Internal Domain Names

Chen Zheng Wei
George Chen

BSides Singapore 2022

Disclaimer: The views expressed herein are those of the presenters and they do not reflect the views of their employers.

Agenda

- Background
- Discovery
- Sample Capture Logs
- Key Observations
- Status
- Triage & Response Quadrant
- “Am I Vulnerable?”
- Remediation
- Challenges
- Next Steps

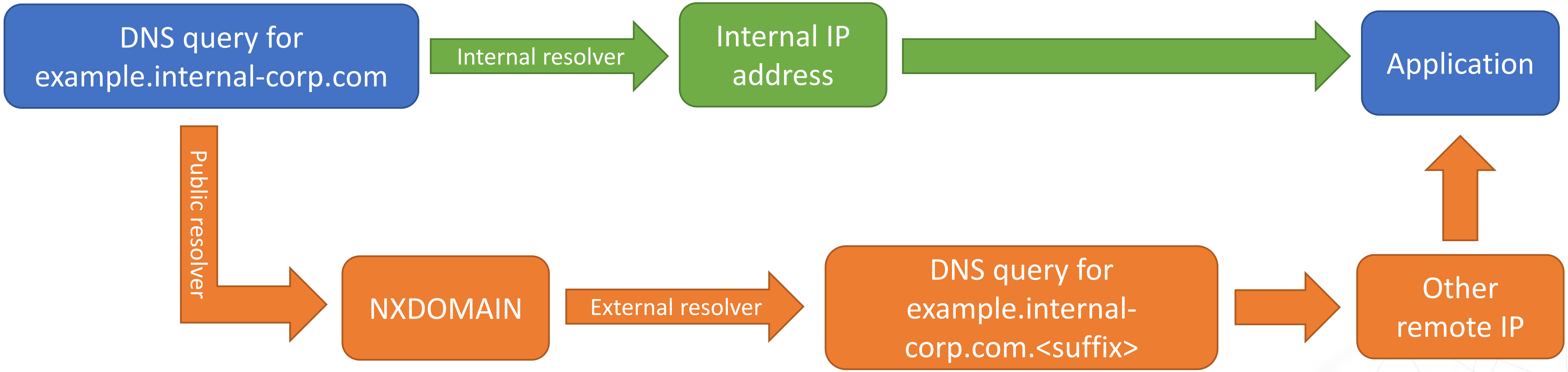
Background

- Domain Name System (DNS)
- "Labels" in DNS (RFC1034 / 1035)
  - <label1>.<label2>.<labelN>.<TLD>
- example – single-label name
- intranet.example.com - unqualified multi-label name
- intranet.example.com. - fully-qualified multi-label name

Background

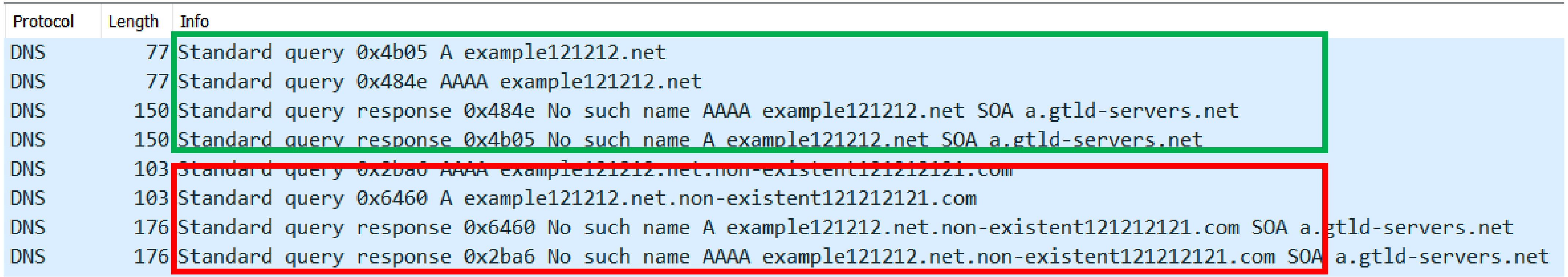
- DNS search suffix
  - DHCP option codes 15 or 119
- Use-cases:
  - Browsing shortcuts: http[:]//go/<shortlink> - popularly used in many internal networks
  - Internal sync clients referencing non-qualified hostnames
  - etc.
- But what happens if you are not connected to your corporate network?

Background


DNS query for example.internal-corp.com
Internal resolver
Internal IP address
Application
Public resolver
NXDOMAIN
External resolver
DNS query for example.internal-corp.com.<suffix>
Other remote IP

Background

Original query/response



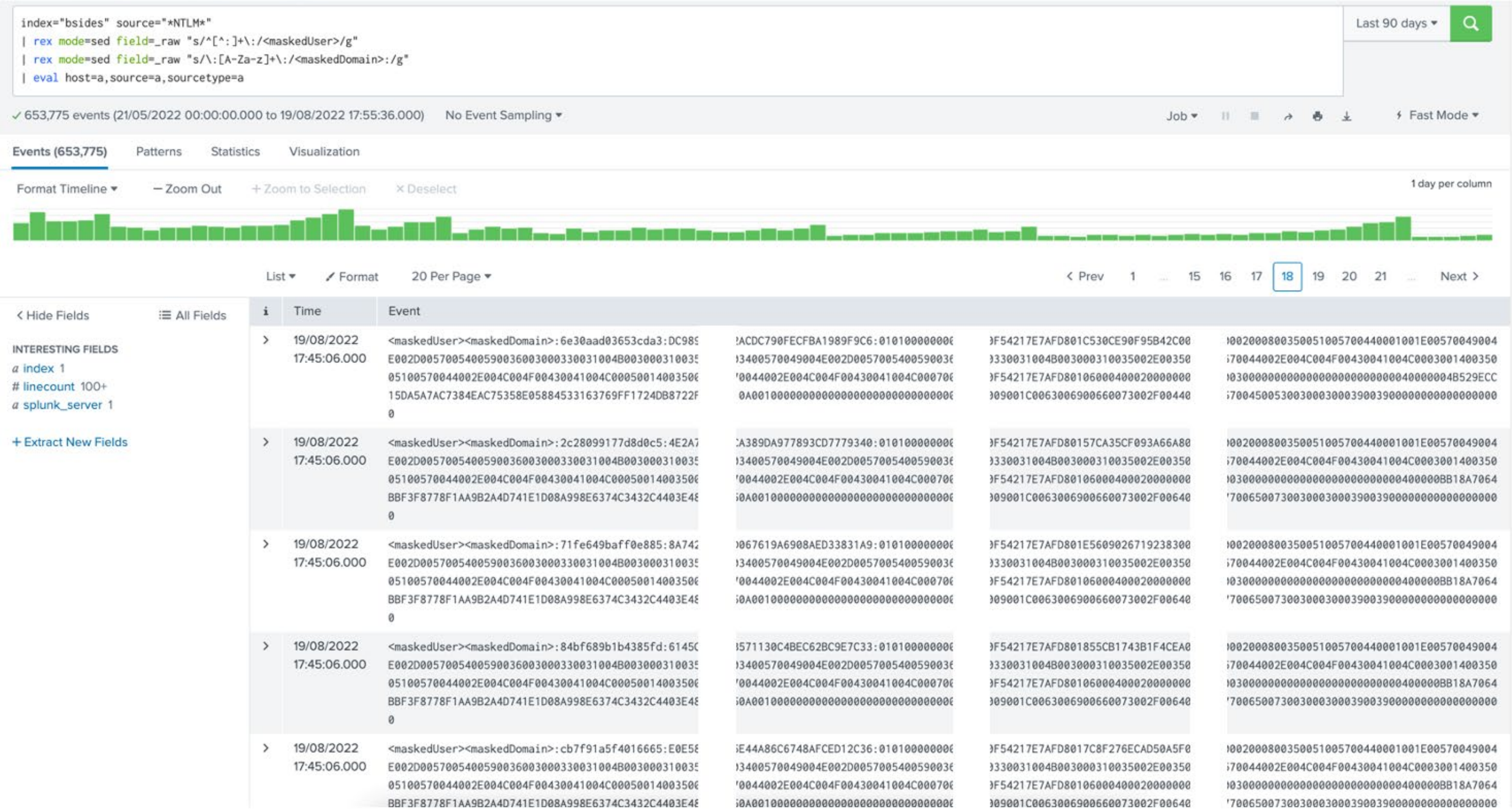
Protocol	Length	Info
DNS	77	Standard query 0x4b05 A example121212.net
DNS	77	Standard query 0x484e AAAA example121212.net
DNS	150	Standard query response 0x484e No such name AAAA example121212.net SOA a.gtld-servers.net
DNS	150	Standard query response 0x4b05 No such name A example121212.net SOA a.gtld-servers.net
DNS	103	Standard query 0x2ba6 AAAA example121212.net.non-existent121212121.com
DNS	103	Standard query 0x6460 A example121212.net.non-existent121212121.com
DNS	176	Standard query response 0x6460 No such name A example121212.net.non-existent121212121.com SOA a.gtld-servers.net
DNS	176	Standard query response 0x2ba6 No such name AAAA example121212.net.non-existent121212121.com SOA a.gtld-servers.net

Subsequent query/response

Discovery

- Initial discovery: own network
- We started registering domains (observed suffixes) and listening to traffic
- Expansion:
  - open data set (ie. Alexa's -> bulk domain check)
  - guess work from certain patterns (~50% hit rate)
  - traffic observation from our domains above
- Domains -> non-disclosure
  - example.internal-corp.com.suffixdomain.com
- Misconfig: browser, OS, network, router, ISP
- 7k+ entities sending unintended traffic to us

Sample Captured Logs



```
index="bsides" source="*NTLM*"
| rex mode=sed field=_raw "s/^[^:]+\:/<maskedUser>/g"
| rex mode=sed field=_raw "s/\:[A-Za-z]+\:/<maskedDomain>:/g"
| eval host=a,source=a,sourcetype=a
```

Last 90 days ▾

✓ 653,775 events (21/05/2022 00:00:00.000 to 19/08/2022 17:55:36.000) No Event Sampling ▾

Job ▾ Fast Mode ▾

Events (653,775) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column

List ▾ Format 20 Per Page ▾ ‹ Prev 1 … 15 16 17 18 19 20 21 … Next ›

‹ Hide Fields ☰ All Fields

INTERESTING FIELDS

a index 1

linecount 100+

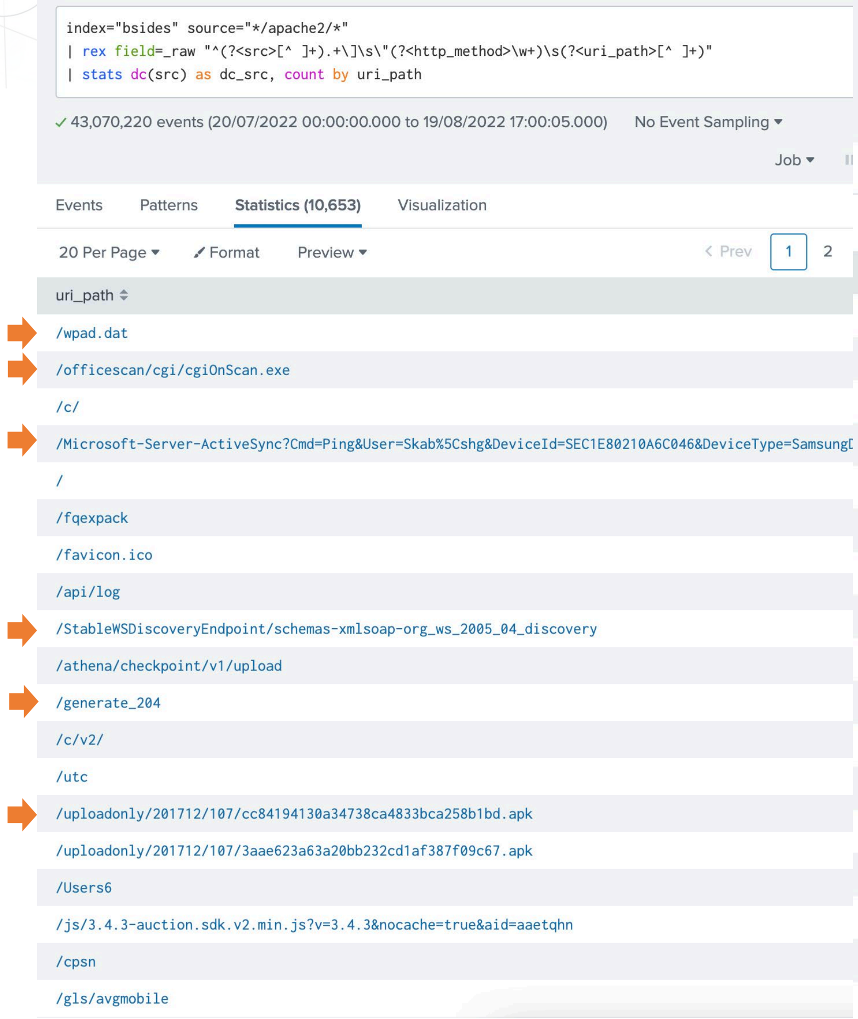
a splunk_server 1

+ Extract New Fields

```
i  Time           Event
›  19/08/2022     <maskedUser><maskedDomain>:6e30aad03653cda3:DC989   2ACDC790FECFBA1989F9C6:010100000000   0F54217E7AFD801C530CE90F95B42C00   0002000800350051005700440001001E00570049004
   17:45:06.000   E002D0057005400590036003000330031004B003000310035   03400570049004E002D0057005400590036   0330031004B003000310035002E00350   570044002E004C004F00430041004C0003001400350
                  05100570044002E004C004F00430041004C00050014003500   70044002E004C004F00430041004C000700   0F54217E7AFD80106000400020000000   0030000000000000000000000000040000004B529ECC
                  15DA5A7AC7384EAC75358E05884533163769FF1724DB8722F   0A00100000000000000000000000000000   009001C0063006900660073002F00440   570045005300300030003900390000000000000000000
                  0
›  19/08/2022     <maskedUser><maskedDomain>:2c28099177d8d0c5:4E2A7   CA389DA977893CD7779340:010100000000   0F54217E7AFD80157CA35CF093A66A80   0002000800350051005700440001001E00570049004
   17:45:06.000   E002D0057005400590036003000330031004B003000310035   03400570049004E002D0057005400590036   0330031004B003000310035002E00350   570044002E004C004F00430041004C0003001400350
                  05100570044002E004C004F00430041004C00050014003500   70044002E004C004F00430041004C000700   0F54217E7AFD80106000400020000000   00300000000000000000000000000400000BB18A7064
                  BBF3F8778F1AA9B2A4D741E1D08A998E6374C3432C4403E48   50A00100000000000000000000000000000   009001C0063006900660073002F00640   7006500730030003000390039000000000000000000
                  0
›  19/08/2022     <maskedUser><maskedDomain>:71fe649baff0e885:8A742   0067619A6908AED33831A9:010100000000   0F54217E7AFD801E5609026719238300   0002000800350051005700440001001E00570049004
   17:45:06.000   E002D0057005400590036003000330031004B003000310035   03400570049004E002D0057005400590036   0330031004B003000310035002E00350   570044002E004C004F00430041004C0003001400350
                  05100570044002E004C004F00430041004C00050014003500   70044002E004C004F00430041004C000700   0F54217E7AFD80106000400020000000   00300000000000000000000000000400000BB18A7064
                  BBF3F8778F1AA9B2A4D741E1D08A998E6374C3432C4403E48   50A00100000000000000000000000000000   009001C0063006900660073002F00640   7006500730030003000390039000000000000000000
                  0
›  19/08/2022     <maskedUser><maskedDomain>:84bf689b1b4385fd:6145C   3571130C4BEC62BC9E7C33:010100000000   0F54217E7AFD801855CB1743B1F4CEA0   0002000800350051005700440001001E00570049004
   17:45:06.000   E002D0057005400590036003000330031004B003000310035   03400570049004E002D0057005400590036   0330031004B003000310035002E00350   570044002E004C004F00430041004C0003001400350
                  05100570044002E004C004F00430041004C00050014003500   70044002E004C004F00430041004C000700   0F54217E7AFD80106000400020000000   00300000000000000000000000000400000BB18A7064
                  BBF3F8778F1AA9B2A4D741E1D08A998E6374C3432C4403E48   50A00100000000000000000000000000000   009001C0063006900660073002F00640   7006500730030003000390039000000000000000000
                  0
›  19/08/2022     <maskedUser><maskedDomain>:cb7f91a5f4016665:E0E58   5E44A86C6748AFCED12C36:010100000000   0F54217E7AFD8017C8F276ECAD50A5F0   0002000800350051005700440001001E00570049004
   17:45:06.000   E002D0057005400590036003000330031004B003000310035   03400570049004E002D0057005400590036   0330031004B003000310035002E00350   570044002E004C004F00430041004C0003001400350
                  05100570044002E004C004F00430041004C00050014003500   70044002E004C004F00430041004C000700   0F54217E7AFD80106000400020000000   00300000000000000000000000000400000BB18A7064
                  BBF3F8778F1AA9B2A4D741E1D08A998E6374C3432C4403E48   50A00100000000000000000000000000000   009001C0063006900660073002F00640   7006500730030003000390039000000000000000000
```

George

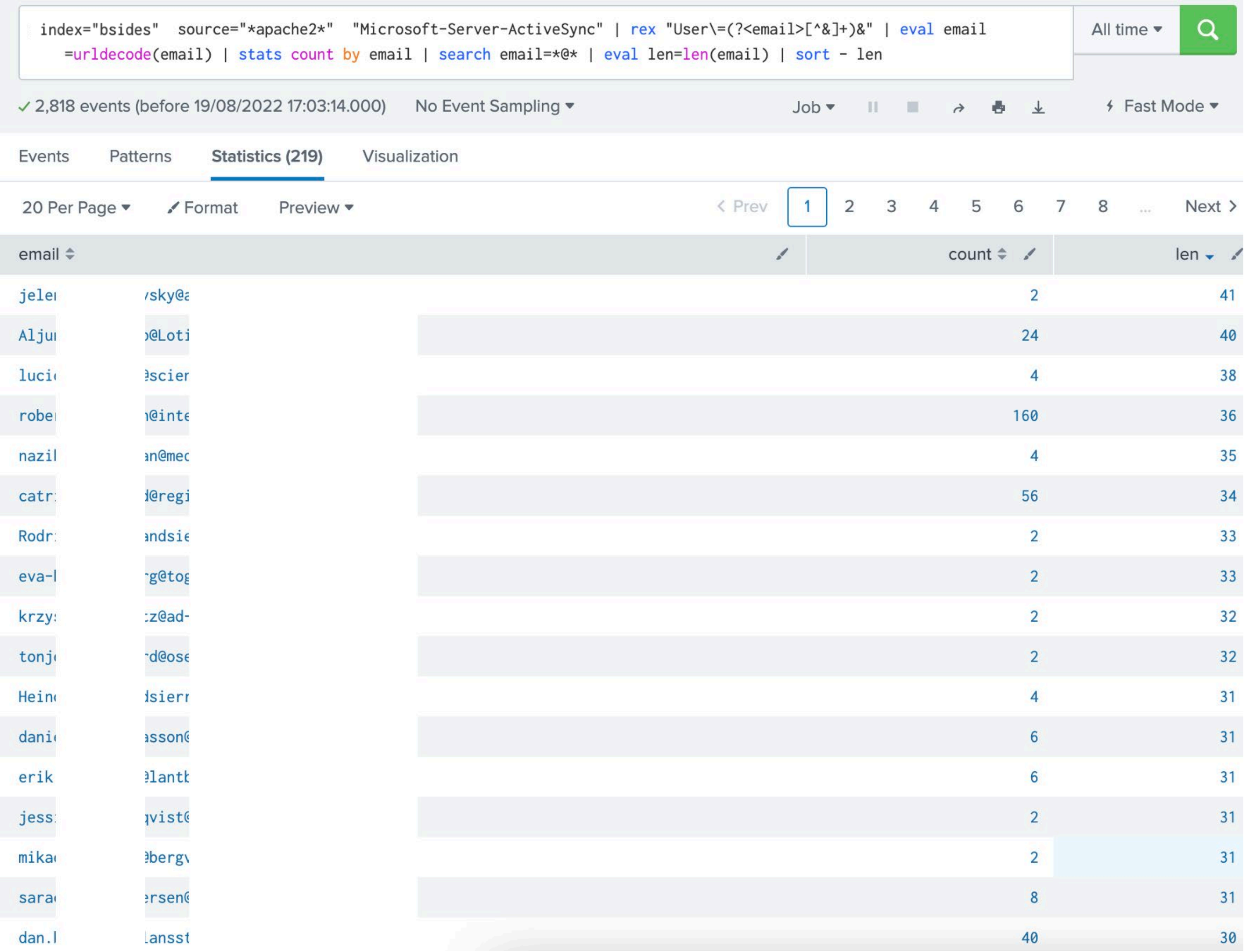
Sample Captured Logs



```
index="bsides" source="*/apache2/*"
| rex field=_raw "^(?<src>[^ ]+).+\]\s\"(?<http_method>\w+)\s(?<uri_path>[^ ]+)"
| stats dc(src) as dc_src, count by uri_path
```

✓ 43,070,220 events (20/07/2022 00:00:00.000 to 19/08/2022 17:00:05.000) No Event Sampling ▾

uri_path
/wpad.dat
/officescan/cgi/cgiOnScan.exe
/c/
/Microsoft-Server-ActiveSync?Cmd=Ping&User=Skab%5Cshg&DeviceId=SEC1E80210A6C046&DeviceType=SamsungD
/
/fqexpack
/favicon.ico
/api/log
/StableWSDiscoveryEndpoint/schemas-xmlsoap-org_ws_2005_04_discovery
/athena/checkpoint/v1/upload
/generate_204
/c/v2/
/utc
/uploadonly/201712/107/cc84194130a34738ca4833bca258b1bd.apk
/uploadonly/201712/107/3aae623a63a20bb232cd1af387f09c67.apk
/Users6
/js/3.4.3-auction.sdk.v2.min.js?v=3.4.3&nocache=true&aid=aaetqhn
/cpsn
/gls/avgmobile



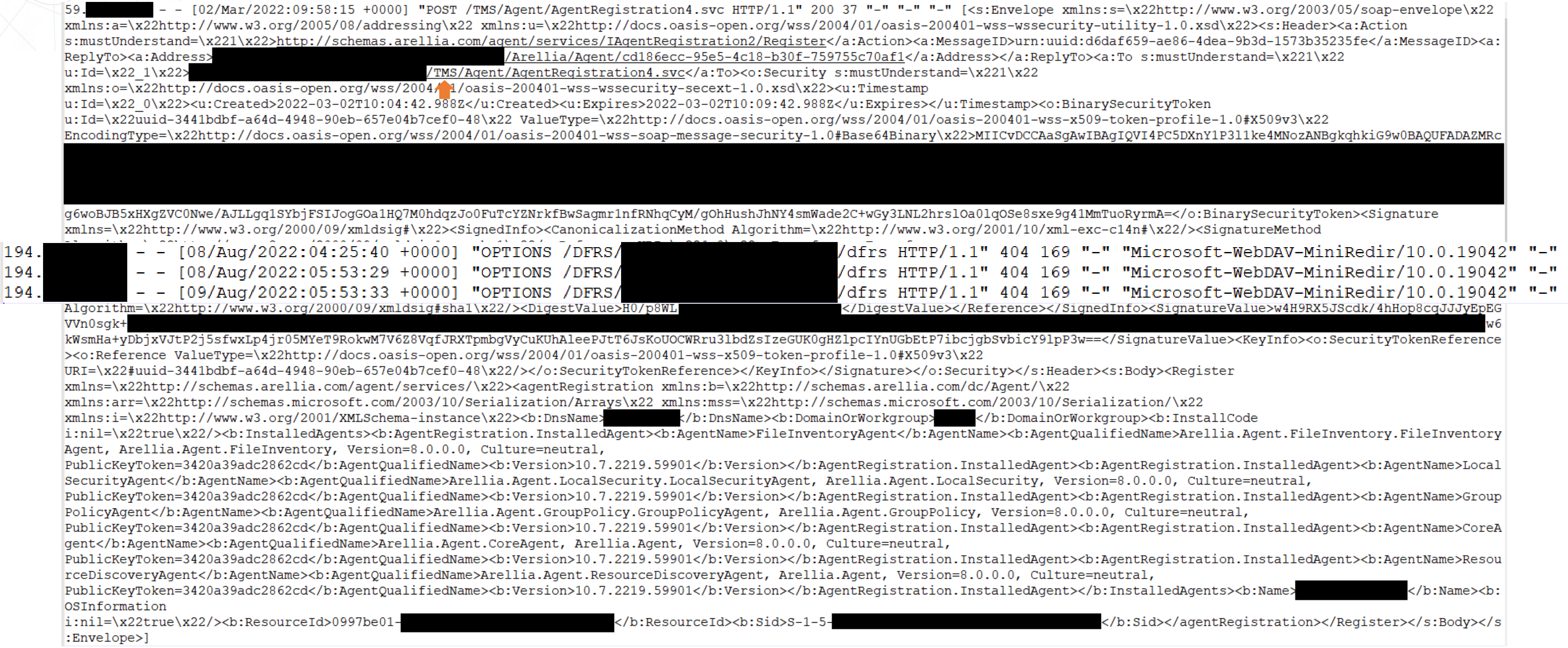
```
index="bsides"  source="*apache2*"  "Microsoft-Server-ActiveSync" | rex "User\=(?<email>[^&]+)&" | eval email
   =urldecode(email) | stats count by email | search email=*@* | eval len=len(email) | sort - len
```

✓ 2,818 events (before 19/08/2022 17:03:14.000) No Event Sampling ▾

email	count	len
jelei [redacted] /sky@a	2	41
Aljui [redacted])@Loti	24	40
luci [redacted] ?scier	4	38
robei [redacted] 1@inte	160	36
nazil [redacted] an@mec	4	35
catr [redacted] d@regi	56	34
Rodr [redacted] andsie	2	33
eva-l [redacted] rg@tog	2	33
krzy [redacted] :z@ad-	2	32
tonj [redacted] rd@ose	2	32
Hein [redacted] dsierr	4	31
dani [redacted] asson@	6	31
erik [redacted] ?lantb	6	31
jess [redacted] qvist@	2	31
mika [redacted] ?bergv	2	31
sara [redacted] ersen@	8	31
dan.l [redacted] .ansst	40	30

George

Sample Captured Logs



```
59.[redacted] - - [02/Mar/2022:09:58:15 +0000] "POST /TMS/Agent/AgentRegistration4.svc HTTP/1.1" 200 37 "-" "-" "-" [<s:Envelope xmlns:s=\x22http://www.w3.org/2003/05/soap-envelope\x22
xmlns:a=\x22http://www.w3.org/2005/08/addressing\x22 xmlns:u=\x22http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd\x22><s:Header><a:Action
s:mustUnderstand=\x221\x22>http://schemas.arellia.com/agent/services/IAgentRegistration2/Register</a:Action><a:MessageID>urn:uuid:d6daf659-ae86-4dea-9b3d-1573b35235fe</a:MessageID><a:
ReplyTo><a:Address>[redacted]/Arellia/Agent/cd186ecc-95e5-4c18-b30f-759755c70af1</a:Address></a:ReplyTo><a:To s:mustUnderstand=\x221\x22
u:Id=\x22_1\x22>[redacted]/TMS/Agent/AgentRegistration4.svc</a:To><o:Security s:mustUnderstand=\x221\x22
xmlns:o=\x22http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd\x22><u:Timestamp
u:Id=\x22_0\x22><u:Created>2022-03-02T10:04:42.988Z</u:Created><u:Expires>2022-03-02T10:09:42.988Z</u:Expires></u:Timestamp><o:BinarySecurityToken
u:Id=\x22uuid-3441bdbf-a64d-4948-90eb-657e04b7cef0-48\x22 ValueType=\x22http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3\x22
EncodingType=\x22http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary\x22>MIICvDCCAaSgAwIBAgIQVI4PC5DXnY1P3l1ke4MNozANBgkqhkiG9w0BAQUFADAZMRc
[redacted]
g6woBJB5xHXgZVC0Nwe/AJLLgq1SYbjFSIJogGOa1HQ7M0hdqzJo0FuTcYZNrkfBwSagmr1nfRNhqCyM/gOhHushJhNY4smWade2C+wGy3LNL2hrslOa0lqOSe8sxe9g41MmTuoRyrmA=</o:BinarySecurityToken><Signature
xmlns=\x22http://www.w3.org/2000/09/xmldsig#\x22><SignedInfo><CanonicalizationMethod Algorithm=\x22http://www.w3.org/2001/10/xml-exc-c14n#\x22/><SignatureMethod
```

```
194.[redacted] - - [08/Aug/2022:04:25:40 +0000] "OPTIONS /DFRS/[redacted]/dfrs HTTP/1.1" 404 169 "-" "Microsoft-WebDAV-MiniRedir/10.0.19042" "-"
194.[redacted] - - [08/Aug/2022:05:53:29 +0000] "OPTIONS /DFRS/[redacted]/dfrs HTTP/1.1" 404 169 "-" "Microsoft-WebDAV-MiniRedir/10.0.19042" "-"
194.[redacted] - - [09/Aug/2022:05:53:33 +0000] "OPTIONS /DFRS/[redacted]/dfrs HTTP/1.1" 404 169 "-" "Microsoft-WebDAV-MiniRedir/10.0.19042" "-"
```

```
Algorithm=\x22http://www.w3.org/2000/09/xmldsig#sha1\x22/><DigestValue>H0/p8WL[redacted]</DigestValue></Reference></SignedInfo><SignatureValue>w4H9RX5JScdk/4hHop8cqJJJyEpEG
VVn0sgk+[redacted]w6
kWsmHa+yDbjxVJtP2j5sfwxLp4jr05MYeT9RokwM7V6Z8VqfJRXTpmbgVyCuKUhAleePJtT6JsKoUOCWRru3lbdZsIzeGUK0gHZlpcIYnUGbEtP7ibcjgbSvbicY9lpP3w==</SignatureValue><KeyInfo><o:SecurityTokenReference
><o:Reference ValueType=\x22http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3\x22
URI=\x22#uuid-3441bdbf-a64d-4948-90eb-657e04b7cef0-48\x22/></o:SecurityTokenReference></KeyInfo></Signature></o:Security></s:Header><s:Body><Register
xmlns=\x22http://schemas.arellia.com/agent/services/\x22><agentRegistration xmlns:b=\x22http://schemas.arellia.com/dc/Agent/\x22
xmlns:arr=\x22http://schemas.microsoft.com/2003/10/Serialization/Arrays\x22 xmlns:mss=\x22http://schemas.microsoft.com/2003/10/Serialization/\x22
xmlns:i=\x22http://www.w3.org/2001/XMLSchema-instance\x22><b:DnsName>[redacted]</b:DnsName><b:DomainOrWorkgroup>[redacted]</b:DomainOrWorkgroup><b:InstallCode
i:nil=\x22true\x22/><b:InstalledAgents><b:AgentRegistration.InstalledAgent><b:AgentName>FileInventoryAgent</b:AgentName><b:AgentQualifiedName>Arellia.Agent.FileInventory.FileInventory
Agent, Arellia.Agent.FileInventory, Version=8.0.0.0, Culture=neutral,
PublicKeyToken=3420a39adc2862cd</b:AgentQualifiedName><b:Version>10.7.2219.59901</b:Version></b:AgentRegistration.InstalledAgent><b:AgentRegistration.InstalledAgent><b:AgentName>Local
SecurityAgent</b:AgentName><b:AgentQualifiedName>Arellia.Agent.LocalSecurity.LocalSecurityAgent, Arellia.Agent.LocalSecurity, Version=8.0.0.0, Culture=neutral,
PublicKeyToken=3420a39adc2862cd</b:AgentQualifiedName><b:Version>10.7.2219.59901</b:Version></b:AgentRegistration.InstalledAgent><b:AgentRegistration.InstalledAgent><b:AgentName>Group
PolicyAgent</b:AgentName><b:AgentQualifiedName>Arellia.Agent.GroupPolicy.GroupPolicyAgent, Arellia.Agent.GroupPolicy, Version=8.0.0.0, Culture=neutral,
PublicKeyToken=3420a39adc2862cd</b:AgentQualifiedName><b:Version>10.7.2219.59901</b:Version></b:AgentRegistration.InstalledAgent><b:AgentRegistration.InstalledAgent><b:AgentName>CoreA
gent</b:AgentName><b:AgentQualifiedName>Arellia.Agent.CoreAgent, Arellia.Agent, Version=8.0.0.0, Culture=neutral,
PublicKeyToken=3420a39adc2862cd</b:AgentQualifiedName><b:Version>10.7.2219.59901</b:Version></b:AgentRegistration.InstalledAgent><b:AgentRegistration.InstalledAgent><b:AgentName>Resou
rceDiscoveryAgent</b:AgentName><b:AgentQualifiedName>Arellia.Agent.ResourceDiscoveryAgent, Arellia.Agent, Version=8.0.0.0, Culture=neutral,
PublicKeyToken=3420a39adc2862cd</b:AgentQualifiedName><b:Version>10.7.2219.59901</b:Version></b:AgentRegistration.InstalledAgent></b:InstalledAgents><b:Name>[redacted]</b:Name><b:
OSInformation
i:nil=\x22true\x22/><b:ResourceId>0997be01-[redacted]</b:ResourceId><b:Sid>S-1-5-[redacted]</b:Sid></agentRegistration></Register></s:Body></s
:Envelope>]
```

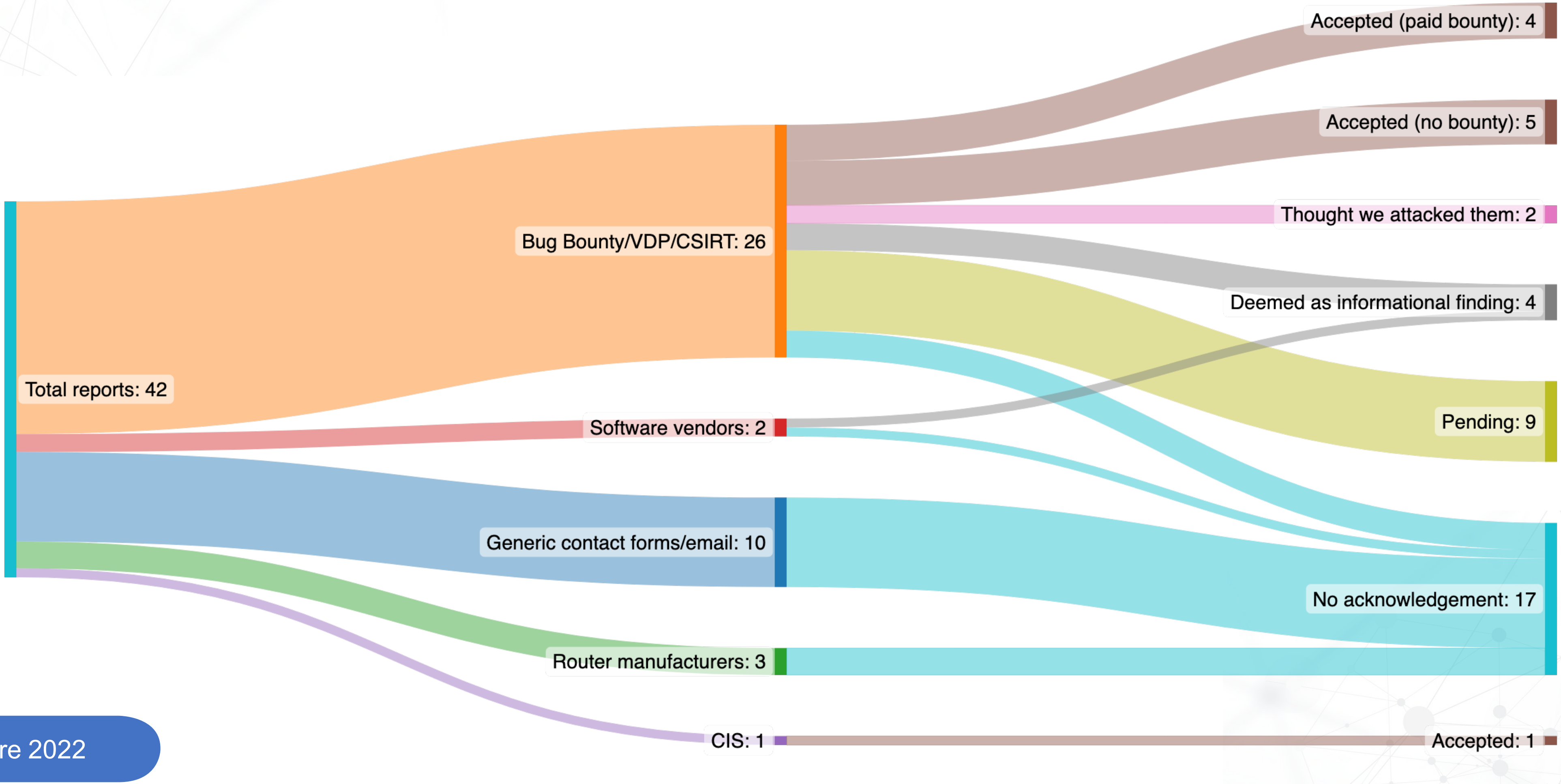
George

Key Observations & Impact

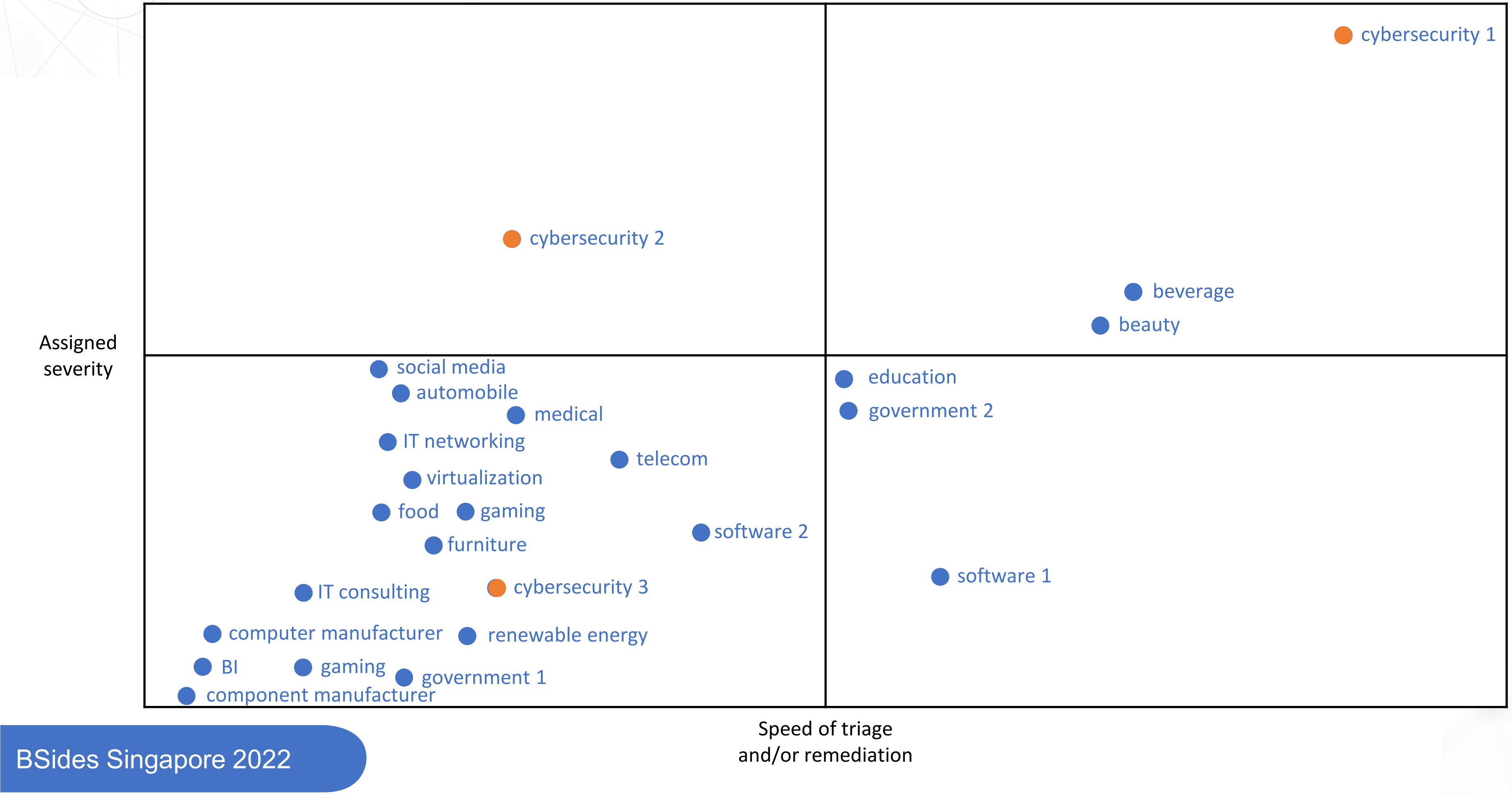
Observations	Potential Impact (we did not attempt these or send anything back)
NTLM v1 & v2 hashes	Offline password cracking. Password reuse. MitM relay attack by network attackers for authentication.
Internal paths, subdomains, asset names, software used, file names	Information disclosure.
Metadata, such as user email addresses and IDs, phone details, locations	Information disclosure.
Request for objects, such as wpad.dat, installers, SCCM deployments, status updates for AV	Adding a proxy layer, serving malware/configuration files.
Error dumps	Information disclosure.
Malware traffic	We’ve also seen expired malware domains, one of which we took over.
HTTP cookies and request bodies	Session hijacking. MitM. Information disclosure.
Update-polling, such as ActiveSync	Sending fake updates.

George

Status


Total reports: 42
Bug Bounty/VDP/CSIRT: 26
Software vendors: 2
Generic contact forms/email: 10
Router manufacturers: 3
CIS: 1
Accepted (paid bounty): 4
Accepted (no bounty): 5
Thought we attacked them: 2
Deemed as informational finding: 4
Pending: 9
No acknowledgement: 17
Accepted: 1

Triage & Response Quadrant



BSides Singapore 2022

BSidesSG

George

“Am I Vulnerable?"

- DNS logs: <your organization domain>.<TLD>.<wildcard>
- Detection / Hunting (Splunk & ELK)

```
index=<dns_logs> domain IN (“<yourCorpDomain1>.*.*”, “<yourCorpDomain2>.*.*”,
(“*.<yourCorpDomain1>.*.*”, “*.<yourCorpDomain2>.*.*”)
| eval list="mozilla"
| `ut_parse(domain,list)`
| stats dc(user) as dc_user values(domain) as domain count by ut_domain
```

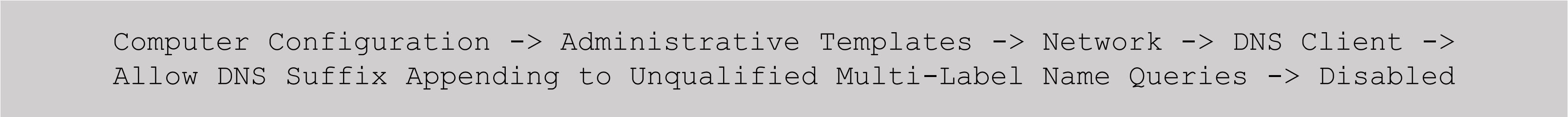
```
query: "<yourCorpDomain>.*.*"
```

- PowerShell (Get-DnsClient):

```
Invoke-Command –ComputerName <remote host> -ScriptBlock {Get-DnsClient}
```

Recommendations

- Windows: deploy the follow GPO to endpoints:

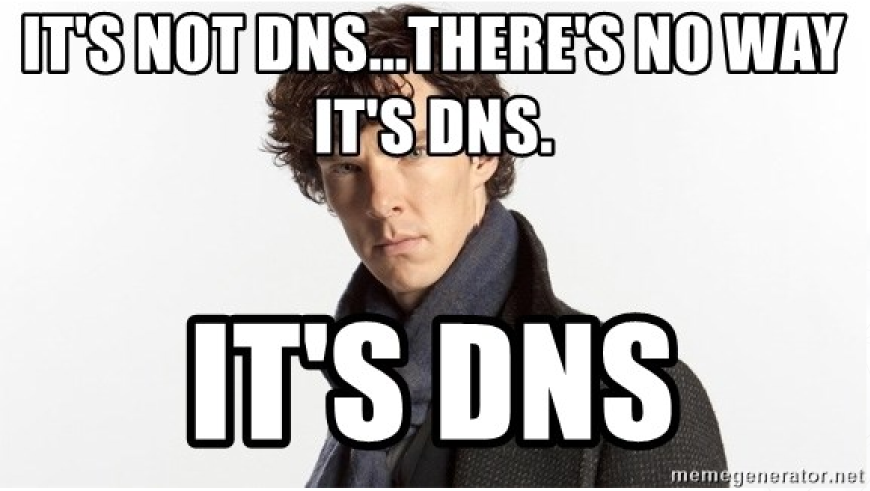


```
Computer Configuration -> Administrative Templates -> Network -> DNS Client ->
Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries -> Disabled
```

- Chrome (and Chromium): set BuiltInDnsClientEnabled to false
- RFC6762 – Home users need to replace it with .local, .internal, .localhost, .invalid, .intranet, .private, .home
- Enterprise should use their corp domain (assuming it's registered).
- Employees should exercise caution when connecting their work devices to an unknown network

Challenges

- Difficulty in explaining risks to companies
  - no public writeups
  - only a minority of companies recognised the risk
- Various root causes coupled with the complexity of different environments
- Inconsistent triage, especially for bug bounty



Next Steps

- Continue to work with vendors/service providers
- Offer domain-transfer to respective “misconfiguration owners”
- Next part of research
    - taking over more expired malware domains and observing traffic

Internal Domain Names

Chen Zheng Wei <zwc299@protonmail.com>

George Chen <thrunter@proton.me>

Writeup: medium.com/@chenzw/internal-domain-names-f1cd2886c654