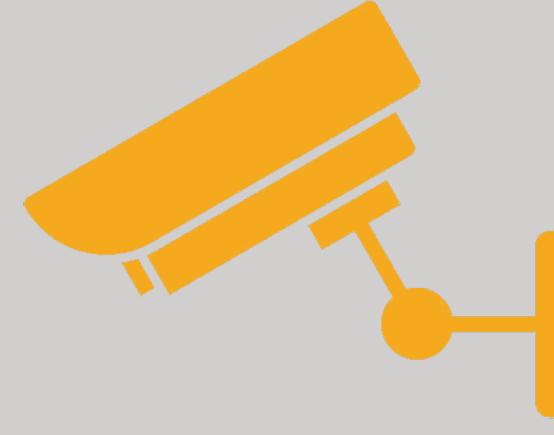


"Everything you touch
leaves a trace"-
Locard's Exchange
Principle



What We Can Find for You?

-> **File & Document Activity:** opened/modified/deleted files, recovered deleted files, download activity.

-> **Application Usage:** executed programs, first/last run times, frequency, detection of hacking tools.

-> **User Account Activity:** logins, remote access attempts, password changes, suspicious accounts.

-> **Internet & Cloud Activity:** browser history, search terms, cookies, cloud sync activity.

-> **USB & External Devices:** device identification, timestamps, drive letters, user association.

-> **System Timeline Reconstruction:** chronological sequence of system events.

TECHNICAL CHEAT SHEET Capabilities -> Tools -> Artifacts

| Capability | Tool | Artifact |
|----------------------------|---------------------------|----------------------------------|
| Recent file access | Registry Explorer | RecentDocs, OpenSaveMRU |
| Deleted file recovery | Recycle Bin parsing | \$I/\$R files |
| Browser downloads | Hindsight / Browser DBs | Chrome History, downloads.sqlite |
| Program execution | WinPrefetchView / PECmd | Prefetch files (.pf) |
| App install/uninstall | Registry Explorer | SOFTWARE Hive Uninstall Keys |
| User application activity | Registry Explorer | UserAssist, BAM/DAM |
| Local accounts/login times | Registry Explorer | SAM Hive |
| Remote Desktop activity | Event Log Explorer | IDs 4624, 4625, 4778, 4779 |
| Browser activity | Hindsight, SQLite tools | History DBs |
| Cloud sync evidence | Registry tools | Cloud logs + registry entries |
| Folder browsing | Shellbag Explorer | Shellbags |
| Shortcut tracking | LNK parsers | .lnk files |
| Task/file access history | Jump List tools | AutomaticDestinations |
| USB device identification | Registry Explorer | USBSTOR |
| USB timestamps | Registry Explorer | GUID keys 0064/0066/0067 |
| USB user association | Registry Explorer | NTUSER.DAT MountPoints2 |
| Timeline creation | PECmd + Timeline Explorer | Prefetch timeline |
| Network usage | SRUM parser | SRUDB.dat |
| Wireless activity | Event Log Explorer | WLAN-AutoConfig log |

Investigation 2

HTTP Analysis

The screenshot displays two separate instances of the Elastic Stack interface, likely from different browser tabs or windows.

Top Dashboard (HTTPD Log Dashboard):

- Header:** elastic, Dashboards > HTTPD Log Dashboard, Find apps, content, and more.
- Search Bar:** url.domain:"squirreldirectory.com"
- Panel:** HTTPD Discovery (13,857 documents)
- Data Table:** Shows log entries with columns: @timestamp, source.ip, http.request.method, url.domain, url.path, and http.response.status_code. Several rows are highlighted in yellow, indicating matches for the search term "squirreldirectory.com".

Bottom Dashboard (Data View):

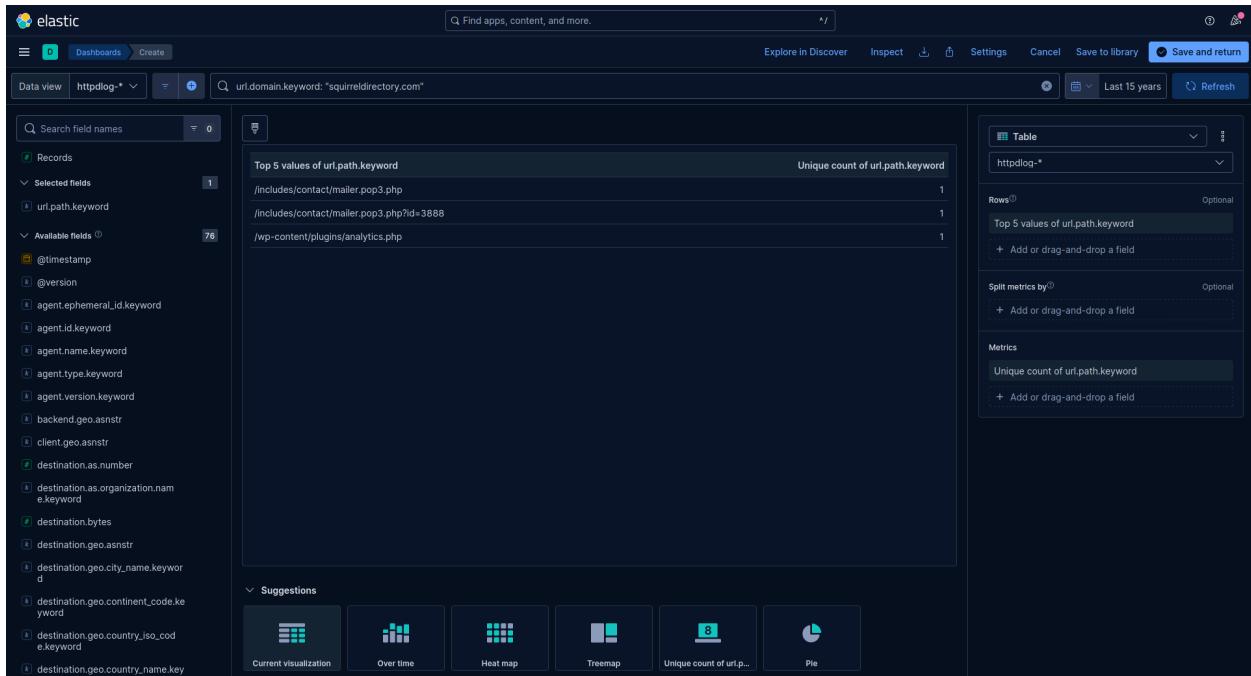
- Header:** elastic, Dashboards > Create, Find apps, content, and more.
- Search Bar:** url.domain.keyword:"squirreldirectory.com"
- Left Panel:** Shows the selected field `source.ip` under `Selected fields`.
- Middle Panel:** Shows a visualization titled "Top 5 values of source.ip" with two results: 172.16.4.10 and 172.16.6.14.
- Right Panel:** Configuration for the visualization, including `Table`, `httpdlog-*`, `Rows` (set to "Top 5 values of source.ip"), `Split metrics by` (optional), and `Metrics` (set to "Unique count of source.ip").

Internal Hosts contacting squirreldirectory.com

172.16.4.10

172.16.6.14

URLs accessed



/wp-content/plugins/analytics.php
/includes/contact/mailer.pop3.php?id=3888
/includes/contact/mailer.pop3.php

User agent strings

The screenshot shows the Elasticsearch Kibana interface. On the left, there's a sidebar with a search bar for 'user_agent.name.keyword' and a list of selected fields: 'source.ip' (2), 'user_agent.name.keyword' (1), and many other available fields like '@timestamp', '@version', 'agent.id.keyword', etc. The main area displays a table titled 'Top 1000 values of user_agent.name.keyword' with columns for 'Top 1000 values of user_agent.name.keyword', 'Top 3 values of source.ip', and 'Count of user_agent.name.keyword'. The table shows data such as 'IE Large Screen' with counts of 7,090 and 6,767 respectively. To the right, there's a visualization builder panel with tabs for 'Table' and 'Rows' (optional), and sections for 'Split metrics by' (optional) and 'Metrics'.

| Top 1000 values of user_agent.name.keyword | Top 3 values of source.ip | Count of user_agent.name.keyword |
|--|---------------------------|----------------------------------|
| IE Large Screen | 172.16.4.10 | 7,090 |
| IE Large Screen | 172.16.6.14 | 6,767 |
| Other | 172.16.4.4 | 878 |
| Other | 172.16.4.10 | 582 |
| Other | 172.16.6.11 | 504 |
| Other | Other | 826 |
| Firefox | 172.16.7.13 | 421 |
| Firefox | 172.16.4.10 | 1 |
| Firefox | 172.16.7.12 | 1 |
| Chrome | 172.16.7.15 | 65 |
| Chrome | 172.16.5.20 | 18 |
| Edge | 172.16.6.11 | 34 |
| Edge | 172.16.5.26 | 20 |
| Edge | 172.16.6.14 | 3 |
| Windows-Update-Agent | 172.16.7.16 | 25 |

IE Large screen was accessed by 172.16.4.10 and 172.16.6.14.

Status Codes

| Top values of url.domain.keyword + 1 other | Count of records |
|---|------------------|
| base-elf › /wsman/SubscriptionManager/WEC | 198 |
| base-elf.shieldbase.lan › /wsman/subscriptions/3CF1C588-5959-4455-8316-5 | 128 |
| base-elf.shieldbase.lan › /wsman/subscriptions/3CF1C588-5959-4455-8316-5 | 37 |
| base-dc › /wsman?PSVersion=5.1.16299.547 | 5 |
| amupdatedl8.microsoft.com › /server/amupdate/amd64/Microsoft/Package/man | 2 |
| amupdatedl4.microsoft.com › /server/amupdate/metadata/UniversalManifest.cat | 1 |
| amupdatedl7.microsoft.com › /server/amupdate/amd64/Microsoft/Package/180 | 1 |

HTTP User Agents

HTTP User Agent Records

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; XBLWP7; ZuneWP7)

Filter for **Filter out**

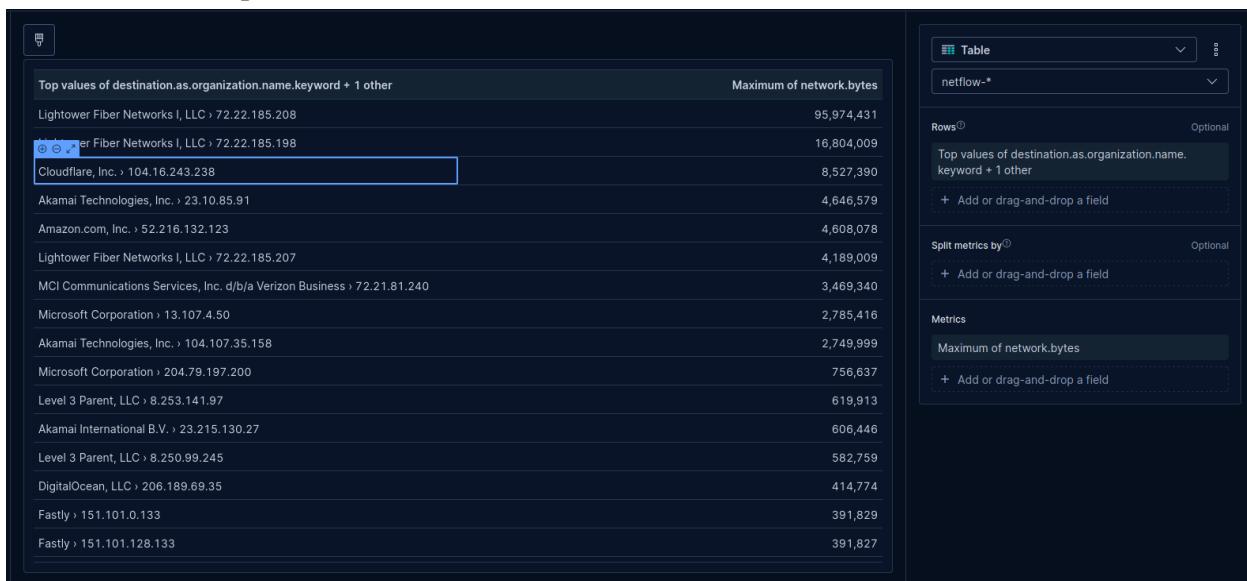
url.domain:"squirreldirectory.com"

NetFlow & Connection Analysis

Top talkers

The top 3 in terms of data volume are 172.16.4.10, 172.16.7.13 and 172.16.4.4. The top 3 in terms of packet count are 172.16.4.10, 172.16.6.14 and 172.16.5.26.

Source destination pairs



In addition to Akamai Cloudflare and DigitalOcean, internal hosts also talked to a number of other hosting companies. These include: fastly, Lighttower Fiber Networks, AppNexus, LeaseWeb, Rocket Fuel and around five others.

There was one record of an internal device talking to a DigitalOcean device in India. This seems a bit odd since all other traffic went to Northwestern Europe or East Asia.

Aside from the ISP, the external host that received the most traffic from the organization was a Cloudflare host at 104.16.243.238. This may be the C2 center. An Akamai host was the runner up receiving about half the traffic. There doesn't appear to be any unencrypted HTTP traffic to either of these hosts.

DNS Analysis

| | |
|--------------------------|--|
| 2018-09-05 08:30:54.431Z | DNS: 172.16.5.28 (client.wns.windows.com A -> wns.notify.windows.com.akadns.net.americas1.notify.windows.com.akadns.net,dm3p.wns.notify.windows.com.akadns.net,52.173.24.17) |
| 2018-09-05 08:30:54.432Z | DNS: 172.16.4.4 (wns.notify.windows.com.akadns.net A -> americas1.notify.windows.com.akadns.net,dm3p.wns.notify.windows.com.akadns.net,52.173.24.17) |
| 2018-09-05 08:30:55.110Z | DNS: 172.16.7.11 (watson.telemetry.microsoft.com A -> modern.watson.data.microsoft.com.akadns.net,40.69.153.67) |

This is an example of legitimate DNS Traffic. The queries represent normal microsoft services and use akadns.net, which is Akamai's DNS infrastructure. There is also a clear response that is not "No response or Reject"

Here is the illegitimate traffic:

| Systlog Discovery | |
|--------------------------|--|
| 16,444 documents | |
| ① @timestamp | ↑ log.syslog.hostname log.syslog.appname |
| ② message | |
| 2018-09-05 08:31:27.231Z | DNS: 172.16.7.15 (88646.internet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:27.232Z | DNS: 172.16.7.15 (76628.internet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:33.231Z | DNS: 172.16.7.15 (88646.extranet.wagonwheelgifts.com A -> Rejected) |
| 2018-09-05 08:31:33.231Z | DNS: 172.16.7.15 (76628.extranet.wagonwheelgifts.com A -> Rejected) |
| 2018-09-05 08:31:33.232Z | DNS: 172.16.4.4 (88646.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:33.232Z | DNS: 172.16.4.4 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:33.232Z | DNS: 172.16.4.4 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:34.231Z | DNS: 172.16.7.15 (88646.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:34.231Z | DNS: 172.16.7.15 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:35.232Z | DNS: 172.16.7.15 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:35.232Z | DNS: 172.16.7.15 (88646.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:36.088Z | DNS: 172.16.4.4 (88646.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:36.088Z | DNS: 172.16.4.4 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:37.232Z | DNS: 172.16.7.15 (76628.extranet.wagonwheelgifts.com A -> No response) |
| 2018-09-05 08:31:37.232Z | DNS: 172.16.7.15 (88646.extranet.wagonwheelgifts.com A -> No response) |

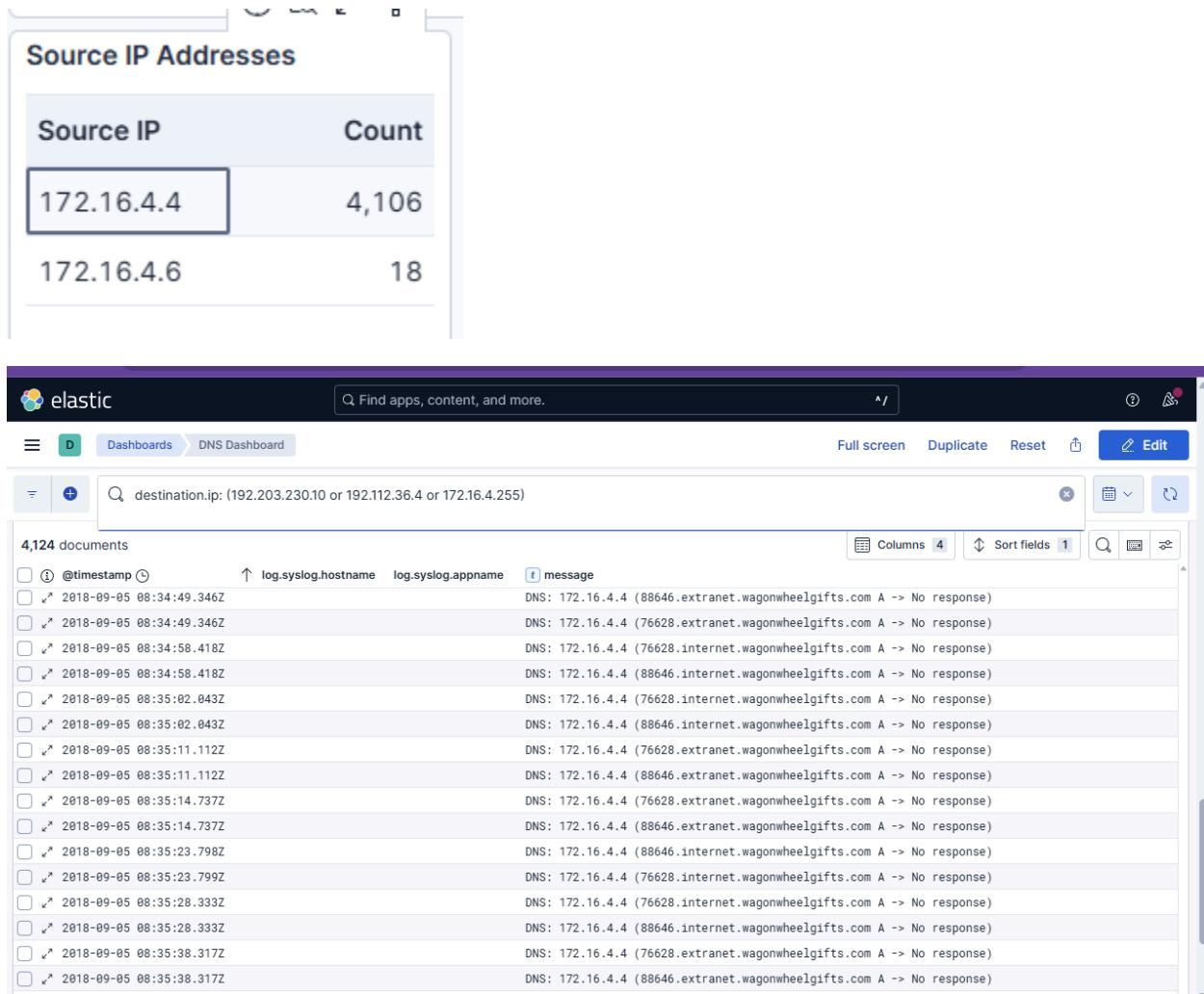
internal hosts such as IPs 172.16.7.15 and 172.16.4.4 are generating the traffic.

| message |
|--|
| DNS: 172.16.7.15 (88646.internet.wagonwheelgifts.com A -> No response) |
| DNS: 172.16.7.15 (76628.internet.wagonwheelgifts.com A -> No response) |
| DNS: 172.16.7.15 (88646.extranet.wagonwheelgifts.com A -> Rejected) |
| DNS: 172.16.7.15 (76628.extranet.wagonwheelgifts.com A -> Rejected) |

These queries all have random prefixes meaning they are likely generated. They also either say

“no response” or “rejected” meaning the DNS resolver couldn’t find a matching record. None of these subdomains actually exist.

This all points to an attacker using a Domain Generator Algorithm which can generate many potential domain names and periodically tries to connect to them until one is registered by its command and control server. This is an automated beaconing attack rather than a legitimate user activity.



Host 172.16.4.4 sent over 4,000 DNS queries directly to root name servers (192.203.230.10, 192.112.36.4) and broadcast address (172.16.4.255). The queries targeted randomized subdomains of wagonwheelgifts.com. This is further evidence of malware beaconing which originated from host 172.16.4.4 (the domain controller).

Cross Log Correlation

Method

We correlated DNS, HTTP, and NetFlow data by matching client IPs (`source.ip`) and timestamps across logs.

This allowed us to trace each host's activity from DNS lookup → connection establishment → HTTP request.

Timeline and Key Findings

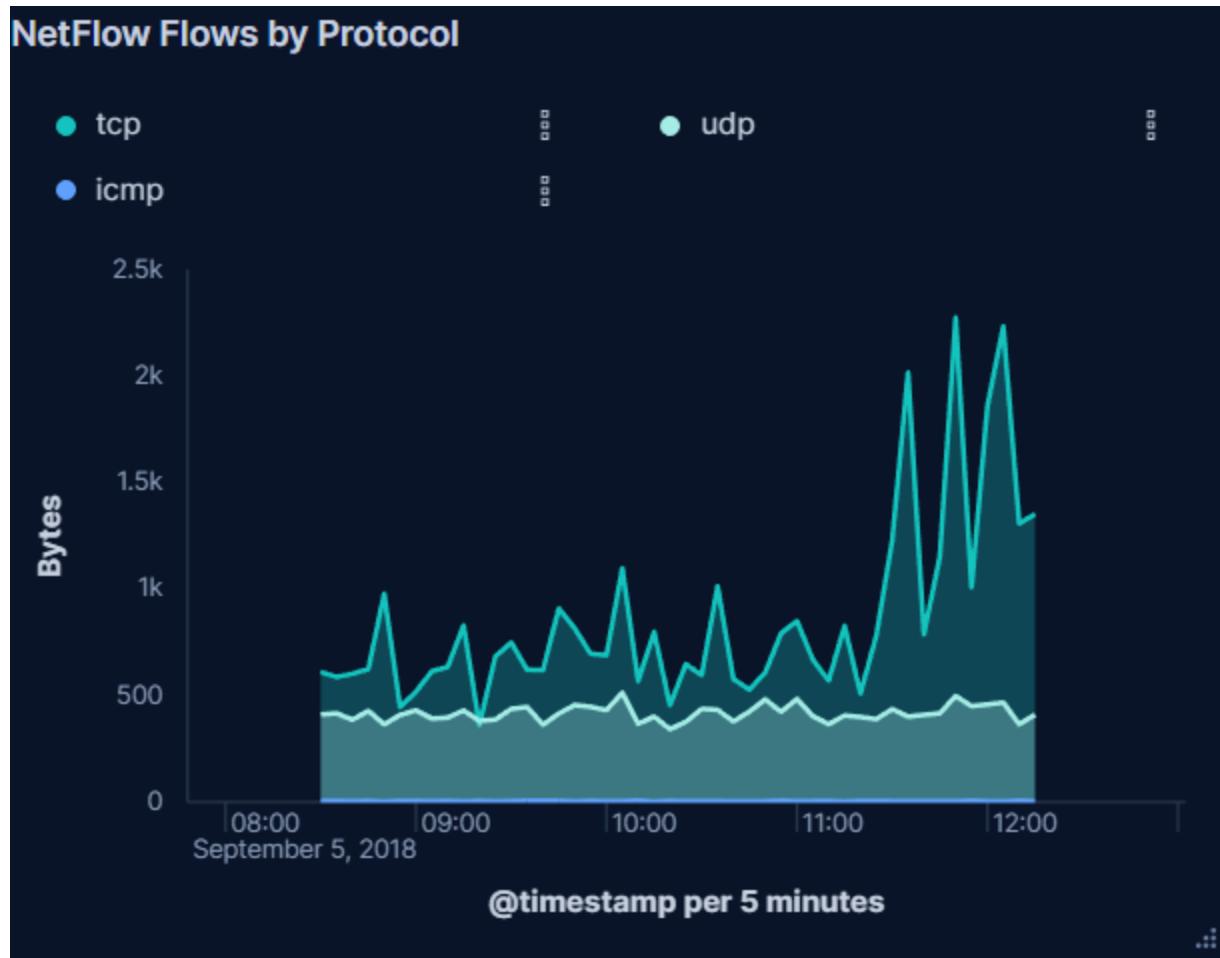
Between **08:30 and 12:20 UTC on 2018-09-05**, two distinct patterns appeared:

1. **High-volume DNS queries** from **172.16.4.4 (domain controller)** and **172.16.7.15 (Windows client)** directed at `*.wagonwheelgifts.com` subdomains, all returning “No response.”
2. **HTTP and NetFlow spikes** beginning around **11:30**, peaking between **11:35–12:05**, mainly from **172.16.6.14 (Windows 10 host “Romanoff”)** and **172.16.4.10 (proxy server)**.

\



The NetFlow timeline (Figure 1) shows these hosts sharply increasing their outbound flows during that same window, while the protocol chart



(Figure 2) confirms the traffic consisted primarily of **TCP and UDP**, typical for HTTP and DNS activity.

Host Behavior Summary

| Host | Role | Observed Services | Domains Queried / Contacted | Behavior Summary |
|------------|----------------------------------|-------------------|--|--|
| 172.16.4.4 | Domain Controller / DNS resolver | DNS | wagonwheelgifts.com, random subdomains | Generated 13k DNS queries including direct root and broadcast requests |

| | | | | |
|-------------------------|-------------------------------------|---------------------|---|--|
| 172.16.7.15 | Segmented workstation | DNS | wagonwheelgifts.com subdomains | 10k+ repetitive failed queries (“No response”), likely infected client generating DGA requests. |
| 172.16.6.14 | Windows 10 workstation (“Romanoff”) | HTTP / HTTPS | squirreldirectory.com | Spikes of HTTP traffic between 11:30–12:05; accessed suspicious PHP scripts using a non-standard user-agent. |
| 172.16.4.10 | Proxy / Squid server | HTTP, RSH (TCP 514) | squirreldirectory.com | Relayed outbound web traffic; user-agent {version:6.2.0.12026, platform:server_win, osversion:10} |
| 172.16.5.x / 6.x | Misc. workstations | DNS / HTTP | Microsoft and Ubuntu domains (tile-service.weather.microsoft.com, daisy.ubuntu.com) | Normal background activity, legitimate update and telemetry traffic. |

Summary

The DGA-like DNS behavior from 172.16.7.15 triggered corresponding load on the domain controller (172.16.4.4), which forwarded many of those requests externally.

Later, around 11:30 UTC, HTTP and NetFlow activity from 172.16.6.14 and 172.16.4.10 spiked, coinciding with connections to squirreldirectory.com, a known malicious host.

This correlation across DNS, HTTP, and NetFlow logs strongly indicates a malware infection using domain-generation and HTTP beaconing mechanisms for command-and-control communication.