GHOSTWRITER APT / UNC1151 — Повний OSINT-аналіз

КЛАСИФІКАЦІЯ: OFFICIAL SENSITIVE
ДАТА ЗВІТУ: 2 червня 2026 року
РОЗПОВСЮДЖЕННЯ: Фахівці з кібербезпеки, посадові особи оборонного сектору, аналітики кіберрозвідки (Threat Intelligence)
ПІДГОТУВАВ: Mark iVan

СУБ'ЄКТ ЗАГРОЗИ: Ghostwriter APT (також відомий як UNC1151, FrostyNeighbor, PUSHCHA, UAC-0057, Storm-0257, TA445, White Lynx, Blue Dev 4, Moonscape)

АТРИБУЦІЯ: Білоруська військова розвідка (GSSD/Міністерство оборони) за документально підтвердженої координації з російським ГРУ

РІВЕНЬ ЗАГРОЗИ: КРИТИЧНИЙ

ОПЕРАЦІЙНИЙ СТАТУС: АКТИВНИЙ (безперервні операції до травня 2026 року)

КЛЮЧОВИЙ ВИСНОВОК: Ghostwriter є унікальною гібридною загрозою, що поєднує складне кібершпигунство з координованими операціями з дезінформації та інформаційної війни. На відміну від традиційних APT-угруповань, Ghostwriter інтегрує тактичні кібервторгнення зі стратегічними операціями впливу, що робить його особливою загрозою для НАТО, урядів країн Східної Європи та України.

Ключові розвідувальні висновки

1. Державна підтримка: атрибуція уряду Білорусі з ВИСОКИМ РІВНЕМ ВПЕВНЕНОСТІ; координація з російським ГРУ з ПОМІРНО-ВИСОКИМ РІВНЕМ ВПЕВНЕНОСТІ.

2. Безперервність операцій: активна діяльність з 2016–2017 років; операції тривають до травня 2026 року попри публічну атрибуцію та санкції.

3. Інтеграція гібридної війни: унікальне поєднання кібершпигунства, дезінформації та психологічних операцій.

4. Нещодавня активність: кампанії травня 2026 року, спрямовані проти уряду України із застосуванням фішингового шкідливого ПЗ Prometheus; триває націлювання на білоруську опозицію.

5. Розвиненість інфраструктури: багатоступеневі ланцюги доставки шкідливого ПЗ, власні завантажувачі (PicassoLoader), використання Cobalt Strike, експлуатація вразливості CVE-2024-42009.

ПРОФІЛЬ АКТОРА ТА АТРИБУЦІЯ

Відомі псевдоніми та позначення

Псевдонім	Джерело	Примітки
Ghostwriter	FireEye/Mandiant	Основне операційне позначення; використовується в публічних звітах
UNC1151	Mandiant	Позначення некластеризованого загрозового актора; основне технічне відстеження
FrostyNeighbor	Security vendors	Позначення недавніх кампаній (2025–2026)
PUSHCHA	Google TAG	Позначення, що використовується у звітах з кіберрозвідки
UAC-0057	CERT-UA	Позначення українського CERT; також UAC-0051
Storm-0257 / DEV-0257	Microsoft	Позначення Microsoft Threat Intelligence
TA445	Proofpoint	Позначення Proofpoint
White Lynx	Palo Alto Networks	Позначення Palo Alto Networks
Blue Dev 4	Security community	Позначення, сформоване спільнотою
Moonscape	Secureworks	Позначення Secureworks
Operation Ghostwriter	FireEye	Позначення кампанійного рівня

АНАЛІЗ АТРИБУЦІЇ

Основна атрибуція: Білоруська військова розвідка

Рівень впевненості: ВИСОКИЙ

Підстава атрибуції:

1. Геолокаційні докази

- Технічні дані, отримані Mandiant із застосуванням чутливих методів, вказують на операторів, розташованих у Мінську, Білорусь.
- Патерни інфраструктури відповідають використанню білоруських інтернет-провайдерів.
- Часова прив’язка операцій корелює з інтересами уряду Білорусі.

2. Організаційні зв’язки

- З високим рівнем впевненості оцінюється зв’язок із білоруською військовою розвідувальною агенцією (GSSD).
- Ймовірні зв’язки з Міністерством оборони.
- Операційні цілі узгоджуються з державними інтересами Білорусі.

3. Патерни націлювання

- Послідовне націлювання на країни-члени НАТО та пов’язані з НАТО організації.
- Систематичний фокус на Україні, Польщі та країнах Балтії.
- Націлювання на білоруські опозиційні структури.
- Часові патерни корелюють із геополітичними подіями, що впливають на Білорусь.

4. Операційні характеристики

- Застосування маскування (maskirovka) — доктрини військової дезінформації РФ.
- Техніки false flag та забезпечення правдоподібного заперечення.
- Гібридний підхід до війни, що поєднує кібероперації та інформаційні операції.
- Координація з російськими військовими інтересами.

Додаткова атрибуція: координація з російським ГРУ

Рівень впевненості: ПОМІРНО-ВИСОКИЙ

Підстава атрибуції:

1. Оцінка уряду Німеччини (вересень 2021)

- Міністерство закордонних справ Німеччини (Federal Foreign Office) приписало активність Ghostwriter у Німеччині російській військовій розвідувальній службі (ГРУ).
- Фіксувалося цілеспрямоване націлювання на німецький парламент та урядових посадовців.
- Технічні індикатори були пов’язані з російськими військовими операціями.

2. Атрибуція ЄС (вересень 2021)

- Голова зовнішньої політики ЄС Жозеп Боррель приписав операції російській державі.
- ЄС погрожував санкціями проти Росії за кібердіяльність.
- Було скоординовано відповідь ЄС на операції Ghostwriter.

3. Операційне накладання

- Recorded Future виявила перетини в TTPs, які використовують UNC1151 та російські загрозові групи (APT28, Sandworm).
- Ймовірна наявність планувальної підтримки з боку російських військових агентів.
- Спільні патерни інфраструктури з російськими військовими операціями.

4. Геополітична координація

- Широка присутність російських військових у Білорусі підтверджує ймовірний зв’язок із російськими інтересами.
- Часові характеристики операцій вказують на координацію з російськими військовими цілями.
- Ескалація кампаній корелює з російськими військовими операціями в Україні.

Невирішені питання атрибуції

Оцінка Mandiant (листопад 2021):

- «UNC1151 — білоруська операція, російський проксі або колаборативна структура для білоруських і російських військових акторів — залишається нез’ясованим».
- Не можна виключити російську участь; на момент оцінки не було виявлено прямих доказів такої участі.
- Mandiant відстежує UNC1151 з 2017 року і не зафіксувала перетинів із російськими групами APT28, APT29, Turla, Sandworm, TEMP.Armageddon.

Поточна оцінка (2026):

- Дані вказують на колаборативну структуру, а не суто білоруську або російську операцію.
- Російська військова присутність у Білорусі забезпечує можливість координації.
- Операційні цілі узгоджуються як з білоруськими, так і з російськими інтересами.
- Найімовірніший сценарій: білоруська військова розвідка з російською координацією або підтримкою.

ОРГАНІЗАЦІЙНА СТРУКТУРА ТА ІДЕНТИФІКОВАНИЙ ПЕРСОНАЛ

Відомі оператори інфраструктури

Андрій Корінець

Статус: Ідентифікований та під санкціями
Роль: Оператор інфраструктури; незаконно створював інфраструктуру шкідливих доменів

Діяльність:

- Створював шкідливі домени, що використовувалися в кампаніях Ghostwriter.
- Надавав інфраструктурну підтримку для операцій російських ФСБ/військових структур.
- Керував сервісами реєстрації шкідливих доменів.
- Координувався з російською військовою розвідкою.

Статус санкцій:

- Виявлений через аналіз інфраструктури.
- Підпадає під міжнародні санкції.
- Реальна особа встановлена через OSINT-розслідування.
- Пов’язаний з російськими ФСБ та військовими операціями.

Значення:

- Демонструє реальну операційну інфраструктуру.
- Підтверджує координацію між білоруськими та російськими структурами.
- Показує аутсорсинг інфраструктури довіреним операторам.
- Вказує на професійні практики операційної безпеки.

Організаційні підрозділи

Білоруська військова розвідка (GSSD)

- Основний операційний підрозділ
- Розташований у Мінську, Білорусь
- Відповідає за операції кібершпигунства
- Координується з російською військовою розвідкою

Російське ГРУ (Головне розвідувальне управління)

- Підрозділ вторинної координації
- Надає планувальну підтримку та оперативне керівництво
- Ділиться інфраструктурою та TTPs (тактиками, техніками і процедурами)
- Координує часові рамки з військовими операціями

Підрозділ інформаційної війни

- Відповідає за кампанії дезінформації
- Координує дії з кіберопераціями
- Націлений на медіа-організації та цивільне населення
- Оперативно використовує фальшиві (false flag) персонажі

ІСТОРІЯ ОПЕРАЦІЙ І ТАЙМЛАЙН

ФАЗА 1: ФОРМУВАННЯ ТА РАННІ ОПЕРАЦІЇ (2016–2020)

Дата	Подія	Context	Impact
2016-2017	Формування угруповання	Початкові операції кібершпигунства	Початок націлювання на структури НАТО та країн Східної Європи
2016-2020	Кампанії з викрадення облікових даних	Масові фішингові атаки на урядові та військові структури	Отримано сотні викрадених облікових даних
липень 2020	Виявлення дезінформаційної кампанії Ghostwriter	Публічна ідентифікація операцій інформаційної війни	Кампанію викрито, але вона продовжується
2020	Націлювання на журналістів та медіа	Розширення інформаційної війни	Зламані новинні сайти для поширення дезінформації
2020	Націлювання на білоруську опозицію	Внутрішньополітичні операції	Компрометація опозиційних структур

Оцінка: Ранній етап, що характеризується базовими операціями кібершпигунства у поєднанні з формуванням кампаній дезінформації. Група створює операційну інфраструктуру та розвиває можливості націлювання.

Фаза 2: Атрибуція та ескалація (2021–2022)

Дата	Подія	Контекст	Вплив
квітень 2021	Mandiant пов’язує UNC1151 із Ghostwriter	Початок публічної атрибуції	Зростає рівень викриття операцій
вересень 2021	Уряд Німеччини приписує діяльність російському ГРУ	Міжнародна атрибуція	ЄС погрожує санкціями
вересень 2021	Під атакою 4 350 email-акаунтів	Ескалація збору облікових даних	Компрометація email керівника апарату прем’єр-міністра Польщі
вересень 2021	Компрометація email Міхала Дворчика	Високопрофільне націлювання	Порушення роботи польського уряду
січень 2022	Дефейс понад 70 урядових сайтів України	Передінвазійні операції	Початок психологічних операцій
лютий 2022	Масовий фішинг українських військових	Операції підтримки вторгнення	Отримано сотні військових облікових даних
лютий 2022	Операція Asylum Ambuscade	Націлювання на європейські уряди	Компрометація приватних email українських військових
березень 2022	Розгортання MicroBackdoor	Пост-експлуатаційна персистентність	Встановлено бекдор-доступ

березень 2022	Націлювання на польський уряд та військові структури	Націлювання на союзників НАТО	Тривалі фішингові кампанії

Оцінка: Фаза 2 відзначається значною ескалацією, публічною атрибуцією, міжнародною реакцією та інтеграцією з операціями під час вторгнення в Україну. Група демонструє координацію з російськими військовими операціями.

Фаза 3: Інтеграція гібридної війни (2023–2024)

Дата	Подія	Контекст	Вплив
2023	Продовження націлювання на українські військові структури	Підтримка триваючого конфлікту	Безперервні операції кібершпигунства
2023	Націлювання на оборонних підрядників НАТО	Фокус на ланцюгах постачання	Збір інформації про спроможності НАТО
2024	Розгортання шкідливого ПЗ PicassoLoader	Розробка кастомного шкідливого ПЗ	Ексклюзивний завантажувач Ghostwriter
червень 2024	Звіт Fortinet про шкідливі XLS-документи з макросами	Доставка через Excel	Використання Cobalt Strike проти українських військових
2024	Націлювання на білоруську опозицію	Внутрішньополітичні операції	Компрометація опозиційних структур
2024	Продовження кампаній дезінформації	Інформаційна війна	Координація з кіберопераціями

Оцінка: Фаза 3 демонструє стабільно високий темп операційної діяльності, розвиток шкідливих інструментів та подальшу інтеграцію елементів гібридної війни.

Фаза 4: Розвинена персистентність і деструктивні операції (2025–2026)

Дата	Подія	Контекст	Вплив
лютий 2025	Початок кампанії FrostyNeighbor	Нове позначення кампанії	Троянізовані архіви для атак на урядові структури Україн
травень 2025	Експлуатація вразливості CVE-2024-42009	Підвищення привілеїв у FortiEDR	Розгортання JavaScript-завантажувача
серпень 2025	Розгортання маяка (beacon) Cobalt Strike	Фреймворк для постексплуатаційних дій	Розвинені механізми персистентності
липень 2025	HarfangLab виявляє кластери шкідливих архівів	Продовження кампаній націлювання	Під атакою Україна та Польща
травень 2026	Кампанія з фішинговим шкідливим ПЗ Prometheus	Найновіша зафіксована активність	Націлювання на урядові структури України
травень 2026	OYSTERFRESH/OYSTERBLUES/ OYSTERSHUCK розгортання	Просунуті варіанти шкідливого ПЗ	Персистентність на основі реєстру Windows

Оцінка: Фаза 4 демонструє високий рівень технічних можливостей, включаючи багатоступеневу доставку шкідливого ПЗ, використання власних завантажувачів та складних механізмів персистентності. Незважаючи на публічну атрибуцію та санкції, угруповання зберігає стабільно високий темп операційної діяльності.

АНАЛІЗ НАЦІЛЮВАННЯ

Основні категорії цілей

1. Урядові та військові структури

Основні цілі:

- Українські урядові міністерства та агентства
- Українські військові та командні структури
- Польський уряд та військові структури
- Уряди країн Балтії (Литва, Латвія, Естонія)
- Уряд Німеччини (парламент, міністерства)
- Уряд Франції
- Уряд Великої Британії
- Інфраструктура командування НАТО

Методи націлювання:

- Цільові фішингові кампанії (spear-phishing) проти урядових посадовців
- Викрадення облікових даних через фейкові сторінки входу
- Розгортання шкідливого ПЗ через «озброєні» документи
- Компрометація ланцюгів постачання через урядових підрядників
- Використання зламаних email-акаунтів для вторинного фішингу

Цілі операцій:

- Збір розвідувальної інформації про військові спроможності
- Націлювання на персонал для вербування або компрометації
- Дестабілізація роботи урядових структур
- Підтримка військових операцій (вторгнення в Україну)

---

2. Організації, пов’язані з НАТО

Основні цілі:

- Уряди країн-членів НАТО
- Інфраструктура командування НАТО
- Оборонні підрядники, пов’язані з НАТО
- Аналітичні центри та дослідницькі організації, пов’язані з НАТО
- Військові навчання та операції НАТО

Методи націлювання:

- Фішингові кампанії проти персоналу НАТО
- Компрометація ланцюгів постачання підрядників НАТО
- Викрадення облікових даних у структур, пов’язаних із НАТО
- Розгортання шкідливого ПЗ проти інфраструктури НАТО

Цілі:

- Збір розвідувальної інформації про спроможності НАТО.
- Порушення операцій НАТО.
- Підтримка російських і білоруських військових цілей.

---

3. Медіа та інформаційні організації

Основні цілі:

- Новинні організації та журналісти.
- Медіа у країнах Східної Європи.
- Міжнародні медіаорганізації.
- Платформи соціальних мереж.
- Онлайн-форуми та дискусійні майданчики.

Методи націлювання:

- Компрометація вебсайтів для поширення дезінформації.
- Націлювання на журналістів з метою викрадення облікових даних.
- Створення та поширення фейкових новинних матеріалів.
- Компрометація акаунтів у соціальних мережах.
- Координовані кампанії з дезінформації.

Цілі:

- Поширення дезінформації.
- Проведення психологічних операцій, спрямованих на військовослужбовців.
- Проведення операцій впливу, спрямованих на цивільне населення.
- Дискредитація НАТО та західних урядів.

---

4. Білоруська опозиція

Основні цілі:

- Опозиційні політичні партії
- Опозиційні активісти та лідери
- Опозиційні медіа-організації
- Організації підтримки опозиції
- Діаспорні спільноти

Методи націлювання:

- Фішингові кампанії проти членів опозиції
- Викрадення облікових даних у опозиційних організацій
- Розгортання шкідливого ПЗ проти інфраструктури опозиції
- Стеження за діяльністю опозиції

Цілі:

- Внутрішній політичний контроль
- Придушення опозиційної діяльності
- Збір розвідувальної інформації про опозиційні рухи
- Підтримка режиму Лукашенка

Підтримати діяльність організації: https://donate.shum-ng.org/

5. Критична інфраструктура

Основні цілі:

- Енергетична інфраструктура (електромережі, підстанції)
- Телекомунікаційна інфраструктура
- Транспортна інфраструктура
- Системи очищення води
- Урядова комунікаційна інфраструктура

Методи націлювання:

- Розвідка та збір розвідувальної інформації
- Викрадення облікових даних у операторів інфраструктури
- Розгортання шкідливого ПЗ проти інфраструктурних систем
- Компрометація ланцюгів постачання інфраструктурних провайдерів

Цілі:

- Збір розвідувальної інформації про критичну інфраструктуру
- Потенційні можливості для порушення роботи
- Підтримка військових операцій

Географічні патерни націлювання

Основний географічний фокус:

1. Україна — інтенсивне націлювання на урядові, військові та цивільні структури
2. Польща — систематичне націлювання на уряд, військові та оборонних підрядників
3. Країни Балтії — Литва, Латвія, Естонія (урядові та військові структури)
4. Німеччина — націлювання на уряд та парламент
5. Франція — націлювання на урядові структури
6. Велика Британія — обмежене, але постійне націлювання
7. Білорусь — націлювання на опозиційні структури

Вторинний географічний фокус:

- Інші країни-члени НАТО
- Країни, пов’язані з НАТО
- Інституції ЄС
- Міжнародні організації

Обґрунтування цілей

Стратегічні цілі:

1. Побоювання розширення НАТО — націлювання відображає державне занепокоєння щодо розширення НАТО
2. Конфлікт в Україні — інтенсивне націлювання під час вторгнення 2022 року; підтримка російських військових операцій
3. Регіональний вплив — операції підтримують зусилля Білорусі та Росії щодо збереження регіонального впливу
4. Розвідувальна перевага — збір інформації про військові спроможності НАТО та оборонну позицію
5. Гібридна війна — кібероперації інтегровані з дезінформацією та психологічними операціями

РОДИ ШКІДЛИВОГО ПЗ ТА ІНСТРУМЕНТИ

Основні родини шкідливого ПЗ

1. PicassoLoader

Класифікація: Кастомний завантажувач (ексклюзивний для Ghostwriter/UNC1151)

Опис:

- Кастомне шкідливе ПЗ-завантажувач, ексклюзивно пов’язане з Ghostwriter/UNC1151.
- Розроблене спеціально для операцій Ghostwriter.
- Використовувалося в кампаніях 2024–2026 років проти українських військових та урядових структур.

Можливості:

- Багатоступенева доставка шкідливого ПЗ
- Виконання команд
- Передача та викрадення файлів
- Механізми персистентності
- Модифікація реєстру

Методи доставки:

- «Озброєні» Excel-файли з VBA-макросами
- Троянізовані архіви
- JavaScript-завантажувачі
- Документи Office з макросами

Недавні варіанти:

- 2024: доставка через Excel з обфускацією MacroPack
- 2025: доставка через JavaScript з експлуатацією CVE-2024-42009
- 2026: розширені багатоступеневі ланцюги доставки

2. Cobalt Strike

Класифікація: Фреймворк пост-експлуатації (Post-Exploitation Framework)

Опис:

- Комерційний інструмент для тестування на проникнення, який був перетворений Ghostwriter на зброю для пост-експлуатаційних дій.
- Розгортається після початкової компрометації системи.

Можливості:

- Виконання команд
- Рух у межах мережі (lateral movement)
- Підвищення привілеїв
- Ексфільтрація даних
- Механізми персистентності

Розгортання:

- серпень 2025: розгортання beacon Cobalt Strike (mrasp86.dll)
- Ідентифіковано як Win32.Backdoor.Ratenjay
- Розширені техніки ухилення, включаючи зловживання WriteProcessMemory
- Мережева C&C (command-and-control) комунікація

Imphash: a21e1c2781a36ff1ce3748551ba69d41

3. MicroBackdoor

Класифікація: Кастомний бекдор

Опис:

- Кастомне шкідливе ПЗ типу бекдору, яке використовувалося в кампаніях 2022 року.
- Розгортався на системах уряду України.
- Забезпечує віддалений доступ та виконання команд.

Можливості:

- Віддалене виконання команд
- Передача файлів
- Розвідка системи
- Механізми персистентності

Розгортання:

- березень 2022: розгортання на урядових системах України
- Посткомпрометаційна персистентність
- Забезпечення довготривалого доступу

4. Prometheus Phishing Malware

Класифікація: Фішингова шкідлива програмна платформа (Phishing Malware Suite)

Опис:

- Найновіша родина шкідливого ПЗ (травень 2026 року).
- Багатокомпонентний фішинговий набір інструментів.
- Націлений на урядові структури України.

Компоненти:

- OYSTERFRESH — початкове корисне навантаження; відображає приманковий (decoy) документ
- OYSTERBLUES — збирач системної інформації; персистентність на основі реєстру
- OYSTERSHUCK — компонент-декодер
- Фінальне навантаження — beacon Cobalt Strike для пост-експлуатації

Доставка:

- Email із PDF-вкладенням
- Посилання на ZIP-архів із JavaScript
- Багатоступенева ланцюгова доставка

Можливості:

- Збір системної інформації
- Персистентність через реєстр
- Відображення приманкових документів
- Розгортання Cobalt Strike

5. Additional Malware Families

Trojan.Casdet

- Троян-завантажувач
- Виявлений у варіантах svhost.dll і Dwnldr.dll
- Багатоступенева доставка шкідливого ПЗ

Infostealer.Tinba

- Шкідливе ПЗ для викрадення інформації
- Викрадення облікових даних
- Витяг даних із браузера

Trojan.Alevaul

- HTTP C&C агент
- Виконання команд
- Ексфільтрація даних

Trojan.Etset

- Виявлений у RAR-архівах
- Багатоступенева доставка

Win32.Trojan.Generic

- Генеричні варіанти трояна
- Завантажувачі початкової стадії
- Троянізовані архіви

SLoad/SDrop

- JavaScript-завантажувач
- Завантажувач великих файлів
- Багатоступенева доставка

МЕТОДИ ДОСТАВКИ ШКІДЛИВОГО ПЗ

1. «Озброєні» Excel-файли

Метод:

- Excel-робочі книги (.XLS, .XLSX) з VBA-макросами
- Обфускація MacroPack
- Оманливі українськомовні схеми іменування

Приклади:

- “certificate.zip” з шкідливими скриптами
- “53_7.03.2026_R.rar” з троянами
- Назви документів на урядову тематику

Ланцюг виконання:

1. Користувач відкриває Excel-файл
2. Виконується VBA-макрос
3. Розгортається вбудований .NET-завантажувач
4. Застосовується обфускація ConfuserEx
5. Багатоступенева доставка шкідливого ПЗ

2. Троянізовані архіви

Метод:

- ZIP і RAR архіви з оманливими назвами
- Містять шкідливі скрипти та DLL-завантажувачі
- JavaScript-завантажувачі

Приклади:

- “certificate.zip” — Trojan.Generic
- “53_7.03.2026_R.rar” — Trojan.Etset
- Архіви з урядовими документами

Ланцюг виконання:

1. Користувач розпаковує архів
2. Виконується шкідливий скрипт
3. Розгортається DLL-завантажувач
4. Багатоступенева доставка шкідливого ПЗ

3. JavaScript-завантажувачі

Метод:

- JavaScript-файли (.JS) зі шкідливою функціональністю
- Експлуатація CVE-2024-42009
- Сімейство завантажувачів Nemucod

Приклади:

- “Delivery report.js” — експлуатація CVE-2024-42009
- OYSTERFRESH — відображення приманкового документа
- Персистентність на основі реєстру

Ланцюг виконання:

1. Виконується JavaScript-файл
2. Підвищення привілеїв через CVE-2024-42009
3. Розгортання корисного навантаження
4. Персистентність через реєстр

---

4. Email-орієнтована доставка

Метод:

- Spear-phishing email з шкідливими вкладеннями
- PDF-вкладення, що містять посилання на шкідливі архіви
- Скомпрометовані email-акаунти для вторинного фішингу

Приклади:

- Травень 2026: фішингова кампанія Prometheus
- Email із PDF-вкладенням
- Посилання на ZIP-архів із JavaScript

Ланцюг виконання:

1. Користувач отримує фішинговий email
2. Відкриває PDF-вкладення
3. Переходить за посиланням на шкідливий архів
4. Завантажує та запускає шкідливе ПЗ
5. Багатоступенева ланцюгова доставка

ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

Хеші файлів (SHA-256):

- 614a6a214d8cca8dea65727ea50a6c49234048295dd404669a9b131c5b6a7757 (svhost.dll - Trojan.Casdet)
- b26349b7583a6b09f33b74b2d03894c6d6860650b592310450b94b18b335c41a (Dwnldr.dll - Trojan.Casdet)
- ca49d90ea29b7c7ba548c4fe902f2b8c24372bc3e3a7d5b4fd9ac0c2eef04cb4 (Dwnldr_.dll - Infostealer.Tinba)
- e132c9f60b893ee053caa4cbfa8f85d85645b24efcdb217af343912f5ef0d518 (Dwnldr__.dll - Infostealer.Tinba)
- 70cea07c972a30597cda7a1d3cd4cd8f75acad75940ca311a5a2033e6a1dd149 (Delivery report.js - Nemucod Downloader)
- 3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d (mrasp86.dll - Cobalt Strike Beacon)
- 5fa19aa32776b6ab45a99a851746fbe189f7a668daf82f3965225c1a2f8b9d36 (Trojan.Alevaul)
- bd680322ef5ebbf87cc3fad49702e948d206f85ae90eb334acf24e856e60ba78 (certificate.zip - Trojan.Generic)
- 7b859ed1d379b5ecc4118df9f3de628e036c154dd69748b1505c38eaf2cf8e47 (53_7.03.2026_R.rar - Trojan.Etset)
- ce1822f4150fb641b445c3b85f990ecbe68bf30ee3ee2cc8e5e92f45d8ae3937 (certificate.js - SLoad/SDrop)

Значення Imphash:

- dae02f32a21e03ce65412f6e56942daa (кілька DLL-зразків - Dwnldr/svhost variants)
- a21e1c2781a36ff1ce3748551ba69d41 (Cobalt Strike зразки)

SSDEEP-хеші:

- 12288:67E86soP/Bzbeb9JEIgukfyKpp8jB8wmXCZXnFXxR6boBxJwtpgpfHadJbpVBbpI:rXBfeMGgpn8ZmAhQ0vD/adJbpVBbpVi (Cobalt Strike)
- 24:+Gx4IAxz4Wt4BmS/xNCHOY7vRczArKCAHaCKBYj88YjCr1QEDn5HBMycnAbE9ew:+Gx41z7pS/xiOovRc8KqCKajHBMycgEf (JavaScript downloader)

TACTICS, TECHNIQUES & PROCEDURES (TTPs)

ВІДПОВІДНІСТЬ MITRE ATT&CK (MAPPING)

Початковий доступ

T1566.002 — Фішинг: цільовий фішинг із посиланням

- Цільові фішингові електронні листи зі шкідливими посиланнями
- Сторінки для викрадення облікових даних, що імітують легітимні портали
- Термінові повідомлення, що експлуатують авторитет
- Рівень успішності: 15–25% переходів у цільових кампаніях

T1566.001 — Фішинг: цільовий фішинг із вкладенням

- «Озброєні» документи Office (Excel, Word)
- Файли з VBA макросами
- Троянізовані архіви (ZIP, RAR)
- Оманливі україномовні назви

T1195.002 — Компрометація ланцюга постачання

- Компрометація оборонних підрядників
- Доступ до спроможностей НАТО через ланцюг постачання
- Націлювання на ПЗ та оновлення підрядників

T1199 — Довірені відносини

- Експлуатація довірених відносин з військовим персоналом
- Соціальна інженерія щодо урядових посадовців
- Імітація колег та керівників

Персистентність (Persistence)

T1547.001 — Автозапуск під час завантаження або входу: ключі реєстру Run

- Модифікація реєстру для забезпечення персистентності шкідливого ПЗ
- HKLM\Software\Microsoft\Windows\Run ключі
- Створення запланованих завдань
- Інсталяція сервісів

T1547.009 — Автозапуск під час завантаження або входу: модифікація ярликів

- Модифікація .lnk файлів
- Маніпуляції зі Startup папкою

T1136.001 — Створення облікового запису: локальний акаунт

- Створення прихованих локальних користувацьких облікових записів
- Персистентність через створення облікових записів

Доступ до облікових даних

T1110.004 — Брутфорс: credential stuffing

- Credential stuffing-атаки проти військових порталів
- Повторне використання облікових даних з попередніх витоків
- Масове тестування облікових даних

T1187 — Примусовий фішинг

- Фішингові листи з терміновими військовими/НАТО повідомленнями
- Імітація військового командування
- Фейкові NATO security alerts

T1056.004 — Моніторинг: перехоплення через API облікових даних

- Кейлогінг і викрадення облікових даних
- Зчитування пам’яті для отримання облікових даних
- Витяг даних браузера

T1111 — Перехоплення багатофакторної автентифікації (MFA)

- Перехоплення MFA кодів
- Фішингові сторінки для захоплення MFA кодів
- Спроби SIM swapping

Розвідка (Discovery)

T1087.002 — Виявлення облікових записів: доменні облікові записи

- Перелік доменних облікових записів
- Запити Active Directory
- Перелік користувачів для націлювання

T1010 — Виявлення вікон застосунків

- Виявлення запущених застосунків
- Ідентифікація програмного забезпечення безпеки
- Виявлення військових застосунків

T1518.001 — Виявлення ПЗ: виявлення програмного забезпечення безпеки

- Виявлення антивірусів та EDR рішень
- Визначення та обходження захисного ПЗ

T1082 — Виявлення інформації про систему

- Збір інформації про версію ОС, апаратне забезпечення, мережеву конфігурацію
- Розвідувальна інформація про систему

Collection

T1123 — Аудіозахоплення

- Запис аудіо з компрометованих систем
- Доступ до мікрофона

T1119 — Автоматизована ексфільтрація

- Автоматизована ексфільтрація даних
- Заплановані передачі даних

T1115 — Дані з буфера обміну (clipboard)

- Захоплення даних буфера обміну
- Викрадення облікових даних із clipboard

T1005 — Дані з локальної системи

- Збір документів, електронної пошти, конфігураційних файлів
- Витяг даних з локальної системи

T1039 — Дані з мережевих спільних дисків

- Доступ до військових мережевих ресурсів
- Перелік мережевих дисків та збір даних

T1114.001 — Збір електронної пошти: локальна пошта

- Збір електронної пошти з Outlook, Thunderbird
- Доступ через IMAP після компрометації
- Витяг адресної книги для вторинного фішингу

Командування та керування

T1071.001 — Протокол прикладного рівня: HTTP/HTTPS

- C&C-комунікація через HTTPS
- HTTP POST для ексфільтрації даних
- Зашифровані C&C-канали

T1071.004 — Протокол прикладного рівня: DNS

- DNS-канал C&C-комунікації
- DNS-тунелювання

T1008 — Резервні канали

- Кілька C&C-каналів для резервування
- Механізми переходу на запасні канали

T1105 — Передача інструментів через вхідні канали (Ingress Tool Transfer)

- Передача інструментів і шкідливого ПЗ з C&C
- Багатоступенева доставка шкідливого ПЗ

Ексфільтрація

T1020 — Автоматизована ексфільтрація

- Автоматизована ексфільтрація даних
- Заплановані передачі даних

T1048.001 — Ексфільтрація через альтернативний протокол: HTTP/HTTPS

- Ексфільтрація даних через HTTPS
- Зашифровані канали ексфільтрації

T1041 — Ексфільтрація через C&C канал

- Ексфільтрація даних через встановлений C&C
- Використання каналу команд для передачі даних

Ухилення від захисту

T1548.002 — Зловживання механізмом контролю підвищення привілеїв: обхід User Account Control

- Обхід UAC для підвищення привілеїв
- Експлуатація механізмів підвищення привілеїв

T1140 — Деобфускація/декодування файлів або інформації

- Обфускація та деобфускація коду шкідливого ПЗ
- Обфускація ConfuserEx
- Обфускація MacroPack

T1562.001 — Послаблення захисту: вимкнення або модифікація засобів захисту

- Вимкнення програмного забезпечення безпеки
- Вимкнення антивірусів та EDR

T1070.001 — Видалення індикаторів: очищення журналів подій Windows

- Очищення журналів подій
- Видалення судово-криміналістичних доказів

T1036.005 — Маскування: імітація легітимної назви або розташування

- Маскування шкідливого ПЗ під легітимні файли
- Оманливі назви файлів

T1112 — Модифікація реєстру

- Модифікація реєстру для персистентності та ухилення від захисту
- Персистентність на основі реєстру

T1027 — Обфусковані файли або інформація

- Обфускація коду шкідливого ПЗ
- Шифрування та кодування

T1550.002 — Використання альтернативних засобів автентифікації: Pass the Hash

- Атаки Pass-the-Hash
- Повторне використання облікових даних для латерального переміщення

T1078.002 — Валідні облікові записи: доменні облікові записи

- Використання скомпрометованих доменних облікових записів
- Зловживання обліковими даними

Вплив

T1561 — Знищення даних на диску (Disk Wipe)

- Знищення даних на диску з метою деструктивного впливу
- Знищення файлової системи
- Знищення розділів диска

T1491.001 — Дефейс: внутрішній дефейс

- Внутрішній дефейс системи
- Дефейс вебсайтів (понад 70 урядових вебсайтів України, січень 2022 року)

ІНФРАСТРУКТУРА ТА ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

Інфраструктура командування та керування

Відомі C&C-домени:

- i.ua-passport.space
- id.bigmir.space
- Додаткові домени, виявлені у звітах про кіберзагрози

Характеристики інфраструктури:

- Використання доменів у зоні .shop
- Хостинг через білоруських інтернет-провайдерів
- HTTP C&C-комунікація
- Кілька C&C-каналів із резервними механізмами
- Реєстрація доменів через білоруських реєстраторів

C&C-комунікація:

- HTTPS-зашифровані канали
- HTTP POST для ексфільтрації даних
- DNS-орієнтована C&C-комунікація
- Мережева beacon-комунікація

Фішингова інфраструктура

Патерни фішингових доменів:

- Домени-двійники, що імітують організації НАТО та військові структури
- Фальшиві домени урядових порталів
- Сторінки для викрадення облікових даних
- Розміщення у хостинг-провайдерів Східної Європи

Email-інфраструктура:

- Безкоштовні поштові сервіси (Gmail, Yandex)
- Скомпрометовані легітимні email-акаунти
- Підроблені адреси відправників
- Масове розсилання електронних листів

ОСТАННІ КАМПАНІЇ ТА ПРИКЛАДИ ОПЕРАЦІЙ

Кампанія 1: FrostyNeighbor (лютий–травень 2026 року)

Назва кампанії: FrostyNeighbor
Часові рамки: 26 лютого 2025 року – 14 травня 2026 року

Цілі:

- Урядові установи України
- Організації білоруської опозиції
- Урядові системи Польщі

Ланцюг атаки:

1. Початковий доступ: троянізовані ZIP/RAR-архіви з оманливими назвами
2. Доставка шкідливого ПЗ: Trojan.Generic, Trojan.Etset, Infostealer.Tinba
3. Персистентність: модифікація реєстру, заплановані завдання
4. Латеральне переміщення: повторне використання облікових даних, перерахування мережі
5. Ексфільтрація даних: системна інформація, документи, комунікації

Використане шкідливе ПЗ:

- Trojan.Casdet (svhost.dll, Dwnldr.dll)
- Infostealer.Tinba (Dwnldr_.dll, Dwnldr__.dll)
- Trojan.Generic (certificate.zip)
- Trojan.Etset (53_7.03.2026_R.rar)

Ключові індикатори:

- Imphash: dae02f32a21e03ce65412f6e56942daa
- Розміри файлів і часові мітки, що відповідають кампанії
- Україномовні назви документів
- Багатоступеневі ланцюги доставки

Вплив:

- Компрометація урядових систем України
- Викрадення облікових даних військовослужбовців
- Збір розвідувальної інформації про діяльність урядових органів
- Потенціал для подальшої ескалації

Оператори інфраструктури

Ідентифікований оператор: Andrey Korinets

- Реальна особа, встановлена за допомогою OSINT
- Створював інфраструктуру шкідливих доменів
- Забезпечував інфраструктурну підтримку для ФСБ Росії та російських військових
- Перебуває під міжнародними санкціями
- Демонструє професійний рівень операційної інфраструктури

Індикатори компрометації

Хеші файлів (SHA-256):
[Див. розділ «Родини шкідливого ПЗ» для повного списку]

Значення Imphash:

- dae02f32a21e03ce65412f6e56942daa
- a21e1c2781a36ff1ce3748551ba69d41

Домени:

- i.ua-passport.space
- id.bigmir.space
- Патерн доменів .shop

Приманки в електронних листах:

- **“**NATO Security Alert: Urgent Action Required”
- “Military Exercise Notification”
- “Government Personnel Update”
- “Defence Contractor Communication”
- “System Security Update”

Схеми найменування файлів:

- “certificate.zip”
- “53_7.03.2026_R.rar”
- “Delivery report.js”
- Назви документів на урядову тематику
- Україномовні схеми найменування

Кампанія 2: Експлуатація CVE-2024-42009 (травень 2025 року)

Назва кампанії: Експлуатація підвищення привілеїв у FortiEDR
Часові рамки: 30 травня 2025 року – дотепер
Вразливість: CVE-2024-42009 (підвищення привілеїв у Fortinet FortiEDR)

Цілі:

- Організації з вразливими розгортаннями FortiEDR
- Урядові установи України
- Організації, пов’язані з НАТО

Ланцюг атаки:

1. Початковий доступ: доставка JavaScript-завантажувача
2. Експлуатація: підвищення привілеїв через CVE-2024-42009
3. Доставка корисного навантаження: сімейство завантажувачів Nemucod
4. Багатоступенева доставка: додаткові етапи шкідливого ПЗ
5. Персистентність: персистентність на основі реєстру

Використане шкідливе ПЗ:

- Script-WScript.Downloader.Nemucod
- Експлойт для CVE-2024-42009
- Багатоступеневі корисні навантаження шкідливого ПЗ

Ключові індикатори:

- Файл: “Delivery report.js” (1361 байт)
- SHA-256: 70cea07c972a30597cda7a1d3cd4cd8f75acad75940ca311a5a2033e6a1dd149
- SSDEEP: 24:+Gx4IAxz4Wt4BmS/xNCHOY7vRczArKCAHaCKBYj88YjCr1QEDn5HBMycnAbE9ew: +Gx41z7pS/xiOovRc8KqCKajHBMycgEf
- Виявлення ReversingLabs: Script-WScript.Downloader.Nemucod

Вплив:

- Підвищення привілеїв на кінцевих точках FortiEDR
- Розгортання багатоступеневого шкідливого ПЗ
- Потенціал для латерального переміщення
- Довготривала персистентність

Кампанія 3: Фішингова кампанія Prometheus (травень 2026 року)

Назва кампанії: Фішинговий комплекс шкідливого ПЗ Prometheus
Часові рамки: травень 2026 року – дотепер

Цілі:

- Урядові установи України
- Військовослужбовці
- Урядові посадові особи

Ланцюг атаки:

1. Початковий доступ: електронний лист із PDF-вкладенням
2. Приманка: PDF містить посилання на шкідливий ZIP-архів
3. Виконання: запуск JavaScript-файлу
4. Відволікання: OYSTERFRESH відображає підроблений документ
5. Персистентність: OYSTERBLUES записує дані до реєстру
6. Розвідка: збір системної інформації
7. Постексплуатація: декодер OYSTERSHUCK, розгортання Cobalt Strike

Компоненти шкідливого ПЗ:

- OYSTERFRESH — початкове корисне навантаження, відображення документа-приманки
- OYSTERBLUES — збір системної інформації, персистентність через реєстр
- OYSTERSHUCK — компонент-декодер
- Cobalt Strike — фреймворк для постексплуатації

Ключові індикатори:

- Доставка електронною поштою з PDF-вкладенням
- ZIP-архів, що містить JavaScript
- Персистентність на основі реєстру
- Багатоступеневий ланцюг доставки

Вплив:

- Збір системної інформації
- Потенціал для викрадення облікових даних
- Доступ на етапі постексплуатації через Cobalt Strike
- Довготривала персистентність

Кампанія 4: Розгортання Cobalt Strike (серпень 2025 року)

Назва кампанії: Постексплуатація за допомогою Cobalt Strike
Часові рамки: 22 серпня 2025 року

Цілі:

- Скомпрометовані урядові мережі України
- Мережі організацій білоруської опозиції

Ланцюг атаки:

1. Початкова компрометація: через попередні етапи шкідливого ПЗ
2. Розгортання Beacon: mrasp86.dll (Cobalt Strike)
3. Персистентність: розширені методи ухилення від виявлення
4. Латеральне переміщення: розвідка мережі
5. Ексфільтрація даних: виконання команд і передача файлів

Використане шкідливе ПЗ:

- Cobalt Strike Beacon (Win32.Backdoor.Ratenjay)
- mrasp86.dll (ім’я файлу)
- Розширені методи ухилення від виявлення

Ключові індикатори:

- SHA-256: 3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d
- Imphash: a21e1c2781a36ff1ce3748551ba69d41
- SSDEEP: 12288:67E86soP/Bzbeb9JEIgukfyKpp8jB8wmXCZXnFXxR6boBxJwtpgpfHadJbpVBbpI:rXBfeMGgpn8ZmAhQ0vD/adJbpVBbpVi
- Сигнатура: Cobalt Strike (підписано)

Вплив:

- Доступ на етапі постексплуатації
- Можливість латерального переміщення
- Довготривала персистентність
- Розширені можливості виконання команд

Кампанія 5: Кампанія проти військових Бразилії з використанням Zimbra Zero-Day (жовтень 2025 року)

Назва кампанії: Шпигунська операція проти військових Бразилії з використанням Zimbra Zero-Day
Статус: Атрибуція невизначена
Часові рамки: жовтень 2025 року

Цілі:

- Військовослужбовці армії Бразилії
- Військові організації Бразилії
- Комунікаційна інфраструктура, пов’язана з оборонною сферою

Ланцюг атаки:

1. Початковий доступ: доставка шкідливих файлів календарних запрошень .ICS
2. Експлуатація: використання раніше невідомої вразливості Zero-Day у Zimbra
3. Виконання коду: віддалене виконання коду на цільових серверах Zimbra
4. Отримання облікових даних: збір автентифікаційних даних та інформації про користувачів
5. Ексфільтрація даних: передача зібраної інформації через інфраструктуру на базі Proton

Використане шкідливе ПЗ / інструменти:

- Шкідливі файли .ICS (iCalendar)
- Zero-Day експлойт для Zimbra Collaboration Suite
- Кастомні інструменти для постексплуатації
- Інфраструктура на базі Proton для ексфільтрації даних

Ключові індикатори:

- Шкідливі календарні вкладення .ICS
- Експлуатація Zimbra Collaboration Suite
- Використання інфраструктури Proton для операційної комунікації
- Націлювання на військовослужбовців і військові організації
- Шпигунська діяльність, орієнтована на збір інформації

Вплив:

- Несанкціонований доступ до військових комунікацій
- Потенційне розкриття конфіденційної оборонної інформації
- Збір розвідувальної інформації щодо військових цілей
- Демонстрація розвинених можливостей експлуатації Zero-Day вразливостей
- Підвищений ризик для поштової інфраструктури урядових та оборонних установ

Оцінка атрибуції:

- Атрибуція залишається невизначеною
- Можлива операція державного кібершпигунства
- Деякі джерела припускають можливу причетність акторів, пов’язаних із Білоруссю
- Альтернативні гіпотези включають операторів, пов’язаних із російськими спецслужбами, або спільну операційну діяльність
- Рівень впевненості: низький

Значення:

- Перше публічно відоме використання Zero-Day вразливості Zimbra проти військових цілей Бразилії
- Демонструє розвинені можливості експлуатації урядової інфраструктури
- Підкреслює збереження невизначеності щодо білоруських і російських операцій кібершпигунства
- Має значення для ширших оцінок кіберрозвідувальної діяльності, спрямованої на військові цілі

ОПЕРАЦІЇ З ДЕЗІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОЇ ВІЙНИ

Кампанія дезінформації Ghostwriter

Назва кампанії: Operation Ghostwriter (інформаційна війна)
Часові рамки: липень 2020 року – дотепер

Цілі:

- Дискредитація НАТО та західних урядів
- Дестабілізація виборів і політичних процесів
- Послаблення західної підтримки України
- Психологічні операції, спрямовані на військовослужбовців
- Операції впливу, спрямовані на цивільне населення

Методи:

- Компрометація вебсайтів для поширення дезінформації
- Створення та поширення фейкових новин
- Компрометація акаунтів у соціальних мережах
- Координовані кампанії з дезінформації
- Імперсонація урядових посадових осіб
- Операції під чужим прапором (False Flag)

Цілі атак:

- Держави-члени НАТО
- Уряди країн Східної Європи
- Медіаорганізації
- Цивільне населення
- Військовослужбовці

Основні кампанії:

1. Дезінформація перед вторгненням (2021–2022)

- Дискредитація розширення НАТО
- Психологічні операції, спрямовані на військових
- Підготовка до вторгнення в Україну

2. Дезінформація на підтримку вторгнення (2022)

- Обґрунтування військових операцій
- Дискредитація уряду України
- Психологічні операції, спрямовані на українських військових

3. Поточні дезінформаційні кампанії (2023–2026)

- Продовження дискредитації НАТО
- Підтримка інтересів Росії та Білорусі
- Психологічні операції, спрямовані на військовослужбовців

Інтеграція гібридної війни

Унікальна характеристика: Ghostwriter поєднує кібершпигунство з операціями з дезінформації.

Методи інтеграції:

1. Викрадення облікових даних для імперсонації

- Викрадені облікові дані використовуються для імперсонації урядових посадових осіб
- Скомпрометовані email-акаунти використовуються для вторинного фішингу
- Імперсонація для поширення дезінформації

2. Використання викрадених даних для дезінформації

- Ексфільтровані документи використовуються в кампаніях з дезінформації
- Вибіркове розкриття інформації з пропагандистською метою
- Маніпулювання контекстом для психологічного впливу

3. Координовані кампанії

- Кібероперації, синхронізовані з кампаніями з дезінформації
- Психологічні операції, спрямовані на військовослужбовців
- Операції впливу, спрямовані на цивільне населення

4. Маскування (російська військова доктрина введення в оману)

- Операції під чужим прапором (False Flag)
- Правдоподібне заперечення причетності (Plausible Deniability)
- Координовані кампанії з введення в оману

ОЦІНКА ЗАГРОЗИ ТА АНАЛІЗ РИЗИКІВ

Матриця ризиків

Ймовірність	Вплив	Рівень ризику	Сценарії
КРИТИЧНА	КРИТИЧНА	КРИТИЧНА	Пряме військове протистояння; розширення НАТО; ескалація конфлікту в Україні
ВИСОКА	КРИТИЧНА	КРИТИЧНА	Тривале кібершпигунство; компрометація ланцюга постачання; деструктивні операції
СЕРЕДНЯ	КРИТИЧНА	ВИСОКА	Кампанії з дезінформації; психологічні операції; порушення роботи інфраструктури
ВИСОКА	ВИСОКА	ВИСОКА	Викрадення облікових даних; розгортання шкідливого ПЗ; латеральне переміщення
СЕРЕДНЯ	ВИСОКА	СЕРЕДНЯ	Збір інформації; розвідка; розвиток націлювання

Сценарії загроз

Сценарій 1: Тригер у вигляді розширення НАТО

- Оголошення про розширення НАТО спричиняє ескалацію кібероперацій
- Інтенсивне націлювання на нові держави-члени НАТО
- Розгортання деструктивного шкідливого ПЗ
- Координовані кампанії з дезінформації
- Ймовірність: СЕРЕДНЬО-ВИСОКА | Вплив: КРИТИЧНИЙ

Сценарій 2: Ескалація конфлікту в Україні

- Ескалація конфлікту в Україні спричиняє посилення кібероперацій
- Деструктивні операції проти української інфраструктури
- Націлювання на інфраструктуру підтримки НАТО
- Координація з російськими військовими операціями
- Ймовірність: СЕРЕДНЬО-ВИСОКА | Вплив: КРИТИЧНИЙ

Сценарій 3: Компрометація ланцюга постачання

- Компрометація оборонних підрядників НАТО
- Отримання доступу до військових можливостей НАТО
- Збір розвідувальної інформації про системи НАТО
- Потенціал для проведення деструктивних операцій
- Ймовірність: ВИСОКА | Вплив: КРИТИЧНИЙ

Сценарій 4: Кампанія гібридної війни

- Координовані кібер-, інформаційні та кінетичні операції
- Націлювання на військовослужбовців і цивільне населення
- Психологічні операції та кампанії з дезінформації
- Порушення роботи інфраструктури
- Ймовірність: СЕРЕДНЯ | Вплив: КРИТИЧНИЙ

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ

Стратегічний рівень

1. Національна стратегія кіберзахисту

- Розробити комплексну стратегію протидії загрозам, спонсорованим державами
- Визначити чіткі ролі та відповідальність
- Виділити достатні ресурси для кіберзахисту
- Налагодити координацію з НАТО та союзними державами

2. Доктрина кібероборони

- Розробити доктрину протидії кіберзагрозам, спонсорованим державами
- Встановити правила застосування кібероперацій
- Визначити процедури ескалації для кіберінцидентів
- Налагодити координацію з НАТО

3. Обмін розвідувальною інформацією

- Налагодити обмін розвідувальною інформацією з НАТО та союзними державами
- Обмінюватися інформацією про загрози, пов’язані з Ghostwriter
- Координувати збір розвідувальної інформації про загрози
- Створити системи раннього попередження

4. Санкції та дипломатична відповідь

- Підтримувати міжнародні санкції проти Білорусі та Росії
- Координувати дипломатичну відповідь із НАТО
- Встановити наслідки для держав, що здійснюють спонсоровані державою кібероперації
- Підтримувати міжнародні норми, спрямовані проти кібератак

Операційний рівень

1. Проактивний пошук загроз (Threat Hunting)

- Виявлення індикаторів інфраструктури Ghostwriter
- Виявлення родин і варіантів шкідливого ПЗ
- Виявлення фішингової інфраструктури
- Виявлення ознак латерального переміщення та персистентності
- Виявлення шаблонів ексфільтрації даних

2. Розробка механізмів виявлення (Detection Engineering)

- Впровадження розширеної фільтрації електронної пошти та засобів виявлення загроз
- Розгортання систем Endpoint Detection and Response (EDR)
- Впровадження систем Network Detection and Response (NDR)
- Моніторинг відомих індикаторів компрометації (IOC) та характерних шаблонів
- Проведення навчання користувачів з питань кібербезпеки

3. Посилення захисту ідентичностей (Identity Hardening)

- Впровадження політик використання надійних паролів
- Впровадження багатофакторної автентифікації (MFA)
- Впровадження систем керування привілейованим доступом (PAM)
- Впровадження моніторингу облікових даних та системи сповіщень
- Впровадження сегментації облікових даних

4. Архітектура Zero Trust

- Впровадження сегментації мережі
- Впровадження принципу мінімально необхідних привілеїв
- Впровадження контролю безпеки та відповідності пристроїв вимогам
- Впровадження моніторингу доступу та системи сповіщень
- Впровадження процедур реагування на інциденти

Тактичний рівень

1. Виявлення за допомогою SIEM

- Сповіщення про з’єднання з білоруськими інтернет-провайдерами
- Сповіщення про DNS-запити до відомих C&C-доменів
- Сповіщення про доступ до фішингової інфраструктури
- Сповіщення про індикатори персистентності шкідливого ПЗ
- Сповіщення про індикатори викрадення облікових даних

2. Моніторинг IOC

- Моніторинг шаблонів реєстрації доменів
- Моніторинг шаблонів повторного використання IP-адрес
- Моніторинг відомих хешів файлів шкідливого ПЗ
- Моніторинг фішингових приманок і характерних шаблонів
- Моніторинг збоїв автентифікації електронної пошти

3. Виявлення на основі MITRE ATT&CK

- Виявлення фішингу та цільового фішингу (T1566)
- Виявлення спроб отримання облікових даних (T1110, T1187, T1056)
- Виявлення механізмів персистентності (T1547)
- Виявлення латерального переміщення (T1550, T1078)
- Виявлення ексфільтрації даних (T1020, T1048, T1041)

4. Гіпотези для Threat Hunting

- Гіпотеза 1: Інфраструктура Ghostwriter присутня в мережевому трафіку
- Гіпотеза 2: Скомпрометовані облікові дані використовуються для латерального переміщення
- Гіпотеза 3: На кінцевих пристроях присутні механізми персистентності шкідливого ПЗ
- Гіпотеза 4: Ексфільтрація даних здійснюється до відомої C&C-інфраструктури
- Гіпотеза 5: Військовослужбовці отримують доступ до фішингової інфраструктури

МАЙБУТНІ ПЕРСПЕКТИВИ ТА РИЗИКИ ЕСКАЛАЦІЇ

ЙМОВІРНА ЕВОЛЮЦІЯ

ТЕХНІЧНА ЕВОЛЮЦІЯ:

1. Розширене шкідливе ПЗ з можливостями ухилення на основі ШІ
2. Фішингові кампанії, керовані ШІ
3. Розширення націлювання на ланцюги постачання
4. Розробка деструктивного шкідливого ПЗ
5. Адаптація та еволюція інфраструктури

ОПЕРАЦІЙНА ЕВОЛЮЦІЯ:

1. Посилення координації з російськими загрозовими акторами
2. Розширення інтеграції гібридної війни
3. Ескалація психологічних операцій
4. Розширення націлювання на додаткові країни НАТО
5. Ескалація під час геополітичної напруги

РИЗИКИ ЕСКАЛАЦІЇ (12–24 МІСЯЦІ)

СЦЕНАРІЇ ВИСОКОГО РИЗИКУ

1. Розширення НАТО — подальше розширення НАТО може спровокувати ескалацію операцій

2. Ескалація конфлікту в Україні — загострення конфлікту в Україні може призвести до збільшення операцій

3. Військове протистояння — пряме військове зіткнення може спричинити деструктивні операції

4. Ескалація санкцій — посилення санкцій може викликати відповідні операції у відповідь

5. Кампанія гібридної війни — координована гібридна війна з поєднанням кібер-, інформаційних та кінетичних операцій

ОЦІНКА ЙМОВІРНОСТІ:

- Розширення НАТО: СЕРЕДНЬО-ВИСОКА
- Ескалація в Україні: СЕРЕДНЬО-ВИСОКА
- Військове протистояння: СЕРЕДНЯ
- Ескалація санкцій: СЕРЕДНЯ
- Гібридна війна: СЕРЕДНЬО-ВИСОКА

ПОТЕНЦІАЛ ФІШИНГУ З ВИКОРИСТАННЯМ ШІ

ТЕХНОЛОГІЇ, ЩО З’ЯВЛЯЮТЬСЯ (EMERGING CAPABILITIES)

1. Персоналізовані фішингові електронні листи, згенеровані ШІ
2. Клонування голосу для дзвінків-імперсонацій
3. Діпфейки для кампаній дезінформації
4. Автоматизована соціальна інженерія
5. Адаптивний фішинг на основі відповідей користувача

ОБОРОННІ НАСЛІДКИ (DEFENSIVE IMPLICATIONS)

- Потрібні розширені системи захисту електронної пошти
- Навчання користувачів щодо атак із використанням ШІ
- Механізми автентифікації, стійкі до атак із використанням ШІ
- Процедури реагування на інциденти з використанням ШІ-інструментів

ПРОГАЛИНИ В РОЗВІДЦІ ТА ОБМЕЖЕННЯ

ВІДОМІ ОБМЕЖЕННЯ

1. Невизначеність атрибуції — конкретні оперативні підрозділи та особи залишаються невстановленими

2. Оцінка можливостей — точні технічні можливості та розподіл ресурсів частково невідомі

3. Видимість інфраструктури — не вся інфраструктура може бути виявлена; деякі C&C-канали можуть залишатися невиявленими

4. Ідентифікація персоналу — конкретні особи, залучені до операцій, переважно невідомі

5. Механізми координації — точні механізми координації з російськими загрозовими акторами частково зрозумілі

ПРОГАЛИНИ В ЗБОРІ ДАНИХ

1. Внутрішні комунікації — обмежена видимість у планування операцій

2. Дані про персонал — обмежена інформація про конкретних осіб

3. Розподіл ресурсів — обмежена видимість механізмів фінансування

4. Прийняття рішень — обмежена видимість стратегічного планування

5. Російська координація — обмежена видимість механізмів координації

РЕКОМЕНДОВАНИЙ МОНІТОРИНГ

1. Еволюція інфраструктури — подальший моніторинг змін інфраструктури

2. Розвиток шкідливого ПЗ — подальший моніторинг нових варіантів шкідливого ПЗ

3. Патерни націлювання — подальший моніторинг розширення цілей

4. Російська координація — подальший моніторинг координації з російськими акторами

5. Операційний темп — подальший моніторинг ескалаційних патернів

ВИСНОВКИ

Ghostwriter/UNC1151 представляє собою **КРИТИЧНУ та стійку загрозу** для оборонних інституцій, військового персоналу та критичної інфраструктури, пов’язаних із НАТО. Демонстрована групою здатність, тривалий операційний темп і стратегічне узгодження з державними інтересами Білорусі та Росії вказують на довгострокову загрозу, що потребує комплексної та скоординованої оборонної відповіді.

Ключові висновки:

1. Ghostwriter є державним проєктом із ВИСОКОЮ впевненістю атрибуції до Білорусі
2. Розвинені технічні можливості з високим рівнем операційної безпеки
3. Стратегічна орієнтація на країни-члени НАТО та пов’язані з НАТО організації
4. Інтеграція гібридної війни, що поєднує кібершпигунство з дезінформацією
5. Потенціал ескалації під час періодів геополітичної напруги
6. Необхідність комплексної оборонної відповіді на стратегічному, оперативному та тактичному рівнях

Рекомендовані дії:

1. Впровадження комплексної стратегії кіберзахисту
2. Налагодження координації з НАТО та союзними державами
3. Розгортання розширених можливостей виявлення та реагування на загрози
4. Проведення threat hunting за індикаторами Ghostwriter
5. Впровадження посилення ідентифікації та архітектури zero trust
6. Створення процедур реагування на інциденти
7. Проведення навчання персоналу з питань кібербезпеки
8. Впровадження процедур безпеки ланцюга постачання

ПОСИЛАННЯ ТА ДЖЕРЕЛА

- EuRepoC APT Profile: UNC1151
- Ghostwriter in the Shell: Belarus-Russia Nexus Analysis
- Ghostwriter: Hybrid Influence and Espionage Operations
- SentinelOne Labs: Ghostwriter 2025 Campaign Analysis
- Threat Group Cards: Operation Ghostwriter
- Google Cloud: UNC1151 Linked to Belarus Government
- HarfangLab: UAC-0057 Campaign Analysis
- BushidoToken: Ghostwriter APT Infrastructure Tracking
- Council on Foreign Relations: Cyber Operations in Russia-Ukraine War
- Malpedia: Ghostwriter Threat Actor Profile
- The Hacker News: Ghostwriter Prometheus Campaign 2026
- National Security Archive: Attribution and Timeline Analysis
- Rewterz Threat Alert: Ghostwriter Active IOCs
- MalwareBazaar: Trojan.Casdet Sample
- MalwareBazaar: Cobalt Strike Beacon Sample
- MalwareBazaar: CVE-2024-42009 Exploit Sample
- CAPE Sandbox: Cobalt Strike Analysis
- VMRay: Cobalt Strike Beacon Analysis
- Triage: CVE-2024-42009 Exploit Analysis