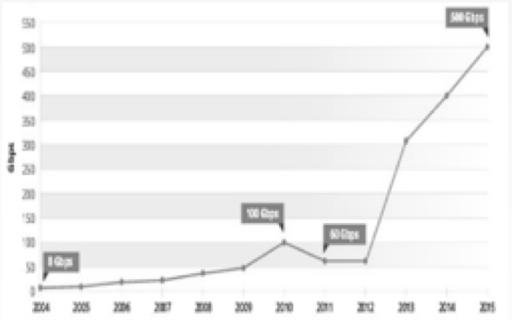
NSFOCUS

THE GANGS BEHIND DDOS ATTACKS

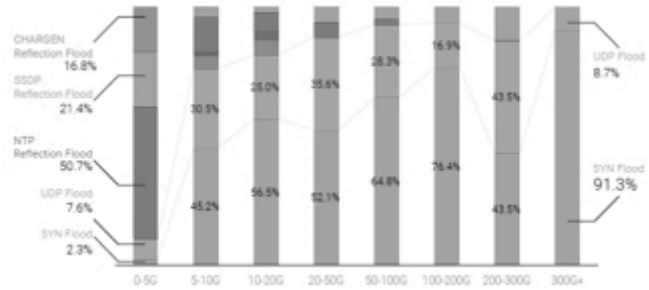
IP CHAIN-GANG BEHAVIOR

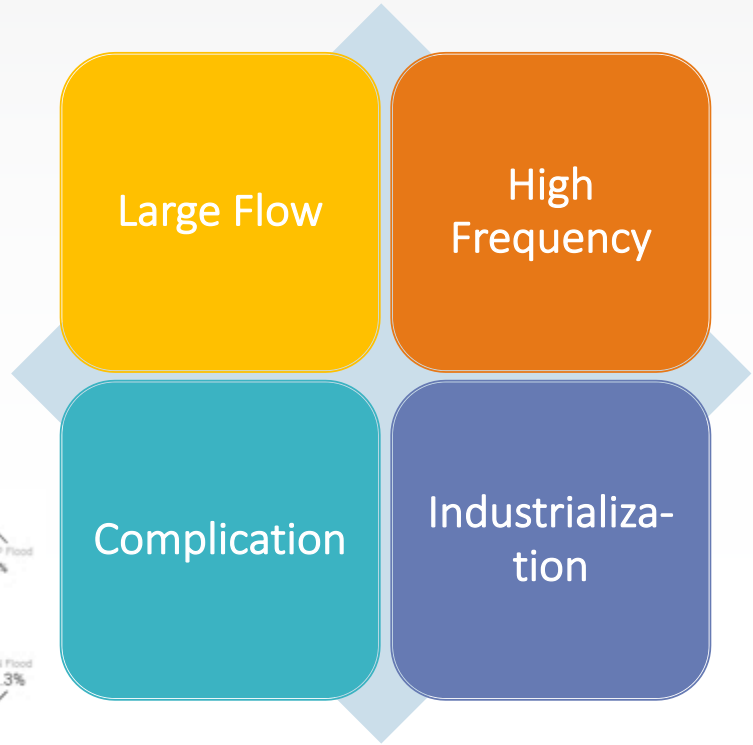
DDOS ATTACK THREAT LANDSCAPE

The peak flow is larger and larger, the max up to 755Gbps.



Large flow is mainly SYN Flood and UDP Flood, and small flow is complex.





DDoS attack happens at a frequency of 20+ times per hour.

Attack trading platform let attack easy and cheap.

CONFIDENTIAL

GLOBAL THREAT INTELLIGENCE SOURCES

NSFOCUS

- Actionable Threat Intelligence
- Real-Time Information Sharing
- Custom Threat Information

- Intelligence from all over the world
- Unique intel from China

NSFOCUS Security Labs

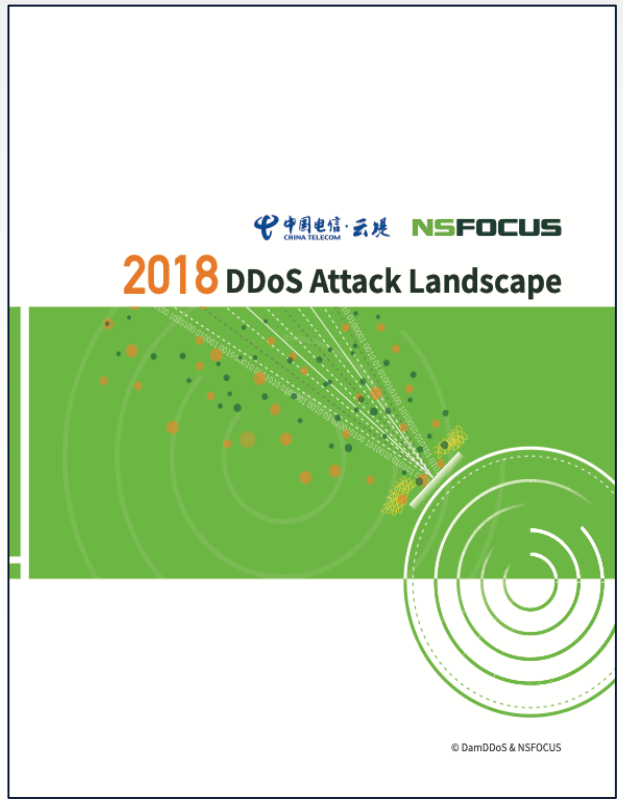
90+ threat researchers, malware experts

4000+ Active Crowd sharing

12,000 Network Sensors

400 Million Endpoints

THREAT INTELLIGENCE INSIGHTS



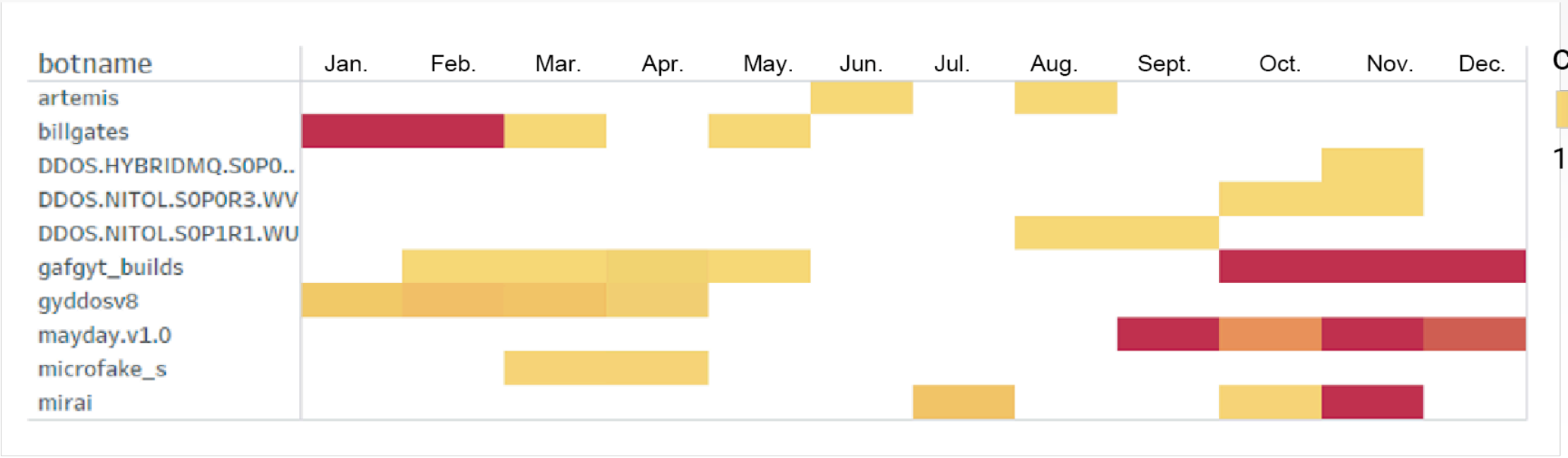
- Based on continuous botnet monitoring
- >450K attack targets

- 25% of attacking sources have been ‘linked’ to repeated attacks

CONFIDENTIAL

BOTNET TREND

Monthly Distribution of Instructions



- Most active between Jan – Mar, and Sep - Dec
- Very quiet Jun – Jul

Source: NSFOCUS: 2017 Botnet Trend Report

DDoS trend

- The most active botnet family types were related to ransomware, cryptomining, and DDoS.
- There were a shift for DDoS botnet families
  - Use of multi-vector attacks
  - Flood were the dominant DDoS attack types.
  - DDoS attack instructions issued to carry out nearly all kinds of attacks
    - TCP flood, SYN flood, ACK flood, UDP flood, DNS flood, HTTP flood, and ICMP flood
  - Modularization

CONFIDENTIAL

BOTNET TREND

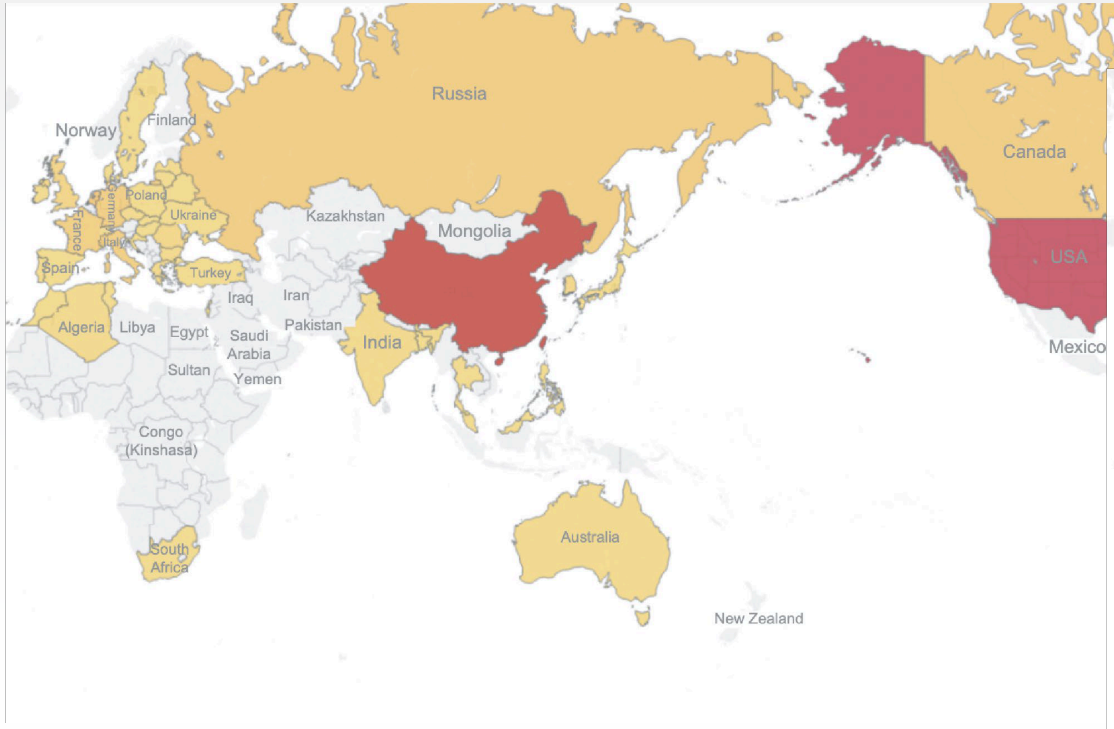
NSFOCUS

Botnets take low and slow approach through Reconnaissance and Testing

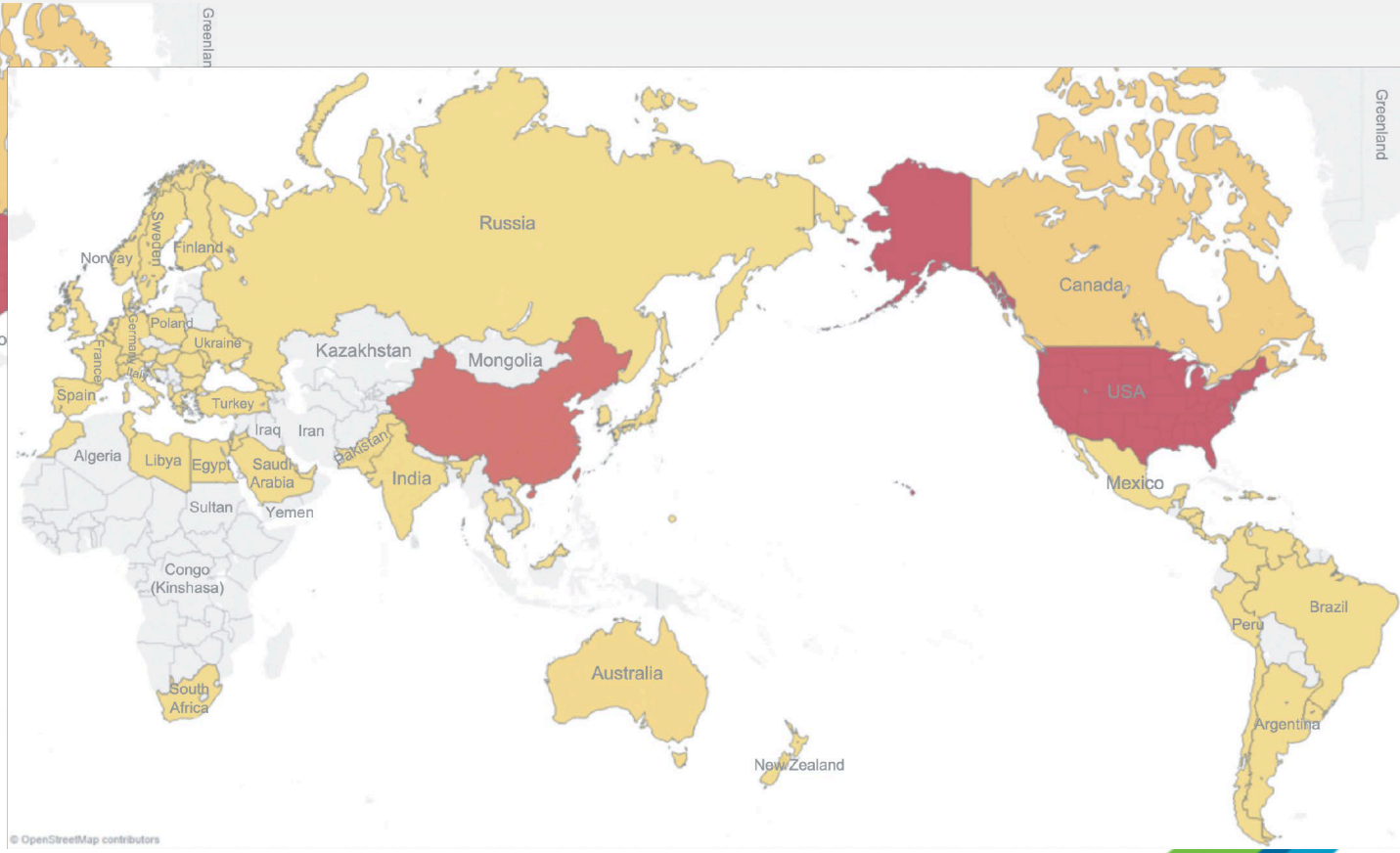
- Botnet controllers were more cautious by repeatedly conducting reconnaissance and testing activities before issuing attack instructions
- Botnet kill chain consists of two phases: pre-intrusion and post-intrusion
- Controllers were careful about delivering malicious programs prior to intrusion
- Often try to reduce detection by forging source IPs and domains, using multilingual texts, and adding misleading or meaningless information
- In contrast, the delivered malicious programs behaved more recklessly
  - They often used simple communication formats and exposed attack sources
  - Made detection of malicious behavior easier during the post-intrusion phase

Source: NSFOCUS: 2017 Botnet Trend Report

BOTNET TREND



C&C Servers

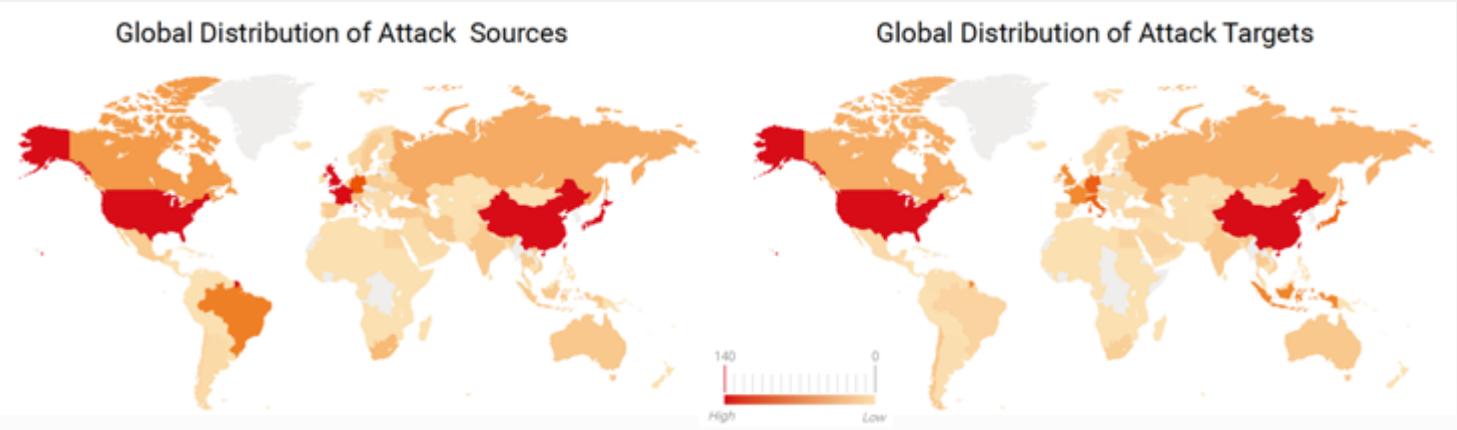


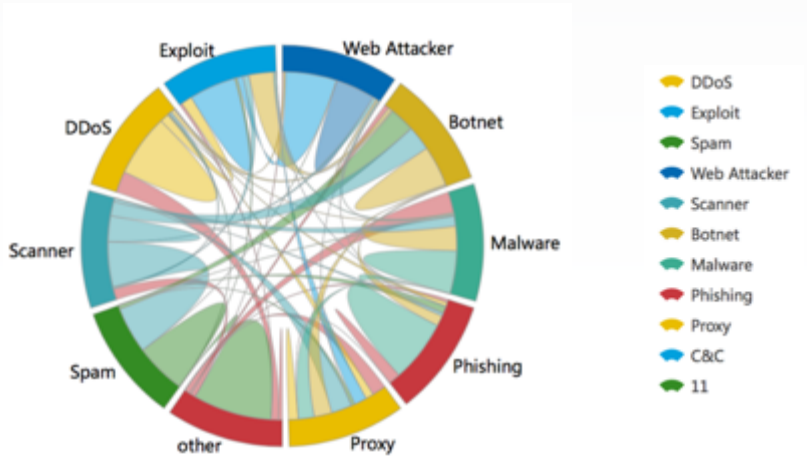
Botnet targets

Source: NSFOCUS: 2017 Botnet Trend Report

CONFIDENTIAL

INSIGHTS INTO THREATS





- Attackers follow economic activities
- 19.3% of attack sources > one type of attacks
- 20% of proxies used for malicious purpose
- 25% of attack sources responsible for 40% of attacks

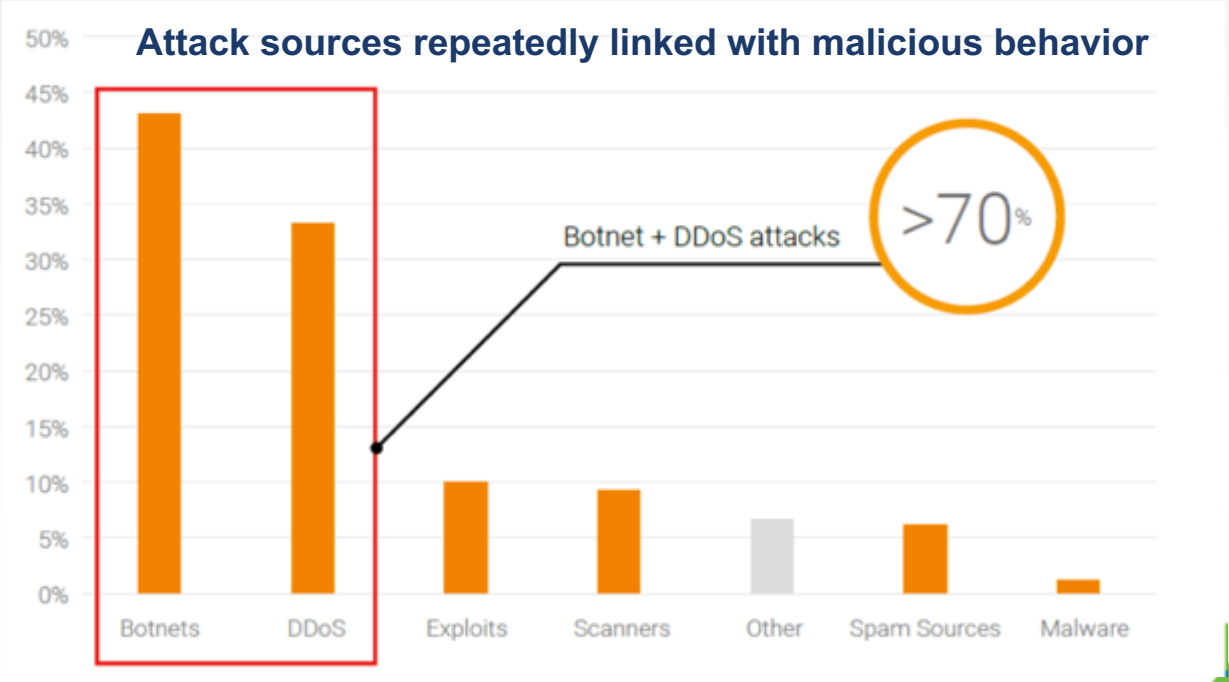
Source: NSFOCUS: 2018 H1 Cybersecurity Insights

REPEATED OFFENDERS

NSFOCUS

Attack sources repeatedly linked with malicious behavior

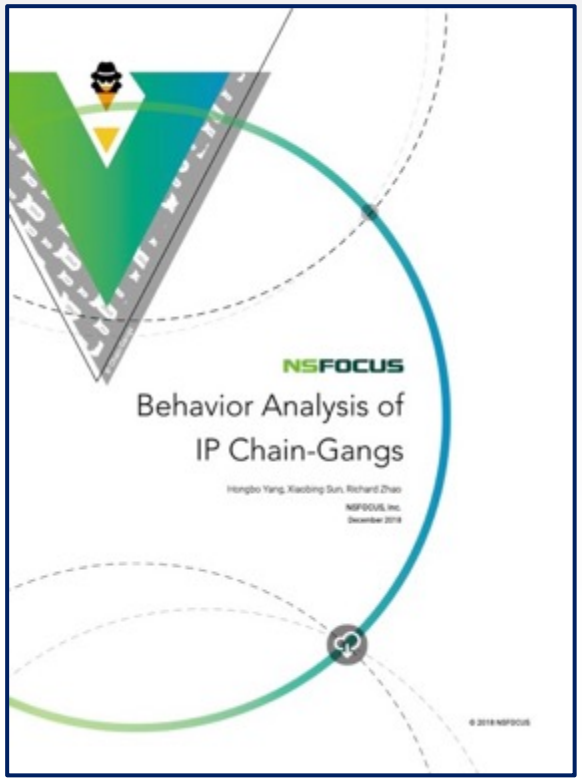
Attack sources repeatedly linked with malicious behavior



CONFIDENTIAL

BEHAVIOR ANALYSIS OF IP CHAIN-GANGS

- Based on NSFOCUS Threat Intelligence (NTI) data
  - Cloud DDoS Service
  - Anti-DDoS crowd sourcing
- 1st in a series about IP Chain-Gangs
  - About IP Chain-Gang behavior
  - About methodology



CONFIDENTIAL

DEFINITION OF IP CHAIN-GANG

- In “NSFOCUS 2018 H1 Cybersecurity Insights” report
  - ‘Recidivists are responsible for 40% of the attacks’
- Botnets
  - A group of bots controlled by the same C&C server
- IP Chain-Gang
  - Controlled by a single threat actor, or a group of related threat actors
  - Exhibit similar behavior
- Bots in a botnet can belong to more than one IP Chain-Gang
- An IP Chain-Gang can consists of bots from more than one botnet

CONFIDENTIAL

DEFINITION OF IP CHAIN-GANG

- Using DDoS data from 2017 to present
- How to identify IP Chain-Gangs
  - Attackers participate in one collaborated attack
    - Individual attacks target the same target at roughly same time
  - If 2 groups overlap, or behaviors are significantly alike, merge into a bigger group
  - Extract core members of the group by purging “occasional attackers”
- A sophisticated machine learning algorithm is used to determine the threshold of the ‘significance’

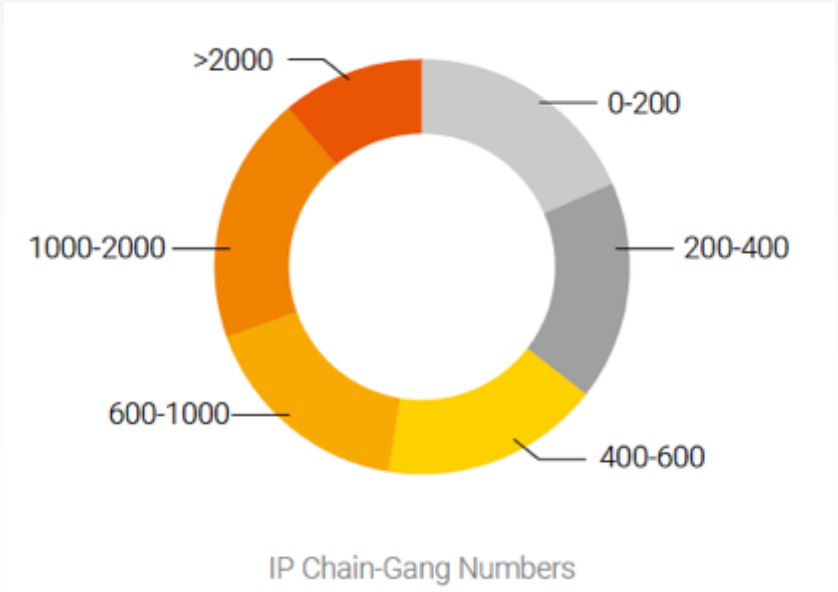
CONFIDENTIAL

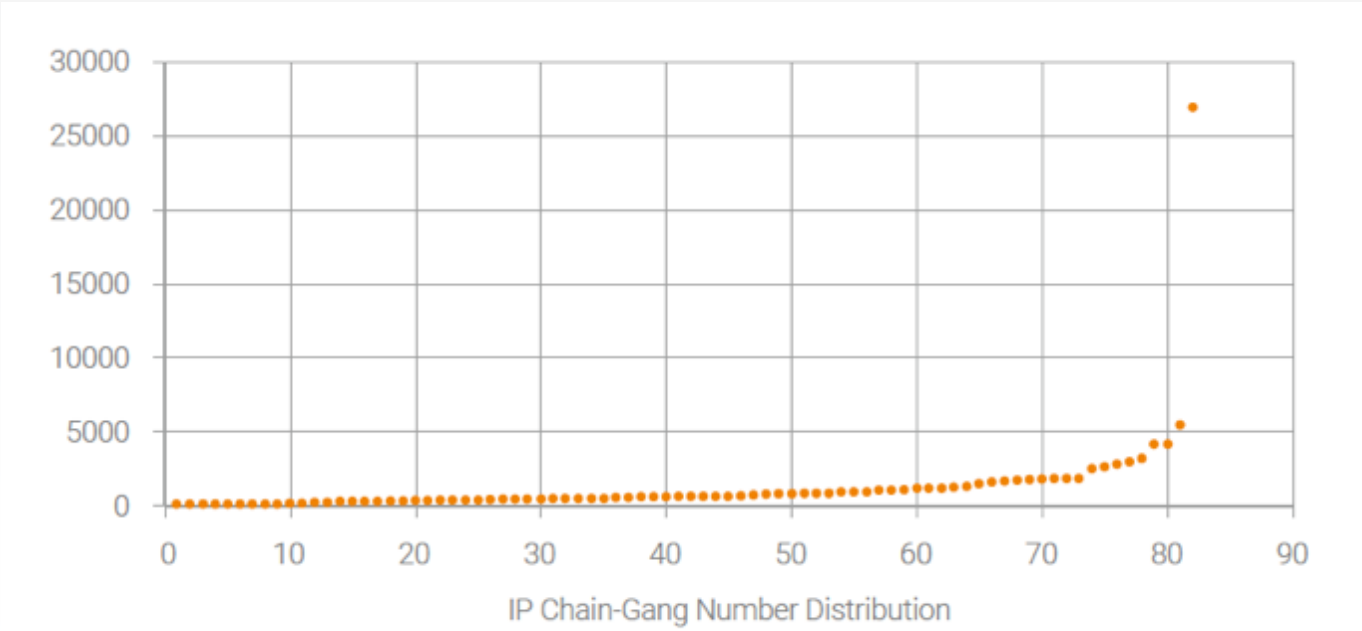
IDENTIFYING IP CHAIN-GANG

- Over 80 active IP Chain-Gangs have been identified
- Restrictive parameters in our algorithm
  - All members in these gangs are serious recidivists
  - Each of them has performed multiple attacks over the period
- Total number of these gang members is only 2% of all attackers, but responsible for 20% of all attacks

CONFIDENTIAL

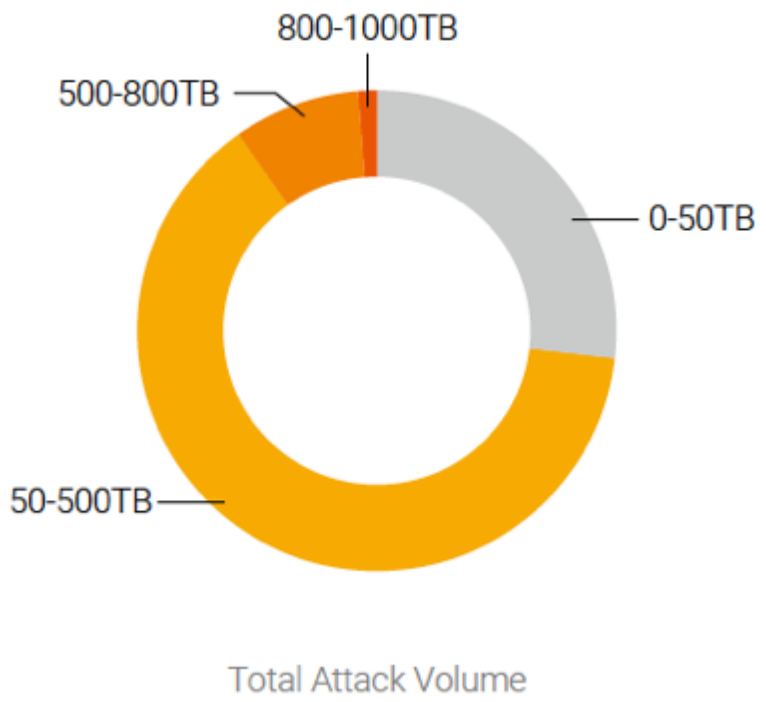
IP CHAIN-GANG SIZE

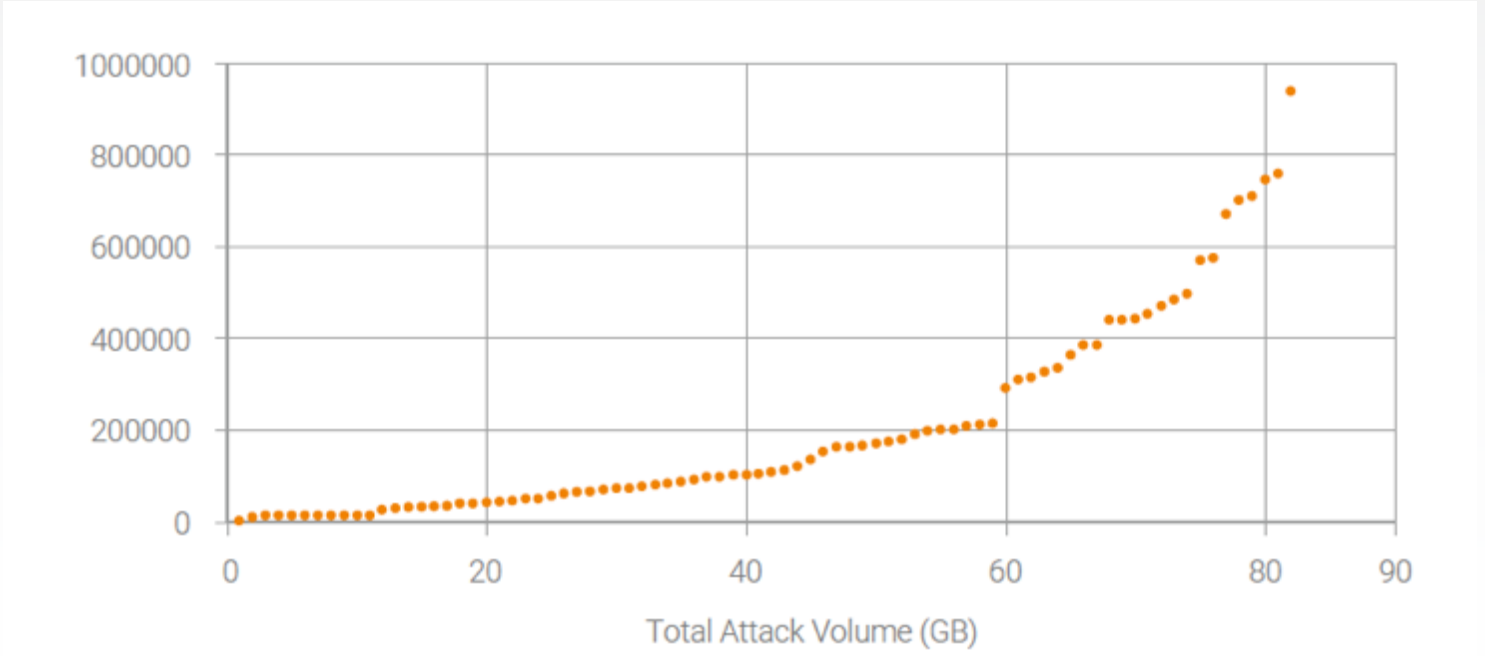




CONFIDENTIAL

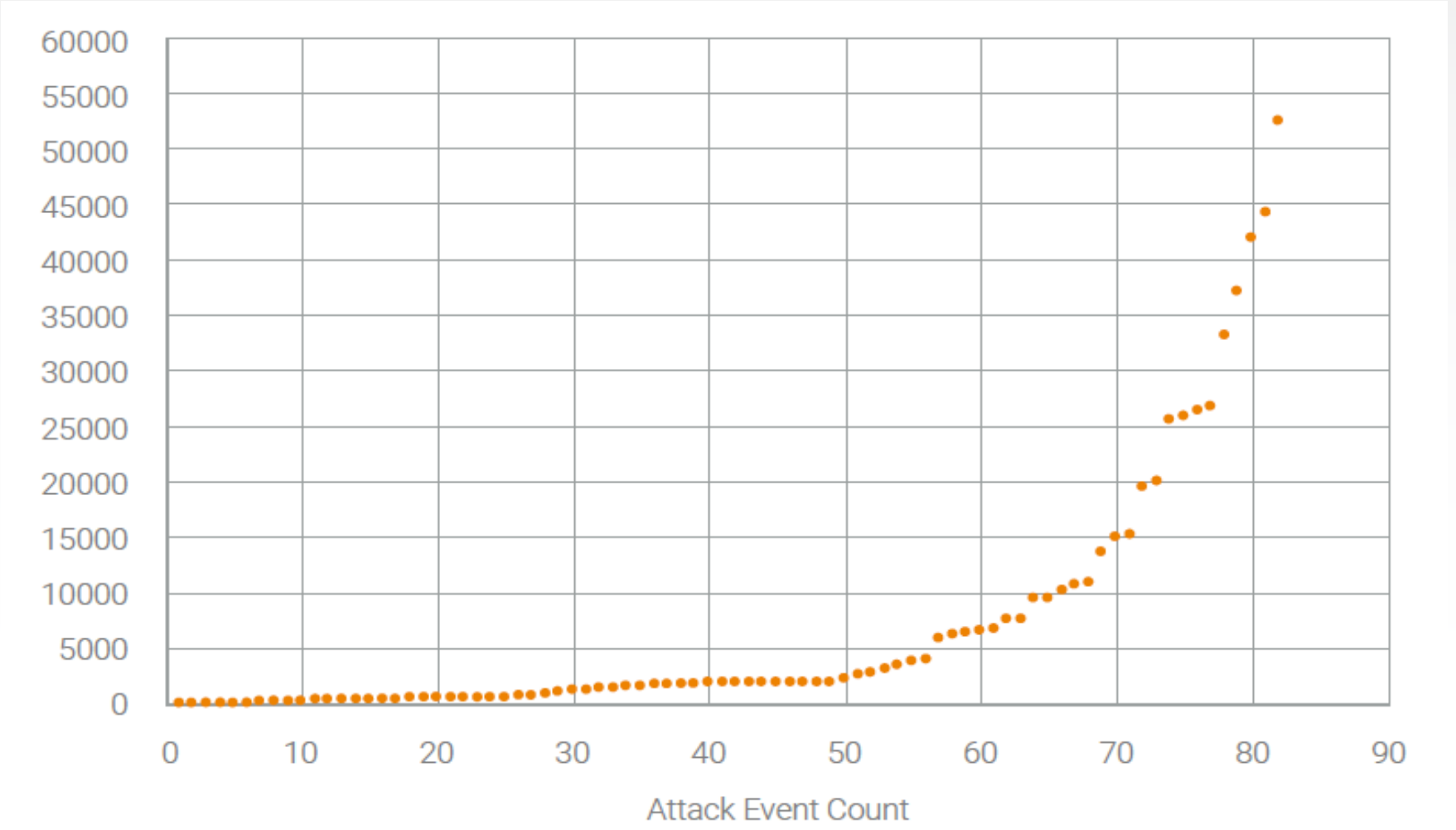
IP CHAIN-GANG TOTAL ATTACK VOLUMES





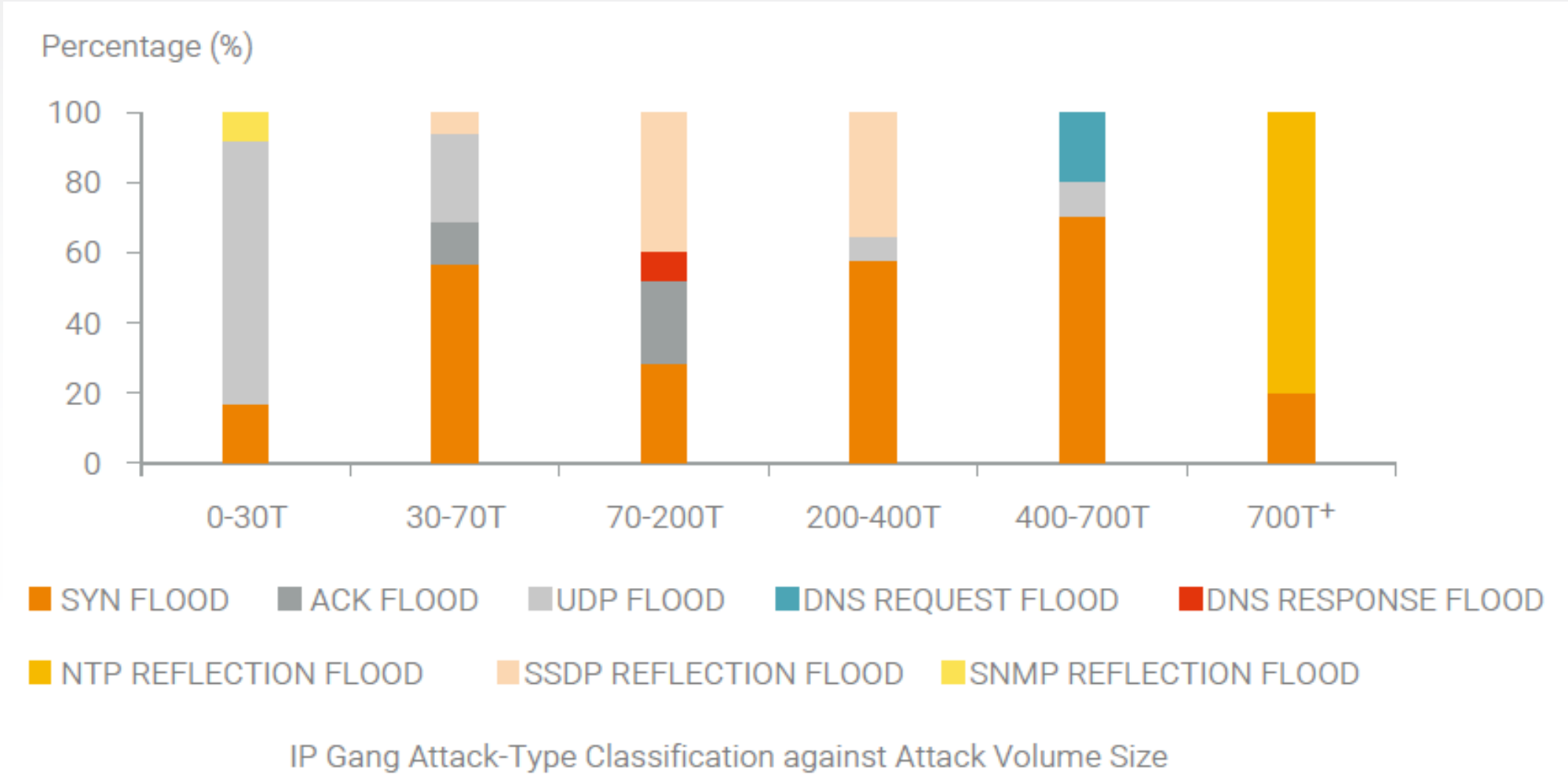
CONFIDENTIAL

IP CHAIN-GANG TOTAL ATTACK COUNT



CONFIDENTIAL

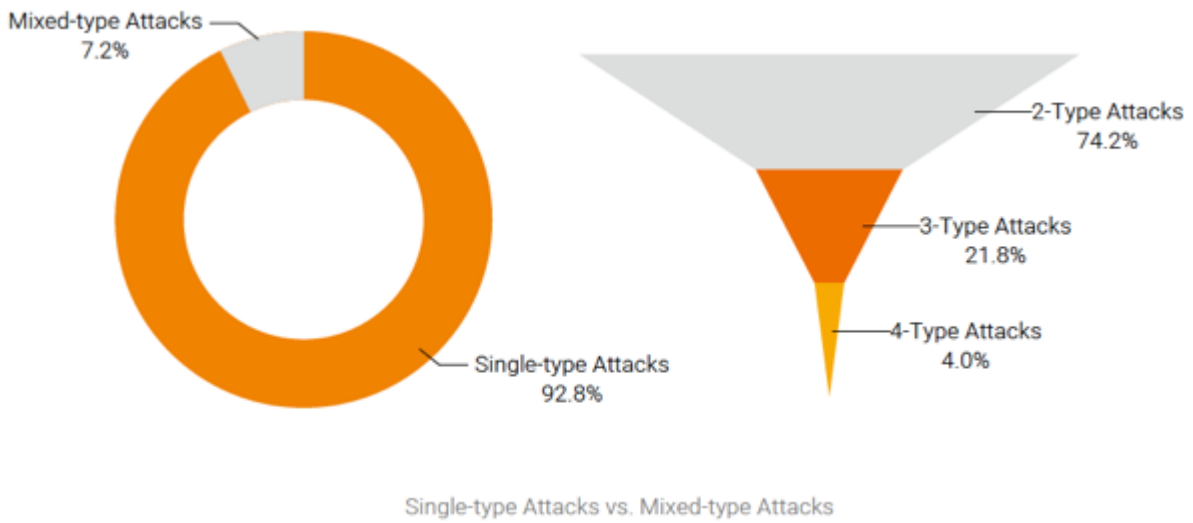
IP CHAIN-GANG ATTACK TYPES



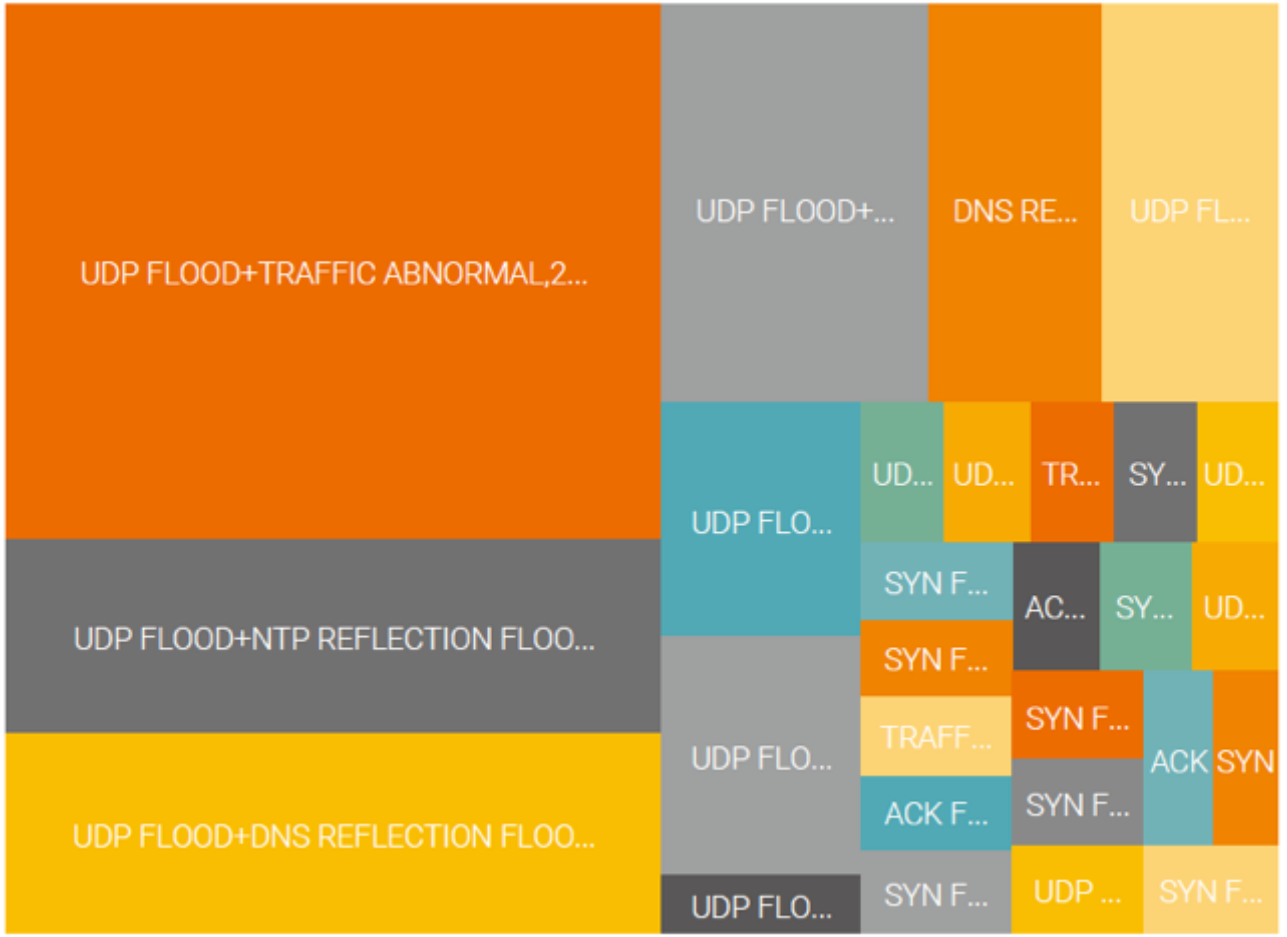
IP Gang Attack-Type Classification against Attack Volume Size

CONFIDENTIAL

IP CHAIN-GANG ATTACK TYPES



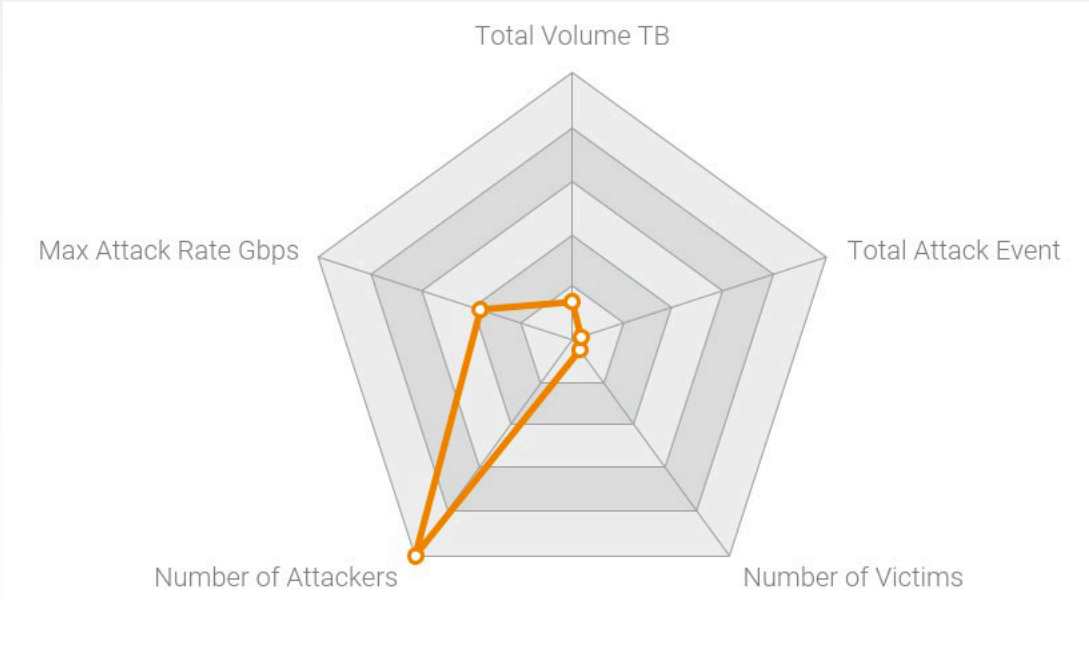
Single-type Attacks vs. Mixed-type Attacks



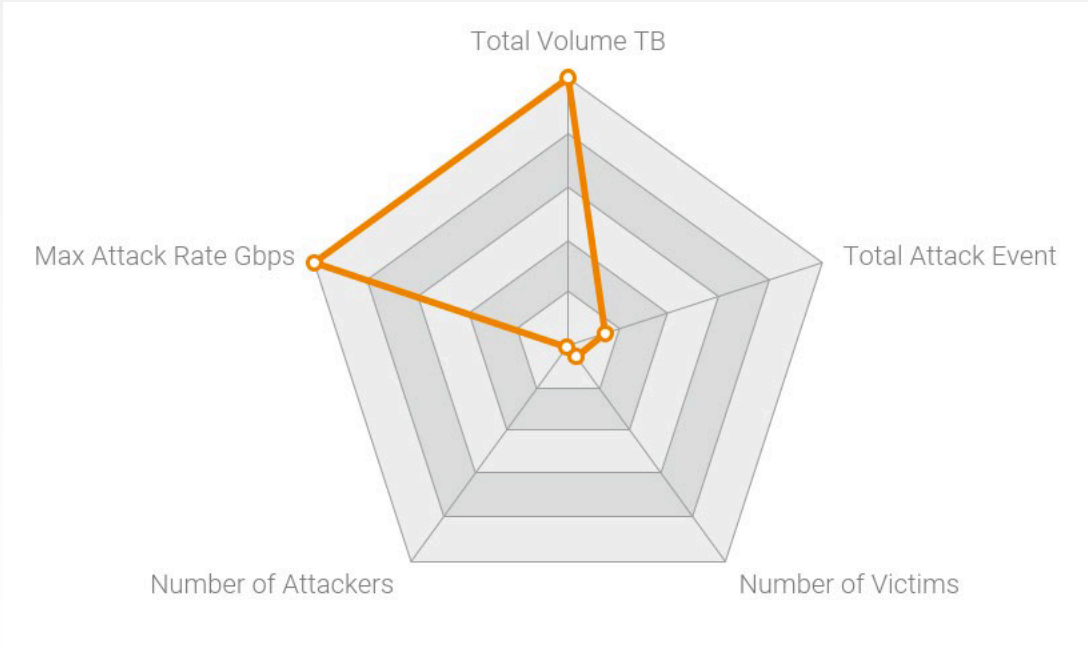
Common Combinations for Mixed-type Attacks

CONFIDENTIAL

GANG PROFILING



MOST ACTIVE



MOST DESTRUCTIVE

CONFIDENTIAL

FUTURE RESEARCH

NSFOCUS

- A basic model for analyzing cyber-attack activities based on IP Chain-Gang behavior
  - Show how a group of attackers controlled by a threat actor can operate and attack in a controlled manner
  - A profiling model to help describe and compare these gangs
- Plan to track IP Chain-Gangs evolving history and study the inner-connections amongst members
- Goals
  - Predict attacks from IP Chain-Gang
  - Build playbooks to develop effective defenses against them

CONFIDENTIAL

More Information

NSFOCUS

- www.nsfocusglobal.com
- Info@nsfocusglobal.com

https://www.linkedin.com/company/nsfocus

https://www.facebook.com/nsfocus/

https://twitter.com/NSFOCUS_Intl