НАЦІОНАЛЬНА АКАДЕМІЯ
НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Науково-дослідний центр
службово-бойової діяльності Національної гвардії України

Науково-дослідна лабораторія
забезпечення службово-бойової діяльності
Національної гвардії України

Збірник тез доповідей X Міжнародної науково-практичної конференції

“Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів”

29 жовтня 2021 року
м. Харків

Оргкомітет конференції

Голова оргкомітету – т.в.о. заступника начальника науково-дослідного центру – начальник науково-дослідної лабораторії забезпечення службово-бойової діяльності Національної гвардії України Національної академії Національної гвардії України, підполковник **Побережний А.А.**

Відповідальний секретар оргкомітету – старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності Національної гвардії України, к.т.н., с.н.с. **Баулін Д.С.**

Члени оргкомітету:
Подригало М.А., д.т.н., професор, завідувач кафедри технології машинобудування і ремонту машин Харківського національного автомобільно-дорожнього університету;
Sergiyenko Oleg, д.т.н., професор, завідувач кафедри прикладної фізики автономного університету Нижньої Каліфорнії, Енсенда, Мексика;
Яковлев М.Ю., д.т.н., професор, провідний науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності Національної гвардії України;
Sagradian Martin, д.т.н., професор, професор кафедри математики та статистики Університету Маккуорі, Сідней, Австралія;
Єрмошин М.О., д.військ.н., професор, професор кафедри зенітних ракетних військ Харківського національного університету Повітряних Сил ім. І. Кожедуба;
Медвідь М.М., д.е.н., професор, заступник начальника навчально-методичного центру – начальник відділу методичного забезпечення навчального процесу Національної академії Національної гвардії України;
Горелишев С.А., к.т.н., доцент, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності Національної гвардії України

Адреса оргкомітету: 61001, м. Харків, площа Захисників України, 3, Національна академія Національної гвардії України, науково-дослідна лабораторія забезпечення службово-бойової діяльності НГУ.

Електронна адреса: ndcnangu@ukr.net

Тези доповідей опубліковано в авторській редакції, мовою оригіналу. Відповідальність за зміст, достовірність інформації, фактичні помилки, точність викладених фактів та можливість використання для відкритого опублікування несуть автори.

X Міжнародна науково-практична конференція:

“Актуальні питання забезпечення службово-бойової діяльності військових формувань та правоохоронних органів”

Мета конференції:

виявлення проблемних питань забезпечення службово-бойової діяльності військових формувань та правоохоронних органів та визначення основних шляхів їх вирішення.

Тематика конференції

1. Науково-технічне супроводження розроблення та модернізації озброєння, військової та спеціальної техніки, технічних засобів для виконання службово-бойових завдань підрозділами військових формувань та правоохоронних органів.

2. Наукове супроводження розроблення навчально-тренувальних засобів та спеціальних тренажерів для підготовки фахівців з експлуатації, відновлення та бойового застосування озброєння та спеціальної техніки військових формувань та правоохоронних органів.

3. Наукове обґрунтування застосування прикладних інформаційних технологій для моделювання службово-бойових дій підрозділів військових формувань та правоохоронних органів і процесів управління ними під час виконання службово-бойових завдань за умов введення різних правових режимів.

4. Сучасні питання удосконалення системи тилового забезпечення службово-бойової діяльності військових формувань та правоохоронних органів.

Проводяться роботи як щодо удосконалення існуючих систем і комплексів з метою поліпшення спроможностей боротьби з сучасними ЗПН, так і щодо розробки перспективних ЗРК (ЗРС), таких як С-500 “Прометей” (Росія), МЕАДС (США, ФРН, Італія), SAMP-T (Франція, Італія) тощо.

До спеціалізованих ПРК наземного базування, які спроможні боротись з балістичними ракетами, відносяться американські комплекси ТХААД та Ізраїльські “Хец” з протиракетами “Ерроу”, а морського базування – система озброєння “Іджис” з протиракетою “Стандарт-3”.

Аналіз характеристик наведених вище ЗРК (ЗРС) показує, що універсальні ЗРК типу С-300, С-350, С-400, “Петріот” можуть перехоплювати нестратегічні БР на дальностях до 40 км і висотах до 25-30 км, протиракетні комплекси ТХААД – на дальностях до 200 км і висотах до 150 км, ПРК “Хец” – на дальностях до 90-100 км і висотах до 40-50 км. Максимальна швидкість БР, що вражаються, для комплексу С-400 становить 4800 м/с, а комплексів ТХААД, “Хец” – 3000-4000 м/с. Комплекси С-400 і ТХААД здатні перехоплювати нестратегічні БР із дальністю стрільби до 3500 км.

З порівняльного аналізу цих характеристик випливає, що можливості комплексів ТХААД і “Хец” щодо прикриття території від ударів балістичних ракет у декілька разів перевищуватиме можливості існуючих універсальних засобів боротьби з балістичними ракетами.

Крім того, слід зауважити, що в умовах комплексного застосування різнотипних ЗПН виникають суперечливі вимоги щодо вибору ЗРК для організації прикриття об’єктів критичної інфраструктури країни та військових об’єктів від ракетних ударів.

Так, своєчасне виявлення нестратегічних балістичних ракет та захоплення їх на автосупроводження вимагає огляду повітряного простору на великих кутах місця і, як правило, у беззавадовій обстановці (відсутності пасивних завад). Виявлення крилатих ракет, як маловисотних цілей, здійснюється на кутах нахилу антенних постів, близьких до нульових, і як правило, на фоні завад від підстилаючої поверхні. Одночасне задовольняння таких суперечливих вимог обумовлює необхідність чіткого розподілення завдань та раціональної побудови бойових порядків угруповання зенітних ракетних військ, що створюється для прикриття об’єктів і військ від ударів нестратегічних балістичних ракет та крилатих ракет.

Прикладом задоволення таких суперечливих вимог є побудова ізраїльської багаторівневої системи протиракетної оборони, в якій використовуються як спеціалізовані ПРК, так і універсальні ЗРК. Аналогічний підхід розподіленого вирішення завдань знищення балістичних та аеродинамічних цілей реалізується в перспективній російській ЗРС С-500 “Прометей”.

УДК 004.056.53

Демидов З.Г., старший науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ

АТАКИ ШИФРУВАЛЬНИКІВ НА СТРАТЕГІЧНО ВАЖЛИВІ ОБ’ЄКТИ

В останні пару років, кажучи про кіберзагрози, найчастіше мають на увазі атаки здирників, а саме шифрувальників. Не залишилися осторонь військові і правоохоронні сили. У 2020-2021 роках з початком пандемії і появою ряду великих угруповань (Maze, REvil, Conti, DarkSide, Avaddon) сформувалася ціла злочинна

екосистема. Це призвело до лавиноподібного зростання числа атак на великі організації по всьому світу, здатні заплатити викуп в сотні тисяч і навіть мільйони доларів США.

Цього року після ряду серйозних інцидентів з шифрувальником, таких як атаки на Colonial Pipeline (оператор найбільшого паливного трубопроводу в США), JBS і Kaseya, і послідував за ними підвищеної уваги з боку влади США і інших країн, ринок кіберзлочинців-вимагачів зазнав серйозних змін: деякі угруповання закрилися, інші провели "ребрендинг".

Більшість відомих угрупувань, про які можна почути в новинах останнім часом, як правило, активно за межами країн СНД. У цьому регіоні, проте, організації теж не можуть відчувати себе в безпеці, оскільки є метою десятків менш відомих груп кіберзлочинців-вимагачів.

У цьому огляді ми розповімо про основні родинах троянців-шифрувальників, найбільш активно атакували бізнес та стратегічно важливі військові об'єкти на території СНД в першій половині 2021 року і їх технічні особливості.

BigBobRoss почав свою активність в самому кінці 2018 року і залишається актуальним до сих пір. Основний вектор його поширення – підбір паролів до RDP. При запуску BigBobRoss показує оператору технічну інформацію, що містить серед іншого ключ, необхідний для подальшої розшифровки файлів. Також шифрувальник відправляє повідомлення з цією інформацією через Telegram. Вміст папок після шифрування виглядає наступним чином: на початку кожного файлу додається електронна адреса зловмисників і ID жертви, потім йдуть оригінальні ім'я і розширення, а після розширення, яке додається шифрувальником. Крім цього, в кожну папку додається записка з контактами зловмисників. Для шифрування програма використовує симетричний алгоритм AES з ключем розміром 128 біт в режимі ECB (режим простої заміни) з криптографічного бібліотеки CryptoPP. У PDB залишилася інформація про назву проекту. Існує ймовірність, що розробник володіє російською мовою, проте з упевненістю цього стверджувати не можна, оскільки назва може бути лише спробою заплутати сліди.

Crysis – це старий шифрувальник, відомий ще з 2016 року. За свою історію він встиг припинити активність і відродитися знову, і на сьогоднішній день продовжує діяти. Код троянця не змінювався вже кілька років, проте він активно поширюється по схемі партнерської програми (RaaS, Ransomware-as-a-Service). Crysis написаний на C / C ++ і скомпільовано в MS Visual Studio. Зловредів шифрує файли алгоритмом AES-256 в режимі CBC. При запуску троянця генерується 256-бітний ключ AES, який шифрується за алгоритмом RSA-1024 з публічним ключем зловмисника, що містяться в тілі троянця. При шифруванні кожного файлу використовується вищевказаний ключ AES, а також згенерований 128-бітний вектор ініціалізації (IV). У оброблений зловредів файл крім зашифрованого вмісту зберігається IV, зашифрований алгоритмом RSA ключ AES, а також допоміжна інформація, в тому числі строкова мітка зловмисника, хеш SHA1 від використаного публічного ключа RSA, оригінальне ім'я файлу, тип шифрування (для малих і великих файлів по різному вибирається частина файлу для шифрування) і контрольна сума. Типовий вектор атаки Crysis – через несанкціонований доступ по RDP. Зловмисник підбирає облікові дані (атака по словнику, повний перебір, покупка готових списків облікових даних у інших зловмисників), підключається по віддаленому з'єднанню до комп'ютера жертви і запускає троянець вручну.

Phobos відомий з 2017 року. На концептуальному рівні (організація коду,

використані розробниками підходи) Phobos багато в чому близький до Crysis. Подібності дозволяють припустити, що або у цих троянців загальний розробник, або розробник Phobos добре знайомий з принципом роботи Crysis. Однак прямих запозичень коду не виявлено, тобто це все-таки різні сімейства троянців, зібрані з різних початкових кодів. Як і більшість сучасних шифрувальників, Phobos поширюється через партнерську програму (RaaS). Основний вектор зараження - несанкціонований доступ до RDP. Phobos написаний на C / C ++ і зібраний в MS Visual Studio. Для шифрування файлів жертви він використовує алгоритм AES-256-CBC, а ключ AES шифрує за допомогою публічного ключа RSA-1024, що міститься в тілі зловреда.

Cryakl – це, напевно, найдавніший з описуваних в даній статті шифрувальників. Його перша версія була виявлена ще в квітні 2014 року. Втім, в сучасних версіях троянця, схоже, не залишилося жодного рядка коду з тих часів. Cryakl безліч разів переписувався, часто зі значними змінами. Поширюється Cryakl через партнерську програму. Найчастіший вектор атаки на сьогоднішній день – через RDP. Для зручності оператора-зловмисника троянець зібраний з підтримкою графічного інтерфейсу. Установки оператор виставляє вручну у вікні програми. Cryakl написаний на Delphi. Для шифрування файлів жертви сучасна версія Cryakl використовує самопісний симетричний шифр, а для шифрування ключа – алгоритм RSA. Цікава особливість актуальних версій Cryakl, які не зустрічалися в інших шифрувальниках – просунута обробка архівних форматів файлів. Так як архіви можуть бути великими за розміром, то шифрувати їх цілком довго, а при шифруванні довільного фрагмента залишається шанс, що частина вмісту вдасться восстановити без розшифровки. У Cryakl реалізовані спеціалізовані процедури для обробки форматів ZIP, 7z, TAR, CAB і RAR (як старих версій, так і RAR5). Він розбирає кожен із зазначених форматів і шифрує лише критичні частини архіву, в результаті добився високої швидкості роботи і запобігає відновленню даних без розшифровки.

Сюди ж хотілося б додати і такі, як **Cryakl / CryLock**, **CryptConsole**, **Fonix/XINOF**, **Limbozar/VoidCrypt**, **Thanos/Hakbit** та **XMRLocker**.

На території СНД діють як давно відомі, так і порівняно нові шифрувальники, орієнтовані на бізнес та стратегічно важливі військові об’єкти. Багато з них активно розвиваються, а деякі з моменту першого виявлення встигли припинити активність і знову повернутися на ринок. Зловмисники використовують різні техніки шифрування, в тому числі досить цікаві, такі як подвійне шифрування в CryptConsole і обробка архівів в Cryakl. Хоча існують різні вектори поширення зловредів, більшість актуальних на сьогодні шифрувальників, атакуючих організації в СНД, проникають в мережу жертви через RDP. Для протидії цьому важливо використовувати стійкі паролі для доменних облікових записів і регулярно їх міняти. Також рекомендується не відкривати доступ по RDP з інтернету, а для підключення до корпоративної мережі використовувати VPN.

УДК69.033.2

Дерев’янко М.О., старший викладач кафедри технічного та тилового забезпечення факультету логістики Національної академії Національної гвардії України, підполковник

МОДЕРНІЗАЦІЯ МОБІЛЬНИХ ЖИТЛОВИХ КОМПЛЕКСІВ З МЕТОЮ ОПТИМІЗАЦІЇ ЇХ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ