

Botnets

Basics and Ways To Track Them



Botnets

Basics and Ways To Track Them

nnnn
dGGGGMMb
@p~qp~~qMb
M|@| |@) M|
@, ----.JM| -'
JS^ _/_/ qKL
dZP qKRb
dZP qKKb
fZP SMMb
HZM MMMM
FqM MMMM
--| " : | \dS"qML
| | ' ' \Zq
-) \ . ---- , |
_---)MMMMMM|
--' hjm



twitter

@botlabsDev

Botnet ?

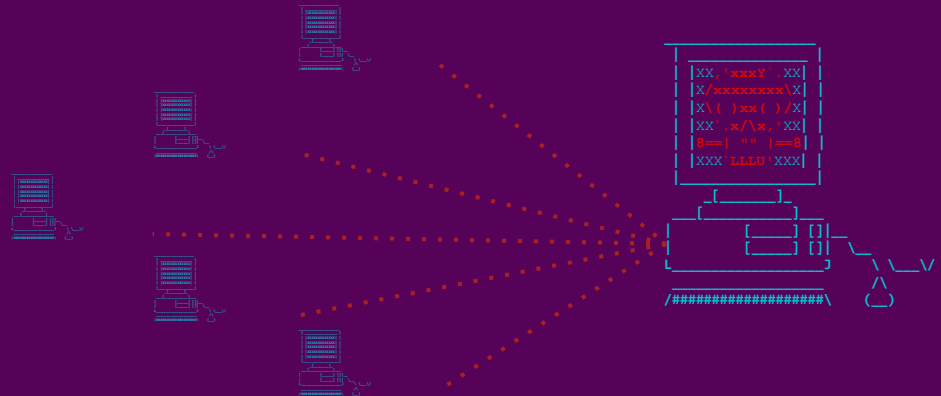
>> A Botnet represents a network of hijacked computer systems
remote controlled without the consent of their owners. <<

Which devices can become part of a botnet?

- Personal Computers
- Mobile Devices
- Internet of Things (IoT)
- Medical / Industrial Devices

How do the systems get infected ?

- Malicious Apps / Programs
- Credential brute force attacks
- Misconfigurations
- Software vulnerabilities



>> Each device connected to the internet represents
a potential target and can be part of a botnet. <<

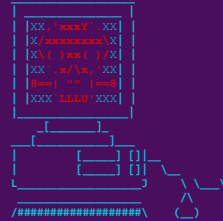
-- Confucius



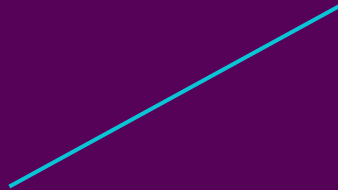
Elements Of A Botnet



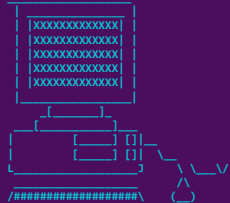
Botmaster / Botherder



Command and Control Server (C&C)

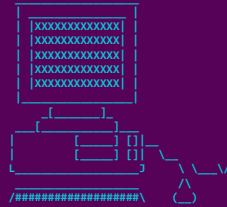


Control Channel



Bot / Zombie / Drone

BOT ->



har.dco.ded.lp

HardcodedDomain.pw



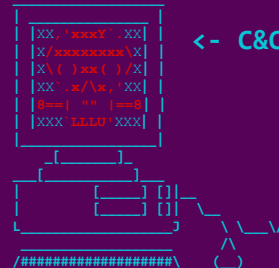
BOT ->



har.dco.ded.lp

HardcodedDomain.pw

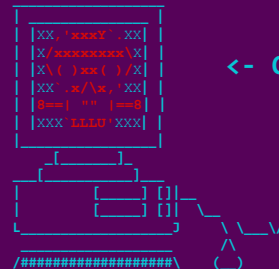
<- C&C



BOT ->



<- C&C



```
zeeeeee-  
z$$$$$"  
d$$$$$"  
d$$$$$P  
d$$$$$P  
$$$$$"  
.$$$$$"  
.$$$$$"  
4$$$$$$$$$$$$$"  
z$$$$$$$$$$$$$"  
*****3$$$$$"  
z$$$$$P  
d$$$$$"  
.$$$$$"  
.$$$$$"  
z$$$$$P  
d$$$$$$$$$$$$$"  
*****$$$$$"  
.$$$"  
.$$$"  
4$P"  
z$"  
zP  
z"  
/  Gilo94'  
^
```

Domain Generation Algorithm (DGA)



Workflow:

- Calculation of domains for specific points in time
- A DGA can create 1 domain per Month or 1000 domains per hour

Goal:

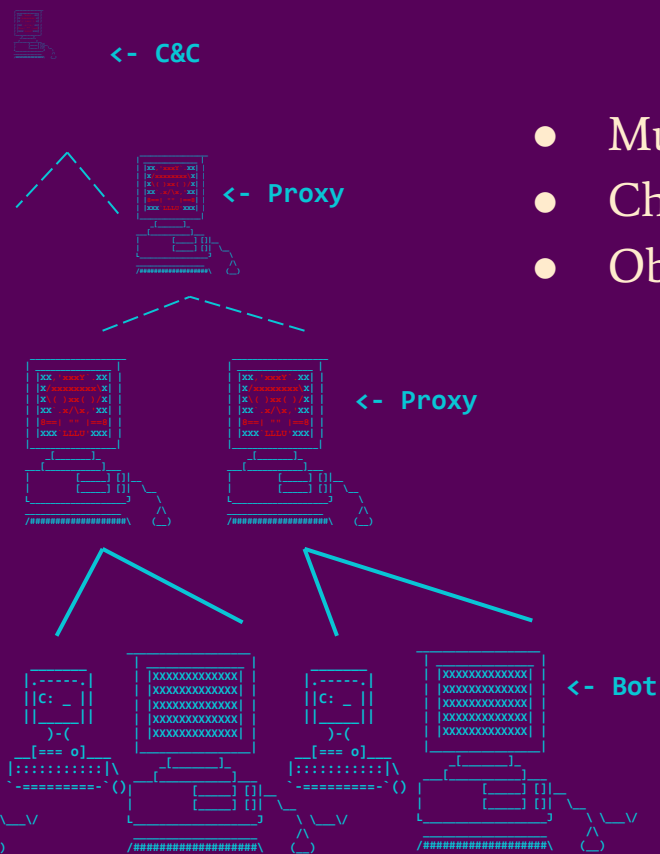
- Prevention of control channel interception



Architecture and Design

- Simple concept
- Fast command distribution
- C&C is central point of failure

Layered Centralized Architecture

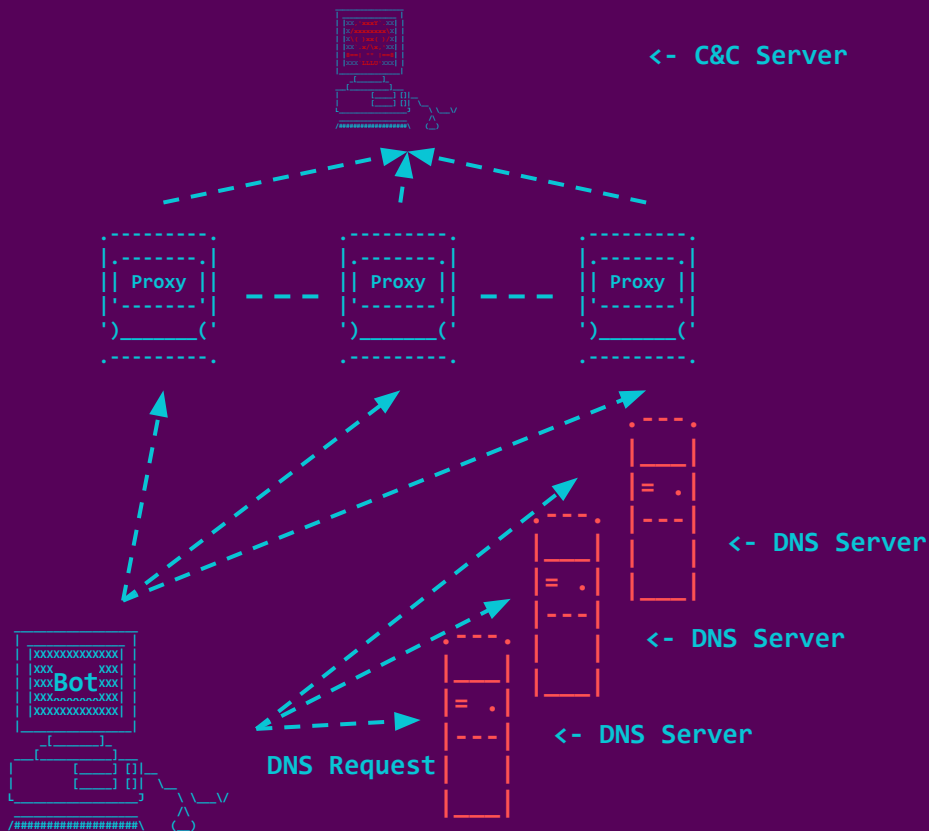


- Multiple layers of proxies
- Chained proxies possible
- Obfuscation of C&C server

- Rapid shifting between systems
 - Shift of DNS A records (TTL: ~5 minutes)
 -
- Proxies systems are hijacked devices

- Obfuscation of botnet infrastructure
- Prevention of C&C takedown

Double Fast Flux Architecture



Workflow:

- Rapid shifting between systems
 - Shift of DNS A records (TTL: ~5 minutes)
 - **Shift of DNS NS records**
- Proxies systems are hijacked devices

Goal:

- Obfuscation of botnet infrastructure
- Prevention of C&C takedown

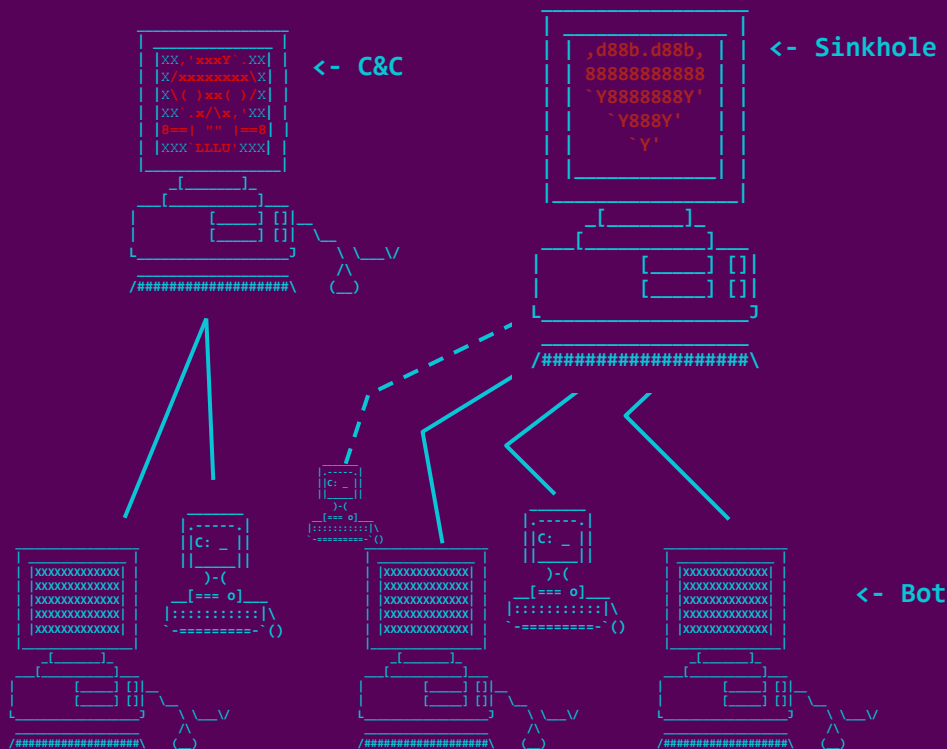
Botnet Revenue Options

- Distributed ...
 - Spam mails
 - Denial of service (DDoS)
 - Click fraud
 - Crypto mining
 - ...
- Access-as-a-Service
 - Data exfiltration, key stealing
 - E-Banking and financial fraud
- Installation-as-a-Service
 - Keylogger
 - Ransomware
- Infrastructure-as-a-Service



Botnet Monitoring

Sinkholing



- Technique for centralized botnet architectures
- DNS or IP redirection
- Malicious domains can be purchased or confiscated

Goal:

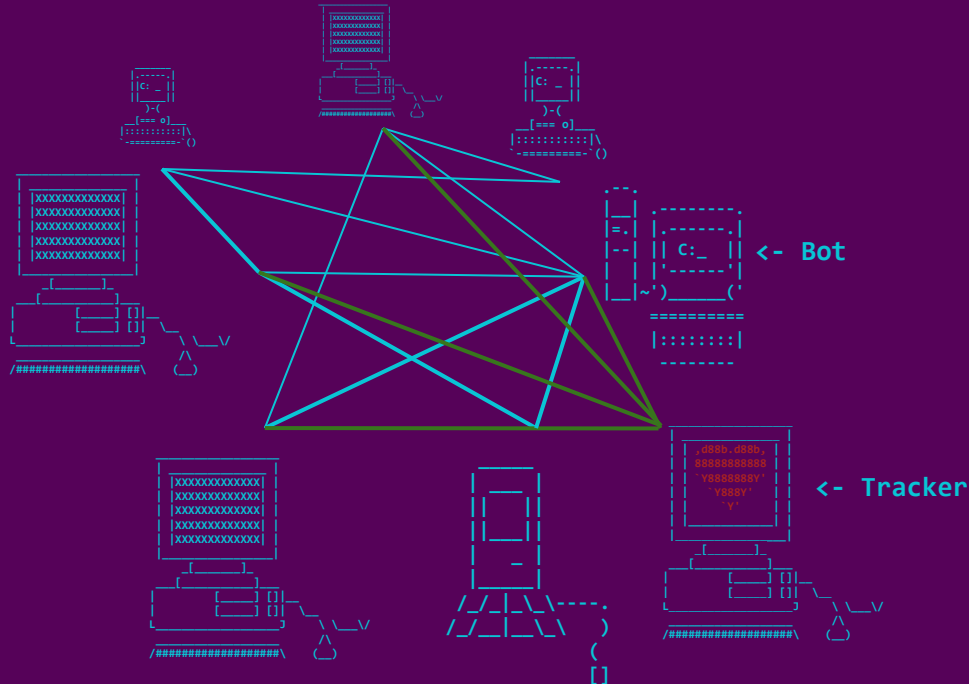
- Interception of control channels
- Gathering insides and statistics

Tracking

- Technique for P2P architecture
- Protocol implementation
- Infiltration of the network as “Bot”

Goal:

- Gathering insides and statistics



Gathering Information

Information Acquisition

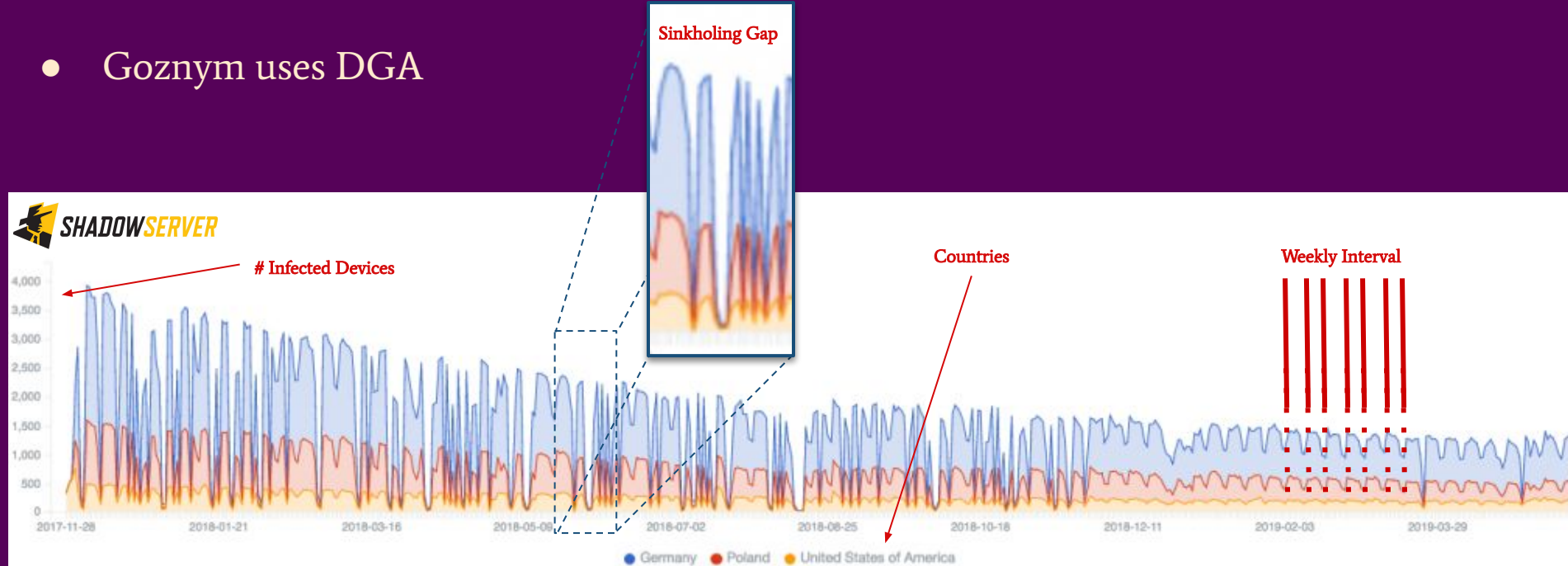
- Where are the C&C servers and the Botmaster located ?
- How active is the botnet ?
- Which type of attacks are executed ?
- Who gets attacked ?
- Is there any cooperation between other threat actors ?
- Acquiring numbers about:
 - infected devices,
 - device types,
 - countries affected,
 - ...



jgs

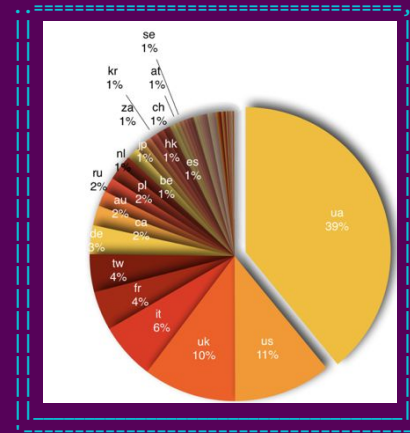
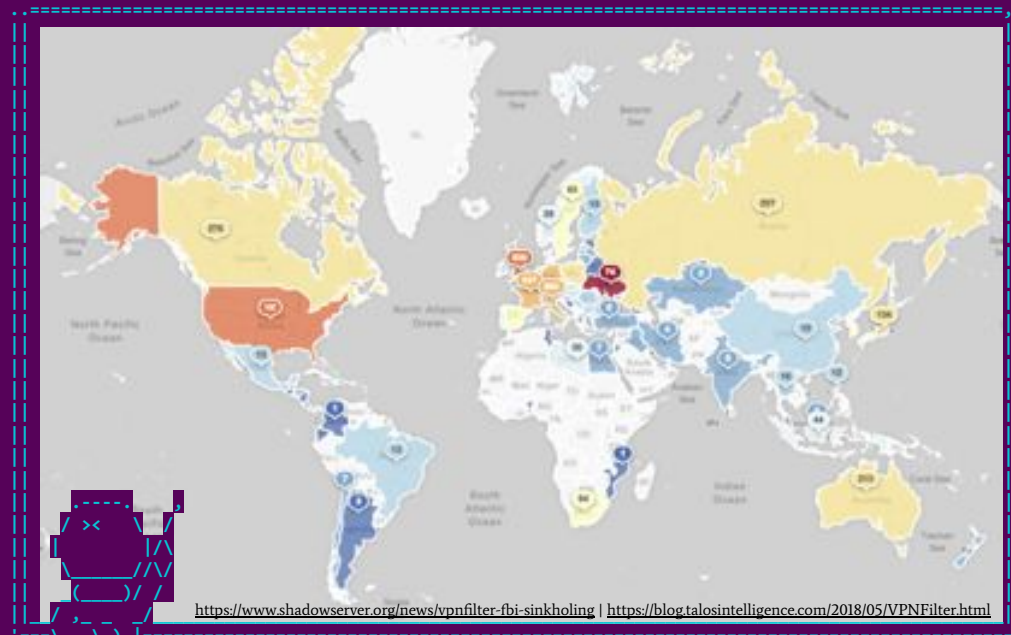
Sinkholing: Goznym

- Goznym uses DGA



<https://www.shadowserver.org/news/goznym-indictments-action-following-on-from-successful-avalanche-operations>

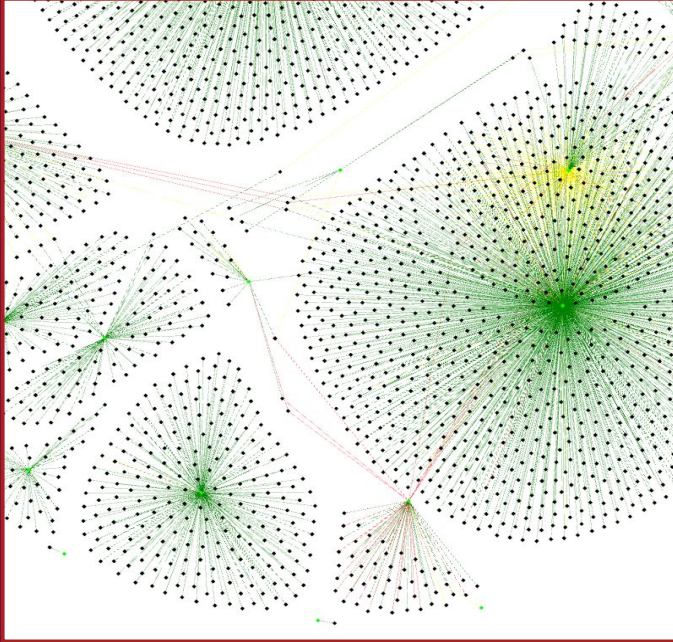
VPNFilter



jgs

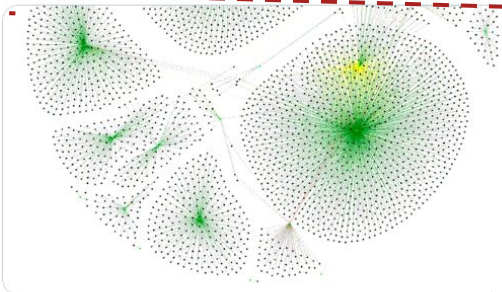
TALOS

Infrastructure Sharing



Myrtus @Myrtus0x0 · 16. Jan. ...

Clustered [#malware](#) C2s I've captured over the last 4-5 months. Green dots are families. Black dots are C2s. If a C2 is just used by one family it has a green edge, if used by two families it has a yellow edge and red for three or more.



13 68 283

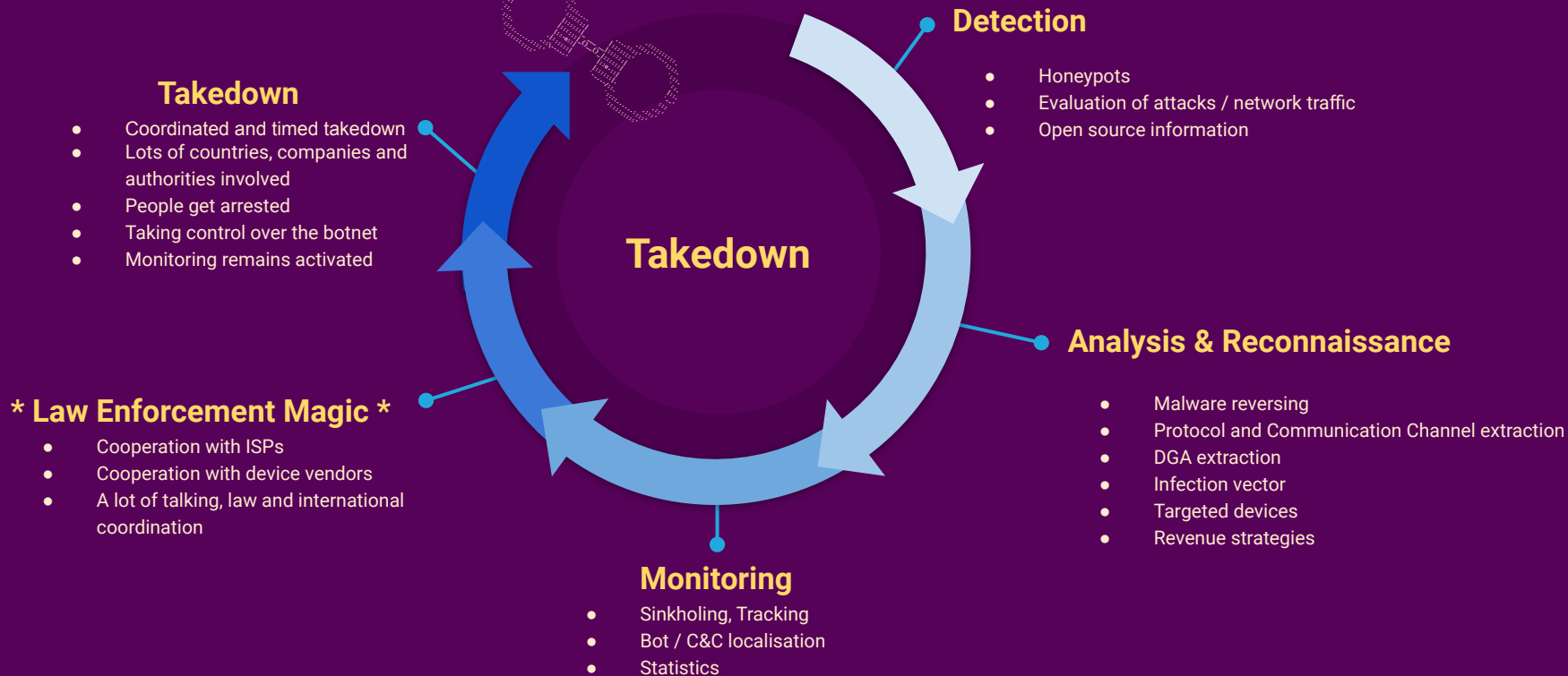
Myrtus @Myrtus0x0 · 16. Jan. ...

Did it to show infrastructure overlap. For instance shared emotet dridex infrastructure

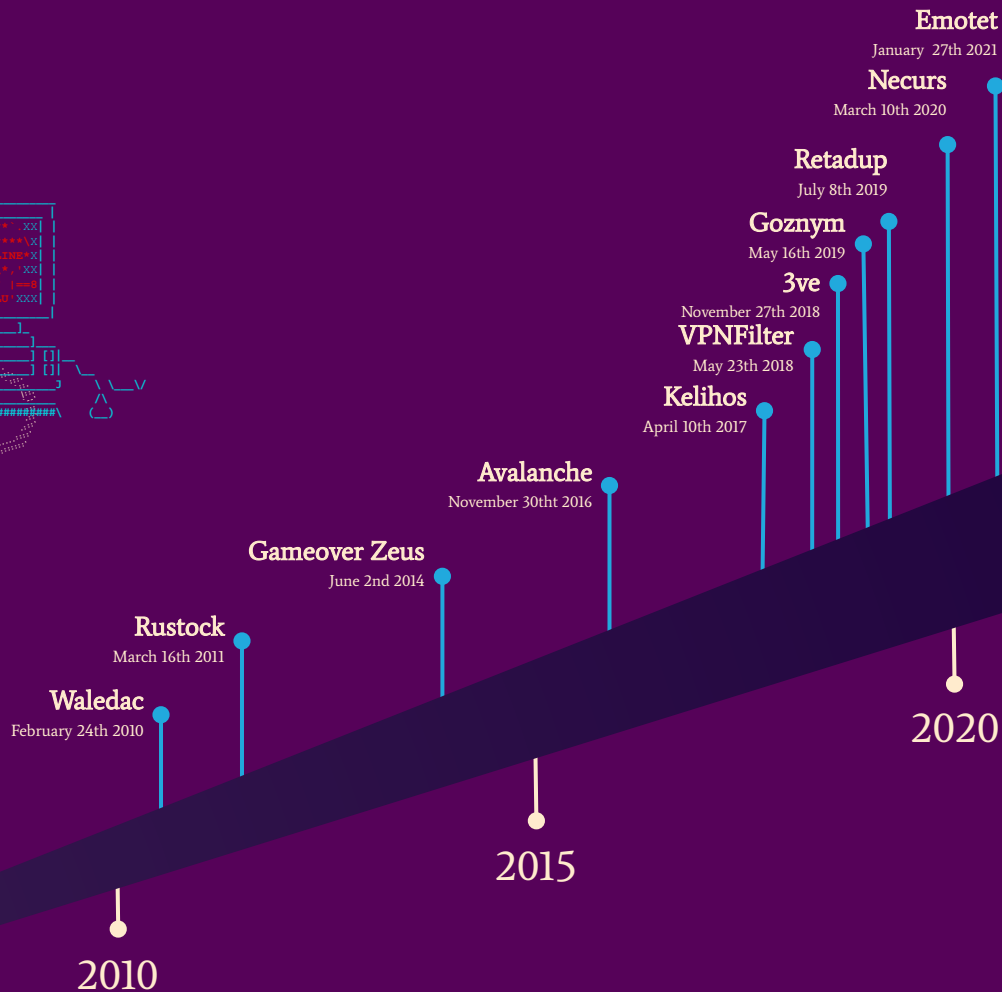
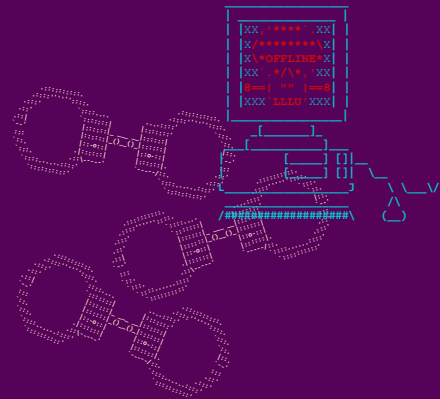
<https://twitter.com/Myrtus0x0/status/1350217540643872768?s=19>

Takedown

Takedown Action Flow



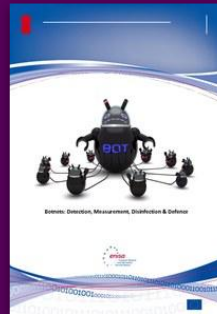
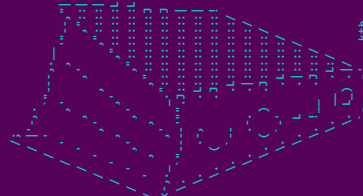
Takedowns



Recommendations

Further Information And Worth Reading

- European Union Agency for Cybersecurity (ENISA)
 - Report: “**Botnets: Measurement, Detection, Disinfection and Defence**”
 - <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>
 - Report: “**Threat Landscape 2020 - Botnet**”
 - <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-botnet>



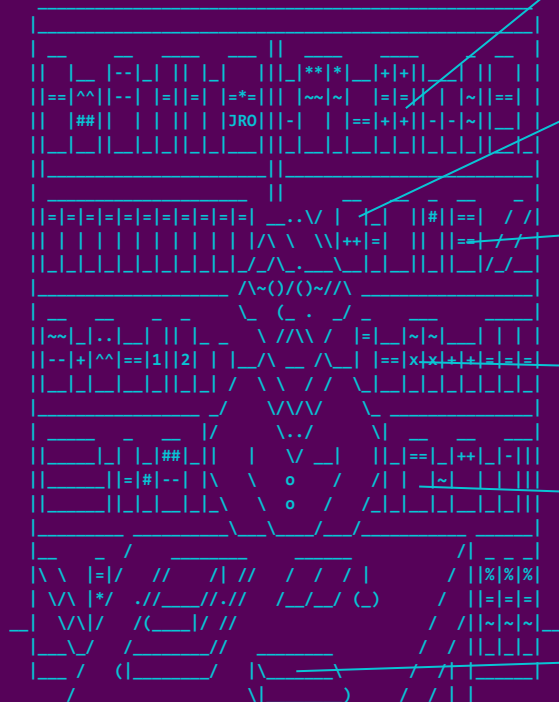
Recommendations



<https://johannesbader.ch>

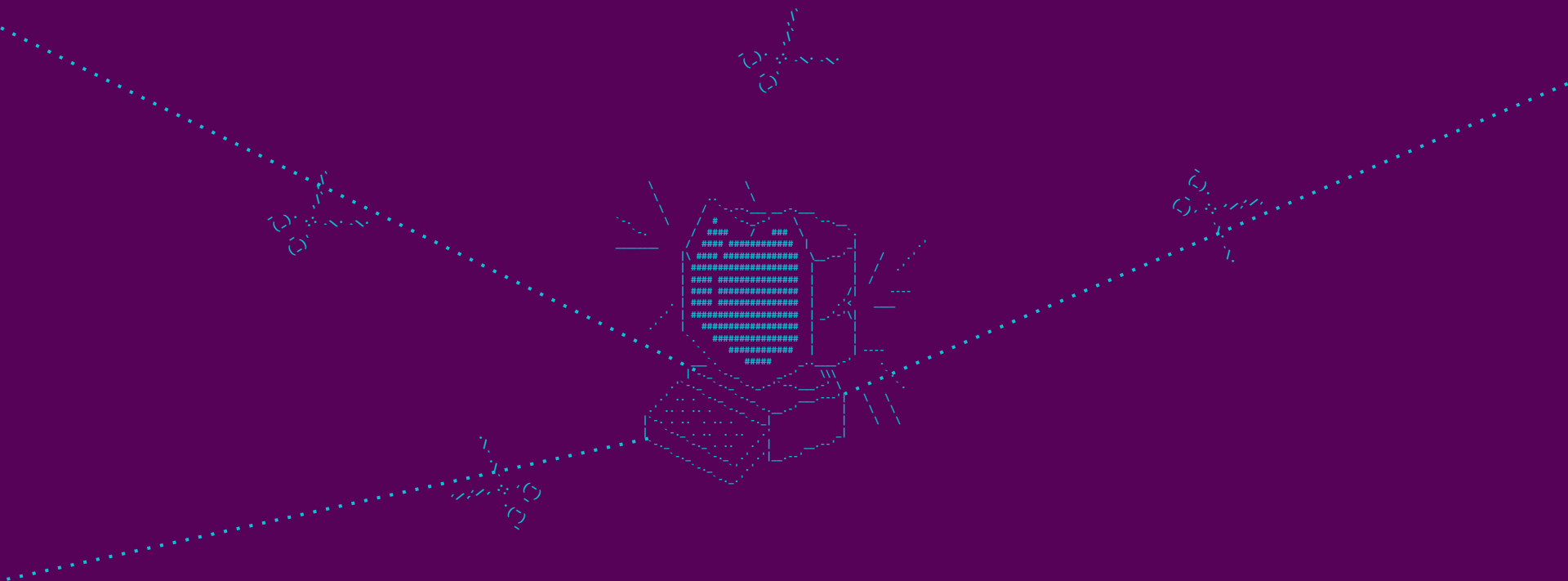


baderj / domain_generation_algorithms



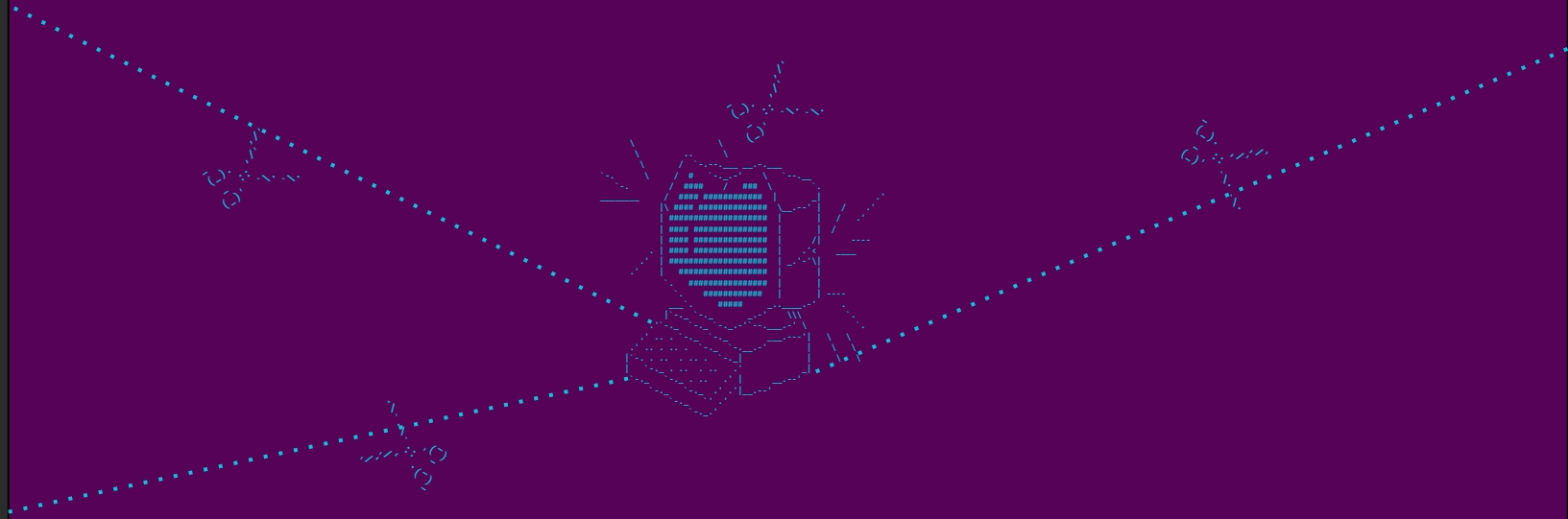
12375

Thanks For Watching



@botlabsDev

Thanks For Watching



twitter

@botlabsDev



Chemnitzer

Linux-Tage

13. und 14. März 2021



