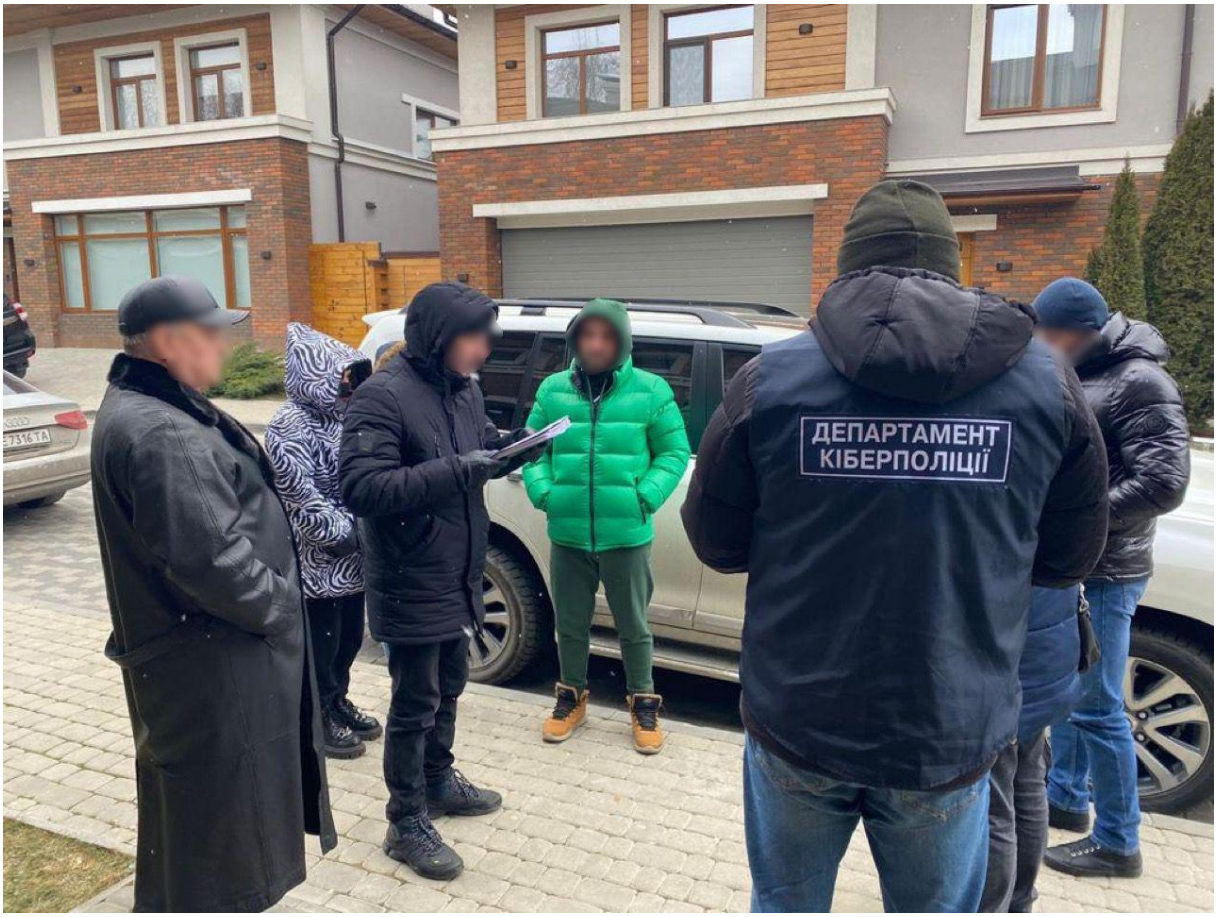
Cyberpolitie ontdekt hackgroep op aanvallen van buitenlandse bedrijven met versleuteld virus

Met behulp van malware, hackers crypto-gegevens en eiste losgeld voor toegang herstel. Meer dan 50 bedrijven in Europa en Amerika hadden te lijden onder illegale acties. De verliezen lopen op tot meer dan een miljoen Dollar.

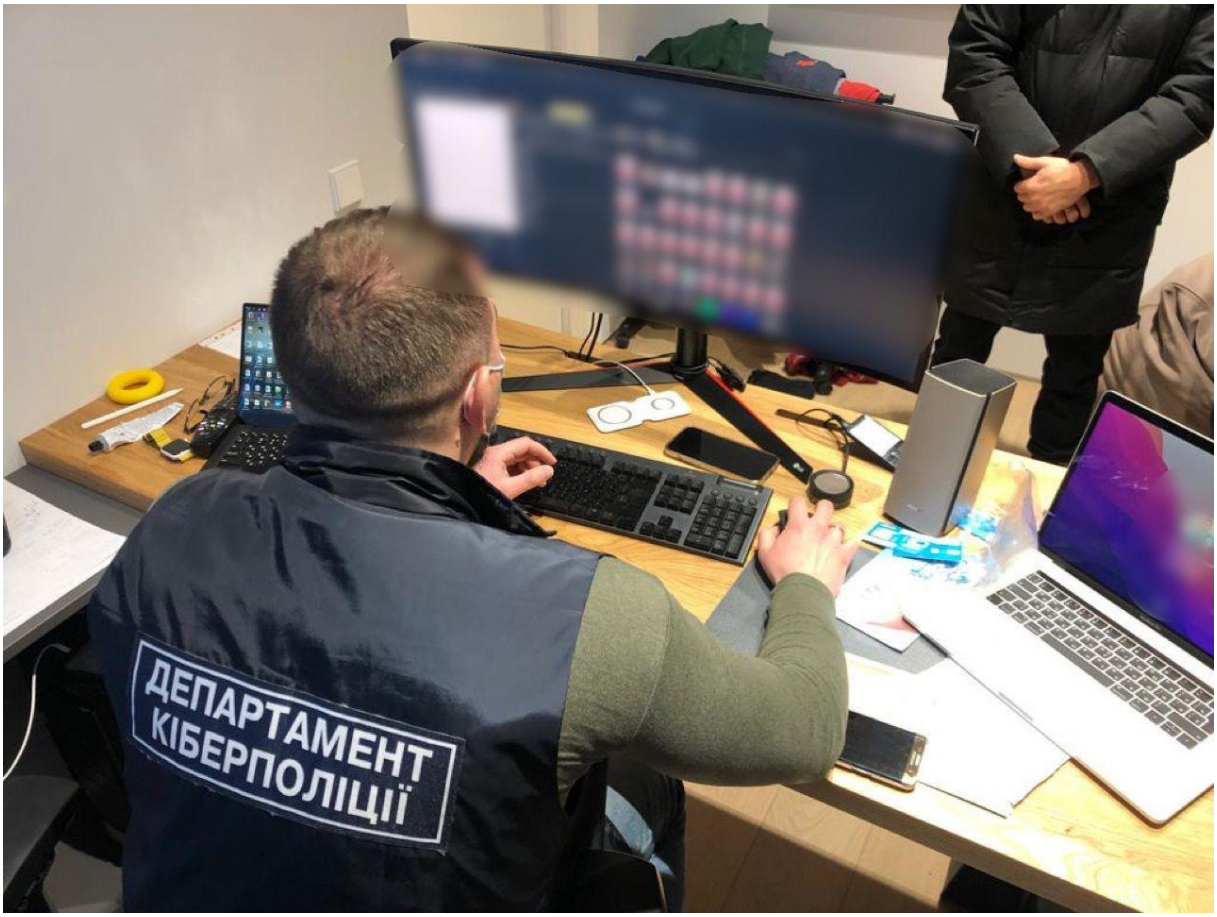
De activiteiten van de hackgroep werden blootgelegd door de cyberpolitie samen met de hoofdonderzoeksafdeling van de nationale politie, sbu-officieren en in samenwerking met collega-wetshandhavers uit het VK en de VS.



De organisator van de groep, een 36-jarige Kievse, voerde samen met zijn vrouw en drie kennissen cyberaanvallen uit op buitenlandse bedrijven.

Met behulp van malware van het ransomware-type, de gegevens van de verdachten crypto-slachtoffers. Ransomware kwam in de techniek door spammailings naar e-mailboxen. Drie performers kregen losgeld voor het herstellen van de toegang tot gegevens op hun eigen crypto wallets.

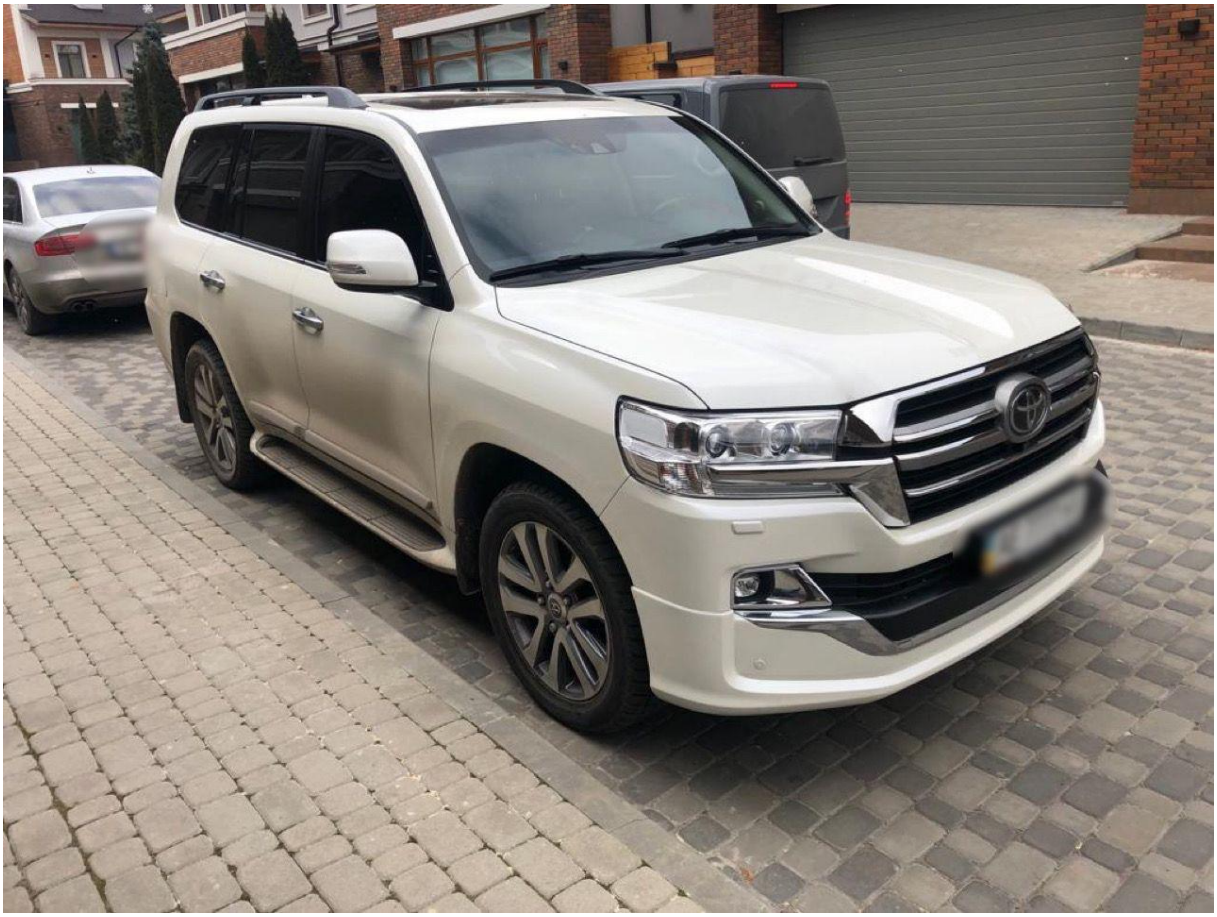
Volgens voorlopige gegevens hebben meer dan 50 bedrijven geleden onder de aanvallen, het totale bedrag aan verliezen bereikt meer dan een miljoen Amerikaanse dollar.



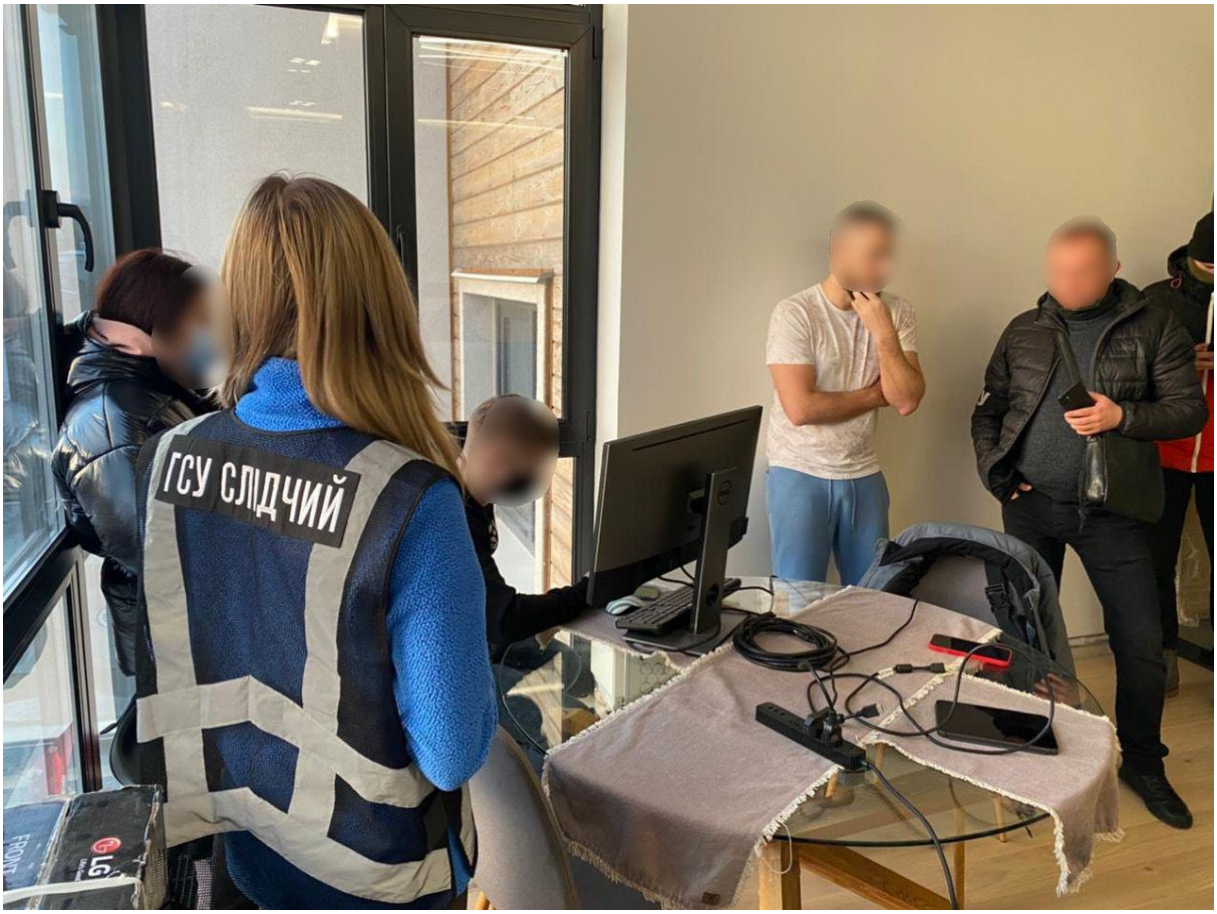
Bovendien hebben de verdachten in opdracht van buitenlandse hackers diensten geleverd voor het subcrimineren van de IP-adressen van gebruikers. Daardoor konden deze laatsten heimelijk illegale activiteiten uitvoeren.

Ook werd vastgesteld dat een van de verdachten werd gezocht door wetshandhavingsinstanties van andere staten. Zo ontving de dader met behulp van het "virus" de bankkaartgegevens van klanten van Britse banken. Op kosten van de slachtoffers kocht de aanvaller verschillende producten in online winkels en verkocht deze vervolgens door.

Politieagenten voerden samen met wetshandhavers uit het Verenigd Koninkrijk en de Verenigde Staten negen huiszoekingen uit in de huizen van de verdachten en in hun auto's. Computerapparatuur, mobiele telefoons, bankpassen, flashdrives en drie auto's werden in beslag genomen.
Medewerkers van de TOR-eenheid van de Patrouillepolitie waren ook betrokken bij de huiszoekingen.



De strafprocedure werd geopend op grond van deel 2 van art. 361 (Ongeoorloofde interferentie met de werking van computers, geautomatiseerde systemen, computernetwerken of telecommunicatienetwerken), deel 2 van art. 361-1 (Creatie met het oog op het gebruik, de distributie of de verkoop van schadelijke software of hardware, evenals de distributie of verkoop ervan), art. 209 (Legalisatie (witwassen) van op criminele wijze verkregen goederen) van het Wetboek van Strafrecht van Oekraïne. Het onderzoek loopt nog.



Procedurele begeleiding wordt uitgevoerd door het Bureau van de Procureur-Generaal.

Cyber Politie Afdeling van de Nationale Politie van Oekraïne