





CHECK POINT RESEARCH

**MISSION**

**IMPOSSIBLE**

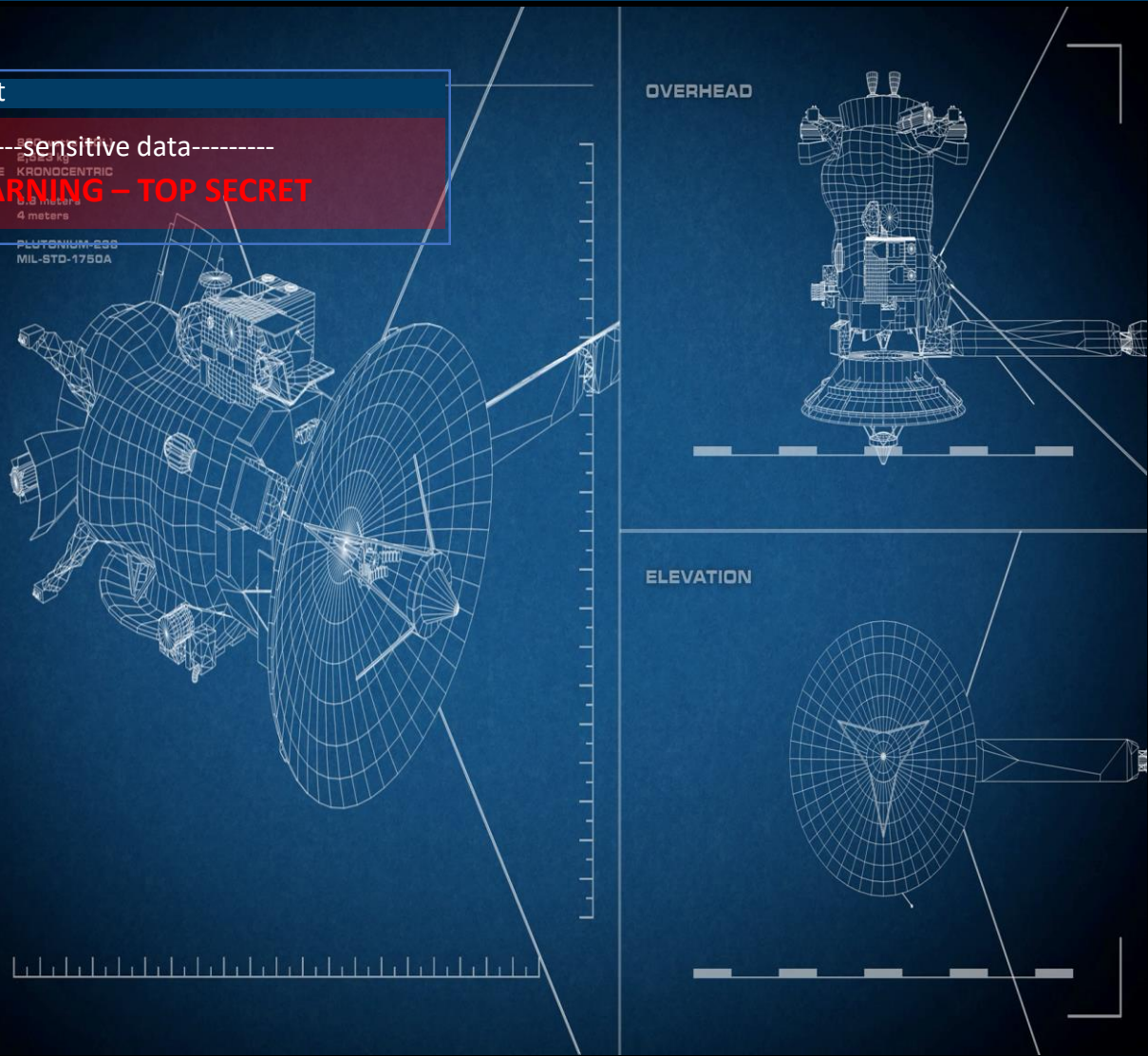
Mission View  
cyber satellite

**Alert**

sensitive data-----  
**WARNING - TOP SECRET**

BUS REFERENCE KRONOCENTRIC  
 WEIGHT 12.5 kg  
 LENGTH 10.50 meters  
 WIDTH 4 meters

POWER PLUTONIUM-238  
 CPU MIL-STD-1750A



View Targets Location 21" 84" 12"

Location view  
top secured location



**Code view A**

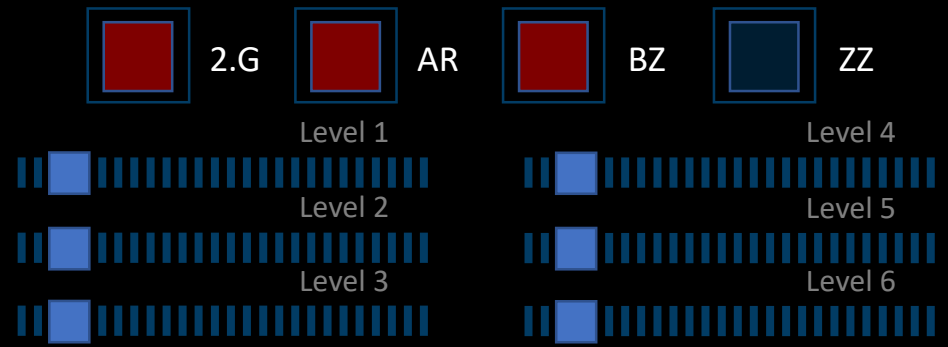
```
// Set up a generic event dispatcher
SimoPlugin.prototype.trackEvent = function(evt) {
    var c = evt['cat'];
    var a = evt['act'];
    var l = evt['lab'] || undefined;
    var v = evt['val'] || undefined;
    var x = {};
    x['nonInteraction'] = evt['ni'] || false;
    if (evt['di']) {
        x['dimension' + evt['di']] = evt['dv'] || undefined;
    }
    this.tracker.send('event', c, a, l, v, x);
};
providePlugin('simoPlugin', SimoPlugin);
})();
```

some text text 21" 84" 12"

Ground D ok active	Air Defense ok active	Space D ok active	Cyber D ok active
--------------------------	-----------------------------	-------------------------	-------------------------

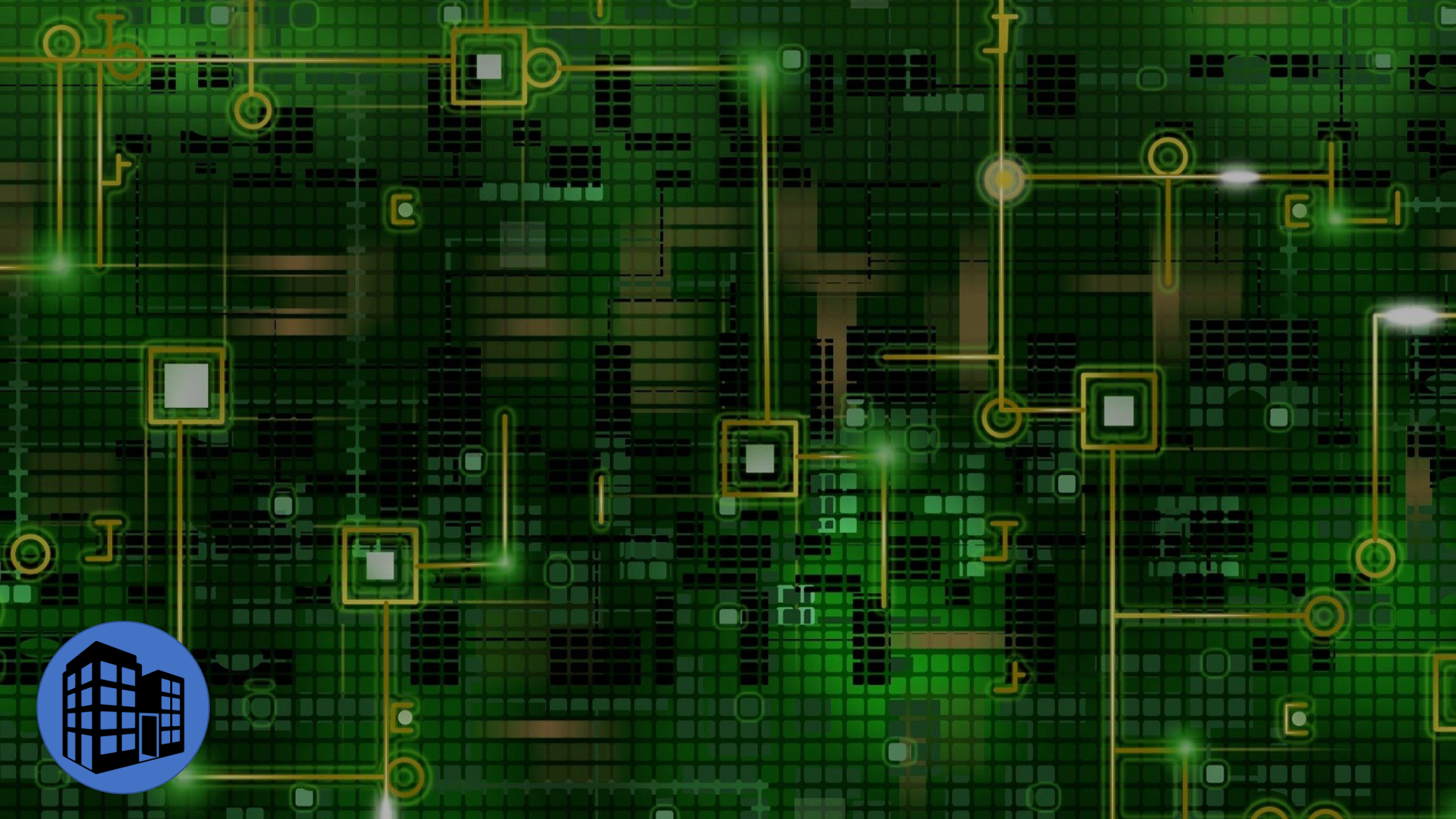
Defense Systems View  
Status - OK

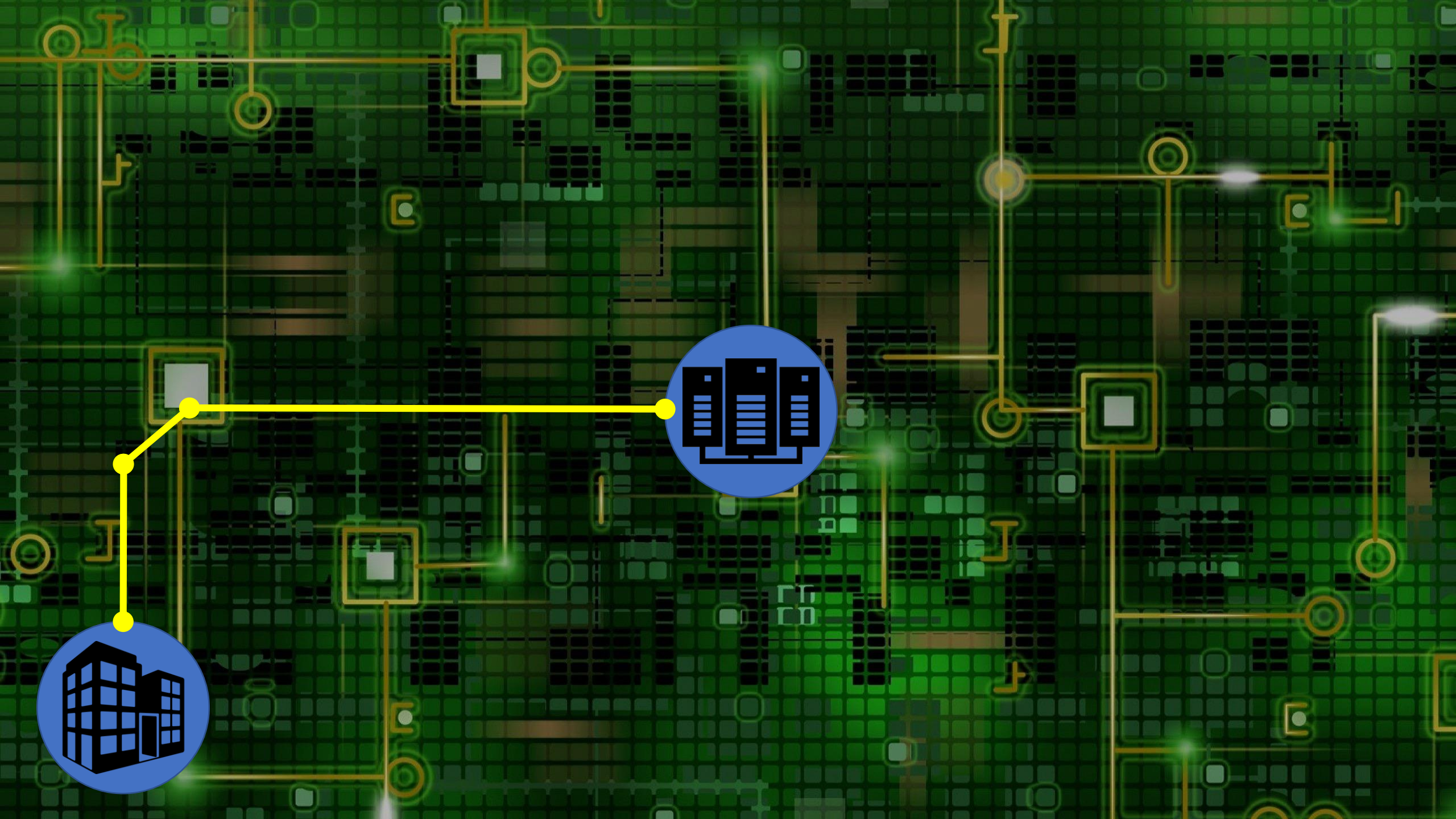
Target Defenses - Operational

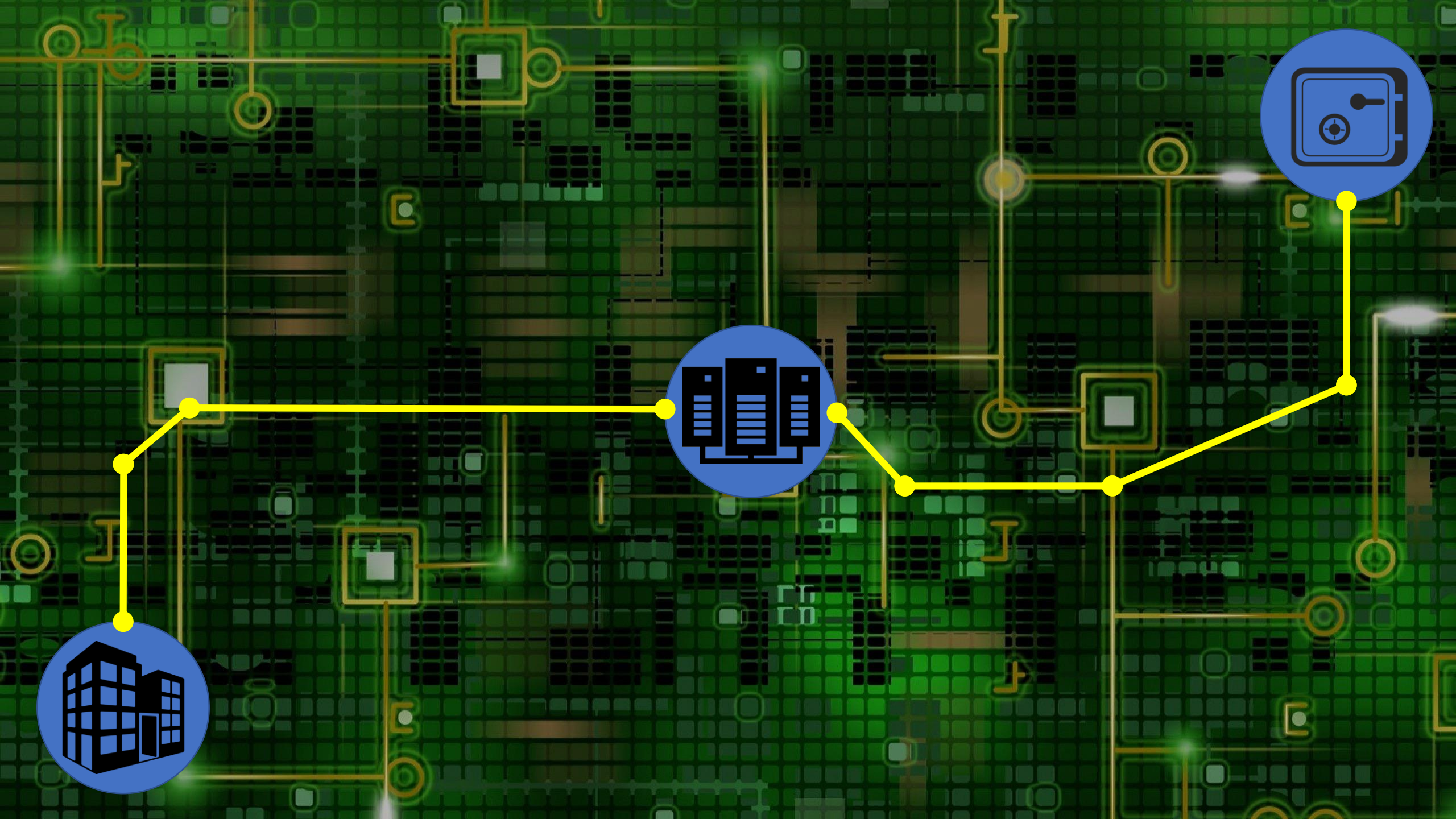


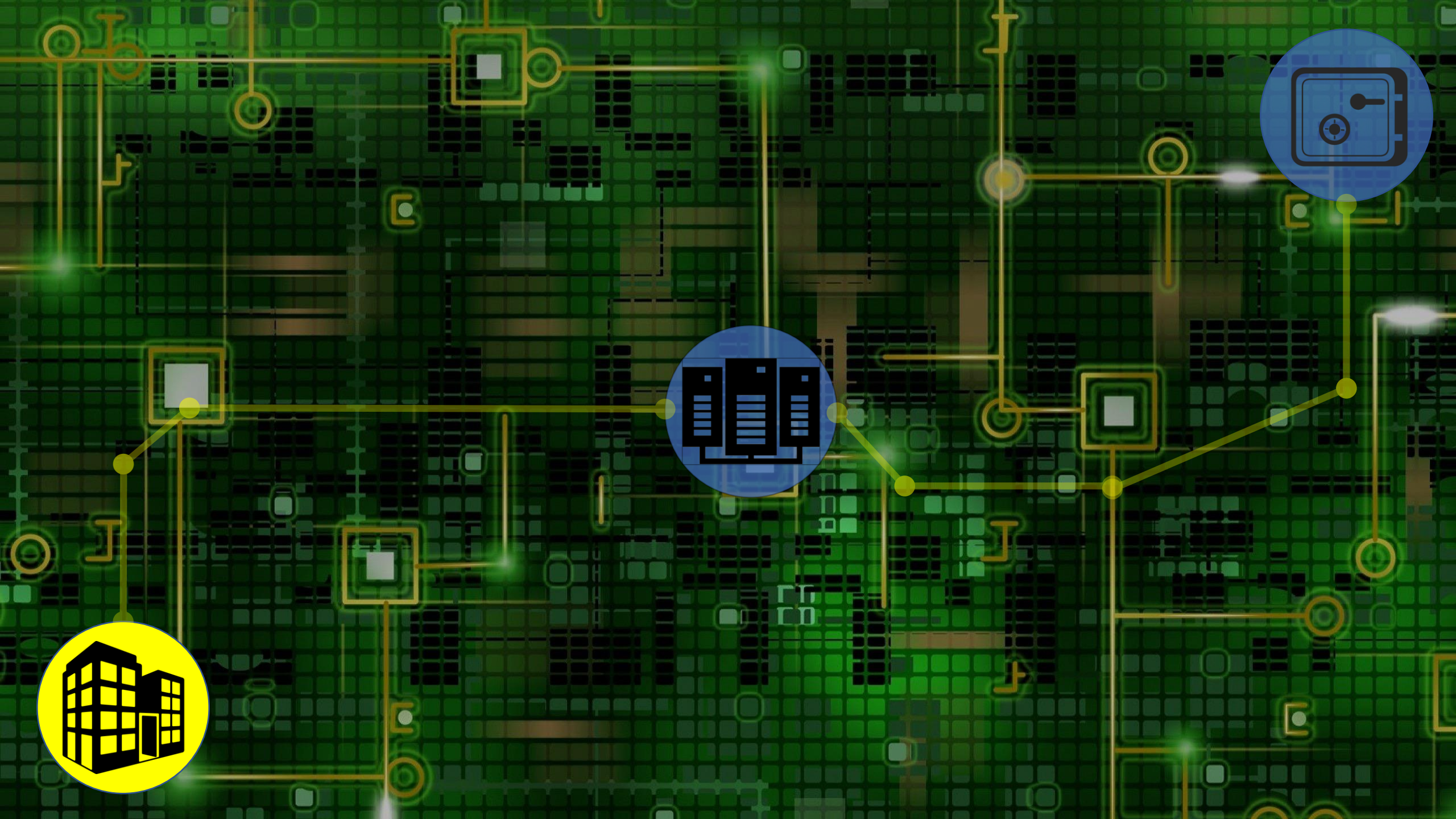
View targets Location 21" 84" 12"

















# EA Games Vulnerability Could Leave 300m Open to Account Hijacking

CONOR REYNOLDS  
27TH JUNE 2019

.....  
+ INCREASE / DECREASE TEXT SIZE -



 Add to favorites



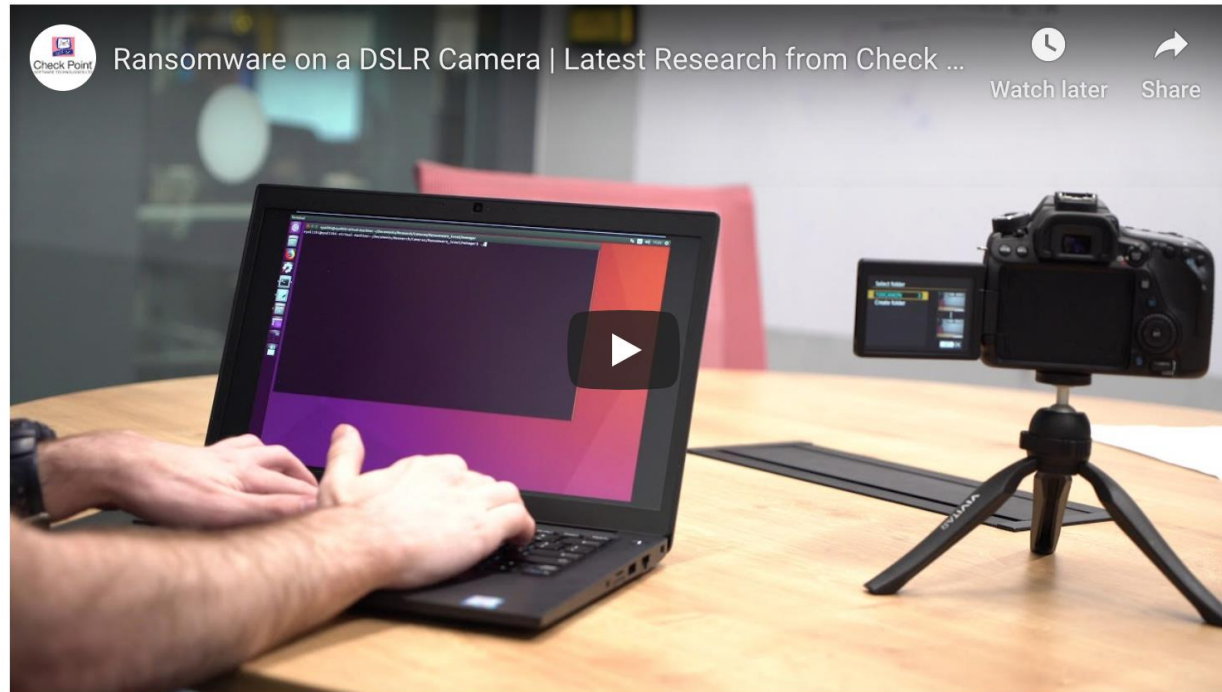
# Security researchers find that DSLR cameras are vulnerable to ransomware attack

14

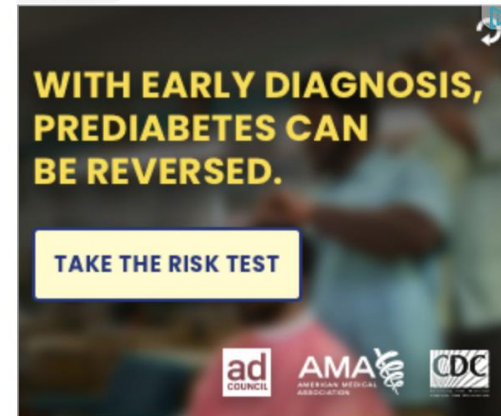
Canon has issued a security advisory and firmware patch for the vulnerability

By Andrew Liptak | @AndrewLiptak | Aug 11, 2019, 2:33pm EDT

f t SHARE



Advertisement



GOOD DEALS

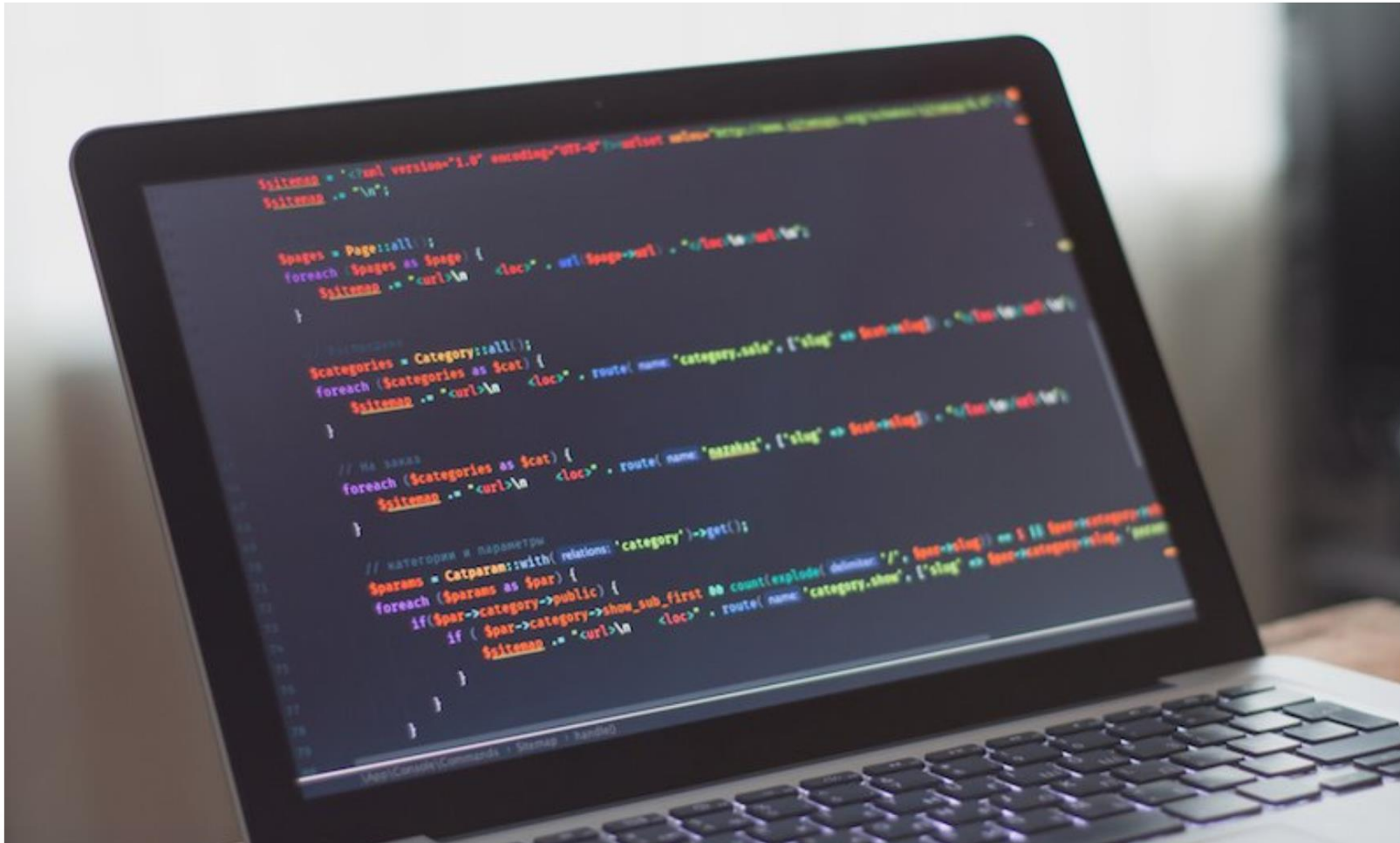


# MOBILE MADNESS Google bug affecting 2.5BILLION 'lets hackers steal emails with one text' – Samsung, Sony, Huawei and all Android phones affected, experts warn

REVEALED

[Sean Keach](#), Digital Technology and Science Editor  
4 Sep 2019, 14:00 | Updated: 4 Sep 2019, 14:54

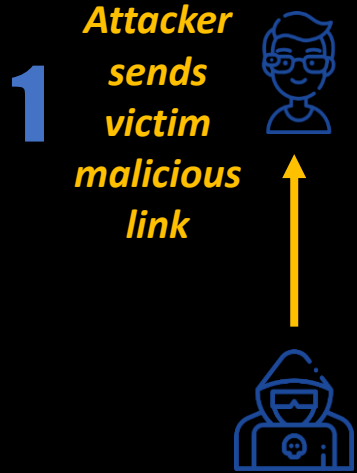
# 19-Year-Old WinRAR Flaw Plagues 500 Million Users











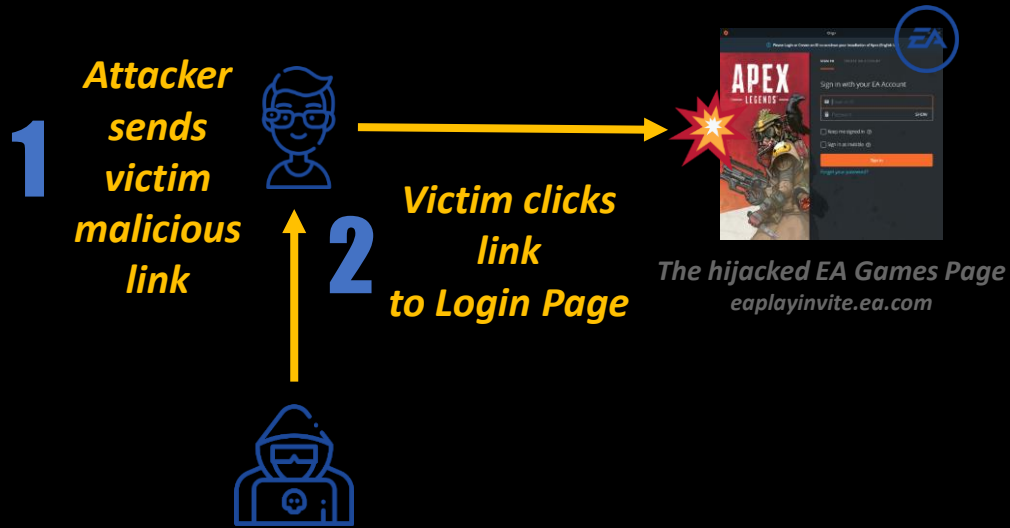
# EA GAMES

**90 Million** Users  
\$5 Billion Revenue



Mission View

Game Console



Target View

EA GAMES



Vulnerable Product

21" 84" 12"

Target Details

Description

# EA GAMES

90 Million Users  
\$5 Billion Revenue



G.28912

21" 84" 12"

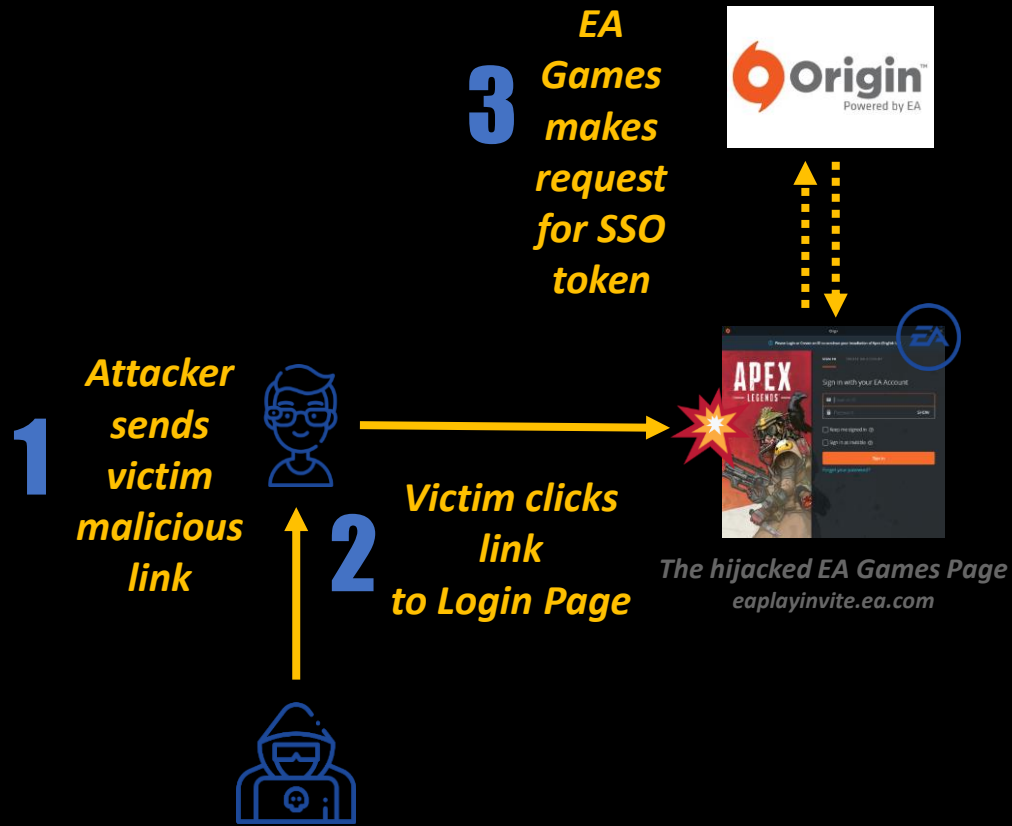
View Targets

Location

21" 84" 12"

Mission View

Game Console



Target View

EA GAMES



Vulnerable Product

21" 84" 12"

Target Details

Description

# EA GAMES

90 Million Users  
\$5 Billion Revenue



## FIFA20



## TITANFALL | 2

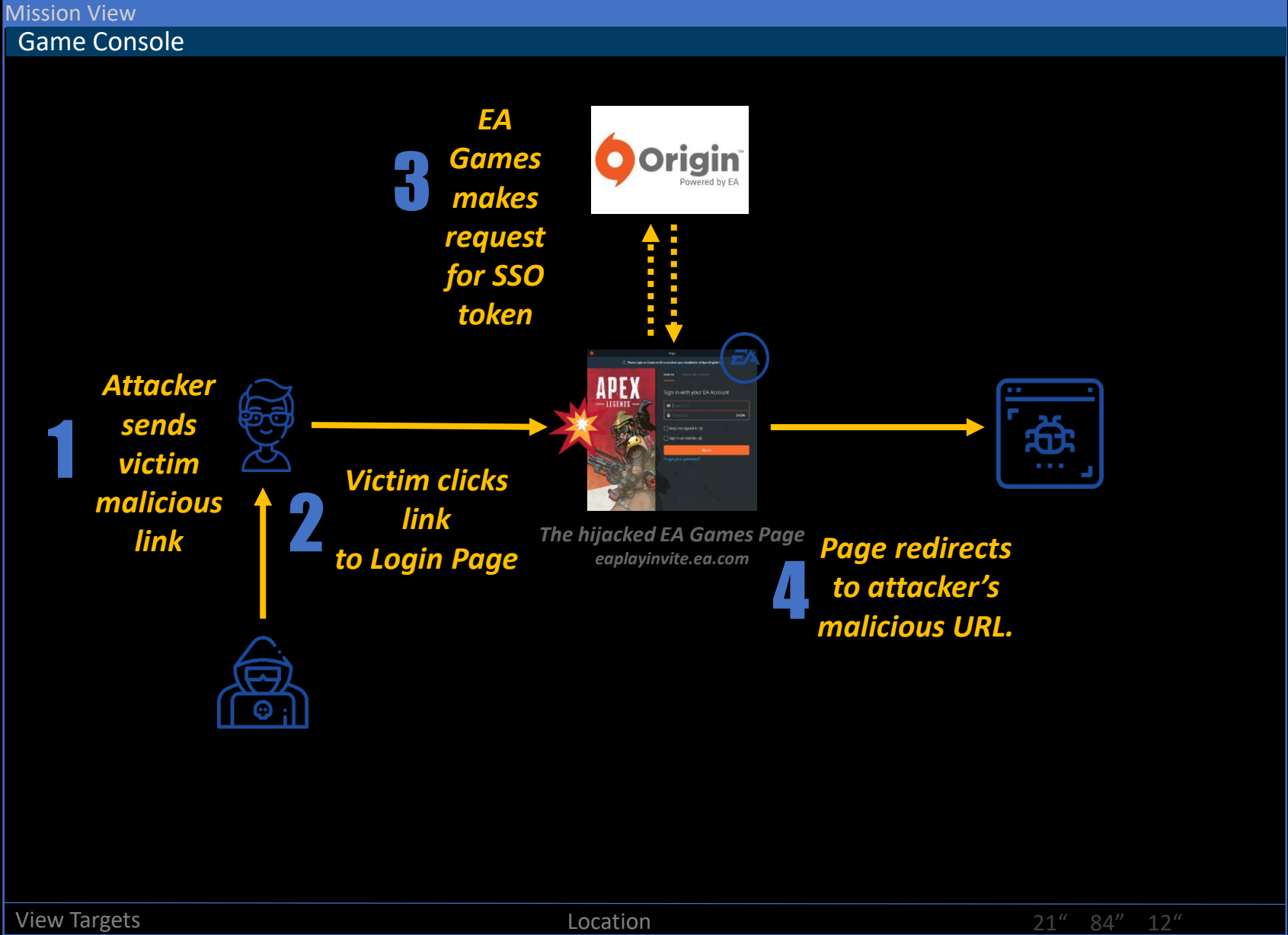
G.28912

21" 84" 12"

View Targets

Location

21" 84" 12"



**Target View**  
EA GAMES

Vulnerable Product 21" 84" 12"

**Target Details**  
Description

**EA GAMES**

90 Million Users  
\$5 Billion Revenue

BATTLEFIELD      FIFA20

The SIMS4      TITANFALL | 2

G.28912 21" 84" 12"



**Target Details**  
Description

# EA GAMES

90 Million Users  
\$5 Billion Revenue

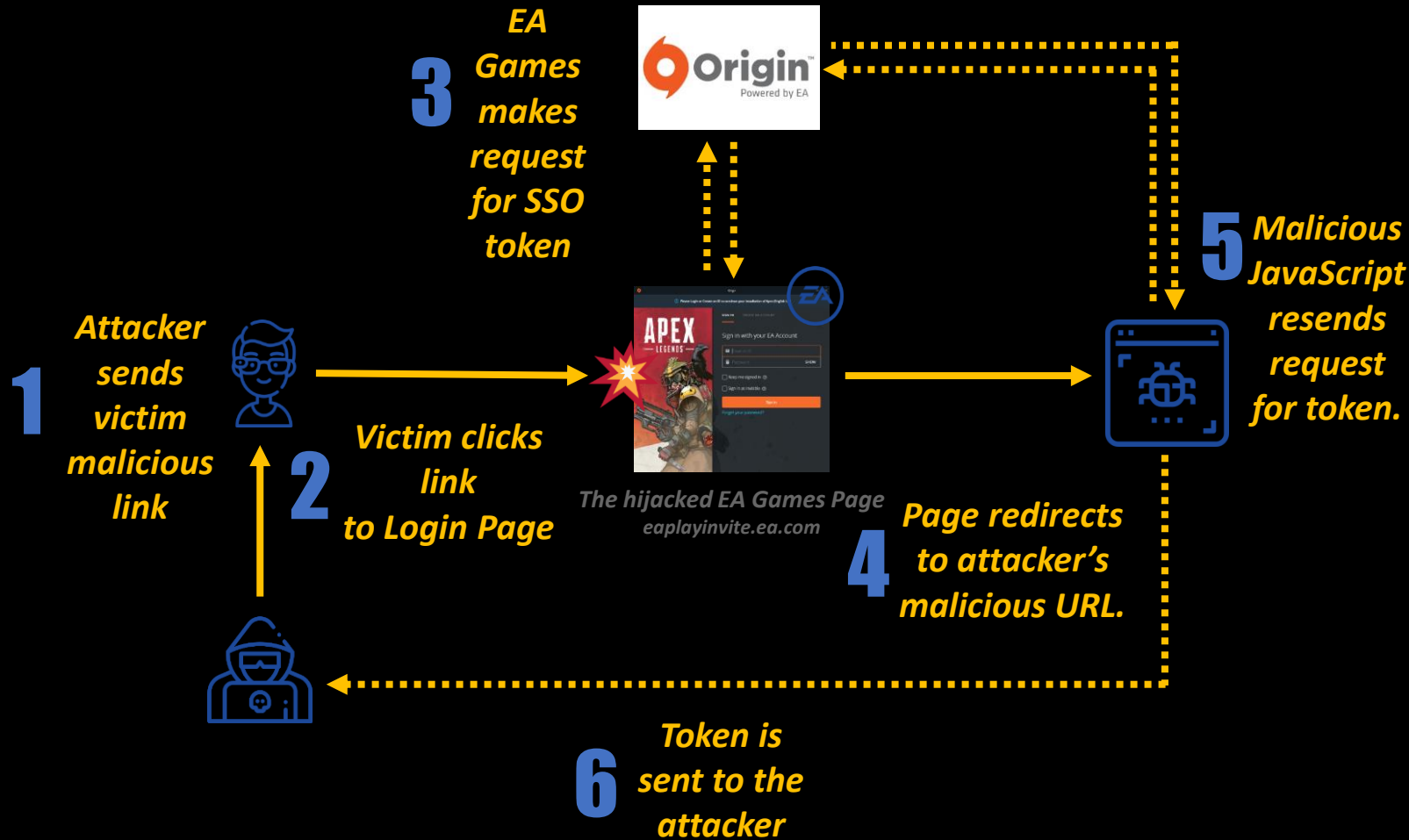
BATTLEFIELD      FIFA20

The SIMS4      TITANFALL | 2

G.28912 21" 84" 12"

Mission View

Game Console



View Targets

Location

21" 84" 12"

Target View

EA GAMES



Vulnerable Product

21" 84" 12"

Target Details

Description

# EA GAMES

90 Million Users  
\$5 Billion Revenue



G.28912

21" 84" 12"

# ACCOUNT

# TAKEOVER



# EA GAMES

90 Million Users

\$5 Billion Revenue



## FIFA20



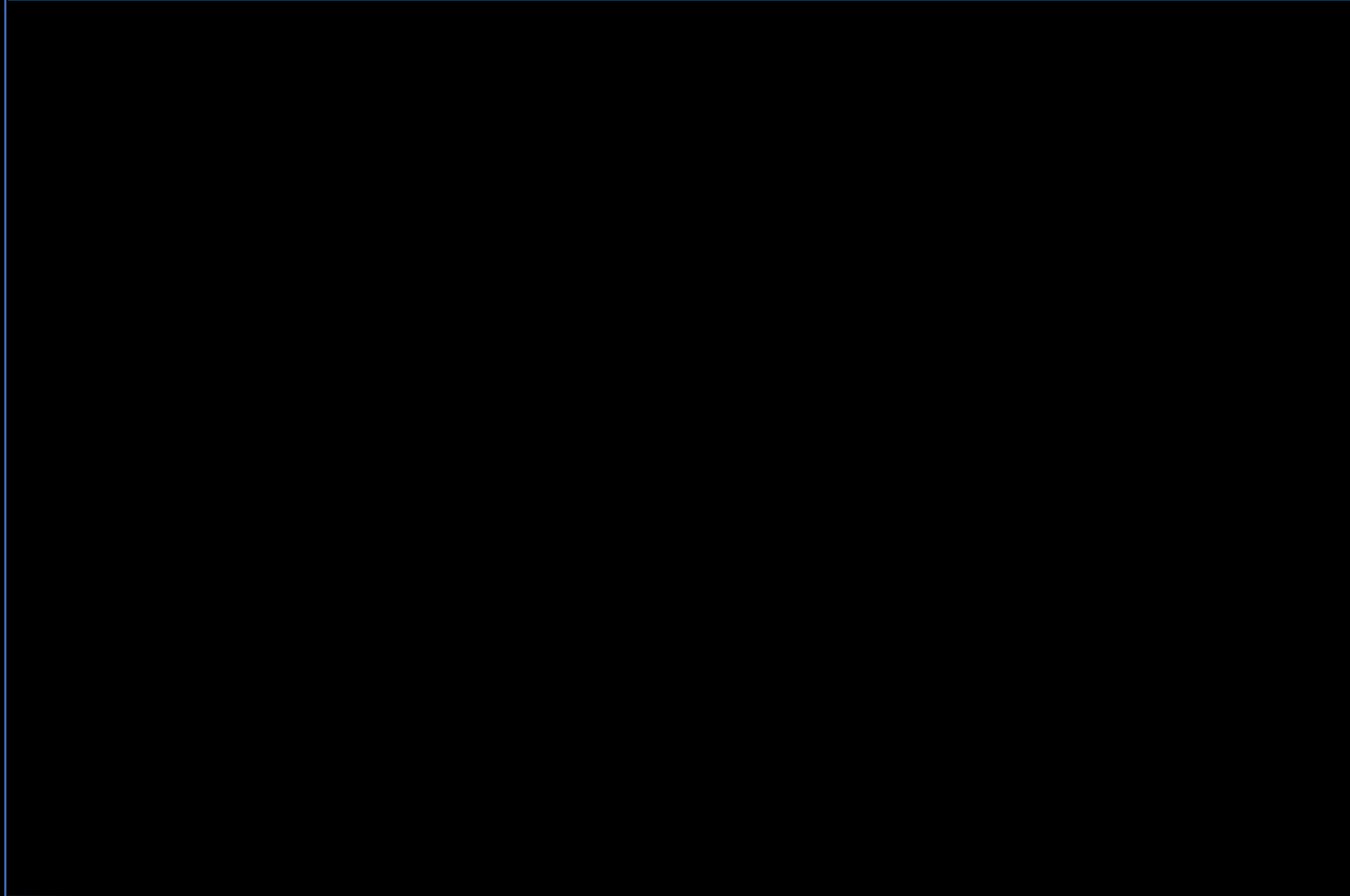
## TITANFALL | 2





Mission View

DSLR Camera



View Targets

Location

21" 84" 12"

Target View

Cannon DSLR Camera



Vulnerable Product

21" 84" 12"

Target Details

Description

**CANON**

**DSLR**

40% Market Share

**20 Million** sold Yearly

**PTP Support**

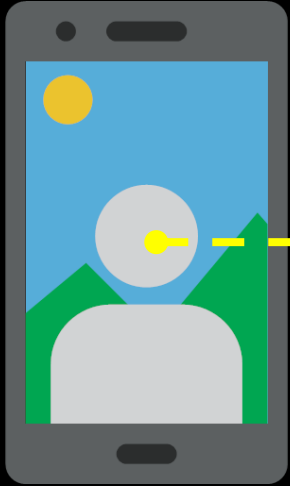
G.28912

21" 84" 12"



Mission View

Provisioning SMS



Next Code

Token 1

9 6 0 5 7 8 3 3

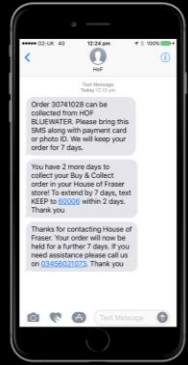
37 second(s) remaining

Copy



Target View

Android Phone



Vulnerable Product

21" 84" 12"

Target Details

Description

Provisioning SMS

OTA Provisioning

Samsung/Huawei/LG/Sony

50% of all Android

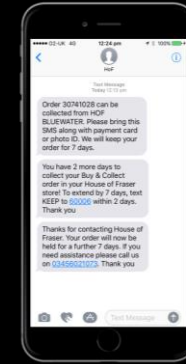
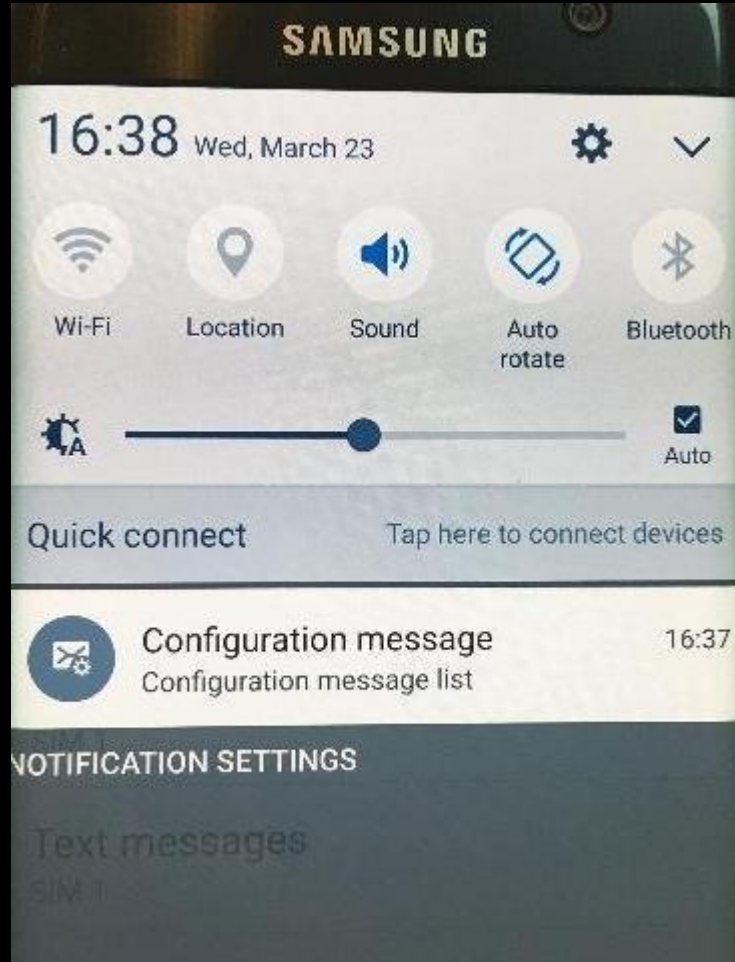
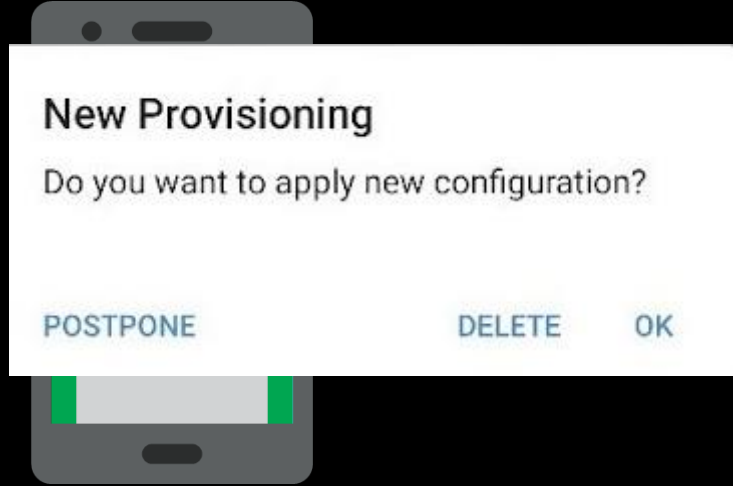
G.28912

21" 84" 12"

View Targets

Location

21" 84" 12"



Vulnerable Product

21" 84" 12"

# Provisioning SMS

## OTA Provisioning

Samsung/Huawei/LG/Sony

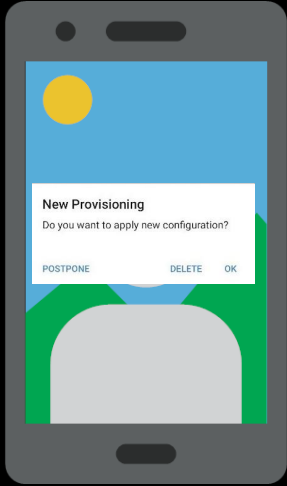
**50% of all Android**

G.28912

21" 84" 12"

Mission View

Provisioning SMS



Alert – Sensitive Data

MMS Message Server  
Browser Homepage  
Mail Server  
Directory Server  
**Proxy Server**  
And More...



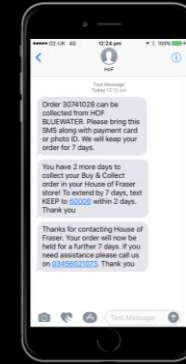
View Targets

Location

21" 84" 12"

Target View

Android Phone



Vulnerable Product

21" 84" 12"

Target Details

Description

**Provisioning SMS**

OTA Provisioning

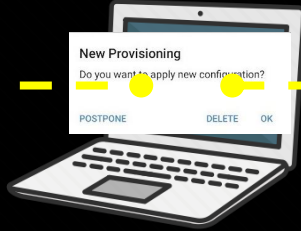
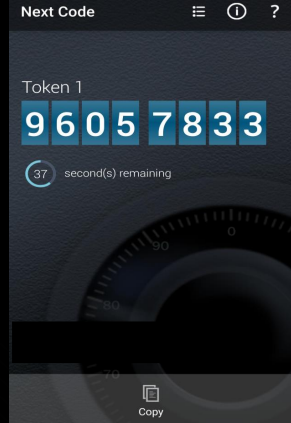
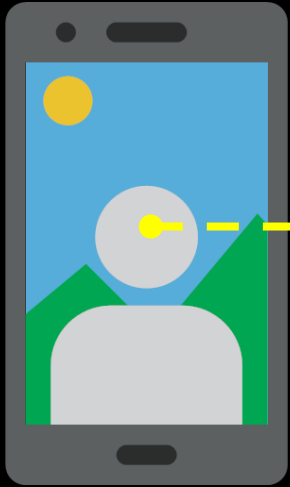
Samsung/Huawei/LG/Sony

**50% of all Android**

G.28912

21" 84" 12"

Mission View  
Provisioning SMS

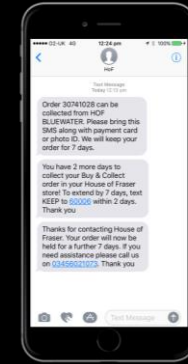


View Targets

Location

21" 84" 12"

Target View  
Android Phone



Vulnerable Product

21" 84" 12"

Target Details  
Description

Provisioning SMS

OTA Provisioning

Samsung/Huawei/LG/Sony

50% of all Android

G.28912

21" 84" 12"

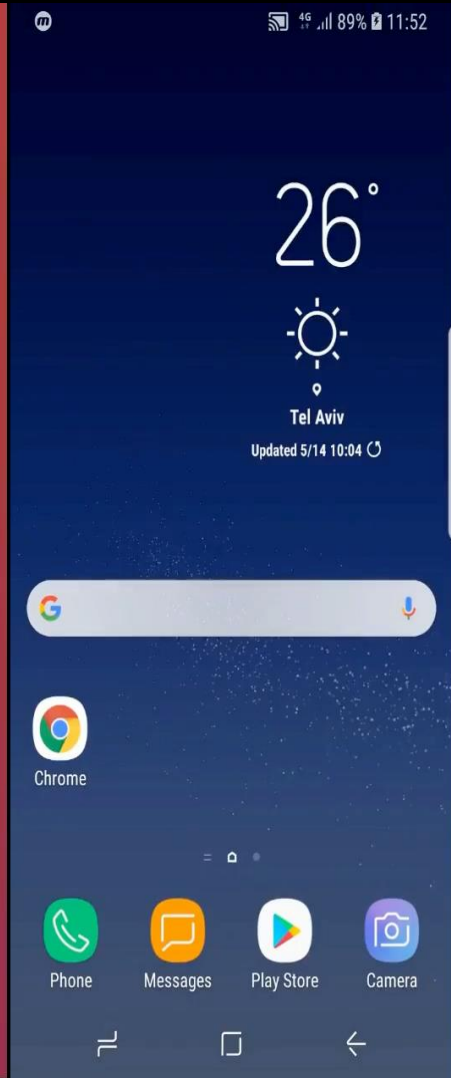
Mission View

Provisioning SMS

```

slavam@slavam800-ubuntu16: ~$ python ~/Work/xx-05-2019/19-05-2019/send_ota_message.py +972585602818

```



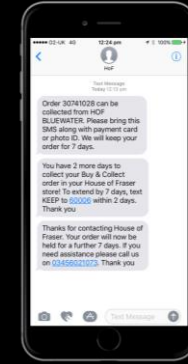
View Targets

Location

21" 84" 12"

Target View

Android Phone



Vulnerable Product

21" 84" 12"

Target Details

Description

Provisioning SMS

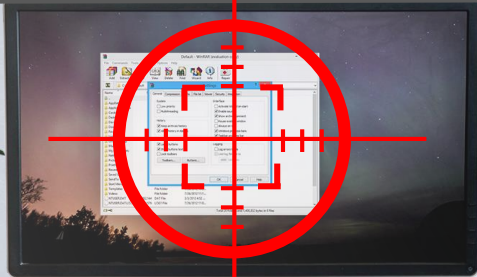
OTA Provisioning

Samsung/Huawei/LG/Sony

50% of all Android

G.28912

21" 84" 12"





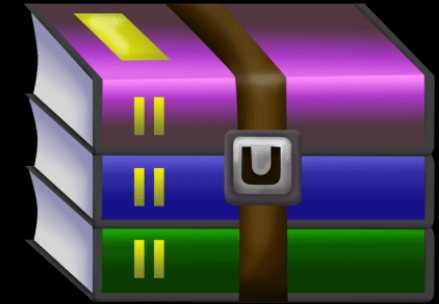
Vulnerability Alert !!

Proprietary Compression Algorithm

Created in 1991

MOSTLY Unmaintained

Supported by **WinRAR ONLY**



**WinRAR**

**500 Million** Users

>30 Supported Types

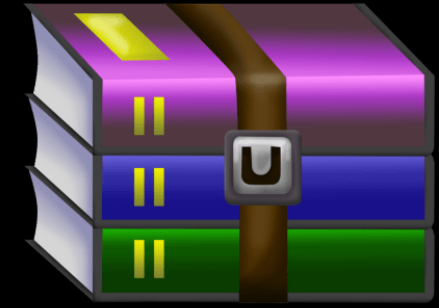
19 Years Old

Mission View

WinRAR

Target View

Archive Software



Vulnerable Product

21" 84" 12"

Target Details

Description

# WinRAR

**500 Million** Users

>30 Supported Types

19 Years Old

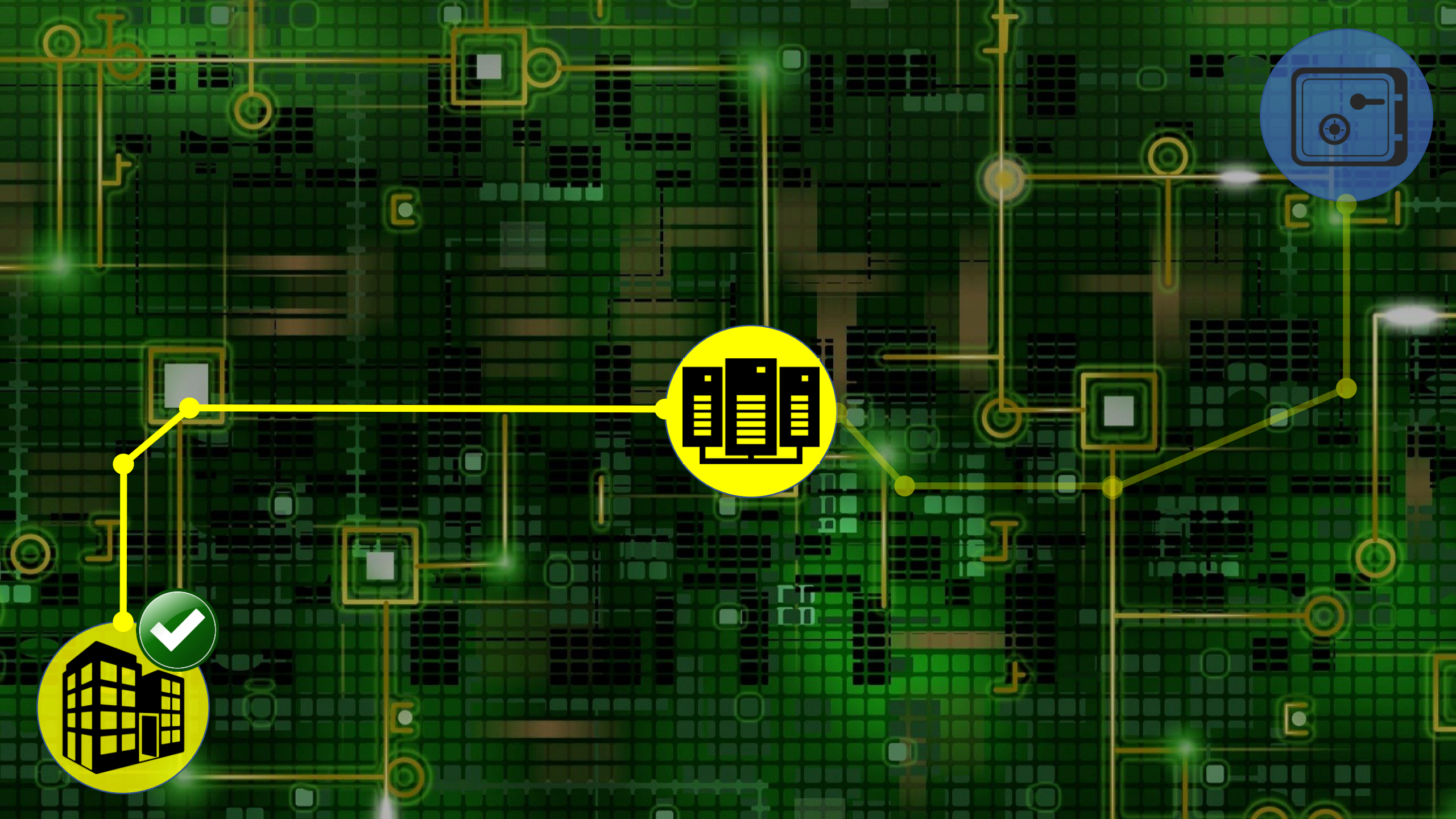
G.28912

21" 84" 12"

View Targets

Location

21" 84" 12"

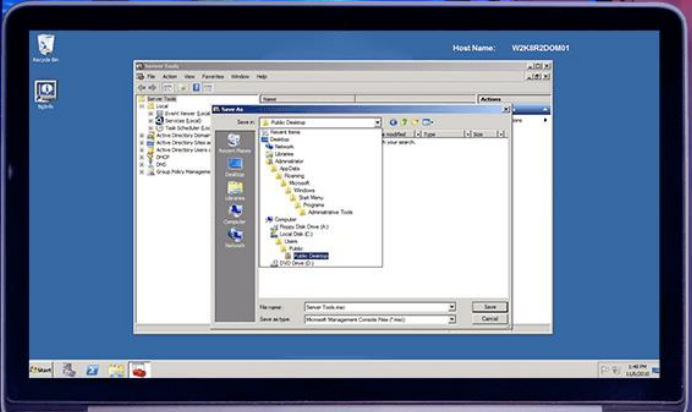






SQLite

```
Please select root device:
-----
SQLite Shell
MESSAGE: 0x00000000, 0x00000000, Network Connection
MESSAGE: 0x00000000, 0x00000000, Ethernet Controller
MESSAGE: 0x00000000, 0x00000000, Ethernet Controller
ERROR: 0x00000000
-----
* * * * *
ERROR: 0x00000000, 0x00000000, Ethernet Controller
ERROR: 0x00000000, 0x00000000, Ethernet Controller
ERROR: 0x00000000, 0x00000000, Ethernet Controller
```





WinBuzzer

WINDOWS 10

OFFICE

AZURE

XBOX

HOLOLENS

ABOUT WINBUZZER ▾

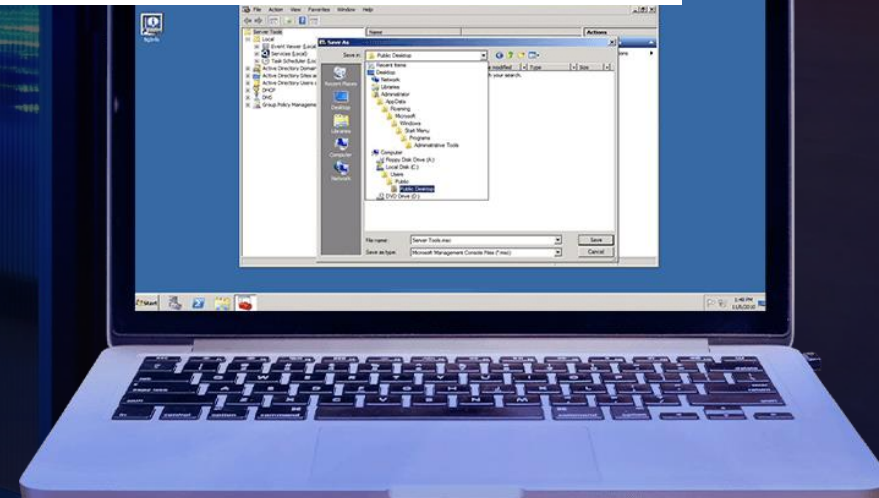


Home > WinBuzzer News > Microsoft Management Console (MMC) Vulnerabilities Leave Windows Open to Attack

WinBuzzer News

# Microsoft Management Console (MMC) Vulnerabilities Leave Windows Open to Attack

*Researchers say flaws in Microsoft Management Console could allow bad actors to gain heightened privileges on an admin-run machine.*



# WDS bug lets hackers hijack Windows Servers via malformed TFTP packets

Last warning to apply Microsoft's November security updates for Windows Servers.



By Catalin Cimpanu for Zero Day | March 6, 2019 -- 14:00 GMT (14:00 GMT) | Topic: Security



## MORE FROM CATALIN CIMPANU



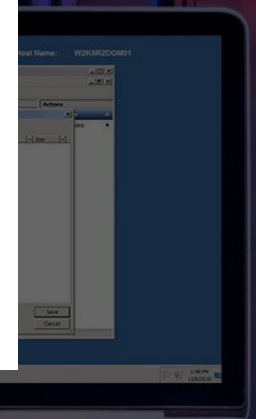
Security  
**Mitsubishi Electric discloses security breach, China is main suspect**



Tech & Work  
**LastPass is in the midst of a major outage**



Security  
**Hacker leaks passwords for more than 500,000 servers.**



# New Hack Works On Every Model Of iPhone And iPad



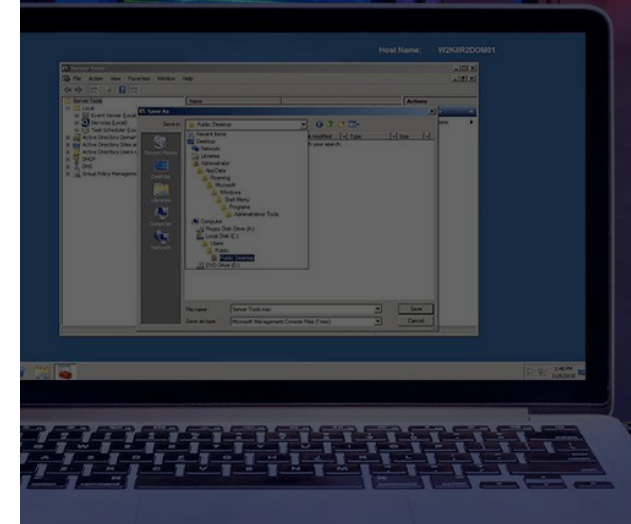
**Gordon Kelly** Senior Contributor ⓘ

Consumer Tech

*I write about technology's biggest companies*

f Apple is having a bad week. Just days after Face ID was hacked and the company's "user-hostile" iPhone battery practices were exposed, an extraordinary story of Apple neglect has resulted in a warning every iPhone and iPad user needs to know about.

in



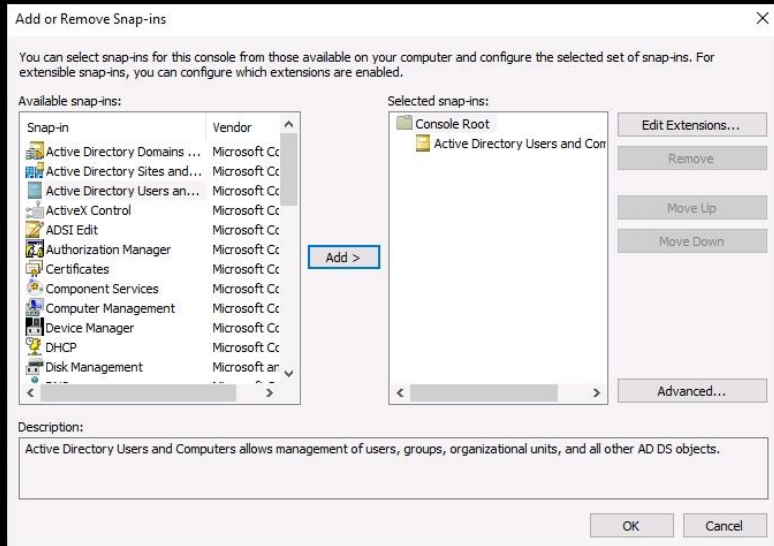






Mission View

MMC Console



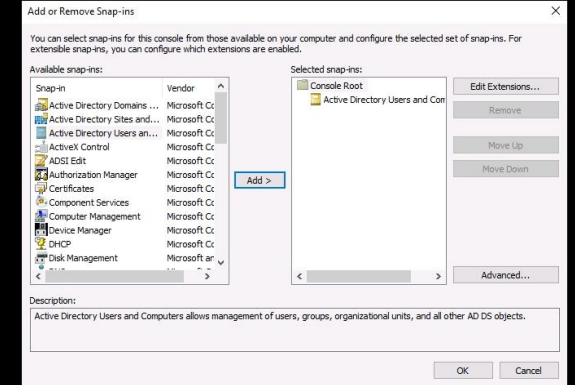
View Targets

Location

21" 84" 12"

Target View

Management Console



Vulnerable Product

21" 84" 12"

Target Details

Description

# MMC

Administrative Tool

Runs on ALL Win>98

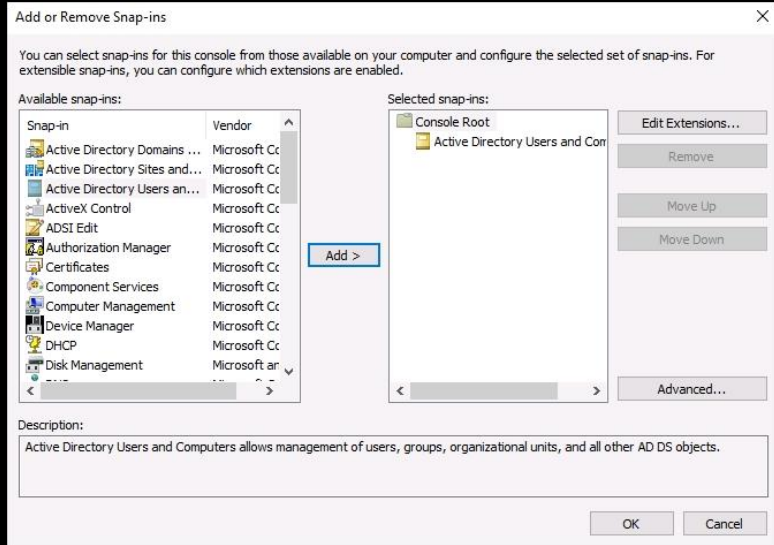
**Downloadable Addons**

G.28912

21" 84" 12"

Mission View

MMC Console



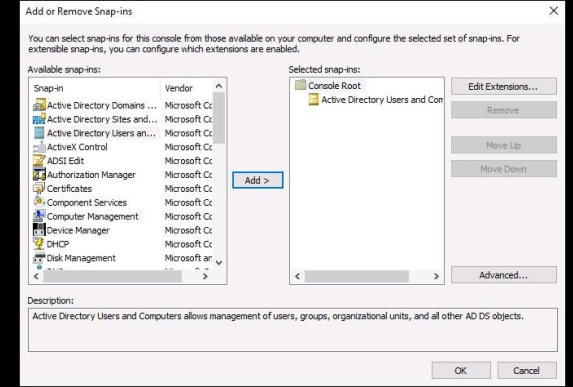
View Targets

Location

21" 84" 12"

Target View

Management Console



Vulnerable Product

21" 84" 12"

Target Details

Description

# MMC

Administrative Tool

Runs on ALL Win>98

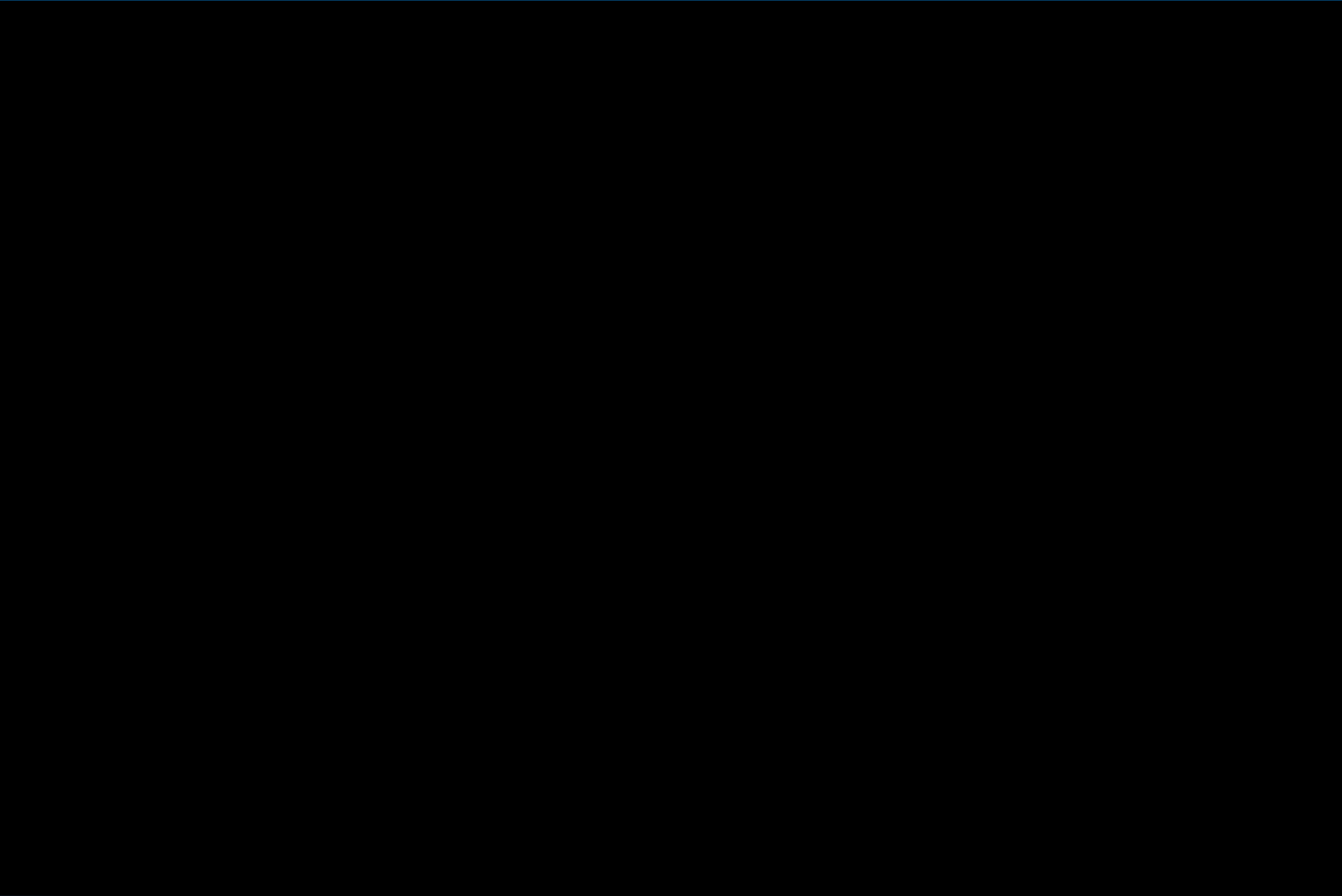
**Downloadable Addons**

G.28912

21" 84" 12"

## Mission View

### MMC Console



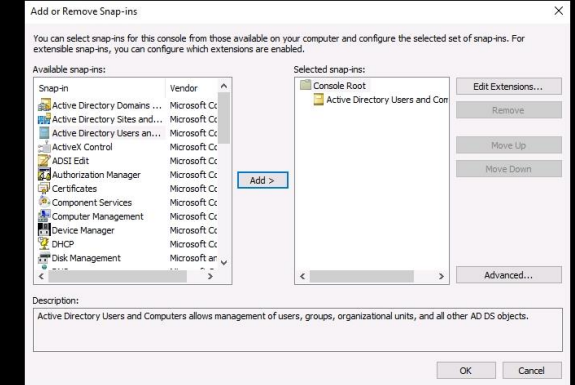
View Targets

Location

21" 84" 12"

## Target View

### Management Console



Vulnerable Product

21" 84" 12"

## Target Details

### Description

# MMC

## Administrative Tool

## Runs on ALL Win>98

## Downloadable Addons

G.28912

21" 84" 12"

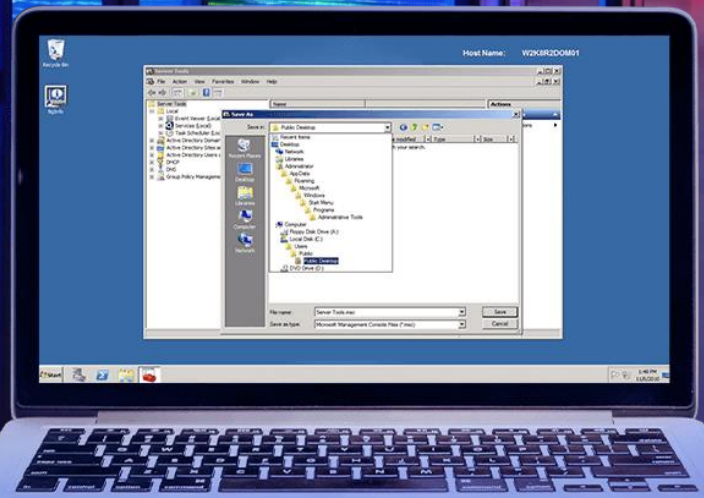


SQLite

```

Please make sure you have the correct path to the
SQLite.dll file in your PATH environment variable.
If you are using the default installation path, you
can run the following command from a command prompt:
setx PATH "%PATH%;C:\Program Files\SQLite" /M
If you are using a custom installation path, you
can run the following command from a command prompt:
setx PATH "%PATH%;C:\Program Files\SQLite" /M
Please refer to the SQLite website for more information:
http://www.sqlite.org

```



Mission View

PXE



Active Directory / WDS



View Targets

Location

21" 84" 12"

Target View

Windows Server

```

Please select boot device:
Built-in EFI Shell
NET0:PXE IP4 Intel(R) I210 Gigabit Network Connection
NET1:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
NET2:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
UEFI OS
Enter Setup

^ and v to move selection
ENTER to select boot device
ESC to boot using defaults

```

Vulnerable Product

21" 84" 12"

Target Details

Description

PXE

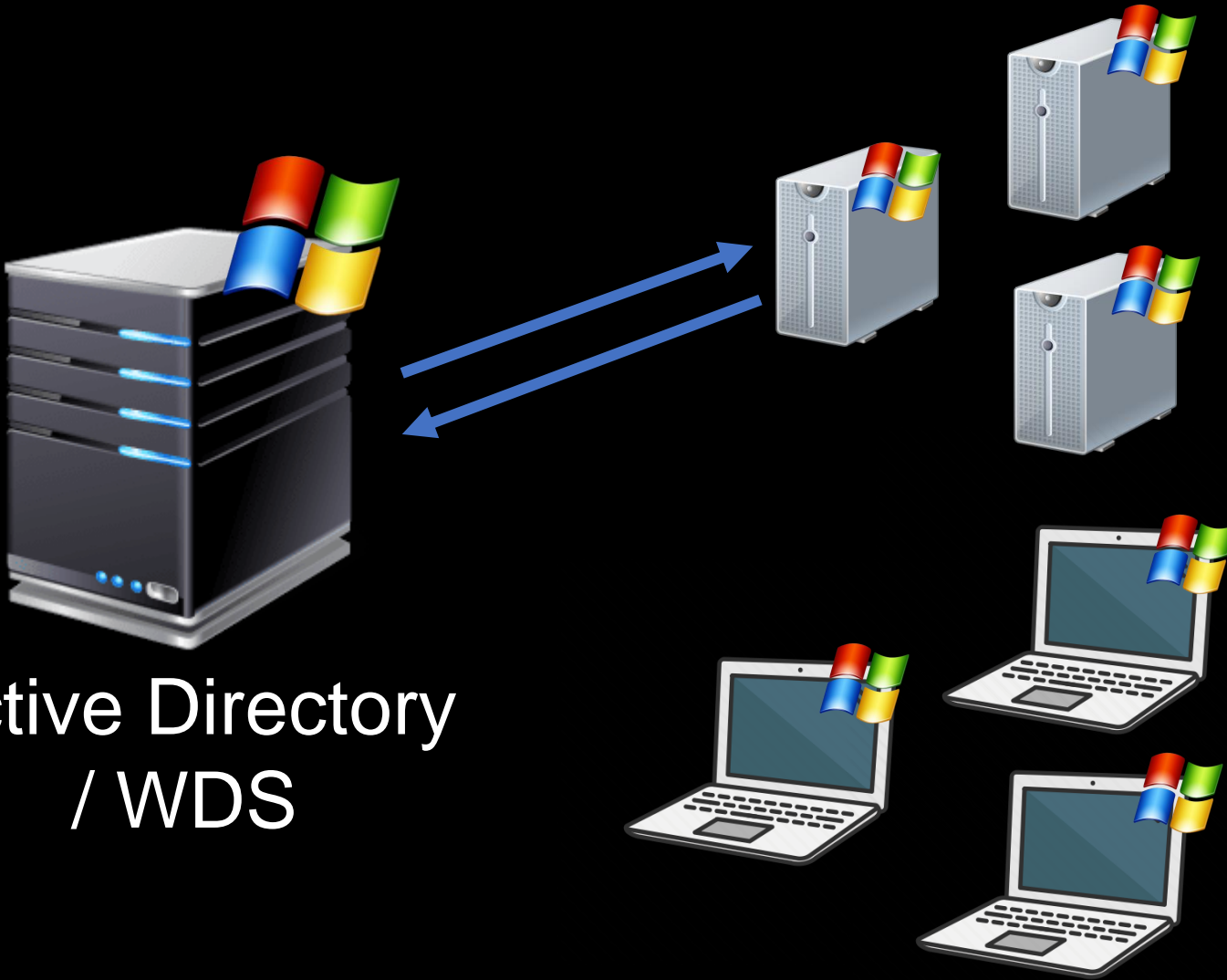
Pre-Boot Execution

Dozens of Flavors

**Bundled with ALL Windows Server**

G.28912

21" 84" 12"



View Targets

Location

21" 84" 12"

```

Please select boot device:
Built-in EFI Shell
NET0:PXE IP4 Intel(R) I210 Gigabit Network Connection
NET1:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
NET2:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
UEFI OS
Enter Setup

^ and v to move selection
ENTER to select boot device
ESC to boot using defaults
  
```

Vulnerable Product

21" 84" 12"

# PXE

Pre-Boot Execution

Dozens of Flavors

**Bundled with ALL  
Windows Server**

G.28912

21" 84" 12"





Active Directory / WDS



View Targets

Location

21" 84" 12"

```

Please select boot device:
Built-in EFI Shell
NET0:PXE IP4 Intel(R) I210 Gigabit Network Connection
NET1:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
NET2:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
UEFI OS
Enter Setup

^ and v to move selection
ENTER to select boot device
ESC to boot using defaults

```

Vulnerable Product

21" 84" 12"

PXE

Pre-Boot Execution

Dozens of Flavors

**Bundled with ALL Windows Server**

G.28912

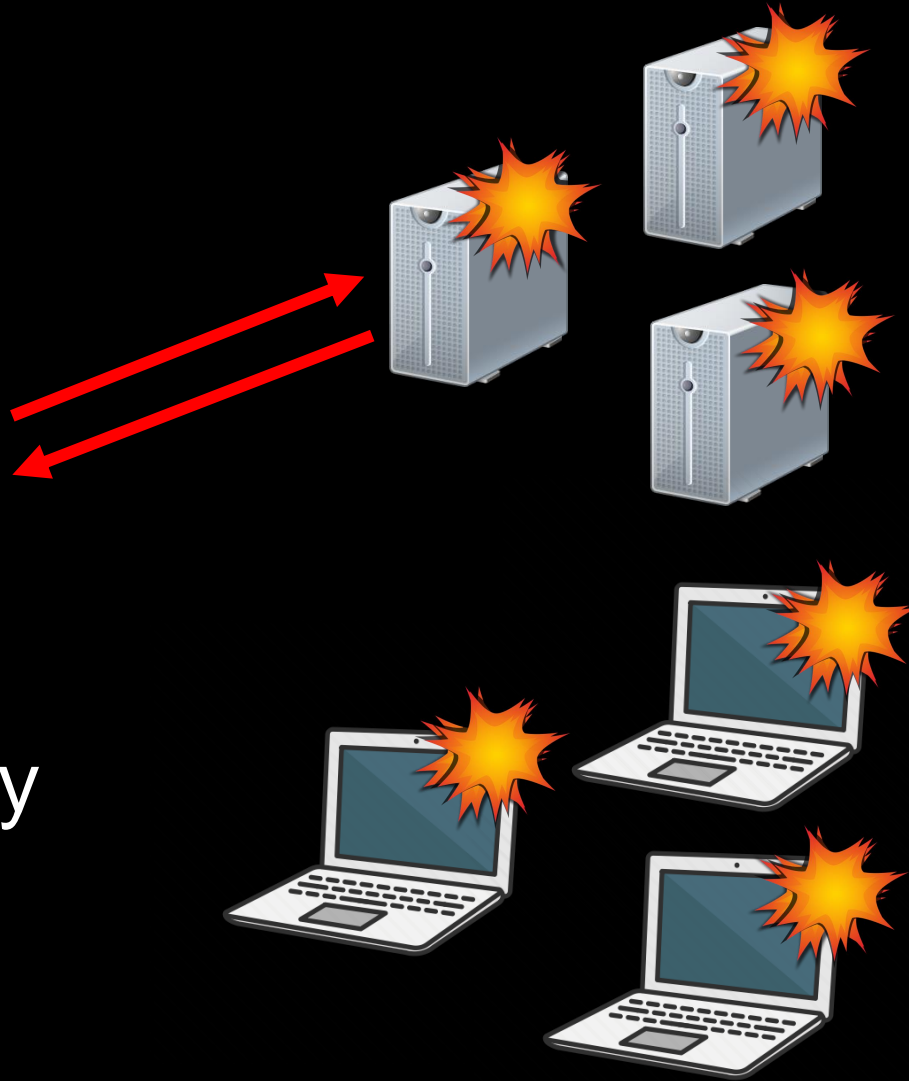
21" 84" 12"

Mission View

PXE



Active Directory / WDS



View Targets

Location

21" 84" 12"

Target View

Windows Server

```

Please select boot device:
Built-in EFI Shell
NET0:PXE IP4 Intel(R) I210 Gigabit Network Connection
NET1:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
NET2:PXE IP4 Oracle Dual Port 10GBase-T Ethernet Controller
UEFI OS
Enter Setup

^ and v to move selection
ENTER to select boot device
ESC to boot using defaults

```

Vulnerable Product

21" 84" 12"

Target Details

Description

PXE

Pre-Boot Execution

Dozens of Flavors

**Bundled with ALL Windows Server**

G.28912

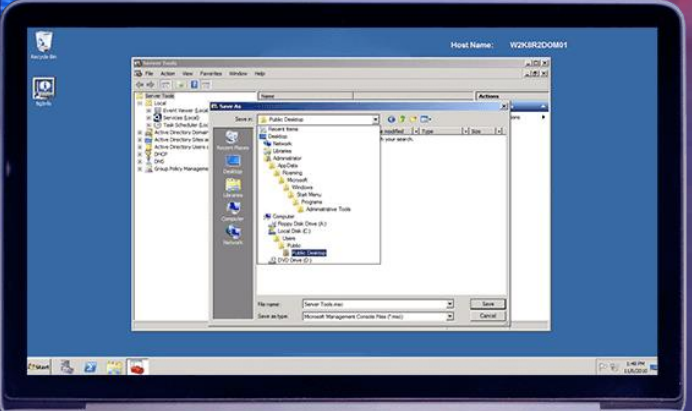
21" 84" 12"



SQLite

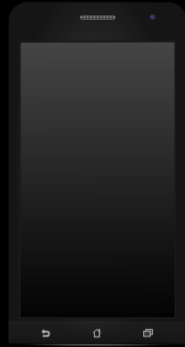


```
-----  
Please select boot device:  
-----  
|  
| Boot-01 (S) Shell  
| Message: 0x00000000, 0x00000000, Network Connection  
| Message: 0x00000000, 0x00000000, Ethernet Controller  
| Message: 0x00000000, 0x00000000, Ethernet Controller  
| Error: 0x00000000  
|  
| * use V to move selection  
| * ESC to select boot device  
| * ! to boot using defaults
```



Mission View

SQLite



View Targets

Location

21" 84" 12"

Target View

Embedded Database



Vulnerable Product

21" 84" 12"

Target Details

Description

# SQLite

Light Database

“Embedded DB”

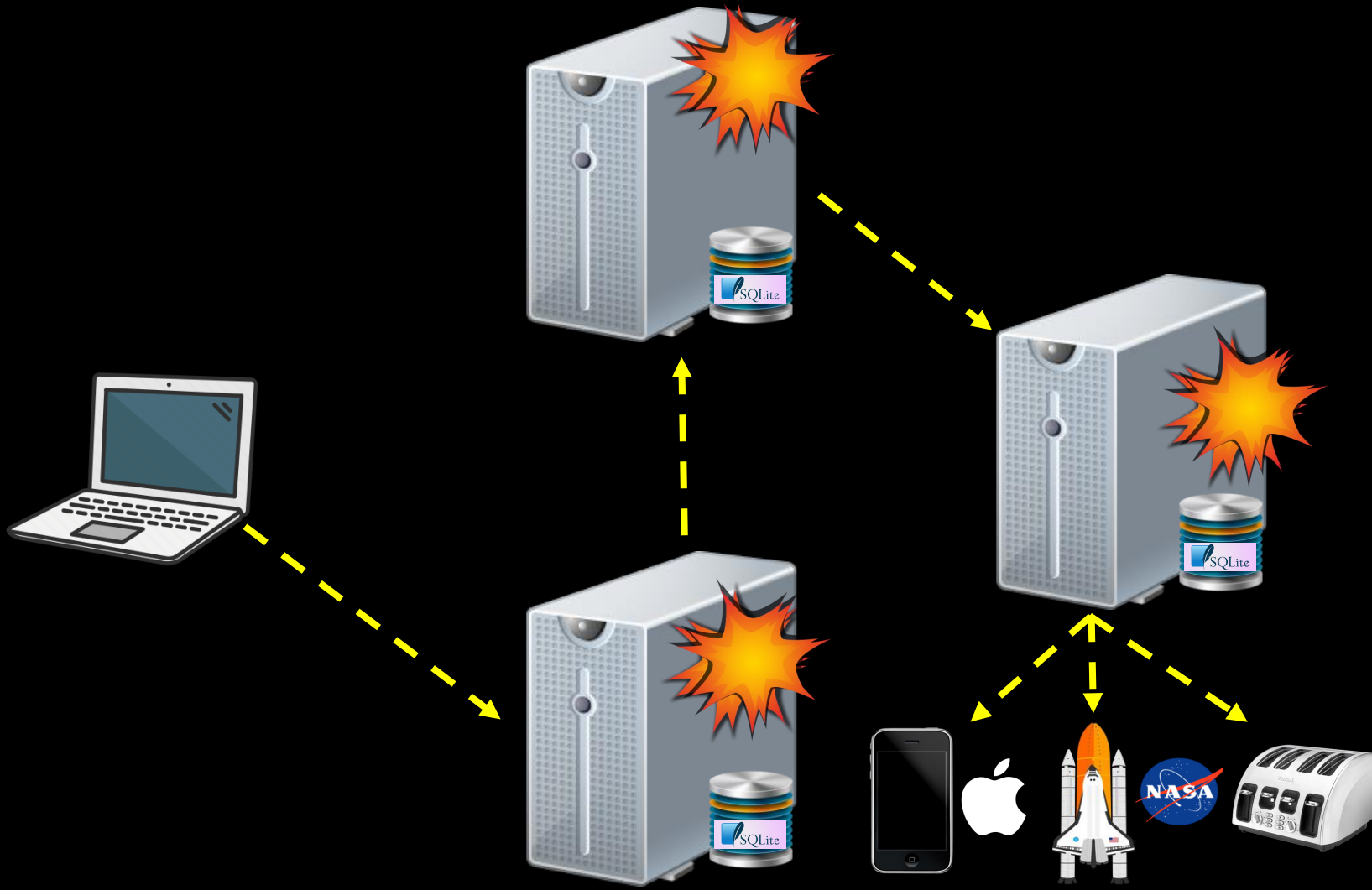
## 1-e12 Installs

G.28912

21" 84" 12"

Mission View

SQLite



View Targets

Location

21" 84" 12"

Target View

Embedded Database



Vulnerable Product

21" 84" 12"

Target Details

Description

# SQLite

Light Database

"Embedded DB"

## 1-e12 Installs

G.28912

21" 84" 12"

Mission View

SQLite

Bot GUID	Bin ID	IP Address	PC Information	Last Online	Action
BC5E0F8AEB3312DFDA8DD09B1	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
C14C057C0902B8CF1BD89D8E	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
7BC8E8528088CC6A2D3BB30	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
08E4C78E6F02AFBEBFF3F2DD	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
A1432E43EFFFDE53C6DBB1F	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
80E2211FF908F3F2FDD5F5BD	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
6FCB3650682D30B3CCC77EC1	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
CE2B4D3D13F2D324EC9A2F1	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
9ACAEC28ED3D678DCF17A8CF	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
CB8BCA02CBE2AC2ECFE0E79B	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
8ADB067068ECCD18D4F79FED	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
70F8FF5BFEECC71B2ABDFE59	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
C50DEFFCECE5DB2B7D8B5F40	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

Showing 0 to 20 of 309 entries, 20 records per page

Password Stealer Backend

View Targets

Location

21" 84" 12"

Target View

Embedded Database



Vulnerable Product

21" 84" 12"

Target Details

Description

SQLite

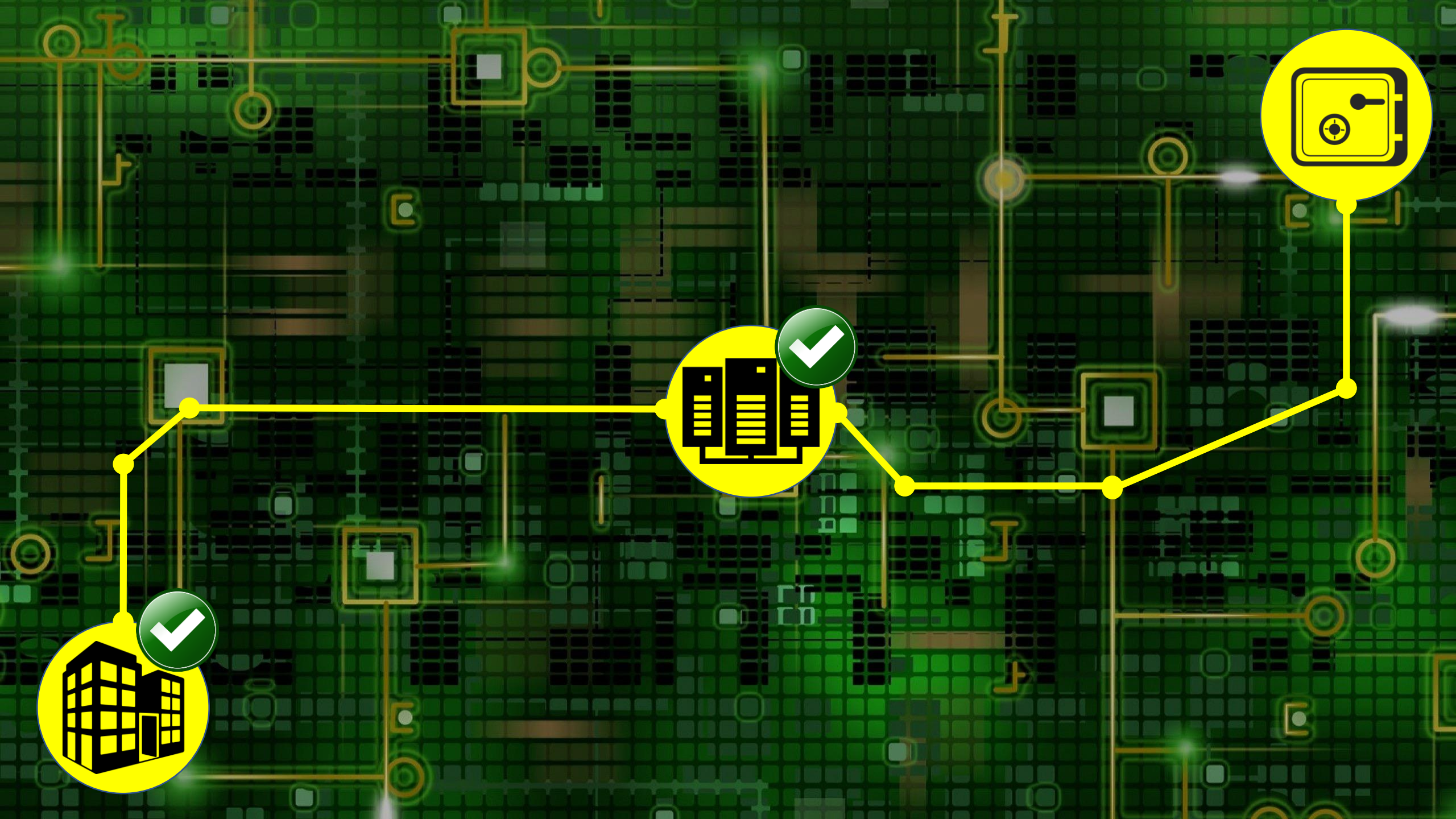
Light Database

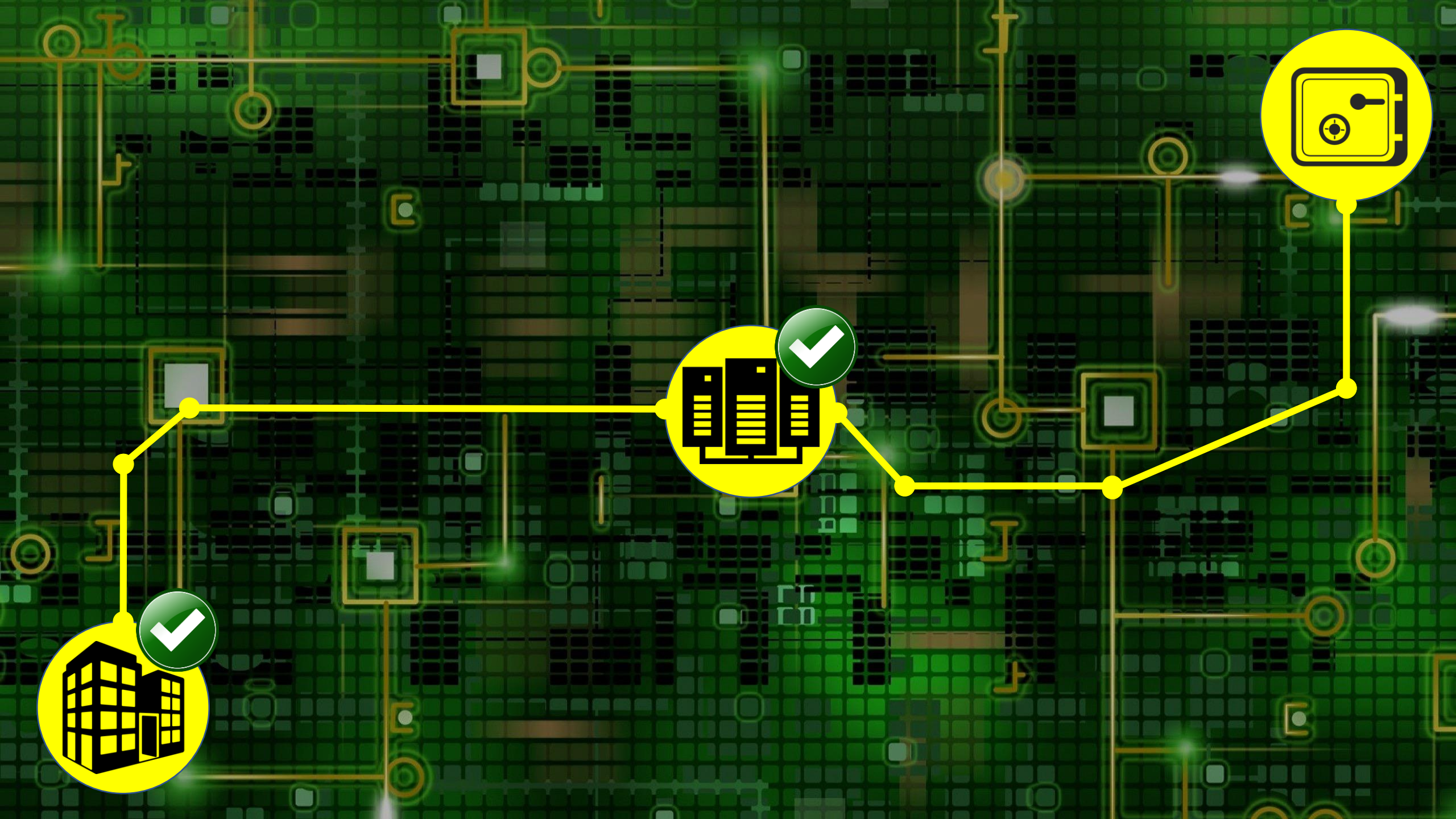
“Embedded DB”

1-e12 Installs

G.28912

21" 84" 12"



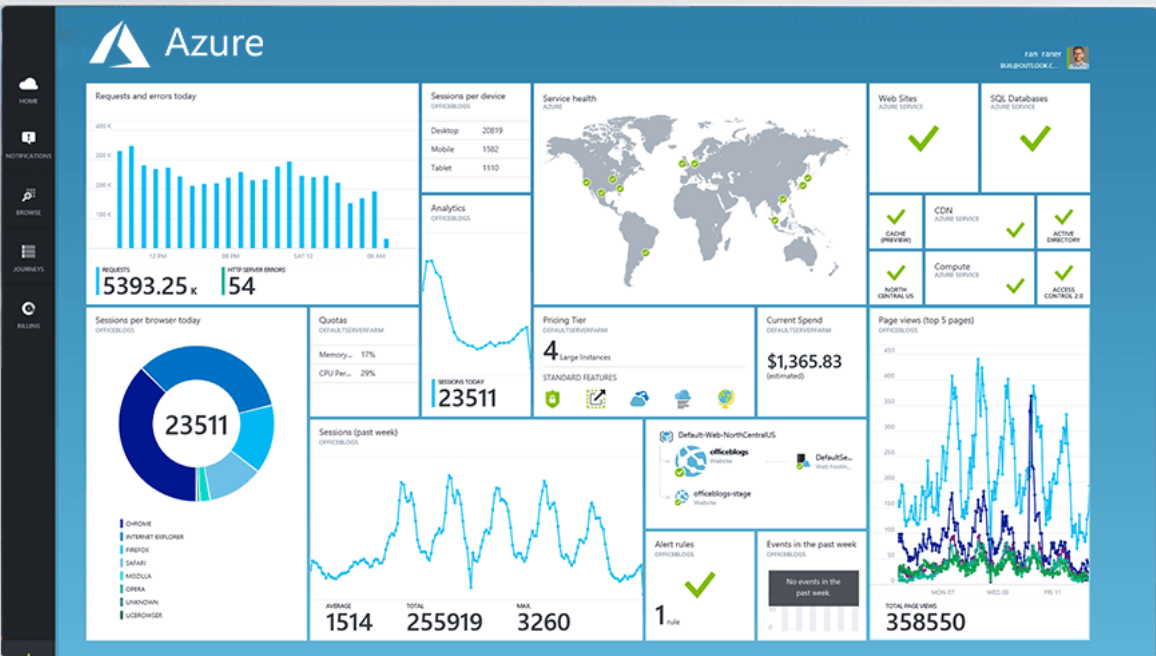






OOOPS





Mission View

Cloud Infrastructure

Workload

Workload

Workload

Workload

Workload

Workload



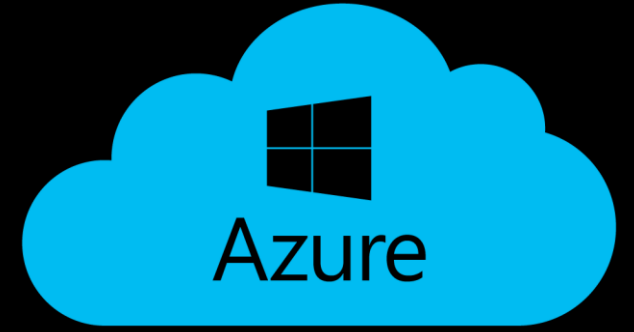
View Targets

Location

21" 84" 12"

Target View

Microsoft Azure



Vulnerable Product

21" 84" 12"

Target Details

Description

**AZURE**

MS Cloud Solution

Top 3 Cloud I/S

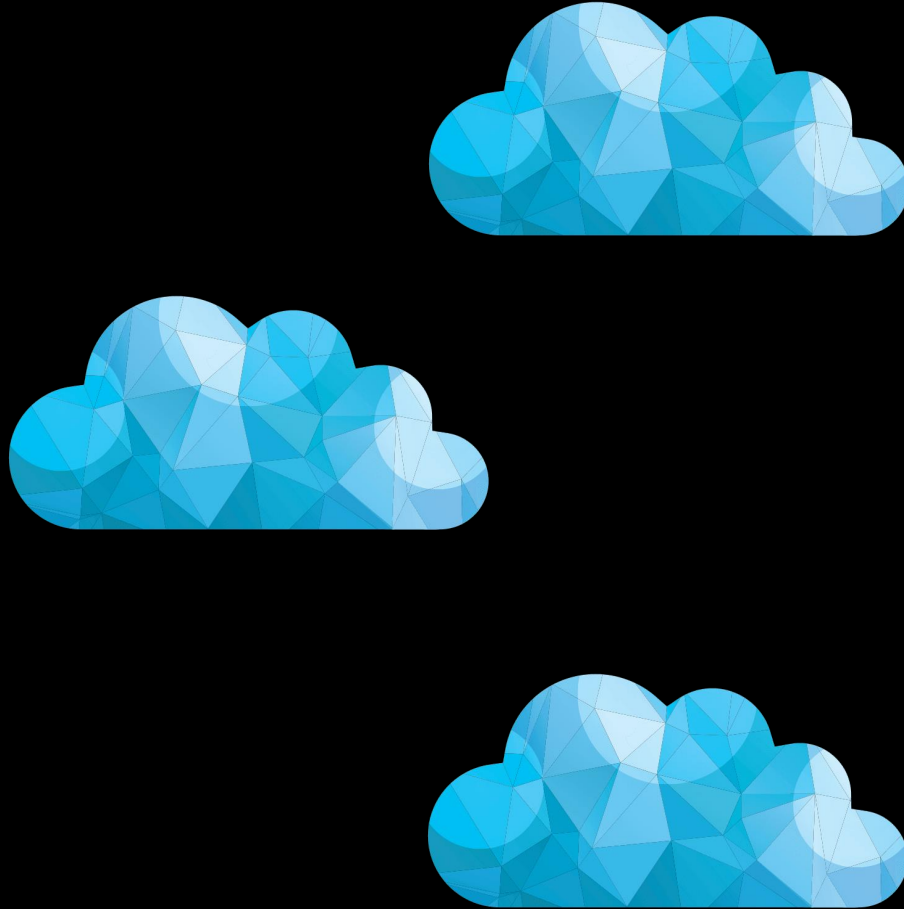
**Millions of Users**

G.28912

21" 84" 12"

Mission View

Cloud Infrastructure



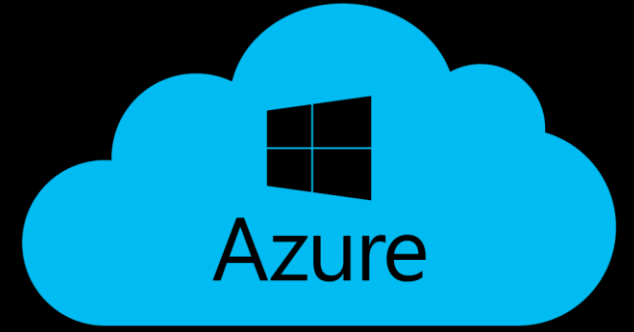
View Targets

Location

21" 84" 12"

Target View

Microsoft Azure



Vulnerable Product

21" 84" 12"

Target Details

Description

# AZURE

MS Cloud Solution

Top 3 Cloud I/S

**Millions of Users**

G.28912

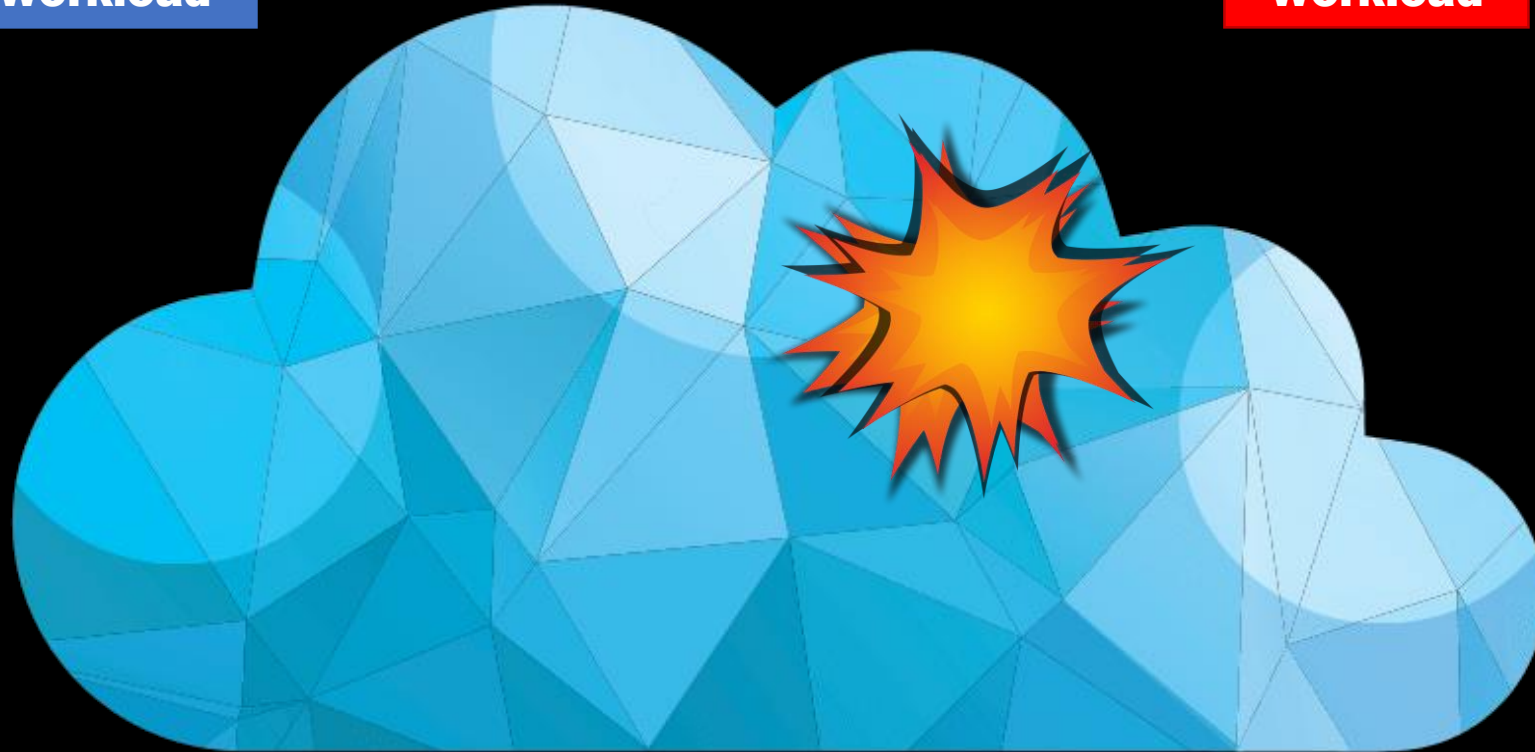
21" 84" 12"

Mission View

Cloud Infrastructure

Workload

Workload



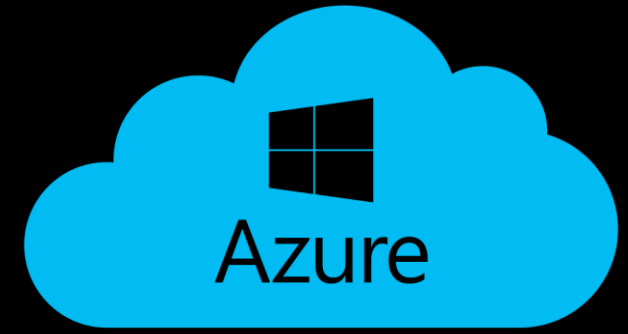
View Targets

Location

21" 84" 12"

Target View

Microsoft Azure



Vulnerable Product

21" 84" 12"

Target Details

Description

# AZURE

MS Cloud Solution

Top 3 Cloud I/S

**Millions of Users**

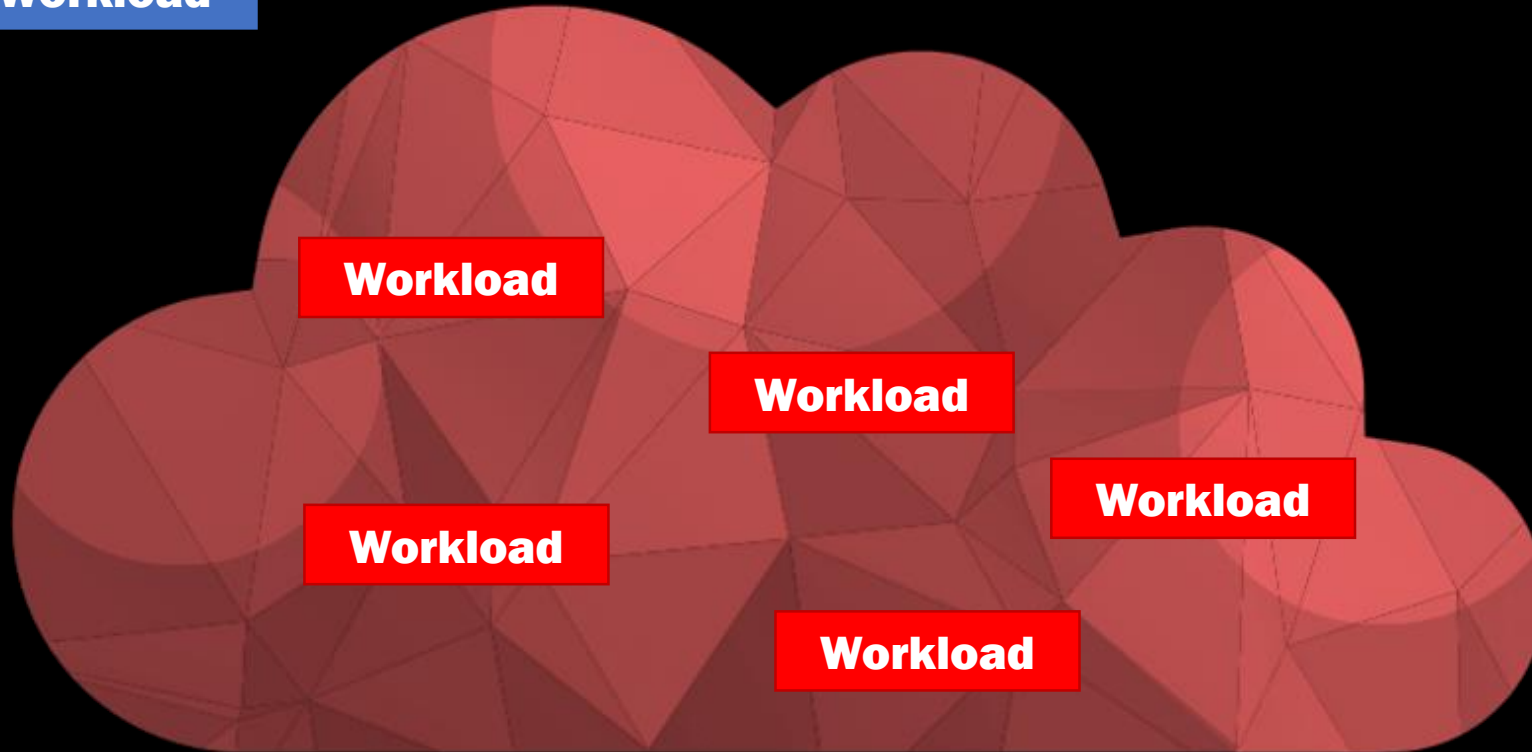
G.28912

21" 84" 12"

Mission View

Cloud Infrastructure

**Workload**



**Workload**

**Workload**

**Workload**

**Workload**

**Workload**

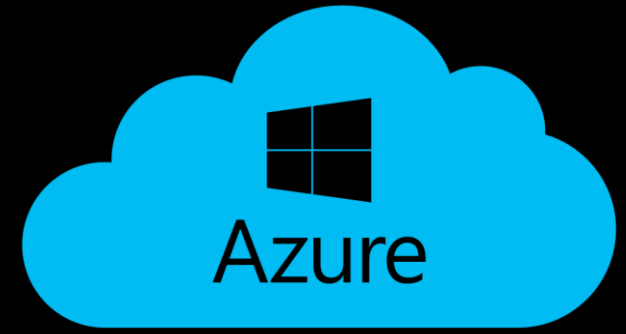
View Targets

Location

21" 84" 12"

Target View

Microsoft Azure



Vulnerable Product

21" 84" 12"

Target Details

Description

# AZURE

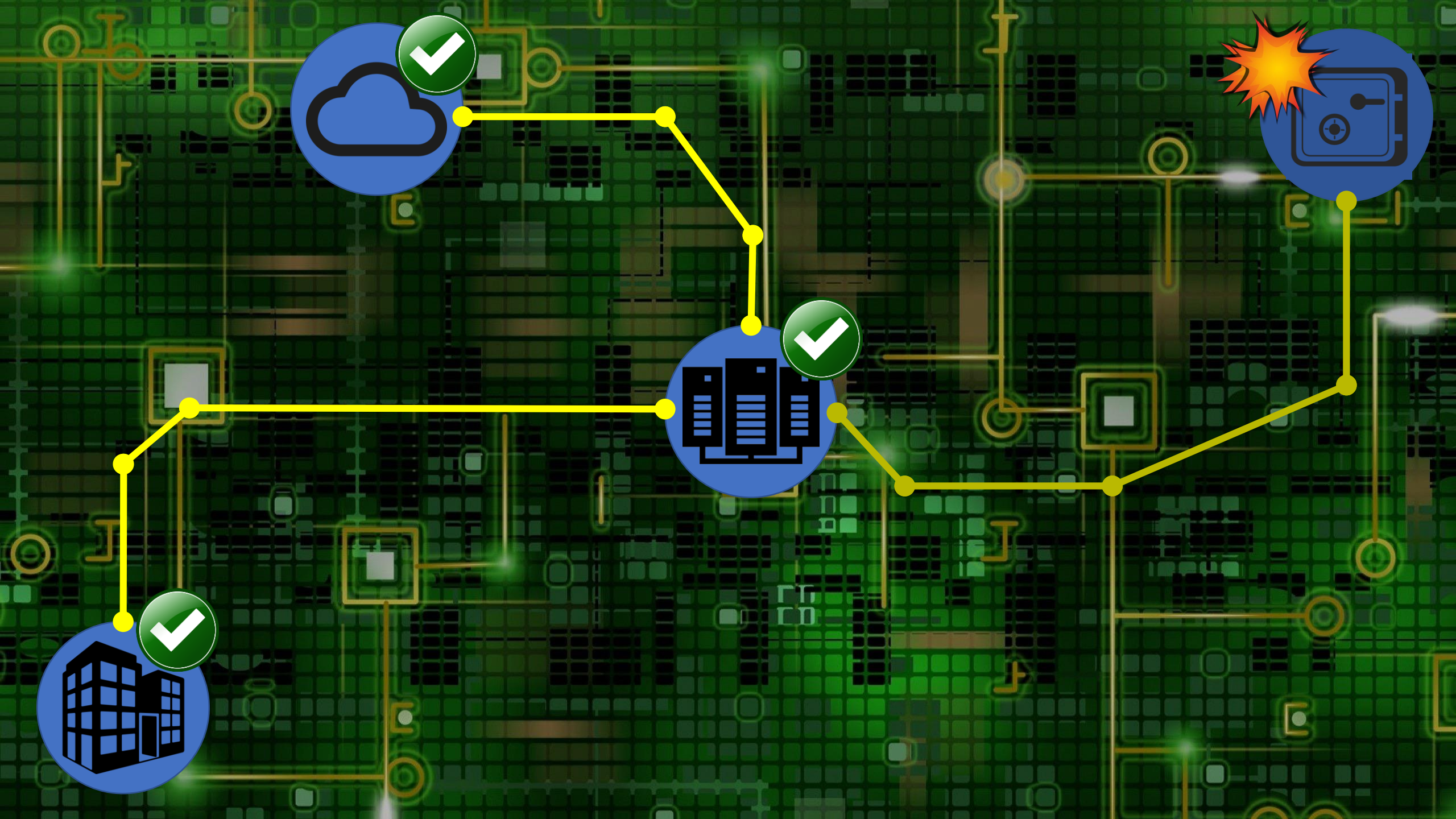
MS Cloud Solution

Top 3 Cloud I/S

**Millions of Users**

G.28912

21" 84" 12"





# THE END



**RESEARCH.CHECKPOINT.COM**



**\_CPRESEARCH\_**

