2024/1778

24.6.2024

REGOLAMENTO DI ESECUZIONE (UE) 2024/1778 DEL CONSIGLIO

del 24 giugno 2024

che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri ([1]), in particolare l'articolo 13, paragrafo 1,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 17 maggio 2019 il Consiglio ha adottato il regolamento (UE) 2019/796.

(2) Le misure restrittive mirate contro gli attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri sono una delle misure previste nel quadro dell'Unione relativo a una risposta diplomatica comune alle attività informatiche dolose (pacchetto di strumenti della diplomazia informatica) e sono uno strumento fondamentale per prevenire, scoraggiare e contrastare tali attività.

(3) Le attività informatiche dolose contro le infrastrutture critiche o i servizi essenziali, anche attraverso l'uso di ransomware e wiper, il targeting delle catene di approvvigionamento e il ciberspionaggio, comprese le attività di furto di proprietà intellettuale, sono in aumento in termini di numero, frequenza e sofisticatezza. Con i loro effetti dirompenti e distruttivi, queste attività rappresentano una minaccia sistemica per la sicurezza, l'economia, la democrazia dell'Unione e la società in generale.

(4) L'uso delle operazioni informatiche che hanno consentito e accompagnato la guerra di aggressione non provocata e ingiustificata della Russia nei confronti dell'Ucraina incide sulla stabilità e sulla sicurezza globali, rappresenta un notevole rischio di escalation e si somma all'aumento già significativo delle attività informatiche dolose al di fuori del contesto dei conflitti armati negli ultimi anni. I crescenti rischi di cibersicurezza e il panorama di minacce informatiche globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti informatici da uno Stato membro all'altro e da paesi terzi all'Unione, richiedono inoltre misure restrittive a norma del regolamento (UE) 2019/796.

(5) Nel quadro dell'azione dell'Unione duratura, mirata e coordinata contro gli autori di minacce informatiche persistenti, sei persone fisiche dovrebbero essere inserite nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive di cui all'allegato I del regolamento (UE) 2019/796. Tali persone sono responsabili di attacchi informatici o vi erano coinvolte con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.

(6) È pertanto opportuno modificare di conseguenza l'allegato I del regolamento (UE) 2019/796,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

L'allegato I del regolamento (UE) 2019/796 è modificato come indicato nell'allegato del presente regolamento.

([1]) GU L 129 I del 17.5.2019, pag. 1.

Articolo 2

Il presente regolamento entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Lussemburgo, il 24 giugno 2024…

Per il Consiglio

Il presidente

J. BORRELL FONTELLES

ALLEGATO

Le voci seguenti sono aggiunte alla sezione «A. Persone fisiche» nell'allegato I del regolamento (UE) 2019/796:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Data di nascita: 3.8.1985 Cittadinanza: russa Sesso: maschile	Ruslan PERETYATKO ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. Ruslan PERETYATKO fa parte del "Callisto Group", gruppo di agenti dell'intelligence militare russa che conduce operazioni informatiche contro Stati membri dell'UE e Stati terzi. Callisto Group (alias "Seaborgium", "Star Blizzard", "ColdRiver", "TA446") ha avviato campagne pluriennali di phishing utilizzate per rubare credenziali e dati di account. Inoltre, Callisto Group è responsabile di campagne mirate a persone singole e a funzioni statali essenziali, anche nei settori della difesa e delle relazioni esterne. Pertanto, Ruslan PERETYATKO è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Data di nascita: 18.5.1987 Luogo di nascita: città di Syktyvkar, Russia Cittadinanza: russa Sesso: maschile	Andrey Stanislavovich KORINETS ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. Andrey Stanislavovich KORINETS è un agente di "Center 18" del Servizio federale di sicurezza (FSB) della Federazione russa. Andrey Stanislavovich KORINETS fa parte del "Callisto Group", gruppo di agenti dell'intelligence militare russa che conduce operazioni informatiche contro Stati membri dell'UE e Stati terzi. Callisto Group (alias "Seaborgium", "Star Blizzard", "ColdRiver", "TA446") ha avviato campagne pluriennali di phishing utilizzate per rubare credenziali e dati di account. Inoltre, Callisto Group è responsabile di campagne mirate a persone singole e a funzioni statali essenziali, anche nei settori della difesa e delle relazioni esterne. Pertanto, Andrey Stanislavovich KORINETS è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (grafia russa) Олександр СКЛЯНКО (grafia ucraina) Data di nascita: 5.8.1973 Passaporto: EC 867868, rilasciato il 27.11.1998 (Ucraina) Sesso: maschile	Oleksandr SKLIANKO ha preso parte ad attacchi informatici con effetti significativi contro Stati membri dell'UE come pure ad attacchi informatici con effetti significativi contro Stati terzi. Oleksandr SKLIANKO fa parte del gruppo di hacker Armageddon, sostenuto dal Servizio federale di sicurezza (FSB) della Federazione russa, che ha compiuto vari attacchi informatici con effetti significativi sul governo dell'Ucraina e sugli Stati membri dell'UE e loro funzionari governativi, anche utilizzando email di phishing e campagne di malware. Pertanto, Oleksandr SKLIANKO è coinvolto in attacchi informatici con effetti significativi contro Stati terzi come pure in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (grafia russa) Микола ЧЕРНИХ (grafia ucraina) Data di nascita: 12.10.1978 Passaporto: EC 922162, rilasciato il 20.1.1999 (Ucraina) Sesso: maschile	Mykola CHERNYKH ha preso parte ad attacchi informatici con effetti significativi contro Stati membri dell'UE come pure ad attacchi informatici con effetti significativi contro Stati terzi. Mykola CHERNYKH fa parte del gruppo di hacker Armageddon, sostenuto dal Servizio federale di sicurezza (FSB) della Federazione russa, che ha compiuto vari attacchi informatici con effetti significativi sul governo dell'Ucraina e sugli Stati membri dell'UE e loro funzionari governativi, anche utilizzando email di phishing e campagne di malware. In qualità di ex dipendente del servizio di sicurezza dell'Ucraina, è accusato in Ucraina di tradimento e di interferenza non autorizzata nel funzionamento di macchine da calcolo elettroniche e di sistemi automatizzati. Pertanto, Mykola CHERNYKH è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data di nascita: 20.4.1989 Luogo di nascita: Serpukhov, Federazione russa Cittadinanza: russa Indirizzo: Serpukhov Sesso: maschile	Mikhail Mikhailovich TSAREV ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Mikhail Mikhailovich TSAREV, noto anche con i soprannomi online "Mango", "Alexander Grachev", "Super Misha", "Ivanov Mixail", "Misha Krutysha" e "Nikita Andreevich Tsarev", svolge un ruolo chiave nell'impiego di programmi malware "Conti" e "Trickbot" ed è coinvolto nel gruppo di minaccia "Wizard Spider" con sede in Russia. I programmi malware Conti e Trickbot sono stati creati e sviluppati dal "Wizard Spider". Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari. Le campagne di Wizard Spider, che utilizzano malware quali Conti, Ryuk e TrickBot, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Mikhail Mikhailovich TSAREV è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data di nascita: 19.5.1982 Luogo di nascita: Abakan, Federazione russa Cittadinanza: russa Sesso: maschile	Maksim Galochkin ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Maksim Galochkin è noto anche con i soprannomi online "Benalen", "Bentley", "Volhvb", "volhvb", "manuel", "Max17" e "Crypt". Galochkin svolge un ruolo chiave nell'impiego di programmi malware TrickBot e Conti ed è coinvolto nel gruppo di minaccia "Wizard Spider". Ha guidato un gruppo di tester, con responsabilità per lo sviluppo, la supervisione e l'attuazione di test per il programma malware TrickBot, creato e impiegato da "Wizard Spider". Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari. Le campagne di Wizard Spider che utilizzano malware quali Conti, Ryuk e TrickBot, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Maksim Galochkin è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024»

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj