TLP:CLEAR
bez ograniczeń w dystrybucji

DZIAŁANIA ROSYJSKIEJ SŁUŻBY SPECJALNEJ GRU

wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne

Maj 2025
Wersja: 1.0

Spis treści

Podsumowanie

Niniejsze wspólne ostrzeżenie (CSA[i]) ma na celu przedstawienie rosyjskiej, sponsorowanej przez państwo, kampanii wywiadowczej w cyberprzestrzeni, wymierzonej w zachodnie podmioty logistyczne oraz przedsiębiorstwa z branży technologii[ii], w szczególności wymierzonej w podmioty z sektora transportowego oraz zaangażowane w dostarczenie zagranicznego wsparcia Ukrainie. Od 2022 roku, zachodnie podmioty logistyczne oraz przedsiębiorstwa IT są zagrożone ukierunkowanymi działaniami prowadzonymi przez należące do rosyjskiego Głównego Zarządu Wywiadowczego (GRU) 85 Główne Centrum Zadań Specjalnych (85th GTsSS[iii]), o numerze jednostki wojskowej 26165 – określane w przestrzeni publicznej przez społeczność cyberbezpieczeństwa szeregiem nazw (ref. „Określenia używane przez branżę cyberbezpieczeństwa"). Ta kampania, skupiona na cyberszpiegostwie, wykorzystuje zróżnicowane, opisane poniżej techniki, taktyki oraz procedury (TTPs[iv]). Służby i agencje będące autorami przedmiotowej publikacji oceniają, że działania te będą w przyszłości kontynuowane w podobnej formie i w podobny sposób, z wykorzystaniem zbliżonych technik.

Osoby decyzyjne oraz odpowiedzialne za ochronę systemów informatycznych w podmiotach logistycznych oraz przedsiębiorstwach technologicznych powinny uwzględnić podwyższone zagrożenie ze strony JW 26165, zwiększyć monitoring sieci, proaktywnie wyszukiwać znanych TTPs oraz wskaźników kompromitacji (IOCs[v]), jak również planować ochronę systemów informatycznych z założeniem, że leżą w zakresie zainteresowania GRU.

Przedstawiona kampania cyberwywiadowcza ukierunkowana na podmioty logistyczne oraz przedsiębiorstwa technologiczne wykorzystuje zróżnicowane, wcześniej upublicznione TTPs i można ją powiązać z szerszą aktywnością JW 26165 ukierunkowaną na kamery IP na Ukrainie i w graniczących z nią krajach NATO.

Niniejsze ostrzeżenie jest autorstwa lub jest popierane przez następujące służby i agencje:

- amerykańską Agencję Bezpieczeństwa Narodowego (*United States National Security Agency - NSA*)
- amerykańskie Federalne Biuro Śledcze (*Federal Bureau of Investigation – FBI*)

- brytyjskie Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (*National Cyber Security Centre – NCSC-UK*)
- niemiecką Federalną Służbę Wywiadu (*Bundesnachrichtendienst - BND*)
- niemieckie Federalne Biuro Bezpieczeństwa Informacji (*Bundesamt für Sicherheit in der Informationstechnik – BSI*)
- niemieckie Federalne Biuro Ochrony Konstytucji (*Bundesamt für Verfassungsschutz - BfV*)
- czeski Wywiad Wojskowy (*Vojenské Zpravodajství - VZ*)
- czeską Narodową Agencję Bezpieczeństwa Cyber oraz Informacji (*Národní Úřad pro Kybernetickou a Informační Bezpečnost - NUKIB*)
- czeską Służbę Bezpieczeństwa Informacji (*Bezpečnostní Informační Služba - BIS*)
- Agencję Bezpieczeństwa Wewnętrznego (ABW)
- Służbę Kontrwywiadu Wojskowego (SKW)
- amerykańską Agencję Cyberbezpieczeństwa oraz Bezpieczeństwa Infrastruktury (*Cybersecurity and Infrastructure Security Agency - CISA*)
- amerykańskie Centrum Przestępczości Komputerowej Departamentu Obrony (*Department of Defense Cyber Crime Center – DC3*)
- amerykańskie Dowództwo Cyber (*United States Cyber Command - USCYBERCOM*)
- australijskie Centrum Bezpieczeństwa Cyberprzestrzeni Departamentu Sygnałów (*Australian Cyber Security Centre – ASD's ACSC*)
- kanadyjskie Centrum Cyberbezpieczeństwa (*Canadian Centre for Cyber Security – CCS)*
- duńską Służbę Wywiadu Wojskowego (*Forsvarets Efterretningstjeneste* – FE)
- estońską Służbę Wywiadu Zagranicznego (*Välisluureamet, VLA)*
- estońskie Narodowe Centrum Cyberbezpieczeństwa (*National Cyber Security Centre – NCSC-EE)*
- francuską Narodową Agencję Bezpieczeństwa Systemów Informatycznych (*Agence Nationale de la Sécurité des Systèmes D'information – ANSSI)*
- holenderską Służbę Wywiadu oraz Bezpieczeństwa (*Militaire Inlichtingen - en Veiligheidsdienst – MIVD)*

Wstęp

Przez ponad dwa lata, rosyjski Główny Zarząd Wywiadowczy (GRU) 85 Główne Centrum Zadań Specjalnych (85th GTsSS), o numerze jednostki wojskowej 26165 – powszechnie nazywany w sektorze cyberbezpieczeństwa m.in. jako „APT28", „Fancy Bear", „Forest Blizzard", „Blue Delta" prowadził kampanię wywiadowczą w cyberprzestrzeni wykorzystując szereg różnych TTPs, w tym odtworzoną zdolność do prowadzenia ataków typu *password spraying*[vi], *spearphishing*[vii], oraz modyfikując uprawnienia do skrzynek poczty elektronicznej Microsoft Exchange.

Pod koniec lutego 2022 roku wiele różnych sponsorowanych przez państwo rosyjskich grup zwiększyło różnorodność prowadzonych działań w cyberprzestrzeni na potrzeby szpiegostwa, niszczenia danych i systemów oraz operacji wpływu – z jednostką wojskową 26165 skupioną głównie na szpiegostwie. [1] W trakcie, gdy rosyjskie siły zbrojne ponosiły porażki i nie udawało im się spełniać postawionych im celów wojskowych, a kraje zachodnie zapewniały wsparcie broniącym się Siłom Zbrojnym Ukrainy, JW 26165 rozszerzyła swoje działania przeciwko podmiotom logistycznymi oraz przedsiębiorstwom technologicznym zaangażowanym w dostawy pomocy. JW 26165 podejmuje również próby uzyskiwania dostępu do podłączonych do sieci Internet kamer zlokalizowanych na przejściach granicznych Ukrainy, w celu monitorowania i śledzenia dostaw pomocy.

Uwaga: Ta publikacja wykorzystuje platformę MITRE ATT&CK® for Enterprise, w wersji 17. Załącznik A: zawiera tabelę aktywności JW 26165 odwzorowanej na techniki i taktyki MIRE ATT&CK. Publikacja wykorzystuje również platformę MITRE D3FEND®, w wersji 1.0.

Charakterystyka ofiar

Prowadzona przez JW 26165 GRU kampania cyberszpiegowska, ukierunkowana na zachodnie firmy z branży logistycznej oraz technologicznej, dotknęła dziesiątki podmiotów, w tym organizacje rządowe, podmioty prywatne oraz komercyjne w praktycznie wszystkich rodzajach transportu – powietrznym, morskim oraz kolejowym. JW 26165 GRU oddziaływała na następujące grupy podmiotów w krajach NATO, Ukrainie oraz podmioty międzynarodowe:

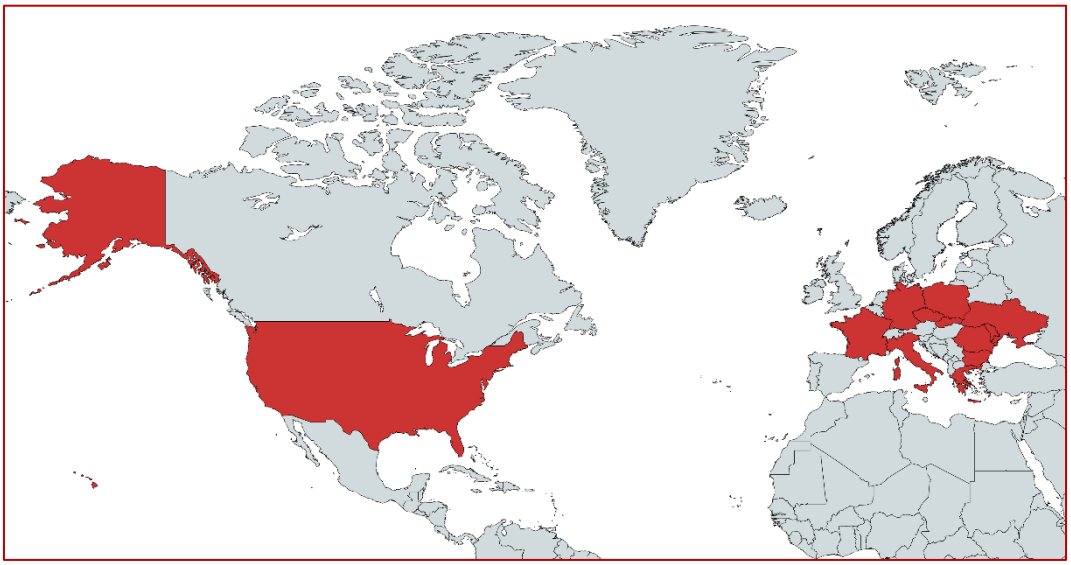
- Sektor zbrojeniowy;
- Transport oraz ośrodki i centra logistyczne (porty, lotniska itd.);
- Morskie;
- Zarządzania Ruchem Lotniczym;
- Usług IT.

W trakcie cyklu działań, JW 26165 rozpoznawała i prowadziła działania przeciwko celom głównym oraz celom powiązanym relacjami biznesowymi z celem głównym w sektorze transportowym, wykorzystując istniejące relacje zaufania i powiązania, aby uzyskać poszerzony dostęp do ich systemów [T1199].

JW 26165 prowadziła również rozpoznanie przynajmniej jednego podmiotu biorącego udział w produkcji systemów sterowania (ICS) i zarządzania liniami kolejowymi, ale nie potwierdzono jego skutecznej kompromitacji [TA0043].

Poniżej wyszczególniono państwa, w których znajdują się podmioty dotknięte działaniami GRU:

- Bułgaria
- Republika Czeska
- Francja
- Niemcy
- Grecja
- Włochy
- Mołdawia
- Polska
- Rumunia
- Słowacja
- Ukraina
- Stany Zjednoczone



Rysunek 1 - lokalizacja geograficzna ofiar działań GRU

Techniki uzyskania początkowego dostępu

Aby uzyskać początkowy dostęp do systemów leżących w zainteresowaniu JW 26165 GRU, wykorzystywała ona różne techniki, w tym (ale nie ograniczone do):

- Zgadywanie danych uwierzytelniających [T1110.001] lub ataki typu Brute force [T1110.003];
- Spearphishing ukierunkowany na uzyskanie danych uwierzytelniających [T1566];
- Spearphishing ukierunkowany na dostarczenie złośliwego oprogramowania [T1566];
- Podatność NTLM w oprogramowaniu Outlook (CVE-2023-23397);
- Podatności w oprogramowaniu Roundcube (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026);
- Eksploitacja podłączonej do sieci Internet infrastruktury, w tym korporacyjnych usług VPN [T1133] poprzez znane publicznie podatności typu SQL Injection [T1190];
- Eksploitacja podatności w oprogramowaniu WinRar (CVE-2023-38831).

JW 26165 GRU wykorzystuje również podatności w szeregu marek oraz modeli urządzeń typu SOHO[viii], aby prowadzić w sposób skryty operacje w cyberprzestrzeni, jak również przekierowywać złośliwy ruch poprzez urządzenia zlokalizowane geograficznie w pobliżu celu [T1665] [2].

Odgadywanie danych uwierzytelniających / ataki typu Brute force

Operacje JW 26165 polegające na odgadywaniu danych uwierzytelniających [T1110.001] wykazują podobną charakterystykę do tych opisanych w jednym z poprzednich CSA *„Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments“* [3]. Bazując na analizie danych sieciowych pochodzących od ofiar, obecna iteracja TTPs wykorzystuje podobną mieszankę sposobów anonimizacji, włączając w to wykorzystanie sieci Tor oraz komercyjnych usług VPN [T1090.003]. Personel JW 26165 często rotuje adresy IP, aby dodatkowo utrudnić wykrycie działań. Wszystkie zaobserwowane próby połączeń odbywały się z wykorzystaniem protokołu TLS.

Spearphishing

Wiadomości spearphishingowe wysyłane przez JW 26165 zawierały odnośniki prowadzące do fałszywych stron logowania [T1566.002] udających szereg różnych podmiotów rządowych oraz zachodnich dostawców usług chmurowych poczty elektronicznej. Te strony były zazwyczaj utrzymywane na darmowych usługach firm trzecich lub na przejętych urządzeniach SOHO i jako przynętę wykorzystywały często prawdziwe dokumenty powiązane z podobnymi podmiotami. Treść dystrybuowanych wiadomości elektronicznych była różnorodna i sięgała od tematów zawodowych po te dotyczące tematyki seksualnej. Wiadomości phishingowe były często wysyłane z przejętych lub z darmowych kont pocztowych [T1586.002, T1586.003]. Zazwyczaj były napisane w rodzimym języku i przeważnie dystrybuowane do jednego, wysoko ukierunkowanego odbiorcy.

Niektóre kampanie wykorzystywały wieloetapowe mechanizmy przekierowania [T1104] weryfikujące geolokalizację adresów IP [T1627.001] oraz charakterystykę przeglądarki [T1627], w celu ochrony infrastruktury służącej do zbierania danych uwierzytelniających lub pozwalających na przechwytywanie tokenów MFA [T1111] oraz CAPTCHA[ix] [T1056]. Połączenia, które nie były zgodne z oczekiwaną lokalizacją lub charakterystyką połączenia, przekierowywane były na niezłośliwy adres URL [T1627], taki jak msn.com. Usługi wykorzystywane do przekierowań to m.in:

- Webhook.site;
- FrgeIO;
- InfinityFree;
- Dynu;
- Mocky;
- Pipedream;
- Mockbin.org.

JW 26165 GRU wykorzystywała spearphishing również do dostarczania złośliwego oprogramowania (m.in. HEADLACE oraz MASEPIE), plików wykonywalnych [T1204.002] dostarczanych poprzez usługi firm trzecich i proxy [T1566.002] oraz skryptów w różnych językach [T1059] takich jak BAT [T1059.003], VBScript [T1059.005], jak również linków do hostowanych skrótów LNK [T1204.001].

Wykorzystanie znanych podatności

W trakcie kampanii JW 26165 GRU wykorzystywała podatność w oprogramowaniu Microsoft Outlook (CVE-2023-23397), w celu zbierania hashy NTLM[x] oraz danych uwierzytelniających poprzez specjalnie skonstruowane zaproszenie do spotkania kalendarza Microsoft Outlook [T1187] [4] [5]. Wykorzystywała również podatności w oprogramowaniu RoundCube (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026), aby wykonywać polecenia powłoki systemowej [T1059], uzyskać dostęp do kont poczty elektronicznej ofiar oraz do odczytania wrażliwych danych z serwerów poczty elektronicznej.

Od co najmniej jesieni 2023, JW 26165 GRU wykorzystuje podatność w oprogramowaniu WinRAR (CVE-2023-38831) pozwalającą na wykonanie dowolnego kodu osadzonego w archiwum, aby uzyskać początkowy dostęp [T1659]. W tym celu JW 26165 GRU wysyłała wiadomości email zawierające złośliwe załączniki [T1566.001] oraz wiadomości zawierające pliki z odnośnikami (linkami) [T1566.002], których odwiedzenie powodowało pobranie złośliwego archiwum zawierającego wskazaną powyżej podatność.

TTPs wykorzystywane po uzyskaniu dostępu

Po uzyskaniu początkowego dostępu z wykorzystaniem jednej ze wspomnianych powyżej technik, personel JW 26165 wykonywał rozpoznanie środowiska w poszukiwaniu danych kontaktowych dodatkowych celi zajmujących kluczowe stanowiska [T1589.002].

Personel JW 26165 wykorzystywał natywne komendy powłoki systemu operacyjnego oraz otwartoźródłowe narzędzia, takie jak Impacket oraz PsExec, aby poszerzać posiadany dostęp w środowisku [TA0008]. W zależności od środowiska ofiary, wykorzystywane były skrypty Impacket w postaci plików wykonywalnych lub skryptów w języku Python. Do poruszania się po środowisku i uzyskiwania dostępu do dalszych systemów wykorzystywany był również protokół RDP [T1021.001] oraz podejmowane były próby skopiowania z kontrolerów domeny Active Directory pliku bazy danych NTDS.dit [T1003.003] z wykorzystaniem natywnych komend Active Directory Domain Services, takich jak:

```
C:\Windows\system32\ntdsutil.exe “active inctance ntds” ifm “create full C:\temp\[a-z]{3}”
quit quit
```

Dodatkowo personel JW 26165 GRU wykorzystywał narzędzia Certipy oraz ADExplorer.exe, do pozyskiwania informacji z kontrolerów domeny Active Directory. Aby umożliwić wykonanie Certipy, na przejętych urządzeniach instalowany był interpreter języka Python [T1059.006]. Przed eksfiltracją pozyskane pliki były pakowane w archiwa .zip [T1560], a następnie przesyłane poprzez uprzednio umieszczony w systemie program OpenSSH [T1048].

W trakcie obsługi jednego z incydentów wykryto, że personel JW 26165 podejmował próby zlokalizowania oraz eksfiltrowania list użytkowników Office 365 oraz podejmował korki mające na celu zapewnienie możliwości długotrwałego, ciągłego pozyskiwania wiadomości poczty elektronicznej. W tym celu manipulował uprawnieniami skrzynek poczty elektronicznej [T1098.002], aby umożliwić długotrwałe pozyskiwanie wiadomości email ze skompromitowanych podmiotów logistycznych, co zostało opisane w artykule DKWOC [6].

Po początkowym uwierzytelnieniu, personel JW 26165 GRU modyfikował uprawnienia dostępowe do folderów kont pocztowych oraz dodawał skompromitowane urządzenia do kontrolowanych przez siebie mechanizmów uwierzytelniania wieloskładnikowego, w celu zwiększenia poziomu zaufania do logowań, ukrycia kompromitacji kont oraz docelowo zapewnienia sobie długotrwałego, skrytego dostępu [T1556.006]. Dodatkowo wykorzystywał skrypty w języku Python, celem uzyskania hasła w postaci jawnej poprzez Group Policy Preferences z wykorzystaniem skryptu Get-GPPPassword.py oraz z użyciem zmodyfikowanego skryptu ldap-dump.py, żeby rozpoznać środowiska MS Windows i przeprowadzać ataki typu *brute force* oraz *password spraying* poprzez protokół LDAP[xi]. Dodatkowo, aby zatrzeć ślady, usuwał zdarzenia z logu zdarzeń z użyciem narzędzia wevtutil [T1070.001].

Po uzyskaniu początkowego dostępu do sieci, personel JW 26165 GRU usiłował uzyskać dostęp do kont z dostępem do wrażliwych informacji dotyczących transportu, takich jak harmonogramy przejazdów kolejowych oraz manifesty transportowe. Konta, na których zależało GRU, zawierały informacje związane z transportem pomocy Ukrainie, takie jak:

- Nadawca;
- Odbiorca;
- Numery pociągów, samolotów oraz statków;
- Lokalizacje początkowe transportów;
- Lokalizacje docelowe transportów;
- Numery rejestracyjne kontenerów;
- Trasy transportów;
- Transportowana zawartość.

Przynajmniej w jednym przypadku JW 26165 GRU podjęła próbę użycia phishingu głosowego [T1566.004] udając personel działu IT, celem uzyskania dostępu do uprzywilejowanych kont.

Złośliwe oprogramowanie

JW 26165 wykorzystywała w opisywanej kampanii różne złośliwe oprogramowanie, od mającego na celu zapewnienie początkowego dostępu, przez zapewnienie persystencji[xii], po eksfiltrację danych. W niektórych przypadkach przebieg ataku obejmował wiele różnych kolejno uruchamianych narzędzi. Wykorzystywano technikę „przejęcia kolejności wyszukiwania plików DLL[xiii]“ [T1574.001], aby uruchomić złośliwe oprogramowanie. Szereg narzędzi stosowanych w opisywanej kampanii przeciwko podmiotom z sektora logistyki jest publicznie znanych, w tym:

- HEADLACE [7]
- MASEPIE [8]

Użycie narzędzi, takich jak OCEANMAP oraz STEELHOOK [8] przeciwko podmiotom z sektora logistyki nie zostało zaobserwowane, natomiast ich użycie przeciwko podmiotom z innych sektorów lub w innych krajach sugeruje, że jeżeli zajdzie taka potrzeba operacyjna, mogą zostać wykorzystane przeciwko podmiotom z sektorów logistyki oraz IT na Ukrainie.

Przetrwanie w systemie

Poza wspomnianą wcześniej modyfikacją uprawnień kont pocztowych, aby zapewnić przetrwanie w systemie i długoterminowy dostęp, personel JW 26165 wykorzystywał

harmonogram zadań[xiv] [T1053.005] klucze Run[xv] rejestru systemowego [T1547.001] oraz umieszczanie złośliwych skrótów [1547.009] w folderach startowych[xvi].

Eksfiltracja

JW 26165 GRU wykorzystywała szereg różnych metod eksfiltracji danych dopasowanych do systemu informatycznego ofiary, wykorzystujących zarówno złośliwe oprogramowanie, jak również tzw. *Living of the land binaries*[xvii]. Aby przygotować dane do eksfiltracji, często wykorzystywano komendy powłoki PowerShell [T1059.001] – na przykład pakowano w archiwum zip pliki planowane do przesłania na kontrolowaną przez GRU infrastrukturę.

Personel JW 26165 GRU wykorzystywał również protokoły używane przez serwery do wymiany danych oraz API, takie jak Exchange Web Servics (EWS[xviii]) i IMAP[xix] [T1114.002] do eksfiltracji danych z serwerów pocztowych. W wielu przypadkach używał okresowego wykonywania zapytań EWS [T1119], celem pozyskiwania nowo wysyłanych oraz odebranych wiadomości email [T1029] (tzn. wiadomości, które pojawiły się na serwerze od czasu ostatniego pobrania przez GRU). Zazwyczaj wykorzystywał infrastrukturę zlokalizowaną geograficznie w pobliżu ofiary. W celu zapewnienia długookresowego, skrytego i niezauważonego pozyskiwania danych wrażliwych, wykorzystywano długie okresy uśpienia pomiędzy kolejnymi eksfiltracjami danych, używano zaufanych, prawdziwych protokołów komunikacyjnych oraz lokalną infrastrukturę.

Powiązania z działaniami ukierunkowanymi na kamery IP

Poza działaniami ukierunkowanymi na podmioty logistyczne, JW 26165 GRU prawdopodobnie wykorzystywała dostęp do kamer IP należących do podmiotów i osób prywatnych, umieszczonych w kluczowych lokalizacjach, takich jak przejścia graniczne, obiekty wojskowe oraz stacje kolejowe celem śledzenia transportów na Ukrainę. Wykorzystywała również w podobnym celu dostęp do usług miejskich, takich jak kamery pozwalające na sprawdzanie korków na drogach.

Od co najmniej marca 2022, JW 26165 GRU prowadziła wielkoskalową kampanię mającą na celu rozpoznawanie [T1592] oraz uzyskiwanie dostępu do strumieni danych zawierających obraz [T1125] z serwerów protokołu Real Time Streaming Protocol

(RTSP) działających na kamerach IP, zlokalizowanych głównie na Ukrainie. Kontrolowane przez JW 26165 GRU serwery wysyłały żądania RTSP DESCRIBE do serwerów RTSP, w większości znajdujących się na kamerach IP [T1090.002]. Żądania DESCRIBE były konstruowane w taki sposób, aby uzyskać dostęp do kamer IP znajdujących się w logicznie oddzielonych sieciach od tych, w których działał router odbierający żądanie. Żądania zawierały zakodowane w Base64 dane uwierzytelniające do serwerów RTSP, wykorzystujące m.in. publicznie udokumentowane domyślne hasła i loginy, jak również ogólne dane uwierzytelniające, w celu przeprowadzenia ataku brute force na urządzenie [T1110].

Poniżej przedstawiony jest przykład takiego żądania RTSP:

```
DESCRIBE rtsp://[Adres IP] RTSP/1.0
Cseq: 1
Authorization: Basic <Dane uwierzytelniające zakodowane w base64>
User-Agent: WebClient
Accept: application/sdp

DESCRIBE rtsp://[adres IP] RTSP/1.0
CSeq: 2
Authorization: Digest username="admin", realm="[a-f0-9]{12}", algorithm="MD5", nonce="[a-f0-
9]{32}", uri="", response=" [a-f0-9]{32}"
User-Agent: WebClient
Accept: application/sdp
```

Zakończona sukcesem odpowiedź RTSP 200 OK zawierała klatkę obrazu rejestrowanego przez kamerę IP oraz metadane kamery IP, takie jak kodek wideo, rozdzielczość oraz inne dodatkowe właściwości zależne od modelu i jej konfiguracji.

Z dostępnej służbom i agencjom, wydającym tę publikację, próby ponad 10 000 kamer, które były celami tej kampanii, dystrybucja geograficzna ofiar wskazuje silne ukierunkowanie na kamery zlokalizowane na Ukrainie oraz w krajach ościennych:

Kraj	Procentowy udział w całości prób
Ukraina	81,0%
Rumunia	9,9%
Polska	4,0%
Węgry	2,8%
Słowacja	1,7%
Inne	0,6%

Działania zapobiegawcze

Ogólne rekomendacje bezpieczeństwa

Architektura i konfiguracja

- Należy stosować właściwą segmentację sieci [D3-NI], ograniczenia dostępu oraz wykorzystywać dodatkowe atrybuty (takie jak informacje o urządzeniu, środowisku, ścieżce dostępu) przy przyznawaniu uprawnień [D3-AMED], docelowo dążąc do wprowadzenia modelu Zero Trust.
    - Przy projektowaniu nowych systemów informatycznych należy rozważyć zastosowanie zasad Zero Trust. Dobór produktów powinien uwzględniać to, w jaki sposób mogą rozwiązać zidentyfikowane ryzyka [9].
- Należy zaimplementować reguły zapory sieciowej blokujące połączenia z urządzeń w sieci innych niż uwierzytelnione urządzenia administracyjne i serwery, aby zapobiec możliwości poruszania się po systemie [D3-ITF].
- Należy wykorzystywać automatyczne narzędzia do audytu logów dostępowych, celem wykrycia potencjalnych naruszeń bezpieczeństwa oraz zidentyfikowania nietypowych żądań dostępu [D3-RAPA].
- W przypadku organizacji wykorzystujących uwierzytelnienie on-prem i serwery poczty elektronicznej on-prem, żądania NTLM/SMB skierowane do zewnętrznej infrastruktury powinny być zablokowane [D3-OTF].
- Organizacje powinny wdrożyć rozwiązania EDR/zbierania logów/inne rozwiązania cyberbezpieczeństwa przynajmniej w systemach przetwarzających

duże ilości wrażliwych danych, takie jak serwery pocztowe oraz kontrolery domeny [D3-PM].
    - Należy przeprowadzić modelowanie zagrożeń, aby zrozumieć w jaki sposób wrażliwe systemy mogą zostać skompromitowane, uwzględniając specyfikę środowiska oraz wdrożone mechanizmy bezpieczeństwa.
- Należy zbierać oraz monitorować logi systemu Windows w poszukiwaniu wybranych zdarzeń, w szczególności tych mogących sugerować, że log systemowy został usunięty [D3-SFA].
- Należy włączyć dodatkowe mechanizmy bezpieczeństwa w systemie Windows, w celu zabezpieczenia urządzenia końcowego i zapobieganiu popularnym technikom uzyskiwania początkowego dostępu [D3-AH]:
    - Należy włączyć „attack surface reduction rules“[xx], aby zapobiec możliwości uruchomienia plików wykonywalnych pochodzących z załączników wiadomości email [D3-ABPI];
    - Należy włączyć „attack surface reduction rules“, aby zapobiec możliwości uruchomienia plików wykonywalnych zlokalizowanych w zapisywalnych katalogach, takich jak Pobrane oraz %APPDATA% [D3-EAL];
    - Jeżeli użytkownik systemu nie ma potrzeby wytwarzania skryptów, należy ograniczyć możliwość uruchomienia plików takich jak batch[xxi], JavaScript oraz PowerShell [10] do znanych, zaufanych skryptów [D3-EI];
    - Należy wyłączyć funkcjonalność Windows Host Scripting oraz skonfigurować powłokę PowerShell do uruchamiania w trybie Constrained [D3-ACH].
- Jeżeli jest to możliwe, należy stosować listy dopuszczeń dla aplikacji i skryptów, aby ograniczyć możliwość wykonania wyłącznie do tych niezbędnych do pracy, blokując wszystkie inne [D3-EAL].
- Otwartoźródłowe reguły detekcji SIGMA mogą być wykorzystywane do stworzenia podstawowej detekcji i ostrzegania o wykonaniu podejrzanych plików lub o przekazaniu podejrzanych argumentów [D3-PSA].

- W przypadku dostawców usług poczty elektronicznej zawierających mechanizm automatycznego sprawdzania odnośników oraz detonacji załączników, zaobserwowano znaczące ograniczenie ilości skutecznych ataków typu spearphishing. Organizacje oraz użytkownicy końcowi powinni korzystać z usług zapewniających dodatkowe mechanizmy bezpieczeństwa [D3-URA].
- Większość podmiotów i organizacji nie ma potrzeby dopuszczania przychodzącego ruchu, w szczególności logowania z usług VPN [D3-NAM]. Logowania z publicznych sieci VPN, włączając w to węzły wyjściowe zlokalizowane w tym samym kraju co docelowy system, powinny być blokowane, o ile jest to możliwe lub jeżeli muszą zostać dopuszczone, powinny generować ostrzeżenia i podlegać sprawdzeniu.
- Użytkownicy powinni być przeszkoleni, aby wykorzystywać wyłącznie dopuszczone systemy firmowe do celów związanych z kwestiami rządowymi i wojskowymi oraz powinni unikać używania prywatnych kont poczty elektronicznej do spraw służbowych. Administratorzy systemów powinni audytować zarówno korespondencję elektroniczną, jak i próby logowań do takich usług, w celu wykrywania nieprawidłowej aktywności.

Większość organizacji nie potrzebuje zezwalać na wychodzące połączenia do usług hostingowych oraz służących do testowania i symulowania działania usług API, które są często wykorzystywane przez JW 26165 GRU. Poniżej wymienione usługi powinny być zablokowane, a wyjątki powinny być dopuszczone tylko wtedy, gdy pojawi się realna potrzeba [D3-DNSDL]:

- *.000.pe
- *.1cooldns.com
- *.42web.io
- *.4cloud.click
- *.accesscan.org
- *.bumbleshrimp.com
- *.camdvr.org
- *.casacam.net
- *.ddnsfree.com
- *.ddnsgeek.com
- *.ddnsguru.com
- *.dynuddns.com
- *.dynuddns.net
- *.free.nf
- *.freeddns.org
- *.frge.io
- *.glize.com
- *.great-site.net

- *.infinityfreeapp.com
- *.kesug.com
- *.loseyourip.com
- *.lovestoblog.com
- *.mockbin.io
- *.mockbin.org
- *.mocky.io
- *.mybiolink.io
- *.mysynology.net
- *.mywire.org
- *.ngrok.io
- *.ooguy.com
- *.pipedream.net
- *.rf.gd
- *.urlbae.com
- *.webhook.site
- *.webhookapp.com
- *.webredirect.org
- *.wuaze.com

Mechanizmy heurystycznej detekcji żądań do nowych subdomen, włączając w to subdomeny powyżej wymienionych dostawców, mogą pozwolić na odkrycie prób phishingu [D3-DNRA]. Logowanie zapytań do każdej subdomeny żądanej przez użytkowników, na przykład poprzez logowanie DNS lub logi zapory sieciowej, mogą pozwolić administratorom systemu na zidentyfikowanie nowych ofiar i celów phishingu.

Zarządzanie dostępem i tożsamością

Organizacje powinny przedsięwziąć kroki, w celu zapewnienia rygorystycznej kontroli dostępu i uchronienia się przed popularnymi technikami kradzieży danych uwierzytelniających:

- Należy wykorzystywać mechanizm uwierzytelnienia wieloskładnikowego (MFA) z silnymi składnikami uwierzytelnienia oraz regularnie wymagać ponownego uwierzytelnienia [D3-MFA] [11] [12]. Silne składniki uwierzytelnienia to takie, których nie można zgadnąć wykorzystując metody słownikowe, więc wymagają znacznie większej ilości prób, aby przełamać je atakiem typu brute force.
- Należy wdrożyć inne mechanizmy zabezpieczenia uprzywilejowanych kont, takie jak ograniczenie ilości kont administracyjnych, wymaganie sprzętowych składników uwierzytelnienia wieloskładnikowego, regularne audyty wszystkich uprzywilejowanych uprawnień przyznanych kontom [D3-JFAPA].
- Należy rozdzielić uprzywilejowane konta zgodnie z rolami oraz zgłaszać ostrzeżenia w przypadku potencjalnego nadużycia uprawnień [D3-UAP]. Na

przykład, konta administracyjne poczty elektronicznej powinny być inne i rozdzielone od kont administracyjnych usługi Active Directory.

- Należy ograniczyć poleganie na hasłach i rozważyć wykorzystanie usług takich jak single sign-on [D3-TBA].
    - Organizacje wykorzystujące mechanizmy uwierzytelnienia oraz pocztę elektroniczną on-premises powinny podjąć kroki w celu całkowitego wyłączenia uwierzytelnienia opartego o NTLM i przejście na bezpieczniejsze mechanizmy, takie jak PKI.
- Nie należy przechowywać haseł w Group Policy Preferences (GPP). Należy usunąć wszystkie hasła znajdujące się w GPP i zmienić wszystkie hasła na kontach odpowiadających hasłom w GPP [D3-CH] [13].
- Należy użyć spowalniania lub czasowego blokowania możliwości logowania [D3-ANET]:
    - Spowalnianie jest preferowane w porównaniu do blokowania. Spowalnianie powinno stopniowo zwiększać odstęp czasowy pomiędzy kolejnymi próbami logowania.
    - Czasowe blokowanie kont może sprawić, że użytkownicy utracą dostęp do swoich kont oraz mogą wymagać odzyskania kont.
    - Wprowadzenie czasowego blokowania kont może pozwolić atakującemu na łatwe wykonanie ataku odmowy usługi (DoS).
    - Jeżeli używane jest czasowe blokowanie możliwości logowania, rekomendowana jest karencja pomiędzy 5, a 10 prób.
- Należy wykorzystywać usługi pozwalające na porównywanie haseł, z hasłami które znajdują się w wyciekach [D3-SPP]. Na przykład „Have I Been Pwned” pozwala na sprawdzenie czy hasło zostało skompromitowane bez przesyłania samego hasła.
- Wszystkie domyślne dane uwierzytelniające [D3-CRO] powinny zostać zmienione. Należy wyłączyć i zablokować wszystkie protokoły wykorzystujące słabe mechanizmy uwierzytelnienia (np. przesłanie hasła otwartym tekstem, przestarzałe lub podane protokoły uwierzytelniania i algorytmy kryptograficzne) lub nie pozwalające na powiązanie ich z mechanizmami MFA [D3-ACH][D3-ET]. Zawsze należy konfigurować mechanizmy kontroli dostępu w taki sposób, aby

zapewnić, że tylko aktywne i poprawnie zabezpieczone i uwierzytelnione konta mogą uzyskać dostęp [13].

Zabezpieczenie kamer IP

Poniżej zamieszczono techniki zabezpieczania kamer IP, które mogą być stosowane, aby chronić je przed opisywaną aktywnością:

- Należy wykorzystywać wyłącznie urządzenia posiadające wsparcie producenta. Modele pozbawione wsparcia powinny zostać wymienione.
- Należy wprowadzać aktualizacje bezpieczeństwa oraz aktualizacje oprogramowania sprzętowego [D3-SU].
- Jeżeli nie jest konieczny, należy zablokować zdalny dostęp do kamery IP [D3-ITF].
- Jeżeli jest to możliwe, należy zapewnić, że dostęp do kamery IP jest chroniony urządzeniem bezpieczeństwa [D3-NAM].
- Jeżeli zdalny dostęp do strumienia obrazu jest wymagany, należy zapewnić, że uwierzytelnienie jest włączone [D3-AA], a dostęp wymaga połączenia przez usługę VPN [D3-ET]. Jeżeli jest to możliwe, należy stosować uwierzytelnienie wieloskładnikowe (MFA) [D3-MFA].
- Należy wyłączyć protokoły i usługi Universal Plug and Play (UPnP), Peer-to-Peer (P2P) oraz anonimowego dostępu na kamerach IP oraz routerach.
- Należy wyłączyć nieużywane porty i usługi (FTP, interfejs web itp) [D3-ACH].
- Jeżeli urządzenie posiada taką możliwość, należy ograniczyć dostęp do RTSP wyłącznie do uwierzytelnionych połączeń [D3-AA].
- Należy audytować wszystkie próby zdalnego uwierzytelnienia, aby mieć pewność, że są prawidłowe i oczekiwane [D3-UBA]. Należy wyjaśniać wszystkie nietypowe bądź niespodziewane próby zalogowania.
- Należy audytować konta użytkowników kamer IP, aby mieć pewność, że odzwierciedlają organizację i są wykorzystywane zgodnie z oczekiwaniami.
- Jeżeli jest to możliwe, należy konfigurować, dostrajać i monitorować logowanie zdarzeń na kamerach IP.

Wskaźniki kompromitacji (IoC)

Uwaga: Niektóre elementy infrastruktury podane jako IoC mogą już nie być kontrolowane przez GRU; mogły należeć do strony trzeciej i zostać przejęte przez GRU; mogą też być współdzielone przez wielu użytkowników, jak np. publiczne wyjścia komercyjnych usług VPN, bądź węzły wyjściowe sieci Tor. Przy tworzeniu reguł detekcji lub analizie logów, należy podchodzić do nich z ostrożnością. Jest praktycznie pewne, że JW 26165 GRU wykorzystuje rozległą infrastrukturę operacyjną oraz TTPs nie ujęte w tej publikacji.

Narzędzia i skrypty

Niezłośliwe narzędzia

Nieautoryzowane lub nietypowe użycie wymienionych poniżej narzędzi może być wskaźnikiem potencjalnej kompromitacji:

- ntdsutil – narzędzie wbudowane w system Windows, wykorzystywane do eksportowania zawartości Active Directory;
- wevtutil – narzędzie wbudowane w system Windows wykorzystywane do usuwania dzienników zdarzeń;
- vssadmin – narzędzie wbudowane w system Windows, które może być wykorzystane do wykonywania kopii dysku systemowego C: serwera;
- ADexplorer – narzędzie autorstwa firmy Microsoft, służące do przeglądania, edycji oraz wykonywania kopii zapasowej usługi Active Directory Certificate Services;
- OpenSSH – otwartoźródłowy klient SSH skompilowany na systemy rodziny Windows;
- schtasks – narzędzie wbudowane w system Windows, wykorzystywane do zapewnienia przetrwania w systemie poprzez mechanizm harmonogramu zadań;
- whoami – narzędzie wbudowane w system Windows, służące do odczytania informacji o użytkowniku;
- tasklist – narzędzie wbudowane w system Windows, służące do odczytania listy aktywnych procesów;

- hostname – narzędzie wbudowane w system Windows, służące do odczytania nazwy urządzenia;
- arp – narzędzie wbudowane w system Windows, służące do odczytania tablicy ARP, używane do rozpoznawania i tworzenia mapy sieci;
- systeminfo – narzędzie wbudowane w system Windows, służące do odczytania obszernych informacji o systemie operacyjnym oraz urządzeniu;
- net – narzędzie wbudowane w system Windows, służące do odczytania szczegółowych informacji o użytkowniku;
- wmic – narzędzie wbudowane w system Windows, służące do interakcji z Windows Management Instrumentation (WMI), używane do odczytywania informacji o systemie, takich jak litery przypisane do partycji logicznych na dyskach;
- cacls – narzędzie wbudowane w system Windows, służące do modyfikowania uprawnień plików;
- icacls - narzędzie wbudowane w system Windows, służące do modyfikowania uprawnień plików;
- ssh – narzędzie wbudowane w system Windows, służące do nawiązywania połączeń protokołem SSH;
- reg – narzędzie wbudowane w system Windows, służące do modyfikowania rejestru systemowego.

Uwaga: Do efektywnego wyszukiwania złośliwego wykorzystania narzędzi lub innych technik *living-off-the-land* potrzebne są dodatkowe heurystyki lub reguły. W przypadku, gdy narzędzia te są wykorzystywane w normalnej pracy, przy detekcji opartej o samo uruchomienie programu, ilość błędów typu *false-positive*[xxii] może być znacząca. Jako punkt odniesienia do stworzenia wszechstronnej, opartej o wiele składników strategii wykrywania zagrożeń można wykorzystać poradnik *Identyfing and Mitigating Living Off the Land Techniques*.

Złośliwe skrypty

- Certipy – otwartoźródłowy skrypt w języku Python, służący do rekonesansu i nadużywania Active Directory Certificate Services;

- Get-GPPPassword.py – otwartoźródłowy skrypt w języku Python, służący do szukania niezabezpieczonych haseł przechowywanych w Group Policy Preferences;
- ldap-dump.py – skrypt służący do zbierania informacji o kontach użytkowników oraz innych informacji przechowywanych w Active Directory;
- Skrypty zawierające ciąg znaków do logowania do kamer Hikvision: „YWRtaW46MTEK”.

Nietypowe argumenty linii komend

Pomimo, że wskazane poniżej narzędzia nie są złośliwe, a wskazane argumenty linii komend mogą być wykorzystane w normalnej pracy, w przedstawionym kontekście są często wykorzystywane do złośliwej aktywności i mogą posłużyć jako wskaźnik kompromitacji:

- edge.exe „-headless-new -disable-gpu”;
- ntdsutil.exe “activate instance ntds” ifm “create full C:\temp\bcp” quit quit;
- ssh -Nf;
- schtasks /create /xml.

IoC wskazujące na eksploitację podatności aplikacji MS Outlook

- md-shoeb@alfathdoor.com.sa
- jayam@wizzsolutions.com
- accounts@regencyservice.in
- m.salim@tsc-me.com
- vikram.anand@4ginfosource.in
- mdelafuente@ukwwfze.com
- sarah@cosmicgold469.co.za
- franch1.lanka@bplanka.com
- commercial@vanadrink.com
- maint@goldenloaduae.com
- karina@bhpcapital.com
- tv@coastalareabank.com
- ashoke.kumar@hbclife.in

- 213.32.252.221
- 124.168.91.178
- 194.126.178.8
- 159.196.128.120

Najczęściej wykorzystywani dostawcy usług poczty elektronicznej

- portugalmail.pt
- mail-online.dk
- email.cz
- seznam.cz

Nazwy archiwów wykorzystywanych do eksploitacji CVE-2023-38831

- calc.war.zip
- news_week_6.zip
- Roadmap.zip
- SEDE-PV-2023-10-09-1_EN.zip
- War.zip
- Zeyilname.zip

Adresy IP wykorzystywane do ataków Brute force

Uwaga: Wskazane adresy IP były wykorzystywane w okresie od czerwca do września 2024 roku. Autorzy ostrzeżenia rekomendują zweryfikowanie wskazanych adresów przed wdrożeniem lub podjęciem działań takich jak blokowanie:

Czerwiec 2024	Lipiec 2024	Sierpień 2024		
192.162.174.94	207.244.71.84	31.135.199.145	79.184.25.198	91.149.253.204
103.97.203.29	162.210.194.2	31.42.4.138	79.185.5.142	91.149.254.75
209.14.71.127		46.112.70.252	83.10.46.174	91.149.255.122
109.95.151.207		46.248.185.236	83.168.66.145	91.149.255.19
		64.176.67.117	83.168.78.27	91.149.255.195
		64.176.69.196	83.168.78.31	91.221.88.76
		64.176.70.18	83.168.78.55	93.105.185.139
		64.176.70.238	83.23.130.49	95.215.76.209
		64.176.71.201	83.29.138.115	138.199.59.43
		70.34.242.220	89.64.70.69	147.135.209.245
		70.34.243.226	90.156.4.204	178.235.191.182
		70.34.244.100	91.149.202.215	178.37.97.243
		70.34.245.215	91.149.203.73	185.234.235.69

		70.34.252.168	91.149.219.158	192.162.174.67
		70.34.252.186	91.149.219.23	194.187.180.20
		70.34.252.222	91.149.223.130	212.127.78.170
		70.34.253.13	91.149.253.118	213.134.184.167
		70.34.253.247	91.149.253.198	
		70.34.254.245	91.149.253.20	

Reguły detekcji

Zmodyfikowany skrypt do przechwytywania hashy NTLM

```
rule APT28_NTLM_LISTENER {
        meta:
                description = "Detects NTLM listeners including APT28's custom one"
        strings:
                $command_1 = "start-process powershell.exe -WindowStyle hidden"
                $command_2 = "New-Object System.Net.HttpListener"
                $command_3 = "Prefixes.Add('http://localhost:8080/')"
                $command_4 = "-match 'Authorization'"
                $command_5 = "GetValues('Authorization')"
                $command_6 = "Request.RemoteEndPoint.Address.IPAddressToString"
                $command_7 = "@(0x4e,0x54,0x4c,0x4d,
0x53,0x53,0x50,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x28,0x00,0x00,
0x01,0x82,0x00,0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,0x88,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00)"
                $command_8 = ".AllKeys"

                $variable_1 = "$NTLMAuthentication" nocase
                $variable_2 = "$NTLMType2" nocase
                $variable_3 = "$listener" nocase
                $variable_4 = "$hostip" nocase
                $variable_5 = "$request" nocase
                $variable_6 = "$ntlmt2" nocase
                $variable_7 = "$NTLMType2Response" nocase
                $variable_8 = "$buffer" nocase

        condition:
                5 of ($command_*)
                or
                all of ($variable_*)
}
```

Plik LNK HEADLACE

```
rule APT28_HEADLACE_SHORTCUT {
        meta:
                description = "Detects the HEADLACE backdoor shortcut dropper. Rule is meant
for threat hunting."

        strings:
                $type = "[InternetShortcut]" ascii nocase
                $url  = "file://"
                $edge = "msedge.exe"
                $icon = "IconFile"

        condition:
                all of them
}
```

Okno dialogowe HEADLACE używane do pozyskiwania danych uwierzytelniających

```
rule APT28_HEADLACE_CREDENTIALDIALOG {
        meta:
                description = "Detects scripts used by APT28 to lure user into entering
credentials"

        strings:
                $command_1 = "while($true)"
                $command_2 = "Get-Credential $(whoami)"
                $command_3 = "Add-Content"
                $command_4 = ".UserName"
                $command_5 = ".GetNetworkCredential().Password"
                $command_6 = "GetNetworkCredential().Password.Length -ne 0"

        condition:
                5 of them
}
```

Główny skrypt HEADLACE

```
rule APT28_HEADLACE_CORE {
        meta:
                description = "Detects HEADLACE core batch scripts"

        strings:
                $chcp = "chcp 65001" ascii
                $headless = "start \"\" msedge --headless=new --disable-gpu" ascii

                $command_1 = "taskkill /im msedge.exe /f" ascii
                $command_2 = "whoami>\"%programdata%" ascii
                $command_3 = "timeout" ascii
                $command_4 = "copy \"%programdata%\\" ascii

                $non_generic_del_1 = "del /q /f \"%programdata%" ascii
                $non_generic_del_3 = "del /q /f \"%userprofile%\\Downloads\\" ascii

                $generic_del = "del /q /f" ascii

        condition:
                (
                        $chcp
                        and
                        $headless
                )
                and
                (
                        1 of ($non_generic_del_*)
                        or
                        ($generic_del)
                        or
                        3 of ($command_*)
                )
}
```

MASEPIE

```
rule APT28_MASEPIE {
        meta:
                description = "Detects MASEPIE python script"

        strings:
                $masepie_unique_1 = "os.popen('whoami').read()"
                $masepie_unique_2 = "elif message == 'check'"
                $masepie_unique_3 = "elif message == 'send file':"
                $masepie_unique_4 = "elif message == 'get_file'"
                $masepie_unique_5 = "enc_mes('ok'"
                $masepie_unique_6 = "Bad command!'.encode('ascii'"
                $masepie_unique_7 = "{user}{SEPARATOR}{k}"
                $masepie_unique_8 = "raise Exception(\"Reconnect"

        condition:
                3 of ($masepie_unique_*)
}
```

STEELHOOK

```
rule APT_28_STEELHOOK {
        meta:
               description = "Detects APT28's STEELHOOK powershell script"

        strings:
               $s_1 = "$($env:LOCALAPPDATA\\\\Google\\\\Chrome\\\\User Data\\\\Local State)"
               $s_2 = "$($env:LOCALAPPDATA\\\\Google\\\\Chrome\\\\User
Data\\\\Default\\\\LoginData)"

               $s_3 = "$($env:LOCALAPPDATA\\\\Microsoft\\\\Edge\\\\User Data\\\\Local
State)"
               $s_4 = "$($env:LOCALAPPDATA\\\\Microsoft\\\\Edge\\\\User
Data\\\\Default\\\\Login Data)"

               $s_5 = "os_crypt.encrypted_key"
               $s_6 = "System.Security.Cryptography.DataProtectionScope"
               $s_7 = "[system.security.cryptography.protectdata]::Unprotect"
               $s_8 = "Invoke-RestMethod"

        condition:
                all of them
}
```

PSEXEC

```
rule GENERIC_PSEXEC {
        meta:
                description = "Detecs SysInternals PSEXEC executable"

        strings:
                $sysinternals_1 = "SYSINTERNALS SOFTWARE LICENCE TERMS"
                $sysinternals_2 = "/accepteula"
                $sysinternals_3 = "Software\\Sysinternals"

                $network_1 = "\\\\%s\\IPC$"
                $network_2 = "\\\\%s\\ADMIN$\\%s"
                $network_3 = "\\Device\\LanmanRedirector\\%s\\ipc$"

                $psexec_1 = "PSEXESVC"
                $psexec_2 = "PSEXEC-{}-"
                $psexec_3 = "Copying %s to %s..."
                $psexec_4 = "gPSINFSVC"

        condition:
                (
                        ( uint16( 0x0 ) == 0x5a4d )
                        and
                        ( uint16( uint32( 0x3c ) ) == 0x4550 )
                )
                and
                        filesize < 1024KB
                and
                (
                        ( any of ( $sysinternals_* ) and any of ( $psexec_* ) )
                        or
                        ( 2 of ( $network_* ) and 2 of ( $psexec_* ) )
                )
}
```

Nazwy używane przez branżę cyberbezpieczeństwa

Branża cyberbezpieczeństwa dostarcza informacje CTI[xxiii], IOCs oraz rekomendacje bezpieczeństwa związane z działaniami JW 26165 GRU. Jakkolwiek nie jest to pełny zbiór, to powiązane nazwy można znaleźć w MITRE ATT&CK G0007, a najczęściej używane w branży to:

- APT28;
- Fancy Bear;
- Forest Blizzard;
- Blue Delta.

Uwaga: Przedsiębiorstwa i organizacje mają różne metody śledzenia grup oraz atrybucji działań w cyberprzestrzeni, opisywane w sektorze prywatnym zbiory

aktywności mogą nie pokrywać się całkowicie z rozpoznaniem SKW, ani innych agencji i służb biorących udział w wydaniu tej publikacji.

Inne odniesienia

Aby przeszukać środowisko pocztowe pod kątem wiadomości email spreparowanych pod kątem podatności CVE-2023-23397, osoby odpowiedzialne za ochronę sieci mogą wykorzystać skrypt opublikowany przez Microsoft: https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/.

Aby wykryć narzędzia pakietu Impacket, osoby odpowiedzialne za ochronę sieci mogą wykorzystać publicznie dostępną regułę YARA: https://github.com/Neo23x0/signature-base/blob/master/yara/gen_impacket_tools.yar.

Cytowane prace

[1] Microsoft. Defending Ukraine: Early Lessons from the Cyber War. 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

[2] FBI et al. Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations. 2024. https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF

[3] NSA et al. Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. 2021. https://media.defense.gov/2021/jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

[4] ANNSI. Campagnes d'attaques du mode opératoire APT28 depuis 2021. 2023. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

[5] ANSSI. Targeting and compromise of French entities using the APT28 intrusion set. 2025. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf

[6] DKWOC. DKWOC zaobserwowało szkodliwą aktywność przeciwko serwerom pocztowym Microsoft Exchange. 2023. https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/wykrywanie-atakow-na-serwery-pocztowe-microsoft-exchange/

[7] IBM. Isreal-Hamas Conflict Lures to Deliver Headlace Malware. 2023. https://www.ibm.com/think/x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deliver-headlace-malware

[8] CERT-UA. APT28: From Initial Attack to Creating Domain Controller Threats in an Hour. 2023. https://cert.gov.ua/article/6276894

[9] NSA. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf

[10] NSA et all. Keeping Powershell: Security Measures to Use and Embrace. 2022. https://media.defense.gov/2022/jun/22/2003021689/-1/-1/1/csi_keeping_powershell_security_measures_to_use_and_embrace_20220622.pdf

[11] National Institute of Standards and Technology (NIST). Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf

[12] NSA. Selecting Secure Multi-factor Authentication Solutions. 2020. https://media.defense.gov/2024/Jul/31/2003515137/-1/-1/0/MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

[13] NSA and CISA. NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

[14] Department of Justice. Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU). 2024. https://www.justice.gov/archives/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

[15] Recorded Future. GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns. 2024. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf

Cel publikacji

Ten dokument został utworzony w ramach realizacji statutowych zadań służb i agencji będących jego autorami, włączając w to: identyfikowanie oraz informowanie o zagrożeniach, opracowywanie i rozpowszechnianie rekomendacji oraz wskazówek cyberbezpieczeństwa. Zawarte w nim informacje mogą być przekazywane bez ograniczeń do wszystkich zainteresowanych podmiotów.

Punkty kontaktowe

Dla podmiotów amerykańskich (United States organisations):

- **National Security Agency (NSA):**
  Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
  Defence Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
  Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
- **Cybersecurity and Infrastructure Security Agency (CISA)**
  All U.S. organisations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or 1-844-Say-CISA. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organisation; and a designated point of contact.
- Department of Defense Cyber Crime Center (DC3)
  Defense Industrial Base Inquiries and Cybersecurity Services: DC3.DCISE@us.af.mil
  Media Inquiries / Press Desk: DC3.Information@us.af.mil

Dla podmiotów brytyjskich (United Kingdom organisations):

- Report significant cyber security incidents to http://ncsc.gov.uk/report-an-incident (monitored 24/7).

Dla podmiotów niemieckich (Germany organisations):

- Bundesnachrichtendienst (BND): Media Relations / Press Desk: + 49 30 20 45 36 30, pressestelle@bnd.bund.de
- BfV Prevention/Economic Protection Unit: +49 30 18792-3322, wirtschaftsschutz@bfv.bund.de
- BSI Service-Center: +49 800 274 1000, service-center@bsi.bund.de

Dla podmiotów czeskich (Czech Republic organisations):

- Security Information Service (BIS): cyber.threats@bis.cz
- National Cyber and Information Security Agency (NUKIB): cert.incident@nukib.gov.cz

Dla podmiotów polskich (Polish organisations):

- Służba Kontrwywiadu Wojskowego (SKW): cyber.int@skw.gov.pl

Dla podmiotów australijskich (Australian organisations):

- Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Dla podmiotów kanadyjskich (Canadian organisations):

- Report incidents by emailing CCCS at contact@cyber.gc.ca

Dla podmiotów estońskich (Estonian organisations):

- Estonian Foreign Intelligence Service (EFIS): info@valisluureamet.ee
- Estonian National Cyber Security Centre (NCSC-EE): ria@ria.ee

Dla podmiotów francuskich (French organizations):

- French organizations are encouraged to report suspicious activity or incydent related to information found in this advisory by contacting ANSSI/CERT-FR by email at cert-fr@ssi.gouv.fr or by phone at: 3218 or +33 970 83 32 18

Załącznik A: techniki i taktyki MITRE ATT&CK

Poniższe tabele przedstawiają zbiorczo wszystkie techniki i taktyki używane przez JW26165 wymienione w publikacji.

Rekonesans

Nazwa taktyki/techniki	ID	Użycie
Reconnaissance	TA0043	Rozpoznawanie co najmniej jednego podmiotu zaangażowanego w produkcję urządzeń ICS do sterowania trakcjami kolejowymi.
Gather Victim Identity Information: Email Addresses	T1589.002	Rozpoznawanie informacji kontaktowych w celu zidentyfikowania dodatkowych celów pełniących kluczowe funkcjach.
Gather Victim Org Information	T1591	Rozpoznawanie osób z działu cyberbezpieczeństwa podmiotu-ofiary.
Gather Victim Org Information: Identify Roles	T1591.004	Rozpoznawanie osób odpowiedzialnych za koordynację transportów.
Gather Victim Org Information: Business Relationships	T1591.002	Rozpoznawanie firm współpracujących z podmiotem-ofiarą.
Gather Victim Host Information	T1592	Wyszukiwanie serwerów Real Time Streaming Protocol (RTSP) działających na kamerach IP.

Budowa zdolności (infrastruktury)

Nazwa taktyki/techniki	ID	Użycie
Compromise Accounts: Email Accounts	T1586.002	Wiadomości phishingowe wysyłane przy użyciu przejętych kont poczty elektronicznej.
Compromise Accounts: Cloud Accounts	T1586.003	Wiadomości phishingowe wysyłane przy użyciu przejętych kont poczty elektronicznej.

Uzyskanie początkowego dostępu

Nazwa taktyki/techniki	ID	Użycie
Trusted Relationship	T1199	Wykorzystanie w celu uzyskania dostępu istniejących relacji zaufania i powiązań biznesowych pomiędzy podmiotami z sektora transportowego, a głównym celem.
Phishing	T1566	Wykorzystanie spearphishingu w celu uzyskania danych uwierzytelniających i dostarczenia złośliwego oprogramowania, aby uzyskać początkowy dostęp do systemu.
Phishing: Spearphinhing Attachment	T1566.001	Wykorzystanie wiadomości email zawierających złośliwy załącznik.
Phishing: Spearphishing Link	T1566.002	Wykorzystanie spearphishingu z linkami do fałszywych stron logowania. Wykorzystanie wiadomości e-mail z osadzonymi linkami, które prowadziły do złośliwego archiwum.
Phishing: Spearphishing Voice	T1566.004	Próba użycia phisingu głosowego, poprzez podszycie się pod personel IT, do uzyskania dostępu do uprzywilejowanych kont.
External Remote Services	T1133	Eksploitacja dostępnej z sieci internet infrastruktury IT, takiej jak urządzenia VPN, do uzyskania początkowego dostępu do systemu.
Exploit Public-Facing Application	T1190	Eksploitacja publicznie znanych podatności oraz SQL Injection do uzyskania początkowego dostępu do systemu.
Content Injection	T1659	Wykorzystanie podatności w oprogramowaniu WinRAR do wykonania kodu osadzonego w archiwum.

Uruchomienie

Nazwa taktyki/techniki	ID	Użycie
User Execution: Malicious Link	T1204.001	Wykorzystanie w spearphishing linków do hostowanych skrótów.
User Execution: Malicious File	T1204.002	Dostarczenie złośliwego oprogramowania poprzez spearphishing.
Command and Scripting Interpreter	T1059	Wykorzystanie spearphishing do dostarczenia skryptów. Wykonanie komend w powłoce systemu.
Command and Scripting Interpreter: PowerShell	T1059.001	Wykorzystanie poleceń PowerShell do przygotowania danych do eksfiltracji.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Wykorzystanie skryptów BAT w spearphishingu.
Command and Scripting Interpreter: Visual Basic	T1059.005	Wykorzystanie skryptów VBScript w spearphishingu.
Command and Scripting Interpreter: Python	T1059.006	Umieszczenie interpretera Python na skompromitowanym systemie, aby umożliwić wykonanie Certipy.

Persystencja

Nazwa taktyki/techniki	ID	Użycie
Account Manipulation: Additional Email Delegate Permissions	T1098.002	Modyfikacja uprawnień do skrzynek pocztowych, aby umożliwić długotrwałe pozyskiwanie wiadomości.
Modify Authentication Process: Multi-Factor Authentication	T1556.006	Dołączenie skompromitowanych kont do kontrolowanych przez atakującego mechanizmów MFA, aby zwiększyć poziom zaufania do dostępu i umożliwić długotrwały dostęp do kont.
Hijack Execution Flow: DLL Search Order Hijacking	T1574.001	Użycie DLL Search Order Hijacking aby uruchomić złośliwe oprogramowanie.
Scheduled Task/Job: Scheduled Task	T1053.005	Użycie Scheduled Tasks do zapewnienia persystencji.

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	Użycie kluczy rejestru Run do zapewnienia persystencji.
Boot or Logon Autostart Execution: Shortcut Modification	T1547.009	Użycie skrótów umieszczonych w folderach startup do zapewnienia persystencji.

Unikanie wykrycia

Nazwa taktyki/techniki	ID	Użycie
Indicator Removal: Clear Windows Event Logs	T1070.001	Usunięcie logów zdarzeń z użyciem narzędzia wevtutil.

Dostęp do danych uwierzytelniających

Nazwa taktyki/techniki	ID	Użycie
Brute Force	T1110	Przesłanie zakodowanych w Base64 danych uwierzytelniających do serwerów RTSP, w tym publicznie udokumentowanych domyślnych danych uwierzytelniających oraz ogólnych prób odgadnięcia haseł.
Brute Force: Password Guessing	T1110.001	Użycie odgadywania danych uwierzytelniających do uzyskania początkowego dostępu.
Brute Force: Password Spraying	T1110.003	Użycie ataku *brute force* do uzyskania początkowego dostępu. Użycie *password spraying* poprzez protokół LDAP.
Multi-Factor Authentication Interception	T1111	Użycie wieloetapowych przekierowań, aby przechwycić i użyć token MFA.
Input Capture	T1056	Użycie wieloetapowych przekierować, aby przechwycić rozwiązanie mechanizmu CAPTCHA.
Forced Authentication	T1187	Użycie podatności w programie Outlook do przechwycenia hashy NTLM poprzez specjalnie przygotowaną wiadomość poczty elektronicznej.
OS Credential Dumping: NTDS	T1003.003	Próba przechwycenia pliku NTDS.dit.
Unsecured Credentials: Group Policy Preferences	T1552.006	Uzyskanie dostępu do haseł w postaci jawnej z *Group Policy Preferences* poprzez Get-GPPPassword.py.

Zbieranie informacji

Nazwa taktyki/techniki	ID	Użycie
Account Discovery: Domain Account	T1087.002	Użycie zmodyfikowanego skryptu ldap-dump.py do zbieranie informacji o środowisku opartym o MS Windows.

Command and Control[xxiv]

Nazwa taktyki/techniki	ID	Użycie
Hide Infrastructure	T1665	Wykorzystanie przejętych urządzeń SOHO do prowadzenia w sposób skryty i anonimowy działań w cyberprzestrzeni, do budowy przekierowań, proxy. Wykorzystanie urządzeń o adresach IP geolokalizowanych w pobliżu ofiary.
Proxy: External Proxy	T1090.002	Przesłanie żądań RTSP DESCRIBE do serwerów RTSP.
Proxy: Multi-hop Proxy	T1090.003	Użycie sieci Tor oraz komercyjnych usług VPN jako elementów infrastruktury anonimizacyjnej.
Encrypted Channel	T1573	Wszystkie połączenia do infrastruktury ofiary realizowane były poprzez protokół TLS.
Multi-Stage Channels	T1104	Użycie wieloetapowych przekierowań.

Unikanie wykrycia (techniki dla urządzeń mobilnych)

Nazwa taktyki/techniki	ID	Użycie
Execution Guardrails	T1627	Użycie wieloetapowych przekierowań sprawdzających właściwości przeglądarki.
Execution Guardrails: Geofencing	T1627.001	Użycie wieloetapowych przekierowań sprawdzających geolokalizację adresu IP nawiązującego połączenie.

Poruszanie się pomiędzy urządzeniami

Nazwa taktyki/techniki	ID	Użycie
Lateral Movement	TA0008	Użycie komend systemu operacyjnego oraz otwartoźródłowych narzędzi, takich jak Impacket oraz PsExec do poruszania się pomiędzy urządzeniami.
Remote Services: Remote Desktop Protocol	T1021.001	Poruszanie się pomiędzy urządzeniami wykorzystując protokół RDP.

Pozyskiwanie informacji

Nazwa taktyki/techniki	ID	Użycie
Email Collection	T1114	Pozyskiwanie wrażliwych danych z serwera pocztowego.
Email Collection: Remote Email Collection	T1114.002	Użycie protokołów służących do wymiany danych z serwerami poczty elektronicznej, takich jak EWS oraz IMAP, do eksfiltracji danych.
Automated Collection	T1119	Użycie okresowych kwerend EWS do pozyskiwania nowych wiadomości email.
Video Capture	T1125	Próby uzyskania dostępu do strumienia obrazu video z kamer IP.
Archive Collected Data	T1560	Pakowanie plików wybranych do eksfiltracji do archiwum .zip.
Archive Collected Data: Archive via Utility	T1560.001	Pakowanie plików wybranych do eksfiltracji do archiwum .zip.

Eksfiltracja

Nazwa taktyki/techniki	ID	Użycie
Exfiltration Over Alternative Protocol	T1048	Próby eksfiltracji danych poprzez umieszczony wcześniej w systemie plik wykonywalny OpenSSH.
Scheduled Transfer	T1029	Użycie okresowych kwerend EWS do pozyskiwania nowych wiadomości email.

Załącznik B: Wykorzystywane podatności

CVE	Oprogramowanie	Szczegóły
CVE-2023-38831	RARLAB WinRAR	Pozwala na wykonanie dowolnego kodu, kiedy użytkownik spróbuje otworzyć niezłośliwy plik znajdujący się wewnątrz archiwum ZIP.
CVE-2023-23397	Microsoft Outlook	Dowolny podmiot, w tym spoza organizacji, może wysłać wiadomość email, która spowoduje nawiązanie połączenia od ofiary do dowolnego systemu, powodując przekazanie hasha Net-NTLMv2. Przejęty hash Net-NTLMv2 może zostać użyty do logowania do innych usług w imieniu ofiary.
CVE-2021-44026	Roundcube Webmail	Oprogramowanie Roundcube w wersjach 1.3.X wcześniejszych niż 1.3.17 oraz w wersjach 1.4.X wcześniejszych niż 1.4.12 jest podatne na SQL Injection poprzez wyszukanie lub parametry wyszukania.
CVE-2020-35730	Roundcube Webmail	Podatność typu XSS występująca w wersjach 1.2.X wcześniejszych niż 1.2.13; 1.3.X wcześniejszych niż 1.3.16; 1.4.X wcześniejszych niż 1.4.10. XSS może zostać wykonany poprzez przesłanie tekstowej wiadomości email z skryptem JavaScript w odnośniku. XSS wynika z błędnej obsługi linków przez linkref_addindex w rcube_string_replacer.php.
CVE-2020-12641	Roundcube Webmail	Oprogramowanie Roundcube w wersjach wcześniejszych niż 1.4.4 pozwala na wykonanie dowolnego kodu poprzez metaznaki powłoki w ustawieniach konfiguracji dla im_convert_path lub im_identify_path w rcube_image.php

Załącznik C: Mechanizmy bezpieczeństwa MITRE D3FEND

Nazwa mechanizmu bezpieczeństwa (zgodnie z nazwami MITRE D3FEND)	ID	Szczegóły
Network Isolation	D3-NI	Należy wdrożyć segmentację sieci. Należy wyłączyć funkcje Universal Plug and Play (UPnP), Peer-to-Peer (P2P) oraz anonimowego (nieuwierzytelnionego) dostępu na routerach oraz kamerach IP.
Access Mediation	D3-AMED	Należy wprowadzić ograniczenia dostępu do zasobów oraz wykorzystywać w procesie nadawania dostępu dodatkowe atrybuty (takie jak informacje o urządzeniu, środowisko, ścieżki dostępu). Kontrola dostępu powinna być skonfigurowana tak, aby zapewnić, że wyłącznie uwierzytelnione i utrzymywane na bieżąco konta otrzymają dopuszczenie.
Inbound Traffic Filtering	D3-ITF	Aby ograniczyć możliwość poruszania się atakującego po sieci, należy skonfigurować zaporę sieciową urządzeń w taki sposób, aby zablokować połączenia przychodzące od innych urządzeń, z wyjątkiem zaufanych usług i serwerów zarządzających.
Resource Access Pattern Analysis	D3-RAPA	Należy wykorzystywać automatyczne narzędzia do przeprowadzenia audytów logów dostępowych pod kątem anomalii i zagrożeń.
Outbound Traffic Filtering	D3-OTF	Należy zablokować połączenia NTLM/SMB wychodzące do zewnętrznej infrastruktury.
Platfrom Monitoring	D3-PM	Należy wdrożyć oprogramowanie typu EDR oraz rozwiązania do zbierania logów na istotnych systemach oraz systemach zawierających duże

		ilości wrażliwych danych (takich jak systemy pocztowe lub kontrolery domen).
System File Analysis	D3-SFA	Należy zbierać oraz monitorować logi systemu Windows pod kątem zdarzeń mogących sugerować, że log został zmodyfikowany lub wyczyszczony.
Application Hardening	D3-AH	Należy włączyć opcjonalne funkcjonalności bezpieczeństwa systemów Windows, aby zwiększyć bezpieczeństwo urządzeń końcowych i zablokować (niektóre) techniki uzyskania początkowego dostępu.
Application-based Process Isolation	D3-ABPI	Należy włączyć regułę ASR blokującą możliwość uruchomienia plików wykonywalnych pochodzących z poczty elektronicznej.
Executable Allowlisting	D3-EAL	Należy włączyć regułę ASR blokującą możliwość wykonania plików z zapisywalnych dla wszystkich ścieżetk takich jak Pobrane lub %APPDATA%.
Executable Isolation	D3-EI	Jeżeli użytkownik nie zajmuje się wytwarzaniem nowych skryptów (PowerShell, JavaScript, batch), należy zablokować możliwość wykonania innych niż znane.
Application Configuration Hardening	D3-ACH	Należy wyłączyć funkcjonalność Windows Host Scripting oraz skonfigurować PowerShell do działania w trybie Constrained. Należy wyłączyć protokoły używające słabych mechanizmów uwierzytelnienia (takich jak hasła w postaci jawnej, przestarzałe bądź podatne usługi oraz algorytmy szyfrowania) lub niewspierające uwierzytelnienia wieloskładnikowego. Należy wyłączyć nieużywane porty i usługi (np. FTP, interfejs web).
Process Spawn Analysis	D3-PSA	Należy wykorzystać otwartoźródłowe reguły SIGMA do stworzenia podstawowej zdolności do

		wykrywania i ostrzegania o wykonaniu podejrzanych plików lub z podejrzanymi argumentami.
URL Reputation Analysis	D3-URA	Należy wykorzystywać usługi zapewniające dodatkowe mechanizmy bezpieczeństwa, takie jak sprawdzanie bezpieczeństwa linków.
Network Access Mediation	D3-NAM	Należy zablokować przychodzący ruch sieciowy, szczególnie próby logowania, do pochodzące z publicznych (komercyjnych) usług VPN. Jeżeli jest to możliwe, należy całkowicie zablokować możliwość logowania z węzłów wyjściowych publicznych usług VPN, włączając w to węzły znajdujące się w Polsce. Jeżeli logowanie z usług VPN jest dozwolone, powinno być monitorowane i weryfikowane. Jeżeli jest to możliwe, kamery IP oraz inne urządzenia IoT powinny znajdować się za urządzeniami bezpieczeństwa.
DNS Denylisting	D3-DNSDL	Należy zablokować wychodzące połączenia do usług hostingowych oraz usług udających API (ang. A*PI mocking*) często używanych przez złośliwe grupy.
Domain Name Reputation Analysis	D3-DNRA	Mechanizmy detekcji żądań web do nowych poddomen mogą pozwolić na wykrycie prób phishingu. Logowanie żądań przesyłanych do wszystkich poddomen może pozwolić na wykrycie nowych prób bądź ofiar phishingu.
Multi-factor Authentication	D3-MFA	Należy używać mechanizmu uwierzytelnienia wieloskładnikowego (MFA) opartego o silny składnik. Usługi zarządzania powinny wymagać częstego ponownego uwierzytelnienia.
Job Function Access Pattern Analysis	D3-JFAPA	Należy wdrożyć dodatkowe mechanizmy bezpieczeństwa dla uprzywilejowanych kont: ograniczenie ilości kont administracyjnych, wdrożenie sprzętowych składników MFA oraz

		regularnie przeglądać istniejące uprzywilejowane konta.
User Account Permissions	D3-UAP	Należy rozdzielić uprzywilejowane konta względem pełnionej roli. Należy audytować uprzywilejowane konta na wszystkich urządzeniach, aby mieć pewność, że oddają strukturę organizacji oraz że są wykorzystywane zgodnie z przeznaczeniem.
Token-based Authentication	D3-TBA	Należy ograniczyć uwierzytelnianie oparte o hasła i zamiast nich wykorzystywać usługi typu *single sign-on*.
Credential Hardening	D3-CH	Nie należy przechowywać haseł w *Group Policy Preferences* (GPP). Należy usunąć i zmienić wszystkie hasła znajdujące się dotychczas w GPP.
Authentication Event Treshholding	D3-ANET	Należy wprowadzić spowalnianie kolejnych logowań. Spowalnianie powinno rosnąć pomiędzy kolejnymi nieudanymi próbami logowania. Jeżeli wykorzystywany jest mechanizm blokowania konta po nieudanych logowaniach, dopuszczona ilość prób powinna być pomiędzy 5 i 10.
Strong Password Policy	D3-SPP	Należy wykorzystywać usługi pozwalające na monitorowanie czy hasło zostało skompromitowane.
Credential Rotation	D3-CRO	Należy zmienić wszystkie domyślne dane uwierzytelniające.
Encrypted Tunnels	D3-ET	Należy wyłączyć protokoły używające słabych mechanizmów uwierzytelnienia. Aby umożliwić połączenie ze zdalnych urządzeń, należy używać VPN.
Software Update	D3-SU	Wszystkie urządzenia powinny mieć zainstalowane aktualizacje bezpieczeństwa oraz

		aktualizacje oprogramowania sprzętowego. Wszystkie używane urządzenia powinny być wspierane. Urządzenia wycofane ze wsparcia producenta powinny zostać wymienione.
Agent Authentication	D3-AA	Dostęp zdalny do urządzeń powinien wymagać uwierzytelnienia. W przypadku kamer IP, dostęp do strumienia RTSP powinien być ograniczony do uwierzytelnionych połączeń.
User Behaviour Analysis	D3-UBA	Należy sprawdzać wszystkie połączenia zdalne i sprawdzać wszystkie niespodziewane bądź nietypowe.

[i] CSA – ang. *Cybersecurity Advisory* – ostrzeżenie przed zagrożeniem w cyberprzestrzeni; Również: JCSA – ang. *Joint Cybersecurity Advisory* – wspólne ostrzeżenie przed zagrożeniem w cyberprzestrzeni, opracowane przez lub popierane (potwierdzane) przez wiele służb lub krajów.
[ii] Rozumiana w kontekście tego CSA jako głównie, dostawcy usług IT.
[iii] Nazwa w języku angielskim: GRU 85th Main Special Service Centre.
[iv] TTP (zamiennie: TTPs) – ang. *Tactics, Techniques, Procedures* – określenie branżowe, podobne w znaczeniu do *modus operandi* – oznacza sposoby prowadzenia działań, w aspekcie technicznym.
[v] IoC (zamiennie: IoCs) – ang. *Indicators of Compromise* – charakterystyczne dane, których wystąpienie pozwala stwierdzić, czy doszło do przełamania zabezpieczeń systemu informatycznego.
[vi] Password Spraying – wariant ataku brute force, sposób przełamywania haseł polegający na używaniu jednego hasła kolejno wobec wielu kont; dzięki temu atakujący zmniejsza szanse na zablokowanie konta i wykrycie ataku.
[vii] Spearphishing – użycie socjotechniki do nakłonienia wybranej ofiary do wykonania szkodliwej dla niej akcji; zazwyczaj używane w kontekście wiadomości email, ale może również
[viii] SOHO – ang. *Small Office/Home Office* – urządzenia przeznaczone do użytku domowego oraz w małych biurach.
[ix] CAPTCHA to zabezpieczenie przed automatycznymi narzędziami próbującymi uzyskać dostęp do zasobu (zazwyczaj strony internetowej).
[x] Hash NTLM – mechanizm kryptograficzny wykorzystywany do uwierzytelnienia.
[xi] LDAP – ang. *Lightweight Directory Access Protocol* – protokół używany do dostępu do informacji przetwarzanych przez usługi katalogowe (np. Active Directory).
[xii] Persystencja (zamiennie: przetrwanie w systemie) – zdolność złośliwego oprogramowania do wznowienia działania po ponownym uruchomieniu systemu operacyjnego.
[xiii] ang. DLL Search Order Hijacking – wykorzystanie algorytmu ładowania do procesu plików DLL aby uruchomić złośliwe oprogramowanie.
[xiv] ang. Schedule Task – wbudowany w system Windows mechanizm uruchamiania zdefiniowanych akcji po wystąpieniu określonego zdarzenia.
[xv] Ogólne określenie kluczy w rejestrze systemu Windows pozwalających na automatyczne uruchomienie programów wraz z uruchomieniem systemu operacyjnego.
[xvi] Ogólne określenie na katalogi w systemie Windows pozwalające na automatyczne uruchomienie programów wraz z uruchomieniem systemu operacyjnego.
[xvii] Living of the Land Binaries and Scripts (tzw. LOLBAS lub LOLBINS) – wbudowane w system operacyjny, niezłośliwe programy, które mogą być wykorzystane do wykonania czynności normalnie realizowanych przez złośliwe oprogramowanie; ich użycie zazwyczaj obniża ryzyko wykrycia.
[xviii] Protokół służący do interakcji z serwerami Microsoft Exchange.
[xix] IMAP – ang. *Internet Message Access Protocol* - protokół, który służy do dostępu do skrzynki poczty elektronicznej przechowywanej na zdalnym serwerze.
[xx] Zestaw dodatkowych opcji konfiguracyjnych w systemie Windows mających na celu podniesienie bezpieczeństwa systemu. Włączenie reguł ASR wymaga wcześniejszych testów, ponieważ, w niektórych konfiguracjach systemu, mogą zakłócić działanie jego funkcji lub programów
[xxi] BATCH - język skryptowy w systemie Windows, wywodzący się z czasów systemu DOS, pozwalający na skryptowanie systemu operacyjnego.
[xxii] W tym kontekście - omyłkowe zaklasyfikowanie normalnego, niezłośliwego zachowania jako złośliwe.
[xxiii] CTI – ang. *Cyber Threat Intelligence* – część branży cyberbezpieczeństwa zajmująca się dostarczaniem informacji o zagrożeniach.
[xxiv] Command and Control – określenie na mechanizmy zarządzania przejętymi urządzeniami albo uruchomionym złośliwym oprogramowaniem.