Changing nature of global security

The secret life of a cyber-vulnerability

Bratislava, November 2019

Vladimir Radunovic
Director, E-diplomacy and Cybersecurity
DiploFoundation
vladar@diplomacy.edu

DiPLO
www.diplomacy.edu

14

15

14

15

A queue in front of Company A's shop… a new model has been released. That night, across the street, above Company B's shop …

```
def dotwrite(ast):
    nodename = getNodename()
    label=symbol.sym_name.get(int(ast[0]),ast[0])
    print '    %s [label="%s' % (nodename, label),
    if isinstance(ast[1], str):
        if ast[1].strip():
            print '= %s"];' % ast[1]
        else:
            print '"]'
    else:
        print '"];'
        children = []
        for  in n, childenumerate(ast[1:]):
            children.append(dotwrite(child))
        print ,'    %s -> {' % nodename
        for  in :namechildren
            print '%s' % name,
```

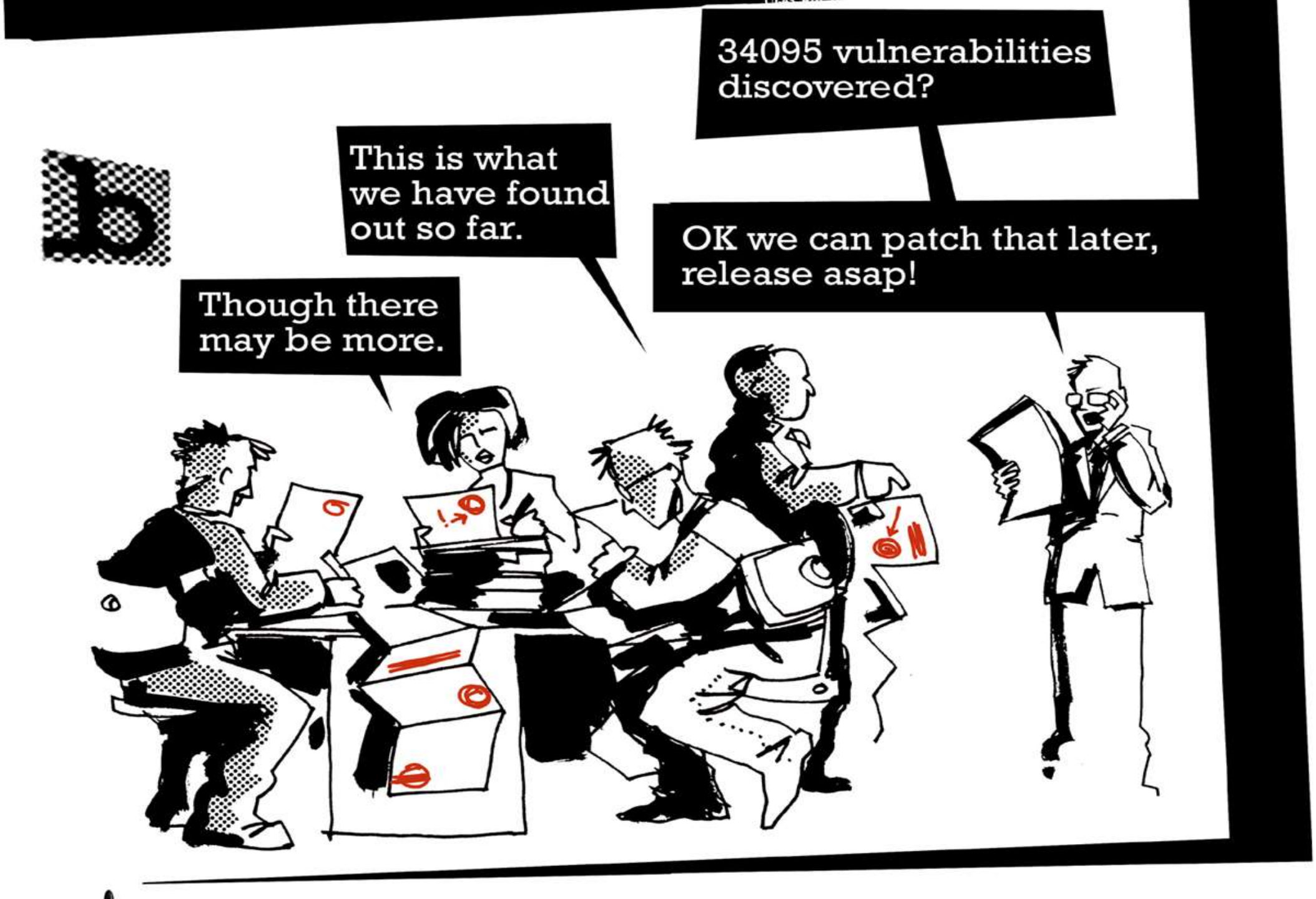
```
OPERATION:  MEM                    PROGRAM
MEM              000010        N00000001

000010 (SAMPLE PROGRAM.NCF ) ;
G00 G17 G40 G80 G90 G54 ;
;
T20 M06 ;
G00 G90 G54 X0. Y0. ;
G43 H20 Z0.5 ;
;
(PROBE - RECTANGLE BLOCK) ;
G65 P9995 W54. A13. D3. E2. H-0.75 ;
;
N1 ;
T1 M06 ( 0.5 INCH ENDMILL ) ;
( OPERATION 1, FACE ) ;
G90 G00 G54 X-1.7405 Y-1.0682 ;
S10000 M03 ;
G43 Z9.15 H01 M08 ;
Z1. ;
G01 Z0. F150. ;
X1.5 ;
Y-0.8864 ;
X-1.5 ;
Y-0.7045 ;
X1.5 ;
Y-0.5227 ;
X-1.5 ;
Y-0.3409 ;
X1.5 ;
Y-0.1591 ;
X-1.5 ;
```

1

```
<?xml version="1.0" ?>
- <feed xmlns="http://www.w3.org/2005/Atom">
    <updated>2012-04-06T14:52:20Z</updated>
    <id>http://code.google.com/feeds/p/v8/svnchanges/basic</id>
    <title>Subversion commits to project v8 on Google Code</title>
    <link rel="alternate" type="text/html"
      href="http://code.google.com/p/v8/source/list" />
    <link rel="self" type="application/atom+xml;type=feed"
      href="http://code.google.com/feeds/p/v8/svnchanges/basic" />
  - <entry>
```

DiPLO
www.diplomacy.edu

The next morning



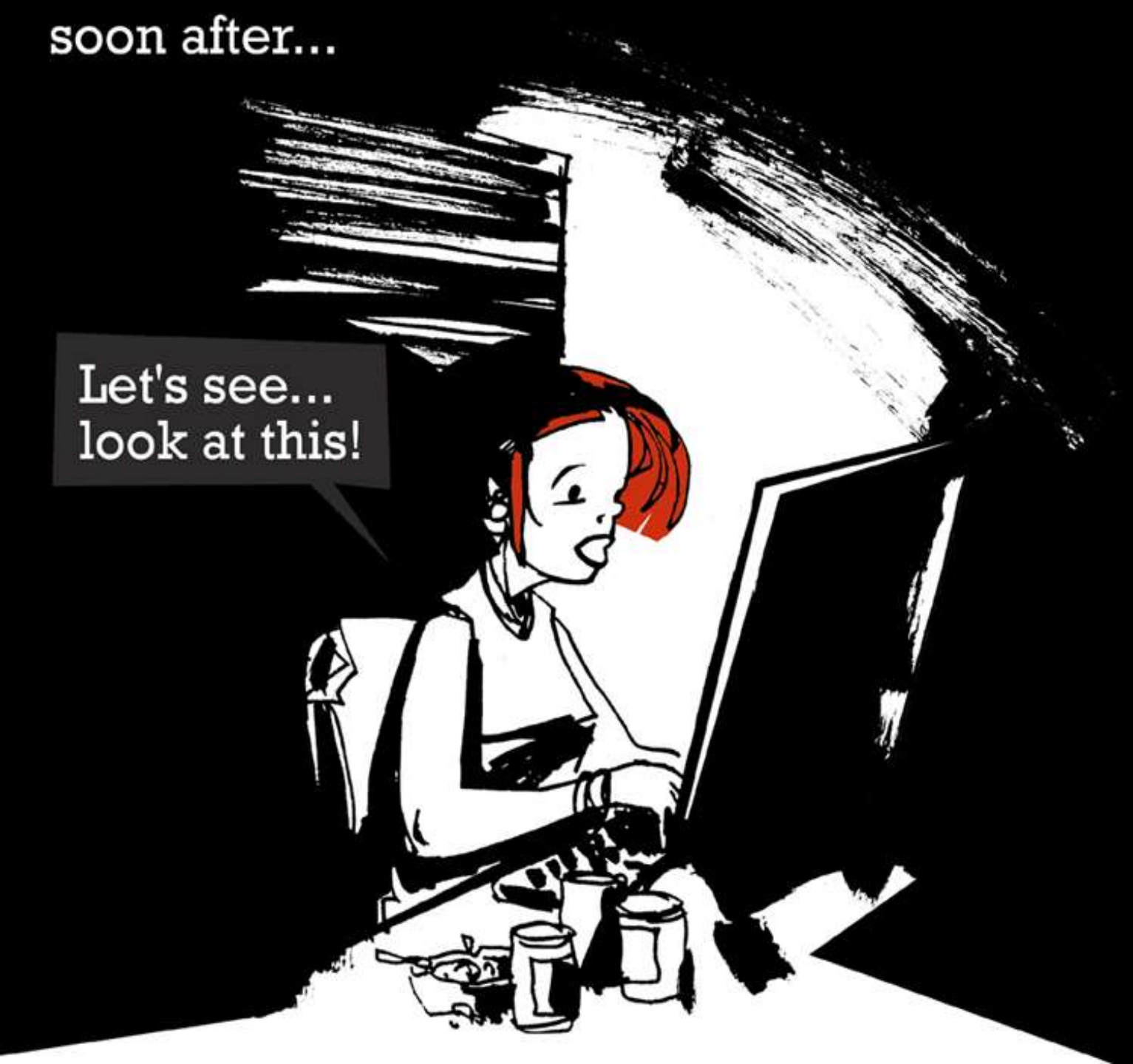
14

15

14

Company B releases a new model!

soon after...




```
ht '    %s [label="%s' % (nodename, label),
isinstance(ast[1], str):
if ast[1].strip():
    = %s"];' % ast[1]
el
    ]'
else
pr    ;'
children = []
for  in n, childenumerat    ]):
   children.append(dotw      d))
print ,'    %s -> {' %
for  in :namechildren
   print '%s' % name,
```

```
OPERATION:  MEM                    PROGRAM

MEM                 000010          N00000001

000010 (SAMPLE PROGRAM.NCF ) ;
G00 G17 G40 G80 G90 G54 ;
;
T20 M06 ;
G00 G90 G54 X0. Y0. ;
G43 H20 Z0.5 ;
;
(PROBE - RECTANGLE BLOCK) ;
G65 P9995 W54. A13. D3. E2. H-0.75 ;
;
N1 ;
T1 M06 ( 0.5 INCH ENDMILL ) ;
( OPERATION 1, FACE ) ;
G90 G00 G54 X-1.7405 Y-1.0682 ;
S10000 M03 ;
G43 Z9.15 H01 M08 ;
Z1. ;
G01 Z0. F15
X1.5 ;
Y-0.886
X-1.5 ;
Y-0.704
X1.5 ;
Y-0.5227
X-1.5 ;
Y-0.3409 ;
X1.5 ;
Y-0.1591 ;
X-1.5 ;
```

```
<?xml version="1.0" ?>
<feed xmlns="http://www.w3.org/
  <updated>2012-04-06T14:52:20
  <id>http://code.google.com/fe
  <title>Subversion commits to pr
  <link rel="alternate" type="text/h
    href="http://code.google.com
  <link rel="self" type="application/
    href="http://code.google.com
- <entry>
```

```
MEM              000010        N00000001

000010 (SAMPLE PROGRAM.NCF ) ;
G00 G17 G40 G80 G90 G54 ;
;
T20 M06 ;
G00 G90 G54 X0. Y0. ;
G43 H20 Z0.5 ;
;
(PROBE - RECTANGLE BLOCK) ;
G65 P9995 W54. A13. D3. E2. H-0.75 ;
;
N1 ;
T1 M06 ( 0.5 INCH ENDMILL ) ;
( OPERATION 1, FACE ) ;
G90 G00 G54 X-1.7405 Y-1.0682 ;
S10000 M03 ;
G43 Z9.15 H01 W08 ;
Z1. ;
G01 Z0. F15
X1.5 ;
Y-0.886
X-1.5 ;
Y-0.704
X1.5 ;
Y-0.5227
X-1.5 ;
Y-0.3409 ;
X1.5 ;
Y-0.1591 ;
X-1.5 ;
```

1

```
<?xml version="1.0" ?>
<feed xmlns="http://www.w3.org/2005/Atom">
  <updated>2012-04-06T14:52:20Z</updated>
  <id>http://code.google.com/feeds/p/v8/svnchanges/basic</id>
  <title>Subversion commits to project v8 on Google Code</title>
  <link rel="alternate" type="text/html"
    href="http://code.google.com/p/v8/source/list" />
  <link rel="self" type="application/atom+xml;type=feed"
    href="http://code.google.com/feeds/p/v8/svnchanges/basic" />
- <entry>
```

Copyright

Begin

$Cep \leftarrow 0, Cdt \leftarrow 0, Nep_1 \leftarrow 0, Ndt_1 \leftarrow 1$

$clock \leftarrow 0$

Repeat

$clock \leftarrow clock + ts$

if $lep = 1$ & $Cdt \neq 0$ **then**

$Ndt_1 \leftarrow Cdt$

$clock \leftarrow 0$

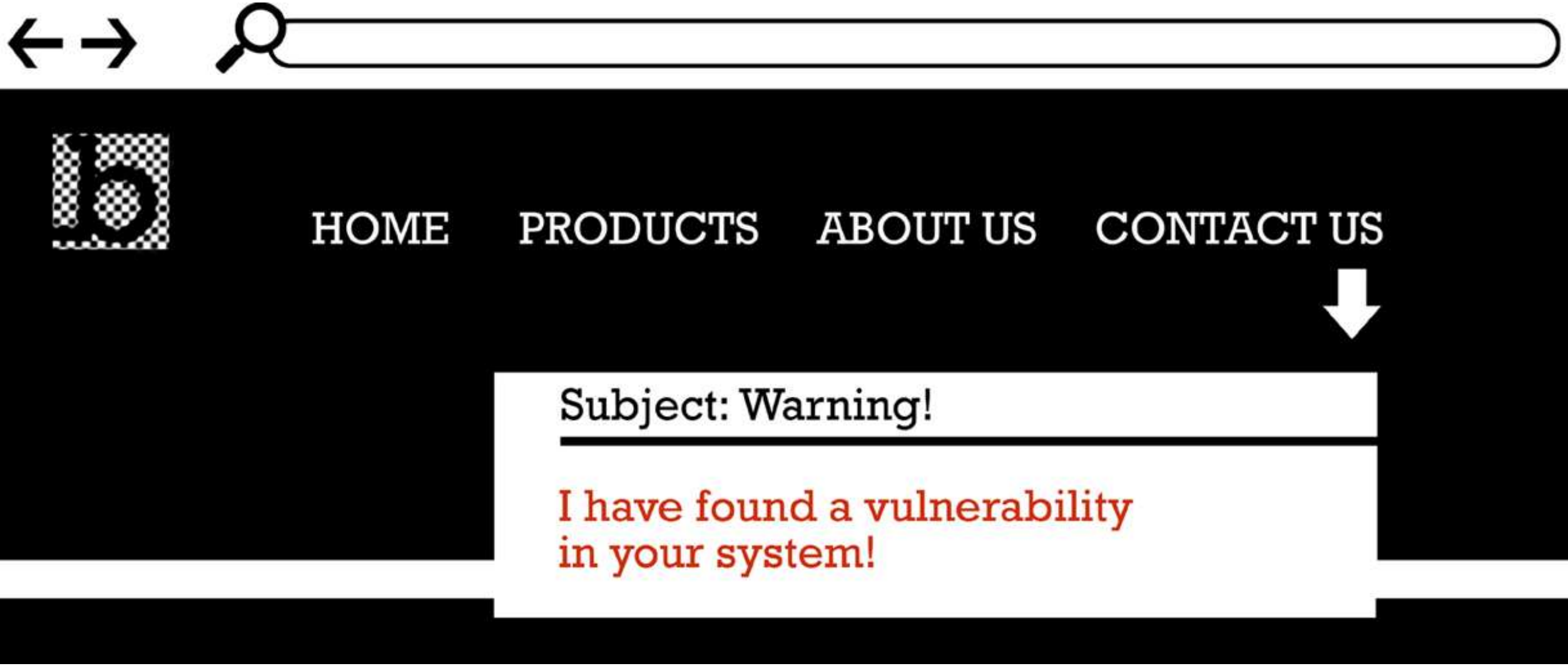
if $clock = dt$ & $Cep \neq 0$ **then**

$Nep_1 \leftarrow Cep$

Access granted

, $Cdt \leftarrow 0$

$Cdt \leftarrow Cdt + 1, Cep \leftarrow 0$


HOME
PRODUCTS
ABOUT US
CONTACT US
Subject: Warning!
I have found a vulnerability
in your system!

Re: Subject: Warning!

...we will prosecute you for breaching our system !

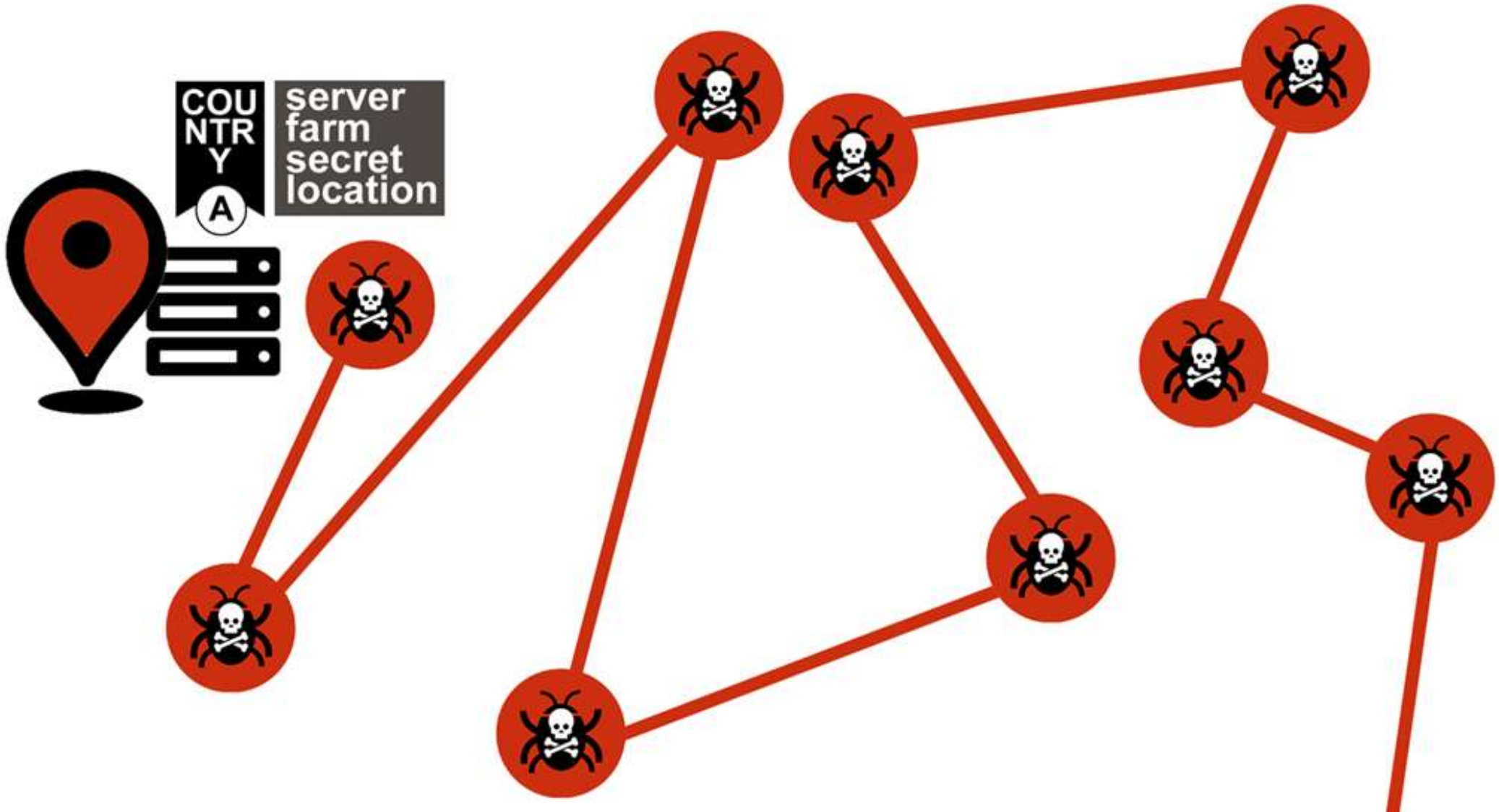
Best regards

> nobody's messing with me!


Hm, interesting.
Let me play with this !
Description
3,000 USD
buy
ctrl+s
ctrl+o
.....
DATA &h17, &hbe, 1, 0, &h88, 4, &h46, &h46
DATA &h81, &hfe, &ha2, &hf, &h7c, &hf6, &h5e, &h1f
DATA &hcb
DIM MachineCode(0 TO 12) AS INTEGER
DIM PokeOffset AS INTEGER
DIM SingleByte AS INTEGER
DEF SEG = VARSEG(MachineCode)
FOR PokeOffset = 0 TO 24
READ SingleByte
POKE VARPTR(MachineCode) + PokeOffset, SingleByte
NEXT
CALL Absolute(VARPTR(MachineCode))
exploit >

> interested?
< yes, same price?
> same price.
> done
< always pleasure doing business with you.

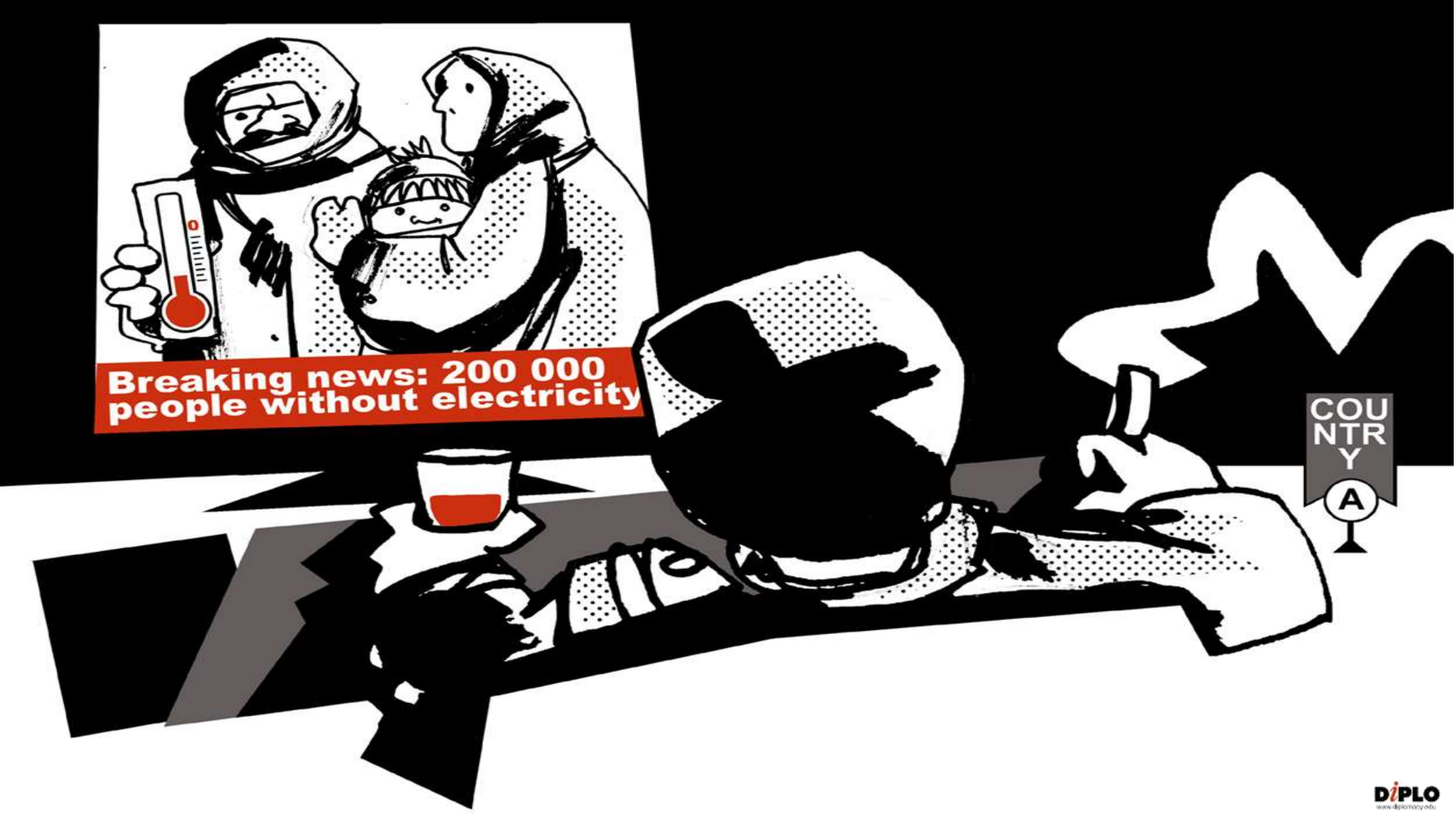

TOP SECRET
CYBER WEAPONS
ON SERVER FARM
SECRET LOCATION
COUNTRY A
server farm secret location
choose weapon
connect to proxy
COUNTRY A




COUNTRY C
important power plant server


MEM 000010 N00000001
000010 (SAMPLE PROGRAM.NCF) ;
G00 G17 G40 G80 G90 G54 ;
T20 M06 ;
G00 G90 G54 X0. Y0. ;
G43 H20 Z0.5 ;
(PROBE - RECTANGLE BLOCK) ;
>run
>waitfor /
>shutdown
>malfunction !!!


CYBER ATTACK


Breaking news: 200 000 people without electricity
COU
NTR
Y
A

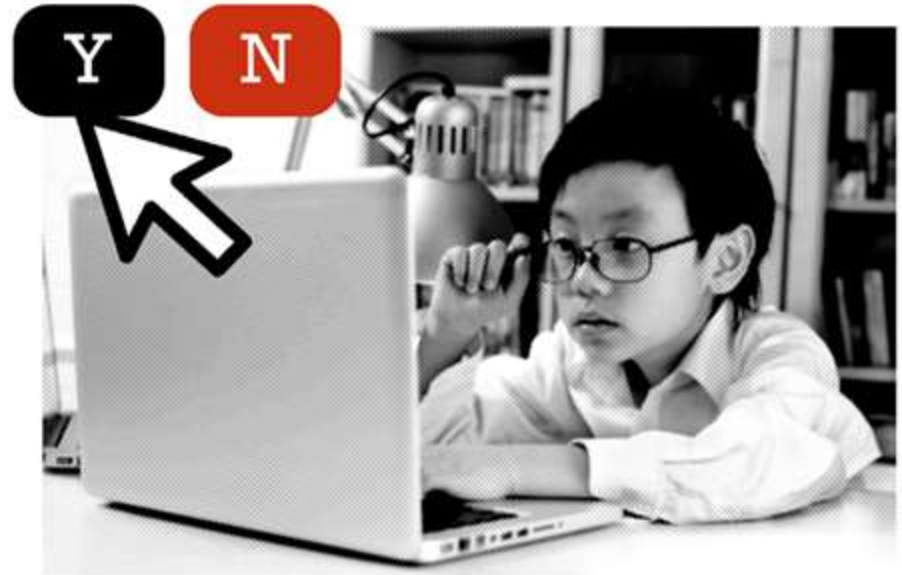

DATA &h81, &hfe, &ha2, &hf, &h7c, &hf6, &h5e, &h1f
DATA &hcb
DIM MachineCode(0 TO 12) AS INTEGER
DIM PokeOffset AS INTEGER
DIM SingleByte AS INTEGER
DEF SEG = VARSEG(MachineCode)
FOR PokeOffset = 0 TO 24
READ SingleByte
POKE VARPTR(MachineCode) + PokeOffset, SingleByte
NEXT
CALL Absolute(VARPTR(MachineCode))
DATA &h17, &hbe, 1, 0, &h88, 4, &h46, &h46
DATA &h81, &hfe, &ha2, &hf, &h7c, &hf6, &h5e, &h1f
DATA &hcb
DIM MachineCode(0 TO 12) AS INTEGER
DIM PokeOffset AS INTEGER
DIM SingleByte AS INTEGER
DEF SEG = VARSEG(MachineCode)
FOR PokeOffset = 0 TO 24
READ SingleByte
POKE VARPTR(MachineCode) + PokeOffset, SingleByte
NEXT
CALL Absolute(VARPTR(MachineCode))
7625!
To:
We discovered this and named it Bugzilla!
DiPLO
www.diplomacy.edu


HOME
PRODUCTS
ABOUT US
CONTACT US
patch !

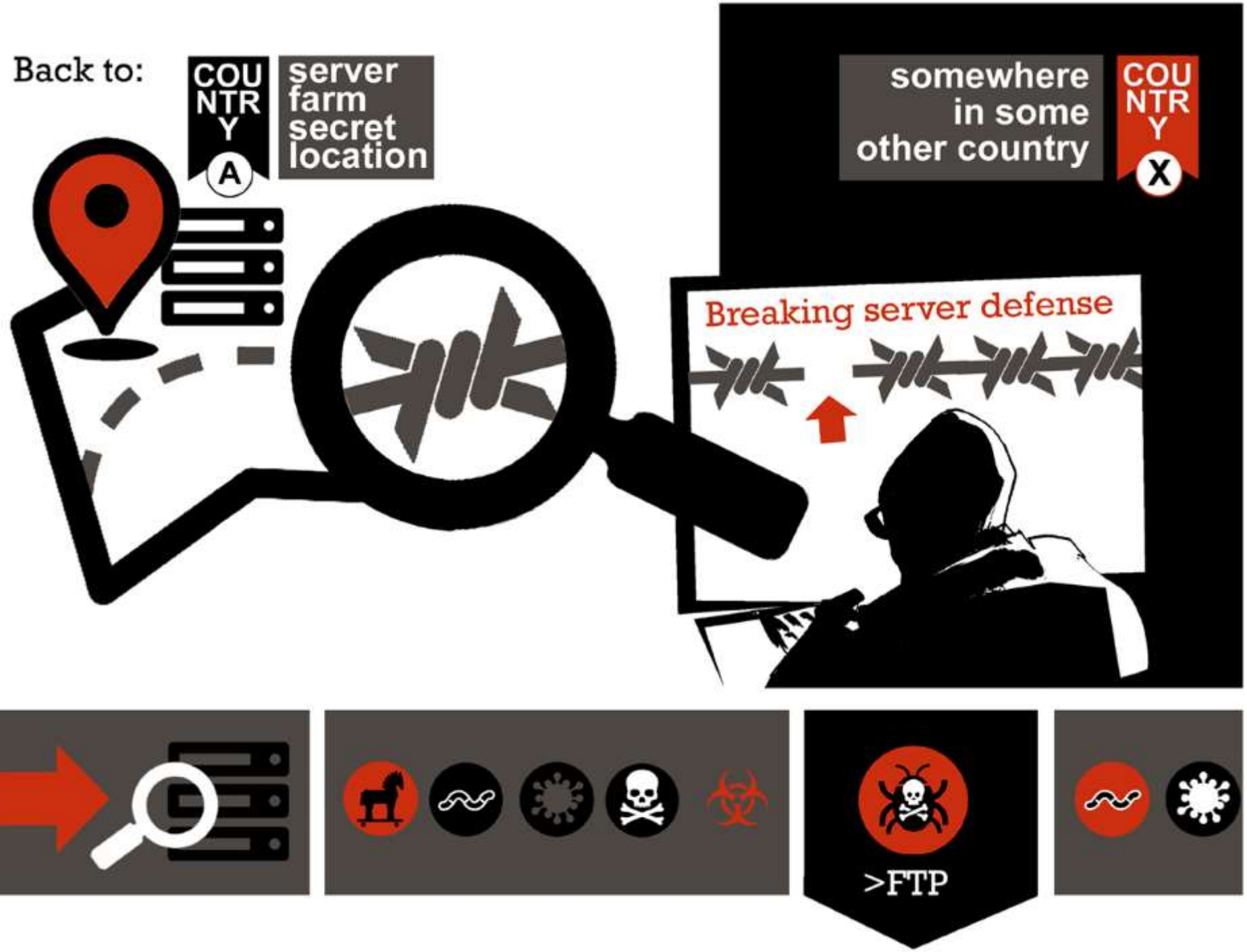
No updates available for your outdated system !

Installing 8 of 10 updates...
This may take a while.

Installing critical updates



somewhere> potential disaster


Back to:
COUNTRY A
server farm secret location
somewhere in some other country
COUNTRY X
Breaking server defense
>FTP


No updates for outdated system.
Pay the ransom!
Update cancelled
Pay the ransom!
System updated.
Protected


Pay the ransom!


This is a complete disaster.
Perhaps we can try to fix this...
later...

> Disaster occurs.

> epilogue

DiPLO
www.diplomacy.edu

> www.diplomacy.edu/cybersecurity
> dig.watch/cybersecurity
> vladar@diplomacy.edu

> run
> The secret life of a vulnerability
> concept: Vladimir Radunovic
> illustration + layout: Vladimir Veljasevic
> production: @DiploFoundation | 2018
> exit