

«LEGAL LIMITS OF PROACTIVE ACTIONS: COREFLOOD BOTNET EXAMPLE»

OGUZ KAAN PEHLİVAN

INDEPENDENT RESEARCHER

Operation Odeona

Basics

Court Decision & Operation

Results & Findings

Basics

- Oldest, in continuous operation, active from 2002
- Motive: DDoS, selling anonymity services, full-fledged bank fraud
- *2,336,542* computer; App. *1,853,005* in USA
- The full extent of the financial loss caused by the Coreflood Botnet is not known, due in part to the large number of infected computers and the quantity of stolen data.
- State and local gov. agencies (17);
- Police Dep. (1);
- Defense Contractor (2);
- Financial Ins. & Banks (5);
- Airport (3);
- College & University (30);
- Hospital (20);
- Private Company & Businesses (100+)

Court

Search and Seizure Warrant; Temporary Restraining Order

- Seize and replace command-and-control servers
- Collect the IP addresses
- Remote “exit,” or stop, command
- A temporary measure

Extention Order

- Continue to temporarily disable the malware
- Notify the ISPs, a form letter
- Instruct infected computers

Operation

- 5 C & C servers and 29 domain names were seized
- Remote “exit,” or stop, command
- How to “opt out
- 19,000 uninstall commands to computers owned by 24 victims.

Results

- Size of the Coreflood, more than 95%
- 3 tier action
- Victim notification
- Coordination with Internet service providers and antivirus vendors
- The operation of the substitute server and take down

Legal Findings

- Domestic, computers reasonably located in USA; inform others
- Consent, limited action (retrain, stop, notify, if accepted actively engage)
- Resilient dijital environment in respect of privacy
- Reasoning «*continue to running on the infected computers will cause a continuing and substention injury to owners and users of infected computers*»
- Financial stability as a public good

Thank You

Stay in Touch

Oguz Kaan Pehlivan

pehlivan.oguzkaan@gmail.com