APT-угрупування Dragonfly

Назва: Dragonfly**.**
Інші назви: Berserk Bear, Blue Kraken, Koala Team, Energetic Bear, Crouching Yeti, TG-4192
Тип: Advanced Persistent Threat (APT).
Походження: Російська Федерація.
Період активності: з ~2010–2011 року – дотепер

Energetic Bear/Crouching Yeti — широко відома APT-група, що діє щонайменше з 2010 року. Як правило, учасники групи атакують різні компанії з фокусом на енергетику та промисловість. Атаковані Energetic Bear/Crouching Yeti компанії розкидані по всьому світу з помітною перевагою Європи та США. У 2016–2017 роках значно зросла кількість атак на компанії в Туреччині.

Основна тактика групи включає розсилку фішингових листів із шкідливими документами, а також зараження різних серверів. Деякі заражені сервери використовуються групою як допоміжні лише для розміщення різного інструментарію та його логів. Інші заражаються спеціально для того, щоб використовувати їх у waterhole-атаках і діставатися з їх допомогою до основних цілей.

Попри те, що зафіксовані атаки не призвели до безпосереднього впливу на системи операційних технологій, їхня структура, вибір цілей і технічна реалізація вказують на потенційну підготовку до операцій із можливістю впливу на економічну діяльність інших країн. Масштаб тактик підтверджує високий рівень зрілості угруповання та його відповідність профілю державного APT-актора.

Наявні докази, що включають кримінальні обвинувачення Міністерства юстиції США та характер вибору цілей, вказують на зв’язок Dragonfly із російськими державними структурами. У сукупності це дозволяє оцінювати діяльність групи як частину ширшої стратегії кіберрозвідки та підготовки до потенційного впливу на критичну інфраструктуру.

Діяльність

Зараження та компрометація серверів по всьому світу(2014-початок 17го):

У аналізі Kaspersky Lab[1] представлено відомості про виявлені сервери, заражені та використовувані угрупуванням, а також наведено результати аналізу веб-серверів, скомпрометованих групою Energetic Bear:

Жертви:

- Туреччина (постраждали ресурси промислових підприємств та нафтовий холдинг, готельний бізнес);
- Україна (уражені банк та енергетична компанія);
- Великобританія (впроваджено шкідливе ПЗ в аерокосмічну компанію);
- Німеччина (атакований розробник та інтегратор ПЗ);
- Греція (зазнав атаки університетський сервер);
- США (мішенню стало нафтогазове підприємство);

Зараження серверів Waterhole здійснювалось за одним і тим же шаблоном: на веб-сторінку або JS-файл впроваджувалось посилання: file://IP/filename.png. За цим посиланням ініціюється запит картинки, в результаті якого користувач підключається до віддаленого сервера протоколу SMB. В даному типі атаки метою зловмисників є вилучення із сесії наступних даних: IP, ім'я користувача, домен, NTLM-хеш пароля. Сама картинка, яка запитується за посиланням, фізично на віддаленому сервері не присутня.

Скомпрометовані сервери в деяких випадках використовувалися для атак на інші ресурси. У ході дослідження заражених серверів було виявлено численні сайти та сервери, які атакуючі сканували різними інструментами, такими як nmap, dirsearch, sqlmap і т.д. Вони не були об'єднані спільною тематикою, а система по якій обирали цілі теж не є очевидною. Найімовірніше, сканування більшої частини ресурсів відбувалося з метою отримання «плацдарму» для розміщення інструментарію атакуючих та подальшої атаки.

Атака угруповання Dragonfly на энергосистему США (2014-2017й)

Назви компаній свідомо замінено на умовні позначення (Company “One”, Company “Three” тощо), оскільки ідентичність жертв не є критичною для розуміння технічних аспектів атаки. Основний фокус зроблено на тактиках і техніках, а не на конкретних організаціях. Такий підхід також відповідає принципам відповідального розкриття інформації та дозволяє уникнути зайвих репутаційних ризиків для постраждалих сторін (Джерело)

Список жертв:

1). Комісія з ядерного регулювання («КЯР»), державна агенція США, відповідальна за регулювання діяльності організацій, що використовують ядерні матеріали, включаючи атомні електростанції;

2). Wolf Creek Nuclear Operating Corporation (WolfCreek), компанія, розташована в Берлінгтоні, штат Канзас, яка управляє атомною електростанцією Wolf Creek Generating Station;

3). “Westar Energy Inc”, компанія, розташована у штаті Канзас, яка була одним із власників Wolf Creek під час змови;

4). “Kansas Electric Power Cooperative” (“KEPCO”), некомерційний кооператив з виробництва та передачі електроенергії, що належить його членам, розташований у штаті Канзас, який був одним із власників Wolf Creek під час змови;

5). Компанія "One", компанія зі зберігання даних, розташована на Середньому Заході США;

6). Компанія “Three”, комерційна будівельна компанія, розташована в Мічигані;

7). Компанія "Four", компанія з відновлюваної енергії, розташована в Нью-Йорку;

8). Компанія "Five", компанія з відновлюваної енергії, розташована в Новій Англії;

9). Компанія “Six”, медіакомпанія з Іллінойсу, яка випускає публікації та веб-сайти, орієнтовані на інженерів. у обробній промисловості, нафтогазовій галузі та сфері систем промислового управління;

10). Компанія “Seven”, розташована в Пенсільванії, яка

надає цифрове кабельне телебачення високої чіткості та високошвидкісний інтернет;

11). Компанія "Eight", енергетична компанія, розташована в Іллінойсі;

12). Компанія "Nine", енергетична компанія, розташована в Огайо; і

13). Компанія “Ten”, американська компанія, що спеціалізується на наданні

консультаційних послуг постачальникам атомної енергії

14). Одна з Компанії-жертви, розташовані за межами Сполучених Штатів, - це компанія "Two", глобальна компанія, що займається SCADA та промисловою автоматизацією.

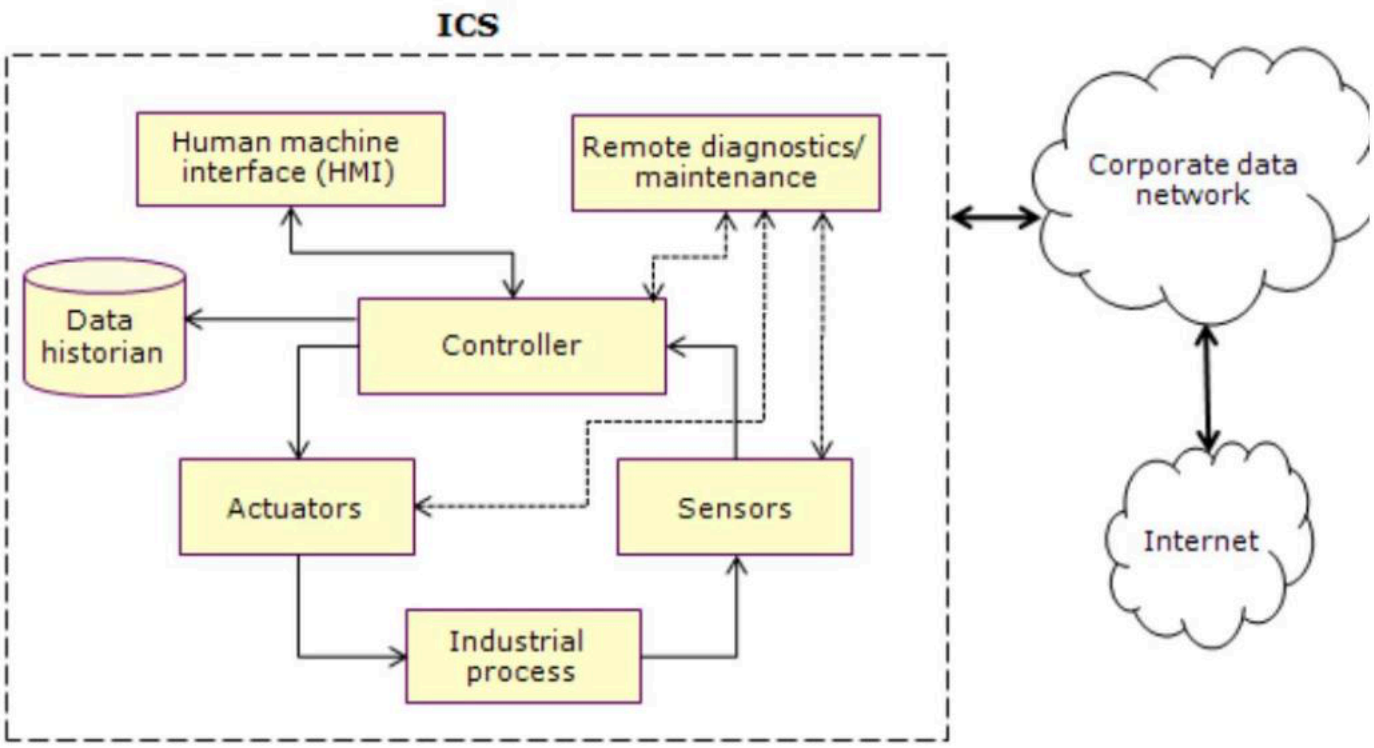
В обох фазах основною ціллю були системи промислового управління (ICS) та їх підсистема SCADA, які використовуються для збору даних, моніторингу та керування обладнанням на об’єктах енергетики.

Фаза Havex:

На першому етапі зловмисники зосередилися на компрометації виробників і постачальників програмного забезпечення для ICS/SCADA. Вони впроваджували шкідливе ПЗ Havex у легітимні оновлення програмного забезпечення, через що шкідливий код поширювався разом із офіційними інсталяційними файлами. Havex дозволяє створювати бекдори та забезпечувати віддалений доступ до скомпрометованих систем, що давало можливість збирати інформацію про мережу, пристрої та користувачів.

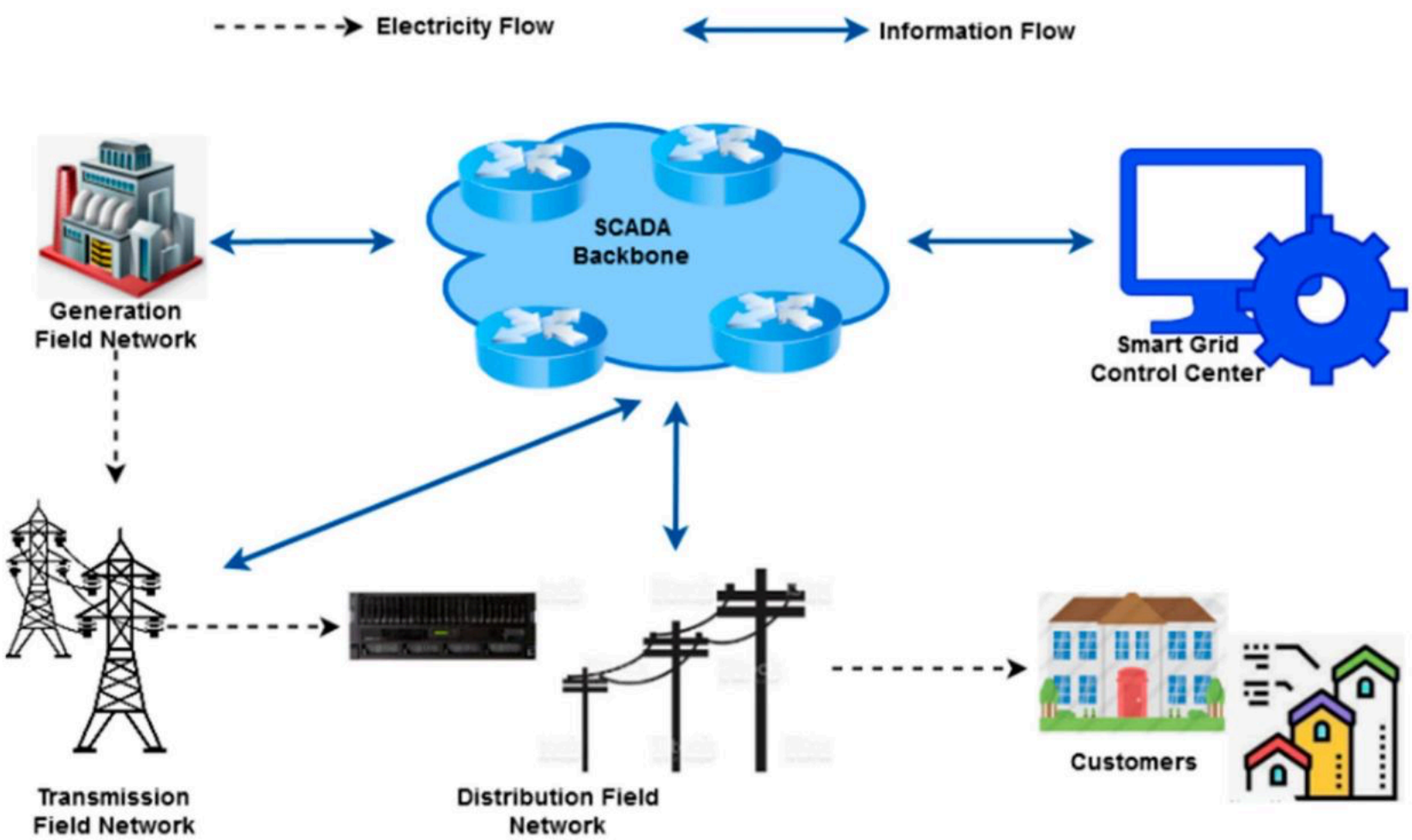
SCADA (Supervisory Control and Data Acquisition) — це підсистема в ICS, яка:

- збирає дані з обладнання
- показує їх оператору
- дозволяє керувати процесами*



Для керування інфраструктурою зловмисники використовували скомпрометовані сервери як проксі. Зокрема, сервер компанії “One” з 2012 по 2013 рік використовувався для маршрутизації трафіку та розгортання інфраструктури командування і контролю (C2). Через нього створювалися і адмініструвалися численні домени, на яких розміщувалися панелі керування Havex.

Також проводилася активна розвідка цілей. Зловмисники досліджували веб-ресурси організацій енергетичного сектору, зокрема пов’язаних з атомною енергетикою. Для отримання доступу до даних вони застосовували SQL-ін’єкції, що дозволяли читати, змінювати інформацію в базах даних і виконувати адміністративні команди. Окремо була проведена компрометація виробника SCADA-рішень (компанія “Two”). Зловмисники отримали доступ до внутрішніх даних, конфігурацій серверів і облікових записів адміністраторів. Після цього вони завантажили BIOS та драйвери, які згодом використали для впровадження шкідливого ПЗ.



У 2013–2014 роках Havex був інтегрований у драйвери цього виробника, доступні для публічного завантаження. Після встановлення такі драйвери автоматично підключалися до серверів управління зловмисників. Один із таких випадків був зафіксований на SCADA-системі електростанції.

Фаза Dragonfly 2.0:

На другому етапі атаки стали більш цілеспрямованими. Основна увага була зосереджена на конкретних компаніях енергетичного сектору та інженерах, які працюють із системами ICS/SCADA.

Зловмисники використовували:

- фішингові атаки;
- злом серверів і використання їх як плацдарму;
- компрометацію веб-сайтів, які відвідують інженери;
- експлуатацію вразливостей для віддаленого виконання коду.

Отримавши доступ до мереж (наприклад, компанії «Three»), вони створювали облікові записи адміністраторів із назвами, схожими на системні (MS_AutoUP, SYSTEM_USER тощо), щоб залишатися непомітними. Далі ці доступи використовувалися для підключення через RDP і створення корпоративних поштових акаунтів.

З цих акаунтів надсилалися фішингові листи, замасковані під заявки на роботу, як наприклад: «Controls Engineer.docx», містили шкідливий код:

From: Kevin North [redacted]
To: [redacted]
Date: 5/5/2017 8:58:01 AM
Subject: CV Kevin North
Attachments CV Controls Engineer.docx

Hello

Over 10 years Controls/Software Experience

Software development for PLC based control systems:
SIEMENS S5, S7-200, S7-300, S7-400 series,
Rockwell 5000, 500 series.
SCADA, HMI configuration.

Various Conveyor system experiences
Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET MPI, ASI, DeviceNet, DH+
EPLAN

Multi – skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and man
engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,

Kevin North

Після відкриття файл ініціював підключення до сервера зловмисників через SMB і передавав хеші облікових даних. Якщо мережа не блокувала такі з’єднання, зловмисники отримували можливість відновити паролі методом bruteforce і використовувати їх для доступу до систем.

Паралельно вони зламували веб-сайти енергетичних компаній і впроваджували шкідливий JavaScript, який викрадав облікові дані відвідувачів. Після отримання доступу до мереж жертв зловмисники встановлювали інструменти для підтримки контролю. Зокрема, використовувався бекдор Goodor, який забезпечував постійний доступ і зв’язок із C2-серверами.

Це дозволяло:

- переміщатися горизонтально (між комп’ютерами);
- підвищувати рівень доступу (вертикальне переміщення);
- отримувати доступ до критичних систем і конфіденційних даних.

Для збору облікових даних активно використовувалися атаки через SMB, включаючи спеціально створені ярлики та скрипти, які передавали хеші паролів без необхідності відкриття файлу (достатньо було відкрити папку).

Атака на Wolf Creek[4]

У 2017 році зловмисники провели атаку на Wolf Creek. Початковий доступ було отримано через фішинг. Після компрометації облікового запису вони багаторазово входили в систему, закріплювали присутність і завантажували шкідливі файли.

У мережі були розміщені:

- бекдори;
- скрипти для збору облікових даних;
- інструменти для подальшого поширення.

Також використовувалися SMB-атаки для отримання нових облікових записів. Зловмисники змогли скомпрометувати додаткові акаунти та розширити свою присутність у мережі. Крім того, вони скомпрометували веб-сайти енергетичних компаній, впроваджуючи шкідливий код через phishing і вразливості CMS, що дозволяло отримувати облікові дані інших користувачів галузі.

Висновки

Загалом атака угруповання Dragonfly на енергетичні компанії в США, завершилася без досягнення їхньої основної мети — отримання контролю над ICS/SCADA-системами та здійснення саботажу. Зловмисникам вдалося здійснити компрометацію корпоративної IT-мережі шляхом фішингових кампаній і збору облікових даних, що дозволило їм проводити розвідку внутрішньої інфраструктури. Водночас критично важливі системи управління були ізольовані завдяки мережевій сегментації, що не дозволило здійснити перехід у середовище операційних технологій. Атака була своєчасно виявлена, після чого відреагували відповідні органи кібербезпеки США, що обмежило подальше просування зловмисників. У результаті не було зафіксовано жодних фізичних пошкоджень чи перебоїв у роботі об’єкта. Цей інцидент розглядається як приклад підготовчої фази складної APT-операції, спрямованої на майбутній потенційний вплив на критичну інфраструктуру. Таким чином, операція завершилася частковим успіхом у зборі розвідувальних даних, але провалом у досягненні стратегічної мети.

Основні цілі атак:

- Енергетичний сектор (електромережі, АЕС, газ/нафта)
- Промислові системи (ICS/SCADA)
- Оборонна та авіаційна галузі
- Державні організації

Мотивація:

- Кіберрозвідка (збір даних)
- Отримання доступу до критичних систем
- Потенційний саботаж інфраструктури

Ключові особи

Марат Тюков, Михайло Гаврилов і Павло Акулов, Евгений Викторович Гладких — співробітники Центру 16 ФСБ. За даними Мін’юсту США, у 2012–2017 роках вони брали участь у кампанії проти урядових структур, зокрема Комісії з ядерного регулювання, а також проти компанії Wolf Creek Nuclear Operating Corporation, що керує АЕС у Канзасі.

SHUM

Evgeny Viktorovich Gladkikh
Евгений Викторович Гладких / Євгеній Вікторович Гладких

Місце народження: Росія
Волосся: Каре
Очі: Карі
Зріст: Приблизно 185 см
Вага: Приблизно 84 кг
Стать: Чоловік
Раса: Біла
Громадянство: Російське

Принаймні з серпня 2014 року і до липня 2018 року Євген Вікторович Гладких, як стверджується, вступив у змову, серед інших, з Державним дослідницьким центром Російської Федерації ФГУП Центральний науково-дослідний інститут хімії та механіки, Центром прикладних розробок та іншими співучасниками, з метою здійснення комп'ютерних вторгнень, спрямованих на енергетичні об'єкти та нафтопереробні заводи в Сполучених Штатах та за кордоном, та заподіяння шкоди цим об'єктам. Гладких та його змовники нібито домовилися та й зробили це, вторгнувшись у операційні технології та комп'ютерні системи із засобами безпеки, щоб встановити шкідливе програмне забезпечення, призначене для зупинки роботи фізичних систем безпеки або їхньої роботи в небезпечний спосіб. У червні 2021 року Окружним судом США було видано федеральний ордер на арешт Гладких, після того, як йому було пред'явлено звинувачення у змові з метою заподіяння пошкодження енергетичному об'єкту; спробі заподіяння пошкодження енергетичному об'єкту; та змові з метою доступу до захищених комп'ютерів та отримання інформації, а також навмисного пошкодження захищених комп'ютерів шляхом знання передачі даних.

Pavel Aleksandrovich Akulov
Павло Олександрович Акулов / Павел Александрович Акулов

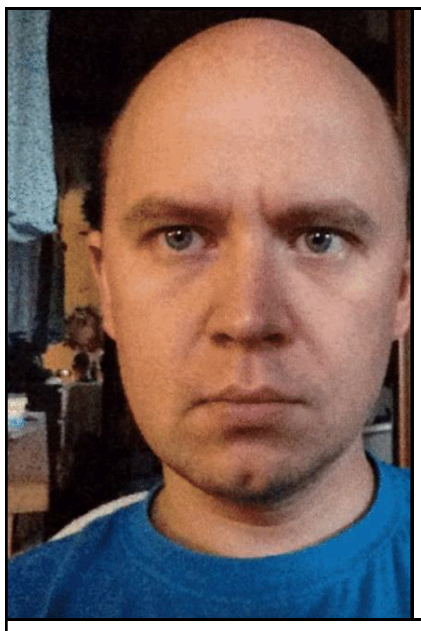
Місце народження: Росія
Колір волосся: світле
Колір очей: блакитний
Стать: чоловіча
Раса: біла
Громадянство: російське
Дата народження: 2 липня 1985 року

Акулов — офіцер Федеральної служби безпеки Росії (ФСБ), який змовився з іншими, щоб отримати та підтримувати несанкціонований постійний доступ до сотень американських та міжнародних енергетичних компаній, тим самим дозволяючи російському уряду порушувати роботу та пошкоджувати такі об'єкти. Акулов є членом підрозділу ФСБ, відомого як Центр 16, за станом на 2013 рік мав звання лейтенанта та працював в оперативній групі під назвою Військова частина 71330. Влада США висунула йому звинувачення у проникненні в комп’ютер, шахрайстві з дротами та крадіжці особистих даних при обтяжуючих обставинах.

Акулов проводив онлайн-розвідку на підтримку фішингових компаній замовників, включаючи розвідку, підтримуючи цільово спрямовані атаки замовників на комп'ютерну мережу WolfCreek і несанкціонований доступ до неї.

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

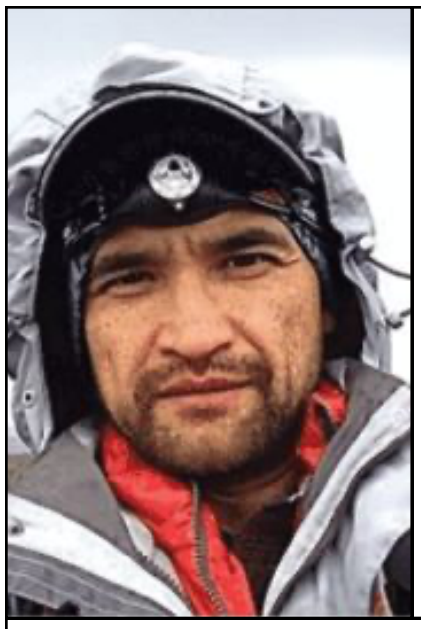
SHUM



Marat Valeryevich Tyukov
Марат Валерьевич Тюков

Місце народження: Росія
Колір очей: сірий
Стать: чоловіча
Раса: біла
Громадянство: росіянин
Дата народження: 17 листопада 1982 року

Марат Валерійович Тюков — офіцер Федеральної служби безпеки Росії (ФСБ), який змовився з іншими, щоб отримати та підтримувати несанкціонований постійний доступ до сотень американських та міжнародних енергетичних компаній, тим самим дозволяючи російському уряду порушувати роботу та пошкоджувати такі об'єкти. Тюков є членом підрозділу ФСБ, відомого як Центр 16, де він працює в оперативній групі під назвою Військова частина 71330. Він здійснив несанкціонований доступ до сервера, що належить компанії “One” де він використовував засіб шпіонажу C2. Тюков також здійснив вторгнення в комп'ютерну мережу компанії “Two”. Потім група підробила оновлення для програмного забезпечення промислового управління компанії “Two”, де воно було доступно для завантаження енергетичними компаніями у всьому світі, включаючи Сполучені Штати (частина Dragonfly/ Havex).



Mikhail Mikhailovich Gavrilov
Михаил Михайлович Гаврилов / Михайло Михайлович Гаврилов

Місце народження: Росія
Колір очей: карий
Стать: чоловіча
Раса: біла
Громадянство: росіянин
Дата народження: 7 листопада 1979 року

Михайло Михайлович Гаврилов — офіцер ФСБ, який змовився з іншими, щоб отримати та підтримувати несанкціонований постійний доступ до сотень американських та міжнародних енергетичних компаній, тим самим дозволяючи російському уряду порушувати роботу та пошкоджувати такі об'єкти. Гаврилов є членом підрозділу ФСБ, відомого як Центр 16, де він працює в оперативній групі під назвою Військова частина 71330. За час служби в цій частині Гаврилов обіймав посади капітана, а пізніше — майора. Гаврилов здійснив атаки на мережу Wolf Creek, а також на компанію «Seven», яку хакери використовували для доступу до різних веб-сторінок входу в веб-пошту енергетичних, комунальних і критично важливих інфраструктурних компаній (вони є частиною Dragonfly 2.0).

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

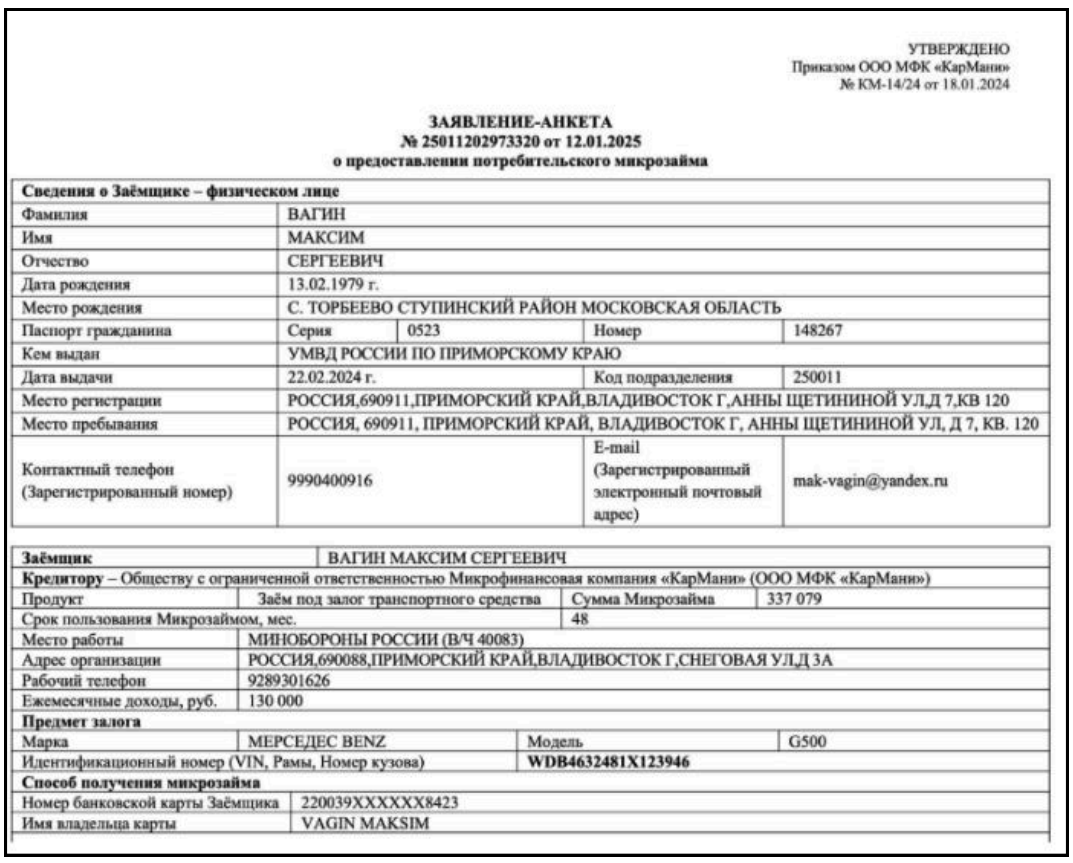
Після зламу компанії Carmoney, яка видає забезпечені позики (її пов'язують з колишньою дружиною диктатора Путіна, Людмилою), Ukrainian Cyber Alliance виявила особисті дані про ще деяких співробітників 16-го центру ФСБ[10]. Привожу знімки даних:

Приказом ООО МФК «КарМани»/
№ КМ-45/24 от 27.02.2024

ЗАЯВЛЕНИЕ-АНКЕТА
№25010422937739 от 04.01.2025
о предоставлении потребительского микрозайма

Сведения о Заёмщике – физическом лице				
Фамилия	СОЛОВЬЕВ			
Имя	ДМИТРИЙ			
Отчество	АЛЕКСЕЕВИЧ			
Предыдущая фамилия				
Предыдущее имя				
Предыдущее отчество				
Дата рождения	25.07.2003 г.			
Место рождения	ЧЕЛЯБИНСКАЯ ОБЛАСТЬ СЕЛО ЧЕСМА			
ИНН				
СНИЛС	200-960-210 09			
Паспорт гражданина (действующий)	Серия	4524	Номер	108296
Кем выдан	ГУ МВД РОССИИ ПО Г. МОСКВЕ			
Дата выдачи	30.05.2024 г.		Код подразделения	770086
Паспорт гражданина (предыдущий)	Серия		Номер	
Место регистрации	РОССИЯ, 457220, ЧЕЛЯБИНСКАЯ ОБЛ, ЧЕСМЕНСКИЙ Р-Н, ЧЕСМА С, КОЛХОЗНАЯ УЛ, Д 54			
Место пребывания	РОССИЯ, 457220, ЧЕЛЯБИНСКАЯ ОБЛ, ЧЕСМЕНСКИЙ Р-Н, ЧЕСМА С, КОЛХОЗНАЯ УЛ, Д 54			
Контактный телефон (Зарегистрированный номер)	9000847013		E-mail (Зарегистрированный электронный почтовый адрес)	

Продукт	Всё Про100 2.0	Сумма Микрозайма	9 900
Срок пользования микрозаймом дней		До 14 дней	
Место работы	ФГКУ "В/Ч 71330".		
Адрес организации	РОССИЯ, 108840, МОСКВА Г, ТРОИЦК Г, КАЛУЖСКОЕ Ш, Д 2		
Рабочий телефон	4959146666		
Ежемесячные доходы, руб.	150 000		
Способ получения микрозайма			
Система Быстрых Платежей (СБП)	79000847013		
Наименование Банка	Sberbank		
Номер банковской карты Заёмщика			
Имя владельца карты			

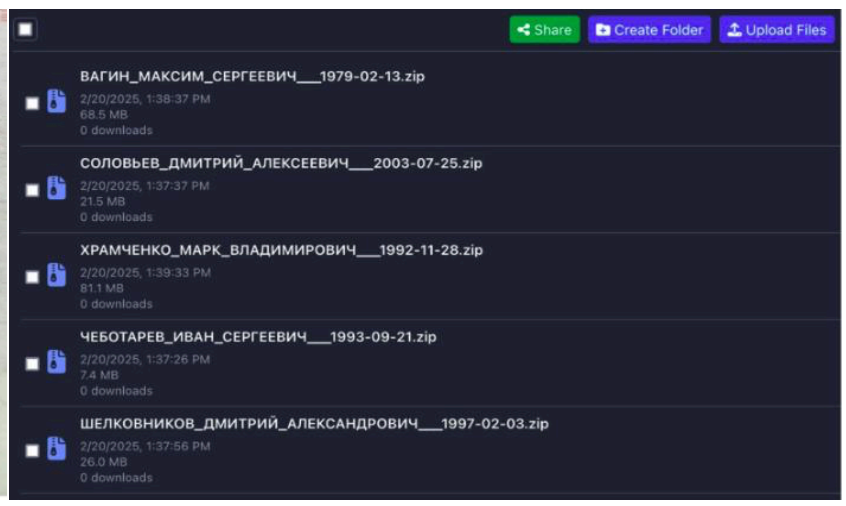


УТВЕРЖДЕНО
Приказом ООО МФК «КарМани»
№ КМ-14/24 от 18.01.2024

ЗАЯВЛЕНИЕ-АНКЕТА
№ 25011202973320 от 12.01.2025
о предоставлении потребительского микрозайма

Сведения о Заёмщике – физическом лице				
Фамилия	ВАГИН			
Имя	МАКСИМ			
Отчество	СЕРГЕЕВИЧ			
Дата рождения	13.02.1979 г.			
Место рождения	С. ТОРБЕЕВО СТУПИНСКИЙ РАЙОН МОСКОВСКАЯ ОБЛАСТЬ			
Паспорт гражданина	Серия	0523	Номер	148267
Кем выдан	УМВД РОССИИ ПО ПРИМОРСКОМУ КРАЮ			
Дата выдачи	22.02.2024 г.		Код подразделения	250011
Место регистрации	РОССИЯ,690911,ПРИМОРСКИЙ КРАЙ,ВЛАДИВОСТОК Г,АННЫ ЩЕТИНИНОЙ УЛ,Д 7,КВ 120			
Место пребывания	РОССИЯ, 690911, ПРИМОРСКИЙ КРАЙ, ВЛАДИВОСТОК Г, АННЫ ЩЕТИНИНОЙ УЛ, Д 7, КВ. 120			
Контактный телефон (Зарегистрированный номер)	9990400916		E-mail (Зарегистрированный электронный почтовый адрес)	mak-vagin@yandex.ru

Заёмщик	ВАГИН МАКСИМ СЕРГЕЕВИЧ		
Кредитору – Обществу с ограниченной ответственностью Микрофинансовая компания «КарМани» (ООО МФК «КарМани»)			
Продукт	Заём под залог транспортного средства	Сумма Микрозайма	337 079
Срок пользования Микрозаймом, мес.		48	
Место работы	МИНОБОРОНЫ РОССИИ (В/Ч 40083)		
Адрес организации	РОССИЯ,690088,ПРИМОРСКИЙ КРАЙ,ВЛАДИВОСТОК Г,СНЕГОВАЯ УЛ,Д 3А		
Рабочий телефон	9289301626		
Ежемесячные доходы, руб.	130 000		
Предмет залога			
Марка	МЕРСЕДЕС BENZ	Модель	G500
Идентификационный номер (VIN, Рамы, Номер кузова)		**WDB4632481X123946**	
Способ получения микрозайма			
Номер банковской карты Заёмщика	220039XXXXXX8423		
Имя владельца карты	VAGIN MAKSIM		



Місцезнаходження

«Центр 16» ФСБ знаходиться по адресі: пр. Вернадского, 12, Moskva, Russia, 119331

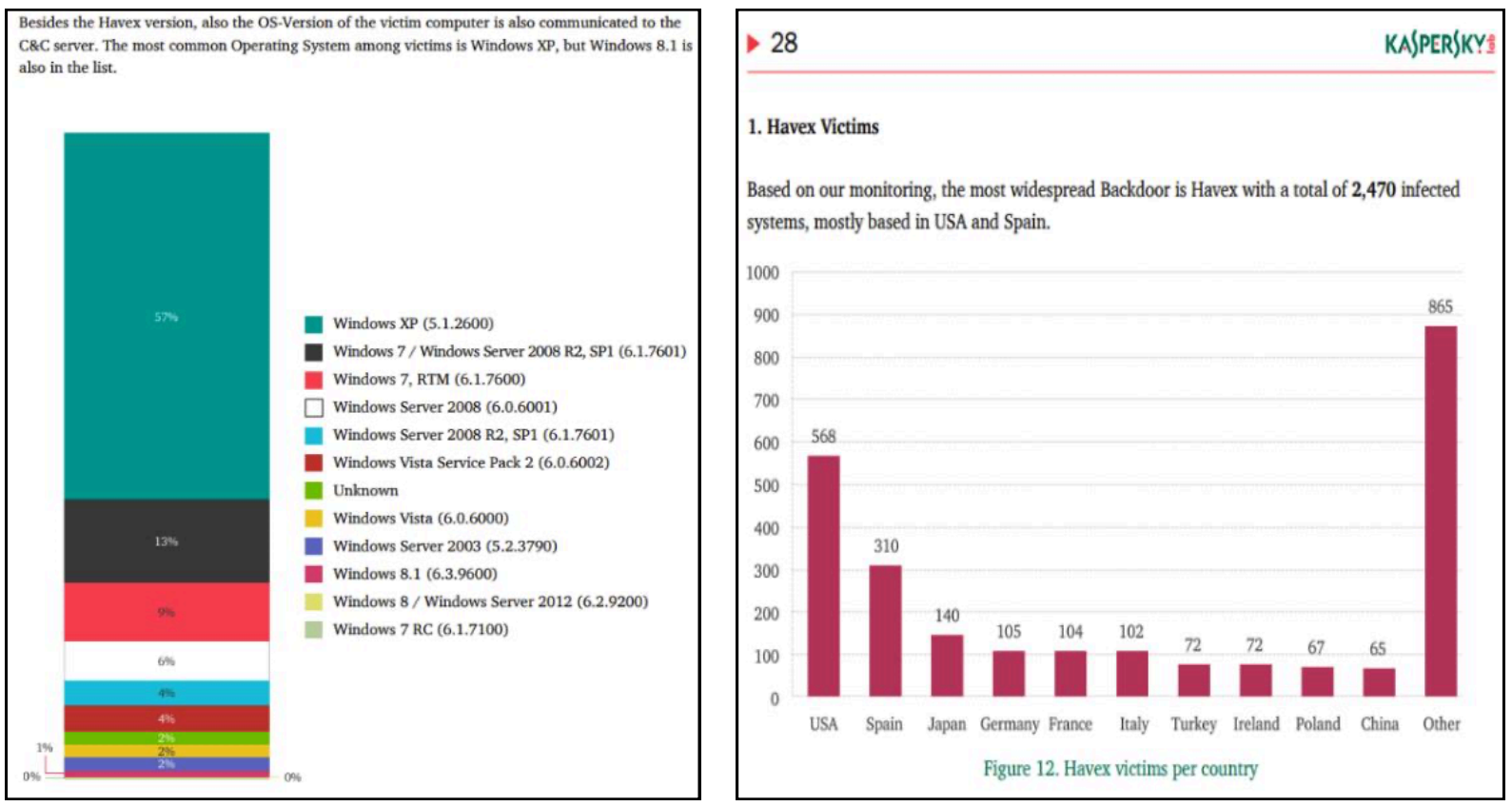
Підтримати діяльність організації: https://donate.shum-ng.org/

Тактики, техніки та процедури

Інструменти

Feature	Dragonfly (2013-2014)	Dragonfly 2.0 (2015-2017)	Link strength
Backdoor.Oldrea	Yes	No	None
Trojan.Heriplor (Oldrea stage II)	Yes	Yes	Strong
Trojan.Karagany	Yes	Yes (Trojan.Karagany.B)	Medium-Strong
Trojan.Listrix (Karagany stage II)	Yes	Yes	Medium-Strong
"Western" energy sector targeted	Yes	Yes	Medium
Strategic website compromises	Yes	Yes	Weak
Phishing emails	Yes	Yes	Weak
Trojanized applications	Yes	Yes	Weak

Улюбленим засобом Dragonfly для віддаленого доступу є інструмент Backdoor.Oldrea, відомий також як Havex або Energetic Bear. Oldrea відкриває "чорний хід" на комп'ютер жертви, надаючи атакуючим можливість викрасти дані та встановити додаткові шкідливі програми. Після встановлення на комп'ютері жертви Oldrea виконує збір системної інформації, складає списки файлів, встановлених програм та доступних жорстких дисків. Крім того, Oldrea отримує дані з адресної книги Outlook і файлів конфігурації VPN.



Звіт лабораторії Касперського за 2018 р. щодо зараженності пристроїв Havex або Energetic Bear.[11]

Другий за частотою використання інструмент Dragonfly - Trojan.Karagany. Karagany підтримує передачу вкрадених даних, завантаження нових файлів та запуск виконуваних файлів на заражених комп'ютерах. Крім того, Karagany дозволяє запускати додаткові модулі, наприклад, засоби збору паролів, створення знімків екрану, каталогізації документів на заражених комп'ютерах тощо.

До списку інструментів також входять наступні інструменти: command-and-control (C2) traffic mechanisms, DNS-based C2 communication, malicious executable files (PE/.exe), шкідливі документи (RTF, PDF, Office), watering hole payloads, drive-by download exploit kits.

Аналітика атаки по методологіям MITRE ATT&CK на енергосистему США:

Класифікуємо дії атакуючих згідно з базою MITRE ATT&CK, це дасть нам змогу перевести розрізнені факти у структуровану модель поведінки.

Початковий доступ до інфраструктури жертв здійснювався через декілька векторів, основним з яких був фішинг (T1566 Phishing), зокрема, розсилка шкідливих вкладень (T1566.001 Spear Phishing Attachment). Виконання шкідливого коду в цьому випадку залежало від дії користувача (T1204 User Execution), який запускав заражені файли (T1204.002 Malicious File).

Паралельно застосовувалися watering hole атаки (T1189 Drive-by Compromise), що дозволяли скомпрометувати користувачів через довірені веб-ресурси. У складніших сценаріях атакуючі використовували компрометацію ланцюга постачання (T1195 Supply Chain Compromise), інтегруючи шкідливий код у легітимне програмне забезпечення, що значно розширювало масштаб первинного доступу. Додатково могли використовуватися вразливості публічних сервісів (T1190 Exploit Public-Facing Application) та сканування інфраструктури (T1595.002 Active Scanning: Vulnerability Scanning) для пошуку точок входу.

Окрім запуску шкідливих файлів, фіксується використання інтерпретаторів команд (T1059), що включає роботу через CLI мережевих пристроїв або Unix shell (T1059.004), що дозволяло гнучко керувати середовищем. Для того, щоб залишатися непомітними, хакери використовували як викрадені облікові дані (T1078 Valid Accounts), включаючи стандартні або слабо захищені акаунти (T1078.001 Default Accounts, T1552 Unsecured Credentials), так і створення нових облікових записів (T1136 Create Account). Додатково застосовувались механізми автозапуску (T1547.001 Registry Run Keys / Startup Folder) та планувальник задач (T1053.005 Scheduled Task), що дозволяли підтримувати доступ навіть після перезавантаження системи.

Після закріплення в мережі здійснювалася активна фаза розвідки (TA0007 Discovery), включаючи аналіз файлової системи (T1083 File and Directory Discovery), облікових записів (T1087.001 Account Discovery: Local Account) та загальної структури мережі. Паралельно застосовувати техніки перехоплення трафіку (T1040 Network Sniffing) для збору додаткових даних і облікових даних. Отримана інформація використовувалася для підготовки подальшого переміщення мережею.

Горизонтальне переміщення здійснювалося через віддалені сервіси (T1021 Remote Services), зокрема RDP (T1021.001 Remote Desktop Protocol), що в поєднанні з валідними обліковими записами дозволяло діяти в межах типової активності користувачів. Такий підхід мінімізує аномалії в поведінці та ускладнює їх виявлення. Додатково, атакуючі могли використовувати легітимні серверні компоненти (T1505 Server Software Component) для розширення контролю над інфраструктурою.

Для управління скомпрометованими вузлами використовувалася інфраструктура командування і контролю (TA0011 Command and Control). Трафік часто маскувався через використання стандартних портів (T1043 Commonly Used Port), проксі (T1090 Proxy) та заплутування даних (T1027 Obfuscated Files or Information). Такі підходи дозволяють знизити ймовірність виявлення та ускладнюють аналіз інфраструктури C2.

Окрему увагу приділяли ухиленню від захисту (TA0005 Defense Evasion). Це включало маскування під легітимні процеси або ресурси (T1036 Masquerading, зокрема T1036.005 Match Legitimate Resource Name), приховування артефактів (T1564 Hide Artifacts) та відключення або модифікацію засобів захисту (T1562.001 Impair Defenses). Також могли застосовуватися механізми блокування індикаторів (T1562.006 Indicator Blocking), що ускладнюють реагування з боку захисних систем.

На фінальних етапах операції відбувалися збір і ексфільтрація даних (TA0010 Exfiltration). Перед передачею дані агрегувалися локально (T1074.001 Data Staged), після чого передавалися через C2-канали (T1041 Exfiltration Over C2 Channel).

У сукупності ці техніки формують повноцінний, багаторівневий цикл атаки, а узгодженість і глибина операцій свідчать про високий рівень організації та підтверджують, що діяльність Dragonfly відповідає профілю складного APT-актора, орієнтованого на довготривалу присутність, розвідку та підготовку до можливих подальших дій.

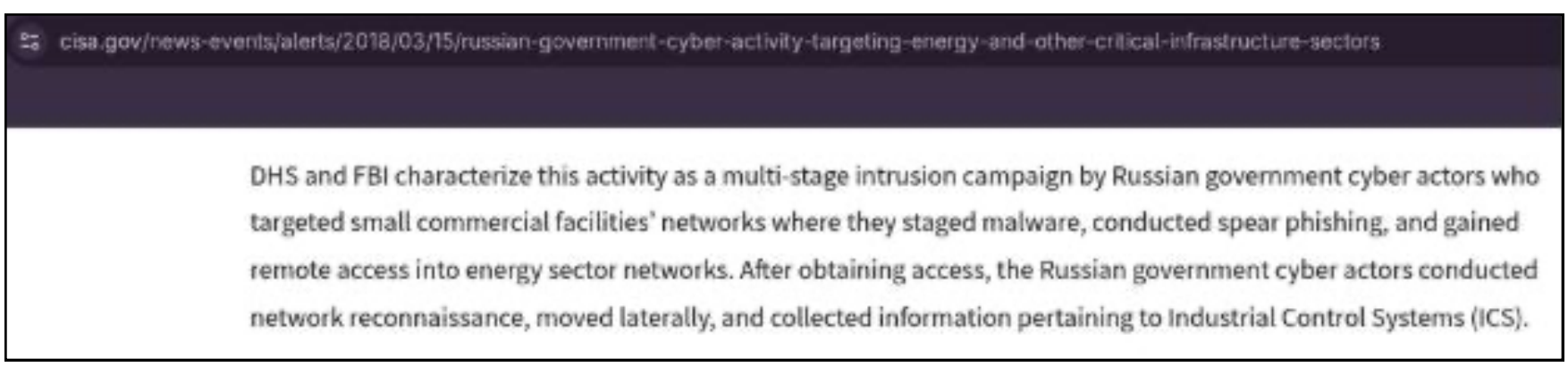
Висновки

У сукупності ці техніки формують повноцінний, багаторівневий цикл атаки, а узгодженість і глибина операцій свідчать про високий рівень організації та підтверджують, що діяльність Dragonfly відповідає профілю складного APT-актора, орієнтованого на довготривалу присутність, розвідку та підготовку до можливих подальших дій.

Причетність Dragonfly до РФ

1) Список жертв чітко збігається з інтересами РФ: енергетичні компанії США та ЄС, оператори електромереж, нафтогазова інфраструктура. Хакери які не працюють на якусь державу, зазвичай не ломають енергетику, це більш типово для державних APT, а не для звичайної кіберзлочинності, до того ж, як для одинаків, в них занадто високий рівень технічних можливостей.

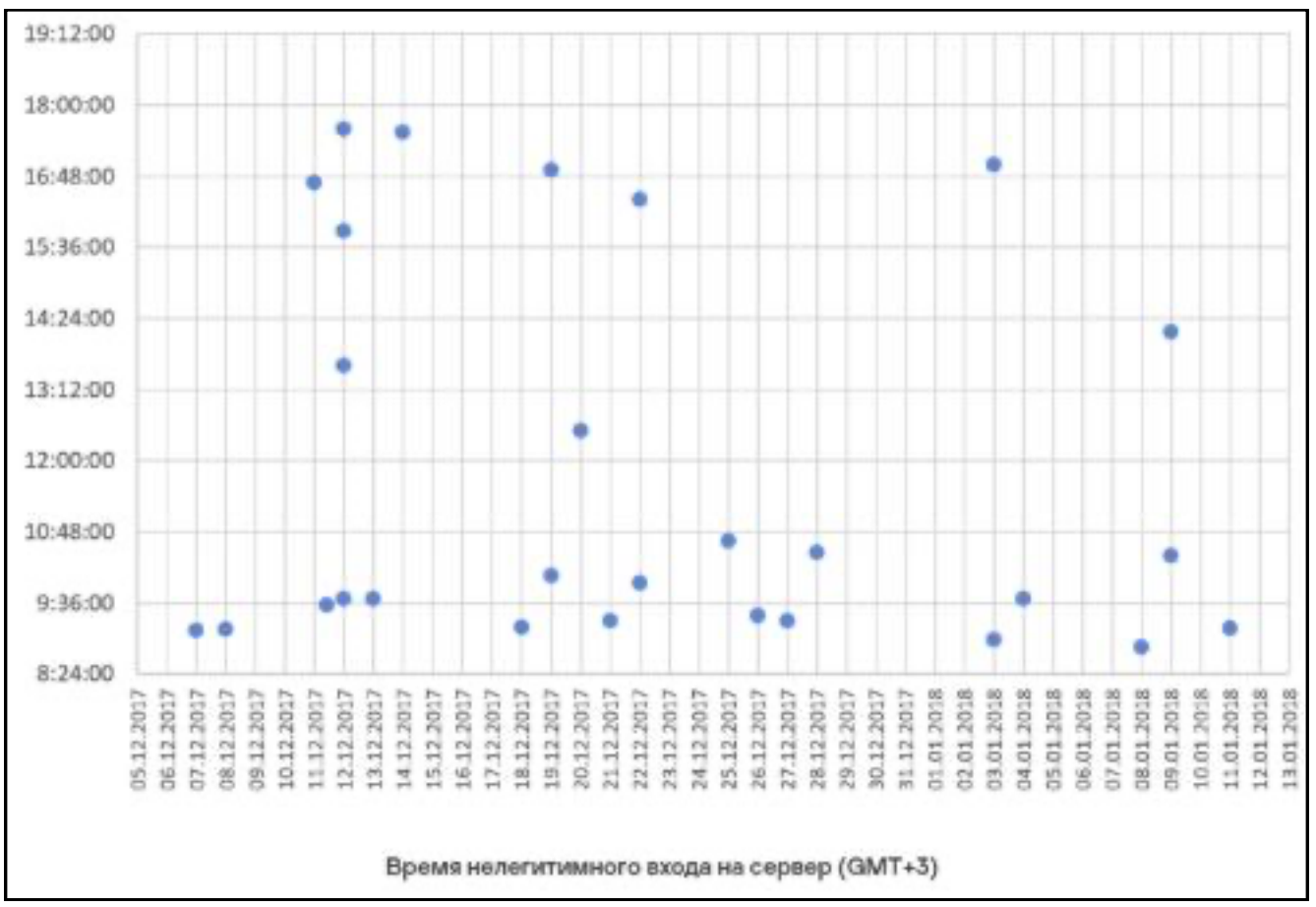
2) Звинувачення на пряму відображено у матеріалах Мін'юсту США: https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors



3) Аналітика показує, що активність відповідає робочому часу Східної Європи:

Symantec: 9:00–18:00 (UTC+4)

Kaspersky Lab: UTC+3 [2]



4) Перетин з іншими російськими APT. Методи та інфраструктура перетинаються з Sandworm Team та APT28, а ці групи вже офіційно атрибутовані РФ (зокрема ГРУ).

Справа в тому, що діяльність Dragonfly демонструє системний і довгостроковий підхід до компрометації критичної інфраструктури, який виходить за межі класичної кіберзлочинності та відповідає моделям державних кібероперацій. Фокус на енергетичному секторі, ICS/SCADA системах і пов’язаних постачальниках програмного забезпечення вказує на стратегічну зацікавленість у створенні доступу до середовищ, що мають прямий вплив на економічні і виробничі процеси.

Атаки звичайних кіберзлочинців, орієнтовані на швидку монетизацію: це масові кампанії з використанням фішингу, ransomware або крадіжки платіжних даних, де головна мета — отримати гроші якнайшвидше і з мінімальними витратами ресурсів. Тому їм не властиво витрачати час на глибоку розвідку або складні багаторівневі проникнення. Натомість атаки на економічний чи енергетичний сектор, характерні для APT-груп, мають довгострокову мету: прихований доступ, збір розвідувальної інформації або підготовка до потенційного впливу на критичну інфраструктуру. Такі операції значно складніші, триваліші й орієнтовані не на швидкий прибуток, а на стратегічний ефект.

Використання компрометації дозволяє отримати початковий доступ до великої кількості цілей із мінімальними витратами, тоді як подальші фази операцій орієнтовані на відбір найбільш цінних жертв і глибоку інтеграцію в їхню інфраструктуру. Такий підхід свідчить про наявність чіткої пріоритизації цілей і ресурсів, що характерно для хакерів, які діють в інтересах держави. Аналіз інциденту Wolf Creek та суміжних атак показує, що основною метою на зафіксованому етапі була не негайна деструктивна дія, а розвідка, накопичення облікових даних і вивчення архітектури мереж. Обмеження атаки на рівні IT-сегменту, пов’язане з ефективною сегментацією мереж, однак це не виключає намірів подальшого переходу до середовища операційних технологій у майбутньому.

Перетин інфраструктури, тактик і підходів Dragonfly з іншими відомими російськими APT-групами, а також відповідність вибору цілей геополітичним інтересам Російської Федерації, посилюють оцінку щодо державної атрибуції. У цьому контексті діяльність угруповання може розглядатися як частина ширшої стратегії підготовки до потенційних кібероперацій, спрямованих на вплив або дестабілізацію енергетичної інфраструктури.

Джерела

1. https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors

2. https://ics-cert.kaspersky.ru/publications/reports/2018/04/23/energetic-bear-crouching-yeti-attacks-on-servers/

3. https://dailystorm.ru/obschestvo/rossiyskie-hakery-iz-energetic-bear-vzlamyvayut-elektrostancii-ssha-chto-o-nih-izvestno

4. https://www.justice.gov/d9/press-releases/attachments/2022/03/24/ks_akulov_gavrilov_tyukov_0.pdf

5. https://www.security.com/threat-intelligence/dragonfly-energy-sector-cyber-attacks

6. https://www.justice.gov/archives/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

7. https://hackyourmom.com/novyny/ssha-ogolosyly-vynagorodu-10-miljoniv-za-infu-pro-hakeriv-fsb/

8. https://www.fbi.gov/image-repository/four-russians.jpg/view

9. https://www.paloaltonetworks.com/blog/2014/07/palo-alto-networks-offers-threat-mitigation-havex-dragonfly-variants/

10. https://t.me/UCAgroup/44

11. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf