Na podstawie MITRE ATT&CK możemy wyróżnić następujące grupy APT, którym przypisuje się atrybucję rosyjską:

Ataki na sieci korporacyjne (Enterprise):

APT28, APT29, Dragonfly 2.0, FIN5, Indrik Spider, Nomadic Octopus, Sandworm Team, TEMP.Veles, turla, Wizard Spider

Ataki na sieci automatyki przemysłowej:

ALLANITE, Dragonfly 2.0, Sandworm Team, TEMP.Veles

Ich motywacja oraz sposoby działania się różnią, ale poniżej przedstawiamy listę najczęściej wykorzystywanych TTP (Taktyki, Techniki, Procedury) jakimi się posługują i które najprawdopodobniej zostaną wykorzystane podczas ataków wraz z propozycją dodatkowych działań uzupełniających do akcji wymaganych przy stopniu alarmowym Charlie-CRP.

Rekomendacje natychmiastowych działań prewencyjnych i reakcyjnych.

Poniżej przedstawiamy rekomendacje, z czego pierwsza jest szczególnie ważna w kontekście podjęcia konkretnych działań związanych z obroną przed atakami APT przez grupy, którym przypisuje się atrybucję rosyjską. ComCERT posiada doświadczenie w realizacji takiego zadania i oferuje wsparcie w tym zakresie. Zainteresowanych prosimy o kontakt (kontakt@comcert.pl).

1. **Przeprowadź modelowanie zagrożeń dotyczące poniżej wymienionych TTP w celu zweryfikowania i ewentualnego podniesienia poziomu zdolności do ochrony i wykrywania wykorzystywanych przez rosyjskie służby technik ataku.**
2. Przeprowadź kampanię informacyjną wśród personelu w celu:
    a. ostrzeżenia przed otwieraniem podejrzanych linków do sensacyjnych wiadomości, korespondencji mailowej, załączników, odwiedzania niezaufanych stron itd.,
    b. zgłaszania wszelkich podejrzanych działań i anomalii systemów informatycznych do wyznaczonych osób.
3. Opracuj wewnętrzne listy kontaktów i zapewnij wsparcie techniczne.
4. Zaktualizuj i załataj wszystkie systemy. Nadaj priorytety łatania znanych, wykorzystanych luk.
5. Wdrożenie uwierzytelniania wieloskładnikowego (MFA – Multi-Factor Authentication)
6. Użycie najbardziej aktualnego oprogramowania antywirusowego.
7. Monitoruj podejrzaną komunikację do/z sieci zewnętrznej oraz w ramach sieci wewnętrznej.
8. Uruchomienie i przegląd systemu gromadzenia i przechowywania dzienników zdarzeń:
    a. Przeglądaj dzienniki uwierzytelniania pod kątem niepowodzeń logowania do systemu i aplikacji na ważnych kontach.

b. Zwróć uwagę na wielokrotne, nieudane próby uwierzytelnienia na wielu kontach.
c. Zwróć uwagę na jeden adres IP używany do wielu kont, z wyłączeniem oczekiwanych logowań.
d. Zwróć uwagę na tzw. "niemożliwe podróże". Niemożliwe przemieszczanie się ma miejsce, gdy użytkownik loguje się z wielu adresów IP, które są od siebie znacznie oddalone (tzn. osoba nie mogłaby realistycznie przemieszczać się między lokalizacjami geograficznymi dwóch adresów IP w okresie między logowaniami).
e. Zwracaj uwagę na procesy i argumenty wiersza poleceń wykonywania programów, które mogą wskazywać na dumping danych uwierzytelniających, zwłaszcza na próby uzyskania dostępu do pliku ntds.dit lub skopiowania go z kontrolera domeny.
f. Zwróć uwagę na podejrzane użycie kont uprzywilejowanych po zresetowaniu haseł lub zastosowaniu zabezpieczeń kont użytkowników.
g. Zwróć uwagę na nietypową aktywność na typowych, uśpionych kontach.
h. Zwracaj uwagę na nietypowe ciągi agenta użytkownika, takie jak ciągi niezwiązane z normalną aktywnością użytkownika, które mogą wskazywać na działanie botów.

9. Szukaj dowodów behawioralnych lub artefaktów opartych na sieci i hoście, pochodzących z niżej wymienionych TTP wykorzystywanych przez grupy APT sponsorowane przez państwo rosyjskie.
10. Dla organizacji posiadających systemy OT/ICS:
    a. Odnotuj nieoczekiwane zachowanie sprzętu, np. nieoczekiwane restarty sterowników oraz innego sprzętu i oprogramowania OT.
    b. Monitoruj i odnotowuj opóźnienia lub zakłócenia w komunikacji z urządzeniami obiektowymi lub innymi urządzeniami OT.

Taktyki, techniki, procedury (TTP)

TTP wykorzystywane przez rosyjskie grupy APT w atakach na sieci korporacyjne.

Taktyka	Technika	Procedura
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Sponsorowane przez państwo rosyjskie grupy APT prowadzą zakrojone na szeroką skalę skanowanie, próbując znaleźć podatne na ataki serwery.
	Phishing for Information [T1598]	Sponsorowane przez państwo rosyjskie grupy APT prowadzą kampanie spearphishingowe w celu zdobycia danych uwierzytelniających.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Sponsorowane przez państwo rosyjskie grupy APT opracowują i wdrażają złośliwe oprogramowanie, w tym destrukcyjne oprogramowanie ukierunkowane na sieci automatyki przemysłowej.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Sponsorowane przez państwo rosyjskie grupy APT wykorzystują publicznie znane luki, jak również luki typu zero-days, w systemach internetowych w celu uzyskania dostępu do sieci.
	Supply Chain Compromise:	Sponsorowane przez państwo rosyjskie grupy APT uzyskują dostęp do sieci organizacji poprzez skompromitowanie

Taktyka	Technika	Procedura
	Compromise Software Supply Chain [T1195.002]	zaufanego oprogramowania firm trzecich (np. atak SolarWinds)
	Spearphishing Attachment (T1566.001)	Sponsorowane przez państwo rosyjskie grupy APT rozsyłają wiadomości e-mail ze złośliwym załącznikiem w celu uzyskania dostępu do systemów ofiar.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Sponsorowane przez państwo rosyjskie grupy APT wykorzystują cmd.exe do wykonywania poleceń na zdalnych komputerach. Używają również PowerShell do tworzenia nowych zadań na zdalnych maszynach, identyfikowania ustawień konfiguracyjnych, eksfiltracji danych oraz wykonywania innych poleceń.
Persistence [TA0003]	Valid Accounts [T1078]	Sponsorowane przez państwo rosyjskie grupy APT wykorzystują pozyskane dane uwierzytelniające z istniejących kont, aby utrzymać stały, długotrwały dostęp do zaatakowanych sieci
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Sponsorowane przez państwo rosyjskie grupy APT prowadzą kampanie zgadywania haseł metodą brute-force oraz kampanie rozpraszania haseł.
	OS Credential Dumping: NTDS [T1003.003]	Sponsorowane przez państwo rosyjskie grupy APT dokonują eksfiltracji danych uwierzytelniających i eksportują kopie bazy danych Active Directory ntds.dit.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Sponsorowane przez państwo rosyjskie grupy APT przeprowadzają operację "Kerberoasting", w ramach której uzyskują tickety Ticket Granting Service (TGS) dla nazw głównych usług Active Directory (SPN).
	Credentials from Password Stores [T1555]	Sponsorowane przez państwo rosyjskie grupy APT wykorzystują wcześniej skompromitowane dane uwierzytelniające konta do próby uzyskania dostępu do haseł Group Managed Service Account (gMSA).
	Exploitation for Credential Access [T1212]	Sponsorowane przez państwo rosyjskie grupy APT wykorzystują lukę CVE-2020-1472 w systemie Windows Netlogon do uzyskania dostępu do serwerów Windows Active Directory.
	Unsecured Credentials: Private Keys [T1552.004]	Sponsorowane przez państwo rosyjskie grupy APT uzyskują prywatne klucze szyfrujące z kontenera Active Directory Federation Services (ADFS) w celu odszyfrowania odpowiadających im certyfikatów podpisu SAML.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Sponsorowane przez państwo rosyjskie podmioty APT wykorzystują wirtualne serwery prywatne (VPS) do kierowania ruchu do celów. Podmioty te często używają VPS-ów z adresami IP w kraju ojczystym ofiary, aby ukryć aktywność wśród legalnego ruchu użytkowników.

TTP wykorzystywane przez rosyjskie grupy APT w atakach na sieci automatyki przemysłowej[1]

Taktyka	Technika	Procedura
Execution Evasion	Change Operating Mode (T0858)	Sponsorowane przez państwo rosyjskie grupy APT zmianiają tryb pracy kontrolera, aby uzyskać dodatkowy dostęp do funkcji technicznych, takich jak pobieranie programu (Program Download)
	Modify Controller Tasking (T0821)	Sponsorowane przez państwo rosyjskie grupy APT modyfikują zadania kontrolera w celu umożliwienia wykonywania własnych programów i manipulowania przebiegiem wykonania i zachowaniem kontrolera.
Persistence	Modify Program (T0889)	Sponsorowane przez państwo rosyjskie grupy APT modyfikują lub dodają program na sterowniku, aby wpłynąć na jego interakcję z procesem fizycznym, urządzeniami peryferyjnymi i innymi hostami w sieci. Modyfikacji programów sterownika dokonują za pomocą funkcji pobierania programu (Program download) wraz z innymi rodzajami modyfikacji programu, takich jak edycja online i dołączanie programu.
	Module Firmware (T0839)	Sponsorowane przez państwo rosyjskie grupy APT instalują złośliwe lub podatne na ataki oprogramowanie sprzętowe w modułowych urządzeniach sprzętowych (firmware).
	System Firmware (T0857)	Sponsorowane przez państwo rosyjskie grupy APT mogą wykorzystywać funkcję aktualizacji oprogramowania sprzętowego w dostępnych urządzeniach do wgrywania złośliwego lub nieaktualnego oprogramowania sprzętowego.

[1] Przedstawione techniki są dedykowane dla sieci automatyki przemysłowej, jednak większość technik zaprezentowanych w powyższej tabelce jest również możliwa do zastosowania.