

ITUEvents

ITU Regional Cybersecurity Forum for Europe and CIS

27-28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence
in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of
infocommunication infrastructure to make cities and human settlements
inclusive, safe, and resilient

POLICIES &
STRATEGIES

CERTIFICATION
FRAMEWORKS

DATA
PROTECTION

SECURITY
CHALLENGES

5G, eSIM
IoT, AI



Hosted and co-organized by:



REPUBLIC OF BULGARIA
State e-Government Agency



REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology
and Communications



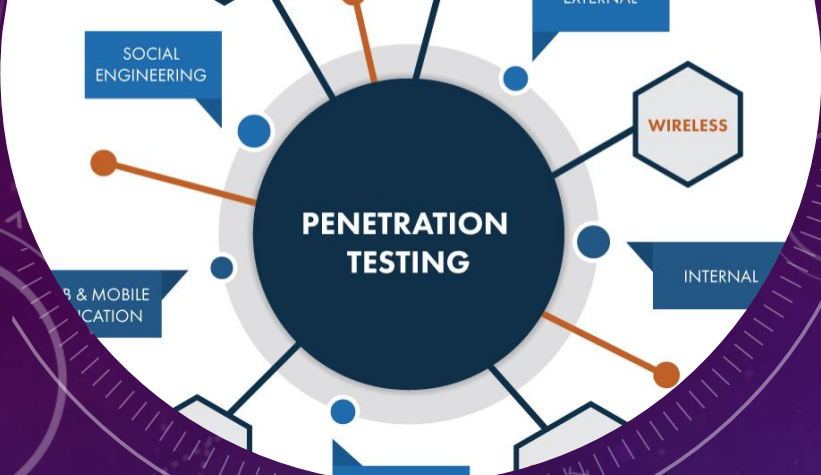
The background features a dark blue gradient with a starry space pattern. Overlaid on this are several technical diagrams, including circular gauges with numerical scales (e.g., 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260) and various circular arrows indicating movement or processes.

KAZAKHSTAN EXPERIENCE IN INCIDENT RESPONSE

CASES FROM EXPERIENCE OF TSARKA TEAM

WHO AM I





WHAT WE ARE DOING

BUG REPORTING





IT IS JUST TO PROVE THAT CYBER SECURITY IS IMPORTANT



IT'S HARD, BUT WE
DON'T GIVE UP

AND CONTINUE
TO WORK

CYBERSECURITY FIGURES FOR TODAY

- 336 critical infrastructure;
- 7 Security Operation Centre;
- Cyber Security Grants Increased from 60 to 674 (target 1300);
- 73% level of awareness about threats cybersecurity;
- 2.5 billion cyberattacks neutralized National coordination information center security;
- Global cybersecurity index increased from 82 to 40 (target 15).



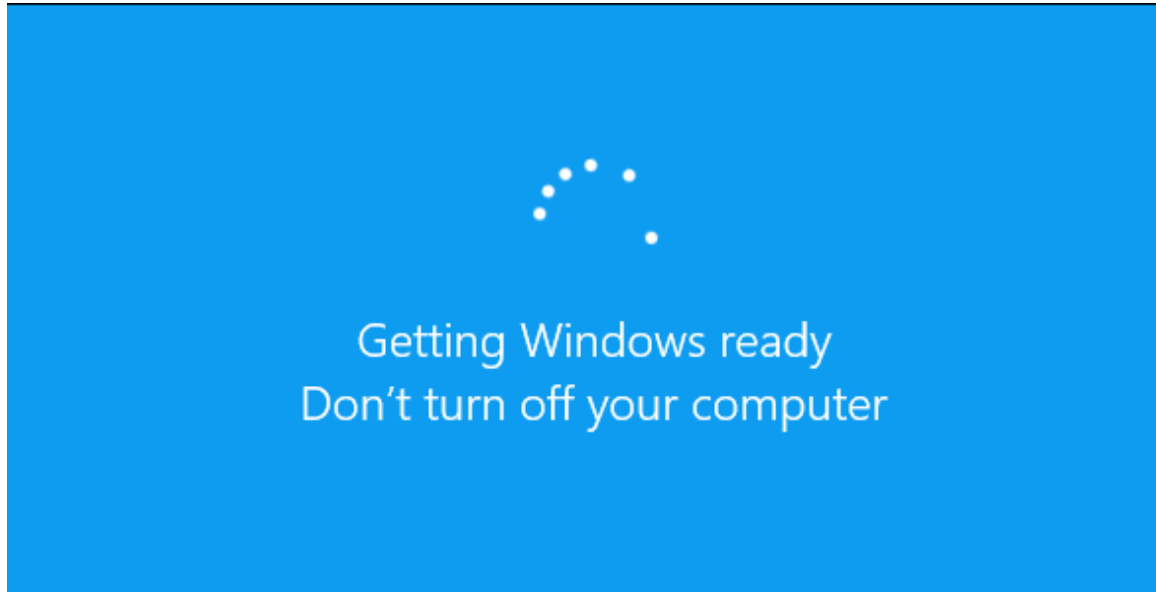
CASE №1

The background features a dark blue gradient with a field of small white stars. Overlaid on this are several technical diagrams in a lighter blue color. In the top right, there is a large circular gauge with a scale from 0 to 210 and a needle pointing to approximately 190. Below it is a smaller circular diagram with concentric lines and arrows. In the bottom right, another circular diagram shows concentric lines and arrows. In the bottom left, a dashed circular arrow points counter-clockwise. In the top left, a partial circular diagram is visible.

Windows 10 Update

VS

Windows 7 Update



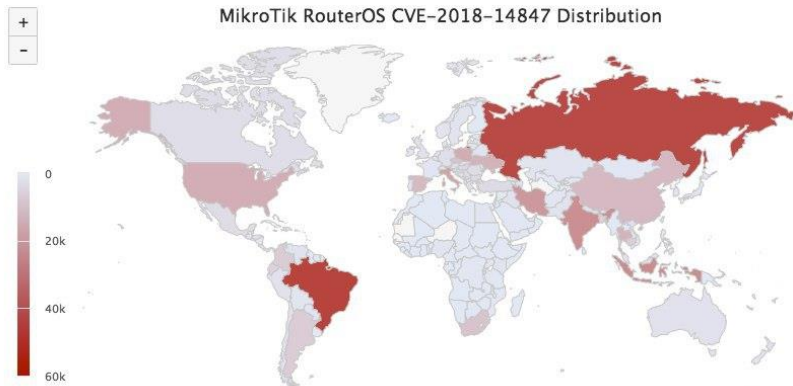
SOLUTION = LICENSED SOFTWARE

CASE №2

The background is a dark blue gradient with a field of small white stars. Overlaid on this are several technical diagrams in a lighter blue color. In the top right, there is a large circular gauge with a scale from 0 to 210 and a needle pointing to approximately 190. Below it is a smaller circular diagram with concentric circles and arrows. In the bottom right, there is another circular diagram with concentric circles and arrows. In the bottom left, there is a partial circular diagram with arrows. In the top left, there is a small circular diagram with a curved arrow.

The following is a Top 20 nations list (device count, country).

```
42376 Brazil/BR
40742 Russia/RU
22441 Indonesia/ID
21837 India/IN
19331 Iran/IR
16543 Italy/IT
14357 Poland/PL
14007 United States/US
12898 Thailand/TH
12720 Ukraine/UA
11124 China/CN
10842 Spain/ES
8758 South Africa/ZA
8621 Czech/CZ
6869 Argentina/AR
6474 Colombia/CO
6134 Cambodia/KH
5512 Bangladesh/BD
4857 Ecuador/EC
4162 Hungary/HU
```



4 SEPTEMBER 2018

7,500+ MikroTik Routers Are Forwarding Owners' Traffic to the Attackers, How is Yours?

[Update]

2018-09-05 11:00 GMT+8, with the generous help from the AS64073, 103.193.137.211 has been promptly suspended and is no longer a threat.

Overview

MikroTik is a Latvian company founded in 1996 to develop routers and wireless ISP systems. MikroTik now provides hardware and software for Internet connectivity in countries around the world. In 1997, MikroTik created the RouterOS software system. In 2002, MikroTik decided to build its own hardware and created the RouterBOARD brand. Each RouterBOARD device runs the RouterOS software system.[\[1\]](#)

According to WikiLeaks, the CIA Vault7 hacking tool Chimay Red involves 2 exploits, including Winbox Any Directory File Read (CVE-2018-14847) and Webfig Remote Code Execution Vulnerability.[\[2\]](#)

Отображение строк 0 - 24 (72346 всего, Запрос занял 0.0790 сек.) [date: 2018-08-12 20:23:51 - 2018-08-12 20:23:30]

```
SELECT * FROM `proxies` ORDER BY `date` DESC
```

1 > >> Количество строк: 25 Фильтровать строки: Поиск в таблице

Сортировать по индексу: Ниодного

+ Параметры

	id	ip	port	schema	country	date	1		
<input type="checkbox"/>	Изменить	Копировать	Удалить	1880006	177.1...	4145	socks4	BR	2018-08-12 20:23:51
<input type="checkbox"/>	Изменить	Копировать	Удалить	22770	207.158.188	4145	socks4	BR	2018-08-12 20:23:48
<input type="checkbox"/>	Изменить	Копировать	Удалить	1850539	200.111.202	4145	socks4	AR	2018-08-12 20:23:47
<input type="checkbox"/>	Изменить	Копировать	Удалить	220593	102.111.5	4145	socks4	KE	2018-08-12 20:23:37
<input type="checkbox"/>	Изменить	Копировать	Удалить	2360935	91.224.189	4145	socks4	RU	2018-08-12 20:23:35
<input type="checkbox"/>	Изменить	Копировать	Удалить	23025	201.216.206	4145	socks4	GT	2018-08-12 20:23:35
<input type="checkbox"/>	Изменить	Копировать	Удалить	309668	197.254.15.66	4145	socks4	KE	2018-08-12 20:23:34
<input type="checkbox"/>	Изменить	Копировать	Удалить	1803153	116.211.112	4145	socks4	CN	2018-08-12 20:23:34
<input type="checkbox"/>	Изменить	Копировать	Удалить	3081717	117.56.58.59	4145	socks4	CN	2018-08-12 20:23:34
<input type="checkbox"/>	Изменить	Копировать	Удалить	1519023	200.201.29	4145	socks4	VE	2018-08-12 20:23:33
<input type="checkbox"/>	Изменить	Копировать	Удалить	2020691	95.211.168.216	4145	socks4	IT	2018-08-12 20:23:32
<input type="checkbox"/>	Изменить	Копировать	Удалить	2783431	89.281.10.204	4145	socks4	AT	2018-08-12 20:23:31

	A	B
1	BR	16555
2	IR	6029
3	ID	4891
4	RU	4813
5	CN	4326
6	TH	3217
7	IN	2991
8	ES	2341
9	PL	2151
10	IT	2122
11	UA	1864
12	CZ	1244
13	ZA	1087
14	BG	945
15	HU	943
16	KH	888
17	BD	712
18	AR	663
19	US	660
20	TR	591
21	RS	573
22	GB	546
23	KZ	539

SOLUTION = UPDATING

BOTNET DATA MONITORING

CASE №3

The background is a dark blue gradient with a field of small white stars. Overlaid on this are several technical diagrams in a lighter blue color. In the top right, there is a large circular gauge with a scale from 0 to 210 and a needle pointing to approximately 190. Below it is a smaller circular diagram with concentric circles and arrows. In the bottom right, there is another circular diagram with concentric circles and arrows. In the bottom left, there is a partial circular diagram with arrows. The overall aesthetic is clean, modern, and technical.

თიბისი ბანკი

გამარჯობა

შეიყვანე მომხმარებელი

შეიყვანე პაროლი

დამახსოვრება

შესვლა

რეგისტრაცია

ბანკი ქართუ
CARTU BANK

GEO | ENG

ფიზიკური პირები | ორიდული პირები

მომხმარებლის სახელი

პაროლი

მონაცემების დამახსოვრება

შესვლა

VISA ისარგებლეთ ბანაკაპორტმა პირიმლივინებით!

Sifio, Apple Pay, Google Pay, Samsung Pay, Mir, UnionPay, Mastercard, Maestro, American Express

Магазин | Платежи | Мой Банк | Red | Бонус | Гид | Maps | Переводы

Уже зарегистрированы

Мобильный телефон

Пароль

Войти


[Забыли пароль?](#)

9:44 LTE

← Біз 5 Mercedes-Benz және 11 Iphone 8 сый...

HALYK BANK
3 hrs ·

Біз 5 Mercedes-Benz және 11 Iphone 8 сыйлықтарын ұсынамыз!



H.A.L.Y.K.B.A.N.K.K.Z [LEARN MORE](#)

Сбербанк
Онлайн

Логин

Пароль

Запомнить меня

Войти

[Забыли логин или пароль?](#)

Регистрация
Нужна карта Сбербанка и мобильный телефон

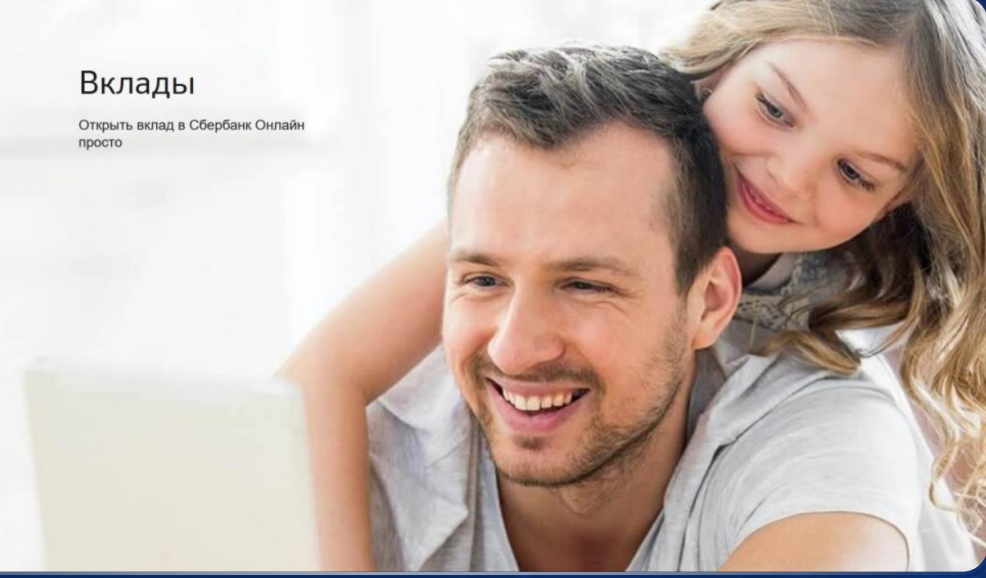
Вклады

Открыть вклад в Сбербанк Онлайн просто

Правила безопасности

Если вас просят ввести пароль входа в Сбербанк Онлайн для отмены или аннулирования операции, не делайте этого. Это мошенники.

Еще совет



PHISHING

Yönetici Girişi

admin

•••••

Giriş Yap

Yonetim Paneli

Giris Yap

PHISHING VS PHISHING



MORTAL KOMBAT X



```
-----  
Array  
(  
    [sifre] => 1  
)
```

```
Array  
(  
    [USER] => nginx  
    [HOME] => /var/lib/nginx  
    [FCGI_ROLE] => RESPONDER  
    [DOCUMENT_ROOT] => /var/www/slider.kz  
    [SCRIPT_FILENAME] => /var/www/slider.kz/s.php  
    [PATH_TRANSLATED] => /var/www/slider.kz/s.php  
    [QUERY_STRING] => op=login  
    [REQUEST_METHOD] => POST  
    [CONTENT_TYPE] => application/x-www-form-urlencoded  
    [CONTENT_LENGTH] => 7  
    [SCRIPT_NAME] => /s.php  
    [REQUEST_URI] => /s.gif?op=login  
    [DOCUMENT_URI] => /s.php  
    [SERVER_PROTOCOL] => HTTP/1.1  
    [REQUEST_SCHEME] => http  
    [GATEWAY_INTERFACE] => CGI/1.1  
    [SERVER_SOFTWARE] => nginx/1.12.2  
    [REMOTE_ADDR] => 179.43.157.112  
    [REMOTE_PORT] => 56126  
    [SERVER_ADDR] => 95.59.127.5  
    [SERVER_PORT] => 8080  
    [SERVER_NAME] => sly.kz  
    [REDIRECT_STATUS] => 200  
    [HTTP_HOST] => sly.kz:8080  
    [HTTP_CONNECTION] => keep-alive  
    [HTTP_CONTENT_LENGTH] => 7  
    [HTTP_CACHE_CONTROL] => max-age=0  
    [HTTP_ORIGIN] => http://housebankkz.com  
    [HTTP_UPGRADE_INSECURE_REQUESTS] => 1  
    [HTTP_CONTENT_TYPE] => application/x-www-form-urlencoded  
    [HTTP_USER_AGENT] => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.  
    [HTTP_ACCEPT] => text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applicati  
    [HTTP_REFERER] => http://housebankkz.com/admin/  
    [HTTP_ACCEPT_ENCODING] => gzip, deflate  
    [HTTP_ACCEPT_LANGUAGE] => ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7  
    [PHP_SELF] => /s.php  
    [REQUEST_TIME_FLOAT] => 1563267616.3364  
    [REQUEST_TIME] => 1563267616  
)  
-----  
Array  
(  
    [sifre] => 1  
)
```

7891	71800881947	1195488a	2019-07-16 08:07:22	IP Banla / Sil
7890	71800798110	1195488a	2019-07-16 08:07:22	IP Banla / Sil
7889	718001801383	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7888	718001841643	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7887	718000874858	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7886	718000420359	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7885	718000436793	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7884	718000038641	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7883	718001180714	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7882	718001869917	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7881	718007523901	1195488a	2019-07-16 08:07:21	IP Banla / Sil
7880	718005442781	1195488a	2019-07-16 08:07:20	IP Banla / Sil
7879	718001898288	1195488a	2019-07-16 08:07:20	IP Banla / Sil
7878	7180002141781	1195488a	2019-07-16 08:07:20	IP Banla / Sil
7877	718000749145	1195488a	2019-07-16 08:07:20	IP Banla / Sil
7876	718000037060	1195488a	2019-07-16 08:07:20	IP Banla / Sil
7875	718000850389	1195488a	2019-07-16 08:07:20	IP Banla / Sil

Yönetim Paneline Hoşgeldiniz

Tüm Kayıtları Sil
Siteyi Pasif Et / Siteyi Akif Et

#	Kullanıcı No	Şifre	SMS1	SMS2	Tarih	Sil
2	7075431332	1488	1488	1922	2019-07-16 09:14:14	IP Banla / Sil

Copy
CSV
Excel
PDF
Print

Search:

ID	Email	Password	Code	Delete
1	7075900000	erke270000		Delete
2	+7705130000	210720000		Delete
4	+7777700000	ggg00000		Delete
5	8747650000	aimanovan000000	aimanovan000000	Delete
6	+7777760000	ggg55500		Delete
7	Jalga0000000000	amina2000		Delete
8	+7702100000	123lok000000		Delete
9	+7708750000	Qwerty0000		Delete
10	+7775700000	12345678	12345678	Delete
11	+7771890000	953000		Delete
12	87024050000	sax000000		Delete
13	77752290000	4142		Delete
14	87758000000	sh000000		Delete
15	+77771900000	290900000		Delete
16	87766620000	ans0000		Delete
17	+77075200000)" >		Delete

Showing 0 to 0 of 0 entries

Previous
Next

PHISHING HUNTER

Mode	Search Word	Where	Duration		
Contains	<input type="text" value="kaspi"/> <input type="button" value="Go!"/>	Recently Added	Last 7 Days		
	Domain	TLD	Len	IDN	Date
		x	x	x	
1	kaspito	com	7	0	2019-07-27
2	kaspi-bank	com	10	0	2019-07-29
3	kaspi-bannk	com	11	0	2019-07-29
4	kaspionlinekz	com	13	0	2019-07-30
5	kaspionlinee-kz	com	15	0	2019-07-31
6	ghukaspirit	com	11	0	2019-08-01
7	gkaspire	com	8	0	2019-08-01
8	workaspire	com	10	0	2019-08-01

EVIL SITE

VALID SITE

USER

```
84 https://static.zdassets.com GET /ekr/asset_composer.45552cb1a14d00ee1zre.js
85 https://homeybank.com GET /vendor-1ef7e994c4dfc6938c24.js
86 https://homebank.kz GET /5a46094c10954e2ea6d39dc89cdd1cbd.svg
87 https://homebank.kz GET /625d5309b9e8e253a9734114f3ea1f2e.svg
88 https://homebank.kz GET /e6b654b93ceda1b5335d80e4871f8c42.svg
89 https://homebank.kz GET /3937820250adf31713ca3fbe38342b17.svg
90 https://homebank.kz GET /8924820b8ac2858ef5e9a4edf0437ca8.svg
91 https://homebank.kz GET /7f186997be9dd21c9d425011f5ac3c81.svg
92 https://widget-mediator.zopim.com GET /s/W/ws/47oWykpqDUI7DqLi/c/1562824022347
93 https://homeybank.com GET /app-1ef7e994c4dfc6938c24.js
94 https://homebank.kz GET /b794467121d8b33af9df2b5845355de8.woff
95 https://homebank.kz GET /c7c4e4c5970da9c4a2aefa4094f62625.woff
96 https://homebank.kz GET /f40651f07d27333e77a9b672415e784f.woff
97 https://homebank.kz GET /42f1447e766c8ef40c33e3b205b976b7.svg
98 https://homebank.kz GET /f33594359d358cfe23b117cb05f067f5.svg
99 https://homebank.kz GET /0739e02291cb0c34c34e30a52860acd0.svg
101 https://ekr.zdassets.com GET /compose/8728e841-6792-42e5-9e95-de2d18054e8f
102 https://ekr.zdassets.com GET /compose/8728e841-6792-42e5-9e95-de2d18054e8f
103 https://homebank.kz GET /19839dbf179ae310d2a9e64246db1412.svg
104 https://homebank.kz GET /362bc29fd595fbacef2c17f79d2ae791.svg
105 https://homebank.kz GET /469bd7790535d6fdb954960cab3b03b8.ttf
```

```
[HTTP_REFERER] => http://housebankkz.com/
```

SOLUTION = TRAINING

HTTP referrer checking

CASE №4

The background is a dark blue gradient with a subtle starry field. On the right side, there are several technical diagrams. One is a large circular gauge with a scale from 0 to 210 and a needle pointing to approximately 190. Another is a smaller circular diagram with concentric circles and arrows. There are also dashed lines and other faint technical symbols scattered across the background.

SOLUTION = HARDENING

APT TEAM

VS

DEFENSIVE





**Let's talk
about the
reasons**

To login click your user name



Captain Silver
6 programs running.

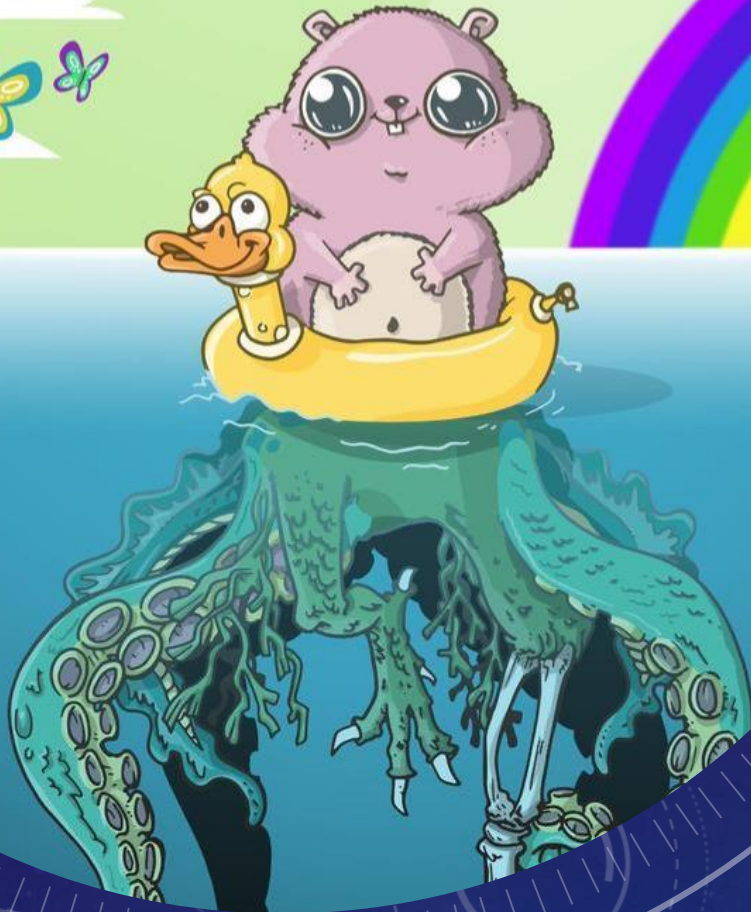
Microsoft®
Windows[®] xp
Pirated Edition

**PIRATED SOFTWARE AND
UPDATE IGNORING**

IGNORING CYBERSECURITY RULES



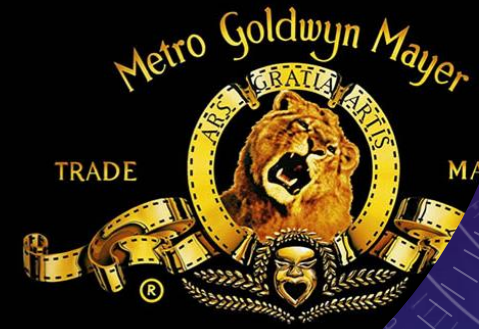
FRONT-END



BACK-END



FRONT-END



NON-SECURITY SOFTWARE
DEVELOPMENT LIFECYCLE

The background is a dark blue field filled with various white and light blue circular and semi-circular patterns. These include concentric circles, dashed lines, and arcs with tick marks, resembling a technical or scientific diagram. Some of the arcs are labeled with numbers such as 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, and 260. The overall aesthetic is clean, modern, and technical.

SHORT VIDEO

ITUEvents

ITU Regional Cybersecurity Forum for Europe and CIS

27-28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence
in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of
infocommunication infrastructure to make cities and human settlements
inclusive, safe, and resilient

POLICIES &
STRATEGIES

CERTIFICATION
FRAMEWORKS

DATA
PROTECTION

SECURITY
CHALLENGES

5G, eSIM
IoT, AI



Hosted and co-organized by:



REPUBLIC OF BULGARIA
State e-Government Agency



REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology
and Communications

