

បដិវត្តន៍នៃការគំរាមគំហែងតាមអ៊ីនធឺណិត តើយើងត្រូវបង្កើនហើយឬទេ?



OU PHANNARITH
MPTC
@phannarith

AV industry in 1998



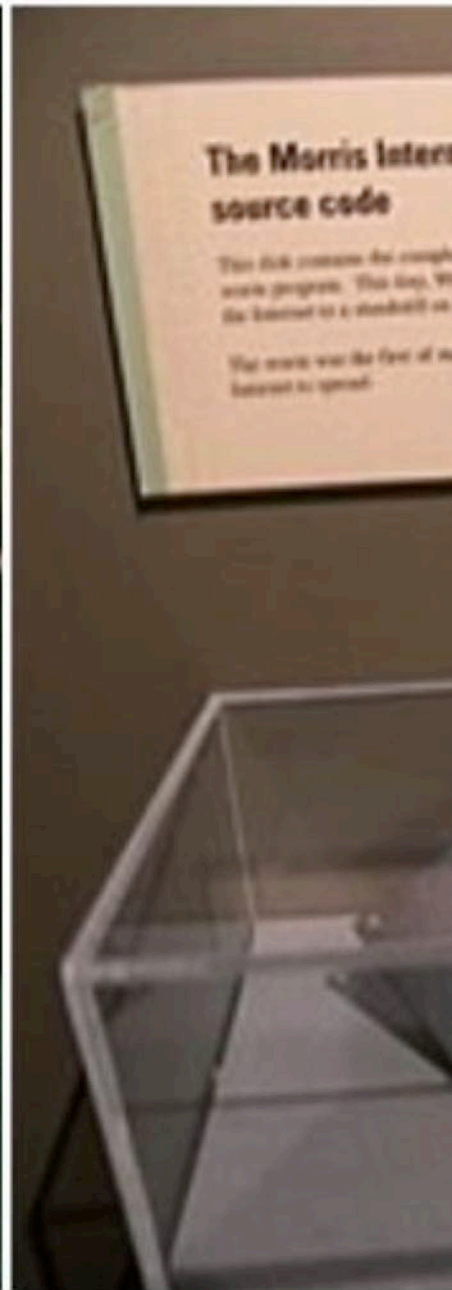
AV industry in 2008



Which computer is not running Antivirus Software?



ARE YOU SURE, YOU ARE SAFE?



Microsoft Outlook

File View Go Tools Actions Help

Reply Reply to All Forward Send and Receive

Inbox

From	Subject	Received
Qui-Gon ...	ILOVEYOU	Thu 5/4/00 0...

From: Qui-Gon Jinn
Subject: ILOVEYOU
To: Obi-Wan Kenobi
Cc:

kindly check the attached LOVELETTER coming from me.





ESTONIA CYBER

DATE:
APRIL 2007

IMPACT:
Estonia's government,
financial, and media online services
were knocked offline





"FLAME" BURNS MIDDLE EAST COMPU
Sophisticated virus hits Iran particularly h
| Rubio on voter ID laws and Latinos: 'What's the big deal?'



ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See your Match

Over 37,65,000 anonymous members!



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

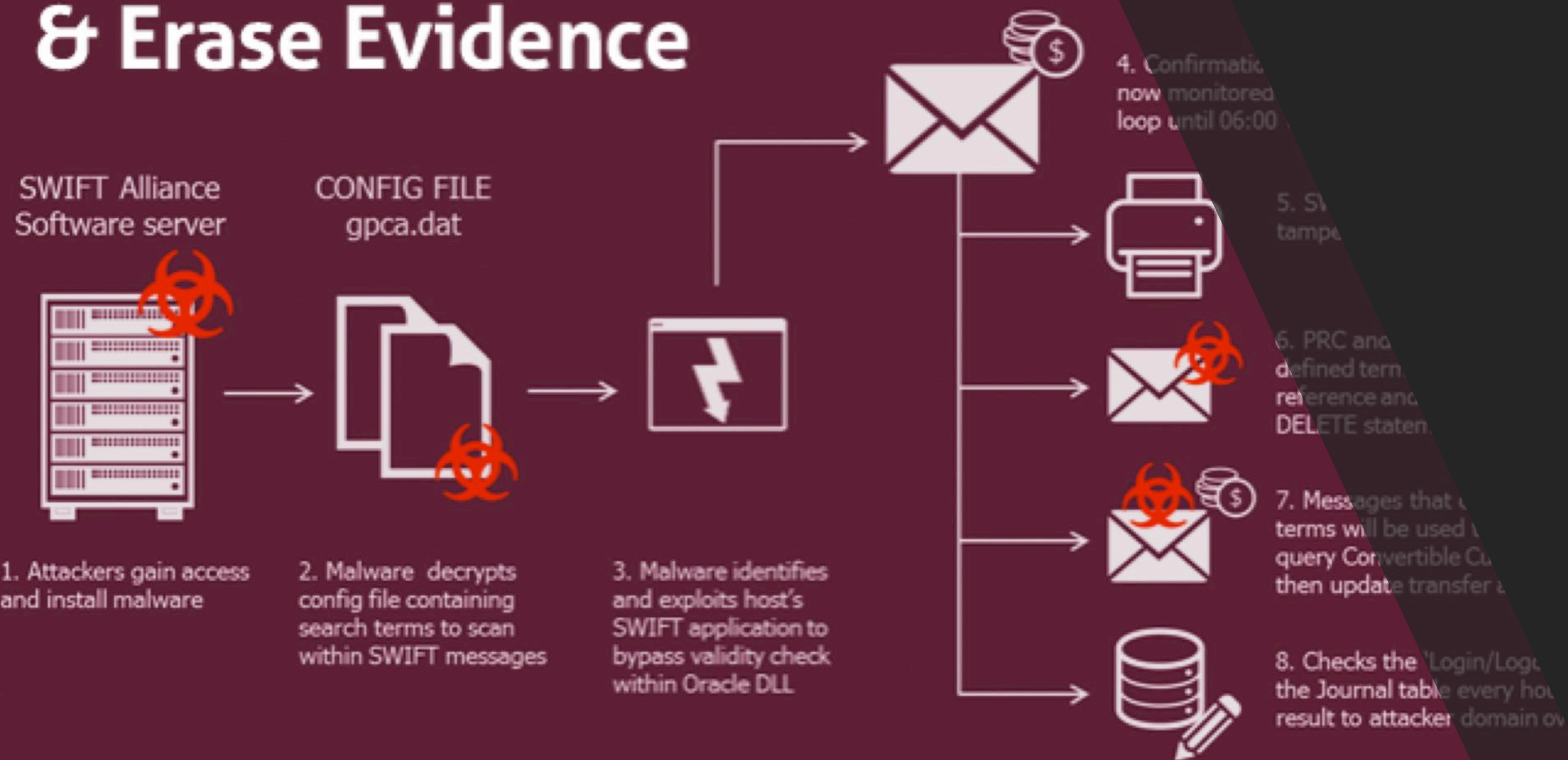
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Hackers accessed SWIFT to Steal & Erase Evidence



'Wannacry' ransomware attacks

Worldwide attack has crippled more than 300,000 computers in 150 countries

● Location of computers attacked by the 'Wannacry' ransomware*

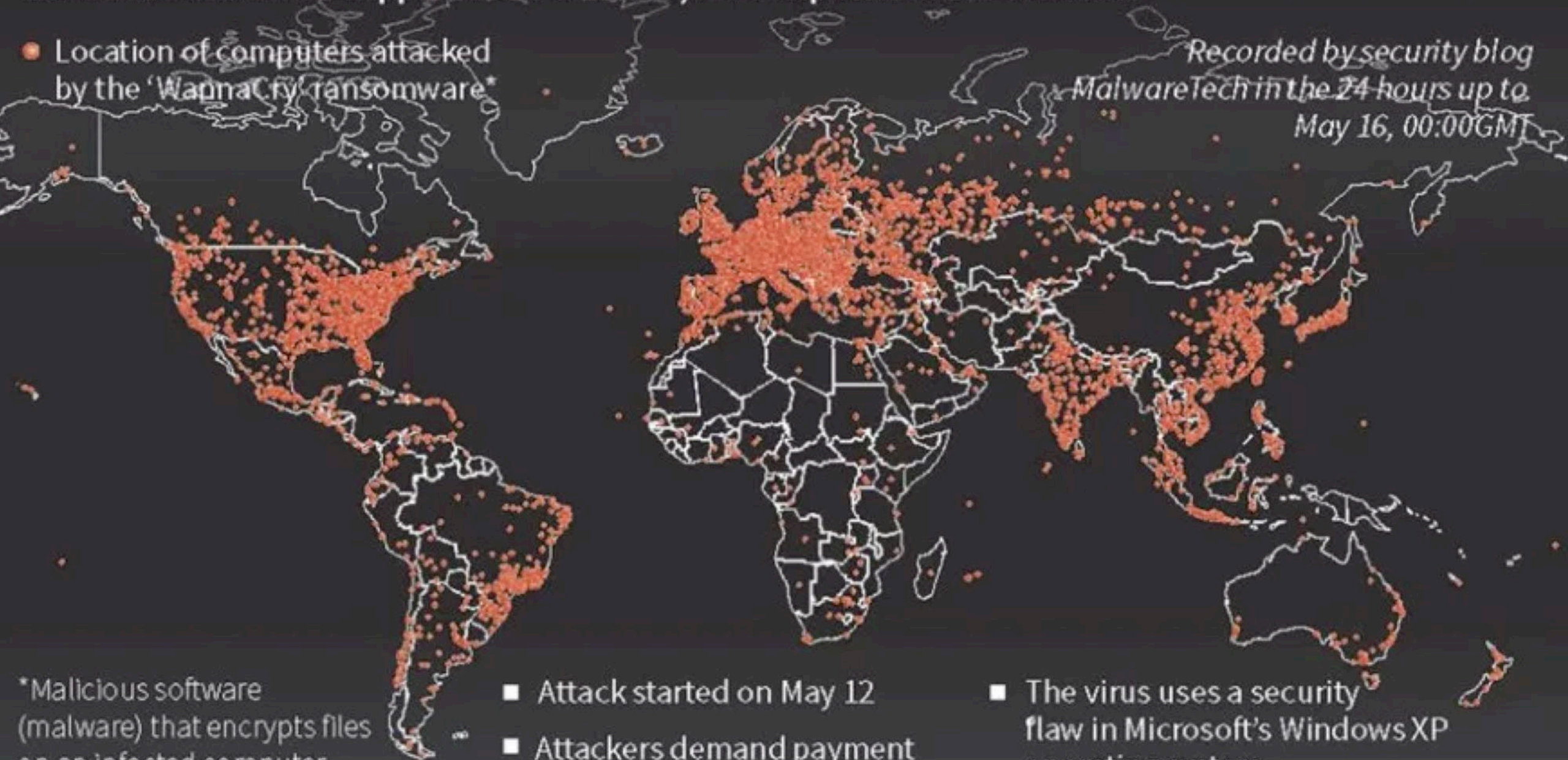
Recorded by security blog
MalwareTech in the 24 hours up to
May 16, 00:00GMT

*Malicious software (malware) that encrypts files on an infected computer and demands payment to

■ Attack started on May 12

■ Attackers demand payment of \$300 in virtual currency

■ The virus uses a security flaw in Microsoft's Windows XP operating system



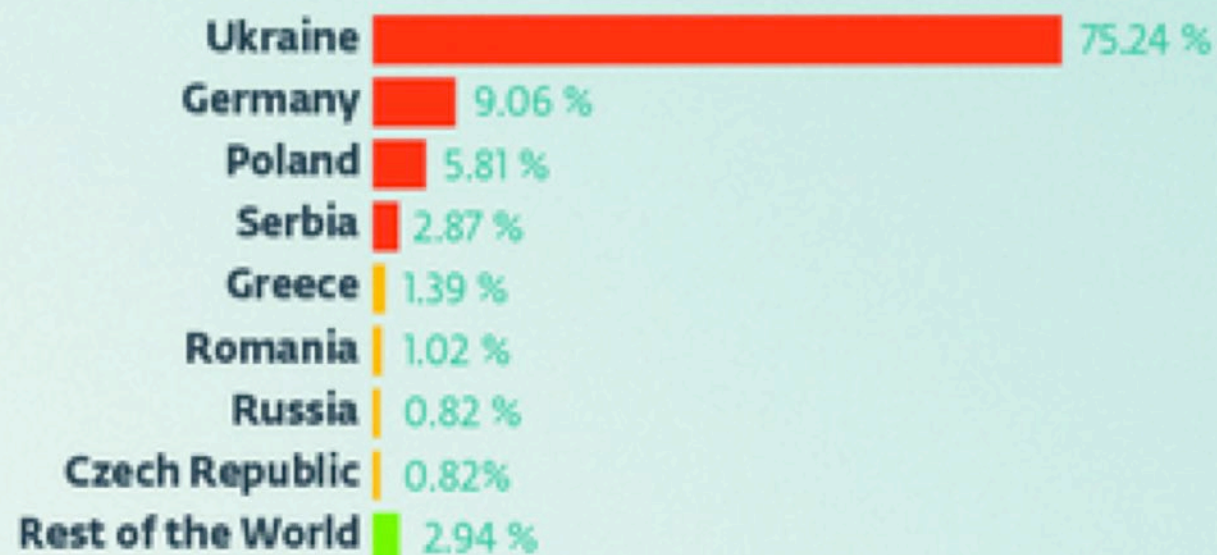


Abfahrt / Departure

Zeit	Über	Nach	Gleis / platform
21:42	F-Süd - Hanau	Wächtersbach	9
21:47	F-Hochst - Kalkheim	Königstein (Ta)	21
21:50	Niederrad - Stadion	Riedstadt Goddellau	6
21:51	Mannheim	Stuttgart Hbf	7
21:52	Friedberg - Gießen	Marburg (Lahn)	14
21:52	Friedberg - Wetzlar	Dillenburg	14
21:53			23
21:55			13
22:05			6
22:06			12
22:10			17
22:10			8
22:15			7
22:17	F-Hochst - Kalkheim	Königstein (Ta)	21
22:17	Hanau - Fulda	Kassel-Wilhelmsh.	9
22:22	Friedberg - Gießen	Treysa	15
22:22	Friedberg - Wetzlar	Siegen	15
22:23	Hanau - Aschaffenburg	Nürnberg Hbf	6
22:25	Flughafen (Airport) - Mainz Hbf	Saarlöcher Hbf	20
22:26	F-Süd - Hanau	Bebra	13

PETYA

Ransomware Outbreak



ENJOY SAFER
TECHNOLOGY™



**On December 23rd, 2015,
hackers caused a blackout
for roughly a quarter
million Ukrainians.**







Connection to 5.206.225.96 23 port [tcp/telnet] succeeded

```
. . .  
  
@88> @88> @88>  
%8P %8P %8P  
888: x888 x888.  
8888~'888X ?888f  
X888 888X '888> .@88u =~8888f8888r u888u. .@88  
X888 888X '888> 888E 4888>'88~ .@88 ~8888~ .88  
X888 888X '888> 888E 4888> ' 9888 9888 88  
X888 888X '888> 888E 4888> 9888 9888 88  
*88%~*88~ '888! 888& ^~8888*~+ 9888 9888 88  
R888~ ~Y~ ~888*~ ~888~ R888~  
 ^Y~ ^Y'
```

- A text-based MUD by Oscar Popodokus -

```
o account? Register at www.elrooted.com  
Enter user> yop  
op  
Enter pass> yop  
**
```

Disconnected by server. |
Press any key to exit.



520

A large red circle containing the number 520 in white. Below the number, the text 'Days / 146 (World Wide)' is written in white.

Days / 146 (World
Wide)

Days until breach discovery



55%

A large blue circle containing the text '55%' in white. Below the text, the text '53% (World Wide)' is written in white.

53% (World Wide)

Breach Notifications by External

Reputation

**Account
Credential**

Legal

nothing

hopping

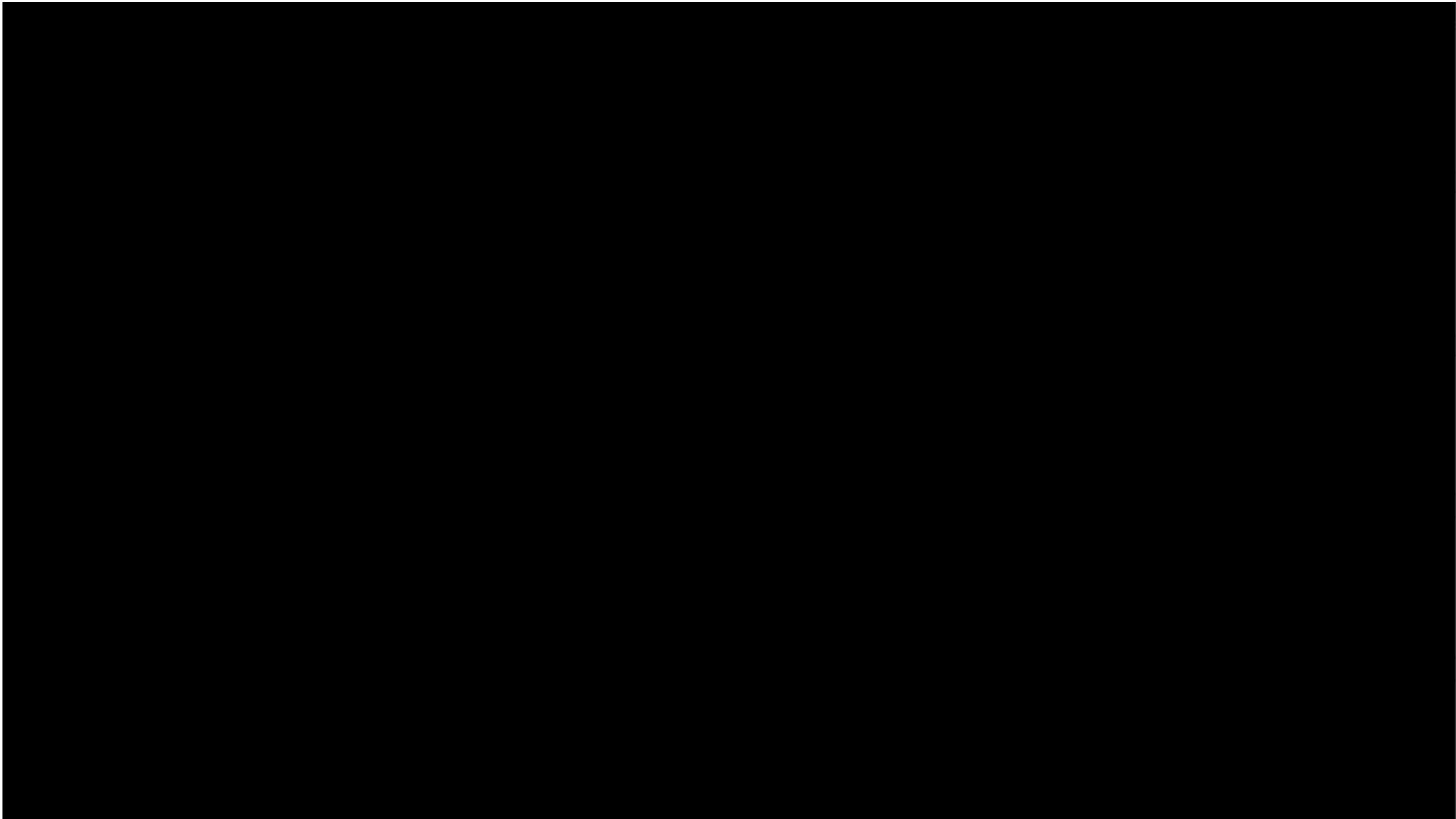
SPAMING

**Hosting
Malware**

**Safe
Home**



BLACK MARKETS





They only need to be right

ONE TIME

We need to be right

EVERY TIME



Vuthea Chheang

1 hr · 🌐

ឱ! ចោរមុខស្រស់ ដោះមិនប្រណី សូម្បីសោភ័ក្តិ ក៏វាមិនលែង។
ទុកតែកងមុខ ឲ្យម្ចាស់ឃើញស្តែង កុំឲ្យរមែង ថាបាត់ទាំងអស់។
— at 📍 Chungbuk National University.

👍 Like 💬 Comment ➦ Share

👍 😂 🤔 Vannak Eng and 37 others

View 1 more comment



Heak Menghok ចោរចិត្តល្អ

Like · Reply · 👍 1 · 1 hr



Khi Hort Not vuthea's bicycle.

Like · Reply · 58 mins



Vuthea Chheang កងខ្លី ពណ៌ទឹកសមុទ្រ

Like · Reply · 57 mins



Eam Voleak Strong haha

Like · Reply · 👍 1 · 47 mins



라승주 be careful. it often happens

Like · Reply · 👍 1 · 43 mins



Write a comment...



THANK YOU

