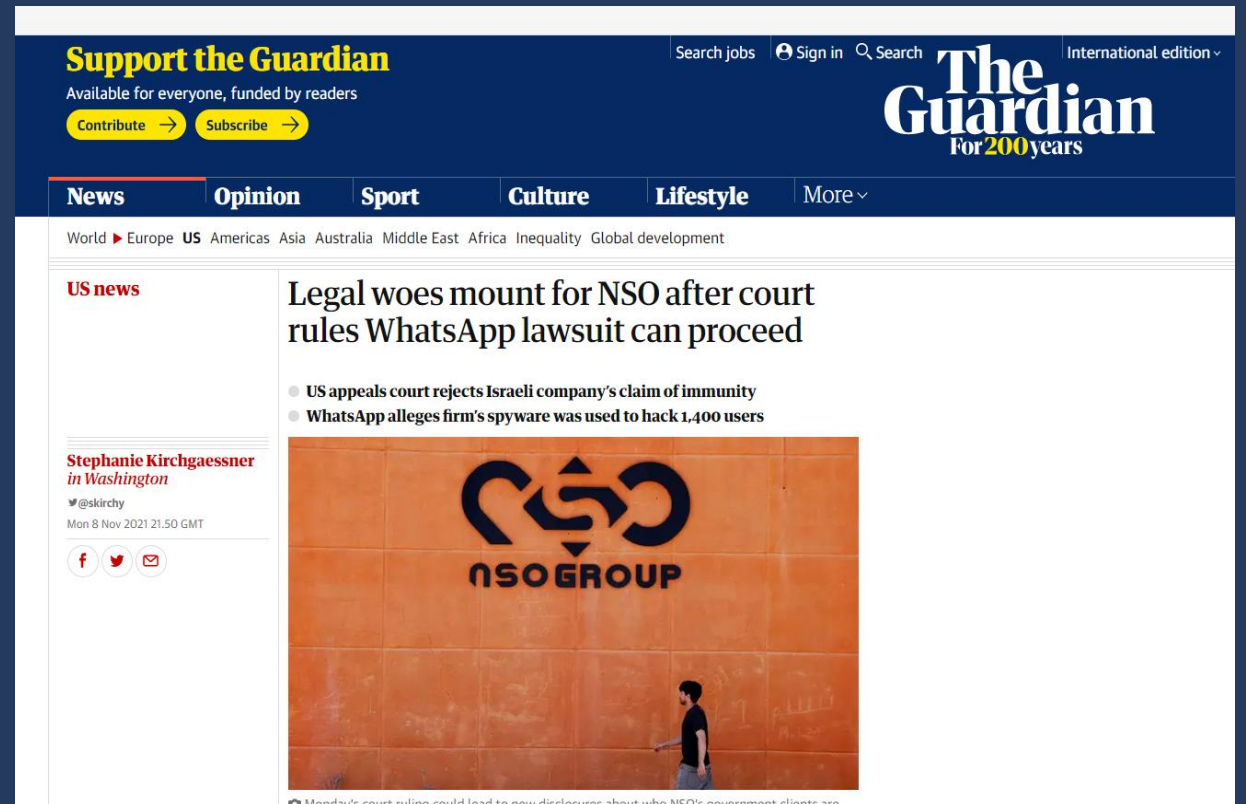


Who are the cyber criminals? Views from the private sector

Aisling Kelly,
Senior Counsel,
International Law Enforcement & National Security

Who are the new kids on the block?

- Large growth of nation state attacks against governments around the world
- Cyber criminals threatening national security
- Disinformation as a criminal offence – political campaigns, election integrity
- Private Sector Offensive Actors (PSOAs) -
What's App v NSO Group Technologies
Hacking as a service package – state developed, sold to private entities



The screenshot shows the top of The Guardian website. At the top left, it says "Support the Guardian" with a subtext "Available for everyone, funded by readers" and buttons for "Contribute" and "Subscribe". To the right, there are links for "Search jobs", "Sign in", and a search bar. The main logo "The Guardian" is prominently displayed with "For 200 years" underneath. Below the logo is a navigation bar with categories: "News", "Opinion", "Sport", "Culture", "Lifestyle", and "More". Underneath the navigation bar, there are regional links: "World", "Europe", "US", "Americas", "Asia", "Australia", "Middle East", "Africa", "Inequality", and "Global development".

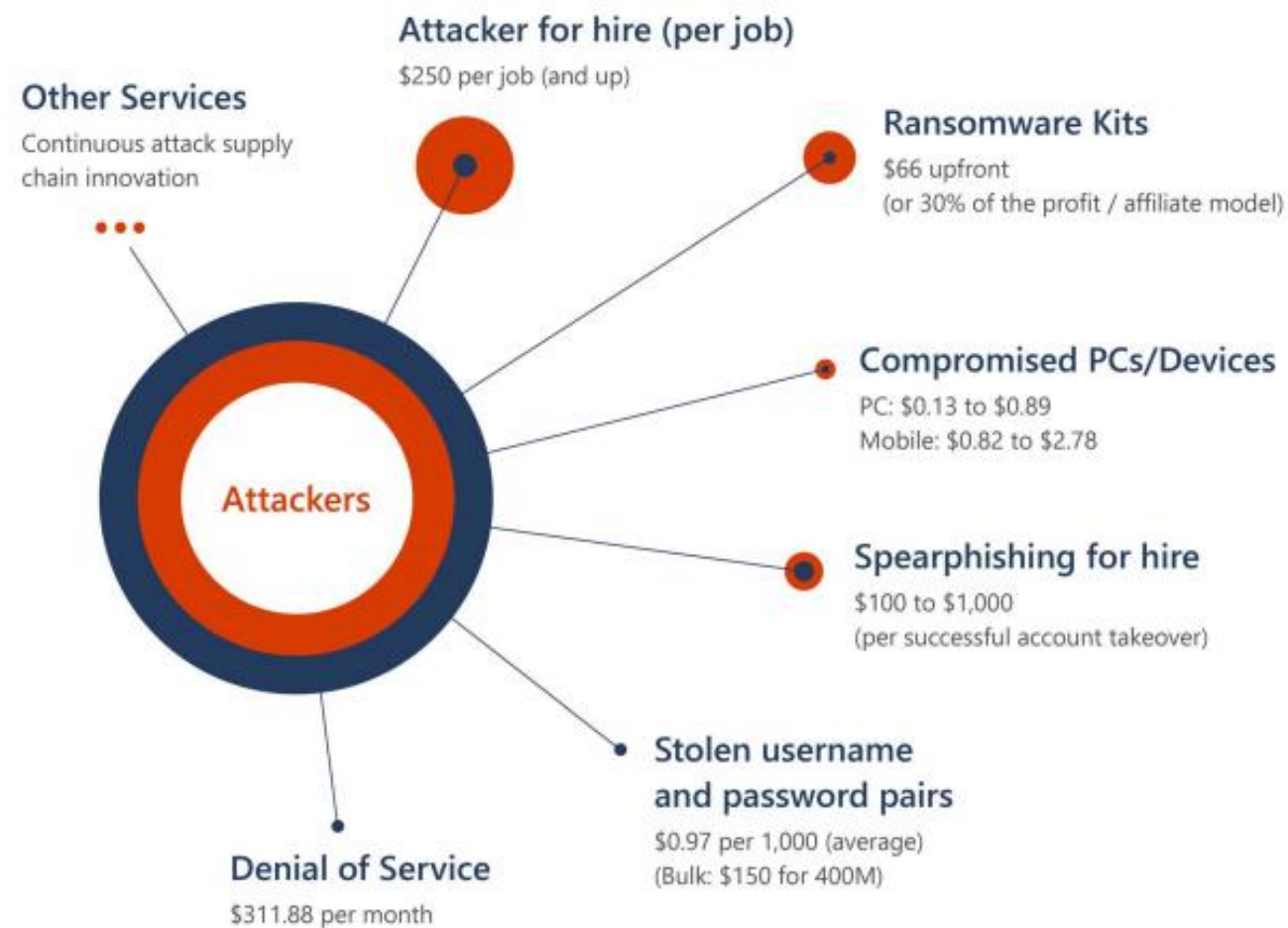
The main article is titled "Legal woes mount for NSO after court rules WhatsApp lawsuit can proceed". It is categorized under "US news". The author is "Stephanie Kirchgaessner in Washington" with a Twitter handle "@skirchy" and a timestamp of "Mon 8 Nov 2021 21:50 GMT". There are social media sharing icons for Facebook, Twitter, and Email. The article features a large image of the NSO Group logo on a wall, with a person walking in the foreground. Below the image, a caption reads: "Monday's court ruling could lead to new disclosures about who NSO's government clients are".

Cyber criminals offer a service now

Franchising the crime

- Your identity is a commodity.
- If your account credentials are stolen there are services that enrich the information with additional details on your identity that includes name, company they work for, roles, seniority in company, and industry associated to the company. With this information you are more susceptible to attack.
- We see more sophisticated cybercrime kits in which not only are victim credentials sent to the phishers running a phishing campaign, but they are also likely going back to the kit's originating author or a sophisticated intermediary for future use.
- Spyware designed to steal credentials was the most common type of malware observed through email delivery and was detected three times as often as the next highest detection.

Average prices of cybercrime services for sale



Organizations now face an industrialized attacker economy with skill specialization and trading of illicit commodities. As seen in this snapshot of average prices, many commodities that can be purchased in the dark markets are very inexpensive, making attacks cheaper and easier to conduct (which also drives up attack volume).

Phish kits: enabling credential harvesting at scale



Phish kit creator writes code that allows phish kit to be configured by kit buyer to indicate collection account where phished credentials are sent. Also included in code is a hidden collection account that will also receive phished credentials.

Phish kits are sold on the dark web. Each kit buyer configures the kit to meet their phishing campaign needs, including their own collection account to receive phished credentials.



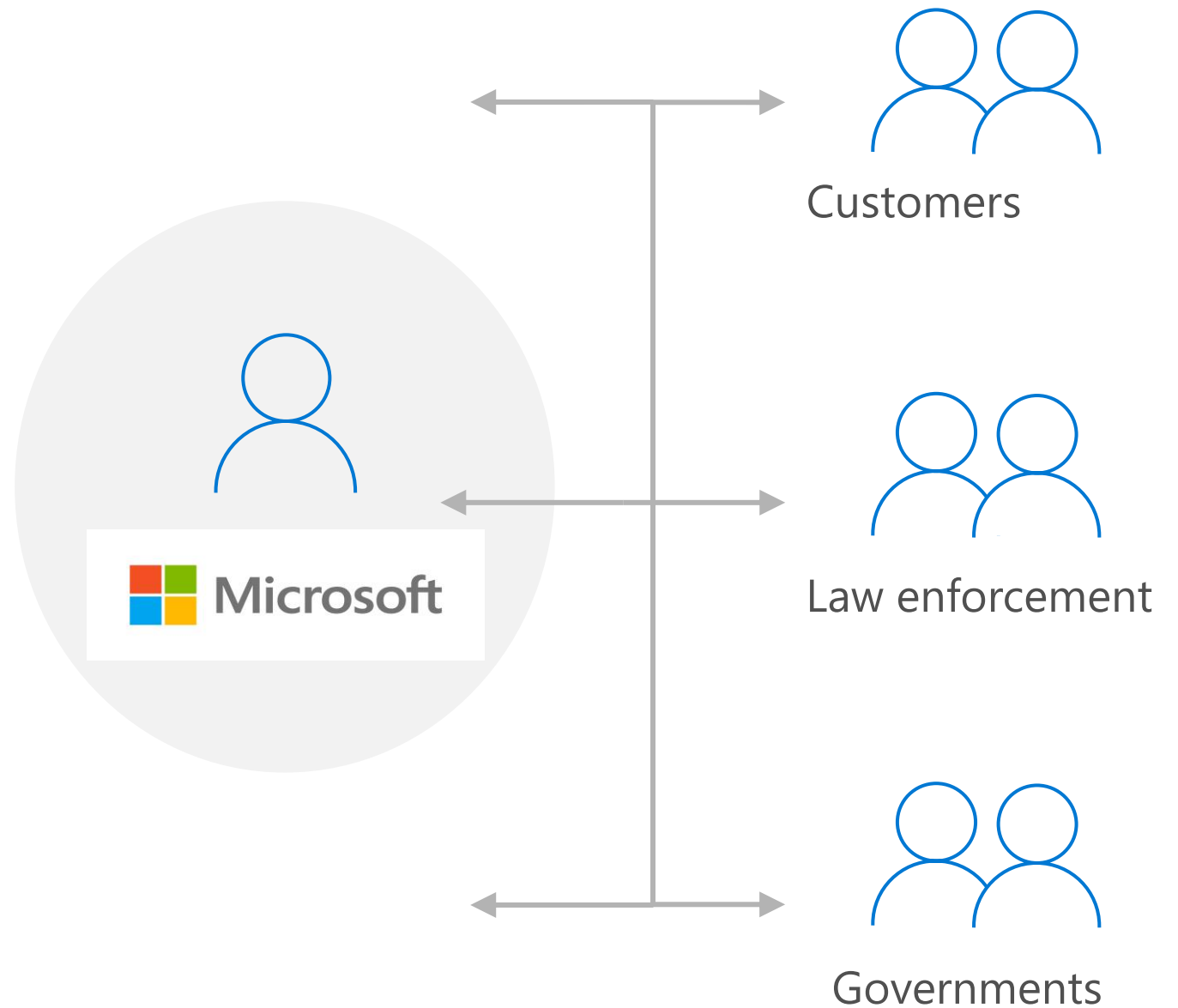
Who's phishing whom?
Kit creators have expertise and resources to carry out more sophisticated and targeted attacks at scale.

Each kit buyer deploys their own campaign. Phished credentials are delivered to both the kit buyer and the kit creator.

Lists of newly harvested credentials feed more targeted attacks at scale.

Criminal justice response to state supported actors

What does Microsoft do to track nation state attacks?



Sample Nation-State Actors

Iran
Cm
Houseblend
Tortoise Shell

CURIUM
US military and defense contractors, IT services, Middle Eastern governments

Iran
P
Charming Kitten

PHOSPHORUS
Diplomatic and nuclear policy communities, academics, and journalists

Iran
Rb
Fox Kitten
Parasite

RUBIDIUM
Israeli logistics companies, IT services, defense

China
Cr
ControlX

CHROMIUM
Energy, communications infrastructure, education, government agencies and services

China
Gd
APT40

GADOLINIUM
Maritime, healthcare, higher education, regional government organizations

China
Hf

HAFNIUM
Higher education, defense industrial base, think tanks, NGOs, law firms, medical research

Turkey
Si
Sea Turtle
UNC1326

SILICON
Telecommunication companies in the Middle East and the Balkans

Turkey

China
Mn
APT5
Keyhole Panda

MANGANESE
Communications infrastructure, defense industrial base, software/technology

China
Ni
APT15
Vixen Panda

NICKEL
Government agencies and services, diplomatic organizations

China
Zr
APT31

ZIRCONIUM
Government agencies and services, diplomatic organizations, economic organizations

China

North Korea

North Korea
Ce
Kimsuky

CERIUM
Think tanks, diplomatic officials, academics, defense and aerospace companies

North Korea
Os
Konni

OSMIUM
Diplomatic officials, think tanks

North Korea
Tl
Kimsuky
Velvet Chollima

THALLIUM
Think tanks, diplomatic officials, academics

North Korea
Zn
Lazarus
LabyrinthChollima

ZINC
Utilities, private companies, think tanks, security researchers

Vietnam

Vietnam
Bi
APT32
OceanLotus

BISMUTH
Human rights and civil organizations

Russia

Russia
Br
Energetic Bear

BROMINE
Government, energy, civil aviation, defense industrial base

Russia
No
UNC2452

NOBELIUM
Government, diplomatic and defense entities, IT software and services, telecommunication, think tanks, NGOs, defense contractors

Russia
Sr
APT28
Fancy Bear

STRONTIUM
Government, diplomatic and defense entities, think tanks, NGOs, higher education, defense contractors, IT software and services

Key:

Country of origin
Symbol
Industry
References

ACTIVITY GROUP
Commonly targeted industries

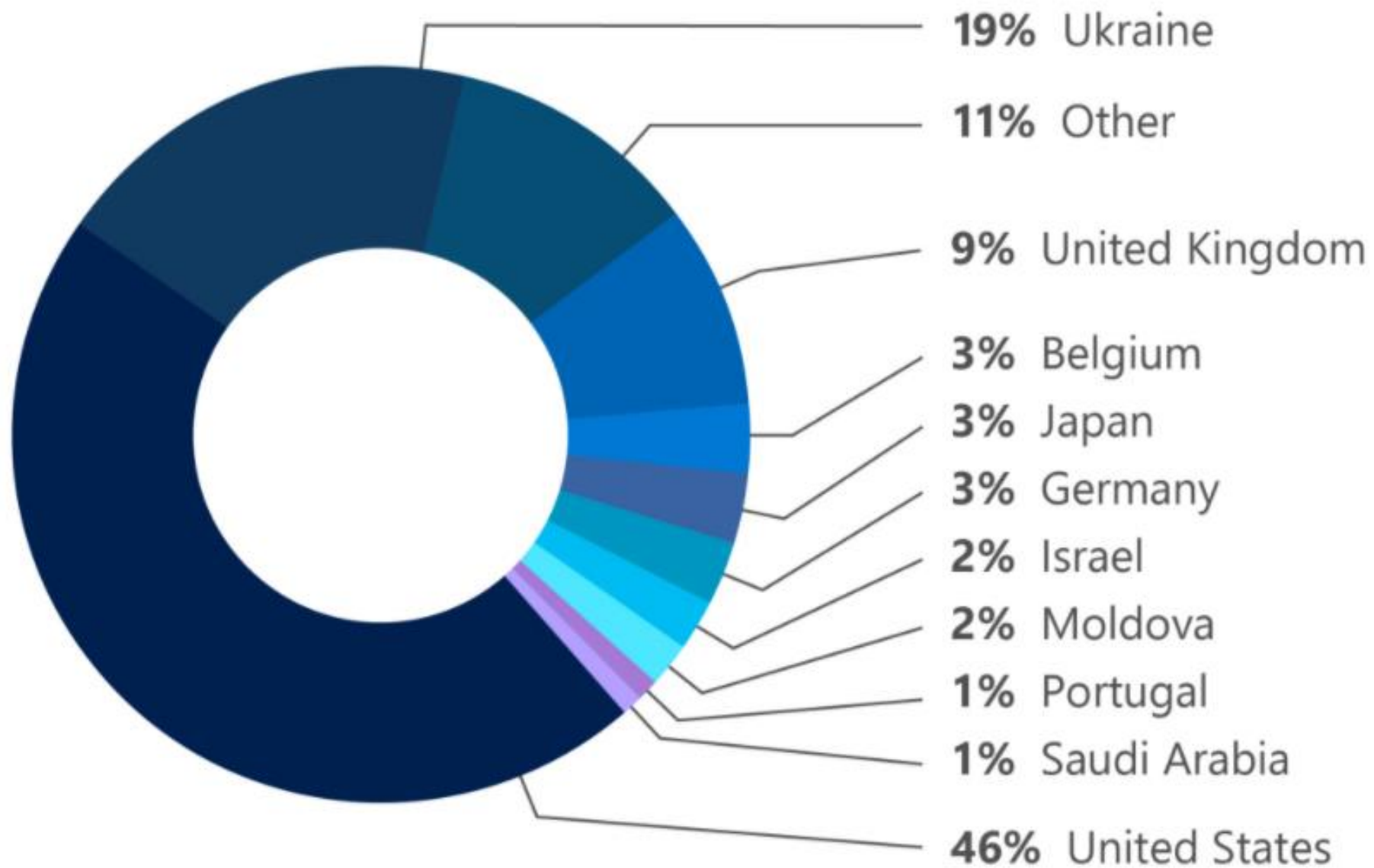


Figure 2: Countries most targeted (July 2020 to June 2021).

DECODING NOBELIUM

Inside The Most Advanced Nation-State Cyberattack In History

Nobelium

[Defending Against Nation-State Attacks | Microsoft Security](#)

- Publically shared information on 13th December 2020.
- Malicious activity which emanates from a particular country to further their national interests.
- Well-resourced and appear to be outside legal process
- IP theft, espionage, R & D
- Focuses on Governments, think tanks and infrastructure and enterprise – Solarwinds
- Software supply chain - malicious code
- 22,500 Nation State Notifications between 2018 – June 2021





Digital Crimes Unit

Civil cases against criminal and nation state actors

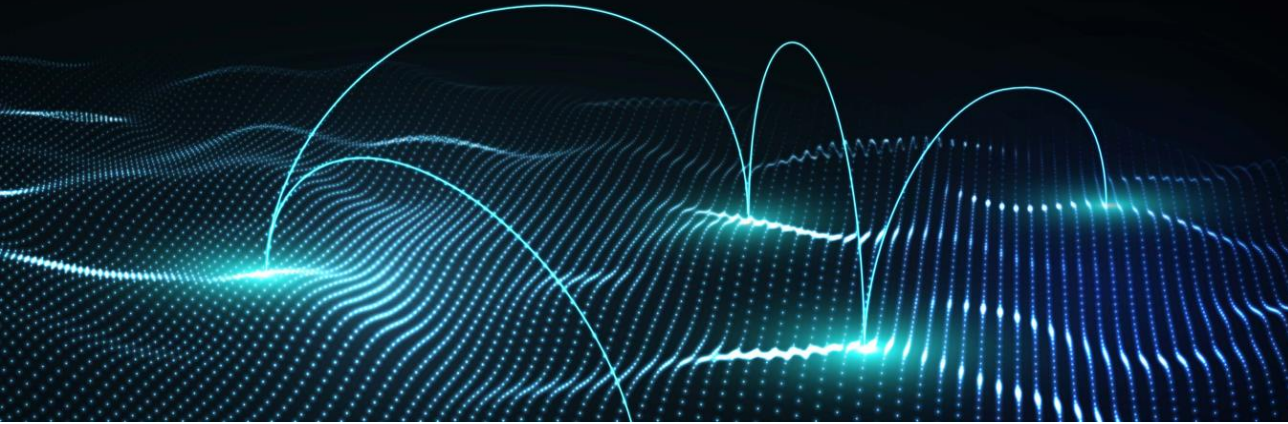
- Disruption through identification of malicious infrastructure.
- Referral of cases to law enforcement agencies worldwide.
- More governments are making cybercrime a priority.
- More governments are coming forward when they are attacked.



What is measured is
managed

Microsoft Digital Defense Report

OCTOBER 2021



[Microsoft Digital Defense Report – Microsoft Security](#)

Law Enforcement Requests Report

Explore law enforcement requests by country dating back to 2013.

[Download the current report >](#)

Law enforcement requests

Twice a year we publish the number of legal demands for customer data that we receive from law enforcement agencies around the world. While this report only covers law enforcement requests, Microsoft follows the same principles for responding to government requests for all customer data.

[Law Enforcement Request Report | Microsoft CSR](#)

Convergence of criminal and national security threats

- Difficult to distinguish between criminal and national security investigations because so many cases are within the scope of authority for both law enforcement and security agencies which requires close coordination between the two.
- We have seen this at Microsoft as our teams focused on nation-state threats and those focused on cybercrime increasingly must collaborate on common threats.
- Ransomware is now dealt with by the Digital Security Team, the Microsoft Threat Intelligence Centre and Digital Crimes Unit.
- In US government circles, the national security division of the Department of Justice taking on an increasingly important role in fighting cybercrime over the past ten years with the creation of the [National Security Cyber Specialists program](#).



Thank You

Aisling Kelly, Senior Counsel, Microsoft