

Ukraine election 2019 polls Maldoc: analysis

4 de April de 2019 Por [Lab52](#)

From Lab52 at S2 Grupo, we have recently detected a malicious document titled "[Ukraine_election_2019_polls.doc](#)". The document was uploaded to Virustotal on March 12nd, 2019 from Germany.

The title and uploading date is especially relevant in this case, because of the existing conflict between Ukraine and Russia and the general elections at Ukraine.

Ukraine election 2019 polls: Who is leading in the polls as Ukraine faces Russian THREAT?

UKRAINE will hold elections on March 31, as 44 candidates battle to win the presidential election race. But who is leading in the polls as Ukraine faces a "serious threat" from Russia?

The three front runners in the Ukraine election race include incumbent President Petro Poroshenko, opposition leader Yulia Tymoshenko and comic actor Volodymyr Zelenskyy. The latest opinion poll, published on Monday, has puts Mr Zelenskyy in first place, with Mr Poroshenko second and Mr Tymoshenko third. Earlier polls also placed the 41-year-old comedian in first place.

The survey, which was carried out by the Kiev International Institute of Sociology, showed Mr Zelenskyy had 15.4 percent of voter support. The current President had 10.5 percent, while the opposition leader had eight percent.

Who is Volodymyr Zelenskyy?

Actor and comic Volodymyr Zelenskyy currently plays a teacher who is elected President of Ukraine in the television show Servant of the People.

Mr Zelenskyy has no political experience but is also a lawyer and businessman. NBC News reported he does not hold rallies in order to gain supporters, but instead, he sells tickets to comedy gigs to share his policies and shares "behind the scenes campaign videos" on Facebook and Youtube.

He has described himself as "very liberal" but if he is elected, he will have to tackle Ukraine's ongoing tensions with Russia.



Document content

Regarding that, the first round of the general elections of Ukrania (15 days before the document was uploaded) took place on March 31st, and the second round will be on April 21st. The result of the elections will have a definitive impact on the conflict between both countries.

To give the reader some geopolitical background, the conflict between Russia and Ukraine began with the Crimea annexation (by the Russian Federation), and has lead to a second conflict due to the disruption of the "*maritime order in the Black Sea and the Sea of Azov*. While the exact content of Ukraine's claims is not publicly known, *it is understood that [Ukraine] include Russia's ongoing construction of a bridge across Kerch Strait and restrictions on passage of Ukrainian vessels through Kerch Strait and the Sea of Azov [...]. Kerch Strait Bridge is intended to create a land connection between Crimea and Krasnodar region which, in light of Ukraine's blockade of Crimea, is crucial for supplies from Russia*".

 [Español](#)

PAGES

- [About](#)
- [Authors](#)
- [Cookies Policy](#)
- [Guest posts](#)
- [Legal Notice](#)
- [Privacy Policy](#)

SEARCH

Search this website ...

AUTHORS

- [Manuel Benet](#) (224)
- [Antonio Villalón](#) (212)
- [Antonio Sanz](#) (103)
- [Colaboradores](#) (84)
- [Maite Moreno](#) (73)
- [Roberto Amado](#) (60)
- [José Rosell](#) (59)
- [Joaquín Moreno](#) (54)
- [Josemi Holguín](#) (54)
- [Jose L. Villalón](#) (50)
- [Joan Soriano](#) (48)
- [Nelo Belda](#) (43)
- [José Vila](#) (43)
- [Antonio Huerta](#) (38)
- [Fernando Seco](#) (38)

[All authors](#)

ARCHIVES

Select Month

META

- [Log in](#)
- [Entries feed](#)



[The text in italics and the image above comes from [this voelkerrechtsblog.org](https://voelkerrechtsblog.org) post and is authored by **Dmytro Koval** and **Valentin J. Schatzl**]

There are three mainly candidates with high probabilities to win the elections: Petro Poroshenko, Yulia Tymoshenko and Volodymyr Zelenskiy. Each one has a specific way to approach the conflict, but the main positions are divided into looking for support from the European Union or get closer to the Russian Federation.

The content of the document [is a real news](#) coming from the conservative and liberal British Daily Express newspaper. European right-wind citizens tend to align against the Kremlin's international policies, what makes this document a good bait.

All the context and sophistication of the content of the document makes it to stand out from the generic campaigns of malware infections, fitting more into TTPs related to APT groups.

Regarding its malicious logic, it depends on macros, which are protected with a password in order to make its analysis more difficult:



Password prompt

This is not a serious problem, since there are many tools that allows to extract them despite that. Once extracted, we see the function responsible for the execution of the threat:



Malware execution function

This function executes the next stages by extracting text in Base64 from the "Company" field of the document metadata, decoding it and launching a "cmd.exe" with WMI.



By executing the next payload through WMI, the process created does not depend on the Microsoft Winword editor but "WmiPrvSE.exe":



The decrypted base64 text consists of a obfuscated Bash command that after several calls to CMD.exe, ends up loading a Powershell.exe with the final Payload.



Base64 encoded payload



Decoded payload

The final Powershell.exe process runs as follows:



Powershell process params

If we take a look, the powershell call has several mistakes in its parameters, in spite of which it is perfectly functional:

- WindowStyl -> WindowsStyle
- EexecutionPol -> ExecutionPolicy

Also, some extra parameters are truncated due to the use of a final "-", but after some iterations of de-obfuscation of the previous command in base64, we have been able to extract several elements that match a payload of a post-exploitation framework known as



Partially deobfuscated payload

```
WorkingHours      False
SlackChannel      False      #general
DefaultProfile    True       /admin/get.php,/news.php,/login/
                                   process.php|Mozilla/5.0 (Windows
                                   NT 6.1; WOW64; Trident/7.0;
                                   rv:11.0) like Gecko
```

Default PowerShell Empire payload config

During its execution, the Powershell process constantly checks the "functiondiscovery.linet" domain through port 8443 using the HTTPS protocol.

26172	1064.059614	185.216.35.182	192.168.0.33	TCP	66	8443 → 49259	[SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
26175	1064.192045	185.216.35.182	192.168.0.33	TCP	54	8443 → 49259	[ACK] Seq=1 Ack=158 Win=30336 Len=0
26176	1064.204190	185.216.35.182	192.168.0.33	TCP	917	8443 → 49259	[PSH, ACK] Seq=1 Ack=158 Win=30336 Len=0
26178	1064.337439	185.216.35.182	192.168.0.33	TCP	113	8443 → 49259	[PSH, ACK] Seq=864 Ack=484 Win=31366 Len=0
26192	1064.730185	185.216.35.182	192.168.0.33	TCP	54	8443 → 49259	[ACK] Seq=923 Ack=766 Win=32512 Len=0
26194	1065.203702	185.216.35.182	192.168.0.33	TCP	144	8443 → 49259	[PSH, ACK] Seq=923 Ack=766 Win=32512 Len=0

Wireshark · Follow TCP Stream (tcp.stream eq 70) · ukrainianos

```
.....F.vh.d...10.<.V.-a...^h[ (. *..L...+3<.
.02.G...J...=
..E.../5...
.....
.2.8.....3.....functiondiscovery.net.
.....Q...M..G.....<.....0.c.c...w8..._...]. ....F.L.KD...<o[ ...4w3...[.
..Y./.....0...0.....(40
..*..H..
.....0
1.0 ..U...US0..
190201105905Z.
200201105905Z0
1.0 ..U...US0.."0
..*..H..
.....0..
.....#Y...@...{U...;..K...|f...nY.....h..W.o\...n%.KHn...[d.
.e..X...30b...@...t.....*...+..F.y.E..b..?.....c.z.jf1..w8...J.{.Gh05.&.L.v...0.^...H...[.Y>.....'q.w'X..).k..R.....
h.D'.m@nn.#.B...O.J.#...zME...4R..g.G.8...e.H.....O.
0".....Yd2k.....P0N0...U.....0ha6..?....X#8Aa".NT0...U.#...0...0ha6..?....X#8Aa".NT0...U.....0
..*..H..
.....LA.I..d.U...)J+.....*..u...b.)Y..o.e...g...W..B.(-.C...^v.....=:..k...d...KdCm...MY<.%... ..|....
3.X...:NZ.....p?...Z..R..*.....v1.!F.\.F.....k.....].A.....4.I].qm...'7...cS...wT...5..U..Q.0..6.?
..D..K.GF.'=.Z...Z...&...Z.....964.FL.q.%..?..r...u.u...t.....rv ..m./>.g... 5Z5...D%.."i..j..wD&.W..
h.....?.....f.....=...kya...h..!&...
```

C2 traffic

Looking for the hash of the document in Virustotal, we see the following comment, which suggests that it may be a dropper of the group APT28 or Hades.


Comments

Mao_Ware

12 days ago

"Suspected Sofacy or Hades Activity Focuses on Upcoming Ukraine Elections"


The truth is that in addition to the pattern of infection and the subject of the document (already exploited earlier by this group in their malicious documents), within the macros of this document we see that the names of functions and their use of WMI coincide with another recent document with hash "8cccdce85beca7b7dc805a7f048fcd1bc8f7614dd7e13c2986a9fa5dfbcbdbdfg", which the researcher @VK_intel suggests may be part of the APT28 toolset. In that case, the threat that was embedded was a dll and much more clearly attributed to this group:



Vitali Kremez
@VK_Intel

Seguir

2018-12-20: Possible #APT28/#Sofacy Implant "UDS 2019 Current Agenda.doc" -> Conference on Underwater Defence & Security -> Base64 Encoded Payload as "adobe" and in "AdobeAcrobat" Registry Replace | C2: photopoststories[.com] Exec: {rundll32.exe, %TEMP%\c\lnb,#1} h/t @securitydoggo



UNDERWATER DEFENCE & SECURITY

"CONTROL THROUGH INNOVATION"

2019 CURRENT AGENDA

TDNUK

UDS 2019 Current Agenda.doc

1. Introduction

2. UDS 2019 Current Agenda

3. UDS 2019 Current Agenda

4. UDS 2019 Current Agenda

5. UDS 2019 Current Agenda

6. UDS 2019 Current Agenda

7. UDS 2019 Current Agenda

8. UDS 2019 Current Agenda

9. UDS 2019 Current Agenda

10. UDS 2019 Current Agenda

11. UDS 2019 Current Agenda

12. UDS 2019 Current Agenda

13. UDS 2019 Current Agenda

14. UDS 2019 Current Agenda

15. UDS 2019 Current Agenda

16. UDS 2019 Current Agenda

17. UDS 2019 Current Agenda

18. UDS 2019 Current Agenda

19. UDS 2019 Current Agenda

20. UDS 2019 Current Agenda

21. UDS 2019 Current Agenda

22. UDS 2019 Current Agenda

23. UDS 2019 Current Agenda

24. UDS 2019 Current Agenda

25. UDS 2019 Current Agenda

26. UDS 2019 Current Agenda

27. UDS 2019 Current Agenda

28. UDS 2019 Current Agenda

29. UDS 2019 Current Agenda

30. UDS 2019 Current Agenda

31. UDS 2019 Current Agenda

32. UDS 2019 Current Agenda

33. UDS 2019 Current Agenda

34. UDS 2019 Current Agenda

35. UDS 2019 Current Agenda

36. UDS 2019 Current Agenda

37. UDS 2019 Current Agenda

38. UDS 2019 Current Agenda

39. UDS 2019 Current Agenda

40. UDS 2019 Current Agenda

41. UDS 2019 Current Agenda

42. UDS 2019 Current Agenda

43. UDS 2019 Current Agenda

44. UDS 2019 Current Agenda

45. UDS 2019 Current Agenda

46. UDS 2019 Current Agenda

47. UDS 2019 Current Agenda

48. UDS 2019 Current Agenda

49. UDS 2019 Current Agenda

50. UDS 2019 Current Agenda

51. UDS 2019 Current Agenda

52. UDS 2019 Current Agenda

53. UDS 2019 Current Agenda

54. UDS 2019 Current Agenda

55. UDS 2019 Current Agenda

56. UDS 2019 Current Agenda

57. UDS 2019 Current Agenda

58. UDS 2019 Current Agenda

59. UDS 2019 Current Agenda

60. UDS 2019 Current Agenda

61. UDS 2019 Current Agenda

62. UDS 2019 Current Agenda

63. UDS 2019 Current Agenda

64. UDS 2019 Current Agenda

65. UDS 2019 Current Agenda

66. UDS 2019 Current Agenda

67. UDS 2019 Current Agenda

68. UDS 2019 Current Agenda

69. UDS 2019 Current Agenda

70. UDS 2019 Current Agenda

71. UDS 2019 Current Agenda

72. UDS 2019 Current Agenda

73. UDS 2019 Current Agenda

74. UDS 2019 Current Agenda

75. UDS 2019 Current Agenda

76. UDS 2019 Current Agenda

77. UDS 2019 Current Agenda

78. UDS 2019 Current Agenda

79. UDS 2019 Current Agenda

80. UDS 2019 Current Agenda

81. UDS 2019 Current Agenda

82. UDS 2019 Current Agenda

83. UDS 2019 Current Agenda

84. UDS 2019 Current Agenda

85. UDS 2019 Current Agenda

86. UDS 2019 Current Agenda

87. UDS 2019 Current Agenda

88. UDS 2019 Current Agenda

89. UDS 2019 Current Agenda

90. UDS 2019 Current Agenda

91. UDS 2019 Current Agenda

92. UDS 2019 Current Agenda

93. UDS 2019 Current Agenda

94. UDS 2019 Current Agenda

95. UDS 2019 Current Agenda

96. UDS 2019 Current Agenda

97. UDS 2019 Current Agenda

98. UDS 2019 Current Agenda

99. UDS 2019 Current Agenda

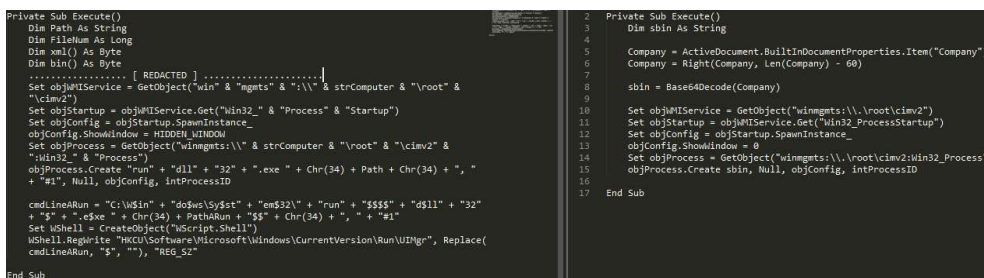
100. UDS 2019 Current Agenda

10:26 - 20 dic. 2018

These are some examples of functions with the same name inside the Macros on both documents and their use of WMI:



Base64decode on both documents



Execute function + WMI logic on both document

Name	IOC
Ukraine_election_2019_polls.doc	8a35b6ecdf43f42dbf1e77235d6017faa70d9c68930bdc891d984a89d1
URL	functiondiscovery[.Jnet:8443/admin/get.php
IP	185.216.35[.]182

*[Subscribe to our Telegram channel for more posts like this:
<https://t.me/BlogSecurityArtWork>]*