Malicious Office files using fileless UAC bypass to drop KEYBASE malware

By SANS Internet Storm Center

Archived: 2026-04-05 18:36:09 UTC

This is a "Guest Diary" submitted by Ismael Valenzuela and Marc Rivero. Interested in writing a guest diary? Let us know via our contact page.

Macro based malware that hides in Microsoft Word or Excel documents is nothing new to Incident Responders and Malware Analysts.

However, something that caught our attention in the last few days was the use of a 'fileless' method to bypass UAC implemented in a malicious Excel file. This method leverages **eventvwr.exe** and was described in detail by the Enigma0x3 team in this post: https://enigma0x3.net/2016/08/15/fileless-uac-bypass-using-eventvwr-exe-and-registry-hijacking/

Bypassing UAC is nothing new either (see the UACME project created by hfiref0x). In fact, a few days ago we knew of a new **Dridex** sample that attempts to bypass UAC by using application compatibility databases (http://blog.jpcert.or.jp/2015/02/a-new-uac-bypass-method-that-dridex-uses.html). What is most interesting about the method described by the Enigma0x3's team, however, is that it doesn't require any kind of privileged file copy, code injection, or placing a DLL anywhere on the disk.

This particular Excel file employs this UAC bypass method to download and execute a malicious binary that is part of a well-known data-stealing family called **KEYBASE**.

SHA256 HASH: *e431bc1bacde51fd39a10f418c26487561fe7c3abee15395314d9d4e621cc38e*

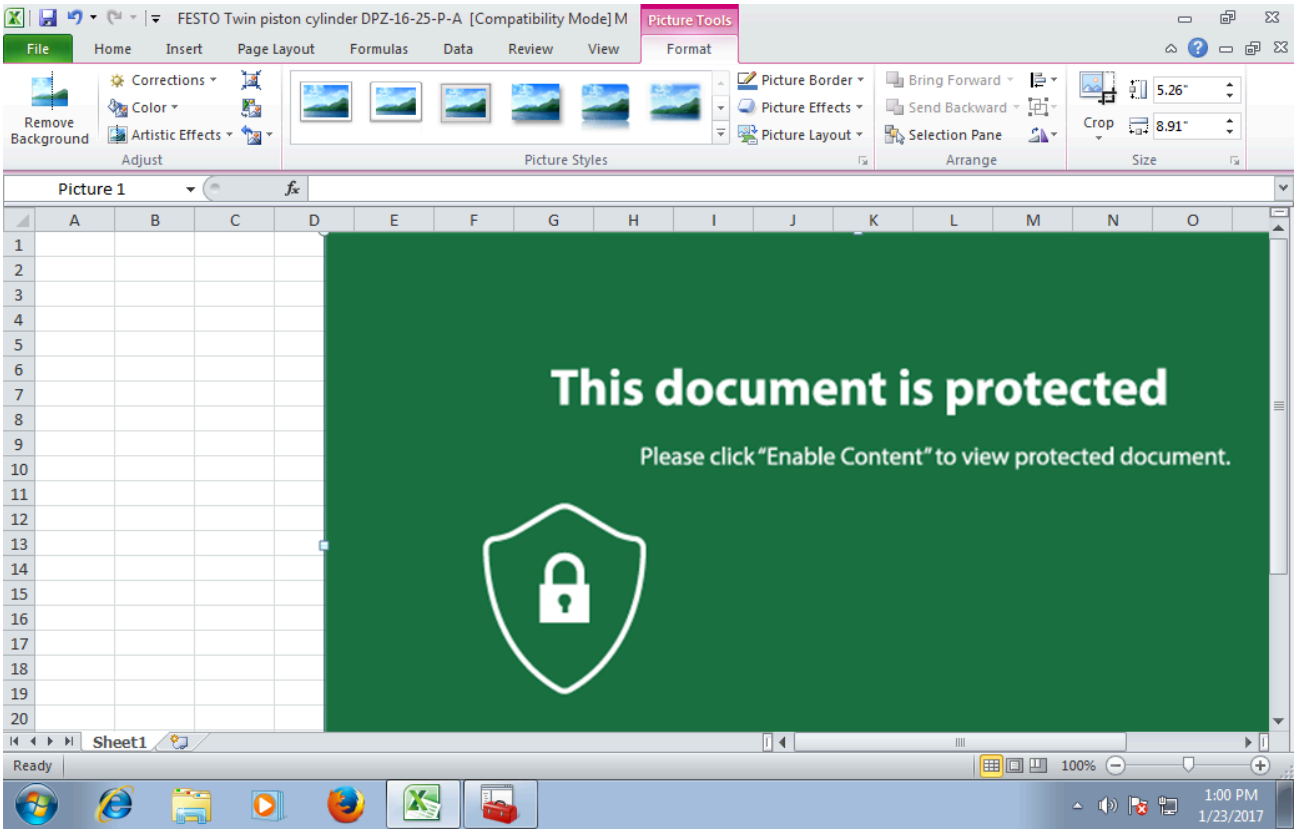


Image 1: This Excel document implements a fileless UAC bypass using eventvwr.exe

KEYBASE is a primarily a keylogger with some other additional capabilities that are commonly found in other non-sophisticated Trojans such as password stealing, clipboard copying, etc.

To understand how this sample behaves and have a look at its capabilities we can use a popular free online resource like "Hybrid Analysis" (https://www.hybrid-analysis.com/) from Payload Security.

Looking at the process list details we can observe what specific processes were spawned when opening the Excel file, along with command line arguments:

Image 2: Dynamic analysis shows the execution of eventvwr.exe and pu457.exe

While the output is pretty self-explanatory, let's dive a bit deeper and explain what's going on there:

- The embedded macro starts a hidden instance of PowerShell.exe (via **cmd.exe**) which downloads a file (mi.exe) from a remote server (**ridart.ru**), storing it in the %TEMP% folder as **pu457.exe**.
- A registry key is added under **HKCU\Software\Classes\mscfile\shell\open\command** pointing to the binary downloaded (more on this on Enigma0x3's post).
- Finally, the PowerShell command invokes **EventViewer.exe**, which will successfully query/open **HKCU\Software\Classes\mscfile\shell\open\command** and execute the malicious file that the registry key points to.
- In case you are wondering, **PING -n 15 127.0.0.1** , as expected, does nothing else but sending 15 ICMP echo requests packets to the iPv4 localhost address, which is just an alternative way to implement the "sleep" command, in an attempt to evade sandbox detection.

The sequence of events described above will ultimately result in code execution **in a high integrity process**, effectively bypassing UAC!

As expected, there is an HTTP connection to **ridart.ru** to download an additional binary (**mi.exe**):

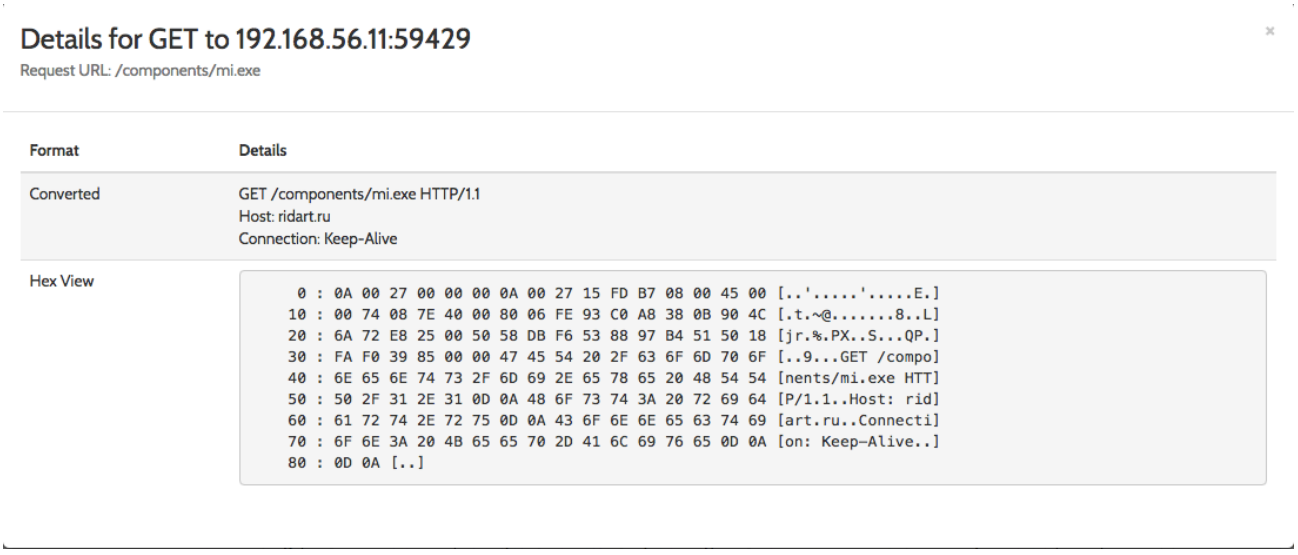


Image 3: Powershell initiates an HTTP GET request to ridart.ru to download mi.exe

The static analysis performed on **pu457.exe** helps us to confirm the capabilities of this Portable Executable:

- **Ability to retrieve keyboard strokes**

```
@43bda5: lea eax, dword ptr [ebp-00000114h]
@43bdab: push eax
@43bdac: call 00407008h ;GetKeyboardState@USER32.DLL
@43bdb1: mov eax, dword ptr [ebx]
```

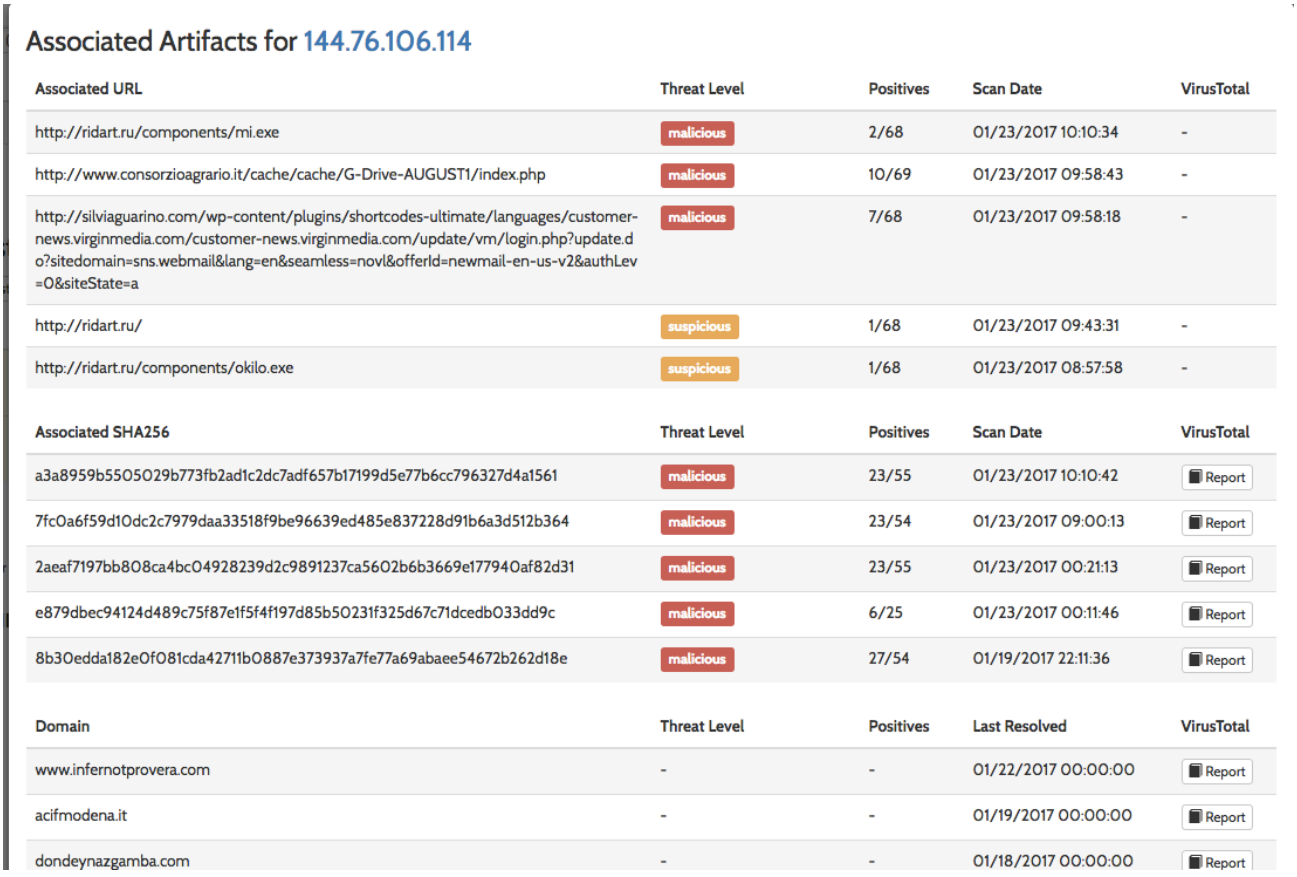
- **Contains ability to query volume size**

```
@408d8f: push edx
@408d90: push eax
@408d91: call 00406990h ;GetDiskFreeSpaceA@KERNEL32.DLL
@408d96: mov ebx, eax
@408d98: mov eax, dword ptr [ebp-04h]
```

- **Contains ability to open the clipboard**

```
@4071de: mov eax, eax
@4071e0: jmp dword ptr [004B15F4h] ;OpenClipboard@USER32.DLL
```

Finally, using these IOCs found during our investigation, we can leverage **Virustotal** (https://www.virustotal.com) to check the reputation of this site and pivot to associated URLs, domains, other related samples. If you check the IP's on the network traffic on Hybrid Analysis, you can extract more malicious information related:



Associated Artifacts for 144.76.106.114

Associated URL	Threat Level	Positives	Scan Date	VirusTotal
http://ridart.ru/components/mi.exe	malicious	2/68	01/23/2017 10:10:34	-
http://www.consorzioagrario.it/cache/cache/G-Drive-AUGUST1/index.php	malicious	10/69	01/23/2017 09:58:43	-
http://silviaguarino.com/wp-content/plugins/shortcodes-ultimate/languages/customer-news.virginmedia.com/customer-news.virginmedia.com/update/vm/login.php?update.do?sitedomain=sns.webmail&lang=en&seamless=novl&offerId=newmail-en-us-v2&authLev=0&siteState=a	malicious	7/68	01/23/2017 09:58:18	-
http://ridart.ru/	suspicious	1/68	01/23/2017 09:43:31	-
http://ridart.ru/components/okilo.exe	suspicious	1/68	01/23/2017 08:57:58	-

Associated SHA256	Threat Level	Positives	Scan Date	VirusTotal
a3a8959b5505029b773fb2ad1c2dc7adf657b17199d5e77b6cc796327d4a1561	malicious	23/55	01/23/2017 10:10:42	Report
7fc0a6f59d10dc2c7979daa33518f9be96639ed485e837228d91b6a3d512b364	malicious	23/54	01/23/2017 09:00:13	Report
2aeaf7197bb808ca4bc04928239d2c9891237ca5602b6b3669e177940af82d31	malicious	23/55	01/23/2017 00:21:13	Report
e879dbec94124d489c75f87e1f5f4f197d85b50231f325d67c71dcedb033dd9c	malicious	6/25	01/23/2017 00:11:46	Report
8b30edda182e0f081cda42711b0887e373937a7fe77a69abaee54672b262d18e	malicious	27/54	01/19/2017 22:11:36	Report

Domain	Threat Level	Positives	Last Resolved	VirusTotal
www.infernotprovera.com	-	-	01/22/2017 00:00:00	Report
acifmodena.it	-	-	01/19/2017 00:00:00	Report
dondeynazgamba.com	-	-	01/18/2017 00:00:00	Report

Image 4: Associated artifacts for 144.76.106.114 (ridart.ru)

As the Enigma0x3 team reminds us in their post, this method to bypass UAC is expected to work on all versions of Windows that implement UAC, including Windows 10, but can be prevented by removing the current user from the Local Administrators group, which is something that you should do anyways!

From a monitoring perspective, it's recommended to monitor and alert on any new registry entries in **HKCU\Software\Classes**, something that can be easily implemented with the latest version of Microsoft's Sysmon, v5 (https://technet.microsoft.com/en-us/sysinternals/sysmon).

Further references:

Full report in Hybrid Analysis:
https://www.hybrid-analysis.com/sample/e431bc1bacde51fd39a10f418c26487561fe7c3abee15395314d9d4e621cc38e?environmentId=100

pu457.exe on Virustotal:
https://www.virustotal.com/es/file/a3a8959b5505029b773fb2ad1c2dc7adf657b17199d5e77b6cc796327d4a1561/analysis/

Information on Keybase:
https://securingtomorrow.mcafee.com/mcafee-labs/malicious-forums-turn-amateur-hackers-into-cybercriminals/

Ismael Valenzuela, GSE #132 (@aboutsecurity)
SANS Instructor & Global Director, Foundstone Services at Intel Security

Marc Rivero @seifreed
Head of Research, Payload Security
