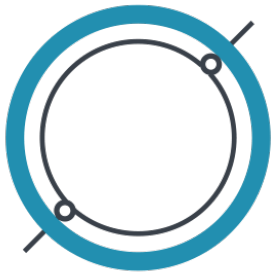
AGAM SECURITY



Prevent cyber attacks with Artificial Intelligence & Automated Threat Management

Jean-Pierre Montaut

- Jean Pierre Montaut is the CTO of Agam Security and the main designer of the Agam-AI cyberdefense appliance built on Artificial Intelligence
- He has a 20 year experience in defending and attacking sensitive infrastructures for governments.

Stéphane Zrehen

- Stéphane Zrehen is the CEO of Agam Security and hold a MSc in Physics & PhD in machine learning from EPFL.
- He has a 25 year experience in Artificial Intelligence applications and data analytics. He is the co-designer of the Artificial Intelligence engine of Agam-AI appliances

AGAM SECURITY

Untraceable attack methods

- HTTP/HTTPS : Web protocol
- CDN
- Video flows
- Perring attack

AGAM SECURITY

Web Protocol

http/https through

1. data padding
2. CSS covers also androids, Iphone and others
3. Java / javascript / html5

1st stage - blind attack

The hacker hacks an official site: www.admin.ch

- Inject into it http/https or css trames. Takes control of the apache server: IIS for
  - Example :Shifts time, induces a sync with ERP and other MS applications -> all MS systems are down.
- The official site contains a hacktool.
- The hacker has a communication of control to the official site.
- Css zero-day: *html will launch a hidden function that calls a system applet

2nd stage – injection client

Visitor goes to admin.ch

- His navigator unvoluntarily catches the backdoor.
- The backdoor gets into the kernel
- Hacker will not take control of the endpoint, but the endpoint will communicate with a C&C
- Hacker communicates with the C&C and gets all information about visitor's network
- Hacker updates through the C&C or the hacked official site, and then decides what actions to take.

3rd stage – communication hacker

Target is caught and identified

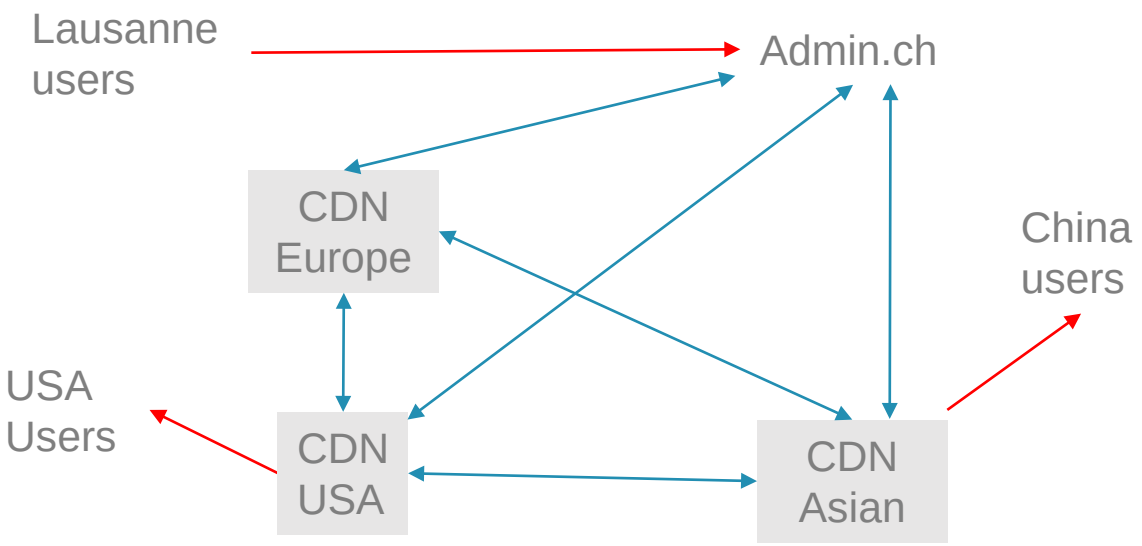
- Hacker communicates with the C&C and gets all information about visitor's network
- Hacker gets list of vulnerabilities about the defense equipment
- Hacker hacks the defense equipment from the **internal** side of the network: install back-doors and sleep.
- When the decision is taken to steal information or destroy, the backdoors are exploited through possibly another C&C

Advanced MS office, open-office, libreoffice zero-days
Some functions call the system/kernel
Undetectable if encrypted in Blowfish.
Do the same as the site attack.
Undetectable
Install an OS keylogger
Stays in all backups and migrations
Self-destruction
Removes all traces

AGAM SECURITY
Prevent cyber attacks with Artificial Intelligence & Automated Threat Management

CDN attack (f. ex. Facebook attack in India)

Pre-cache : images, videos, … locally cached



- Hack the CDN: cache server
  Hack with a C&C
- Same effects as the Web protocol attack
- Example: Indian attack on Facebook: login and passwords for the zone were collected

- Advantages: official site remains clean
- Hard to detect
- Nobody looks into the CDN
- All CDNs communicate trustfully between themselves
- Attack on one CDN can thus infect all CDNs

Hacking a CDN contaminates a wide geographical area

AGAM SECURITY
Prevent cyber attacks with Artificial Intelligence & Automated Threat Management

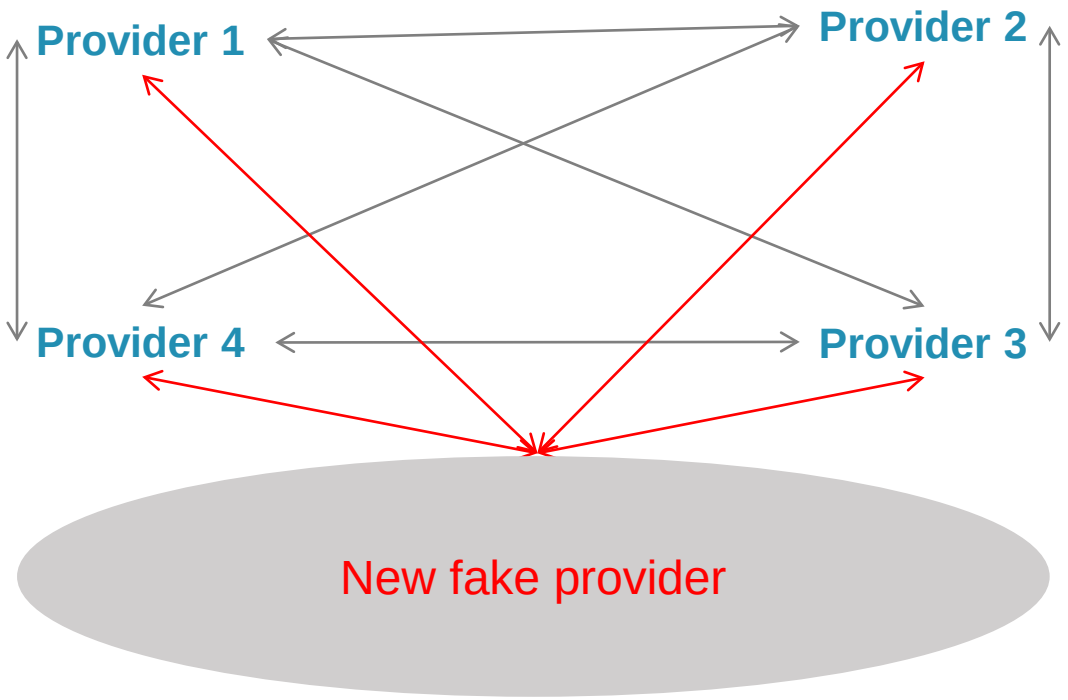
Virus H264

1. RTPD video and streaming protocol
2. Dailymotion and Youtube are already infected
3. RTP: when opening a video stream
   A. Payload: divx or mpeg2, format, codec…
   B. Data transfer protocol
   C. RTCP is launched: unused protocol implemented in video streams
      I. Packets
      II. One packet is called Packet APP
         - SSRC/CSR
         - Name of the program: ASCII
         - Application - dependant data
      III. This is read by the navigator, which launches the executable.
      IV. Can even exchange invisible files.

AGAM SECURITY

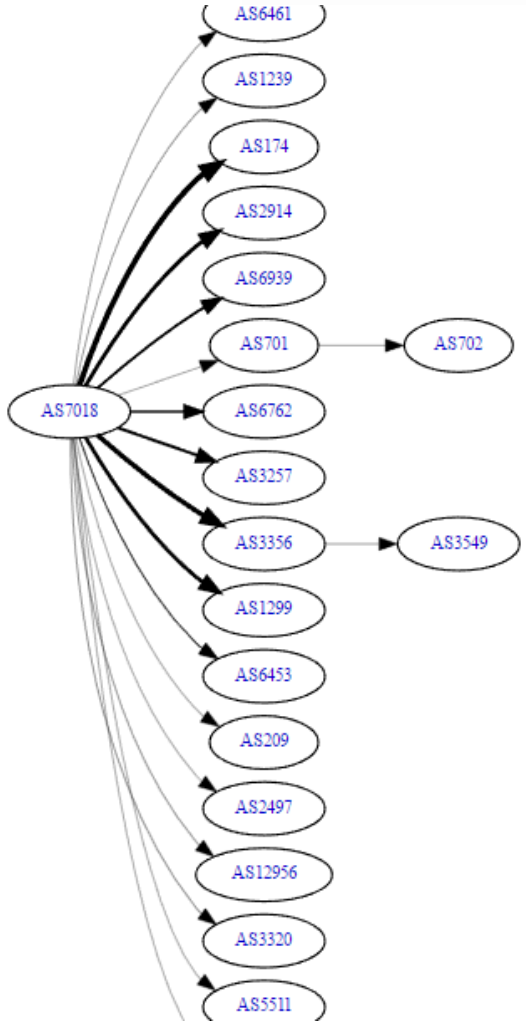
Peering attack

- A provider Swisscom/VTX/Sunrise etc…
- All providers trust each other through BGP protocol (L3)



Connect to the network
Collects all informations in DB
Tell everyone to pass communications in priority through it since it says it is the fastest

Peering system




```
as-block:       AS1299 - AS1309
descr:          RIPE NCC ASN block
remarks:        These AS Numbers are assigned to network operators in the RIPE NCC service region.
mnt-by:         RIPE-NCC-HM-MNT
created:        2002-08-22T14:58:01Z
last-modified:  2014-02-24T13:15:15Z
source:         RIPE

aut-num:        AS1299
org:            ORG-TCA23-RIPE
as-name:        TELIANET
import:         from  AS57 accept AS-NLG-TO-TRANSIT
mp-import:      afi ipv6 from AS57 accept AS-NLG-TO-TRANSIT
import:         from  AS62 accept AS-C1
mp-import:      afi ipv6 from AS62 accept AS-C1
import:         from  AS109 accept AS-CISCO
mp-import:      afi ipv6 from AS109 accept AS-CISCO
import:         from  AS158 accept AS158
mp-import:      afi ipv6 from AS158 accept AS158
import:         from  AS174 accept AS174
mp-import:      afi ipv6 from AS174 accept AS174
import:         from  AS209 accept AS209
mp-import:      afi ipv6 from AS209 accept AS209
import:         from  AS237 accept AS-MICHNET
mp-import:      afi ipv6 from AS237 accept AS-MICHNET
import:         from  AS286 accept AS-KPN
mp-import:      afi ipv6 from AS286 accept AS-KPN
import:         from  AS293 accept AS-ESNET
mp-import:      afi ipv6 from AS293 accept AS-ESNET
import:         from  AS302 accept AS-BCMI1
mp-import:      afi ipv6 from AS302 accept AS-BCMI1
import:         from  AS553 accept AS-BELWUE
mp-import:      afi ipv6 from AS553 accept AS-BELWUE
import:         from  AS559 accept AS-SWITCH
mp-import:      afi ipv6 from AS559 accept AS-SWITCH
import:         from  AS577 accept AS577:AS-CUSTOMERS
mp-import:      afi ipv6 from AS577 accept AS577:AS-CUSTOMERS
import:         from  AS701 accept AS701
mp-import:      afi ipv6 from AS701 accept AS701
import:         from  AS702 accept AS702:RS-EURO
import:         from  AS702 accept AS702:RS-CUSTOMER
mp-import:      afi ipv6 from AS702 accept AS702:RS-EURO
mp-import:      afi ipv6 from AS702 accept AS702:RS-CUSTOMER
import:         from  AS714 accept AS-APPLE
mp-import:      afi ipv6 from AS714 accept AS-APPLE
import:         from  AS786 accept AS-JANETUS
```

AGAM SECURITY

We protect the integrity of your know-how
and ensure the sustainable development
of your organization.

AGAM
SECURITY

AGAM SECURITY SARL
Rue des terreaux 13
1003 lausanne

info@agamsecurity.ch
agamsecurity.ch