“Il valore della scienza sta nella lungimiranza. Nuove sfide richiedono un ripensamento delle forme e dei metodi delle operazioni di combattimento”, così era intitolato l’articolo che riportava l’intervento del Capo di Stato Maggiore russo, Generale Valerij Vasil’evič Gerasimov, tenuto ad una conferenza all’Accademia di Scienza Militare di Mosca (2013). Si traduce in una gamma di azioni che variano dagli attacchi cibernetici alle campagne di contro-informazione, dai richiami costanti al nucleare, alle operazioni sotto copertura. Tali attacchi datano dal 2014 e sono rivolti contro il settore energetico e dei trasporti, i media, in concomitanza con le elezioni locali, fornitori di energia, contro istituzioni finanziarie statali (FIs) e compagnie ferroviarie.

Elenco Malware NGW

DDoS	Distributed Denial-of-Service, portali web di alcuni organi del governo, attacchi settore finanziario, campagne di disinformazione e attività distruttive di sabotaggio.
Whisper Gate	contiene tre singoli componenti implementati, incluso un bootloader dannoso che corrompe i dischi locali rilevati, un downloader basato su Discord e un file wiper. L'attività si è verificata più o meno nello stesso momento in più siti Web.
Hermetic Wiper	primo malware ufficiale della guerra Russo-Ucraina, dalle funzionalità devastanti, coinvolto in attacchi mirati verso obiettivi strategici del Paese “consiste nel distruggere i dati presenti su un dispositivo e renderli irrecuperabili, minando il corretto funzionamento del sistema operativo in esecuzione”.
Cyclops Blink	associato al Threat Actor russo conosciuto come Sandworm (alias Voodoo Bear). Distribuito verso dispositivi di rete esposti sul web e sulla rete Internet, sopprime l’aggiornamento “WatchGuard”. Già segnalate da Cisa, Fbi, National Security Agency, National cyber security centre e il nostro CSIRT che, con la collaborazione dell’Agenzia Cyber Nazionale, ha pubblicato una nota in cui si dice espressamente che tale malware è distribuito anche sul territorio italiano.
Filecoder.NKH	distribuito attraverso una compromissione della catena di approvvigionamento di una società informatica ucraina
XDATA	distribuito per un breve periodo attraverso un meccanismo di aggiornamento del software di M.E. Doc, prodotto software di contabilità ucraino utilizzato da molte aziende
FakeCry	è stato distribuito attraverso un aggiornamento malevolo di M.E. Doc, una famiglia di malware che impersona il famigerato ransomware WannaCry
NotPetya	distribuito attraverso lo stesso meccanismo M.E. Doc, con test precedenti probabilmente distribuiti attraverso il SWC di un sito web di un media ucraino Utilizza strumenti per agire sulla percezione dell’avversario cercando di alterarne scelte strategiche e comportamento per manipolarne il processo decisionale o sfruttare a proprio vantaggio, le divisioni interne che ne conseguono, indebolendolo a tal punto da realizzare l’obiettivo prefissato.
Bad Rabbit	contro la rete di trasporti ucraina attraverso il SWC di siti in diversi paesi, tra i quali l’Ucraina, la Russia, la Turchia e la Bulgaria.
Black Energy	creato negli anni duemila dall’hacker noto Cr4sh e venduto per circa 700 dollari nel 2007. Si è evoluto nel corso degli anni. Attribuito a Voodoo Bear (versione 3) in associazione con il wiper KillDisk (aka PassKillDisk). Utilizzato per una serie di attacchi DDoS nel 2008 contro network georgiani
Mimikatz	worm per il furto di credenziali Aumenta il potenziale impatto sulle reti dopo l’infiltrazione iniziale.
Eternal Blue	per la vulnerabilità CVE-2017-0144. Aumenta il potenziale impatto sulle reti dopo l’infiltrazione iniziale.