Pro-Ukraine Threat Actor 'Team OneFist' Claimed to Compromise Russian Paper Mill OT

Critical Infrastructure (CI) | Fusion (FS)

August 19, 2022 08:12:58 PM, 22-00019704, Version: 1

Executive Summary

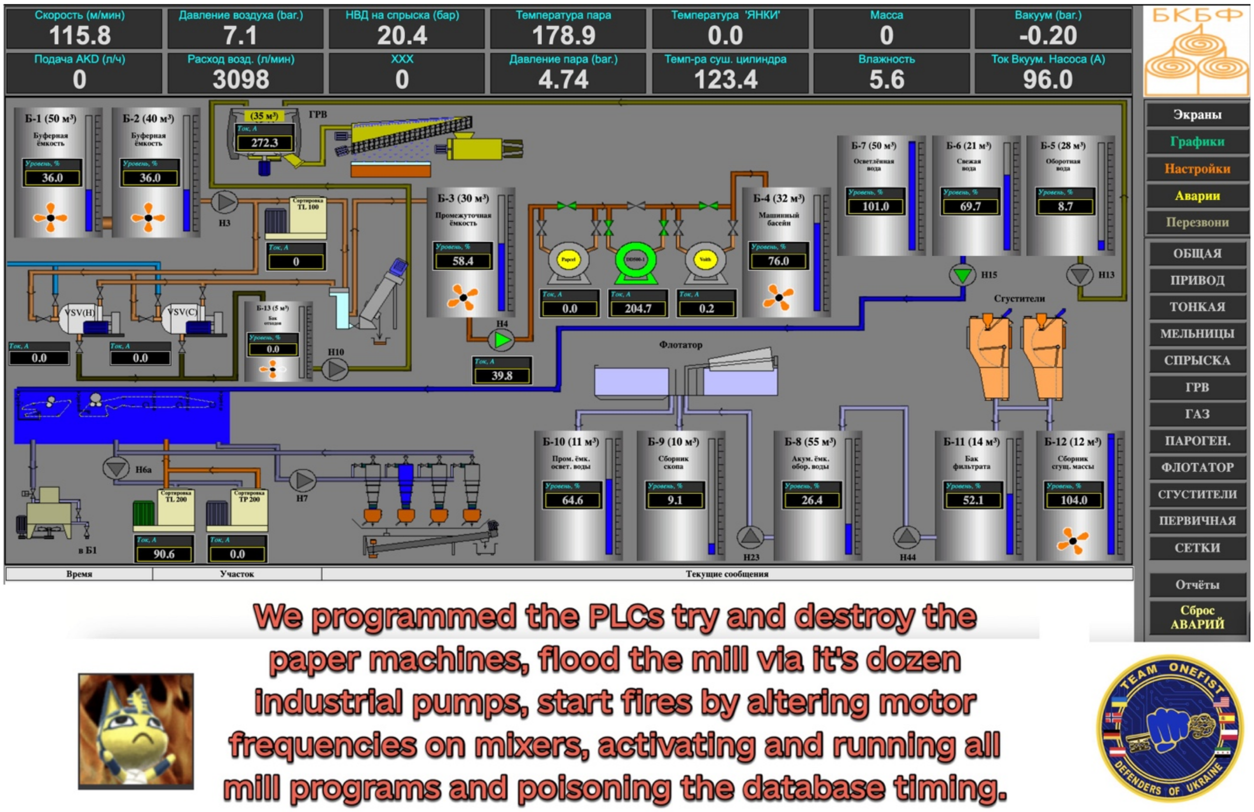
- On Aug. 16, 2022, the English-speaking actor "Voltage" from "Team OneFist" claimed to have successfully compromised operational technology (OT) assets of a Russian paper mill in an attempt to cause physical impacts.
- While Mandiant cannot fully corroborate the actor's claims, it is plausible the actor accessed internet-accessible human-machine interfaces (HMI) of a Russian paper mill and an OpenSCADA instance.
- While we doubt the actor was able to significantly impact the control processes, the incident highlights how low-sophistication threat actors can gain access to publicly accessible assets supporting OT. OT asset owners can mitigate this activity by hardening externally facing assets.

Threat Detail

On Aug. 16, 2022, the English-speaking actor "Voltage" from "Team OneFist" (aka "TeamOneFist") claimed to have successfully attacked operational technology (OT) assets of Kupros paper mill in Novosibirsk, Russia, in an attempted to cause physical impact. The actor posted the claim along with screenshots and a video on their social media. Team OneFist is a pro-Ukraine hacktivist group that appears affiliated with other hacktivist collectives targeting Russia, including "Anonymous."

- The actor dubbed the attack Operation Papyrus and stated that it was conducted in support of Ukraine during the Russia/Ukraine conflict.
- Voltage claimed to have gained root access to the mill's OT network. With that access, they reportedly locked legitimate users out of the system and altered PLC instructions in order to cause a physical impact. We doubt the actor was successful in altering PLC instructions as they did not share evidence of accessing a PLC and they have not previously shown the capability required to accomplish such an attack.
- The actor shared two screenshots and a short video showing what appears to be a human machine interface (HMI) for a paper mill (Figures 1–2).
  - The HMIs show the name and logo for another Russian paper company named бкбф (translated to BKBF in English), which is in Borovichi, Russia. It is unclear why the threat actor listed a different victim in their social media posts.
  - We are unaware of how the actor obtained the screenshots and video recording. However, it is possible that they used online discovery tools, such as Shodan or Censys, to find assets accessible to the internet to gain access to the victim network. This is a tactic we have seen other

hacktivists and cyber criminals leverage in targeting OT assets (22-00013224, 21-00011999, 20-00001205).

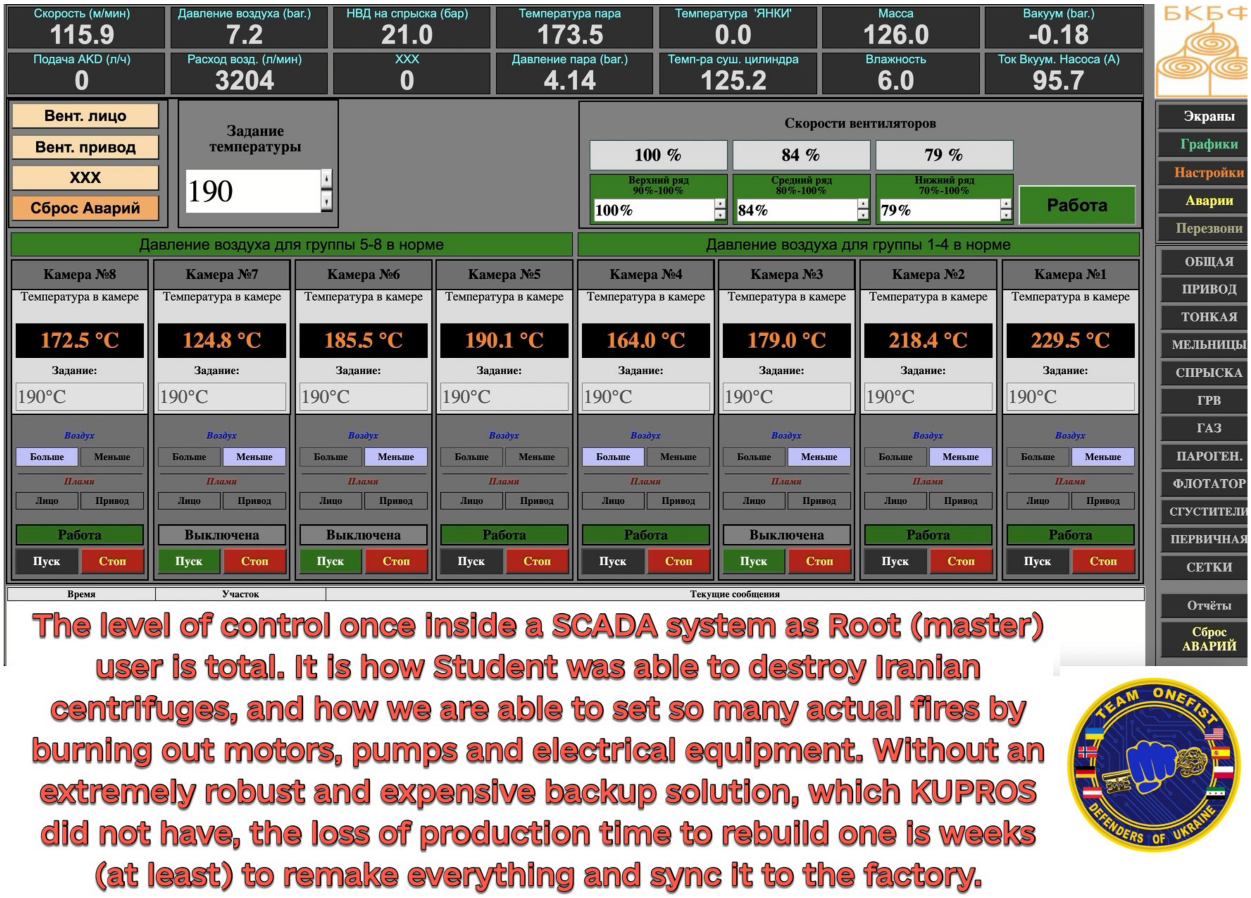


Скорость (м/мин)	Давление воздуха (bar.)	НВД на спрыска (бар)	Температура пара	Температура 'ЯНКИ'	Масса	Вакуум (bar.)
115.8	7.1	20.4	178.9	0.0	0	-0.20
Подача AKD (л/ч)	**Расход возд. (л/мин)**	**XXX**	**Давление пара (bar.)**	**Темп-ра суш. цилиндра**	**Влажность**	**Ток Вкуум. Насоса (А)**
0	3098	0	4.74	123.4	5.6	96.0

БКБФ
Б-1 (50 м³) Буферная ёмкость Уровень, % 36.0
Б-2 (40 м³) Буферная ёмкость Уровень, % 36.0
(35 м³) Ток, А 272.3
ГРВ
Н3
Сортировка TL 100
Ток, А 0
Б-3 (30 м³) Промежуточная ёмкость Уровень, % 58.4
Н4
Ток, А 39.8
Ток, А 0.0
Ток, А 204.7
Ток, А 0.2
Б-4 (32 м³) Машинный бассейн Уровень, % 76.0
Б-7 (50 м³) Осветлённая вода Уровень, % 101.0
Б-6 (21 м³) Свежая вода Уровень, % 69.7
Б-5 (28 м³) Оборотная вода Уровень, % 8.7
Н15
Н13
Сгустители
Флотатор
VSV(H)
VSV(C)
Ток, А 0.0
Ток, А 0.0
Б-13 (5 м³) Уровень, % 0.0
Н10
Н6а
Сортировка TL 200
Сортировка TP 200
Н7
Ток, А 90.6
Ток, А 0.0
в Б1
Б-10 (11 м³) Пром. ёмк. освет. воды Уровень, % 64.6
Б-9 (10 м³) Сборник скопа Уровень, % 9.1
Н23
Б-8 (55 м³) Акум. ёмк. обор. воды Уровень, % 26.4
Н44
Б-11 (14 м³) Бак фильтрата Уровень, % 52.1
Б-12 (12 м³) Сборник сгущ. массы Уровень, % 104.0
Время
Участок
Текущие сообщения
Экраны
Графики
Настройки
Аварии
Перезвони
ОБЩАЯ
ПРИВОД
ТОНКАЯ
МЕЛЬНИЦЫ
СПРЫСКА
ГРВ
ГАЗ
ПАРОГЕН.
ФЛОТАТОР
СГУСТИТЕЛИ
ПЕРВИЧНАЯ
СЕТКИ
Отчёты
Сброс АВАРИЙ
TEAM ONEFIST
DEFENDERS OF UKRAINE

We programmed the PLCs try and destroy the paper machines, flood the mill via it's dozen industrial pumps, start fires by altering motor frequencies on mixers, activating and running all mill programs and poisoning the database timing.

Figure 1: Screenshot of an HMI associated with the BKBF paper factory



Скорость (м/мин)	Давление воздуха (bar.)	НВД на спрыска (бар)	Температура пара	Температура 'ЯНКИ'	Масса	Вакуум (bar.)
115.9	7.2	21.0	173.5	0.0	126.0	-0.18
Подача AKD (л/ч)	**Расход возд. (л/мин)**	**XXX**	**Давление пара (bar.)**	**Темп-ра суш. цилиндра**	**Влажность**	**Ток Вкуум. Насоса (А)**
0	3204	0	4.14	125.2	6.0	95.7

Задание температуры: 190

Скорости вентиляторов

Верхний ряд 90%-100%	Средний ряд 80%-100%	Нижний ряд 70%-100%
100 %	84 %	79 %
100%	84%	79%

Работа

Давление воздуха для группы 5-8 в норме

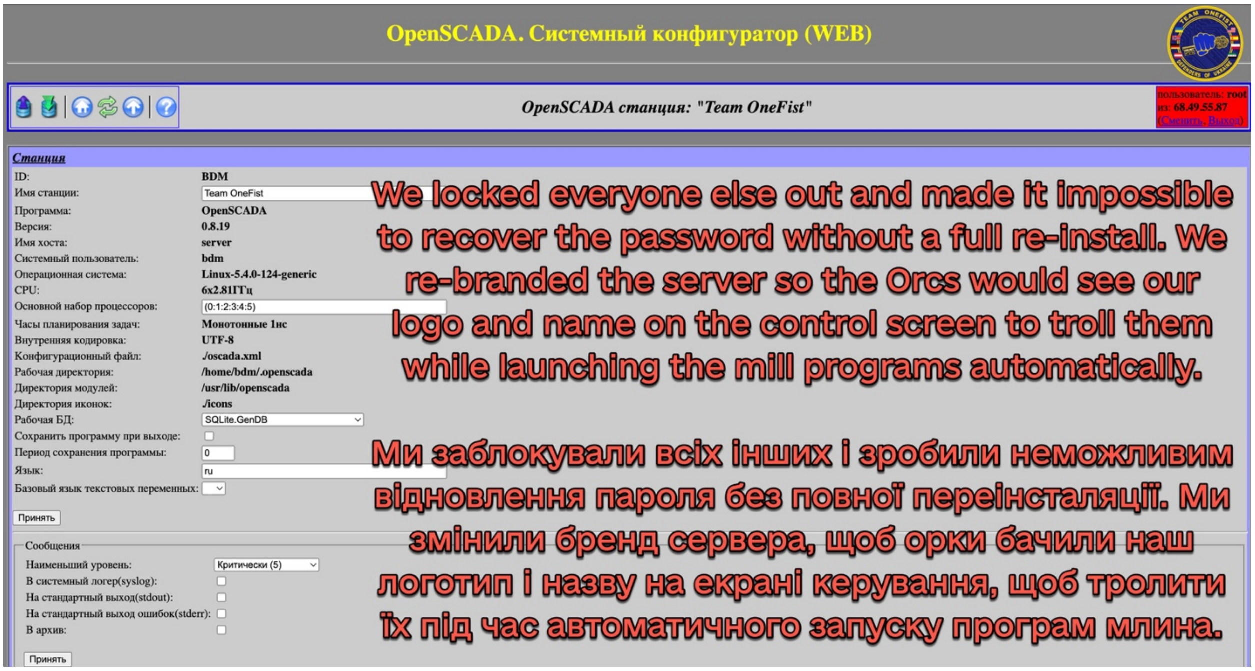
Давление воздуха для группы 1-4 в норме

	Камера №8	Камера №7	Камера №6	Камера №5	Камера №4	Камера №3	Камера №2	Камера №1
Температура в камере	172.5 °C	124.8 °C	185.5 °C	190.1 °C	164.0 °C	179.0 °C	218.4 °C	229.5 °C
Задание:	190°C	190°C	190°C	190°C	190°C	190°C	190°C	190°C
	Работа	Выключена	Выключена	Работа	Работа	Выключена	Работа	Работа

The level of control once inside a SCADA system as Root (master) user is total. It is how Student was able to destroy Iranian centrifuges, and how we are able to set so many actual fires by burning out motors, pumps and electrical equipment. Without an extremely robust and expensive backup solution, which KUPROS did not have, the loss of production time to rebuild one is weeks (at least) to remake everything and sync it to the factory.

Figure 2: Screenshot of an HMI associated with the BKBF paper factory

- The actor also shared screenshots showing OpenSCADA use and station interface (Figures 3–4). It is unclear if this system is related to either the BKBF or Kupros paper mills.
    - OpenSCADA is an open supervisory control and data acquisition (SCADA) and HMI system and is used in the manufacturing sector.
    - Two IPs can be seen in the screenshots.
        - 68[.]49[.]55[.]87 is a U.S.-based IP associated with Comcast. It is possible that the actor used this IP as an exit point in accessing their target.
        - 78[.]36[.]140[.]20 is a Russia-based IP and leads to a login page for a networking device manufactured by Eltex, a Russian manufacturer for communication devices.



OpenSCADA. Системный конфигуратор (WEB)

OpenSCADA станция: "Team OneFist"

пользователь: root
из: 68.49.55.87
(Сменить, Выход)

Станция

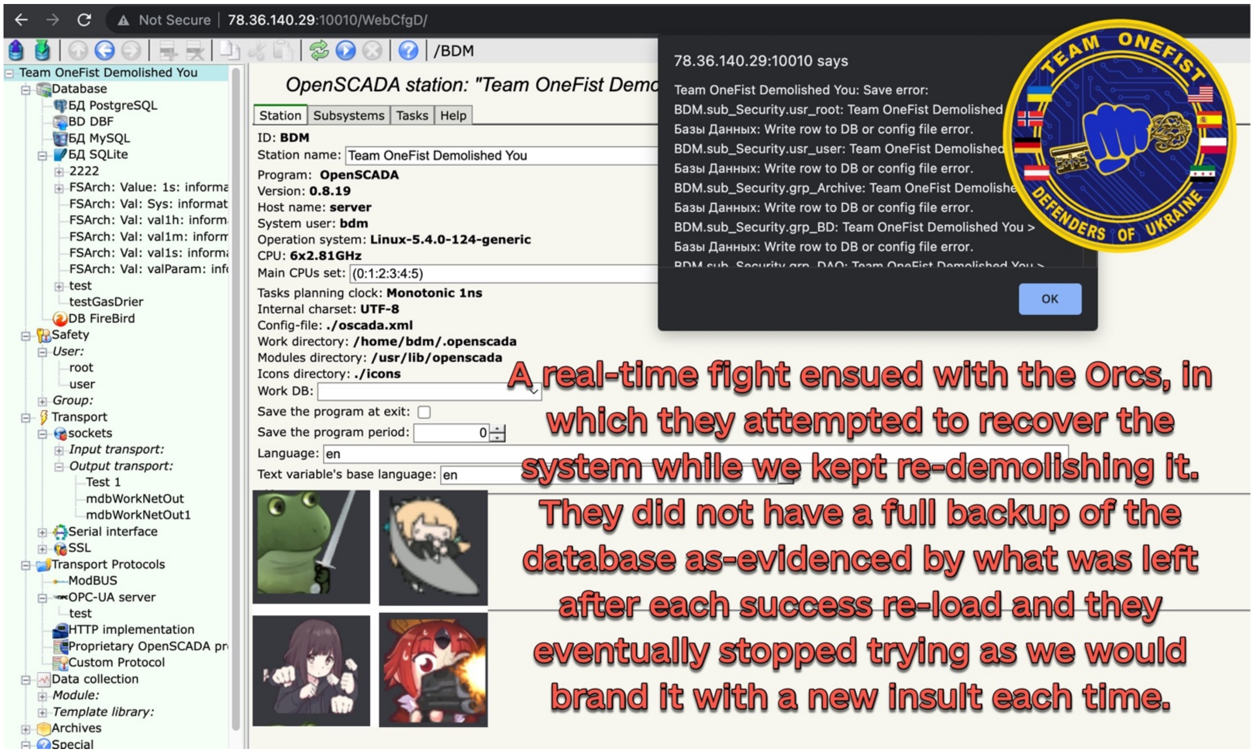
ID: BDM
Имя станции: Team OneFist
Программа: OpenSCADA
Версия: 0.8.19
Имя хоста: server
Системный пользователь: bdm
Операционная система: Linux-5.4.0-124-generic
CPU: 6x2.81ГГц
Основной набор процессоров: (0:1:2:3:4:5)
Часы планирования задач: Монотонные 1нс
Внутренняя кодировка: UTF-8
Конфигурационный файл: ./oscada.xml
Рабочая директория: /home/bdm/.openscada
Директория модулей: /usr/lib/openscada
Директория иконок: ./icons
Рабочая БД: SQLite.GenDB
Сохранить программу при выходе: □
Период сохранения программы: 0
Язык: ru
Базовый язык текстовых переменных:

Сообщения
Наименьший уровень: Критически (5)
В системный логер(syslog): □
На стандартный выход(stdout): □
На стандартный выход ошибок(stderr): □
В архив: □

We locked everyone else out and made it impossible to recover the password without a full re-install. We re-branded the server so the Orcs would see our logo and name on the control screen to troll them while launching the mill programs automatically.

Ми заблокували всіх інших і зробили неможливим відновлення пароля без повної переінсталяції. Ми змінили бренд сервера, щоб орки бачили наш логотип і назву на екрані керування, щоб тролити їх під час автоматичного запуску програм млина.

Figure 3: An OpenSCADA station interface



Not Secure | 78.36.140.29:10010/WebCfgD/

/BDM

OpenSCADA station: "Team OneFist Demo

ID: BDM
Station name: Team OneFist Demolished You
Program: OpenSCADA
Version: 0.8.19
Host name: server
System user: bdm
Operation system: Linux-5.4.0-124-generic
CPU: 6x2.81GHz
Main CPUs set: (0:1:2:3:4:5)
Tasks planning clock: Monotonic 1ns
Internal charset: UTF-8
Config-file: ./oscada.xml
Work directory: /home/bdm/.openscada
Modules directory: /usr/lib/openscada
Icons directory: ./icons
Work DB:
Save the program at exit: □
Save the program period: 0
Language: en
Text variable's base language: en

```
78.36.140.29:10010 says
Team OneFist Demolished You: Save error:
BDM.sub_Security.usr_root: Team OneFist Demolished
Базы Данных: Write row to DB or config file error.
BDM.sub_Security.usr_user: Team OneFist Demolished
Базы Данных: Write row to DB or config file error.
BDM.sub_Security.grp_Archive: Team OneFist Demolishe
Базы Данных: Write row to DB or config file error.
BDM.sub_Security.grp_BD: Team OneFist Demolished You >
Базы Данных: Write row to DB or config file error.
BDM.sub_Security.grp_DAQ: Team OneFist Demolished You >
```

A real-time fight ensued with the Orcs, in which they attempted to recover the system while we kept re-demolishing it. They did not have a full backup of the database as-evidenced by what was left after each success re-load and they eventually stopped trying as we would brand it with a new insult each time.

Figure 4: An OpenSCADA station interface

Voltage and Team OneFist Likely to Continue Targeting Internet-Accessible OT in Russia

While Mandiant cannot fully corroborate the actor's claims, it is plausible that the actor gained access to internet-accessible OT devices. We previously reported on Voltage and Team OneFist targeting these types of assets in Russia, and we expect these actors to continuing conducting this type of activity.

- In June 2022, the actor claimed to have successfully attacked and disabled a cellular network router allegedly supporting a rail system in Russia (22-00015784). The threat likely exploited a known vulnerability in the system to gain filesystem access and then executed native file deletion commands in the command line interface to impact the device.

Outlook

While the actor was unlikely able to significantly impact the control process, the incident highlights how low-sophistication threat actors could gain access to publicly accessible assets that could support OT. We expect these hacktivists to continue targeting internet-accessible OT in Russia and globally. Asset owners should harden externally facing assets, including network devices. Hardening should include vulnerability patching, implementing multi-factor authentication, and account hardening (e.g., change default credentials).

Please rate this product by taking a short four question survey

First Version Publish Date

August 19, 2022 08:12:58 PM

Threat Intelligence Tags

Actors

- TeamOneFist
  Aliases
  - TeamOneFist

Affected Industries

- Manufacturing

Intended Effects

- Interference with ICS

Motivations

- Anti-Corruption/Anti-Establishment/Information Freedom

Target Geographies

- Russia

Version Information

Version:1, August 19, 2022 08:12:58 PM

MANDIANT ADVANTAGE