OPERATION

ENDGAME

COVERAGE BY TIL

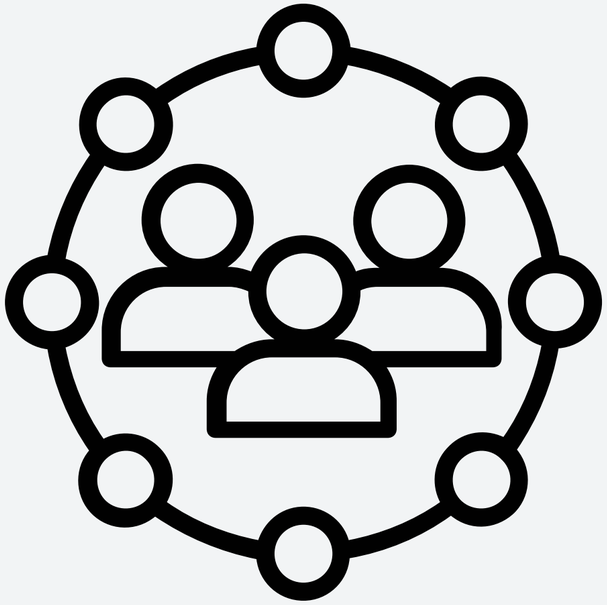
OPERATION ENDGAME

THE RECENT EUROPOL-LED INITIATIVE, OPERATION ENDGAME, MARKS THE LARGEST EVER OFFENSIVE AGAINST BOTNETS. IT DISMANTLED AN EXTENSIVE DROPPER MALWARE NETWORK BETWEEN MAY 27-29, 2024. LET'S DELVE INTO THE DETAILS.

OPERATION ENDGAME UNFOLDS

OPERATION ENDGAME, COORDINATED FROM EUROPOL'S HEADQUARTERS, TARGETED NOTORIOUS DROPPERS LIKE ICEDID, SYSTEMBC, PIKABOT, SMOKELOADER, BUMBLEBEE, AND TRICKBOT.

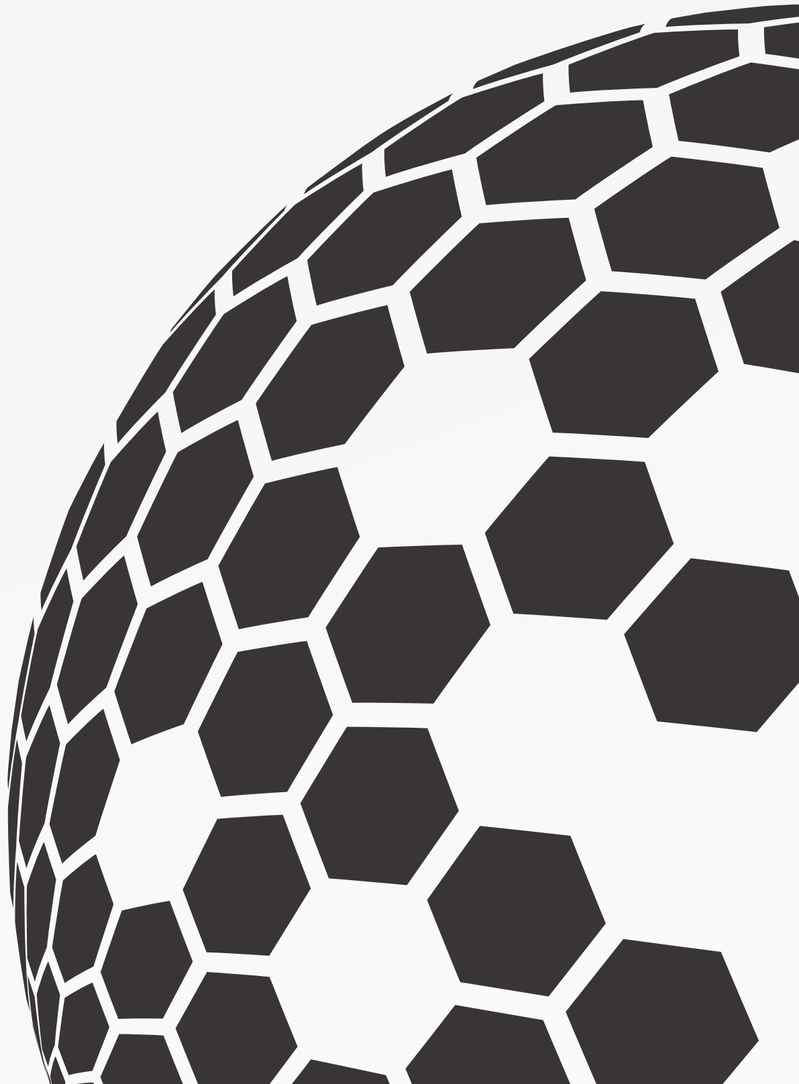
THIS COORDINATED EFFORT INVOLVED MULTIPLE COUNTRIES AND AGENCIES, AIMING TO DISRUPT THESE CYBERCRIMINAL SERVICES BY ARRESTING KEY PLAYERS, DISMANTLING CRIMINAL INFRASTRUCTURES, AND FREEZING ILLEGAL ASSETS.



SOURCE: EUROPOL

INTERNATIONAL COOPERATION

THE OPERATION WAS LED BY FRANCE, GERMANY, AND THE NETHERLANDS, WITH SUPPORT FROM EUROPOL AND EUROJUST. COUNTRIES LIKE DENMARK, THE UK, THE USA, ARMENIA, BULGARIA, LITHUANIA, PORTUGAL, ROMANIA, SWITZERLAND, AND UKRAINE PARTICIPATED. PRIVATE PARTNERS, INCLUDING BITDEFENDER AND PROOFPOINT, ALSO PLAYED CRUCIAL ROLES.



IMPACT AND RESULTS

THE OPERATION RESULTED IN SIGNIFICANT ACHIEVEMENTS:

- FOUR ARRESTS (ONE IN ARMENIA, THREE IN UKRAINE)
- SIXTEEN LOCATION SEARCHES (ARMENIA, NETHERLANDS, PORTUGAL, UKRAINE)
- OVER 100 SERVERS TAKEN DOWN OR DISRUPTED GLOBALLY
- OVER 2,000 DOMAINS SEIZED BY LAW ENFORCEMENT

ONE SUSPECT EARNED AT LEAST €69 MILLION IN CRYPTOCURRENCY BY RENTING OUT CRIMINAL INFRASTRUCTURE FOR RANSOMWARE DEPLOYMENT. THESE ASSETS ARE NOW UNDER CONSTANT SURVEILLANCE, WITH LEGAL PERMISSIONS FOR FUTURE SEIZURES.

SOURCE: EUROPOL

UNDERSTANDING DROPPERS

DROPPERS ARE MALWARE DESIGNED TO INSTALL OTHER MALICIOUS SOFTWARE. THEY OPERATE IN FOUR PHASES: INFILTRATION, EXECUTION, EVASION, AND PAYLOAD DELIVERY.

THESE STAGES ENABLE CYBERCRIMINALS TO BYPASS SECURITY MEASURES AND DEPLOY ADDITIONAL HARMFUL PROGRAMS LIKE RANSOMWARE AND SPYWARE.

SPECIFIC DROPPERS TARGETED

- **SYSTEMBC**: FACILITATES ANONYMOUS COMMUNICATION BETWEEN INFECTED SYSTEMS AND COMMAND-AND-CONTROL SERVERS.
- **BUMBLEBEE**: DELIVERED VIA PHISHING CAMPAIGNS, ENABLING FURTHER PAYLOADS ON COMPROMISED SYSTEMS.
- **SMOKELOADER**: USED PRIMARILY AS A DOWNLOADER FOR ADDITIONAL MALWARE.
- **ICEDID**: INITIALLY A BANKING TROJAN, NOW SERVES BROADER CYBERCRIME PURPOSES.
- **PIKABOT**: A TROJAN USED FOR INITIAL ACCESS, ENABLING RANSOMWARE, REMOTE CONTROL, AND DATA THEFT.

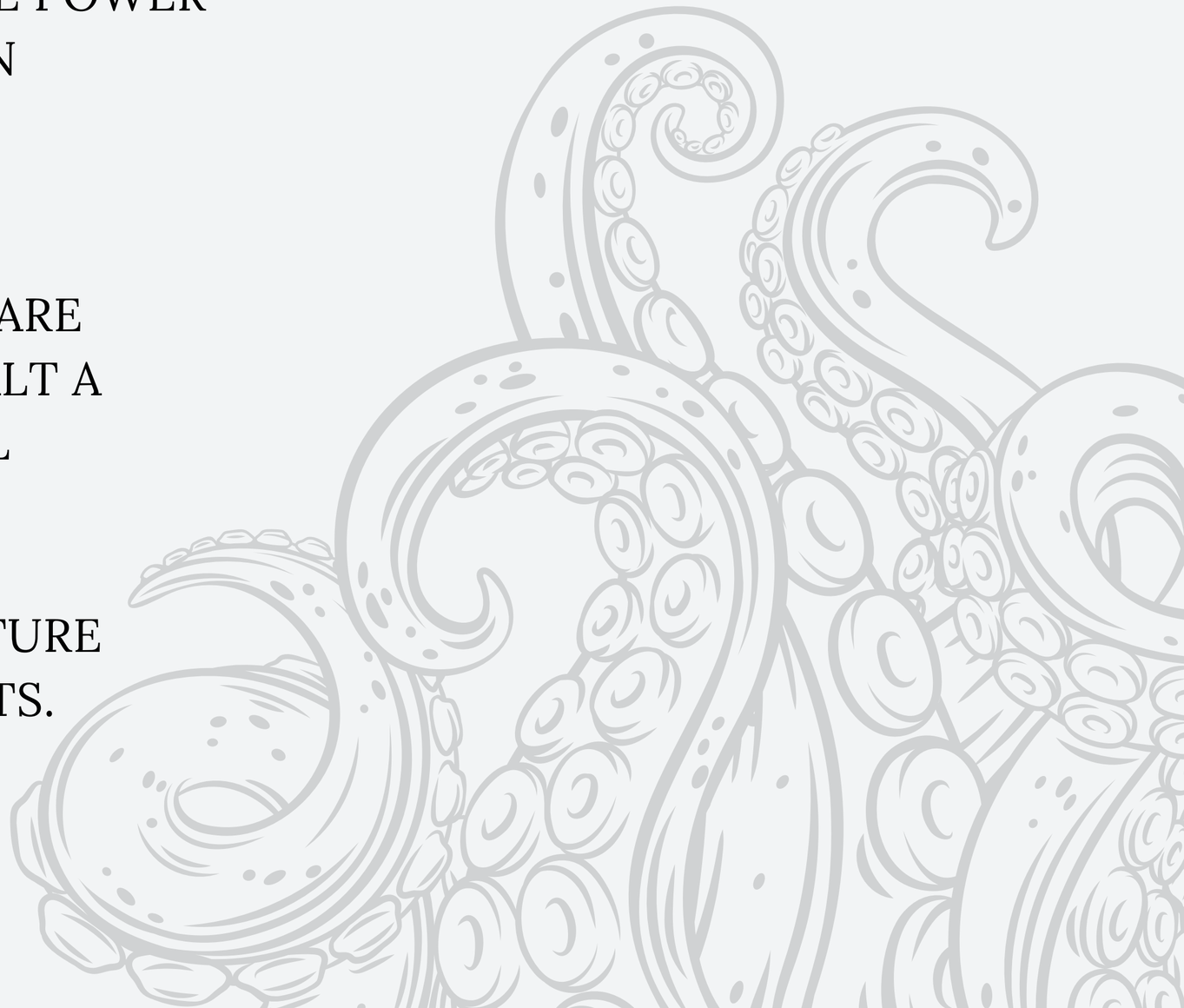
FUTURE ACTIONS

OPERATION ENDGAME DOESN'T END HERE. NEW ACTIONS WILL BE ANNOUNCED ON ITS DEDICATED WEBSITE. ADDITIONALLY, EIGHT FUGITIVES LINKED TO THESE ACTIVITIES, WANTED BY GERMANY, WILL BE ADDED TO EUROPE'S MOST WANTED LIST ON MAY 30, 2024.

OPERATION ENDGAME SHOWCASES THE POWER OF INTERNATIONAL COLLABORATION IN CYBERSECURITY.

BY TARGETING AND DISMANTLING KEY COMPONENTS OF THE DROPPER MALWARE ECOSYSTEM, THIS OPERATION HAS DEALT A SIGNIFICANT BLOW TO CYBERCRIMINAL ACTIVITIES.

IT SETS A STRONG PRECEDENT FOR FUTURE EFFORTS IN COMBATING CYBER THREATS.



QUICKLY MADE BY

REZA RAFATI

FROM

THREAT INTELLIGENCE LAB

THREATINTELLIGENCELAB.COM