RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART4-T11

Attacking The Dark Corners of The Internet

Yaniv Balmas

Head Of Cyber Research
Check Point Software Technologies
@ynvb

Isaac Dvir

Director of Mobile Threat Prevetion
Check Point Software Technologies
@isaacDvir

CYBER MISCONCEPTIONS

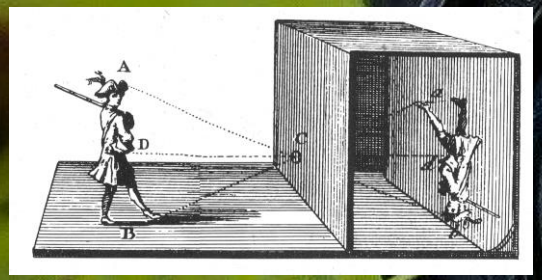
"The trouble with the world is not that people know too little; it's that they know so many things that just aren't so."

Mark Twain

Somethings have nothing to do with Cyber…

CAMERAS

945



1953

1988

But Who Uses Cameras Anyway?!

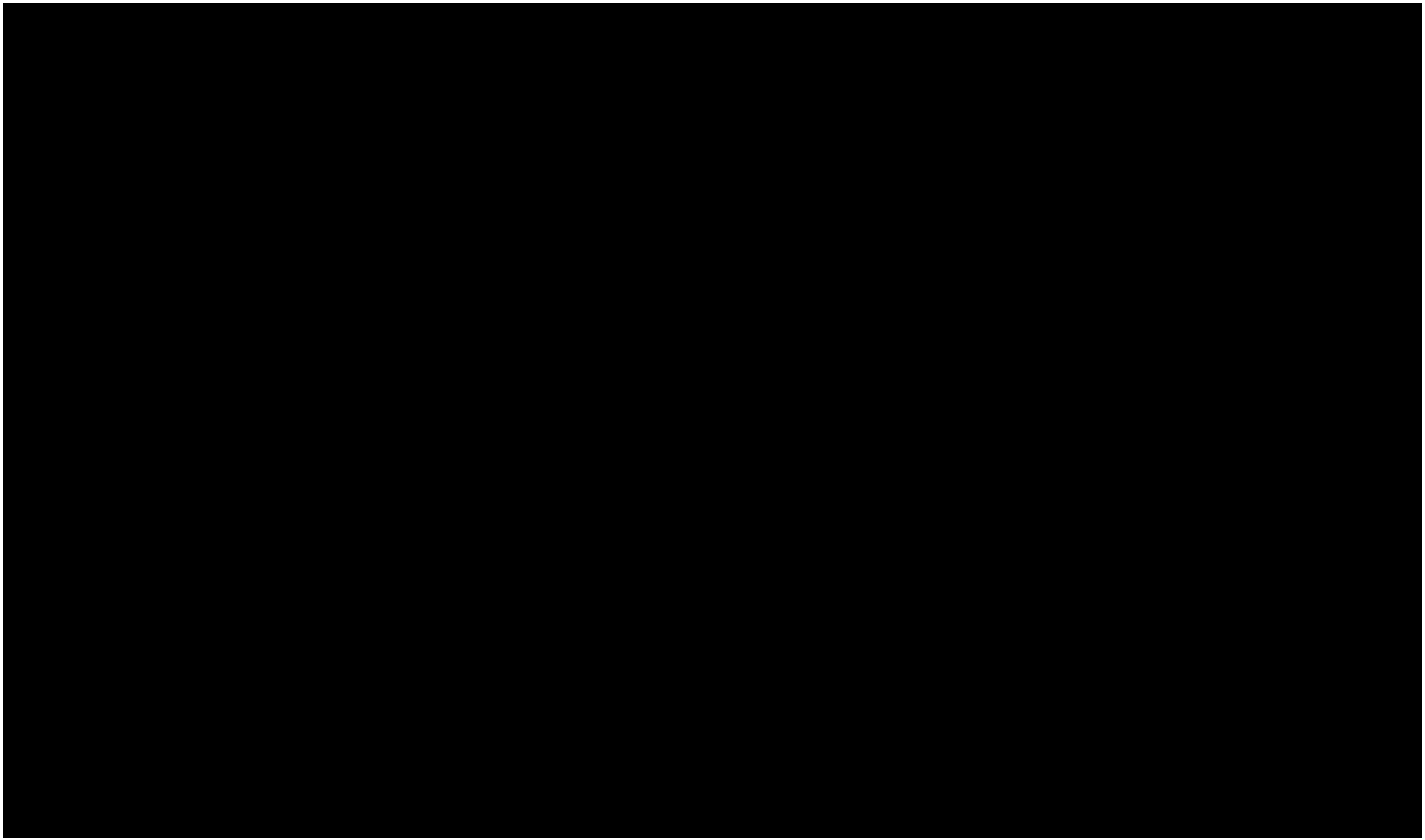
- News Stations
- Professional Photographers
- Surveillance
- Everyone

But Why Canon?!

- We love Canon
- Canon has 40% of the DSLR Camera Market Share
- Over 20 Million Sold in 2019 alone
- Used by *many* people
- Has PTP Support

PTP

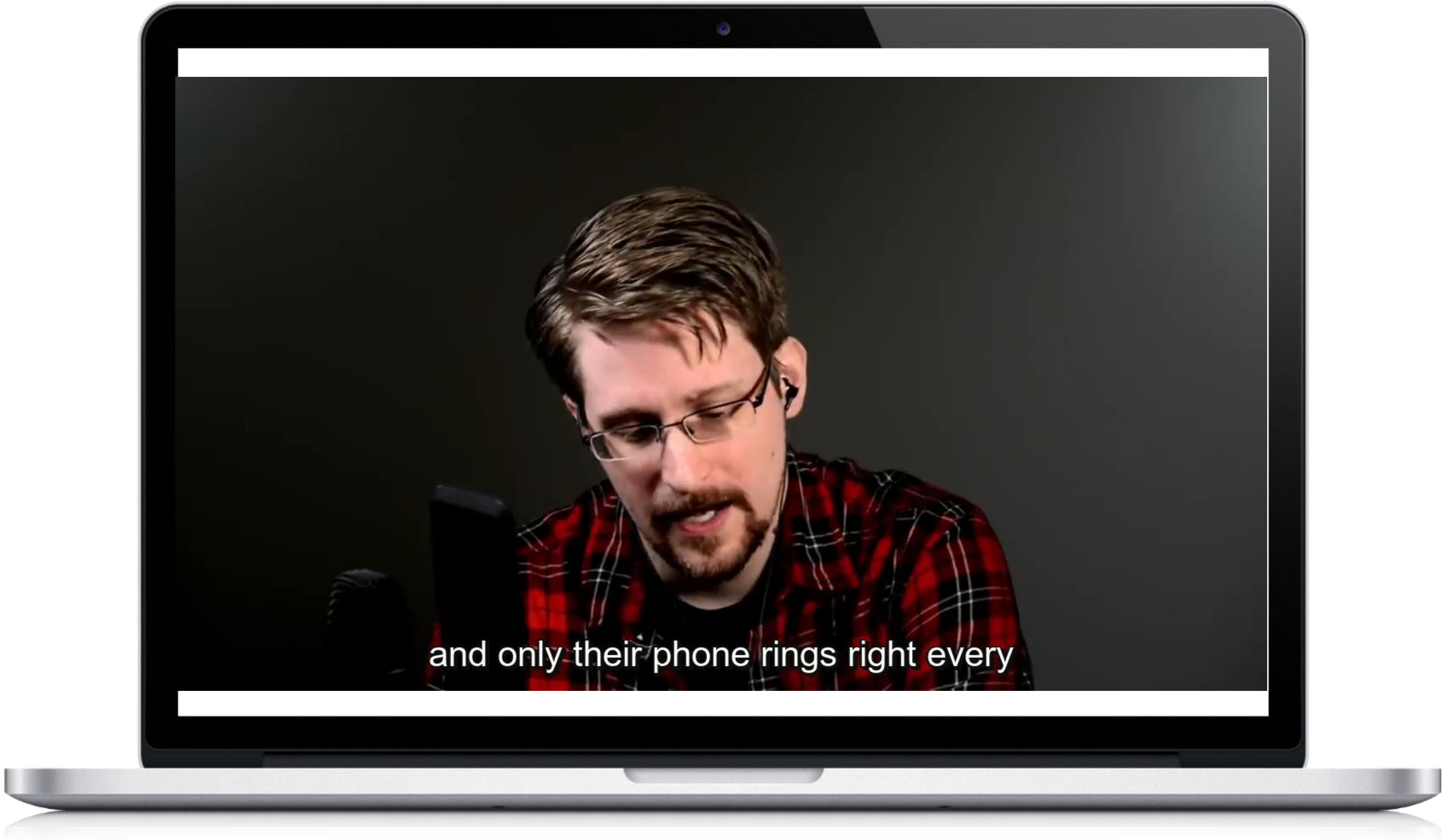
- “Picture Transfer Protocol”
- Designed at 2001
- Originally intended for any picture transfer
- Today commonly referred to picture transferring over WiFi



Effective Mobile Threats Cost Millions of $$$

Mobile Threat Landscape

- In today's world mobile attacks are difficult to implement
- OS mitigations are very effective
- A successful attacks very limited
- Breaching the OS limits costs $$$


and only their phone rings right every

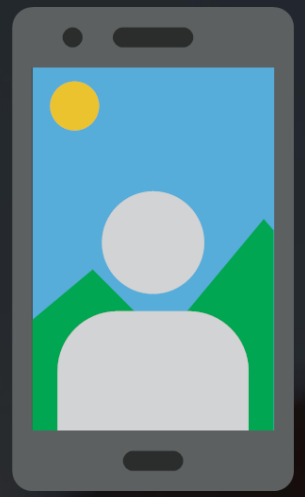
Here I am Here I am…

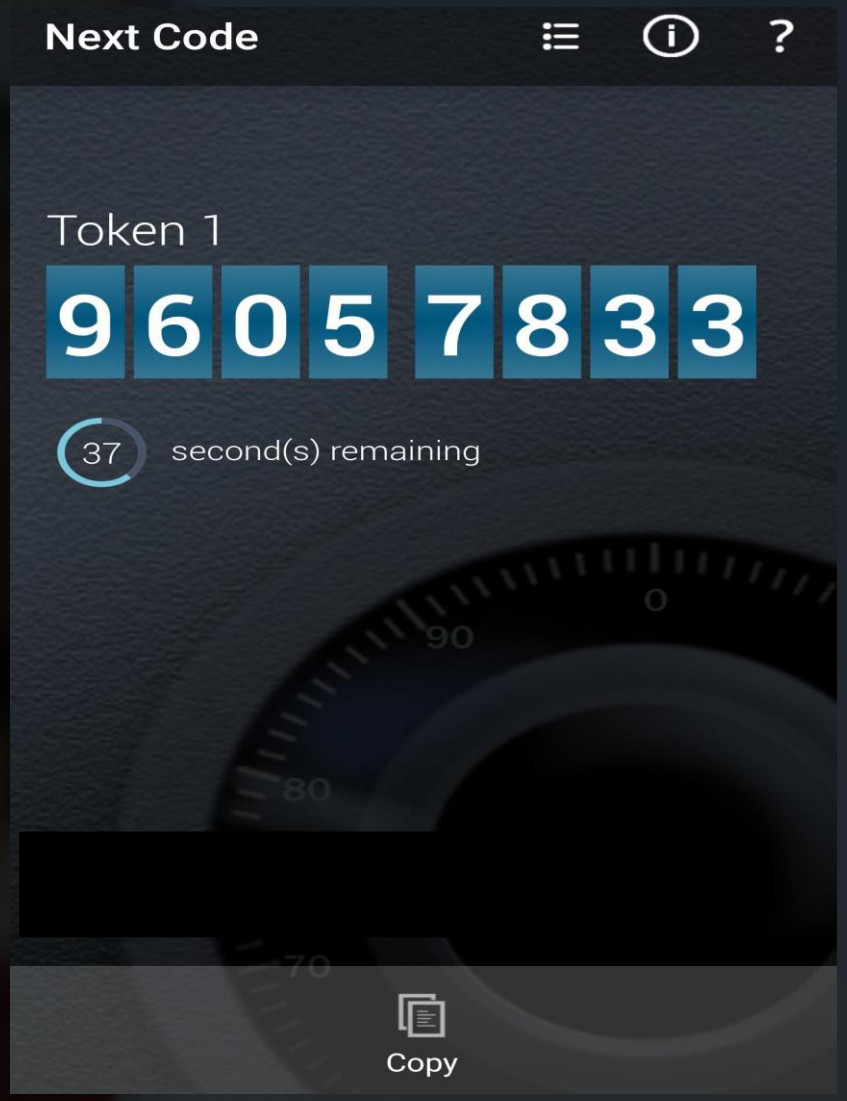
- The operator sends a special message as soon as it detects a new device on the network
- It's been Used to deploy the operator-specific settings, such as the address of MMS service center
- The message format is defined by *Open Mobile Alliance*

Open Mobile Alliance

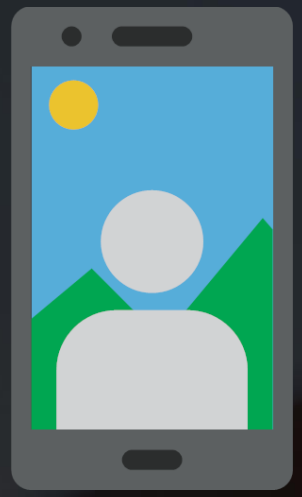
- Standards body coordinating the mobile industry
- Members are equipment & software vendors, and network operators
- Board of Directors includes representatives (as of this year) from ARM, AT&T, Ericsson, Intel, Nokia, Orange, Qualcomm, Sierra Wireless & T-Mobile

Standard Mobile Use Case…

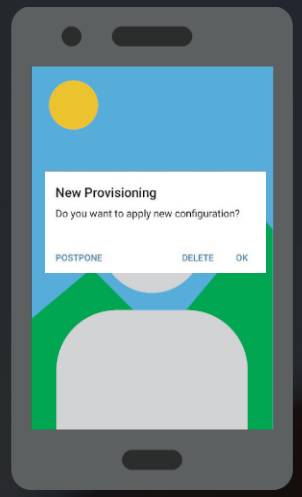




Standard Mobile Use Case…



OTA Provisioning



MMS Message Server

Browser Homepage

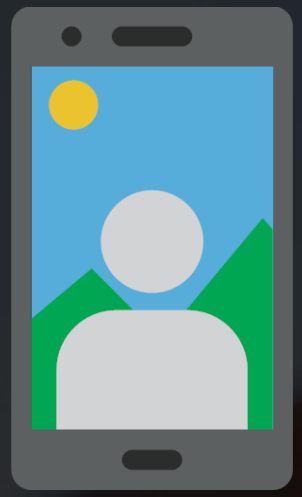
Mail Server

Directory Server

Proxy Server

And More…

OTA Provisioning



MMS Message Server

Browser Homepage

Mail Server

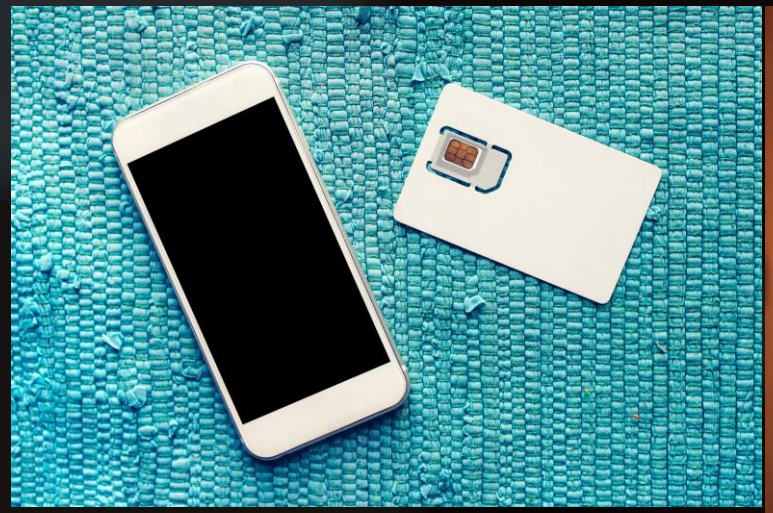
Directory Server

Proxy Server

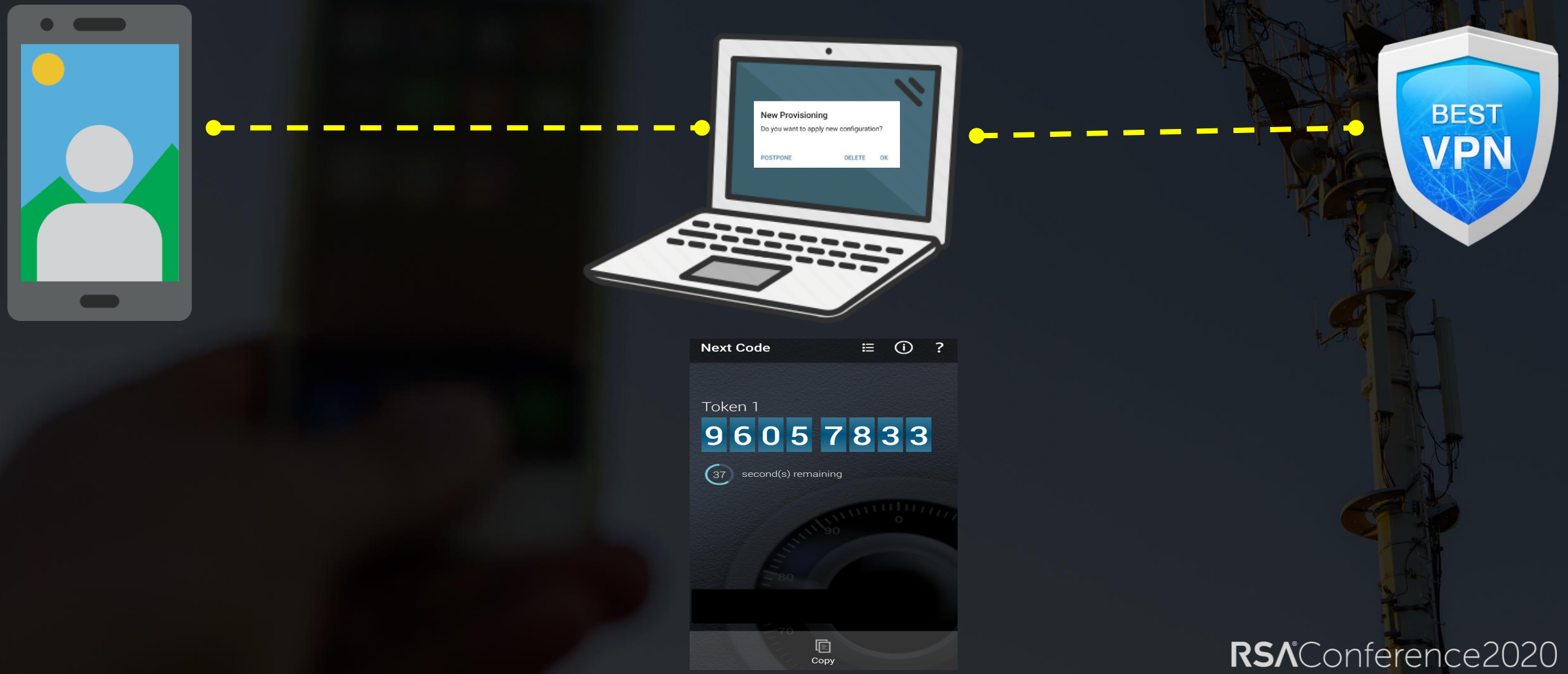
And More…

Authentication

- Usually authentication is based on IMSI
- In some cases – no authentication at all
- Messages do not provide any visual indicator



Breaking the Mobile Misconception

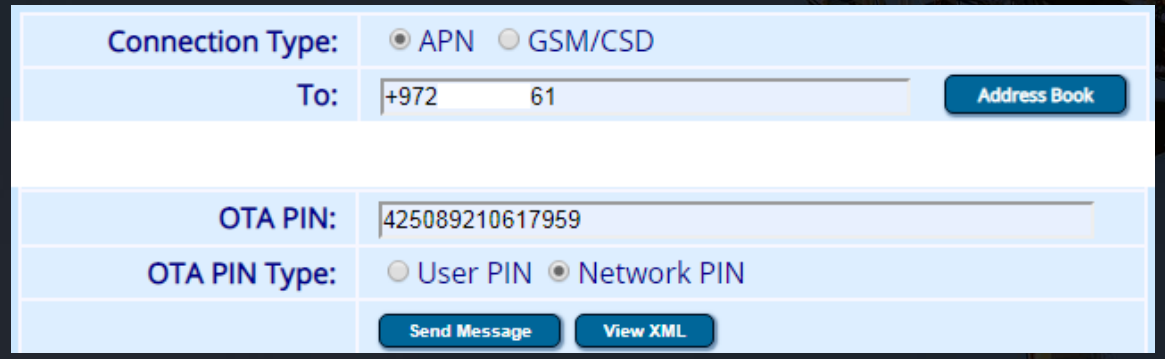


Breaking the Mobile Misconception

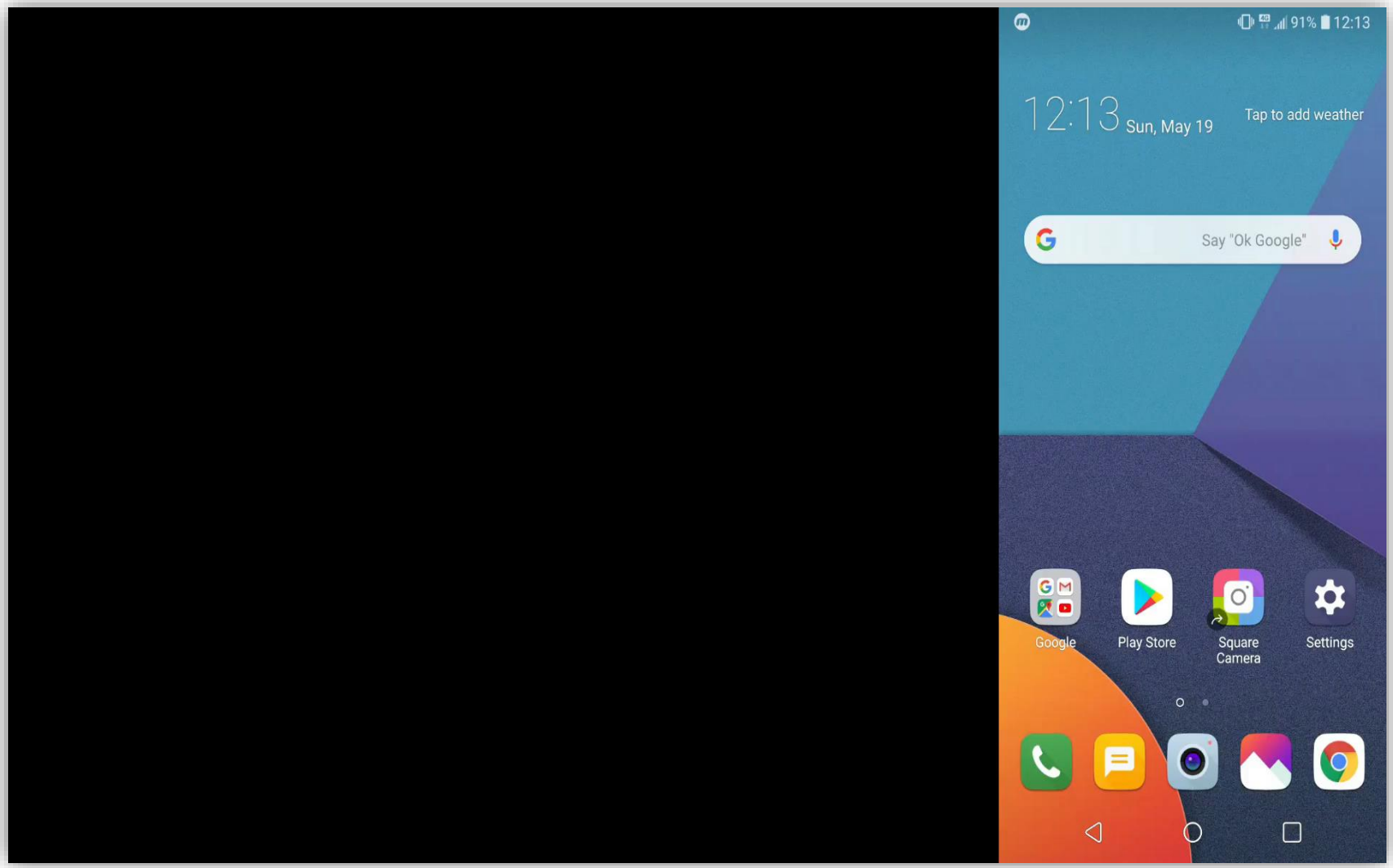
USB GSM dongle
(~30$) + SIM

+

Simple Script to build CP PDUs
(NowSMS)



=


91% 12:13
12:13 Sun, May 19
Tap to add weather
Say "Ok Google"
Google
Play Store
Square Camera
Settings

We know everything about Email Based attacks

Email Attacks

- Email is leading the attack vectors
  - Malicious Attachments
  - “Drive-By” malicious links
  - Documents (read: Office Macros)
- Defiantly not new
- Certainly not sophisticated

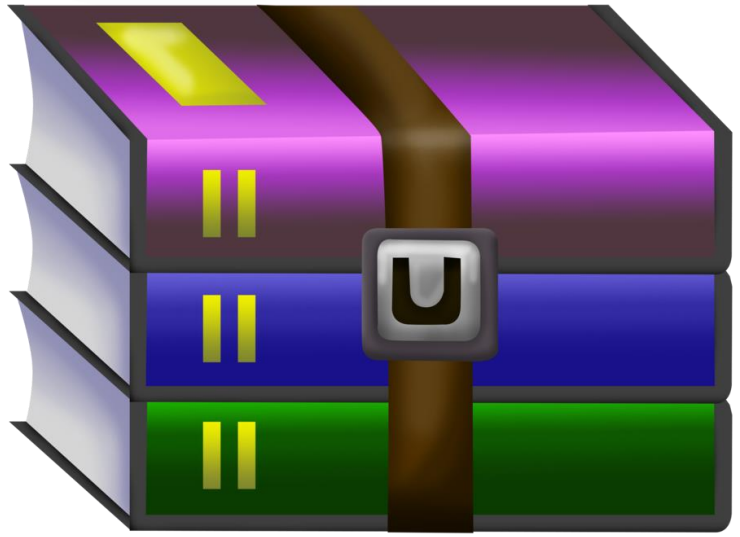
EASY TO DETECT

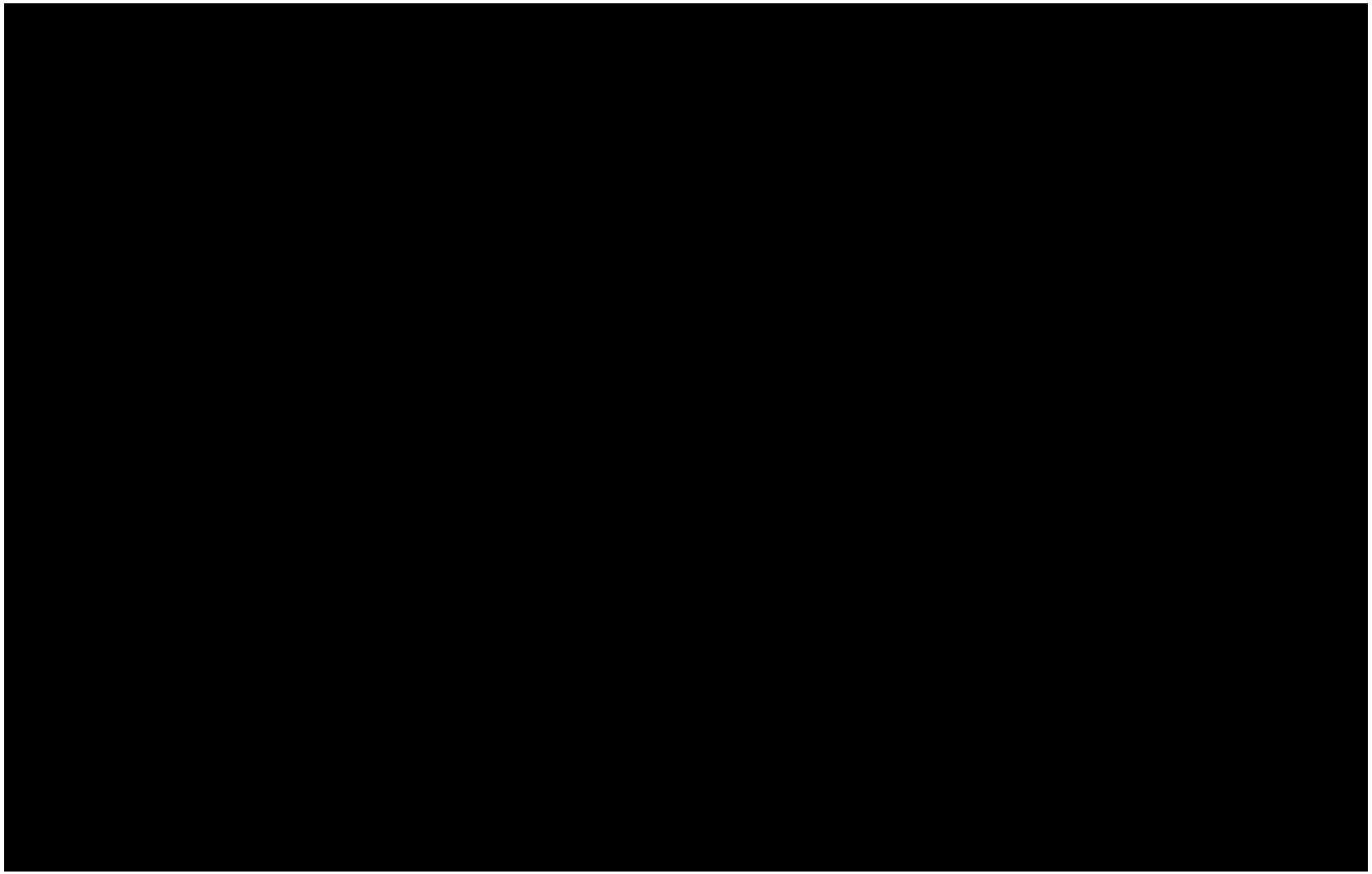
ACE

- Proprietary compression algorithm
- Created in 1991
- Today, mostly unmaintained
- Supported by WINRAR only (!!!)

WINRAR

- File archiver utility for Windows
- Over 30 supported archive file types
- Endless trial version \o/
- Over 500 Million install base (!!!)

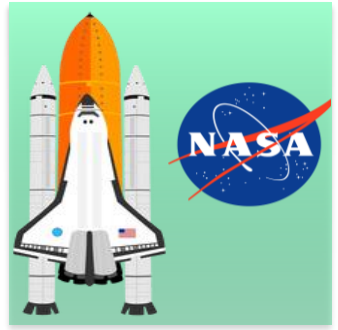




If its been well reviewed, its considered safe

SQLite

- SQLite is the most famous Embedded Database
- A light Database
- All information is stored on a single SQLite file
- Has over a TRILLION installations
- One of the mostly commonly used databases
- One of the most **commonly reviewed** databases



SQLite Vulnerability Use Case

Issue when loading malicious SQLite Database

- WebSQL
- Web API
- Queried from JS
- SQLite Backend

- CVE 2015-7036
- BH2017 – Chaitin
- Magellan

SQLite Vulnerability Use Case

Issue when loading malicious SQLite Database

SQLite Vulnerability Use Case

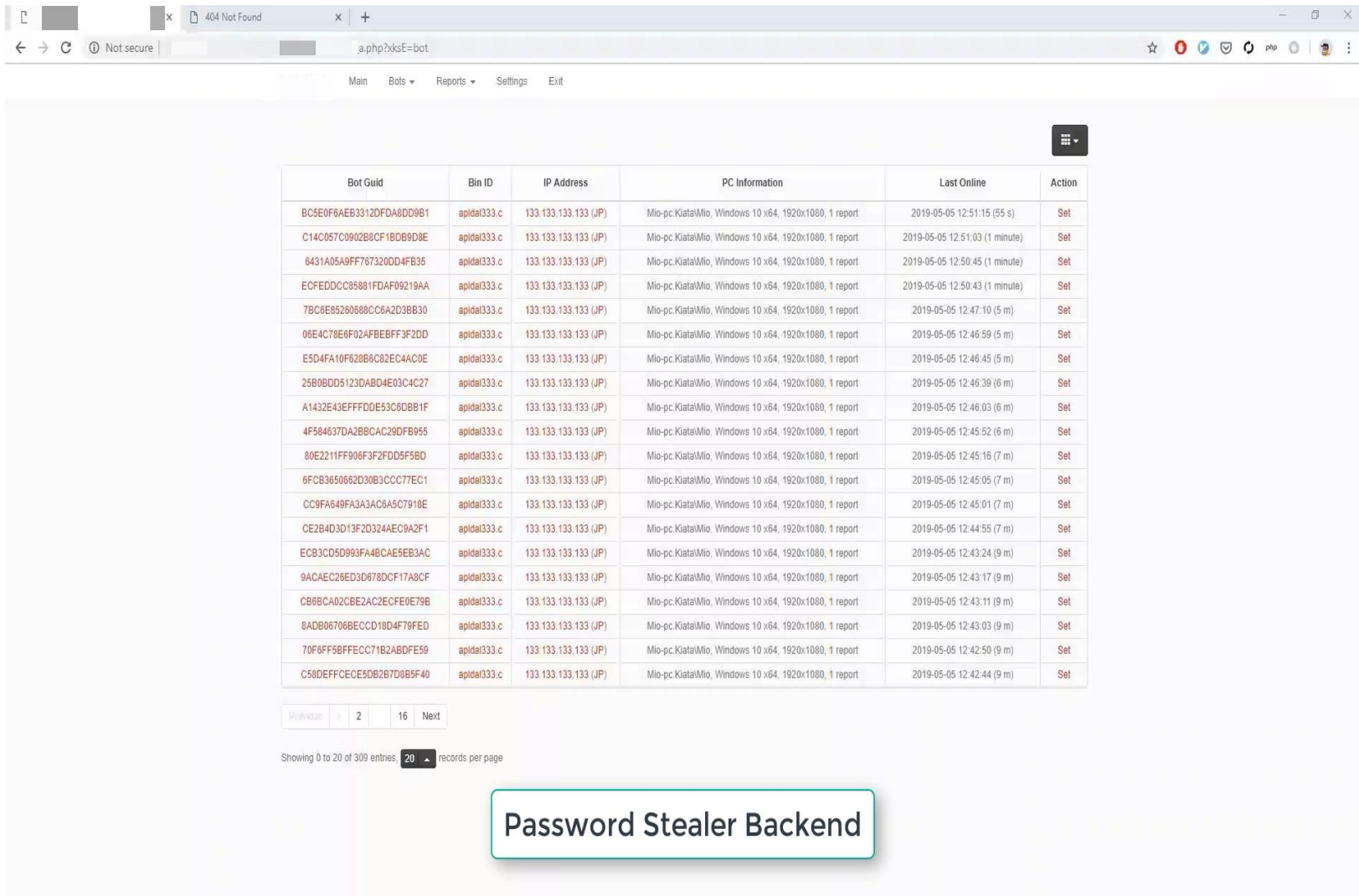
Issue when loading malicious SQLite Database

”InfoStealer” Malware Backend

Privilege Escalation on Windows/Linux

Persistence on Mobile Devices

CVE 2019-8602
CVE 2019-8600
CVE 2019-8577
CVE 2019-8598
...


404 Not Found
Not secure
a.php?xksE=bot
Main
Bots
Reports
Settings
Exit
Bot Guid
Bin ID
IP Address
PC Information
Last Online
Action
BC5E0F6AEB3312DFDA8DD9B1 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:51:15 (55 s) Set
C14C057C0902B8CF1BDB9D8E apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:51:03 (1 minute) Set
6431A05A9FF767320DD4FB35 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:50:45 (1 minute) Set
ECFEDDCC85881FDAF09219AA apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:50:43 (1 minute) Set
7BC6E85260688CC6A2D3BB30 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:47:10 (5 m) Set
06E4C78E6F02AFBEBFF3F2DD apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:46:59 (5 m) Set
E5D4FA10F628B6C82EC4AC0E apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:46:45 (5 m) Set
25B0BDD5123DABD4E03C4C27 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:46:39 (6 m) Set
A1432E43EFFFDDE53C6DBB1F apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:46:03 (6 m) Set
4F584637DA2BBCAC29DFB955 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:45:52 (6 m) Set
80E2211FF906F3F2FDD5F5BD apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:45:16 (7 m) Set
6FCB3650662D30B3CCC77EC1 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:45:05 (7 m) Set
CC9FA649FA3A3AC6A5C7918E apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:45:01 (7 m) Set
CE2B4D3D13F2D324AEC9A2F1 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:44:55 (7 m) Set
ECB3CD5D993FA4BCAE5EB3AC apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:43:24 (9 m) Set
9ACAEC26ED3D678DCF17A8CF apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:43:17 (9 m) Set
CB6BCA02CBE2AC2ECFE0E79B apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:43:11 (9 m) Set
8ADB06706BECCD18D4F79FED apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:43:03 (9 m) Set
70F6FF5BFFECC71B2ABDFE59 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:42:50 (9 m) Set
C58DEFFCECE5DB2B7D8B5F40 apidal333.c 133.133.133.133 (JP) Mio-pc.Kiata\Mio, Windows 10 x64, 1920x1080, 1 report 2019-05-05 12:42:44 (9 m) Set
2
16
Next
Showing 0 to 20 of 309 entries
20
records per page
Password Stealer Backend

Application Stores are Bullet Proof

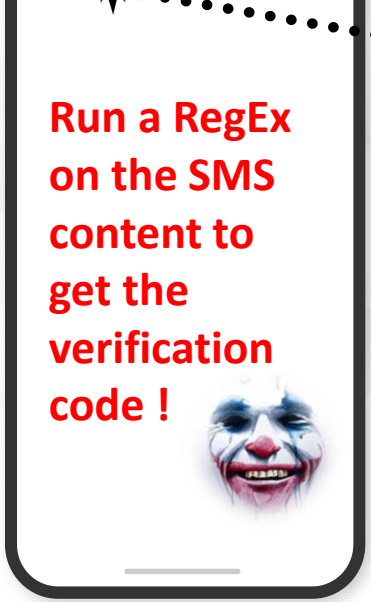
Steals SMSs and number of Android contacts

Steals Device information

your money!

THE JOKER MECHANISM :

The User installs malicious app with a dropper from the Play Store



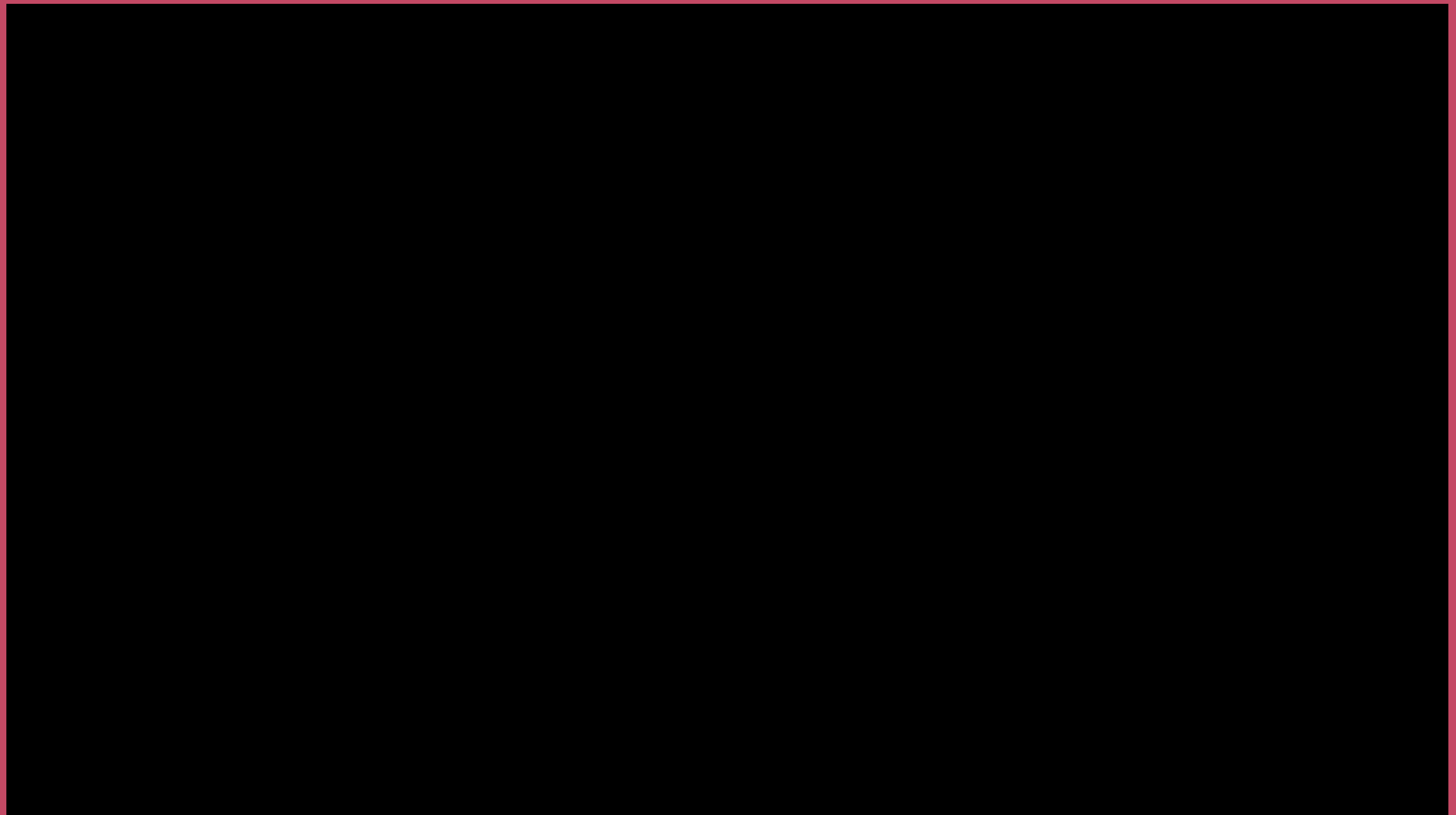
Loading of 2nd stage malware

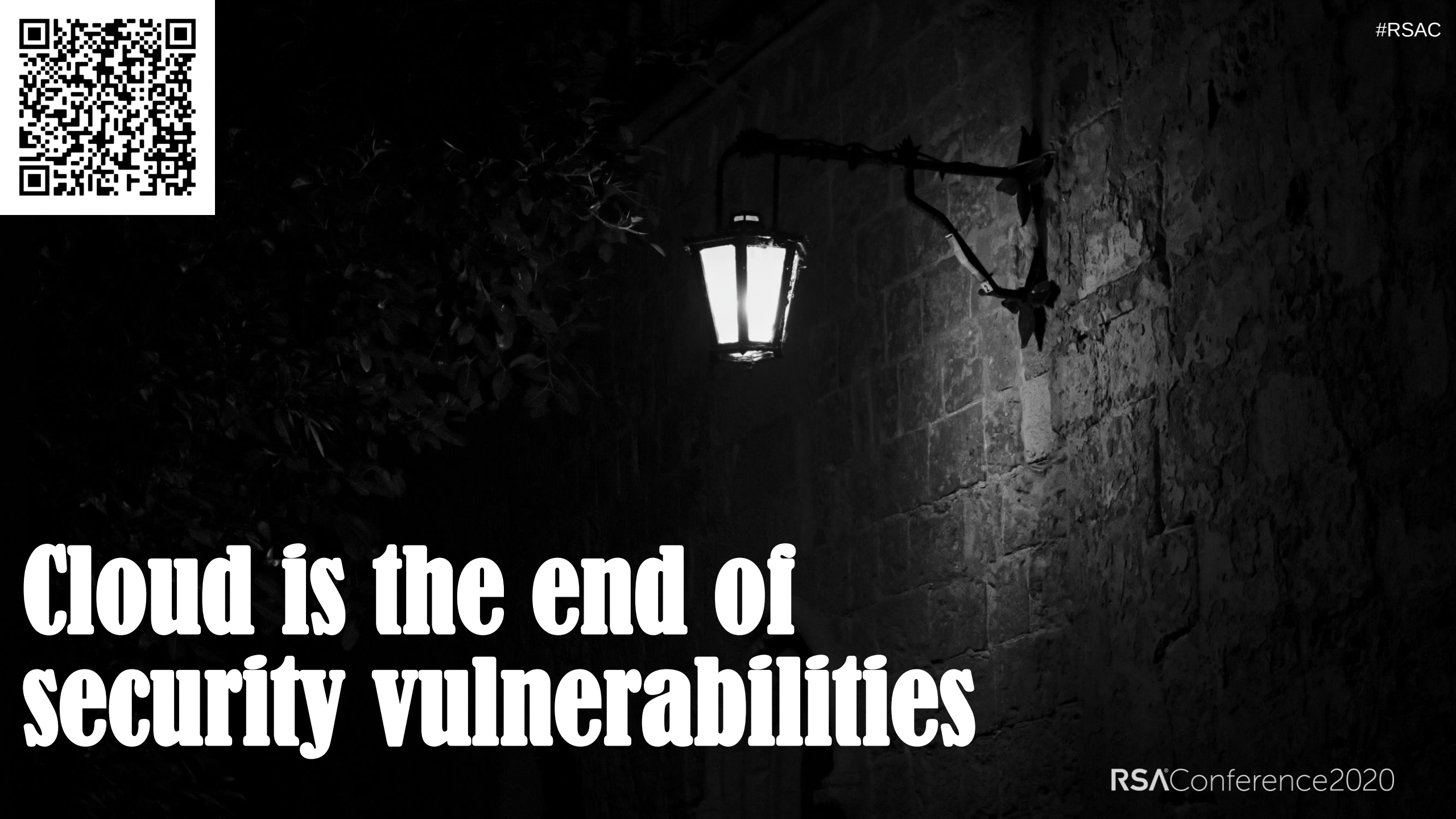
Check country via MCC
Use notification listener to grab SMS
Register the victim to premium services

The App communicates with Command & Control server to start malicious activity. Launching the 2nd stage of the malware configuration.

1-days in Google Play

- A mobile app typically uses dozens of reusable components written.
- An app may keep using the outdated version of the code even years after the vulnerability is discovered.
- long-known vulnerabilities may persist even in apps recently published on Google Play
- The following demo shows the PoC video file from the original CVE-2016-3062 report causing the latest version of VivaVideo app (com.quvideo.xiaoying, over 100 million downloads) to crash.

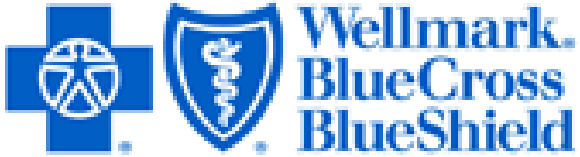




Cloud is the end of security vulnerabilities

Azure

- Microsoft Cloud Solution
- Top 3 Cloud Infrastructure World Wide
- Millions Of Users



Just Someone Else's Computer…

Business Process

Patient Data

Financial Transactions

Business Data

Just Someone Else's Computer…

Business Process

Patient Data

Financial Transactions

Business Data

Just Someone Else's Computer…

Workload

Workload

Workload

Workload

Workload

Workload

Workload

Workload

Workload

Workload

Workload

Workload

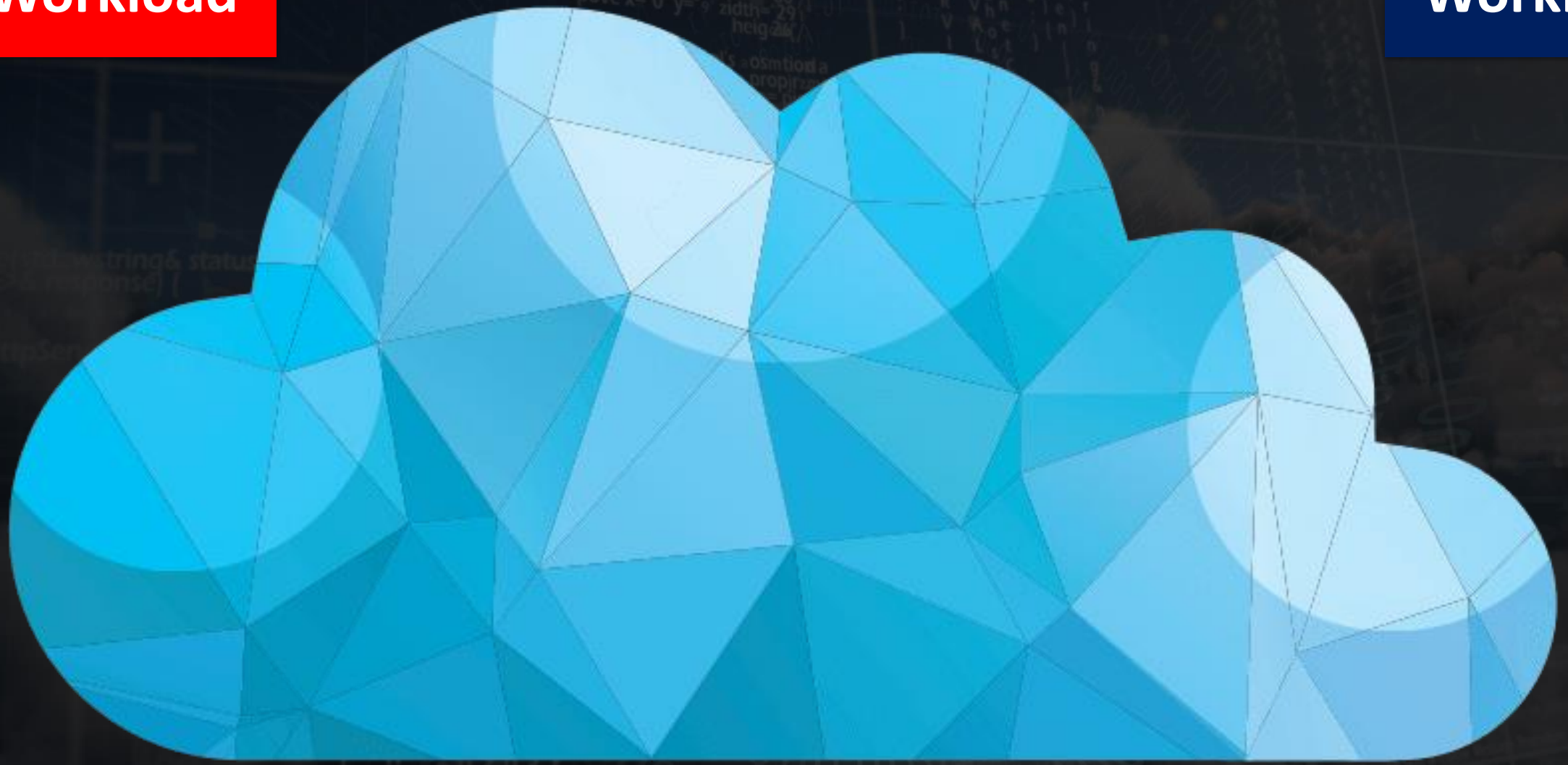
Workload

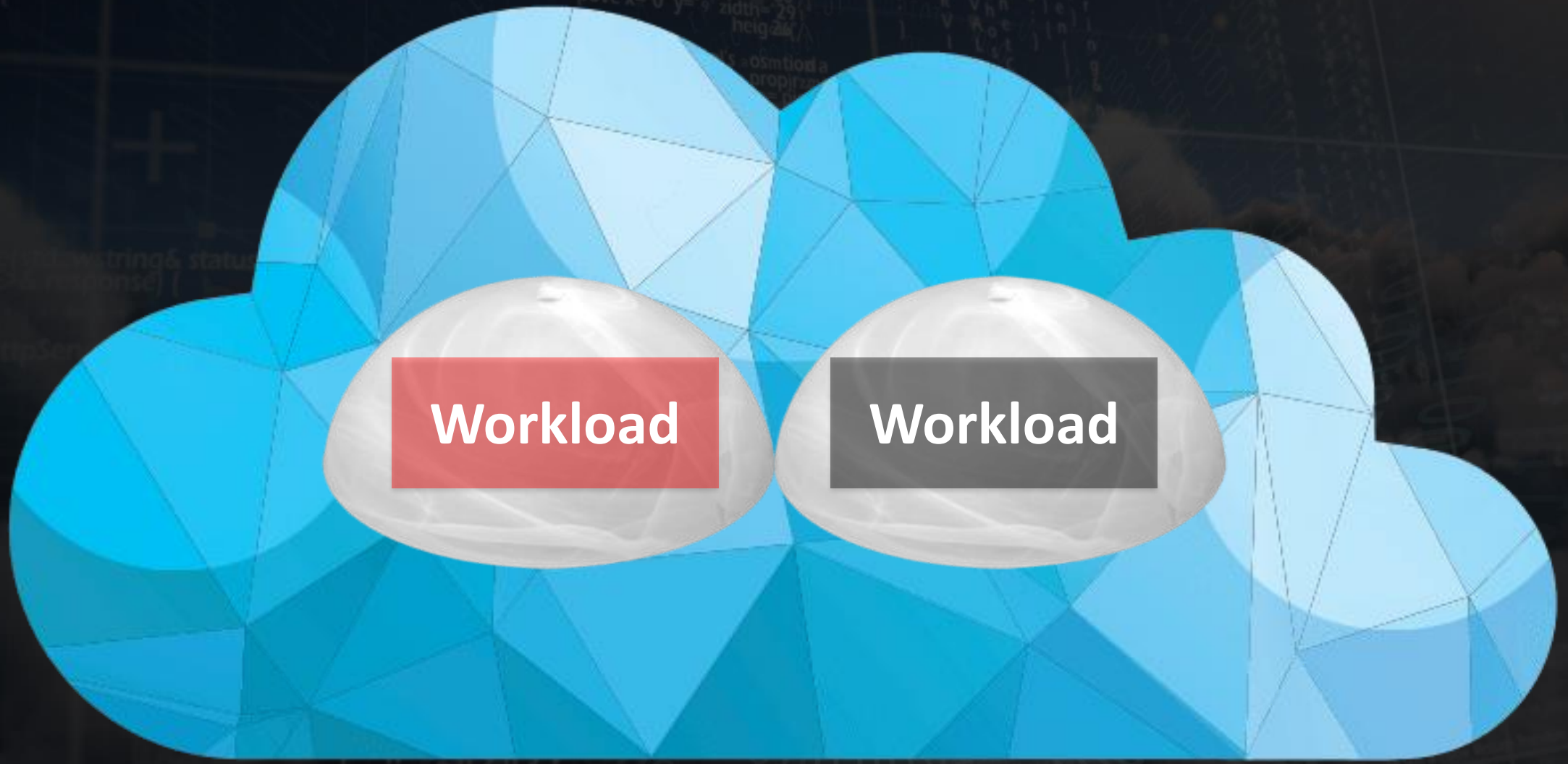
Workload

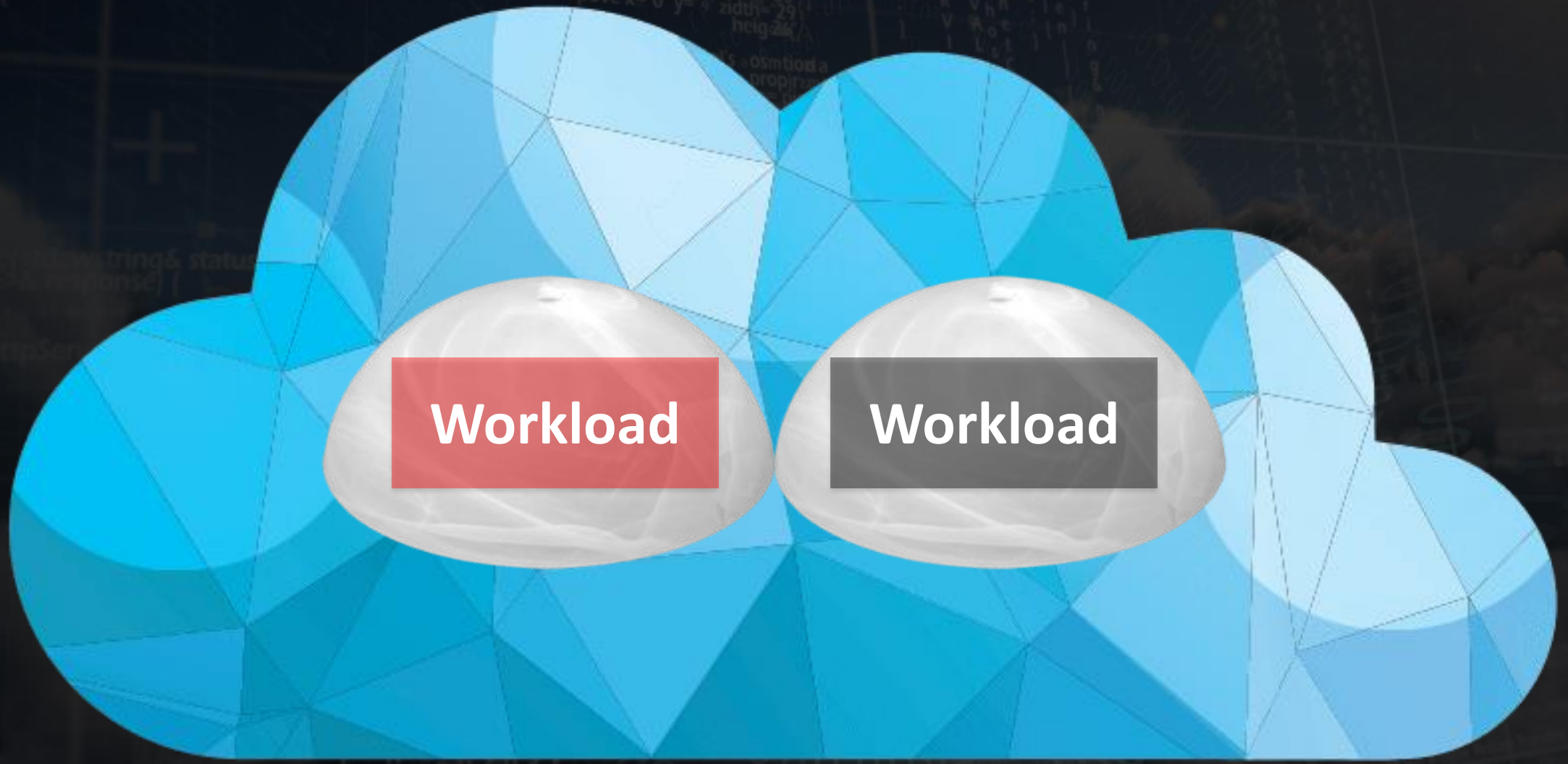
Workload

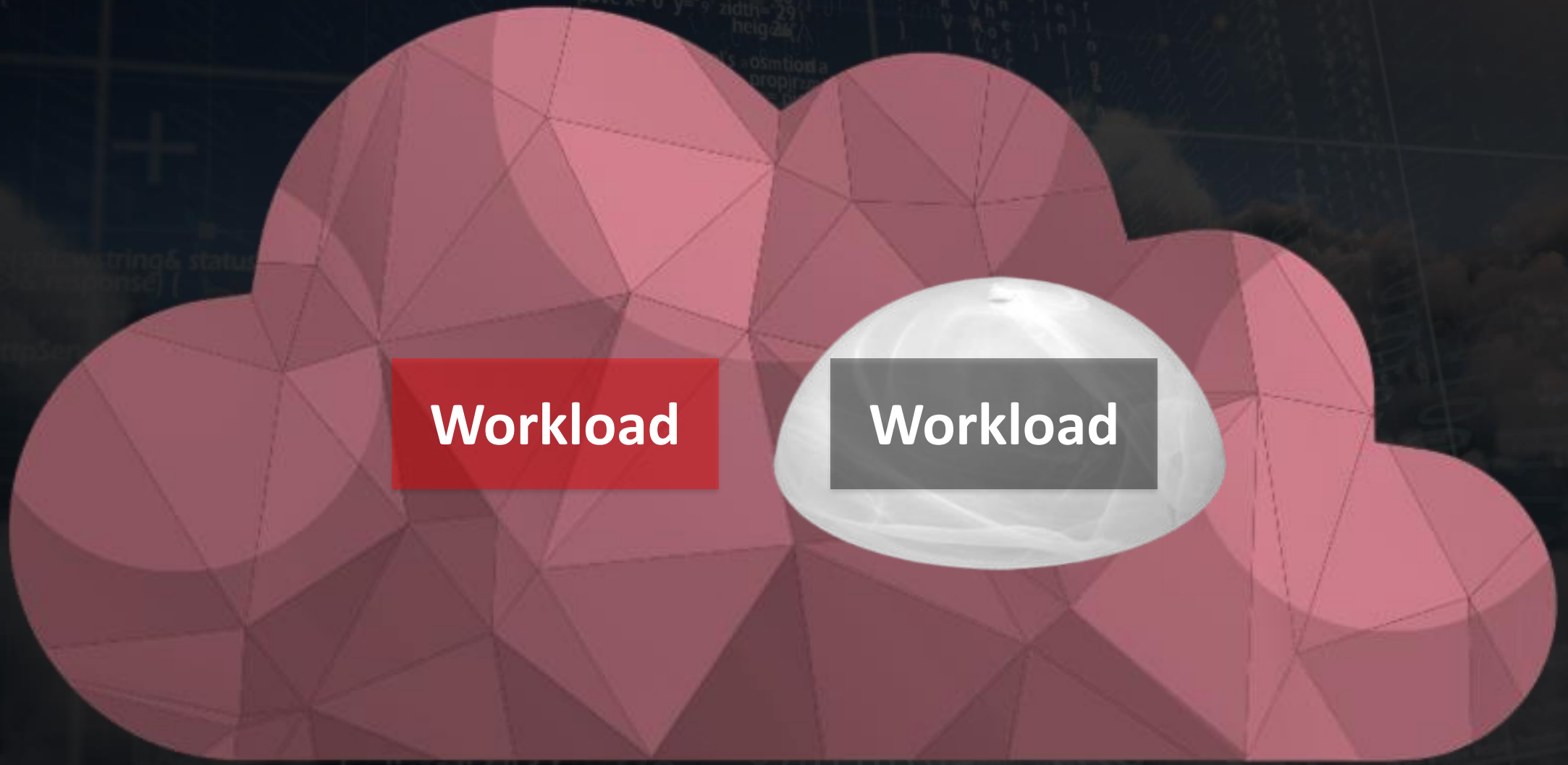
Workload

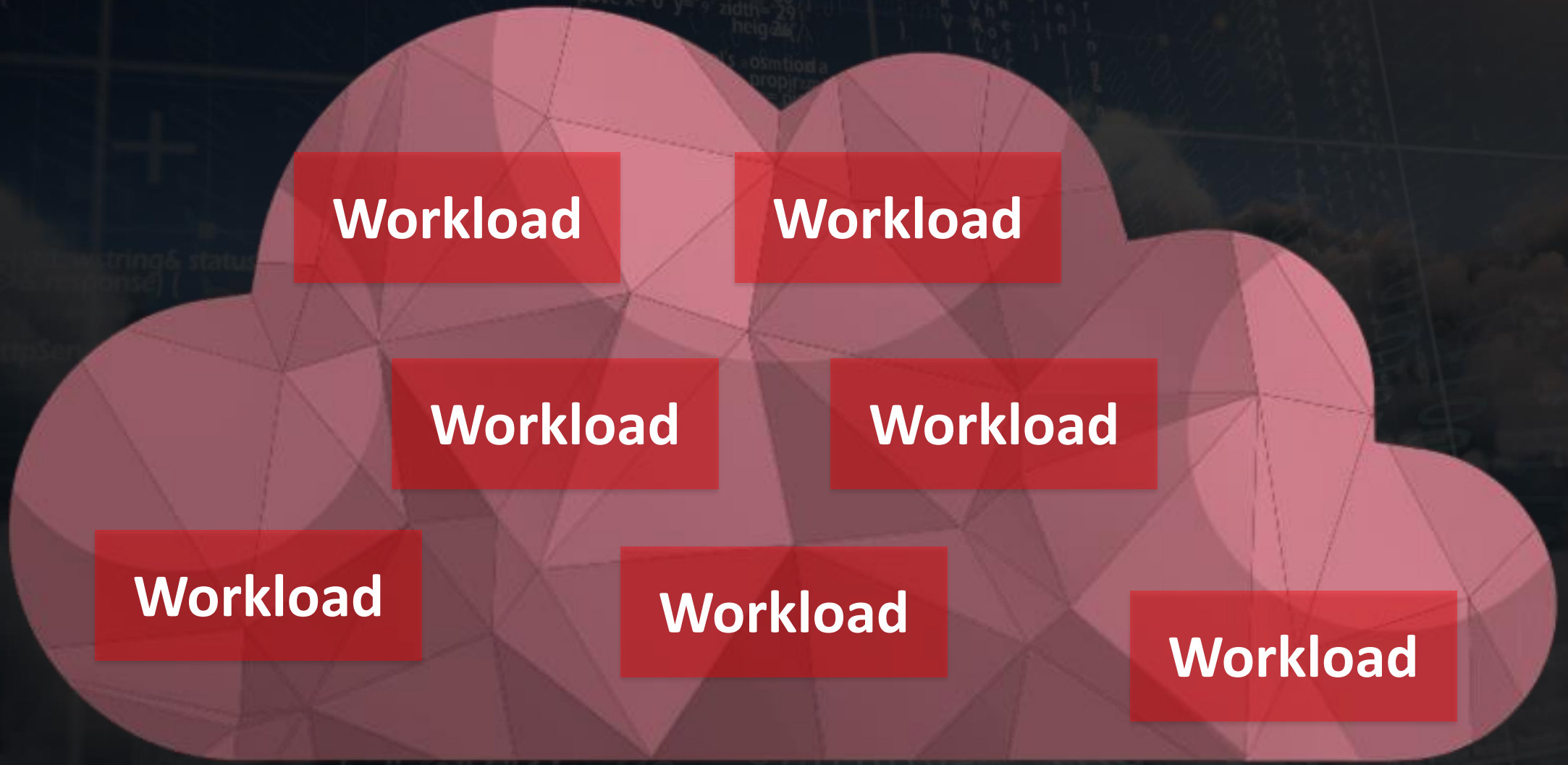
Workload




Workload
Workload


Workload
Workload


Workload
Workload


Workload
Workload
Workload
Workload
Workload
Workload
Workload


Look for The Dark Corners of
Your Battle

Don’t Fall For Rumors

New Technology Comes With a Risk


Take Your Time to
Review Each New
Device\Technology


Apply to Your Risk Model


We will all (most probably) have job security for a long time ☺


cp<r>
CHECK POINT RESEARCH
#RSAC
THE
END
RESEARCH.CHECKPOINT.COM
CPRESEARCH
RSAConference2020