# THE
# UNBEARABLE LIGHTNESS
# OF
# APTing


# WHO ARE WE?

## Ron Davidson

Head of Threat Intelligence and Research

Check Point Software Technologies

## Yaniv Balmas

Security Researcher

Check Point Software Technologies

# APT

**Advanced**

**Persistent**

**Threat**

# APT

**Advanced**

"An **APT** is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time."

techtarget.com

**Threat**

# APT

**Advanced**

"An **APT** is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time."

techtarget.com

"**APT** is a set of stealthy and continuous computer hacking processes ... **APT** usually targets organizations and/or nations for business or political motives."

WIKIPEDIA
The Free Encyclopedia

# APT

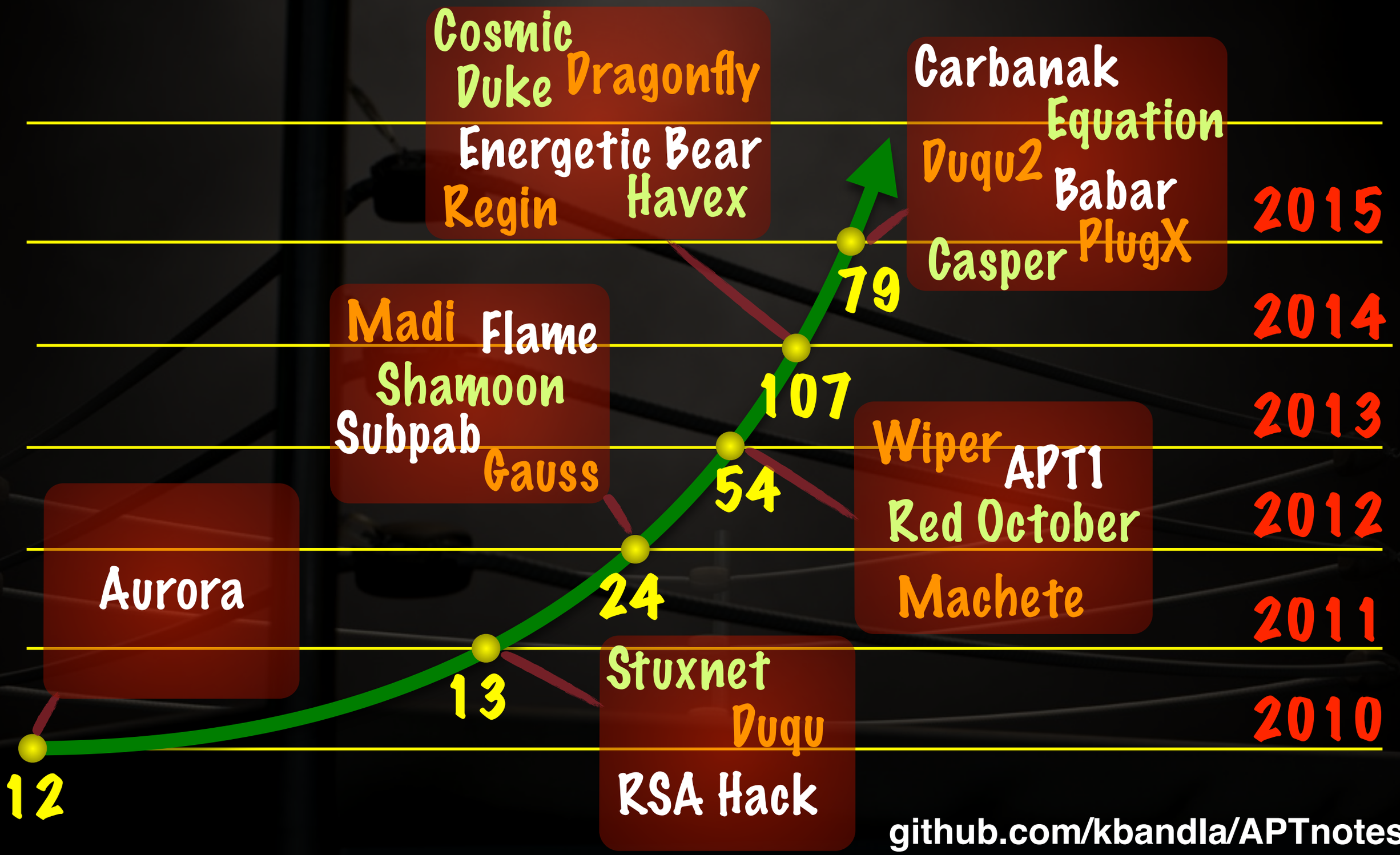

"An **APT** is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time."

techtarget.com

"**APT** is a set of stealthy and continuous computer hacking processes ... **APT** usually targets organizations and/or nations for business or political motives."

WIKIPEDIA
The Free Encyclopedia

# APT HISTORY

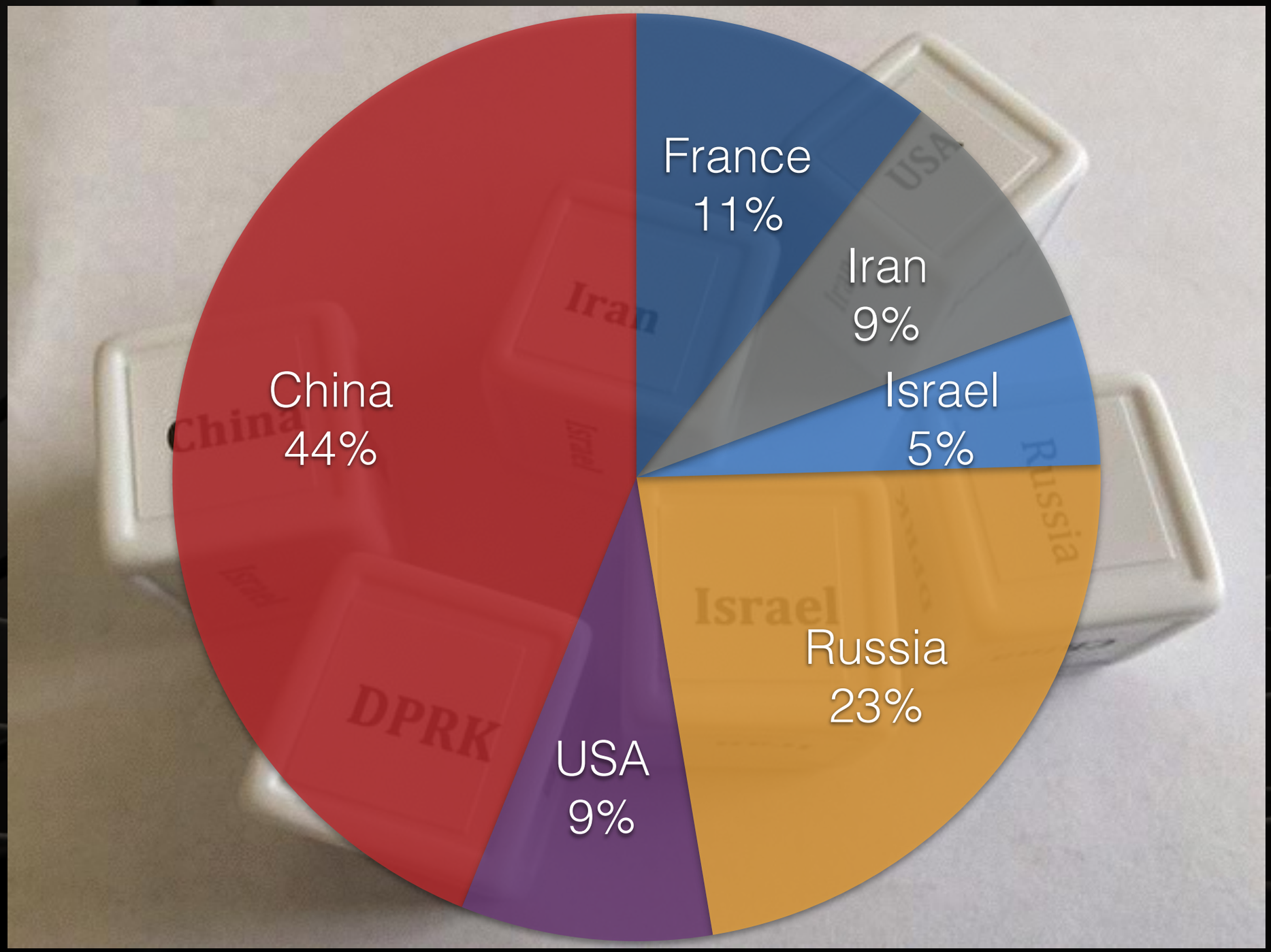



github.com/kbandla/APTnotes

# WHAT'S COMMON?


@AttributionDice

# WHAT'S IN COMMON?




@AttributionDice

# WHEN IN DOUBT...

It's probably China!

# WITH GREAT POWER COME GREAT APTS




# VOLATILE CEDAR

- A targeted campaign
- Has been active since late 2012
- Operation was terminated following our publication at March 2015

# WHY VOLATILE CEDAR?


Explosive-443

```
D 56 52 3A 76 33 3A 44 4C 44 2D   ..DLD-VR:v3:DLD-
4 2D 54 4E 3A 36 39 40 31 32 30   VR=DLD-TN:69@120
1                 31    35        @112@108@111@115
1                 34    40        @105@118@101@45@
0 35 31 40 3A 44 4C 44 2D 54 4E   52@52@51@:DLD-TN
2 43 48 3A 74 72 75 65 3A 44 4C   .DLD-RCH:true:DL
F 44 4C 44 2D 52 4C 3A 30 3A 44   D-RCH.DLD-RL:0:D
B 44 4C 44 2D 52 4E 3A 38 37 40   LD-RL;DLD-RN:87@
1 30 40 31 30 30 40 31 31 31 40   105@110@100@111@
1 35 40 33 32 40 37 33 40 31 31   119@115@32@73@11
```

# Israel Confirms It Was Cyber Attack Target

**By Barbara Opall-Rome** *12:20 p.m. EDT June 24, 2015*


*(Photo: Israel Ministry of Defens*

TEL AVIV — Defense Minister Moshe Ya'alon confirmed Wednesday that Israel was the target of cyber attacks by Iran during last summer's Gaza war and by Hezbollah, which reportedly ran an operation going back three years.

Speaking at an international cyber security conference at Tel Aviv University, Ya'alon insisted "no significant damage" was inflicted by Iranian operatives, terror organizations and hackers who targeted government, military and economic sites during the July-August 2014 Operation Protective Edge.

He confirmed for the first time findings from Tel Aviv-based Check Point Software Technologies, which reported to its clients in March that Israel, several Western countries and other Mideast states had since 2012 been targets of a sustained cyber spying campaign that the company believed was run out of Lebanon.

At the time, Check Point did not specifically name Hezbollah as the culprit for the cyber spying campaign, which the company dubbed "Volatile Cedar." It only noted that command-and-control servers supporting malware activities were traced to a hosting company in Lebanon, while several other servers were registered with "a very similar" Lebanese address. According to the cyber security and information technology firm, the campaign was based on Trojan horse computer malware planted in its targets, which was activated to collect data over extended periods.

"Monitoring these cyber infections was very challenging, due to the numerous ways in which they were disguised by the hackers," the Check Point report noted.

# HEZBOLLAH


فإن حزب الله هم الغالبون
حزب الله
المقاومة الإسلامية في لبنان

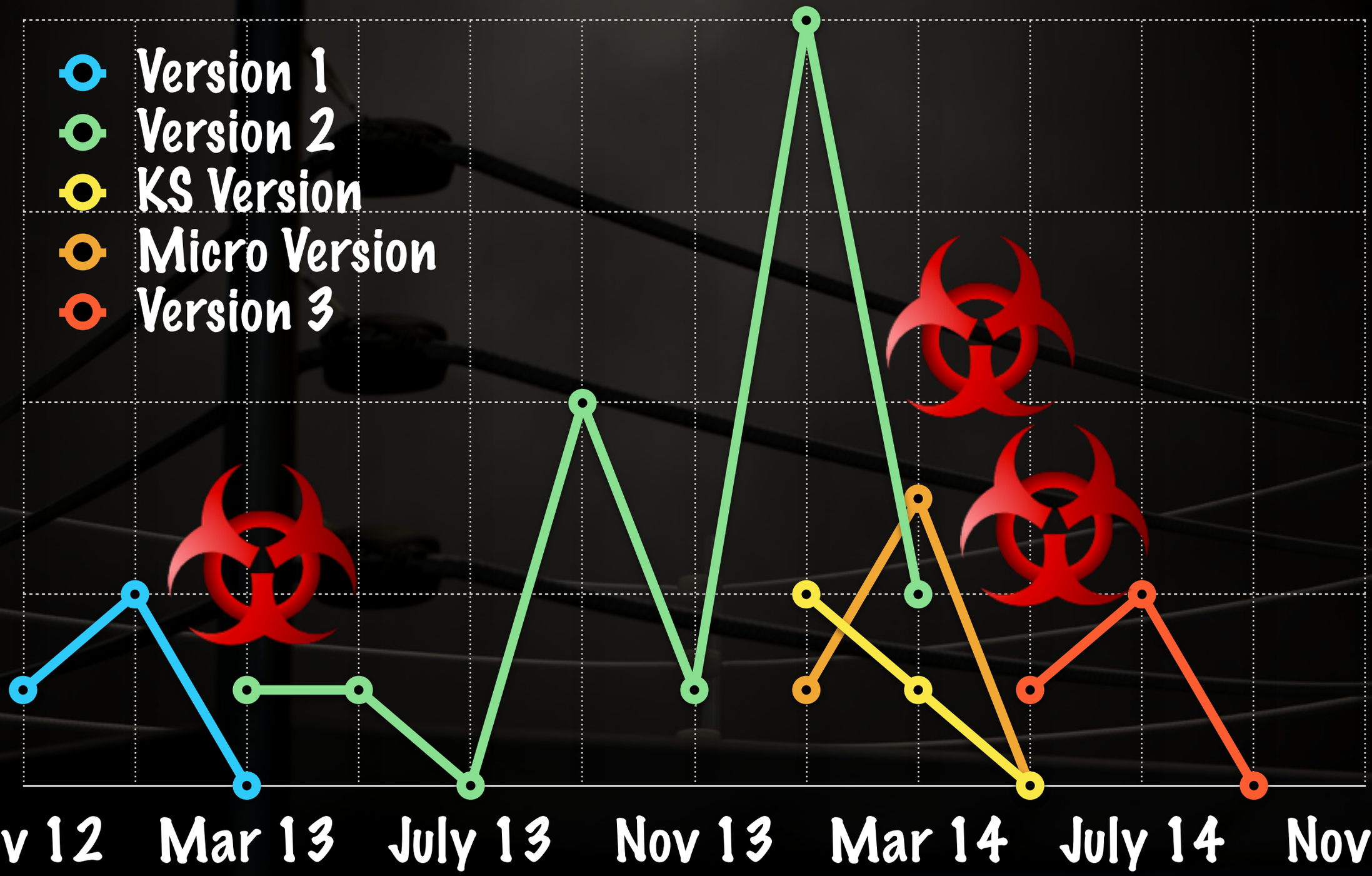
# HEZBOLLAH

- “Party of God”
- Islamist political and militant group
- Part of the Lebanese government
- Funded by Iran
- Official flag contains an AK-47

# HEZBOLLAH

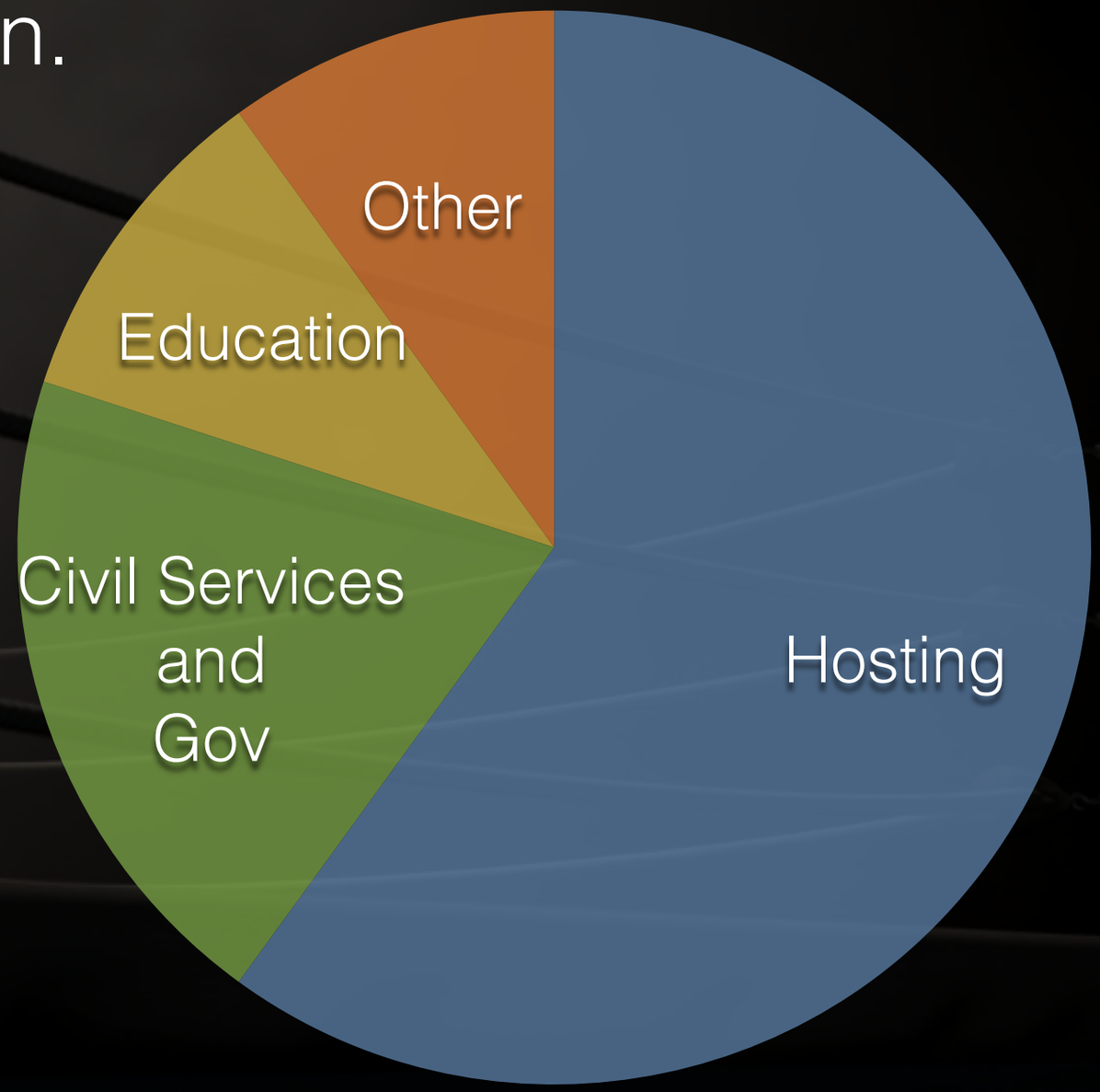
- “Party of God”
- Islamist political and militant group
- Part of the Lebanese government
- Funded by Iran
- Official flag contains an AK-47

# PERSISTENT


Version 1
Version 2
KS Version
Micro Version
Version 3
Nov 12
Mar 13
July 13
Nov 13
Mar 14
July 14
Nov 14

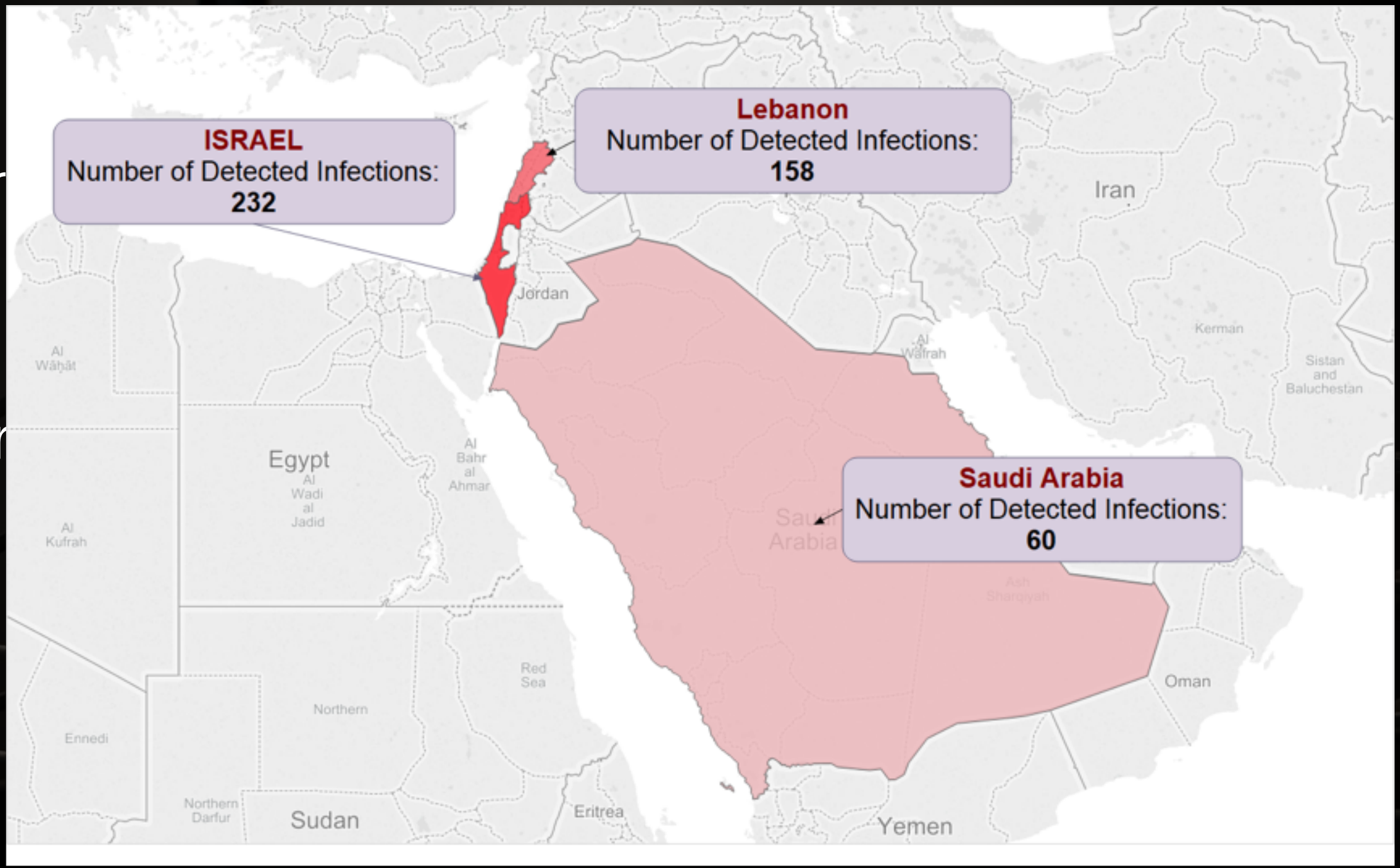
# THREAT

- Targets were carefully chosen.



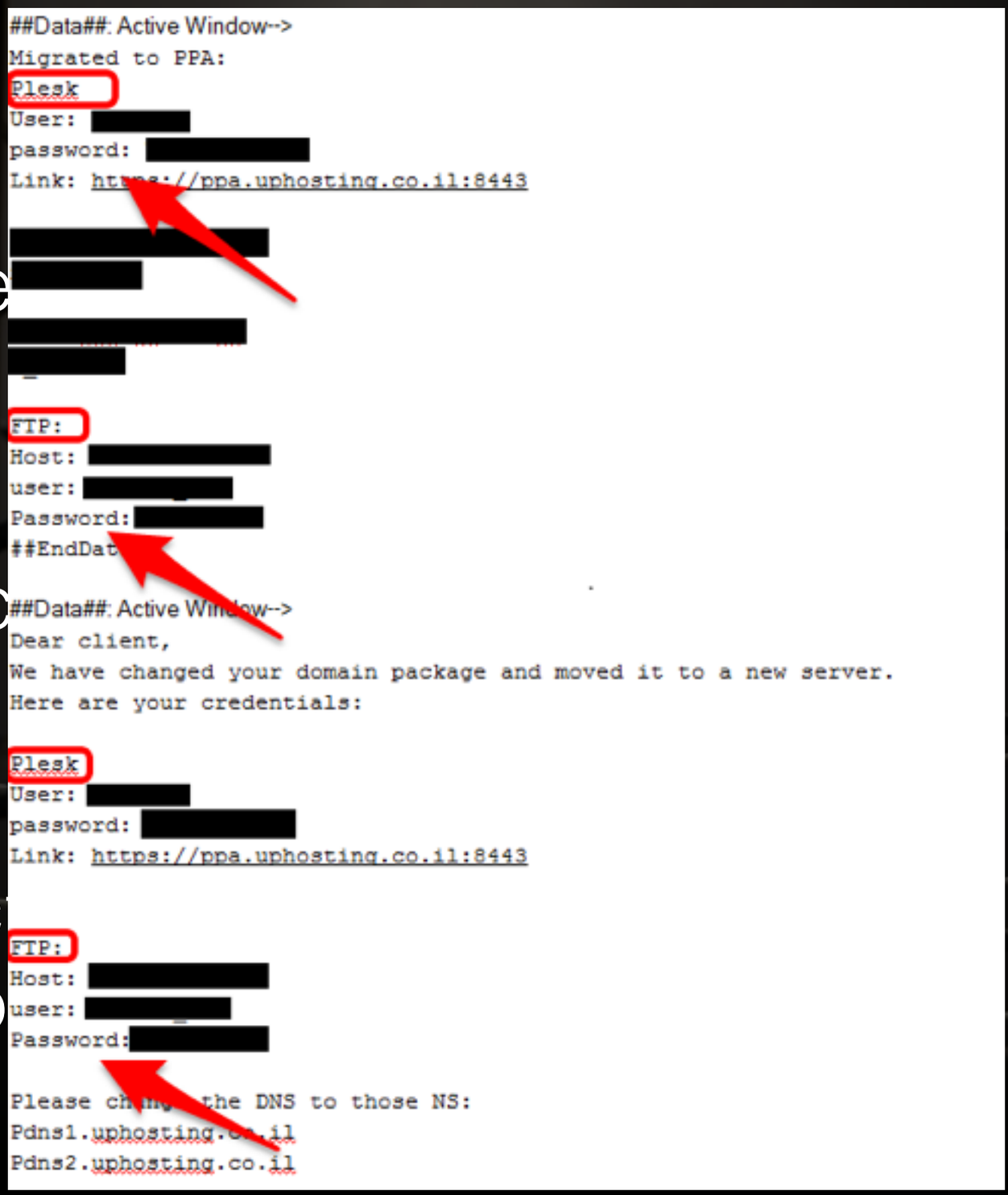
# THREAT

- Tar
- Ver



# THREAT

- Targets were
- Very specific
- Malicious ac and clip-board lo



# ADVANCED?!

# ADVANCED?!

Keith B.

ALEXANDER

VS

Hassan

NASRALLAH

# Round 1

# ATTACK VECTOR

# STUXNET

## Attack Vector

- Deliver USB drives into a super secured site
- USB Contains 4 0-days
- CPLink vulnerability
- Lateral movement via peer to peer RPC

# VOLATILE CEDAR

## Attack Vector

- The target itself might be a hard nut to crack.
- Look in its proximity…
- Exploit default un-patched IIS installations.
- Insert a web-shell and a key-logger into compromised servers.
- Use key-logging data for lateral movement.

# Round 2

# PERSISTENCE

# EQUATION

## Persistence

- Insert implant code into hard-drive firmware
- Support 12 different HDD vendors/variations
- Possibly infect boot sector

# VOLATILE CEDAR

## Persistence

- Install as a new service
- What if service gets removed\stopped?
- Use web-shell to restart\reinstall it

# Round 3

# COMMAND AND CONTROL

# PLUGX

## Command & Control

- Victim-side C&C servers are legit hosts
- A custom DNS resolver is used by the malware
- This DNS is hijacked and redirects to the C&C server

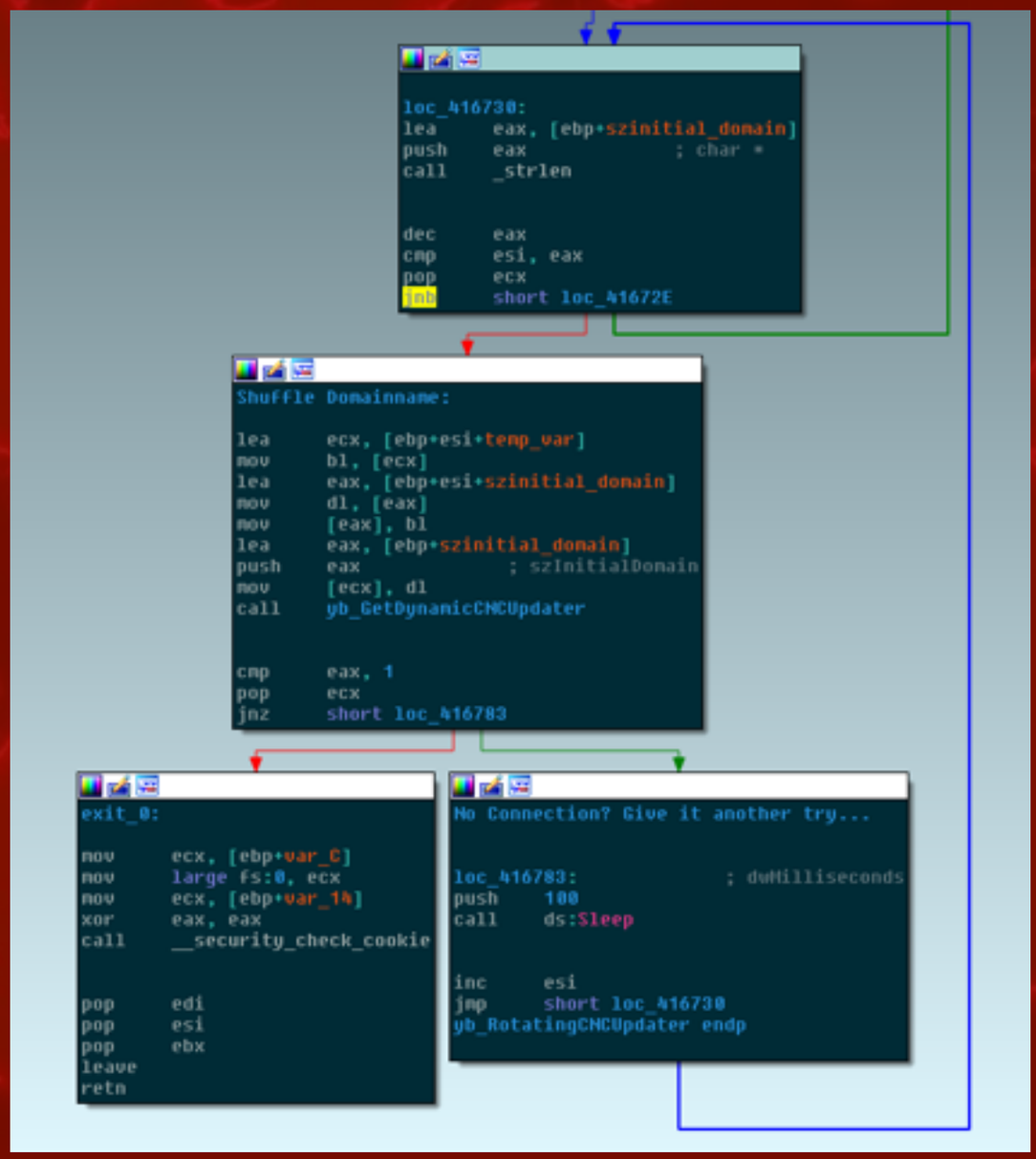
# VOLATILE CEDAR

## Command & Control

# VOLATILE CEDAR

## Command & Control

- “Advanced”



# VOLATILE CEDAR

## Command & Control

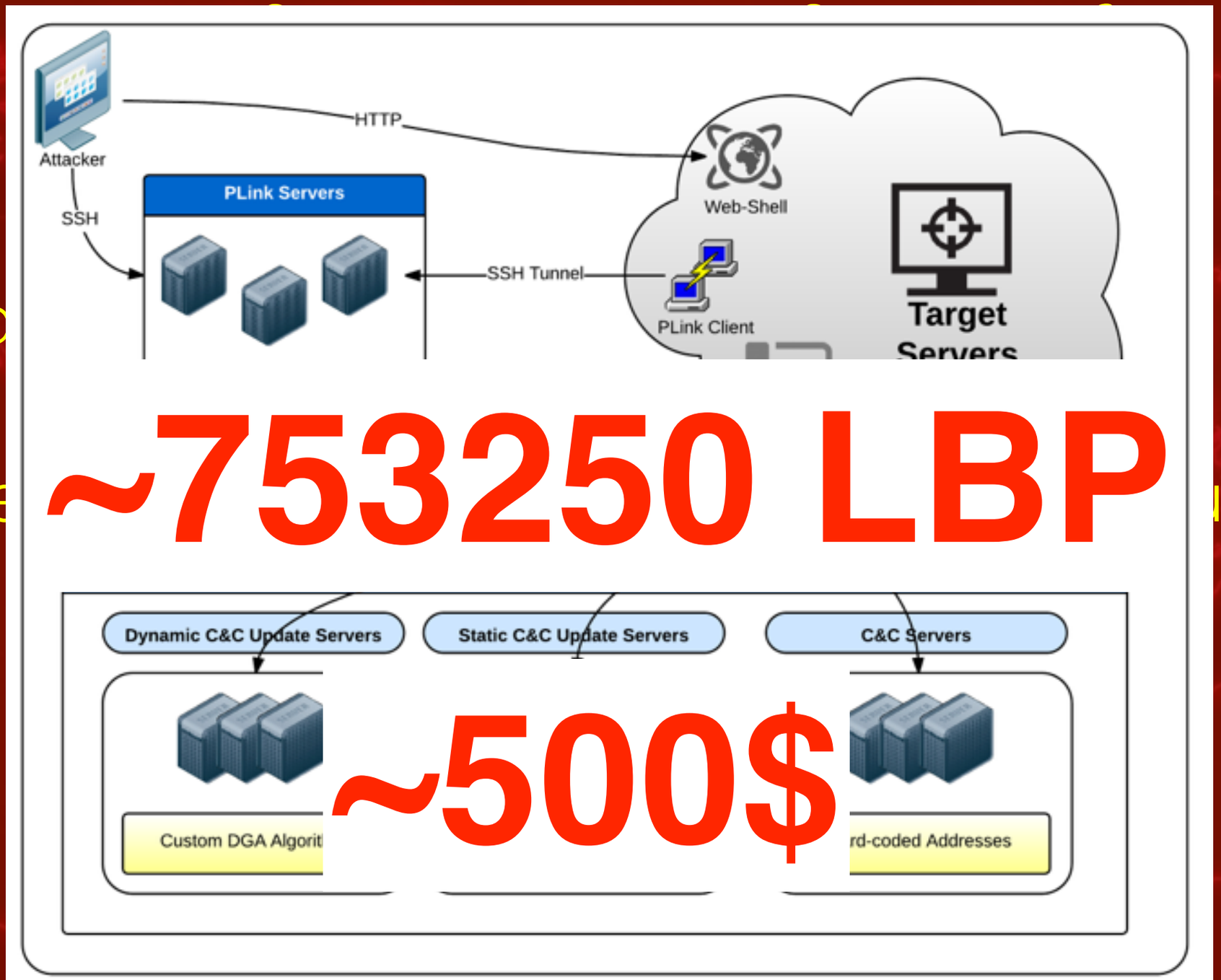
- "Advanced"

**re**dotnetexplorer
e**rd**otnetexplorer
ed**ro**tnetexplorer
edo**rt**netexplorer
edot**rn**etexplorer
edotn**re**texplorer

...

# VOLATILE CEDAR

- "Ac
- Use




ucture

# Round 4

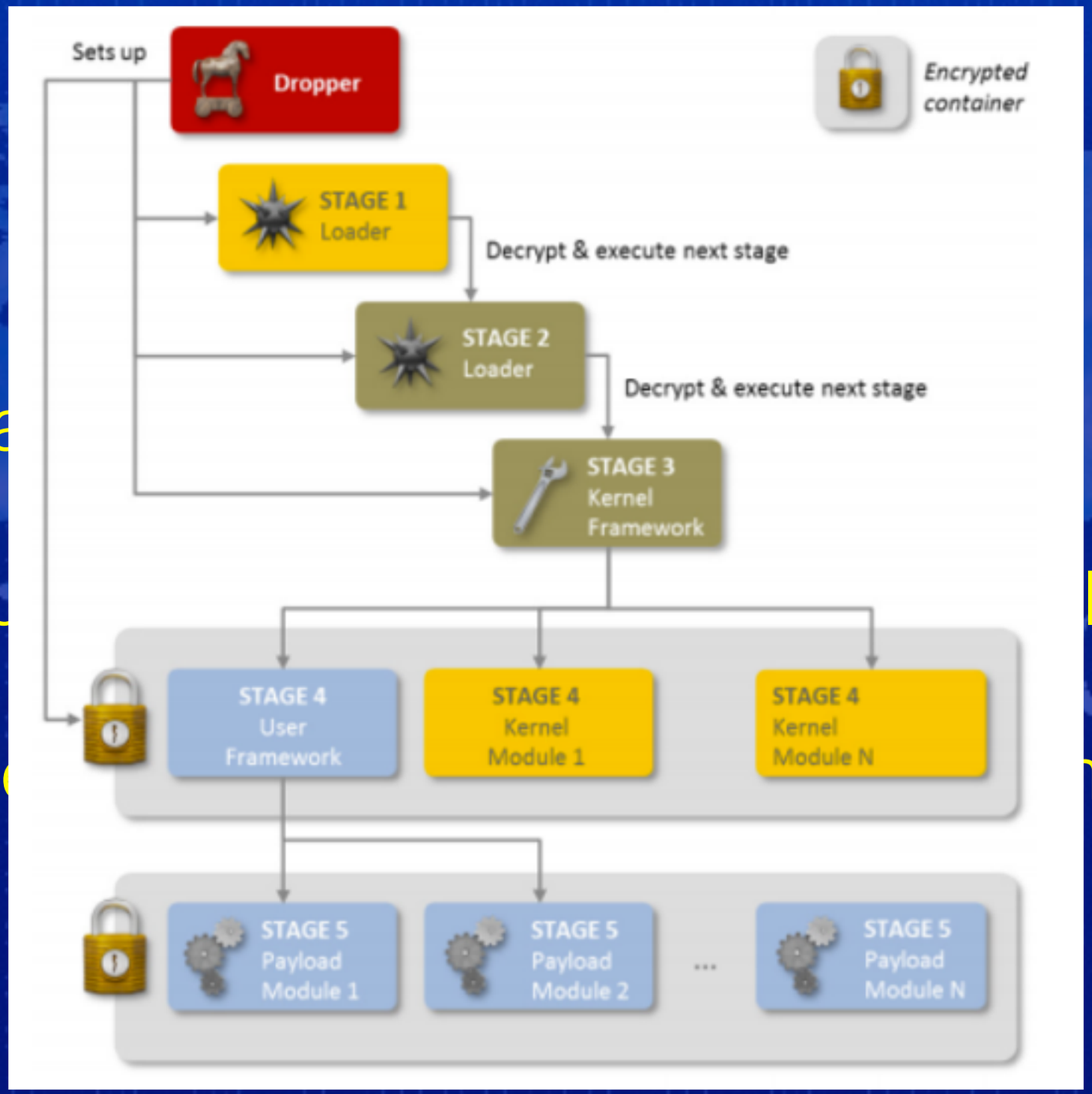
# STEALTH

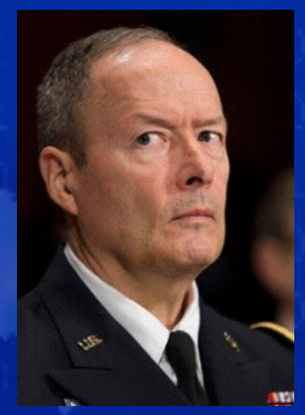
# REGIN

## Stealth

- Six stage architecture.
- Use both user-land code and kernel modules.
- Store stages in a custom Virtual File System.

# REGIN



- Six stage a
- Use both u les.
- Store stag m.

# VOLATILE CEDAR

## Stealth

- Create a dedicated thread to monitor process CPU activity.
- Once CPU usage is greater than the threshold
- Restart the process ;)

# Round 5

# ENCRYPTION

# EQUATION

## Encryption

- Usage of AES, RC5 and RC6
- A unique RC6 implementation designed for better performance.

# VOLATILE CEDAR

## Encryption

- Reversed Strings.

google.com → moc.elgoog

# VOLATILE CEDAR

## Encryption

- Reversed Strings.
- Oh, wait… That might be too easy to spot
- Use Base-64!

google.com → moc.elgoog → bW9jLmVsZ29vZw==

# VOLATILE CEDAR

## Encryption

- Reversed Strings.
- Oh, wait… That might be too easy to spot
- Use Base-64!
- Oh no, now it looks like Base-64.

google.com → moc.elgoog → bW9jLmVsZ29vZw==

# VOLATILE CEDAR

## Encryption

- Reversed Strings.
- Oh, wait… That might be too easy to spot
- Use Base-64!
- Oh no, now it looks like Base-64.

google.com → moc.elgoog → bW9jLmVsZ29vZw== → ==wZv92ZsVmLj9Wb

# CONCLUSIONS

- “Advanced” is a very subjective term
- Dedication can sometimes be as effective as resources
- APT is no longer the sole domain of multi-billion dollar organizations.

# MORE RECENT EXAMPLES

- The Spy Kittens Are Back: Rocket Kitten 2
  - Cedric Pernet - Trend Micro
  - Eyal Sela - ClearSky

# ROCKET KITTEN 2

## Threat?

"We believe the espionage factor and **political context** make their attacks unique and very different from traditional targeted attacks... This is an obvious case of **politicaly inspired or motivated espionage**."

"550 Targets, most of which are located in the Middle East... **policy research, diplomacy**, all aspects of international affairs, **defense, security**, journalism, human rights... **Israeli academic institution**... scientists, journalists, researchers, and sometimes **expatriated Iranians** living in Western countries..."

# ROCKET KITTEN 2

## Persistent?

"**Numerous attempts** to attack the same (chosen) targets for as long as necessary"

"**Barrage targets** until they eventually slip"

"The attackers do make up for these disadvantages with **persistence**..."

# ROCKET KITTEN 2

## Advacned?

"Simple tools and lack of professionalism... they don't seem to put much effort into quality

"The group is not very technically sophisticated... analysis of their code showed deficits and mistakes that a professional cybercriminal would not make... actors used off-the-shelf and low-quality tools""

# MWI AS AN APT TOOL

- A new Word Document Exploit Kit
  - Art Villeneuve, Joshua Homan, Fireeye
  - “advertised as an “APT” tool to be used in targeted attacks”
- Microsoft Word Intruder RTF Sample Analysis
  - Omni Herscovici, Check Point
- Microsoft Word Intruder Revealed
  - Gabor Szappanos, SophosLabs Hungary

# MWI CAMPAIGN TARGETS

An airline Carrier

Ministry of Education

Government Export Agency

The Municipalities Computation Center

The Supreme Court Network

The Social Security Authority

Government Aviation Authority

Medical Centers

A university computation center

# THANK YOU!

rond@checkpoint.com
yanivb@checkpoint.com @ynvb