{ Linnea }

Tobias Ruck - Miranda Mowbray
Hewlett-Packard Enterprise

How to
select clients from network where
clients have malware

{ Linnea }

Tobias Ruck - Miranda Mowbray
Hewlett-Packard Enterprise

How to
select clients **from** network **where**
clients have malware

Infected Clients

connect('mymalware.com')

Algorithms

d

com')

Blacklist

block these:
mymalware.com
cnc.com
* *
.

Possible seeds:
date
twitter trends
pants colour

aaaggegd.com hobtlexs.cc ihjipaii.com ahjk
opblbrpo.ws bunesli zgldjilr.com opegu
fjrvt.net fumzby dedm.com vgc
auayrzmq.net flrwsm.net eb
ccebmavp.net fxxnppu.net c
htwtrhvc.com ynimut.ws ktd
excqop.ws hiiofr jp.com sqjjstlf.
kwivtysx.n zezi bofz.com abip
ketswohu wzk.cc eok
hmajswm ws xybgf
jqkojoe jlyzio
jaag.cc vav.n
cj.ws go bn.cc
xaurspk ws xbp
roovjjcj.r bpyiuzl
hsb.ws g hltd zwaffj.w
wu.ws xpantpxa.net njzvecqs.net xkuzwtzi.c

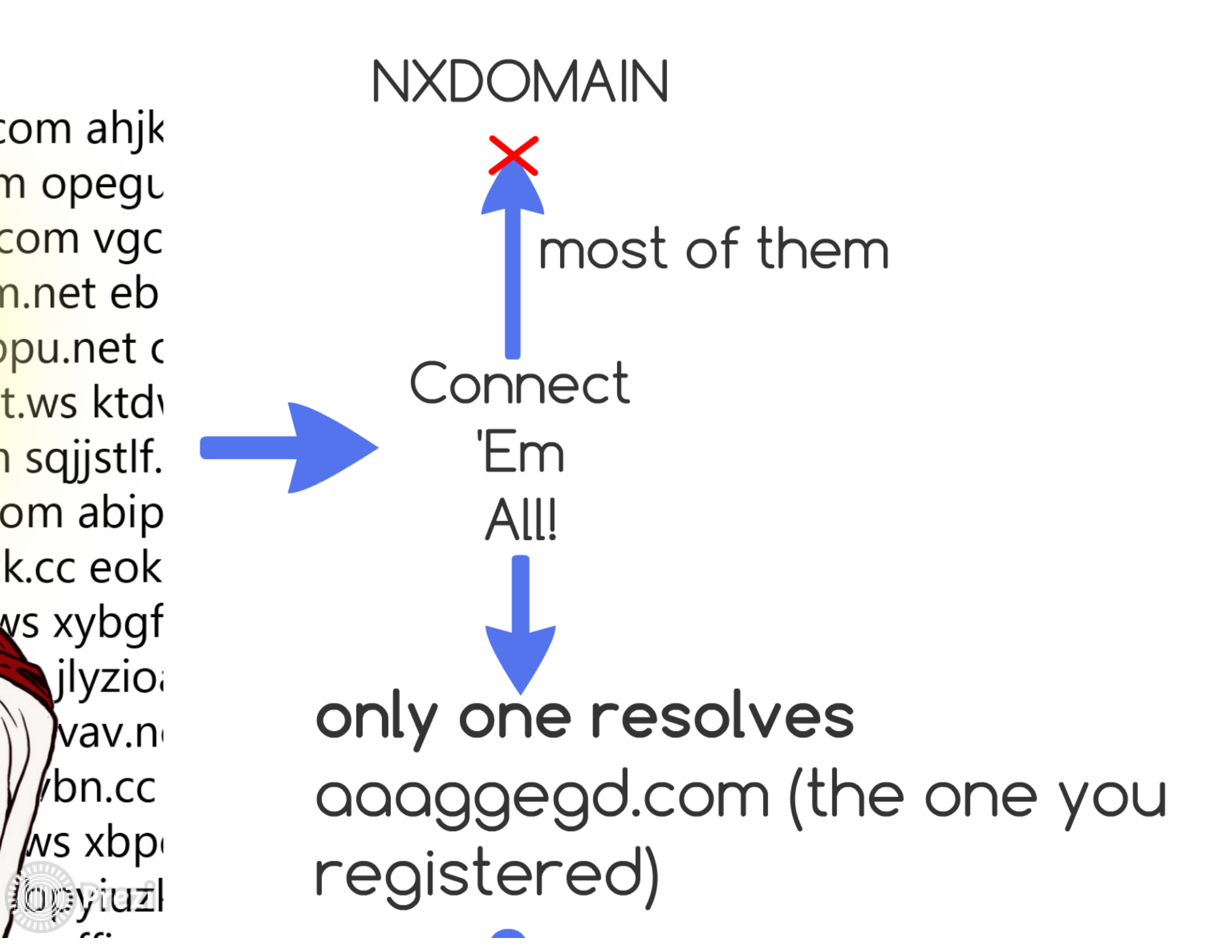
NXDOMAIN

most of

Connect
'Em
All!

only one resol
aaaggegd.com
registered)

Domain Generation Algorithms


com ahjk
m opegu
com vgc
n.net eb
pu.net c
t.ws ktdv
sqjjstlf.
om abip
k.cc eok
ws xybgf
jlyzio
vav.n
bn.cc
ws xbp
NXDOMAIN
most of them
Connect
'Em
All!
only one resolves
aaaggegd.com (the one you
registered)

Possible seeds:
date
twitter trends
pants colour

NXDOMAIN

most of them

Connect
'Em
All!

only one resolves
aaaggegd.com (the one you registered)

Domain Generation Algorithms

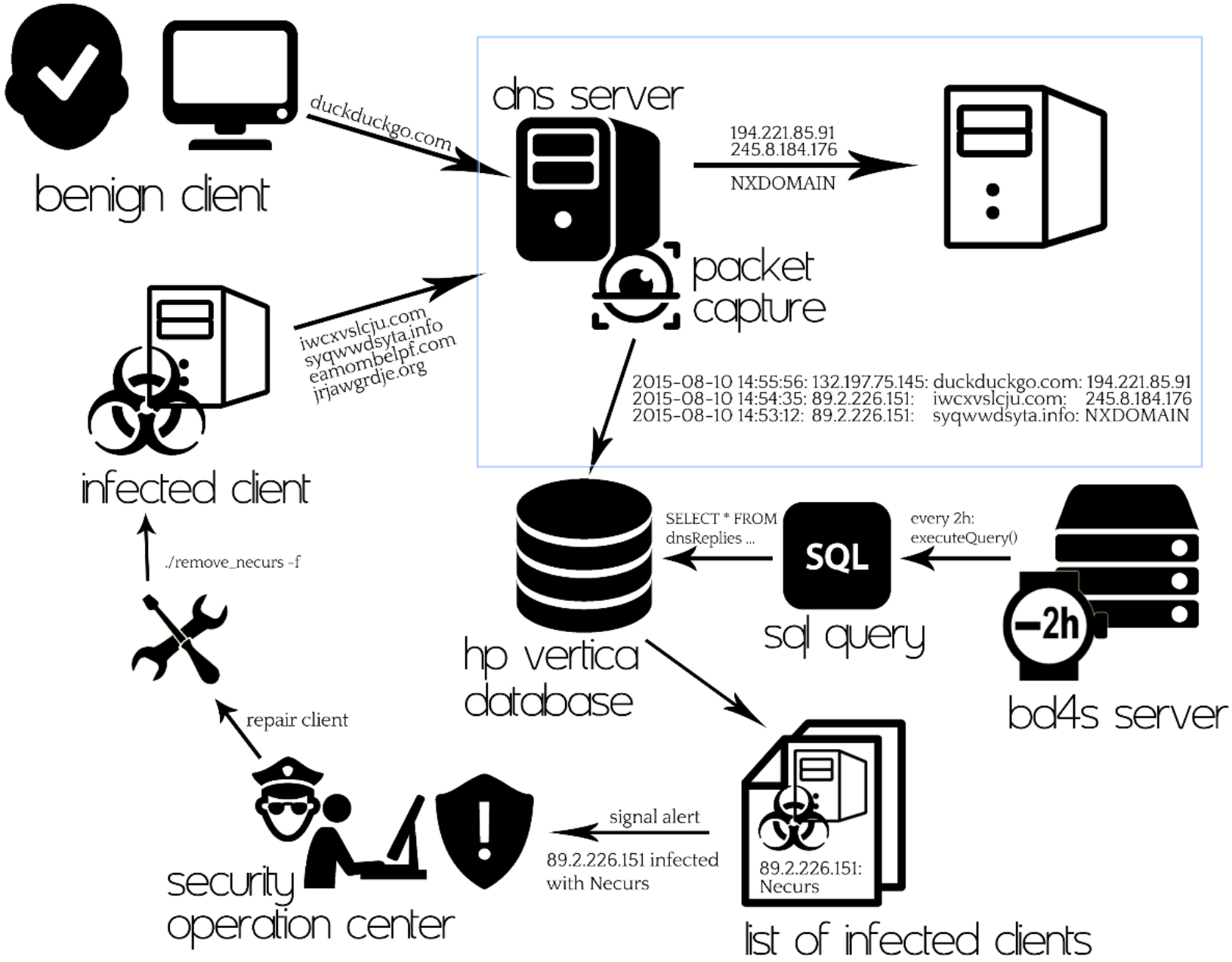
Infected Clients

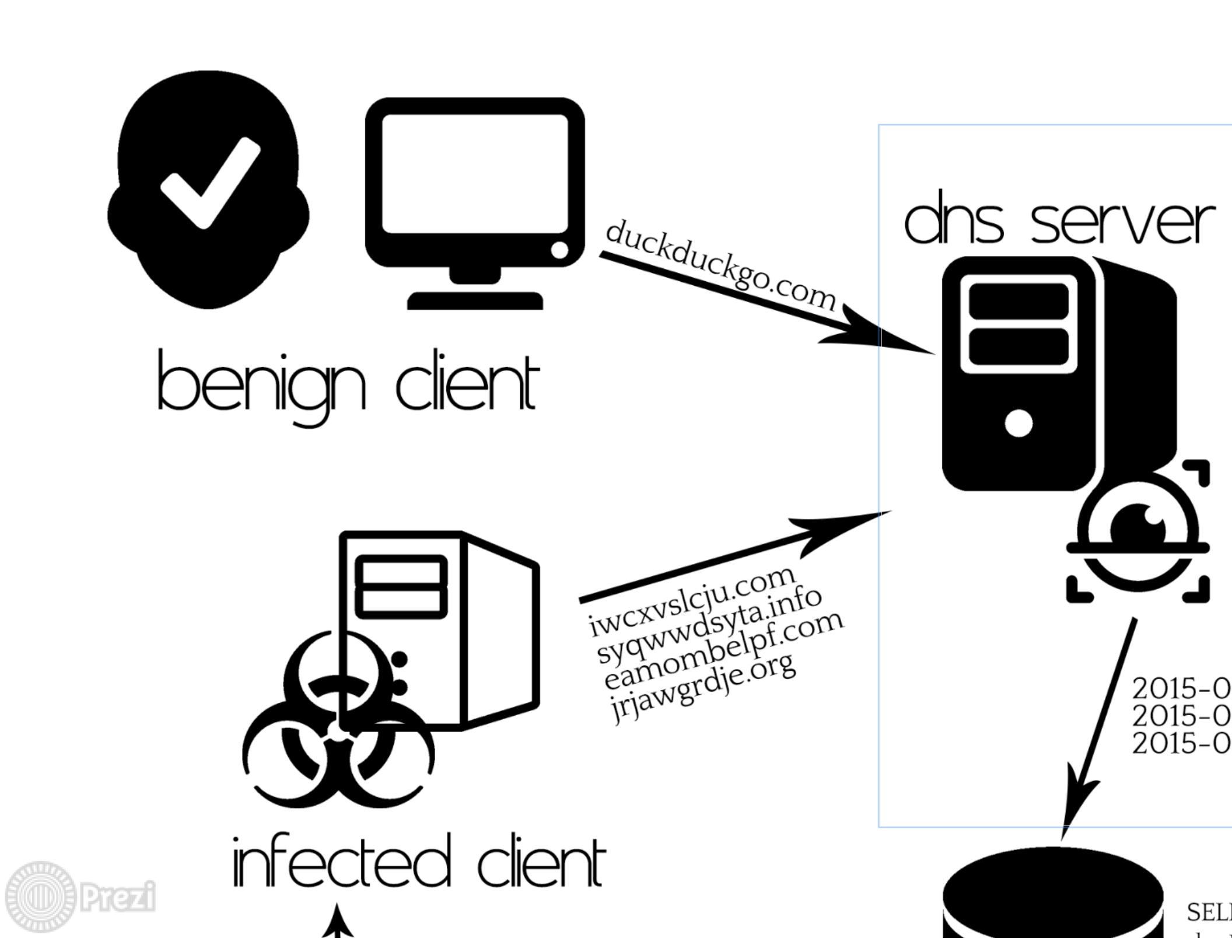
connect('mymalware.com')

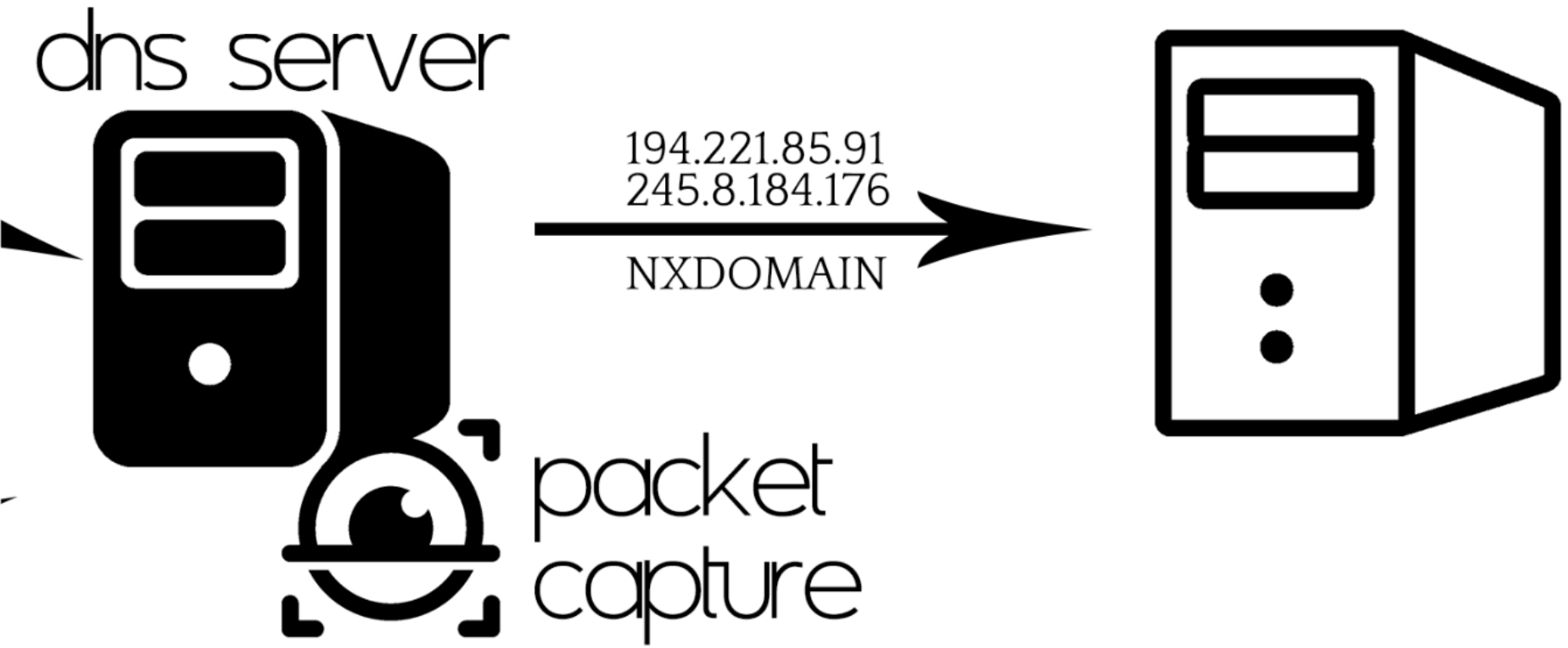
Blacklist

block these:
mymalware.com
cnc.com
* *
.

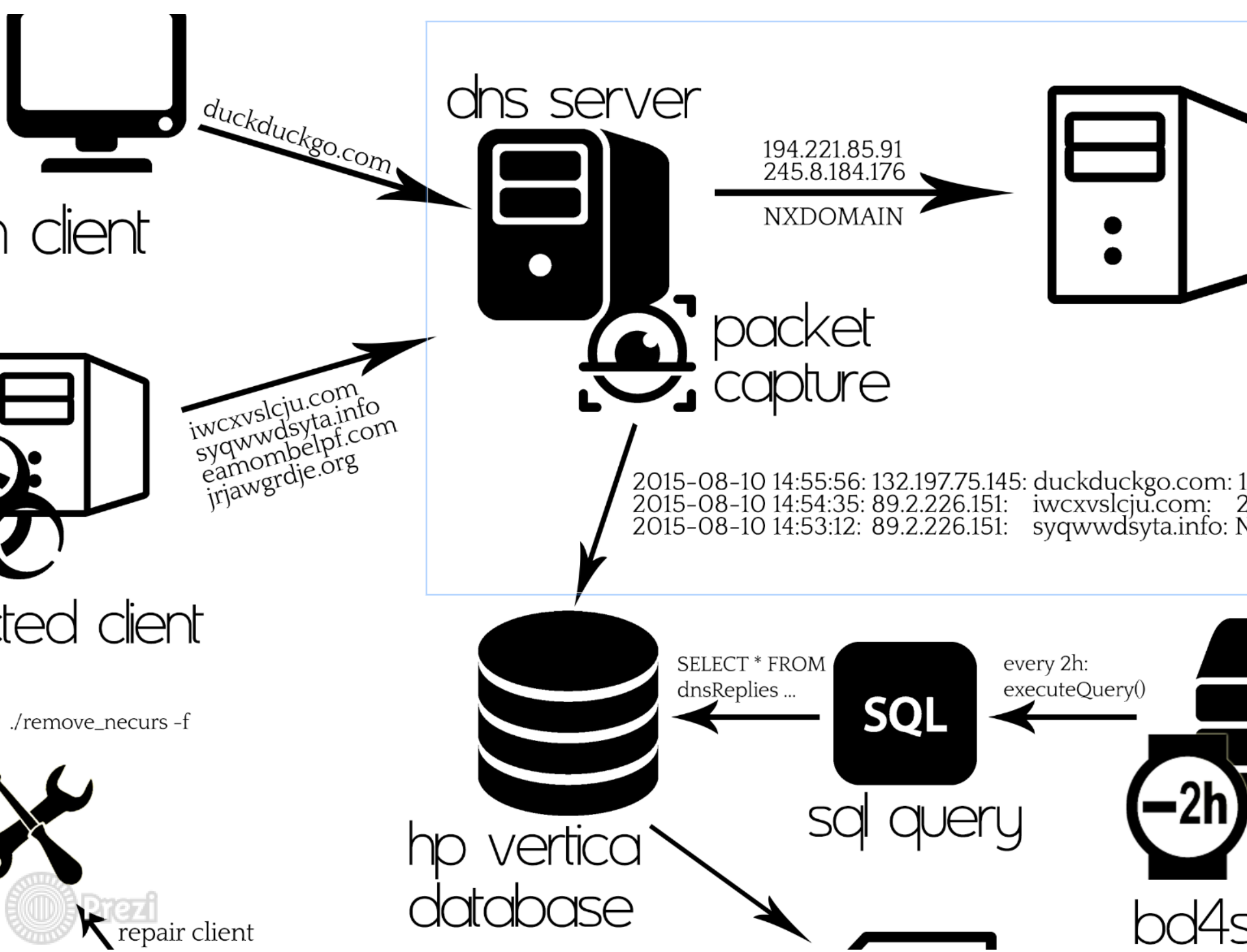
Your Console

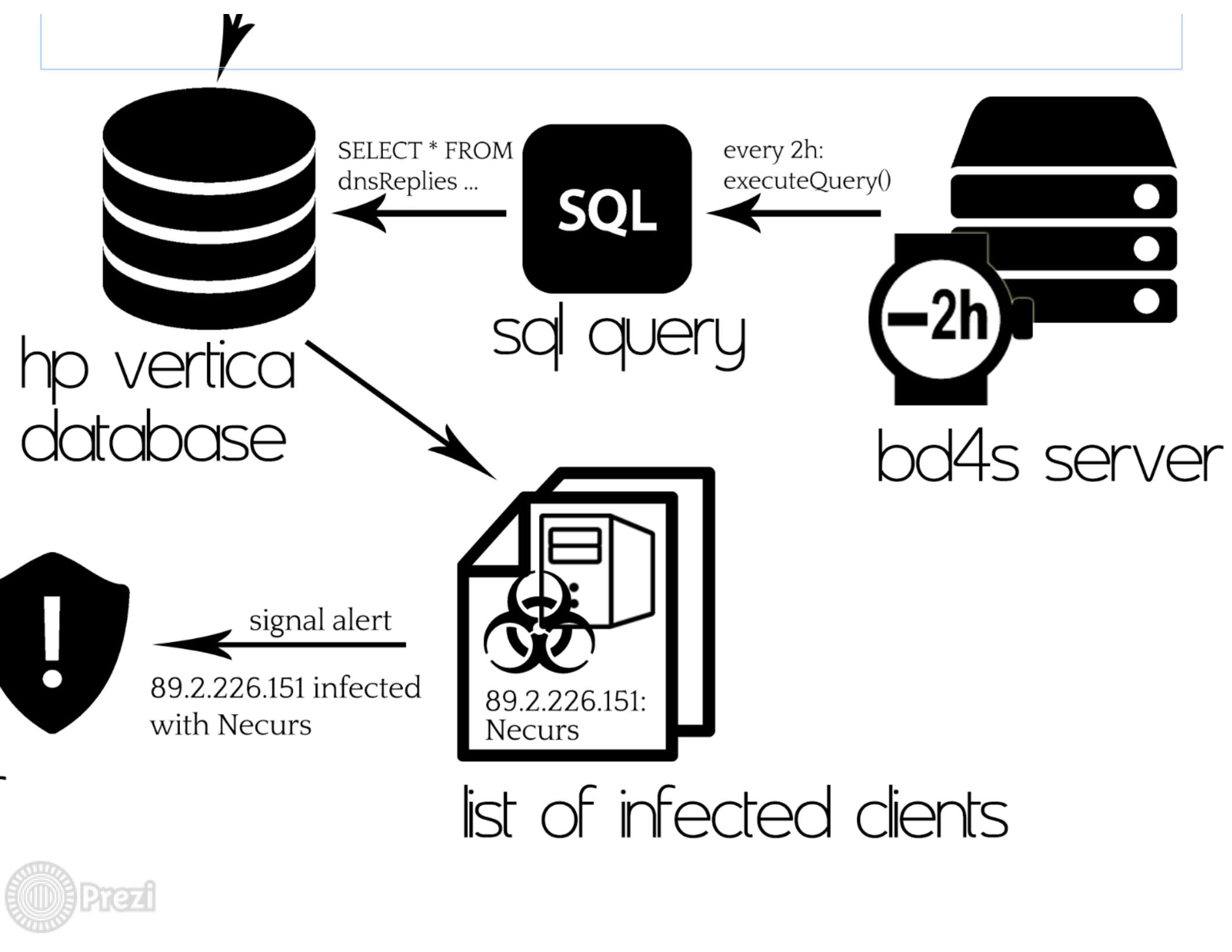

benign client
duckduckgo.com
dns server
194.221.85.91
245.8.184.176
NXDOMAIN
packet capture
iwcxvslcju.com
syqwwdsyta.info
eamombelpf.com
jrjawgrdje.org
infected client
2015-08-10 14:55:56: 132.197.75.145: duckduckgo.com: 194.221.85.91
2015-08-10 14:54:35: 89.2.226.151: iwcxvslcju.com: 245.8.184.176
2015-08-10 14:53:12: 89.2.226.151: syqwwdsyta.info: NXDOMAIN
SELECT * FROM dnsReplies ...
SQL
every 2h: executeQuery()
sql query
−2h
bd4s server
hp vertica database
./remove_necurs -f
repair client
signal alert
89.2.226.151 infected with Necurs
89.2.226.151: Necurs
security operation center
list of infected clients

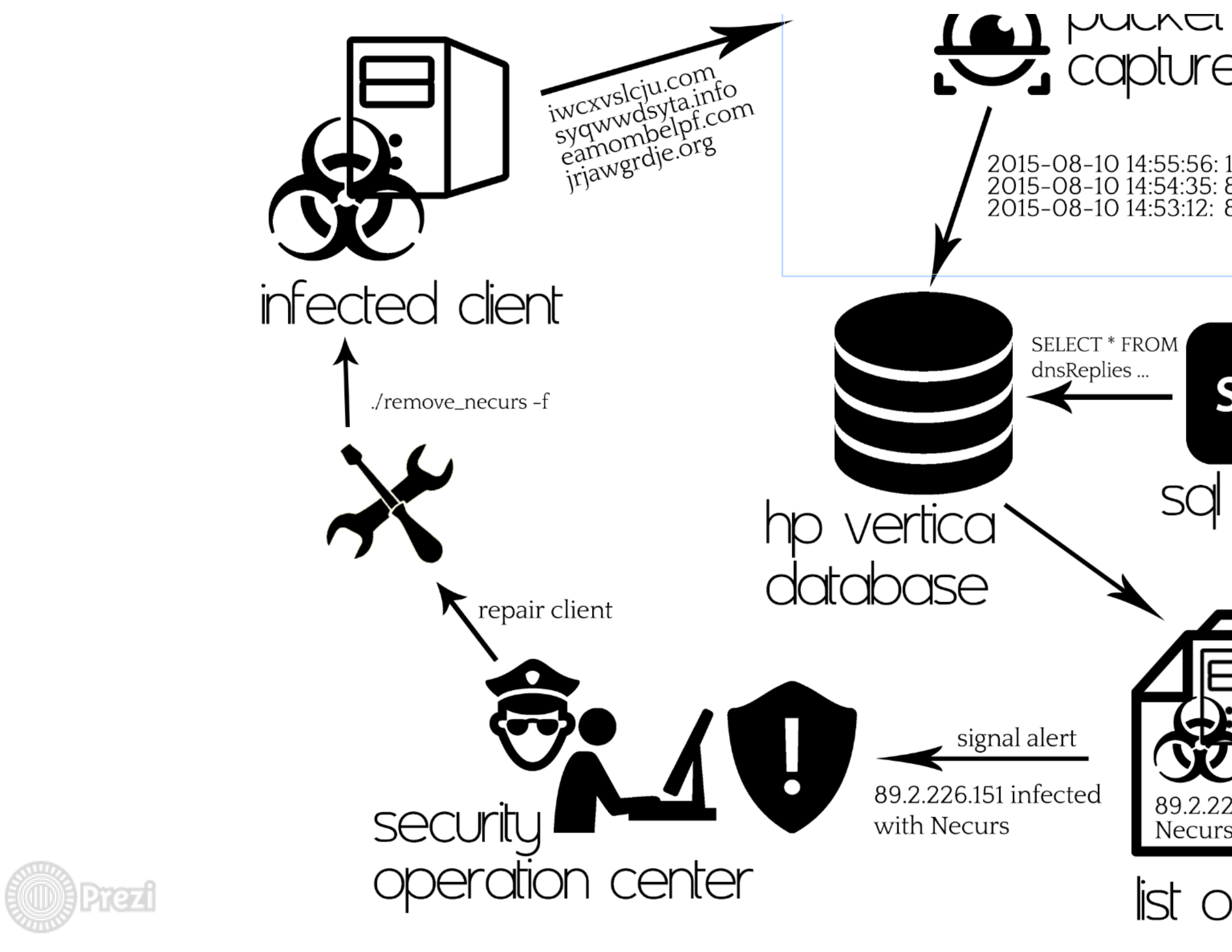

benign client
duckduckgo.com
dns server
infected client
iwcxvslcju.com
syqwwdsyta.info
eamombelpf.com
jrjawgrdje.org
2015-0
2015-0
2015-0
SEL



2015-08-10 14:55:56: 132.197.75.145: duckduckgo.com: 194.221.85.91
2015-08-10 14:54:35: 89.2.226.151: iwcxvslcju.com: 245.8.184.176
2015-08-10 14:53:12: 89.2.226.151: syqwwdsyta.info: NXDOMAIN


client
duckduckgo.com
dns server
194.221.85.91
245.8.184.176
NXDOMAIN
packet
capture
iwcxvslcju.com
syqwwdsyta.info
eamombelpf.com
jrjawgrdje.org
2015-08-10 14:55:56: 132.197.75.145: duckduckgo.com: 1
2015-08-10 14:54:35: 89.2.226.151: iwcxvslcju.com: 2
2015-08-10 14:53:12: 89.2.226.151: syqwwdsyta.info: N
ted client
./remove_necurs -f
SELECT * FROM
dnsReplies ...
SQL
every 2h:
executeQuery()
sql query
hp vertica
database
-2h
bd4s
repair client


SELECT * FROM
dnsReplies ...
SQL
every 2h:
executeQuery()
sql query
hp vertica
database
bd4s server
signal alert
89.2.226.151 infected
with Necurs
89.2.226.151:
Necurs
list of infected clients


packet
capture
iwcxvslcju.com
syqwwdsyta.info
eamombelpf.com
jrjawgrdje.org
2015-08-10 14:55:56: 1
2015-08-10 14:54:35: 8
2015-08-10 14:53:12: 8
infected client
SELECT * FROM
dnsReplies ...
./remove_necurs -f
hp vertica
database
repair client
signal alert
89.2.226.151 infected
with Necurs
security
operation center
89.2.22
Necurs
list o

Matsnu

com taletalk-alarm.com t

smart-media.com towelb

Matsnu

swimming-wonder.com taletalk-alarm.com testreveal-designer.com title-smart-media.com towelbecome-maintenance.com video-drink-enthusiasm.com wall-mortgage.com layer-run-river.com knee-communicate.com dimension-retain.com drawer-proposed.com earth-apologize.com metal-range-point.com relative-walk.com relation-happen.com spitepack-goal.com town-reason-knowledge.com gate-boot-ability.com key-sentence.com golf-cash-spirit.com handpin-airconsider.com hook-carpet-difference.com hook-provide.com hostspace-tank.com husband-champion.com image-meet-sex.com user-survey-medicine.com demand-foot-company.com mistake-adopt.com

Gotta catch 'em all!

```
SELECT dst, request, timestamp
FROM (
    SELECT request, dst, timestamp,
```

Gotta catch 'em all!

```
SELECT dst, request, timestamp
 FROM (
    SELECT request, dst, timestamp,
       COUNT(has1hyphen) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_0,
       COUNT(has2hyphen) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_1,
       COUNT(request) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_requests
    FROM (
       SELECT request, dst, MAX(timestamp) AS timestamp,
          (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
          (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
       FROM hplDNSReplies
       WHERE timestamp >= '2015-08-06 00:00:00' AND timestamp <= '2015-08-06 01:59:59'
          AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
          AND (cat = 'NXDOMAIN')
       GROUP BY dst, request, d0, d1
    ) d
 ) f
 WHERE f.number_requests >= 25  AND  number_0+number_1 >= 20  AND  number_0 >= 9
    AND number_0 < 200  AND  number_1 >= 9
```

```
  COUNT(has2hyphen) OVER (PARTITION BY dst ORDER BY timestamp
          RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOW
     AS number_1,
  COUNT(request) OVER (PARTITION BY dst ORDER BY timestamp
          RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOW
     AS number_requests
FROM (
  SELECT request, dst, MAX(timestamp) AS timestamp,
     (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
     (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
  FROM hplDNSReplies
  WHERE timestamp >= '2015-08-06 00:00:00' AND timestamp <= '2015-08-06 01:59:59'
     AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
     AND (cat = 'NXDOMAIN')
  GROUP BY dst, request, d0, d1
) d

HERE f.number_requests >= 25  AND  number_0+number_1 >= 20  AND  number_0 >= 9
 AND number_0 < 200  AND  number_1 >= 9
```

```
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING A
    AS number_1,
COUNT(request) OVER (PARTITION BY dst ORDER BY tim
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING A
    AS number_requests
ROM (
SELECT request, dst, MAX(timestamp) AS timestamp,
    (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
    (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
FROM hplDNSReplies
WHERE timestamp >= '2015-08-06 00:00:00' AND timestam
    AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
    AND (cat = 'NXDOMAIN')
GROUP BY dst, request, d0, d1
)
```

Gotta catch 'em all!

```
ECT dst, request, timestamp
OM (
SELECT request, dst, timestamp,
  COUNT(has1hyphen) OVER (PARTITION BY dst ORDER BY timestamp
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
    AS number_0,
  COUNT(has2hyphen) OVER (PARTITION BY dst ORDER BY timestamp
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
    AS number_1,
  COUNT(request) OVER (PARTITION BY dst ORDER BY timestamp
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
    AS number_requests
FROM (
  SELECT request, dst, MAX(timestamp) AS timestamp,
    (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
    (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
  FROM hplDNSReplies
  WHERE timestamp >= '2015-08-06 00:00:00' AND timestamp <= '2015-08-06 01:59:59'
    AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
    AND (cat = 'NXDOMAIN')
  GROUP BY dst, request, d0, d1
```

```
        AS number_requests
    FROM (
        SELECT request, dst, MAX(timestamp) AS timestamp,
            (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
            (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
        FROM hplDNSReplies
        WHERE timestamp >= '2015-08-06 00:00:00' AND timestamp <= '2015-08-06 01:59:59'
            AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
            AND (cat = 'NXDOMAIN')
        GROUP BY dst, request, d0, d1
    ) d
) f
WHERE f.number_requests >= 25  AND  number_0+number_1 >= 20  AND  number_0 >= 9
     AND number_0 < 200  AND  number_1 >= 9
```

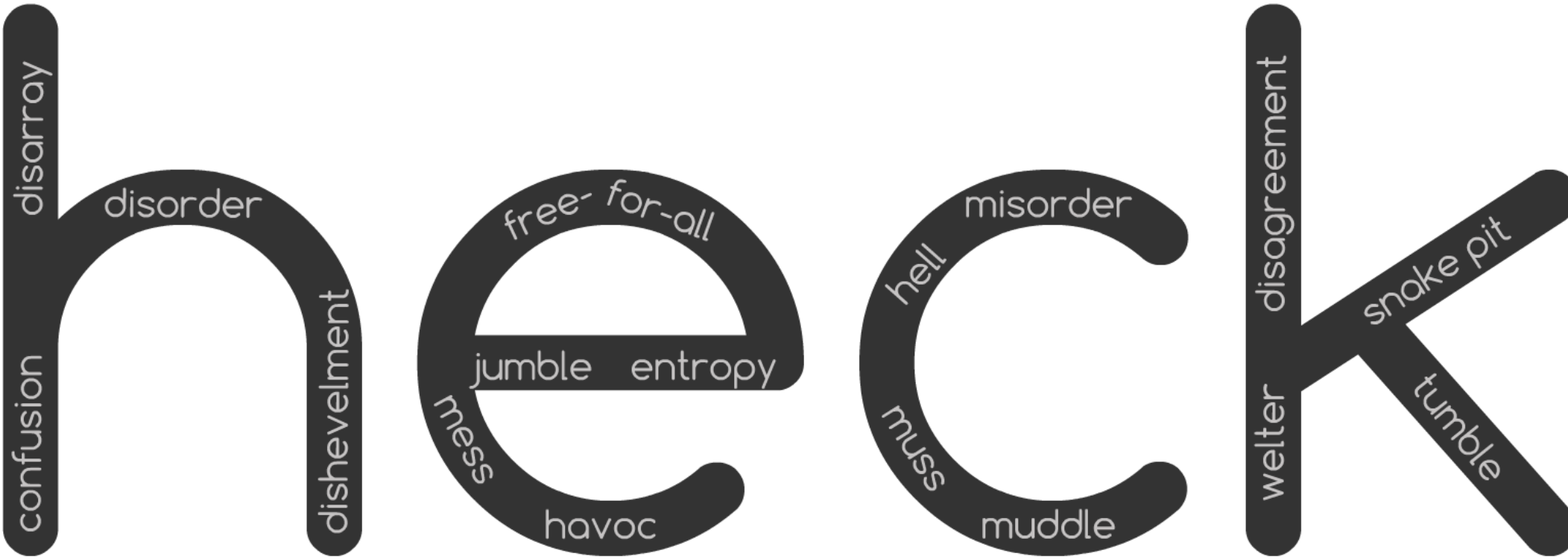
Gotta catch 'em all!

```
SELECT dst, request, timestamp
 FROM (
    SELECT request, dst, timestamp,
       COUNT(has1hyphen) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_0,
       COUNT(has2hyphen) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_1,
       COUNT(request) OVER (PARTITION BY dst ORDER BY timestamp
                RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING)
          AS number_requests
    FROM (
       SELECT request, dst, MAX(timestamp) AS timestamp,
          (REGEXP_COUNT(d1, '-') = 1 OR NULL) AS has1hyphen,
          (REGEXP_COUNT(d1, '-') = 2 OR NULL) AS has2hyphen
       FROM hplDNSReplies
       WHERE timestamp >= '2015-08-06 00:00:00' AND timestamp <= '2015-08-06 01:59:59'
          AND REGEXP_INSTR(request, '^[a-z-]{11,23}\.com$') > 0
          AND (cat = 'NXDOMAIN')
       GROUP BY dst, request, d0, d1
    ) d
) f
 WHERE f.number_requests >= 25  AND  number_0+number_1 >= 20  AND  number_0 >= 9
     AND number_0 < 200  AND  number_1 >= 9
```

Linnea for the rescue

Making a language just for the heck of it

```
{
   timestamp >= t0 - 2h, timestamp <= t0,        Within 2h timeslot
   nxdomain,                                     NXDOMAIN
   match(domain, '^[a-z-]{11,23}\.com$')         Match letters and hyphens
},
{
   [client:1h|true] >= 25,                       At least 25 queried per client
   [client:1h|count(d1, '-') = 1] +              At least 20 w. 1 or 2 hyphens per
       [client:1h|count(d1, '-')  = 2] >= 20,       client
   [client:1h|count(d1, '-') = 1] >= 9,          At least 9 w. 1 hyphen per client
   [client:1h|count(d1, '-') = 1] < 200,         Less than 200 w. 1 hyphen per client
   [client:1h|count(d1, '-') = 2] >= 9           At least 9 w. 2 hyphens per client
}
```


disarray
disorder
confusion
dishevelment
free- for-all
jumble
entropy
mess
havoc
misorder
hell
muss
muddle
disagreement
snake pit
welter
tumble

Linnea for the rescue

Making a language just for the heck of it

```
{
   timestamp >= t0 - 2h, timestamp <= t0,        Within 2h timeslot
   nxdomain,                                     NXDOMAIN
   match(domain, '^[a-z-]{11,23}\.com$')         Match letters and hyphens
},
{
   [client:1h|true] >= 25,                       At least 25 queried per client
   [client:1h|count(d1, '-') = 1] +              At least 20 w. 1 or 2 hyphens per
       [client:1h|count(d1, '-')  = 2] >= 20,       client
   [client:1h|count(d1, '-') = 1] >= 9,          At least 9 w. 1 hyphen per client
   [client:1h|count(d1, '-') = 1] < 200,         Less than 200 w. 1 hyphen per client
   [client:1h|count(d1, '-') = 2] >= 9           At least 9 w. 2 hyphens per client
}
```

date	domain
2015-08-11 09:13:38	accident-sharp.com
2015-08-11 09:14:58	ambition-court.com
2015-08-11 09:15:02	amount-drive.com
2015-08-11 09:28:19	problemcoat-weight.com
2015-08-11 09:28:55	reading-persuade.com
2015-08-11 09:29:55	red-base-chance.com
2015-08-11 09:29:57	request-finance.com
2015-08-11 09:30:16	research-spot.com
2015-08-11 09:32:59	shame-show-cream.com
2015-08-11 09:33:24	size-lost-park.com
2015-08-11 09:34:12	space-belt-rate.com
2015-08-11 09:35:31	timetengstell.com
2015-08-11 09:35:38	standardsucceed.com
2015-08-11 09:35:40	star-appear-map.com
2015-08-11 09:35:47	strategy-borrow.com

2015-08-11 09:40:14 guarantee-value.com
2015-08-11 09:40:19 quarter-smell.com
2015-08-11 09:41:24 lady-sandwich.com
2015-08-11 09:41:30 challengediscover.com
2015-08-11 09:41:42 brother-hang.com
2015-08-11 09:43:18 bend-shoot-stress.com
2015-08-11 09:43:24 wall-bottle-assistant.com
2015-08-11 09:57:49 plane-branch.com
2015-08-11 09:57:54 plateadvanced.com
2015-08-11 09:58:04 pleasurerepair.com
2015-08-11 09:58:18 pot-blank-text.com
2015-08-11 09:58:24 poundresort-skin.com
2015-08-11 09:58:49 professorloose.com
2015-08-11 09:58:56 programcredit.com

people|history|way|art|money|world|information|map|two|family|government|health|system|computer|meat|year|thanks|music|person|reading|method|data|food|understanding|theory|law|bird|literature|problem|software|control|knowledge|power|ability|economics|love|internet|television|science|library|nature|fact|product|idea|temperature|investment|area|society|activity|story|industry|media|thing|oven|community|definition|safety|quality|development|language|management|player|variety|video|week|security|country|exam|movie|organization|equipment|physics|analysis|policy|series|thought|basis|boyfriend|direction|strategy|technology|army|camera|freedom|paper|environment|child|instance|month|truth|marketing|university|writing|article|department|difference|goal|news|audience|fishing|growth|income|marriage|user|combination|failure|meaning|medicine|philosophy|teacher|communication|relation|restaurant|satisfaction|sector|signature|significance|song|tooth|town|vehicle|volume|wife|accident|airport|appointment|arrival|assumption|baseball|chapter|committee|conversation|database|enthusiasm|error|explanation|farmer|gate|girl|hall|historian|hospital|injury|instruction|maintenance|manufacturer|meal|perception|pie|poem|presence|proposal|reception|replacement|revolution|river|son|speech|tea|village|warning|winner|worker|writer|assistance|breath|buyer|chest|chocolate|conclusion|contribution|cookie|courage|dad|desk|drawer|establishment|examination|garbage|grocery|honey|impression|improvement|independence|insect|inspection|inspector|king|ladder|menu|penalty|piano|potato|profession|professor|quantity|reaction|requirement|salad|sister|supermarket|tongue|weakness|wedding|affair|ambition|analyst|apple|assignment|assistant|bathroom|bedroom|beer|birthday|celebration|championship|cheek|client|consequence|departure|diamond|dirt|ear|fortune|friendship|funeral|gene|girlfriend|hat|indication|intention|lady|midnight|negotiation|obligation|passenger|pizza|platform|poet|pollution|recognition|reputation|shirt|sir|speaker|stranger|surgery|sympathy|tale|throat|trainer|uncle|youth|time|work|film|water|example|while|business|study|game|life|form|air|day|place|number|part|field|fish|back|process|heat|hand|experience|job|book|end|point|type|home|economy|value|body|market|guide|interest|state|radio|course|company|price|size|card|list|mind|trade|line|care|group|risk|word|fat|force|key|light|training|name|school|top|amount|level|order|practice|research|sense|service|piece|web|boss|sport|fun|house|page|term|test|answer|sound|focus|matter|kind|soil|board|oil|picture|access|garden|range|rate|reason|future|site|demand|exercise|image|case|cause|coast|action|age|bad|boat|record|result|section|building|mouse|cash|class|nothing|period|plan|store|tax|side|subject|space|rule|stock|weather|chance|figure|man|model|source|beginning|earth|program|chicken|design|feature|head|material|purpose|question|rock|salt|act|birth|car|dog|object|scale|sun|note|profit|rent|speed|style|war|bank|craft|half|inside|outside|standard|bus|exchange|eye|fire|position|pressure|stress|advantage|benefit|box|frame|issue|step|cycle|face|item|metal|paint|review|room|screen|structure|view|account|ball|discipline|medium|share|balance|bit|black|bottom|choice|gift|impact|machine|shape|tool|wind|address|average|career|culture|morning|pot|sign|table|task|condition|contact|credit|egg|hope|ice|network|north|square|attempt|date|effect|link|post|star|voice|capital|challenge|friend|self|shot|brush|couple|exit|front|function|lack|living|plant|plastic|spot|summer|taste|theme|track|wing|brain|button|click|desire|foot|gas|influence|mood|notice|rain|wall|base|damage|distance|feeling|pair|saving|staff|sugar|target|text|animal|author|budget|discount|file|ground|lesson|minute|officer|phase|reference|register|sky|stage|stick|title|trouble|bowl|bridge|campaign|character|club|edge|evidence|fan|letter|lock|maximum|novel|option|pack|park|plenty|quarter|skin|sort|weight|baby|background|carry|dish|factor|fruit|glass|joint|master|muscle|red|strength|traffic|trip|vegetable|appeal|chart|gear|ideal|kitchen|land|log|mother|net|party|principle|relative|sale|season|signal|spirit|street|tree|wave|belt|bench|commission|copy|drop|minimum|path|progress|project|sea|south|status|stuff|ticket|tour|angle|blue|breakfast|confidence|daughter|degree|doctor|dot|dream|duty|essay|father|fee|finance|hour|juice|luck|milk|mouth|peace|pipe|stable|storm|substance|team|trick|afternoon|bat|beach|blank|catch|chain|consideration|cream|crew|detail|gold|interview|kid|mark|mission|pain|pleasure|score|screw|sex|shop|shower|suit|tone|window|agent|band|bath|block|bone|calendar|candidate|cap|coat|contest|corner|court|cup|district|door|east|finger|garage|guarantee|hole|hook|implement|layer|lecture|lie|manner|meeting|nose|parking|partner|profile|rice|routine|schedule|swimming|telephone|tip|winter|airline|bag|battle|bed|bill|bother|cake|code|curve|designer|dimension|dress|ease|emergency|evening|extension|farm|fight|gap|grade|holiday|horror|horse|host|husband|loan|mistake|mountain|nail|noise|occasion|package|patient|pause|phrase|proof|race|relief|sand|sentence|shoulder|smoke|stomach|string|tourist|towel|vacation|west|wheel|wine|arm|aside|associate|bet|blow|border|branch|breast|brother|buddy|bunch|chip|coach|cross|document|draft|dust|expert|floor|god|golf|habit|iron|judge|knife|landscape|league|mail|mess|native|opening|parent|pattern|pin|pool|pound|request|salary|shame|shelter|shoe|silver|tackle|tank|trust|assist|bake|bar|bell|bike|blame|boy|brick|chair|closet|clue|collar|comment|conference|devil|diet|fear|fuel|glove|jacket|lunch|monitor|mortgage|nurse|pace|panic|peak|plane|reward|row|sandwich|shock|spite|spray|surprise|till|transition|weekend|welcome|yard|alarm|bend|bicycle|bite|blind|bottle|cable|candle|clerk|cloud|concert|counter|flower|grandfather|harm|knee|lawyer|leather|load|mirror|neck|pension|plate|purple|ruin|ship|skirt|slice|snow|specialist|stroke|switch|trash|tune|zone|anger|award|bid|bitter|boot|bug|camp|candy|carpet|cat|champion|channel|clock|comfort|cow|crack|engineer|entrance|fault|grass|guy|is|are|has|get|see|need|know|would|find|take|want|does|learn|become|come|include|thank|provide|create|add|understand|consider|choose|develop|remember|determine|grow|allow|supply|bring|improve|maintain|begin|exist|tend|enjoy|perform|decide|identify|continue|protect|require|occur|write|approach|avoid|prepare|build|achieve|believe|receive|seem|discuss|realize|contain|follow|refer|solve|describe|prefer|prevent|discover|ensure|expect|invest|reduce|speak|appear|explain|explore|involve|lose|afford|agree|hear|remain|represent|apply|forget|recommend|rely|vary|generate|obtain|accept|communicate|complain|depend|enter|happen|indicate|suggest|survive|appreciate|compare|imagine|manage|differ|encourage|expand|prove|react|recognize|relax|replace|borrow|earn|emphasize|enable|operate|reflect|send|anticipate|assume|engage|enhance|examine|install|participate|intend|introduce|relate|settle|smell|assure|attract|distribute|overcome|owe|succeed|suffer|throw|acquire|adapt|adjust|argue|arise|confirm|encouraging|incorporate|justify|organize|ought|possess|relieve|retain|shut|calculate|compete|consult|deliver|extend|investigate|negotiate|qualify|retire|rid|weigh|arrive|attach|behave|celebrate|convince|disagree|establish|ignore|imply|insist|pursue|remaining|specify|warn|accuse|admire|admit|adopt|announce|apologize|approve|attend|belong|commit|criticize|deserve|destroy|hesitate|illustrate|inform|manufacturing|persuade|pour|propose|remind|shall|submit|suppose|translate|be|have|use|make|look|help|go|being|think|read|keep|start|give|play|feel|put|set|change|say|cut|show|try|check|call|move|pay|let|increase|turn|ask|buy|guard|hold|offer|travel|cook|dance|excuse|live|purchase|deal|mean|fall|produce|search|spend|talk|upset|tell|cost|drive|support|remove|return|run|appropriate|reserve|leave|reach|rest|serve|watch|charge|break|stay|visit|affect|cover|report|rise|walk|pick|lift|mix|stop|teach|concern|fly|born|gain|save|stand|fail|lead|listen|worry|express|handle|meet|release|sell|finish|press|ride|spread|spring|wait|display|flow|hit|shoot|touch|cancel|cry|dump|push|select|conflict|die|eat|fill|jump|kick|pass|pitch|treat|abuse|beat|burn|deposit|print|raise|sleep|advance|connect|consist|contribute|draw|fix|hire|join|kill|sit|tap|win|attack|claim|drag|drink|guess|pull|wear|wonder|count|doubt|feed|impress|repeat|seek|sing|slide|strip|wish|collect|combine|command|dig|divide|hang|hunt|march|mention|survey|tie|escape|expose|gather|hate|repair|scratch|strike|employ|hurt|laugh|lay|respond|split|strain|struggle|swim|train|wash|waste|convert|crash|fold|grab|hide|miss|permit|quote|recover|resolve|roll|sink|slip|suspect|swing|twist|concentrate|estimate|prompt|refuse|regret|reveal|rush|shake|shift|shine|steal|suck|surround|bear|dare|delay|hurry|invite|kiss|marry|pop|pray|pretend|punch|quit|reply|resist|rip|rub|smile|spell|stretch|tear|wake|wrap|was|like|even|film|water|been|well|were|example|own|study|must|form|air|place|number|part|field|fish|process|heat|hand|experience|job|book|end|point|type|value|body|market|guide|interest|state|radio|course|company|price|size|card|list|mind|trade|line|care|group|risk|word|force|light|name|school|amount|order|practice|research|sense|service|piece|web|boss|sport|page|term|test|answer|sound|focus|matter|soil|board|oil|picture|access|garden|open|range|rate|reason|according|site|demand|exercise|image|case|cause|coast|age|boat|record|result|section|building|mouse|cash|class|dry|plan|store|tax|involved|side|space|rule|weather|figure|man|model|source|earth|program|design|feature|purpose|question|rock|act|birth|dog|object|scale|sun|fit|note|profit|related|rent|speed|style|war|bank|content|craft|bus|exchange|eye|fire|position|pressure|stress|advantage|benefit|box|complete|frame|issue|limited|step|cycle|face|interested|metal|paint|review|room|screen|structure|view|account|ball|concerned|discipline|ready|share|balance|bit|black|bottom|gift|impact|machine|shape|tool|wind|address|average|career|culture|pot|sign|table|task|condition|contact|credit|egg|hope|ice|network|separate|attempt|date|effect|link|perfect|post|star|voice|challenge|friend|warm|brush|couple|exit|experienced|function|lack|plant|spot|summer|taste|theme|track|wing|brain|button|click|correct|desire|fixed|foot|gas|influence|notice|rain|wall|base|damage|distance|pair|staff|sugar|target|text|author|complicated|discount|file|ground|lesson|officer|phase|reference|register|secure|sky|stage|stick|title|trouble|advanced|bowl|bridge|campaign|club|edge|evidence|fan|letter|lock|option|organized|pack|park|quarter|skin|sort|weight|baby|carry|dish|exact|factor|fruit|muscle|traffic|trip|appeal|chart|gear|land|log|lost|net|season|spirit|tree|wave|belt|bench|closed|commission|copy|drop|firm|frequent|progress|project|stuff|ticket|tour|angle|blue|breakfast|doctor|dot|dream|essay|father|fee|finance|juice|luck|milk|mixed|mouth|pipe|please|stable|storm|team|amazing|bat|beach|blank|busy|catch|chain|cream|crew|detail|detailed|interview|kid|mark|pain|pleasure|score|screw|sex|sharp|shop|shower|suit|tone|window|wise|band|bath|block|bone|calendar|candidate|cap|coat|contest|court|cup|district|finger|garage|guarantee|hole|hook|implement|layer|lecture|lie|married|narrow|nose|partner|profile|rice|schedule|telephone|tip|bag|battle|bed|bill|bother|cake|code|curve|dimension|ease|farm|fight|gap|grade|horse|host|husband|loan|mistake|nail|noise|occasion|package|pause|phrase|race|sand|sentence|shoulder|smoke|stomach|string|surprised|towel|vacation|wheel|arm|associate|bet|blow|border|branch|breast|buddy|bunch|chip|coach|cross|document|draft|dust|floor|golf|habit|iron|judge|knife|landscape|league|mail|mess|parent|pattern|pin|pool|pound|request|salary|shame|shelter|shoe|tackle|tank|trust|assist|bake|bar|bell|bike|blame|brick|chair|closet|clue|collar|comment|conference|devil|diet|fear|fuel|glove|jacket|lunch|monitor|mortgage|nurse|pace|panic|peak|provided|reward|row|sandwich|shock|spite|spray|surprise|till|transition|weekend|yard|alarm|bend|bicycle|bite|blind|bottle|cable|candle|clerk|cloud|concert|counter|dirty|flower|grandfather|harm|knee|lawyer|load|loose|mirror|neck|pension|plate|pleased|proposed|ruin|ship|skirt|slice|snow|stroke|switch|tired|trash|tune|worried|zone|anger|award|bid|boot|bug|camp|candy|carpet|cat|champion|channel|clock|comfort|cow|crack|disappointed|empty|engineer|entrance|fault|grass|guy|highlight|island|joke|jury|leg|lip|mate|nerve|passage|pen|pride|priest|promise|resort|ring|roof|rope|sail|scheme|script|slight|smart|sock|station|toe|tower|truck|witness

rinciple|relative|sale|season|sign
essay|father|fee|finance|hour|ju
y|sex|shop|shower|suit|tone|win
king|partner|profile|rice|routine|
host|husband|loan|mistake|mou
r|branch|breast|brother|buddy|b
|shoe|silver|tackle|tank|trust|as
pite|spray|surprise|till|transition|
ip|skirt|slice|snow|specialist|stro

fund|take|want|does|learn|becom

swimming-wonder.com taletalk-alarm.com testreveal-designer.com title-smart-media.com towelbecome-maintenance.com video-drink-enthusiasm.com wall-mortgage.com layer-run-river.com knee-communicate.com dimension-retain.com drawer-proposed.com earth-apologize.com metal-range-point.com relative-walk.com relation-happen.com spitepack-goal.com town-reason-knowledge.com gate-boot-ability.com key-sentence.com golf-cash-spirit.com handpin-airconsider.com hook-carpet-difference.com hook-provide.com hostspace-tank.com husband-champion.com image-meet-sex.com user-survey-medicine.com demand-foot-company.com mistake-adopt.com accident-sharp.com ambition-court.com amount-drive.com problemcoat-weight.com reading-persuade.com red-base-chance.com request-finance.com research-spot.com shame-show-cream.com size-lost-park.com space-belt-rate.com timetengstell.com standardsucceed.com star-appear-map.com strategy-borrow.com term-cow-record.com tongue-warm-funeral.com traffic-insist.com troubleabuse.com uncle-officer.com uncle-structure.com university-spread.com vehicleroof-entrance.com weekend-chart.com wheel-suggest.com winner-care-sir.com throat-prefer.com document-boss.com brain-tune-influence.com guarantee-value.com quarter-smell.com lady-sandwich.com challengediscover.com brother-hang.com bend-shoot-stress.com wall-bottle-assistant.com plane-branch.com plateadvanced.com pleasurerepair.com pot-blank-text.com poundresort-skin.com professorloose.com programcredit.com

[Tea|bag] Syntax

Counts the number of surrounding domains matching some predicates

[a_0,..., a_n:T|ρ]

- Go through all remaining domains within timestamp±T
- Keep those that match in all properties a_0,..., a_n with the current domain.
- Keep those that fulfil ρ
- Return the number of remaining elements

[client:1h|d0 = 'com'] >= 20

Observe:
Linnea syntax is much shorter, though less flexible.

However, flexible enough to capture all the malware types we've found so far

```
...
FROM (
    SELECT COUNT(d0 = 'com') OVER (PARTITION BY d.dst ORDER BY d.timestamp
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING) AS number_1
    FROM (
        ...
    )
)
WHERE number_1 >= 20
```

- Keep those that match in all properties a_0,..., a
  the current domain.
- Keep those that fulfil ρ
- Return the number of remaining elements

[client:1h|d0 = 'com'] >= 20

```
...
FROM (
    SELECT COUNT(d0 = 'com') OVER (PARTITION BY d.dst ORDER BY d.timestamp
        RANGE BETWEEN INTERVAL '1 hour' PRECEDING AND INTERVAL '1 hour' FOLLOWING) AS number_1
    FROM (
        ...
    )
)
WHERE number_1 >= 20
```

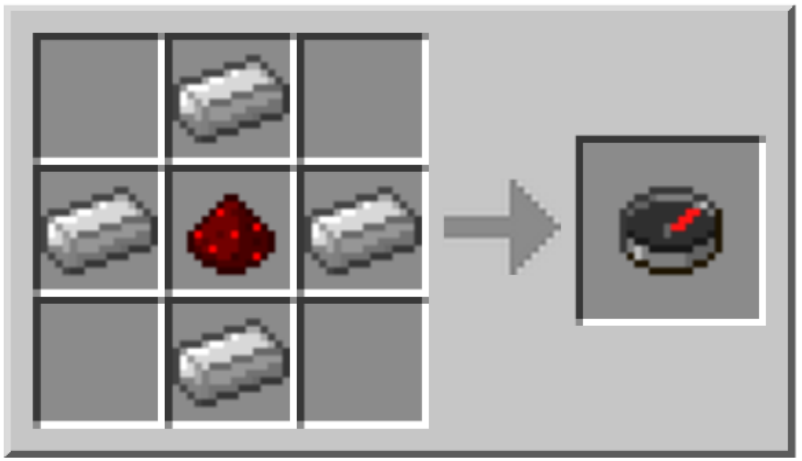
Ob
Lin
tha

Ho
cap
we

Observe:
Linnea syntax is much shorter, though less flexible.

However, flexible enough to capture all the malware types we've found so far

So How Do I Craft A Linnea Rule?



1st Layer: fast to compute

- non-resolving (=NXDOMAIN)
- allowed characters
- allowed 2-lengths
- allowed suffixes

} Regex

- min. num. of certain characters
- ...

2nd Layer: slower to compute

- min. num. within timeframe
- min. num. with hyphens
- min. num. with numbers
- max. num. with certain suffix
- ...

1st Layer: fast to compute

non-resolving (=NXDOMAIN)
allowed characters
allowed 2-lengths
allowed suffixes
} Regex
min. num. of certain characters
...

Also, avoid confusion with other malware families

2nd Layer: slower to compute

min. num. within timeframe
min. num. with hyphens
min. num. with numbers
max. num. with certain suffix
...

Also, avoid confusion with other malware families

1st Layer: fast to compute

non-resolving (=NXDOMAIN)
allowed characters
allowed 2-lengths
allowed suffixes
} Regex
min. num. of certain characters
...

Also, avoid confusion with other malware families

2nd Layer: slower to compute

min. num. within timeframe
min. num. with hyphens
min. num. with numbers
max. num. with certain suffix
...

New-DGA-v1

0e5da2e5.com 0e5da2e5.net
0e5da2e5.info 042d5450.com
042d5450.net 042d5450.info
64ef65d5.com 64ef65d5.net
64ef65d5.info 7ca407e9.com
7ca407e9.net 7ca407e9.info 1f204bf7.com
1f204bf7.net 1f204bf7.info 55bd934a.com
55bd934a.net 55bd934a.info

New-DGA-v1

```
{
   timestamp >= t0 - 2h, timestamp <= t0,
   nxdomain,
   match(domain, '^[a-f0-9]{8}\.(com|info|net)$')
},
{
   [client:1h| [client,d1:1h|true] >= 2 ] >= 10
}
```

At least 10 queries that have a counterpart with a different suffix but with same d_1

Pushdo

www.tafelxofomy.kz www.myxabuchuva.kz
www.watalasogec.kz www.sudeqobhewaf.kz
www.zosuxaxekyd.kz www.pamusafvokpe.kz
www.xuruwokafgo.kz www.vumuccersop.kz
www.xudokcesesj.kz www.wunxucyabo.kz
www.perocuncokwu.kz www.kujegobbopfo.kz
www.vakugoxutazq.kz www.duqjuclaco.kz
www.zyahyifopve.kz www.qubopacedovy.kz
www.dehazloples.kz www.xervuzyafe.kz
www.vunmelfeme.kz www.copaxudoxaf.kz
www.jocejezxula.kz www.magedavokruh.kz
www.mazuxepelve.kz www.cyifobcoje.kz
www.xotucvalyaj.kz www.dosaftequdex.kz
www.gexyojawaxer.kz www.decowakolufo.kz
www.mafazqazbuc.kz www.zyajobjapat.kz

Pushdo

```
{
   timestamp >= t0 - 2h, timestamp <= t0,
   nxdomain,
   match(domain, '^(www\.)?[a-z]{9,12}\.(com|in|info|kz|net)$'),
   count(d1, '[aeiou]') / l1 > 0.35
},
{
   [client:1h|true] >= 20,
   [client:1h|d0 in 'com','in','info','net'] < [client:1h|d0='kz']
}
```

Include non-kz-domains

Prevent confusion with Flashfake

Bankpatch, Bedep, Conficker, DGA10, Dyre, Expiro, Matsnu, New-DGA-V1, Necurs, Pitou, Pushdo, Pykspa, Ramdo, Runforestrun, Shiotob, SillyFDC.

https://github.com/EyeOfPython/Linnea

Our environment for 11th August 2015:

- 18 million NXDOMAIN entries
- 308k distinct by 69k clients
- Vertica DB on a HP DL30 configuration

Execution times, 2h timeslots:
Max: 2.1 s
Min: 0.9 s
Mean for all 16 rules: 19.3 s

Results:

- Independent analysis (by eye): 10/16 malware families present
- All detected by the queries.
- Clients: 2 FN, 1 FP
- 72 clients correctly identified

Our environment for 11th August 2015:

- 18 million NXDOMAIN entries
- 308k distinct by 69k clients
- Vertica DB on a HP DL30 configuration

Execution times, 2h timeslots:
Max: 2.1 s
Min: 0.9 s
Mean for all 16 rules: 19.3 s

Results:

- Independent analysis (by eye): 10/16 malware families present
- All detected by the queries.
- Clients: 2 FN, 1 FP
- 72 clients correctly identified

How do we compare?

VS machine learning, pure SQL, lexical analysis

+

- Can tell you type of malware
- Transparent: No fuzzy classifier
- Writing Linnea rules isn't too difficult (compared to pure SQL)

–

- Only for known malware
- Have to design a rule for each malware by hand

Pros occupy more area than cons
=> Our stuff is clearly very good.

Thank you for your attention!