



CROWDSTRIKE

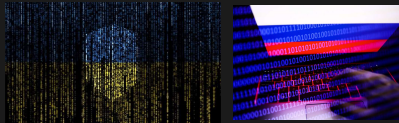


X-FILES RUSSIA UNDETECTED

- Russia's "Laboratory of Cyber Operations"
- Sandworms / Voodoo Bears Attack on UKR Critical Infrastructures
- Ukraine's defensive and counter offensive Activities
- Networking / Q&A



Ukraine - well prepared since 2008



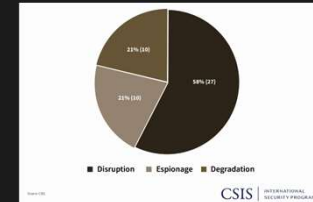
1st Cyber War

Two Countries with offensive / counter offensive measures.



Attack growth:

- 2020: 800
- 2021: 1400
- 2022: 4500
- 10 – 15 Serious Events per day



Objectives

According to CSIS in 2022
58% Disruption
21% Espionage
21% Degradation



Russia's “Laboratory of Cyber Operations”

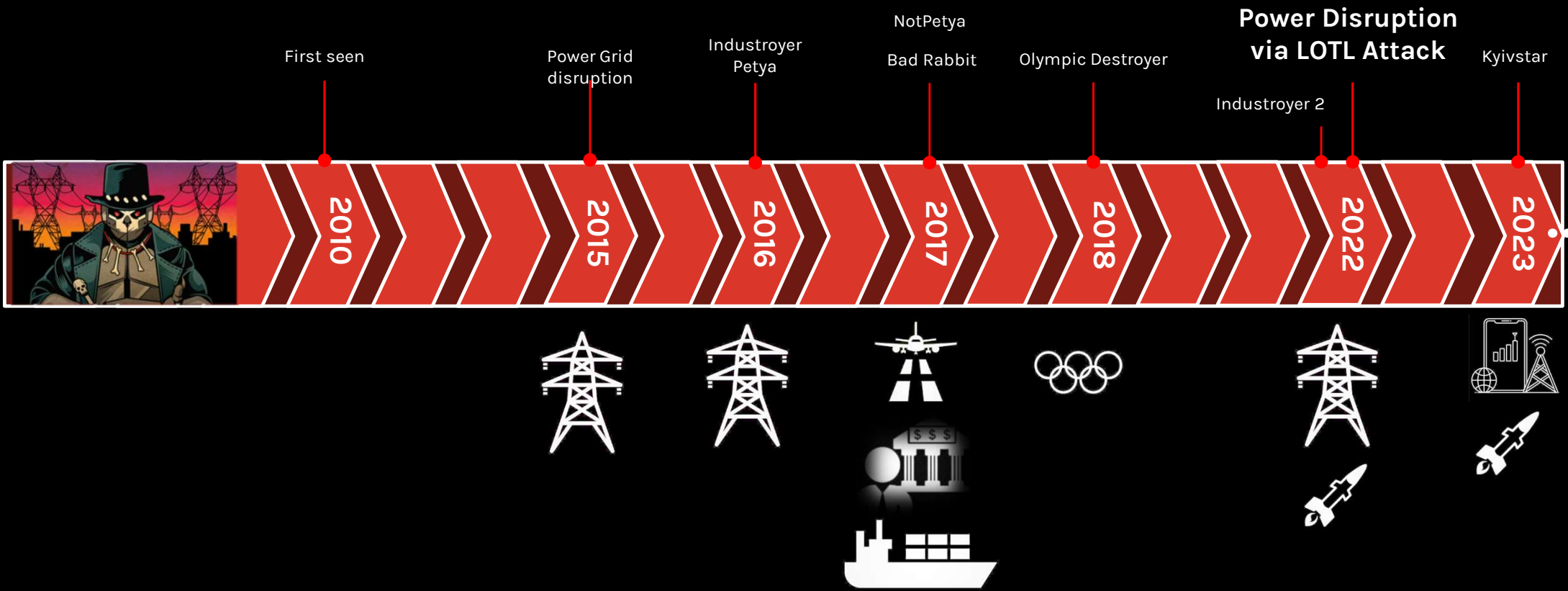
Voodoo Bear

Aka: Seashell Blizzard, Quedagh, SANDFISH, Telebots, Sandworm, ELECTRUM, FROZENBARENTS, UAC-0082, Sunglow Blizzard, Hades, Blue Echidna, BlackEnergy Group, IRON VIKING, IRIDIUM, DEV-0665

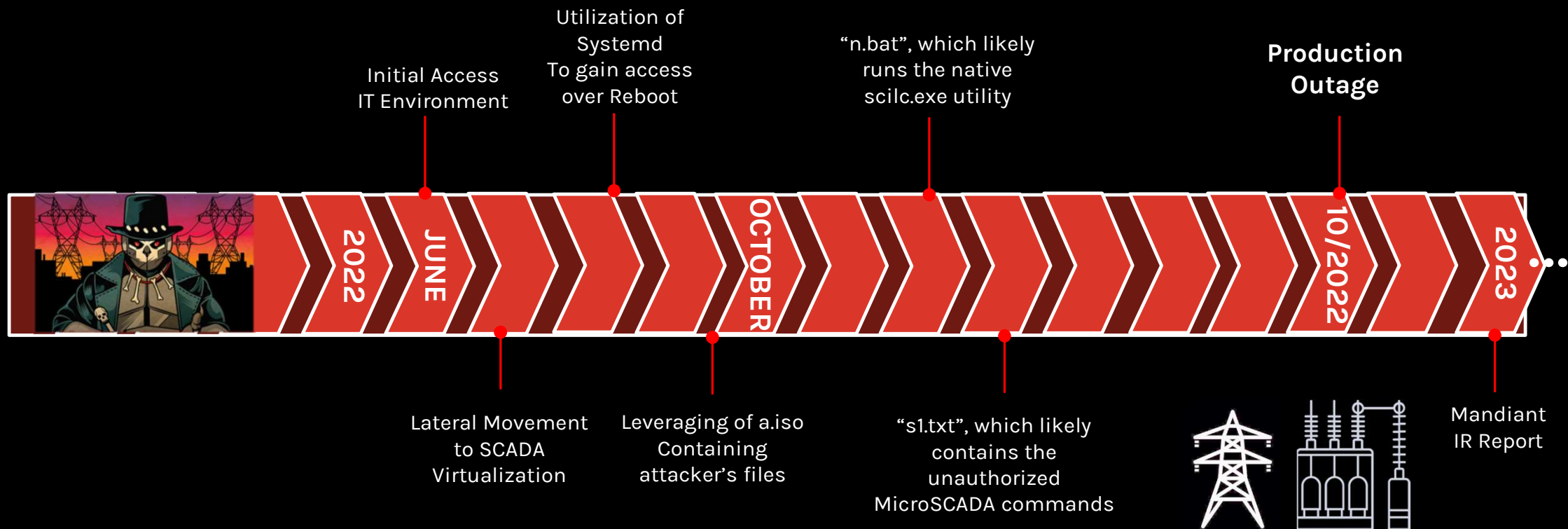
VOODOO BEAR is a Russia-based adversary assessed with high confidence to be attributable to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Главное разведывательное управление, abbreviated to ГРУ/GRU).



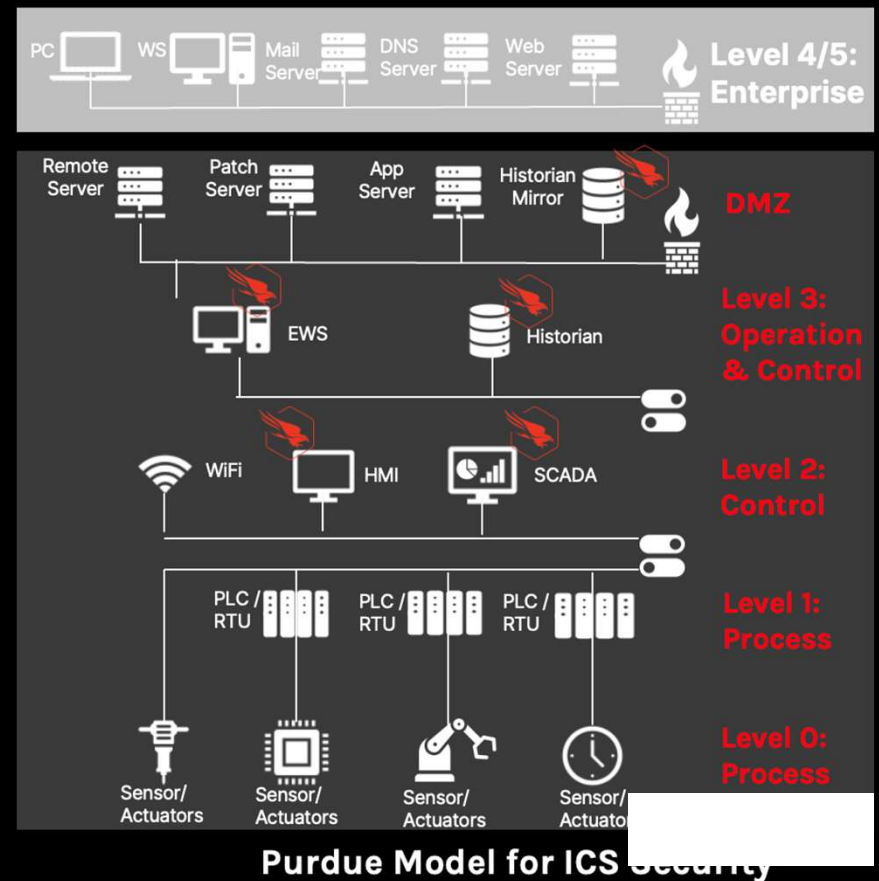
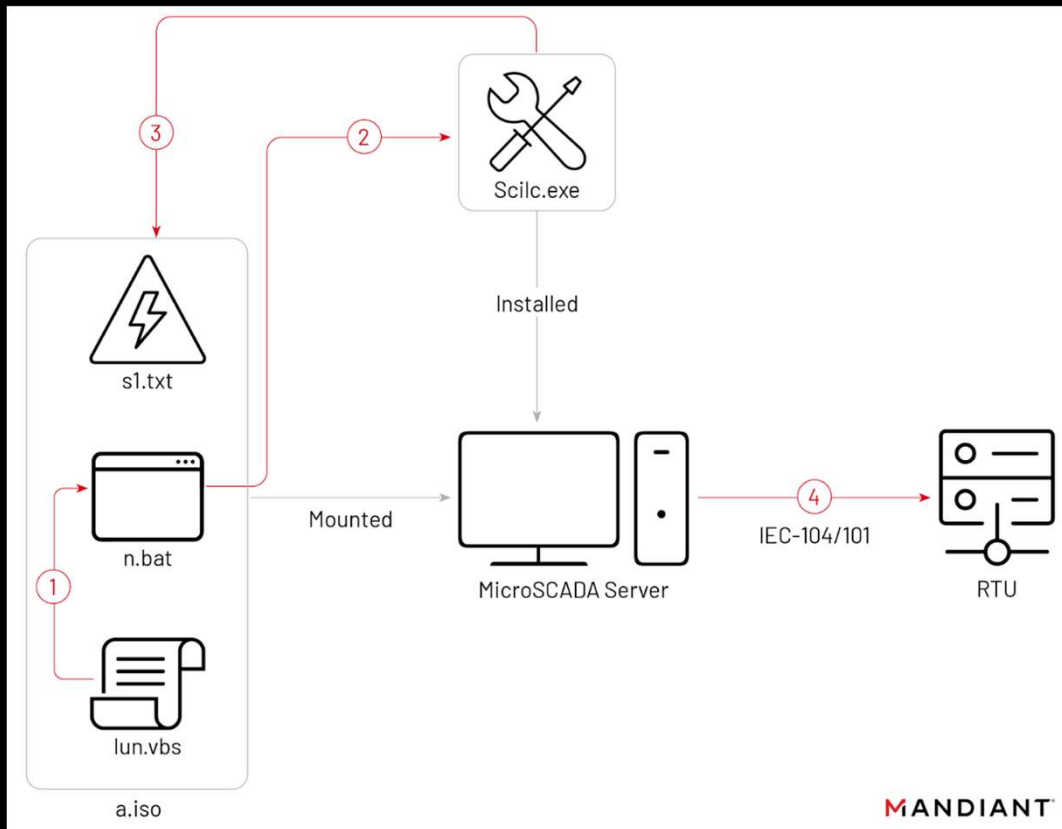
Voodoo Bear Activities



Voodoo Bear Novel Attack Against Operational Technology



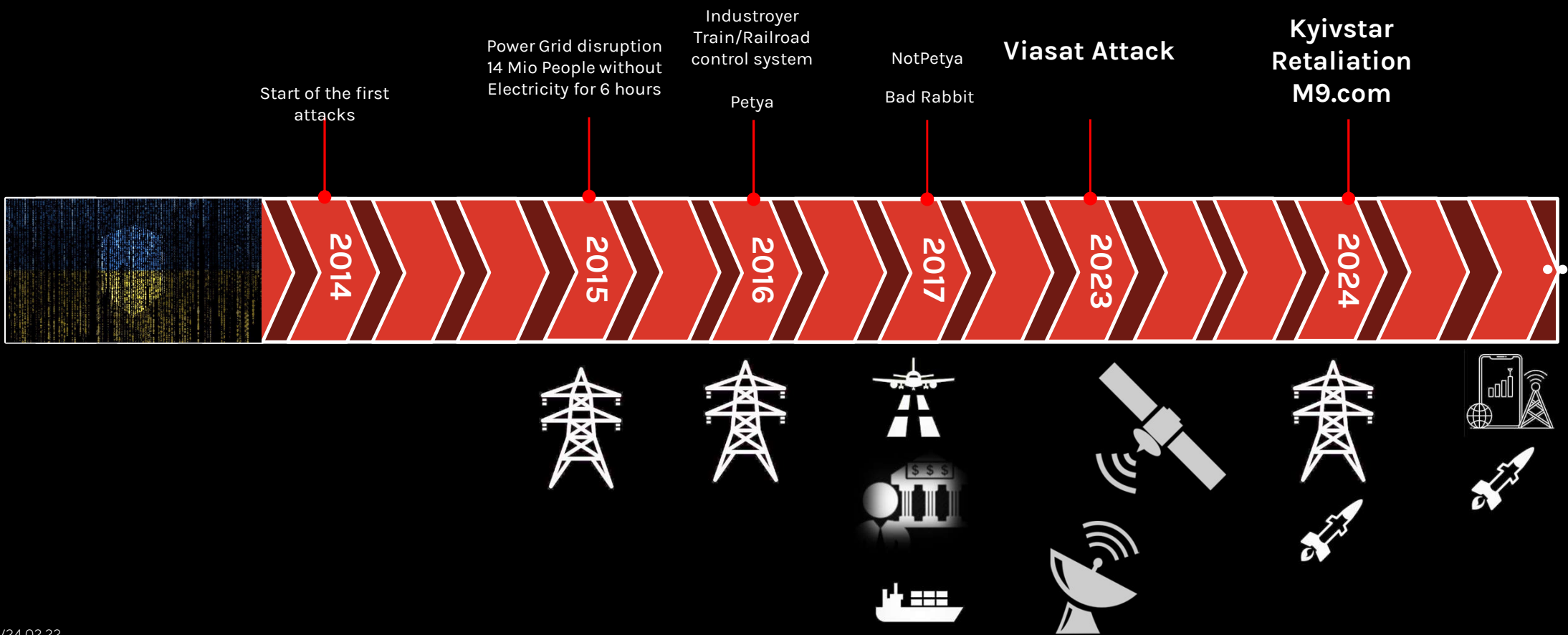
Russia - undetected





Ukraine's “(Cyber) Line Of Defense”

Ukraine's defensive and counter offensive Activities





Unpacking the Blackjack Group's Fuxnet Malware

Gaining access to Russia's 112 emergency service number.

Sharing details about and code from the Fuxnet malware used in the attack

Deleting servers, workstations and databases; 30 TB of data has been wiped, including backup drives.

Dumping passwords from multiple internal services



Hacking and bricking sensors and controllers in critical infrastructure (including airports, subways, gas-pipelines), all of which have been disabled.

Disabling network appliances such as routers and firewalls

Disabling access to the Moscollector office building (all keycards have been invalidated).

- Screenshots on "ruexfil"
- Unconfirmed screenshots of stolen data, from its attack against Moscollector



← → ↻ 🌐 ruexfil.com/mos/

MOSCOLLECTOR TAKEDOWN - 9th of April 2024

Russia's Industrial Sensor and Monitoring Infrastructure has been disabled: moscollector.ru
Hacked data is available at <https://ruexfil.com/mos>

It includes Russia's Network Operation Center (NOC) to monitor and control Gas, Water, Firealarm and many others, including a vast network of remote sensors and IoT controllers. A total of 87,000 sensors have been disabled.

Milestones:

- Initial access June 2023.
- Access to [112 Emergency Service](#).
- 87,000 [sensors](#) and controls have been disabled (including Airports, subways, gas-pipelines, ...).
- [Fuxnet](#) (stuxnet on steroids) was deployed earlier to slowly and physically destroy sensory equipment (by NAND/SSD exhaustion and introducing bad CRC into the firmware). ([YouTube Video 1](#), [YouTube Video 2](#)).
- Fuxnet has now started to flood the RS485/MBus and is sending 'random' commands to 87,000 embedded control and sensory systems (carefully excluding hospitals, airports, ...and other civilian targets).
- All servers have been deleted. All routers have been reset to factory reset. Most workstations (including the admins workstations) have been [deleted](#).
- Access to the office building has been disabled (all key-cards have been invalidated).
- Moscollector has recently been [certified by the FSB](#) for being 'secure & trusted' (picture included)
- Defaced the webpage (<https://web.archive.org/web/20240409020908/https://moscollector.ru/>)

The media pack, screenshots and videos are available here: <https://ruexfil.com/mos/takedown> ([.onion](#))



Dumps of usernames and passwords from Moscollector main datacenter servers.

SMB	192.168.	445	DC1	Moscollector.local\Cr		Ауди	
SMB	192.168.	445	DC1	Moscollector.local\Ne		Ауди	
SMB	192.168.	445	DC1	Moscollector.local\Mc		Ауди	
SMB	192.168.	445	DC1	Moscollector.local\Ku		Ауди	
SMB	192.168.	445	DC1	Moscollector.local\Kr		Ауди	
SMB	192.168.	445	DC1	Moscollector.local\Av		Веду	
SMB	192.168.	445	DC1	Moscollector.local\Iv		ір	
SMB	192.168.	445	DC1	Moscollector.local\Bl		Инже	
SMB	192.168.	445	DC1	Moscollector.local\Ag		Пере	нк
SMB	192.168.	445	DC1	Moscollector.local\Ep		Заме	рр
SMB	192.168.	445	DC1	Moscollector.local\Pa		Гене	
SMB	192.168.	445	DC1	Moscollector.local\Ta		Энер	
SMB	192.168.	445	DC1	Moscollector.local\Pa		Техн	л
SMB	192.168.	445	DC1	Moscollector.local\Iv		Инже	
SMB	192.168.	445	DC1	Moscollector.local\Be		Заме	рр
SMB	192.168.	445	DC1	Moscollector.local\Kc		Заме	рр
SMB	192.168.	445	DC1	Moscollector.local\mk			
SMB	192.168.	445	DC1	Moscollector.local\di		РЭК-	
SMB	192.168.	445	DC1	Moscollector.local\de		дежу	
SMB	192.168.	445	DC1	Moscollector.local\Gr		Наче	ни
SMB	192.168.	445	DC1	Moscollector.local\Al		Веду	
SMB	192.168.	445	DC1	Moscollector.local\Zh		Техн	л
SMB	192.168.	445	DC1	Moscollector.local\Sa		Заме	



Dumps of databases from key servers.

Schema	Name	Type	Owner	Persistence	Size	Description
public	BA_Scheme	table	smvu-production-admin-group	permanent	16 kB	Хранение информации о версии схемы, необходимо для пр
public	BL_Channel	table	smvu-production-admin-group	permanent	33 MB	[IFX] Описывают
public	CA_Apple	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Список аг
public	Data_Auto	table	smvu-production-admin-group	permanent	2792 kB	[IFX] Каналы де
public	Data_Auto	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Правила э
public	Data_Auto	table	smvu-production-admin-group	permanent	480 kB	[IFX] Правила э
public	Data_Auto	table	smvu-production-admin-group	permanent	112 kB	[IFX] Зоны авто
public	Data_Char	table	smvu-production-admin-group	permanent	1887 MB	[IFX] Журнал ди
public	Data_Char	table	smvu-production-admin-group	permanent	252 MB	[IFX] Хранит те
public	Data_Char	table	smvu-production-admin-group	permanent	47 MB	[IFX] Хранит те
public	Data_Char	table	smvu-production-admin-group	permanent	11 MB	[IFX] Таблица р
public	Data_Char	table	smvu-production-admin-group	permanent	772 MB	[IFX] Журнал из
public	Data_Char	table	smvu-production-admin-group	permanent	1417 MB	[IFX] Журнал из
public	Data_Ext	table	smvu-production-admin-group	permanent	551 GB	[IFX] Агрегат х
public	Data_Guar	table	smvu-production-admin-group	permanent	1712 kB	[IFX] Хранит те
public	Data_Hier	table	smvu-production-admin-group	permanent	74 MB	[IFX] Дерево ус
public	Data_Hier	table	smvu-production-admin-group	permanent	17 MB	[IFX] Дерево ие
public	Data_Sess	table	smvu-production-admin-group	unlogged	126 MB	[IFX] Хранение
public	Data_Setl	table	smvu-production-admin-group	permanent	1144 kB	[IFX] Хранение
public	Data_Sigs	table	smvu-production-admin-group	permanent	32 kB	[IFX] Таблица с
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Реализует
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Реализует
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Набор все
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Набор су
public	Decl_Char	table	smvu-production-admin-group	permanent	16 kB	[IFX] Типы кан
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Набор ди
public	Decl_Char	table	smvu-production-admin-group	permanent	16 kB	[IFX] Набор воз
public	Decl_Char	table	smvu-production-admin-group	permanent	8192 bytes	[IFX] Набор еди



Dumps of plaintext credentials from a Django-based web server, likely responsible for the sensor management system.

← → ↻ ruexfil.com/mos/takedown/employees_passwords_django.html


https://cts.moscollector.ru/c	login/	And		Ar
https://cts.moscollector.ru/c	login/	Bar		Be
https://cts.moscollector.ru/c	login/	Bel		Al
https://cts.moscollector.ru/c	login/	Bel		Fe
https://cts.moscollector.ru/c	login/	Bor		46
https://cts.moscollector.ru/c	login/	But		o5
https://cts.moscollector.ru/c	login/	Chu		o6
https://cts.moscollector.ru/c	login/	Eli		Ei
https://cts.moscollector.ru/c	login/	Fel		fe
https://cts.moscollector.ru/c	login/	Glu		Re
https://cts.moscollector.ru/c	login/	Gur		ge
https://cts.moscollector.ru/c	login/	Har		Ha
https://cts.moscollector.ru/c	login/	Kar		Yv
https://cts.moscollector.ru/c	login/	Kuk		ki
https://cts.moscollector.ru/c	login/	Lar		Mv
https://cts.moscollector.ru/c	login/	Leb		Le
https://cts.moscollector.ru/c	login/	Leb		~r
https://cts.moscollector.ru/c	login/	Lys		g
https://cts.moscollector.ru/c	login/	Mer		L



Identifying Equipment Targeted in the Attack

Screenshots released by the attackers indicate that the impacted sensors are manufactured by a company named AO SBK, a Russian company that manufactures a variety of sensor types, ranging from gas measurement sensors to environmental monitoring equipment.

```
$ ssh sbk@10.51.175.18
Debian GNU/Linux 10
|
SBK TMSB Debian Buster Cons
Support: https://ao-sbk.ru
```

A red arrow pointing from the right towards the URL 'https://ao-sbk.ru' in the terminal output.

Sensors:



Telemetric security system module (TMSB)



Security Data Transmission Module (SDCM)



Security sensor module (MDSB-10)



Radio wave volumetric security detector (DSSB)



Temperature and humidity sensor (TVSB)



Security system control module (SCM)



Tee tap for safety system (TSSB)



Fire and security system console (PPOSB)



Security line signal amplifier (LSSB)



Line signal amplifier - network bridge (ULSB-A)



Voice communication device for security systems (USRSB)



Gas analyzer of the security system (GASBM)



Mobile gas analyzer for security systems (GASBM-P)



Magneto-resistive security detector (MRSB)



THANK YOU

bernhard.nocker@crowdstrike.com

<https://www.linkedin.com/in/bnocker/>

