



MikroTik and Behaviour based IDS

Paul Greeff
support@lucidview.net

Contents

1. Who are we
2. The problem
3. Case 1: Malware and persistent connections
4. Case 2: Malware mechanism
5. LucidView Made for Mikrotik
6. Combatting untrustworthy connections
7. MikroTik Enforcer Portal by LucidView
8. Thank you



Who are we



<https://www.lucidview.net>



Inappropriate content

Statistics

50% of kids admit to viewing adult, violent or sexual content

80% of kids 11 - 17 social media broke rules and signed up too young/

Cyber bullying etc.

Provide visibility

Source

<https://www.telegraph.co.uk/news/2016/04/04/half-of-children-view-adult-or-violent-material-online-says-poll/>

<http://yourekavach.com/blog/wp-content/uploads/2015/06/1226418744-Mother-and-son.jpg>

https://smallbiztrends.com/wp-content/uploads/2016/05/shutterstock_311472353-850x476.jpg

The problem

2018 Incident Highlights

- 95% of breaches could have been prevented (ISOC)
- 3.2% decrease in reported breach incidents (RBS)
- 5 billion records exposed. (RBS)
- \$8 billion financial impact of ransomware (CV)
- 12% rise in business targeted ransomware (Symantec)
- \$12.5 billion in global EAC/BEC losses since 2013 (FBI)



<https://mybroadband.co.za/news/security/334570-wannacry-was-the-top-ransomware-of-2019.html>
<https://www.cybervision.co.za/articles-city-of-johannesburg-suffers-ransomware-attack/>
<https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/>

The problem

City Power 2019 - ransom data (July and October)

"We have dozens of back doors inside your city. We have control of everything in your city. We also compromised all passwords and sensitive data such as finance and personal population information," reads the ransom note

Liberty - ransom database

Wannacry top ransomware of 2019



<https://www.fin24.com/Companies/ICT/lazarus-group-behind-recent-cyberattack-on-south-africa-kaspersky-20190814>

<https://www.lucidview.net/the-prevalence-of-ransomware/>

<https://www.cybersecurity-insiders.com/liberty-insurance-of-south-africa-becomes-cyber-attack-victim/>

<https://www.scmagazineuk.com/johannesburg-city-ransomware-attack-again/article/1663733>

Case 1: Malware and persistent connections

Complaint

Slow Internet

Slow services

Dropped connections

Queued emails

Mail servers not accepting mails



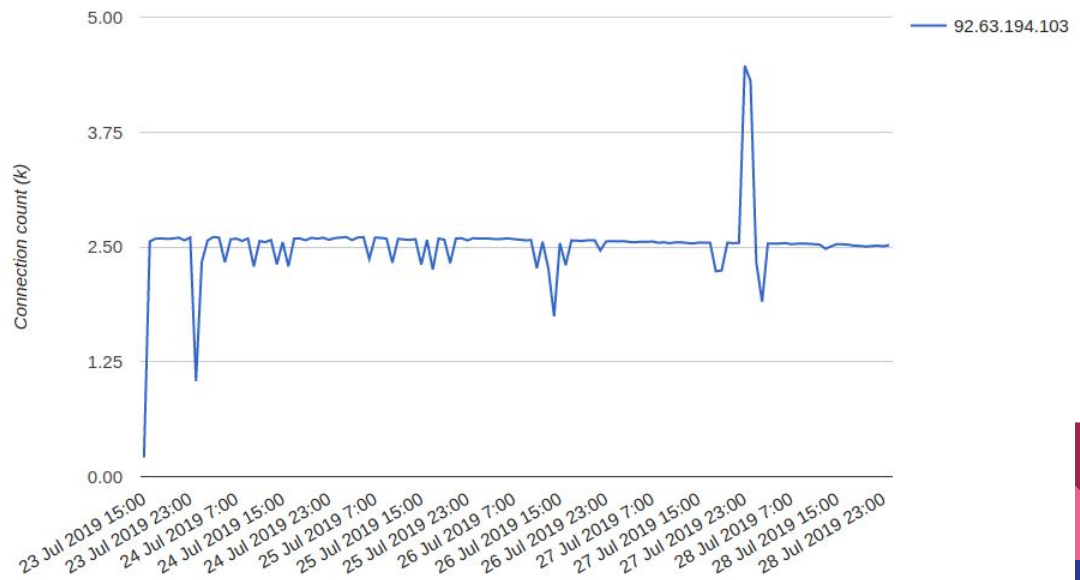
Line Chart: Top Categories - Weekly

The Line Chart illustrates the top categories in connection count



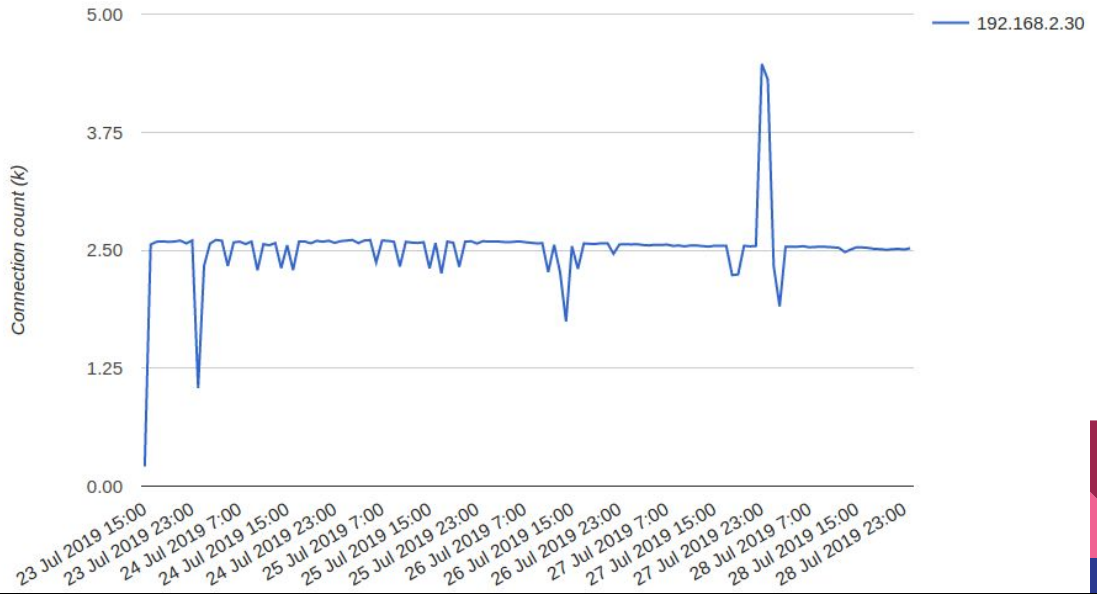
Line Chart: Suspicious Host - Weekly

This Line Chart shows the "Suspicious" host and the connections made



Line Chart:: Source IP - Weekly


This Line Chart shows the Source IP that: "Suspicious" source is connecting to.



Wannacry infection located and eliminated on infected hosts.

This IP address has been reported a total of **123** times from 20 distinct sources. 92.63.194.103 was first reported on March 11th 2019, and the most recent report was **4 months ago**.

Old Reports: The most recent abuse report for this IP address is from **4 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	↑↓ Date	↑↓ Comment	Categories
✓ lequanglam	11 Sep 2019	Bruteforcing port 3389 (Remote Desktop) - Exceed maximum 10 attempts/hour	Port Scan Brute-Force
✓ etu brutus	10 Sep 2019	19/9/10@04:10:37: FAIL: Alarm-Intrusion address from=92.63.194.103 ...	Hacking Brute-Force IoT Targeted
✓ RoboSOC	07 Sep 2019	Honeypot attack, port: 445, PTR: PTR record not found	Hacking
 bSebring	07 Sep 2019	09/07/2019-19:00:00.463789 92.63.194.103 Protocol: 6 ET SCAN NMAP -sS window 1024	Port Scan
✓ NotACaptcha	07 Sep 2019	Unauthorised access (Sep 7) SRC=92.63.194.103 LEN=40 TTL=243 ID=31690 TCP DPT=445 WINDOW=1024 SYN	Port Scan

<https://www.abuseipdb.com/check/92.63.194.103>

Case 1: Malware and persistent connections

Cause of symptoms

Malware infected host on VMWare server, impacting other hosts - WannaCry ransomware cryptoworm.

Infected host goes down and has to be rebuild due to infection

Mail server goes down due to infection

Wannacry - " It propagated through EternalBlue, an exploit developed by the United States National Security Agency (NSA)"



https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Case 1: Malware and persistent connections

Options

1. **Visibility - identify the problem (RouterOS and LucidView)**
2. Action - limit the action of the infected host
3. Action - sanitise the infected host



Case 1: Malware and persistent connections

1. Visibility - identify the problem

Netflow

```
/ip traffic-flow
set active-flow-timeout=5m cache-entries=8M enabled=yes interfaces=sfp1-internet
/ip traffic-flow target
add dst-address=1.1.1.1 port=9995
```

Syslog

```
/system logging action
add name=syslog remote=1.1.1.1 target=remote
/system logging
add action=syslog topics=dns,!packet
```

But how?



Case 2: Malware mechanism

Complaint

Slow Internet

Broken connections

Email queues and emails not being accepted

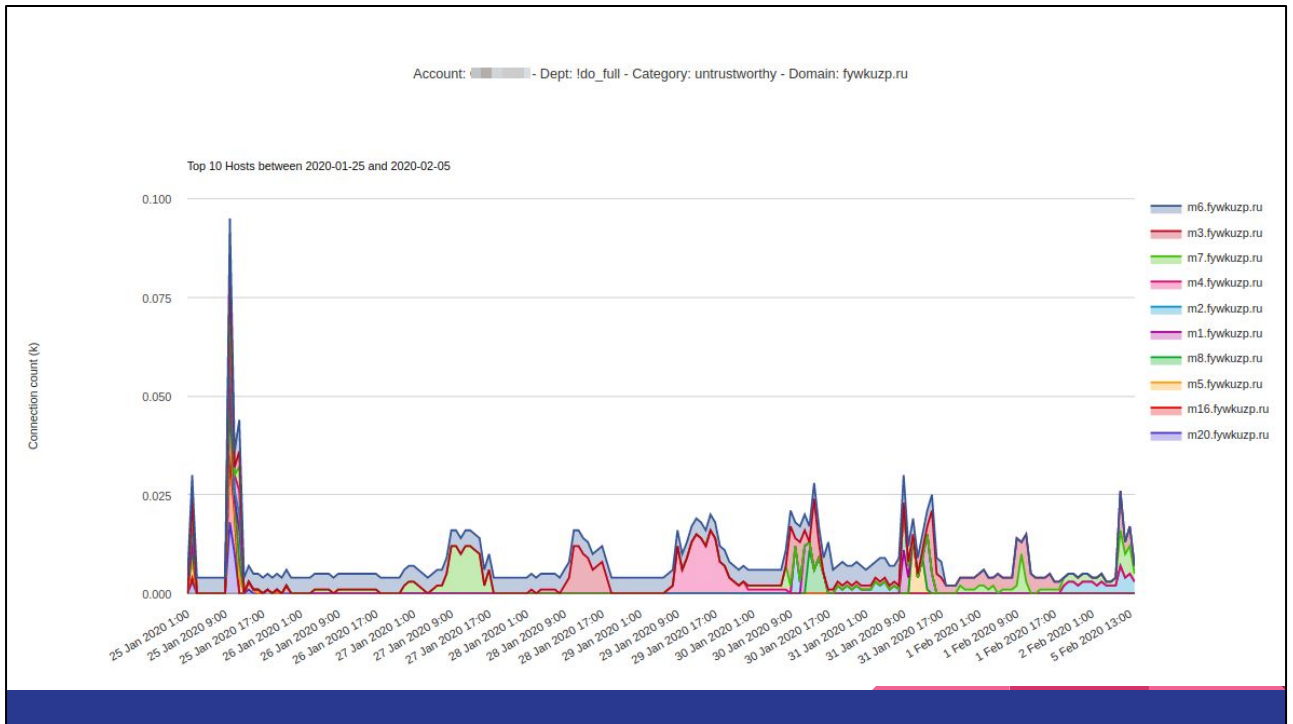


Case 2: Malware mechanism

Interesting DNS queries

```
13:39:04.494410 IP 10.0.3.17.36729 > 1.1.1.1.53: 58515+ A? v1.ciyzjlin.org. (33)
13:39:04.496160 IP 1.1.1.1.53 > 10.0.3.17.53645: 18360 NXDomain 0/1/0 (95)
13:39:04.496550 IP 1.1.1.1.53 > 10.0.3.17.36729: 58515 NXDomain 0/1/0 (96)
13:39:04.496709 IP 10.0.3.17.36730 > 1.1.1.1.53: 62195+ A? m22.fnfdjue.com. (33)
13:39:04.497646 IP 1.1.1.1.53 > 10.0.3.17.49923: 14876 NXDomain 0/1/0 (96)
13:39:04.499792 IP 10.0.3.17.61336 > 1.1.1.1.53: 63805+ A? m30.bbxqxbn.com. (33)
13:39:04.500439 IP 10.0.3.17.61452 > 1.1.1.1.53: 12404+ A? m6.hhqbikx.com. (32)
13:39:04.500615 IP 1.1.1.1.53 > 10.0.3.17.61336: 63805 NXDomain 0/1/0 (106)
13:39:04.500663 IP 10.0.3.17.36731 > 1.1.1.1.53: 25605+ A? m16.mxybawp.cc. (32)
13:39:04.501280 IP 1.1.1.1.53 > 10.0.3.17.36731: 25605 NXDomain 0/1/0 (99)
```

TCPDump



Filtered by .ru domain. Many TLDs are in the reports.

IP Addresses Performing DGA DNA DDoS - Current Day Report

Host count, is the total number of unique Hosts that the DGA requested.

Count, is the total number of DNS queries

[Go to 60 Minute Report](#)

Source IP	Host Count	Count	Top Hosts
[REDACTED]	548	7506	v1.qigkyubu.ru,v1.fbkiknuj.ru,v1.ttjyemg.ru,v1.zboxkzt.ru,v1.cpodseh.ru,v1.tsgpjccs.ru,v1.dd
[REDACTED]	517	6492	v1.knucizwu.ru,v1.gaqrswqb.ru,v1.ttjyemg.ru,v1.xtetrbwu.ru,v1.jyppbor.ru,v1.lhkoczo.ru,v1.
[REDACTED]	511	6279	v1.hrkdwazf.ru,v1.kquosqjp.ru,v1.jyppbor.ru,v1.aaueuotl.ru,v1.zdppgkz.ru,v1.riryjuueb.ru,v1
[REDACTED]	377	4026	v1.riryjuueb.ru,v1.tzobylw.ru,v1.mkialie.ru,v1.sgibommf.ru,v1.bqpgmrdt.ru,v1.wshakrt.ru,v1.x
[REDACTED]	446	4008	v1.mxmtmim.ru,v1.bngkuxd.ru,v1.pydzqce.ru,v1.yhemqfh.ru,v1.xzoswpg.ru,v1.eswuje.ru,v1
[REDACTED]	314	3396	v1.qigkyubu.ru,v1.wshakrt.ru,v1.yyuojr.ru,v1.lhkoczo.ru,v1.gtztahj.ru,v1.bqpgmrdt.ru,v1.ttj
[REDACTED]	285	2586	v1.uirxpw.ru,v1.xcsgsjs.ru,v1.sgibommf.ru,v1.gjfhigf.ru,v1.ddfaagk.ru,v1.gdxisleb.ru,v1.aleu

Case 2: Malware mechanism

Analysis of action

DNS resolution of random host.

Hosts do not resolve, so it seems.

DDoS on DNS service - ADs cannot service DNS.



Case 2: Malware mechanism

Analysis of action

v1.ciyzjlin.org

m22.fnfdjue.com

m16.mxybawp.cc

Host: Single letter, follow by one or two numbers

Domain: Seven letters

TLD: Any valid TLD it seems.



Case 2: Malware mechanism

A brief history of malware

Command and control host

Infected host

Hard coded IPs

Hard coded domains

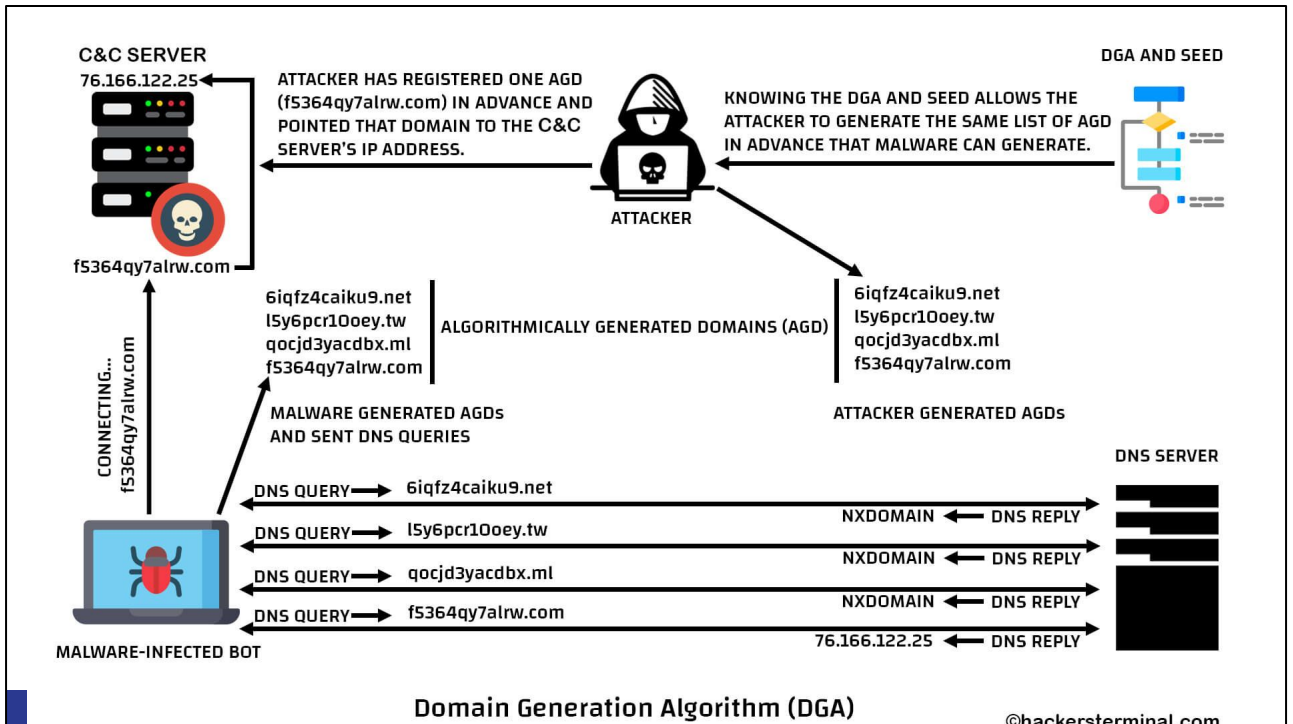
Domain Generating Algorithms (DGA)

Date and time controlled

DGA can be used for good - CDNs, researchers
Many types of DGA to prevent collisions



<https://hackerterminal.com/domain-generation-algorithm-dga-in-malware/>



<https://hackersterterminal.com/domain-generation-algorithm-dga-in-malware/>

Case 2: Malware mechanism

"Beyond magic numbers, magic strings or magic domain names are also used for generating DGA domains. Currently, there are not many effective methods to detect these seeds beyond reverse engineering the binary."

"Security researchers found a new malware called MyloBot (detected by Trend Micro as TSPY_MYLOBOT.A) that features sophisticated evasion, infection, and propagation techniques"

"The malware allows the attackers to gain full control of the infected machine, enabling them to add payloads for other purposes such as banking Trojans, keyloggers, and distributed denial of service (DDoS) use."



<https://blogs.akamai.com/2018/01/a-death-match-of-domain-generation-algorithms.html> (more detailed analysis of specific DGA and mechanisms of action)
<https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/mylobot-uses-sophisticated-evasion-and-attack-techniques-deletes-other-malware>
(Mylobot)

<https://blog.centurylink.com/mylobot-continues-global-infections/> (Mylobot infection hosts and domains correlate with that collected by LucidView)

Case 2: Malware mechanism

Options

1. Visibility - identify the problem
2. **Action - limit the action of the infected host** (RouterOS and LucidView)

Firewalling

Block DNS

3. **Action - sanitise the infected host**



LucidView Made for Mikrotik

<https://mikrotik.com/mfm/software>

“LucidView’s Enforcer is a MikroTik configuration script that allows a MikroTik router to lever off LucidView’s powerful cloud Content Filter, and/or provides meaningful Internet Traffic Reports.”

Visibility

DNS blocking

Firewall blocking



Security



Security Rating :

High

Based on your category blocking profile

Overview of your Enforcer

Reporting

1 Network Schedules defined.
The Privacy Policy has not been accepted,
therefore source IP addresses are **not** logged.

[View Reports](#)

Familiar Devices

16 Devices are defined.
16 Devices bypassing Catblock.

[Show Devices](#)

Time Based Rules

No time based rules exist. Try creating one!

[Time Rule Management](#)

Category Blocking

46 whitelist entries.
Categories Currently Blocked:

- Torrent
- Adult
- Anonymizer

[View Category Blocking](#)

WiFi Configuration

Wifi is : Enabled
Password has been set
Channel : Auto

[Wi-Fi Settings](#)

FairShare

FairShare is disabled.

[FairShare Configuration](#)

Generating Enforcer Install Script for Bolt-on Enforcer :

The Enforcer Bolt-on solution caters for existing Mikrotik installations that will benefit from the cloud content filter and reporting provided by LucidView. The Enforcified Mikrotik is still managed by your network team via your preferred tools with the additional functionality of content filter and reporting.

Enforcer Unique ID:

Password

Mikrotik Internal IP

192.168.56.103

If left blank, the above default IP will be issued.

Once "Generate Script" has been clicked, your download will start automatically.

Ensure that you have read, and understand [this document](#) as it contains imperative information regarding the Enforcer type, and its purpose.

Cancel

Generate Script

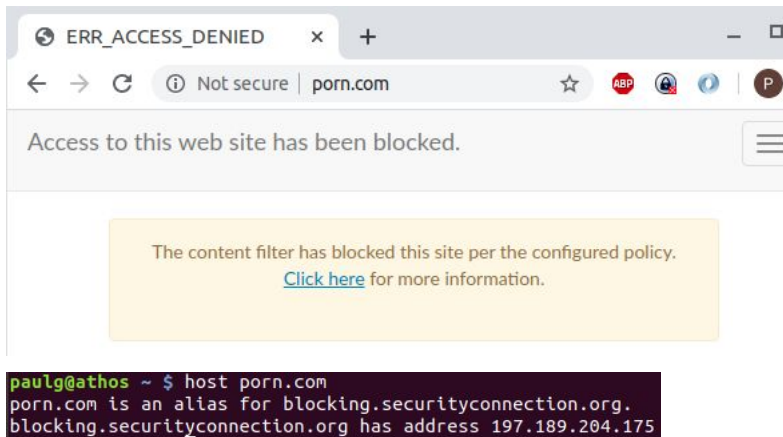


```
[admin@MikroTik] > /import [REDACTED]
* Installing... This script usually completes within about 60 seconds.
W Please do not interrupt.
  If there are any problems applying the bolt on script we will attempt to
  remove all traces of the script so you can attempt it again later.
  If you would like to remove the bolt on script, run this script again.
  Reapplying the script will trigger the complete removal of the script.
* Create Cloud VPN.
* Cloud remote access.
* Configure DNS server.
W NB: Please ensure your PPPoE client (if applicable) is configured to
  NOT use the peer DNS as this will override the category blocking.
* Add NAT rules to intercept DNS.
* Add filter rules for the LucidView cloud reject list and allow DNS.
W Make sure the kill lists are above any allow all rules so that they are effective.
* Allow DNS requests.
W If the Mikrotik has an IP on the Internet, consider modifying the
  firewall rule to only allow DNS requests from the local network.
* Configure Netflow export to LucidView Cloud.
* Configure DNS logging.
* Add Scheduler Script to test VPN availability.
* Set the cache entries for traffic flow to max allowed by the Mikrotik.

Script file loaded and executed successfully
```

Combating untrustworthy connections

DNS filtering



Combatting untrustworthy connections

Dynamic IP filtering

```
4   ;;; lvcloud_kill_list_external  
   chain=forward action=reject dst-address-list=lvcloud_kill_list_external
```

#	LIST	ADDRESS	CREATION-TIME
0	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.128.109.216	feb/06/2020 12:00:37
1	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.156.170.134	feb/06/2020 12:00:37
2	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.158.178.74	feb/06/2020 12:00:37
3	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.240.238.87	feb/06/2020 12:00:37
4	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.36.47.10	feb/06/2020 12:00:37
5	D ;;; lvcloud_kill_list_external	lvcloud_k... 1.42.4.139	feb/06/2020 12:00:37



Combatting untrustworthy connections

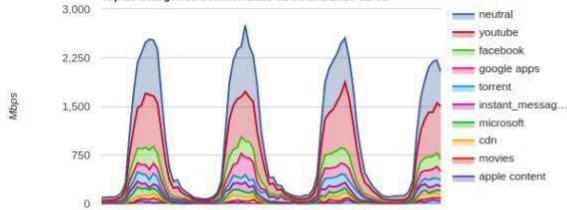
Blocked IPs updated frequently.

```
[monitor@MikroTik] > ip firewall address-list print count-only where list~"lvcloud_kill_list_external"  
27740  
[monitor@MikroTik] > ip firewall address-list print count-only where list~"lvcloud_kill_list_external"  
27873
```



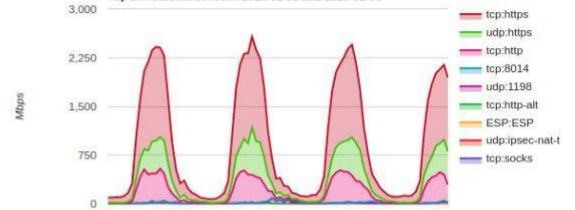
Bandwidth by Category

Top 10 Categories between 2020-02-03 and 2020-02-06



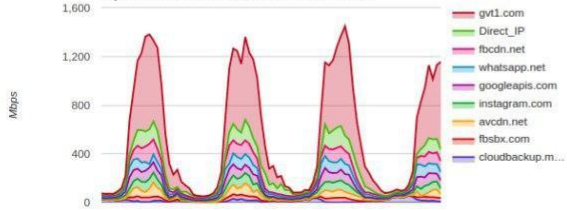
Bandwidth by Protocol

Top 9 Protocols between 2020-02-03 and 2020-02-06



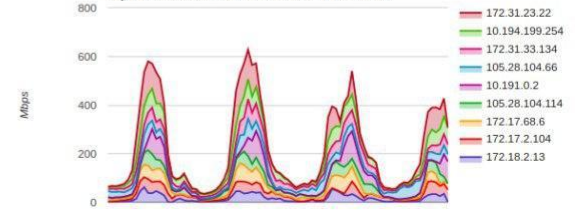
Bandwidth by Domain

Top 9 Domains between 2020-02-03 and 2020-02-06



Bandwidth by Source IP

Top 9 Source IPs between 2020-02-03 and 2020-02-06



Not suitable for you?

```
Script file loaded and executed successfully
[admin@MikroTik] > /import [REDACTED]
! It appears the script has already been installed.
* Uninstalling.
* Remove Cloud VPN.
* Removing filter rules.
* Removing NAT rules.
* Removing address list entries.
* Remove DNS entries.
* Remove Netflow target.
* Remove DNS syslog upload.
* Remove Cloud access.
* Remove VPN test Scheduler script.
Script file loaded and executed successfully
```



LucidView's MikroTik Enforcer Portal



MikroTik Enforcer Portal Pros

- Scales
- Affordable
- DNS and firewall blocking
- Simple to add (download complete script and modify to suit application)
- Detailed reporting
- Automated reporting (i.e., security reports to your inbox)
- Customised branding
- Youtube and Google safe search
- Torrent and Suspect blocking
- Time based rules



Thank you

<https://www.lucidview.net/>

Web content filtering and log data analysis with Mikrotik routers - MUM Turkey

<https://mum.mikrotik.com/2018/TR/agenda>

