guerra in Ucraina

Guerra ibrida e dominio *cyber*

Dopo lo scoppio della guerra in Ucraina, iniziata il 24 febbraio 2022, soggetti pubblici e privati di Stati membri della NATO sono stati vittime di attacchi informatici attribuiti ad attori russi o filo-russi.

In termini generali, com'è noto, la Federazione Russa ha dedicato molte energie al campo della «guerra ibrida» (vedi, tra gli altri, Dominioni e Tafuro Ambrosetti 2020), compresa proprio la cosiddetta «quinta dimensione» del conflitto ovvero il dominio *cyber* (cfr. Maurer e Hinck 2018; Beccaro 2021). Tali sforzi da parte di Mosca hanno conosciuto un'ulteriore espansione con la guerra in Ucraina.

Gli attacchi informatici DDoS contro obiettivi italiani

In questo contesto, anche l'Italia, a marzo 2022 inserita da Mosca nel novero degli Stati ostili per il suo sostegno all'Ucraina, ha subito attacchi informatici attribuiti a gruppi filo-russi. In particolare, a partire dall'11 maggio 2022 alcuni siti web di istituzioni e anche di attori privati italiani sono finiti sotto attacco; tra questi portali vi sarebbero stati quelli del Senato della Repubblica, dell'Istituto Superiore di Sanità (ISS) e dell'Automobile Club d'Italia (ACI) (Santarpia 2022).

Gli attacchi informatici eseguiti nella giornata dell'11 maggio e nei giorni successivi sono stati di tipo DDoS (*Distributed Denial of Service*): con questa espressione si designa un malfunzionamento dovuto a un attacco informatico che causa la saturazione deliberata delle risorse di un sistema informatico, come un sito web su un web server, fino a renderlo non più in grado di erogare il servizio; a differenza del semplice DoS (*Denial of Service*), nel caso dell'attacco DDoS il traffico che colpisce la vittima proviene da molteplici fonti.

In particolare, come confermato ufficialmente dal CSIRT (Computer Security Incident Response Team) italiano, istituito presso l'Agenzia per la cybersicurezza nazionale (ACN) (cfr. Marrone et al. 2021), questi attacchi «sono stati condotti utilizzando tecniche che differiscono dai più comuni attacchi DDOS di tipo volumetrico passando inosservati quindi ai sistemi di protezione comunemente utilizzati sul mercato contro questo tipo di attacchi poiché avvengono utilizzando una banda limitata. Tali tecniche DDOS, definite di tipo applicativo, mirano a saturare le risorse dei sistemi che erogano i servizi tra cui i server web. Nel caso specifico è stato rilevato l'utilizzo della tecnica definita "Slow HTTP" che, di norma, utilizza richieste HTTP GET per saturare le connessioni disponibili di un server web» (CSIRT 2022, p. 1).

Il collettivo Killnet

Gli attacchi informatici dell'11 maggio 2022 sono stati rivendicati online da un collettivo *hacker* chiamato Killnet. Tale gruppo era stato menzionato alcune settimane prima anche in un *alert* della CISA (Cybersecurity and Infrastructure Security Agency), l'agenzia federale per la cybersicurezza e la protezione delle infrastrutture critiche degli Stati Uniti, insieme ad altri «gruppi cybercriminali allineati con la Russia» (*Russian-aligned cybercrime groups*), giudicati una minaccia a organizzazioni che gestiscono infrastrutture critiche. Secondo il medesimo documento, a marzo 2022 Killnet aveva anche portato a termine un attacco DDoS contro un aeroporto degli Stati Uniti (il Bradley International Airport, il più trafficato del Connecticut) (CISA 2022).

Il collettivo Killnet ha esibito le proprie intenzioni e minacce su internet. In particolare, il suo principale canale sulla piattaforma Telegram è apparso a gennaio 2022. Nondimeno, sino allo

scoppio della guerra in Ucraina, Killnet appariva come un gruppo cybercriminale, specializzato in attacchi DDoS.

Soltanto dal giorno successivo all'invasione russa dell'Ucraina, il gruppo ha evidenziato apertamente le proprie simpatie a favore di Mosca, inizialmente con messaggi ostili nei confronti delle azioni messe in atto contro la Russia da Anonymous, il famigerato movimento di hacktivisti (attivisti *hacker*), che si è schierato a sostegno dell'Ucraina. Il collettivo filo-russo ha quindi invitato altri *hackers* a unirsi alla propria missione. Sotto il nome di Killnet operano ora diversi sotto-gruppi, come Legion, Mirai e Jacky (De Lucia 2022; Frediani 2022).

La portata degli attacchi informatici di Killnet

Nei mesi scorsi gli attacchi informatici ad opera del collettivo Killnet sono cresciuti notevolmente. Secondo le informazioni attualmente disponibili, i destinatari di queste attività ostili avrebbero incluso obiettivi della Romania, della Repubblica Ceca, della Polonia, dell'Estonia e della Lettonia. Pochi giorni prima degli attacchi ai danni di obiettivi italiani sarebbero stati presi di mira anche siti web di istituzioni tedesche (Gebauer et al. 2022).

Com'è stato notato, gli attacchi subiti da soggetti istituzionali italiani non hanno comportato conseguenze assai severe; essi hanno interrotto la disponibilità dei siti web colpiti per una durata temporanea limitata, senza mettere a repentaglio la fornitura di servizi essenziali per i cittadini. Oltretutto, gli attacchi non hanno compromesso alcuna infrastruttura critica (Rigoni e Filippone 2022).

Conclusioni

Gli attacchi informatici contro obiettivi italiani rivendicati dal collettivo Killnet dopo lo scoppio della guerra in Ucraina hanno mirato a produrre un impatto rilevante sul piano simbolico, di fatto ampliato dalla copertura mediatica di questi fatti, ma non hanno determinato un danno economico consistente o un reale vantaggio militare (Rigoni e Filippone 2022).

Nondimeno, la minaccia potenziale posta da attacchi informatici merita attenzione, specialmente in questa congiuntura segnata dalla guerra in Ucraina.

Bibliografia

- Beccaro, A. (2021). *Il concetto di Gray zone: la dottrina GERASIMOV e l'approccio russo alle operazioni ibride. Possibili convergenze con la dottrina Cinese. Obiettivi strategici e metodologia d'impiego nello scenario geopolitico attuale. Prospettive del ruolo del Potere Aereo e Spaziale nei "Gray zone Scenarios"*, Ricerca, Centro Militare di Studi Strategici (CeMiSS) - Centro Alti Studi per la Difesa (CASD), testo disponibile al sito: https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/Beccaro_AP_SMD_01_SMA_04.aspx (consultato il 10 giugno 2022).
- CISA (2022). *Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, Cybersecurity and Infrastructure Security Agency, 20 aprile, testo disponibile al sito: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (consultato il 10 giugno 2022).
- CSIRT (2022). *Attacchi DDOS ai danni di soggetti nazionali ed internazionali avvenuti a partire dall'11 Maggio 2022: Analisi e mitigazione (BL01/220513/CSIRT-ITA)*, Computer Security Incident Response Team – Italia, 13 maggio, testo disponibile al sito: https://www.csirt.gov.it/contenuti/attacchi-ddos-ai-danni-di-soggetti-nazionali-ed-internazionali-avvenuti-a-partire-dall11-maggio-2022-analisi-e-mitigazione-bl01-220513-csirt-ita (consultato il 10 giugno 2022).

- De Lucia, E. (2022). KillNet, chi è la cyber gang vicina al Cremlino che sta attaccando l'Italia, Cybersecurity360, 16 maggio, https://www.cybersecurity360.it/nuove-minacce/killnet-chi-e-la-cyber-gang-vicina-al-cremlino-che-sta-attaccando-litalia/ (consultato il 10 giugno 2022).
- Dominioni, S. e Tafuro Ambrosetti, E., eds. (2020). *Framing Russian Hybrid Warfare, Dossier*, ISPI, 4 luglio, testo disponibile al sito: https://www.ispionline.it/it/pubblicazione/framing-russian-hybrid-warfare-26792 (consultato il 10 giugno 2022).
- Frediani, C. (2022). Gli attacchi ai siti italiani, Guerre di rete, 15 maggio, testo disponibile al sito: https://guerredirete.substack.com/p/guerre-di-rete-gli-attacchi-ai-siti?s=r (consultato il 10 giugno 2022).
- Gebauer, M., Röbel, S., Rosenbach, M. e Wiedmann-Schmidt, W. (2022). Putin-Fans attackieren deutsche Behördenseiten, Der Spiegel, 6 maggio, testo disponibile al sito: https://www.spiegel.de/politik/deutschland/killnet-cyberangriffe-wladimir-putin-fans-attackieren-deutsche-behoerdenseiten-a-2be17f20-3688-4674-b82d-d7889a532c80 (consultato il 10 giugno 2022).
- Marrone, A., Sabatino, E. e Credi, O. (2021). *L'Italia e la difesa cibernetica*, Documenti IAI, Istituto Affari Internazionali (IAI), 30 settembre, testo disponibile al sito: https://www.iai.it/it/pubblicazioni/litalia-e-la-difesa-cibernetica (consultato il 10 giugno 2022).
- Maurer, T. e Hinck, G. (2018). *Russia: Information Security Meets Cyber Security*, in F. Rugge (ed.), Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace, Report, ISPI, testo disponibile al sito: https://www.ispionline.it/it/pubblicazione/confronting-axis-cyber-21458 (consultato il 10 giugno 2022).
- Rigoni, A. e Filippone, R. (2022). *Killnet: guerra informatica o mediatica?*, Commentary, ISPI, 20 maggio, testo disponibile al sito: https://www.csirt.gov.it/contenuti/attacchi-ddos-ai-danni-di-soggetti-nazionali-ed-internazionali-avvenuti-a-partire-dall11-maggio-2022-analisi-e-mitigazione-bl01-220513-csirt-ita (consultato il 10 giugno 2022).
- Santarpia, V. (2022). Attacco hacker russi a siti Italia, anche Senato e Iss presi di mira, *Corriere della Sera, 11 maggio*, testo disponibile al sito: https://www.corriere.it/cronache/22_maggio_11/attacco-hacker-russi-siti-italia-anche-senato-difesa-presi-mira-612c2c38-d149-11ec-b465-8b7c23727ee0.shtml (consultato il 10 giugno 2022).