SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

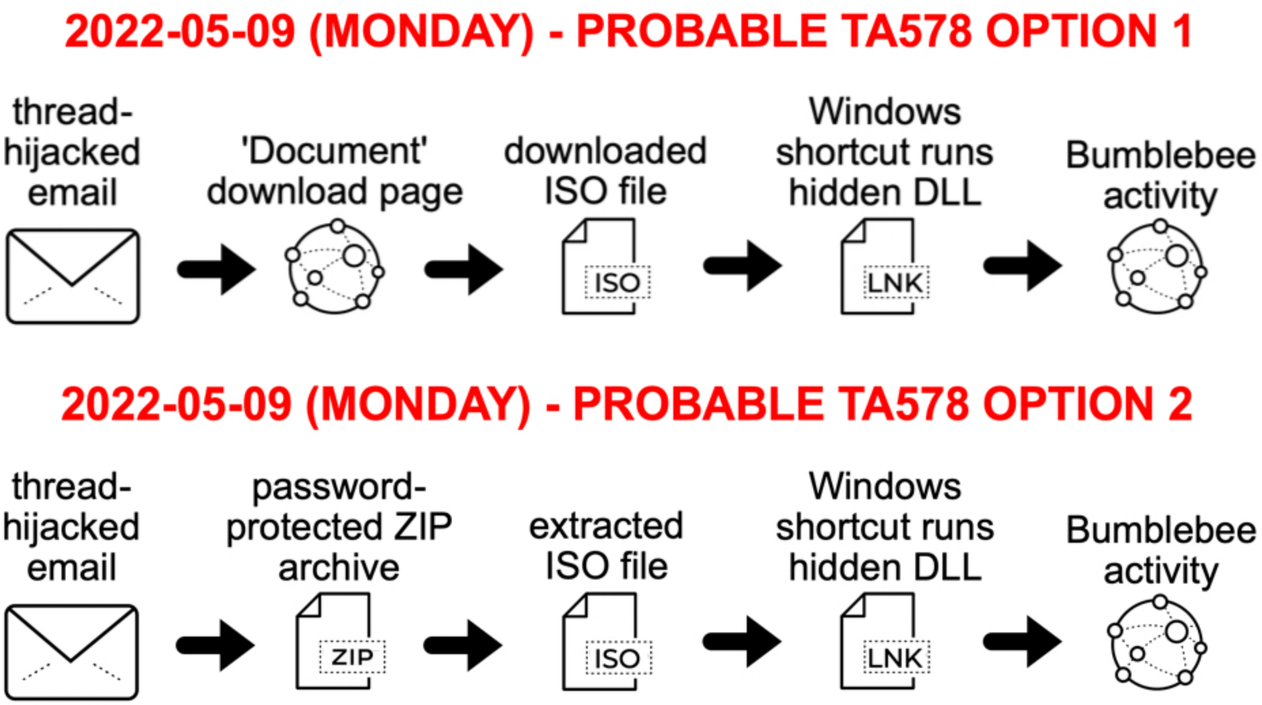
isc.sans.edu/diary/rss/28636

TA578 using thread-hijacked emails to push ISO files for Bumblebee malware

Published: 2022-05-11
Last Updated: 2022-05-11 05:40:22 UTC
by Brad Duncan (Version: 1)
0 comment(s)
INTRODUCTION:

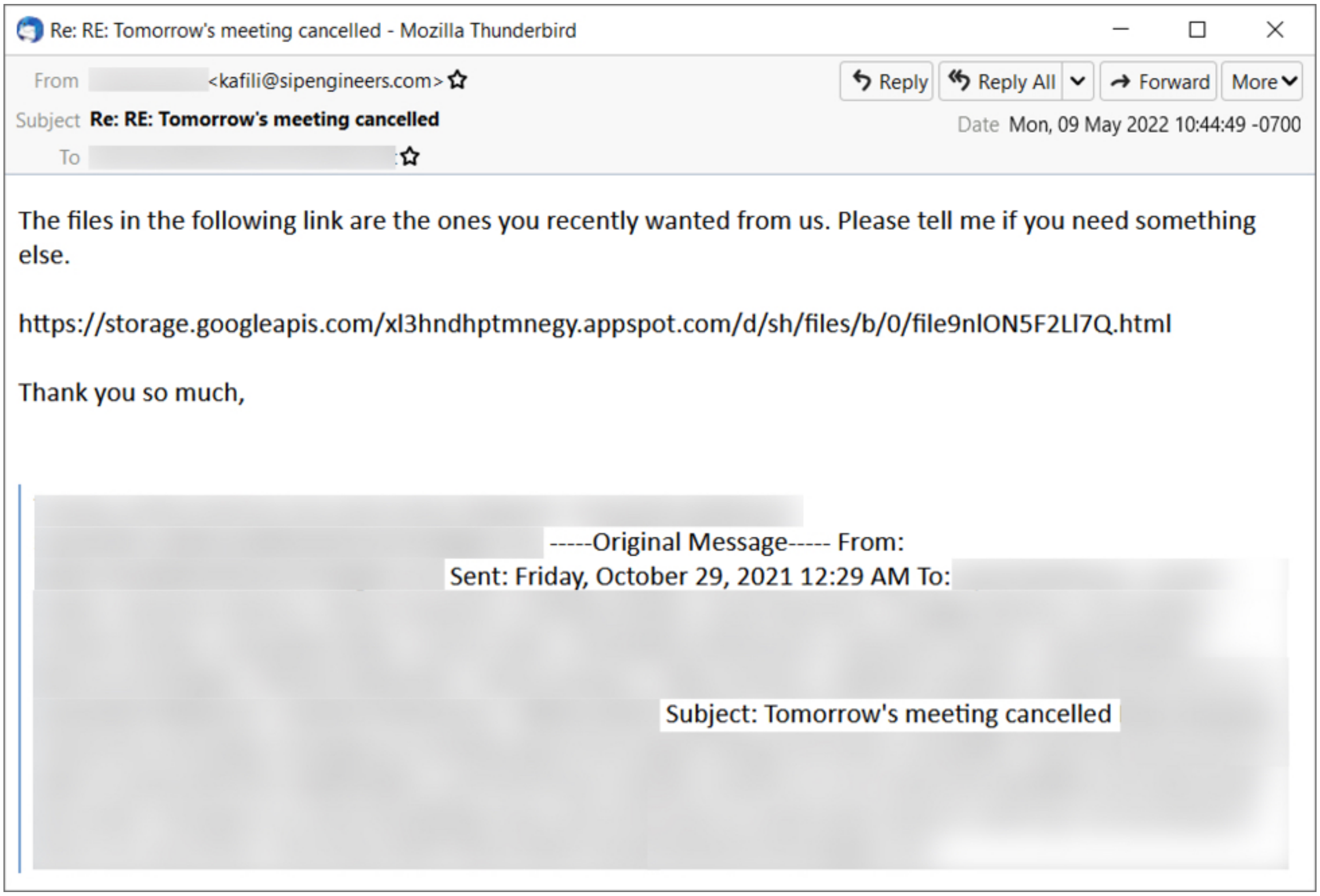
Identified by Proofpoint as the threat actor behind the Contact Forms campaign, TA578 also appears to be pushing ISO files for Bumblebee malware through thread-hijacked emails. These threat-hijacked emails either have links to ***storage.googleapis.com*** URLs similar to those used in the Contact Forms campaign, or they have password-protected zip attachments. Either method delivers an ISO file containing files to install Bumblebee malware.

Today's diary compares two examples of ISO files for Bumblebee malware from Monday 2022-05-09 that appear to be from TA578.


2022-05-09 (MONDAY) - PROBABLE TA578 OPTION 1
thread-hijacked email
'Document' download page
downloaded ISO file
ISO
Windows shortcut runs hidden DLL
LNK
Bumblebee activity
2022-05-09 (MONDAY) - PROBABLE TA578 OPTION 2
thread-hijacked email
password-protected ZIP archive
ZIP
extracted ISO file
ISO
Windows shortcut runs hidden DLL
LNK
Bumblebee activity

Shown above: Infection chains from TA578 on Monday 2022-05-09.

INFECTION CHAIN COMPARISON: LINK TO 'DOCUMENT' DOWNLOAD PAGE:



From [redacted] <kafili@sipengineers.com>

Subject **Re: RE: Tomorrow's meeting cancelled**

To [redacted]

Date Mon, 09 May 2022 10:44:49 -0700

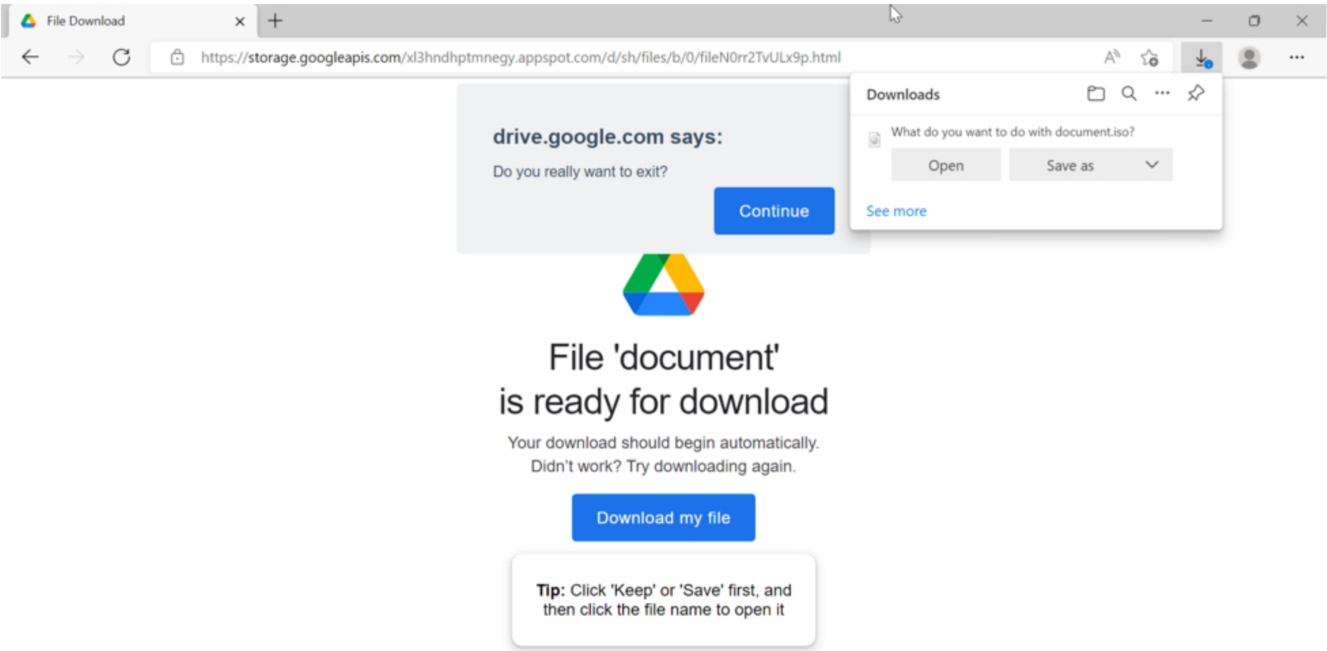
The files in the following link are the ones you recently wanted from us. Please tell me if you need something else.

https://storage.googleapis.com/xl3hndhptmnegy.appspot.com/d/sh/files/b/0/file9nlON5F2Ll7Q.html

Thank you so much,

> [redacted]
> -----Original Message----- From: [redacted]
> Sent: Friday, October 29, 2021 12:29 AM To: [redacted]
> Subject: Tomorrow's meeting cancelled [redacted]

Shown above: TA578 Thread-hijacked email with malicious storage.googleapis.com link.



File Download

https://storage.googleapis.com/xl3hndhptmnegy.appspot.com/d/sh/files/b/0/fileN0rr2TvULx9p.html

drive.google.com says:

Do you really want to exit?

Continue

Downloads

What do you want to do with document.iso?

Open | Save as

See more

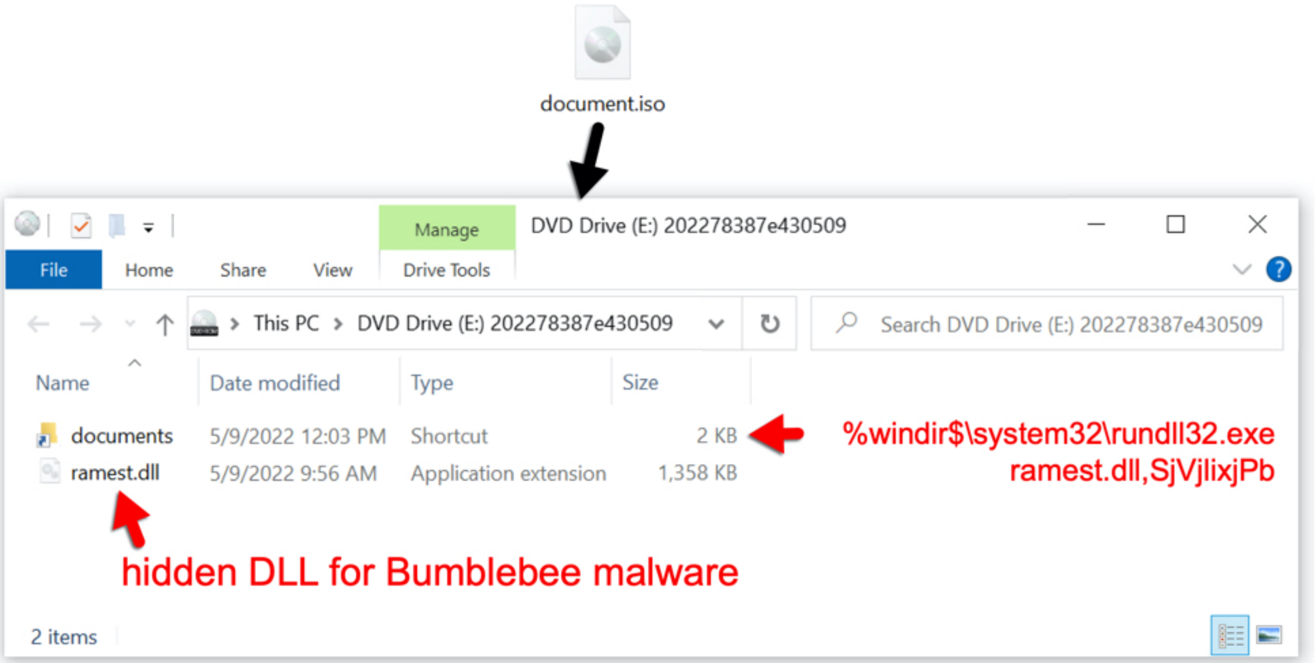
File 'document'
is ready for download

Your download should begin automatically.
Didn't work? Try downloading again.

Download my file

Tip: Click 'Keep' or 'Save' first, and then click the file name to open it

Shown above: TA578 'document' download page hosted on storage.googleapis.com URL delivers malicious ISO file for Bumblebee malware.



document.iso

DVD Drive (E:) 202278387e430509

Manage
File
Home
Share
View
Drive Tools
This PC > DVD Drive (E:) 202278387e430509
Search DVD Drive (E:) 202278387e430509

Name	Date modified	Type	Size
documents	5/9/2022 12:03 PM	Shortcut	2 KB
ramest.dll	5/9/2022 9:56 AM	Application extension	1,358 KB

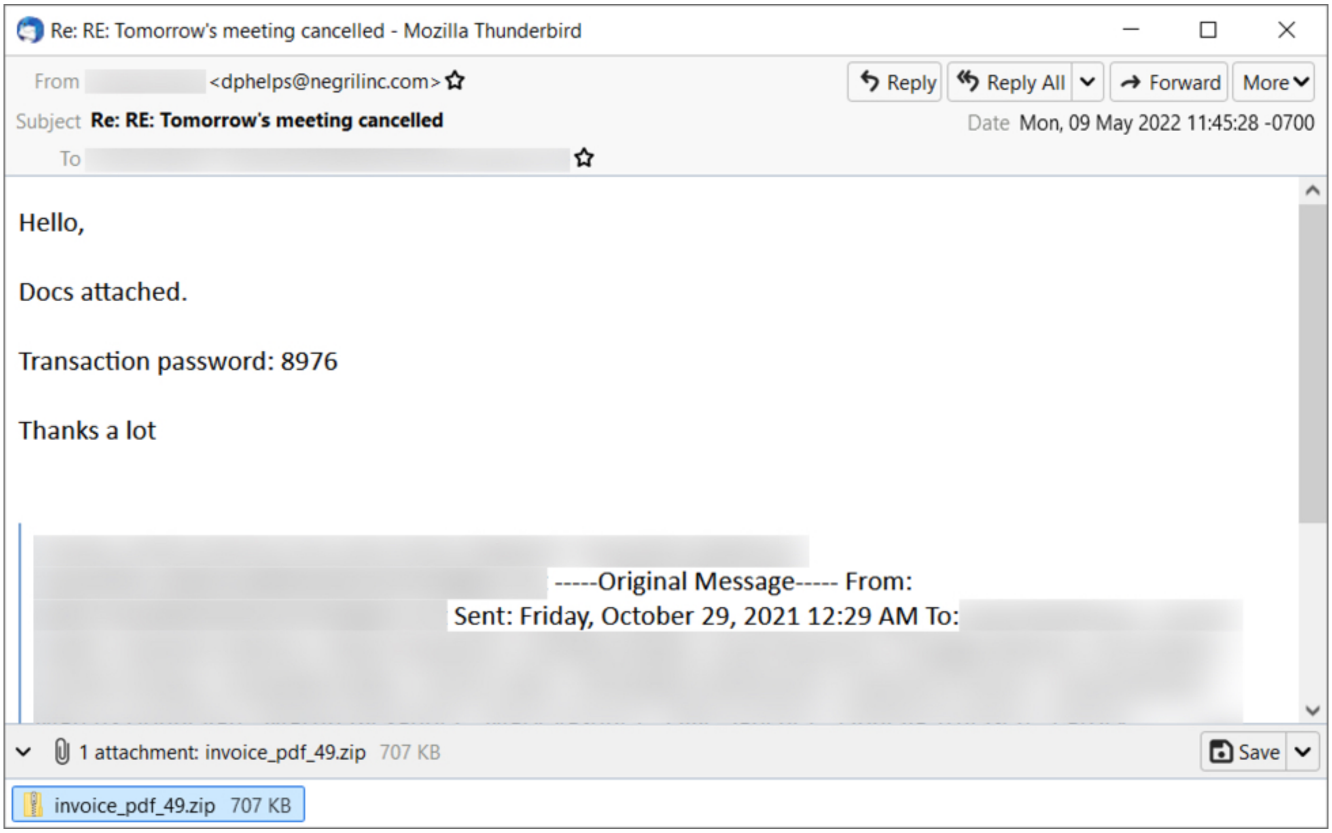
%windir$\system32\rundll32.exe ramest.dll,SjVjlixjPb

hidden DLL for Bumblebee malware

2 items

*Shown above: Contents of downloaded **document.iso** file.*

INFECTION CHAIN COMPARISON: PASSWORD-PROTECTED ZIP ATTACHMENT:



Re: RE: Tomorrow's meeting cancelled - Mozilla Thunderbird

From [redacted] <dphelps@negrilinc.com>

Subject **Re: RE: Tomorrow's meeting cancelled**

Date Mon, 09 May 2022 11:45:28 -0700

To [redacted]

Hello,

Docs attached.

Transaction password: 8976

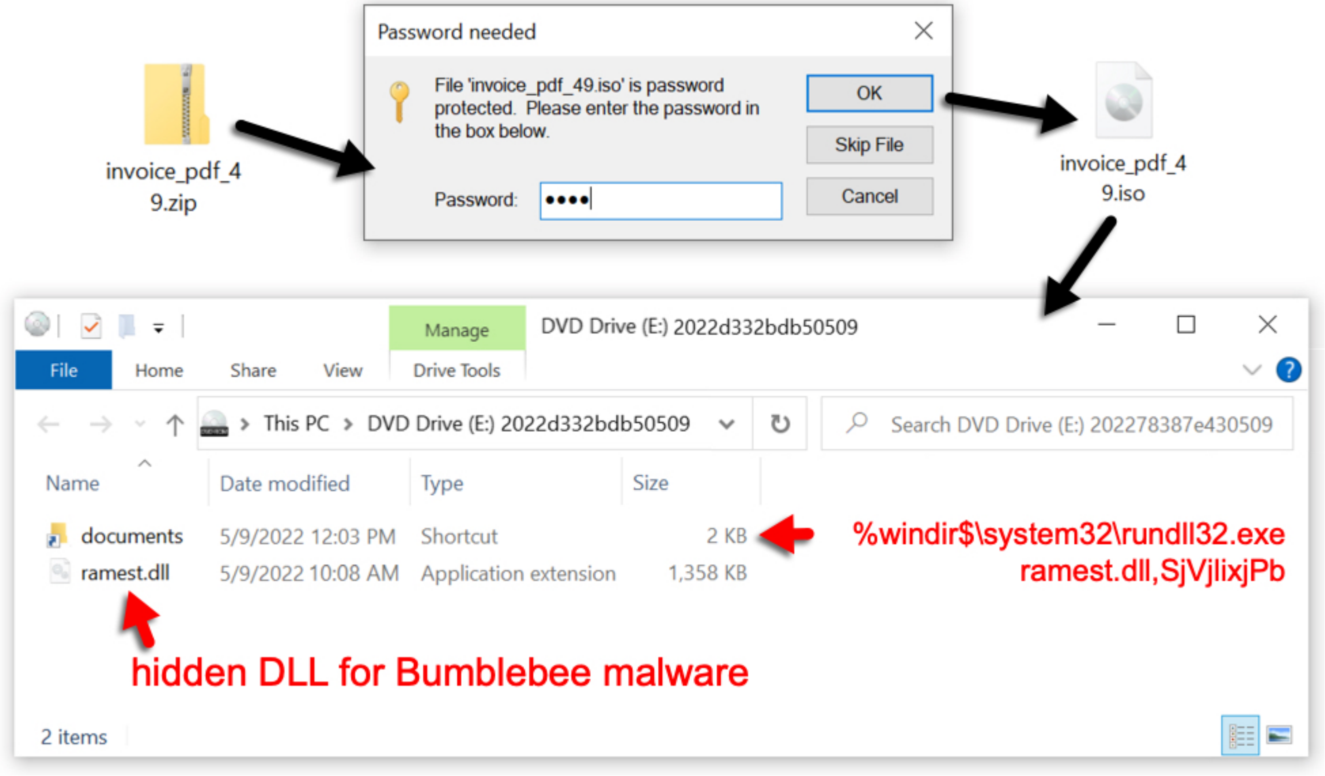
Thanks a lot

[redacted] -----Original Message----- From: [redacted] Sent: Friday, October 29, 2021 12:29 AM To: [redacted]

1 attachment: invoice_pdf_49.zip 707 KB

invoice_pdf_49.zip 707 KB

Shown above: TA578 email with password-protected zip attachment.



Password needed

File 'invoice_pdf_49.iso' is password protected. Please enter the password in the box below.

Password: ••••

DVD Drive (E:) 2022d332bdb50509

Name	Date modified	Type	Size
documents	5/9/2022 12:03 PM	Shortcut	2 KB
ramest.dll	5/9/2022 10:08 AM	Application extension	1,358 KB

%windir$\system32\rundll32.exe ramest.dll,SjVjlixjPb

hidden DLL for Bumblebee malware

Shown above: Malicious ISO file for Bumblebee malware extracted from password-protected zip attachment.

ISO FILE COMPARISON:

SHA256 hash: 330b01256efe185fc3846b6b1903f61e1582b5a5127b386d0542d7a49894d0c2

- File size: 2,883,584 bytes
- File name: ***document.iso***
- File description: malicious ISO file sent by 'documents' download page

SHA256 hash: e9084037805a918e00ac406cf99d7224c6e63f72eca3babc014b34863fb81949

- File size: 2,883,584 bytes
- File name: ***invoice_pdf_49.iso***
- File description: malicious ISO file extracted from password-protected zip attachment

ISO CONTENT COMPARISON:

SHA256 hash: 22e033c76bb1070953325f58caeeb5c346eca830033ffa7238fb1e4196b8a1b9

- File size: 1,612 bytes
- File name: ***documents.lnk***
- File description: Windows shortcut in both ***document.iso*** and ***invoice_pdf_49.iso***
- Shortcut: %windir%\system32\rundll32.exe ramest.dll,SjVjlixjPb

SHA256 hash: e6357f7383b160810ad0abb5a73cfc13a17f4b8ea66d6d1c7117dbcbcf1e9e0f

- File size: 1,390,592 bytes
- File name: ***ramest.dll***
- File description: Bumblebee 64-bit DLL in document.iso

SHA256 hash: f398740233f7821184618c6c1b41bc7f41da5f2dbde75bbd2f06fc1db70f9130

- File size: 1,3900,80 bytes
- File name: ***ramest.dll***
- File description: Bumblebee 64-bit DLL in invoice_pdf_49.iso

Note: Both of the above ***ramest.dll*** files have the same import hash (imphash) of 66356a654249c4824378b1a70e7cc1e5

SIMILARITIES TO CONTACT FORMS CAMPAIGN:

TA578 'document' download pages are similar to 'Stolen Images Evidence' pages used for the Contact Forms campaign. Both are hosted on ***storage.googleapis.com*** pages with ***appspot.com*** in the URL. Both generate traffic to a malicious URL ending in ***logo.jpg*** that returns script with base64 text used to generate a malicious ISO file for download.

The following are 4 examples of URLs generated by 'document' download pages for malicious ISO files in May 2022:

- hxxps://baronrtal[.]com/img/logo.jpg
- hxxps://bunadist[.]com/img/logo.jpg
- hxxps://omnimature[.]com/img/logo.jpg
- hxxps://vorkinal[.]com/img/logo.jpg

The following are 4 examples of URLs generated by 'Stolen Images Evidence' pages for malicious ISO files in May 2022:

- hxxps://bunadist[.]com/images/logo.jpg
- hxxps://curanao[.]com/images/logo.jpg
- hxxps://goranism[.]com/images/logo.jpg
- hxxps://olodaris[.]com/images/logo.jpg

As seen above, 'Stolen Images Evidence' pages generate URLs ending in ***/images/logo.jpg***, while 'document' download pages generate URLs ending in ***/img/logo.jpg***.

URLs hosted on ***storage.googleapis.com*** for 'Stolen Images Evidence' pages end with ***?l=*** or ***?h=*** or similar strings ollowed by a numeric value. For example, ***hxxps://storage.googleapis[.]com/oieqeh1cxwnd81.appspot.com/bl/file/sh/0/fWpa4HT4ck6v6.html?l=827470894993112750*** is a URL for a recent 'Stolen Images Evidence' page.

URLs hosted on ***storage.googleapis.com*** for 'document' download pages end in ***.html***. For example: ***hxxps://storage.googleapis[.]com/pz3ksj5t45tg4t.appspot.com/q/pub/file/0/filejBWdkst6Ua3s.html*** is a URL for a recent 'document' download page.

FINAL WORDS:

The Contact Forms campaign switches between pushing ISO files for Bumblebee malware, or pushing ISO files for IcedID (Bokbot) malware, and I've seen both during the same week. Since February 2022, TA578 has been noted pushing both families of malware. And in recent weeks, TA578 has been using thread-hijacked emails to distribute ISO files for Bumblebee malware. TA578 might also distribute IcedID using the same type of thread-hijacked messages.

While the malware may be different, I occasionally find Cobalt Strike from either Bumblebee or IcedID when testing samples in Active Directory (AD) environments. Cobalt Strike can lead to ransomware or other malicious activity.

If TA578 activity is caught and stopped in its early stages, potential victims might avoid more serious harm.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: TA578 malware Bumblebee
0 comment(s)

Top of page
×

Diary Archives