

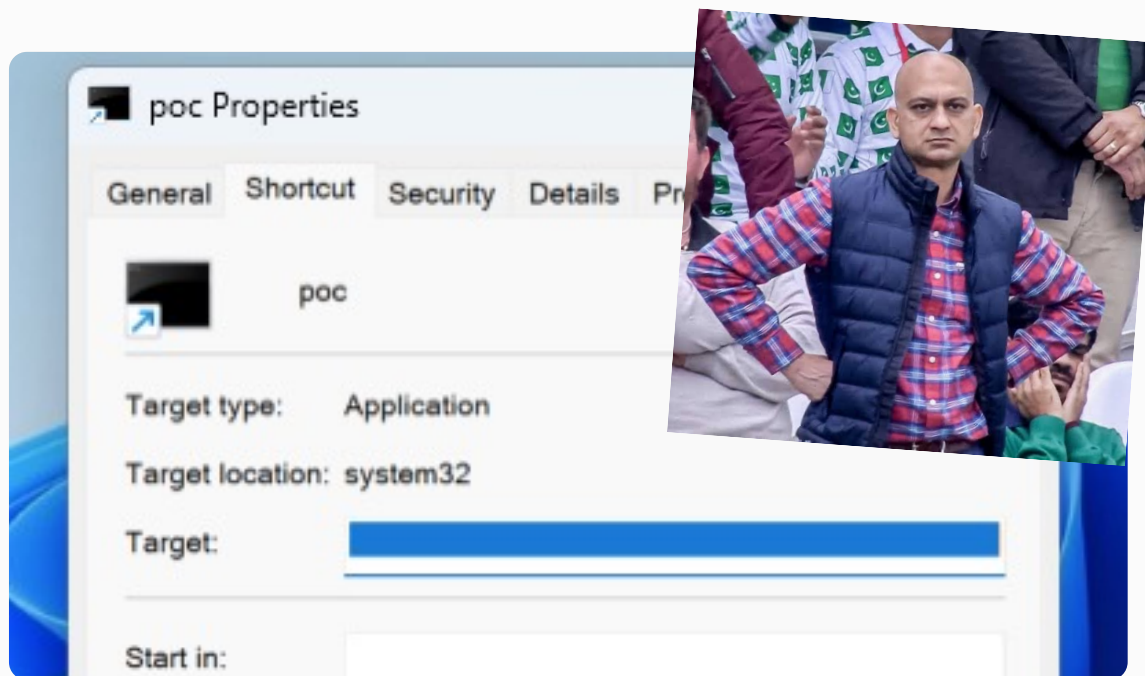
LT #09

**WINDOWS LNK ""ZERO DAY""
EXPLOITED BY "11 STATE-
SPONSORED GROUPS"**

BUT WE COUNTED 12...

ZDI-CAN-25373

MARCH 18, 2025



“Windows Shortcut **Exploit** Abused as **Zero-Day** in **Widespread APT** Campaigns”



“exposes organizations to **significant risks of data theft** and cyber espionage”



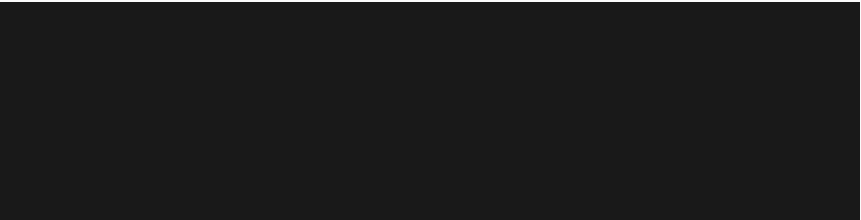
“dating back to **2017** [...] **11 state-sponsored groups** [...] motivated by **cyber espionage** [...] nearly 1000 samples”



YARA pro-tip: strings are optional

```
rule [REDACTED] {  
  condition:  
    (filesize > 100) and (filesize < 90MB)  
    and (uint32(0) == 0x0000004C)  
    and ((uint32be(4) == 0x01140200) and (uint32be(8) == 0x00000000))  
    and (uint8(0x14) & 0x20 == 0x20)  
    and (uint8(0x14) & 0x80 == 0x80)  
    and (  
      ((uint8(0x14) & 0x03 == 0x03)  
      and (  
        (  
          (((uint8(0x14) >> 2) & 0x01) + ((uint8(0x14) >> 3)  
          and for all i in [REDACTED]  
            for any s in [REDACTED]  
              uint16((0x4C + 0x02 + uint16(0x4C) + uint32(0x  
        ))  
      ))  
    ))  
  )  
  or  
    (  
      (((uint8(0x14) >> 2) & 0x01) + ((uint8(0x14) >> 3)  
      and (  
        (for all i in [REDACTED]  
          for any s in [REDACTED]  
            uint16((0x4C + 0x02 + uint16(0x4C) + uint32(
```

THIS IS ALL A LIE!!!!11



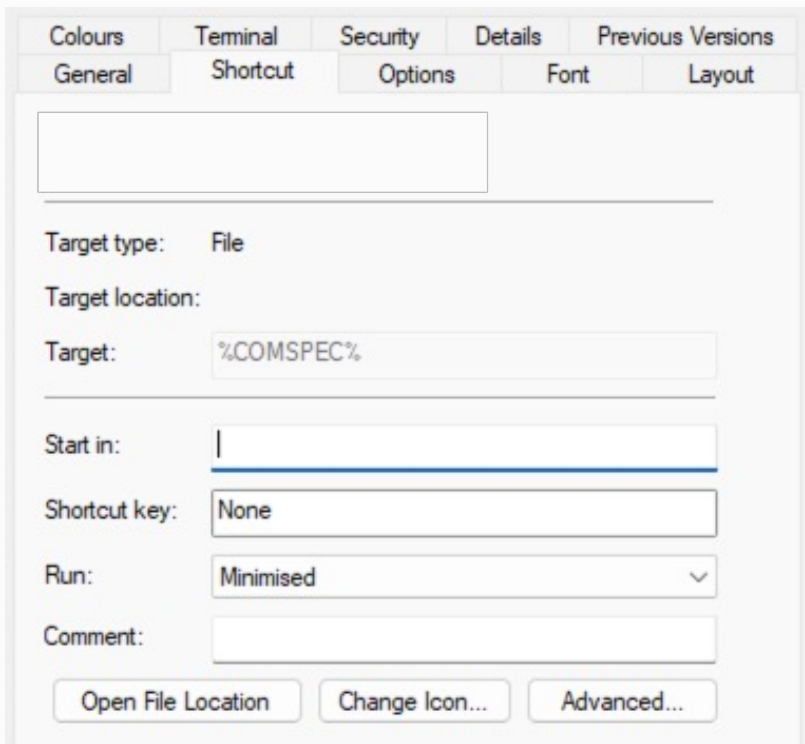
```
STRING_DATA = [NAME_STRING] [RELATIVE_PATH] [WORKING_DIR]
               [COMMAND_LINE_ARGUMENTS] [ICON_LOCATION]
```

All StringData structures have the following structure.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
CountCharacters																String (variable)															



"ZDI-CAN-25373" WITH BENEFITS



Colours Terminal Security Details Previous Versions

General Shortcut Options Font Layout

Target type: File

Target location:

Target: %COMSPEC%

Start in:

Shortcut key: None

Run: Minimised

Comment:

Open File Location Change Icon... Advanced...

Icon index: 135
Windowstyle: SW_SHOWMINNOACTIVE
Hotkey: UNSET - UNSET {0x0000}

LINK INFO: {}

DATA:

Description: ''
Command line arguments: %
Icon location: 齣倣鈴%

EXTRA: {}

LECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
<https://github.com/EricZimmerman/LECmd>

Command Line: -f C:\Users\ .lnk

Processing C:\ .lnk

Error opening C:\ .lnk. Message: Index and count must refer to a location within the buffer. (Parameter 'bytes')

System.ArgumentOutOfRangeException: Index and count must refer to a location within the buffer. (Parameter 'bytes')
at System.Text.UnicodeEncoding.GetString(Byte[] bytes, Int32 index, Int32 count)
at Lnk.LnkFile..ctor(Byte[] rawBytes, String sourceFile, Int32 codepage)
at Lnk.Lnk.LoadFile(String lnkFile, Int32 codepage)
at LECmd.Program.ProcessFile(String lnkFile, Boolean quiet, Boolean removableOnly, String datetimeFormat, Boolean nid, Boolean neb, Int32 codepage)

ANYWAY; THE LNKS...

Unique. First seen mid-March 25, distributed in



Intricate / indirect exec of a stage 1.



Download, exec + persistence for stage 2.

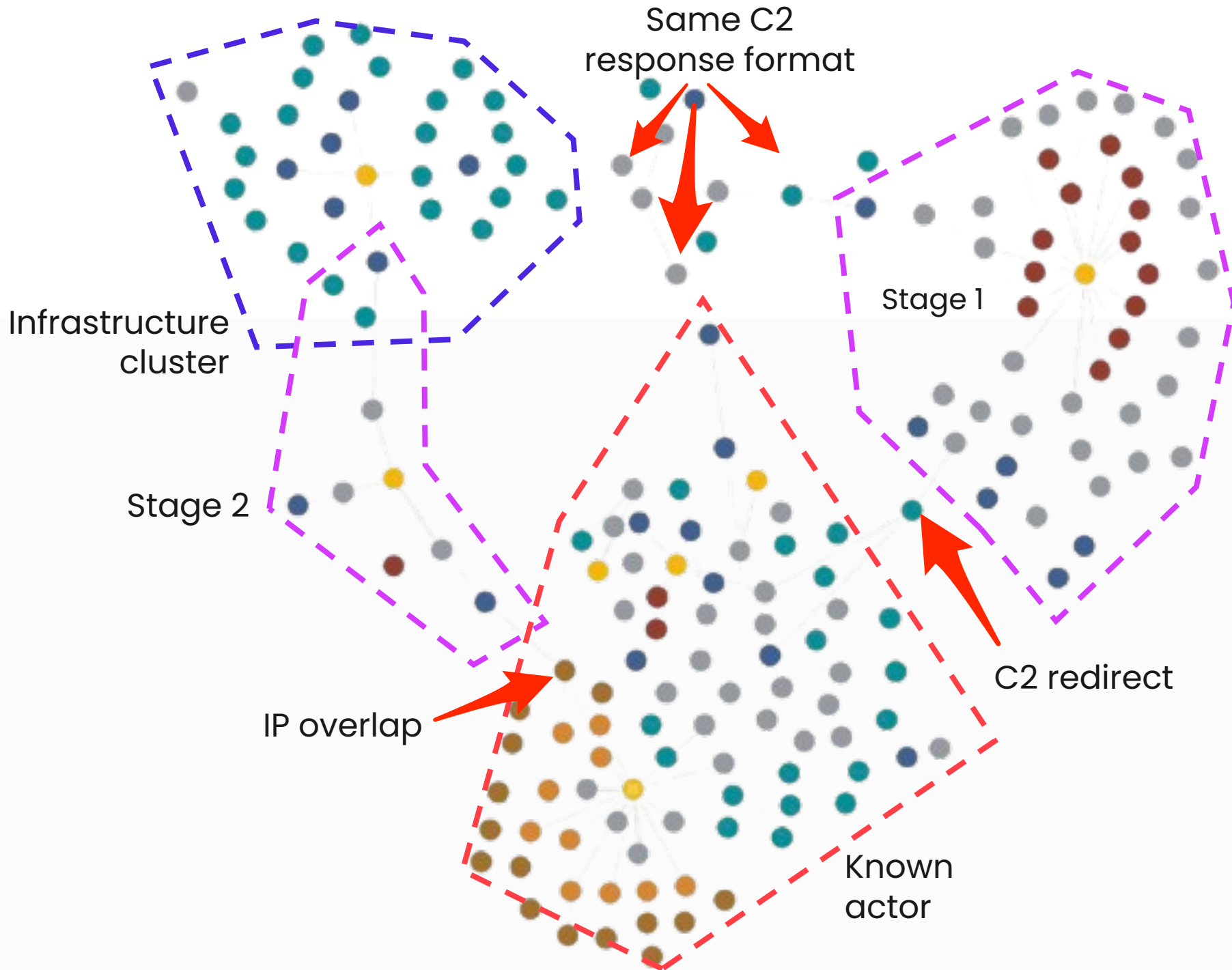


stage 2 candidate.



HERE COME YOUR 12TH

ATTRIBUTION





Pierre DELCHER, Cyber Threat Research
harfanglab.io/insidethelab

