# New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

bleepingcomputer.com/news/security/new-bumblebee-malware-replaces-contis-bazarloader-in-cyberattacks/

Ionut Ilascu

By
Ionut Ilascu

- April 28, 2022
- 07:45 AM
- 0

A newly discovered malware loader called Bumblebee is likely the latest development of the Conti syndicate, designed to replace the BazarLoader backdoor used to deliver ransomware payloads.

The emergence of Bumblebee in phishing campaigns in March coincides with a drop in using BazarLoader for delivering file-encrypting malware, researchers say.

BazarLoader is the work of the TrickBot botnet developers, who provided access to victim networks for ransomware attacks. The TrickBot gang is now working for the Conti syndicate.

In a report in March on a threat actor tracked as ‘Exotic Lily’ that provided initial access for Conti and Diavol ransomware operations, Google's Threat Analysis Group says that the actor started to drop Bumblebee, instead of the regular BazarLoader malware, to deliver Cobalt Strike.

## Bumblebee delivery methods

Eli Salem, lead threat hunter and malware reverse engineer at Cybereason says that the deployment techniques for Bumblebee are the same as for BazarLoader and IcedID, both seen in the past deploying Conti ransomware.

Proofpoint confirms Salem’s finding, saying that they’ve observed phishing campaigns where “Bumblebee [was] used by multiple crimeware threat actors previously observed delivering BazaLoader and IcedID.”

"Threat actors using Bumblebee are associated with malware payloads that have been linked to follow-on ransomware campaigns" - Proofpoint

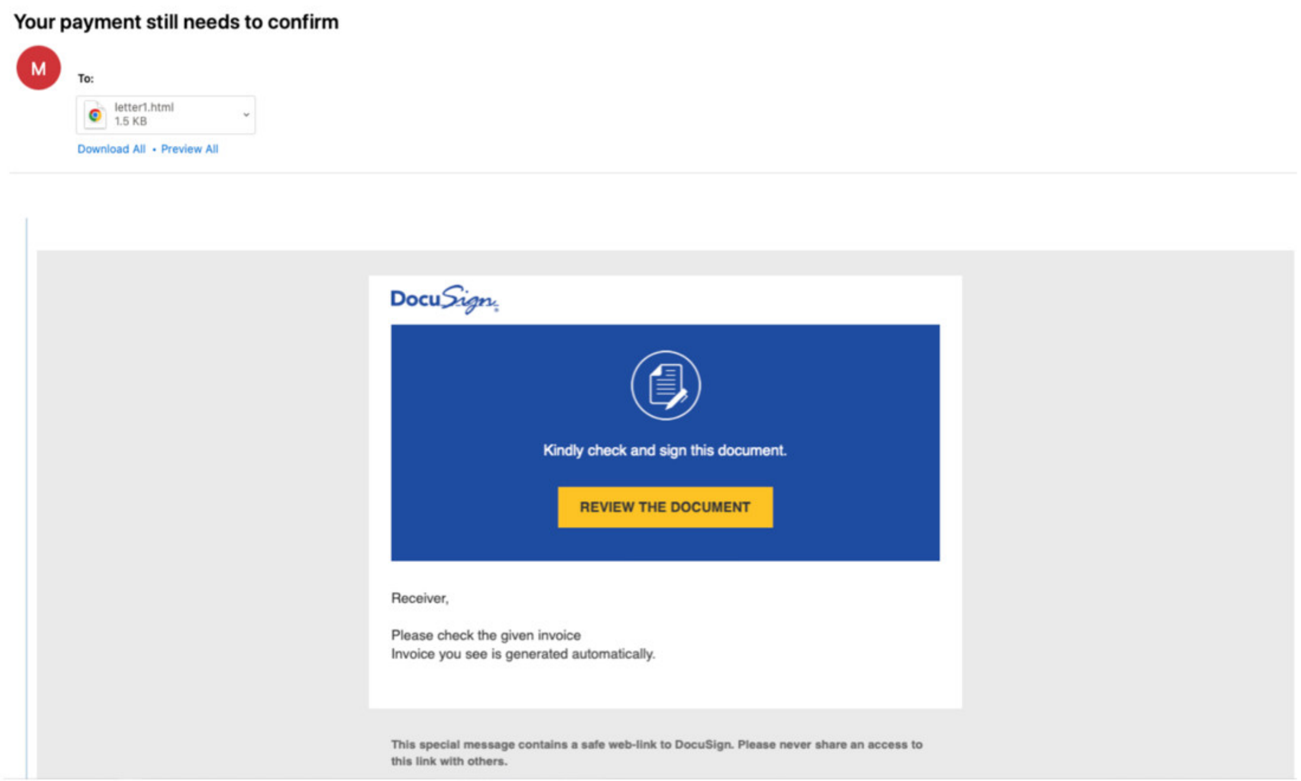
The company also notes that “several threat actors that typically use BazaLoader in malware campaigns have transitioned to Bumblebee” to drop shellcode and the Cobalt Strike, Sliver, and Meterpreter frameworks designed for red team security assessment.

At the same time, BazaLoader has been missing from Proofpoint's data since February.

In a report today, Proofpoint says that it observed multiple email campaigns distributing Bumblebee within ISO attachments that contained shortcut and DLL files.

One campaign leveraged a DocuSign document lure that led to a ZIP archive with a malicious ISO container hosted on Microsoft’s OneDrive cloud storage service.

The researchers say that the malicious email also included an HTML attachment that appeared as an email to an unpaid invoice, Proofpoint says.



Your payment still needs to confirm

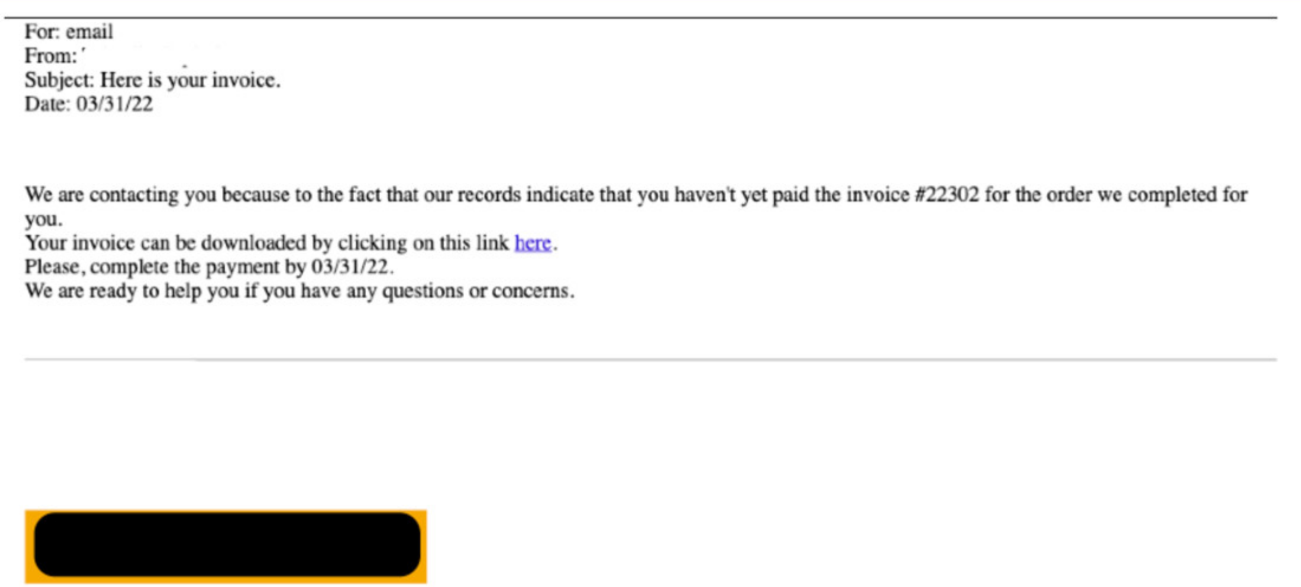
To:

Kindly check and sign this document.

Receiver,

Please check the given invoice
Invoice you see is generated automatically.

This special message contains a safe web-link to DocuSign. Please never share an access to this link with others.



For: email
From: '
Subject: Here is your invoice.
Date: 03/31/22

We are contacting you because to the fact that our records indicate that you haven't yet paid the invoice #22302 for the order we completed for you.
Your invoice can be downloaded by clicking on this link here.
Please, complete the payment by 03/31/22.
We are ready to help you if you have any questions or concerns.

[redacted]

*source: Proofpoint*

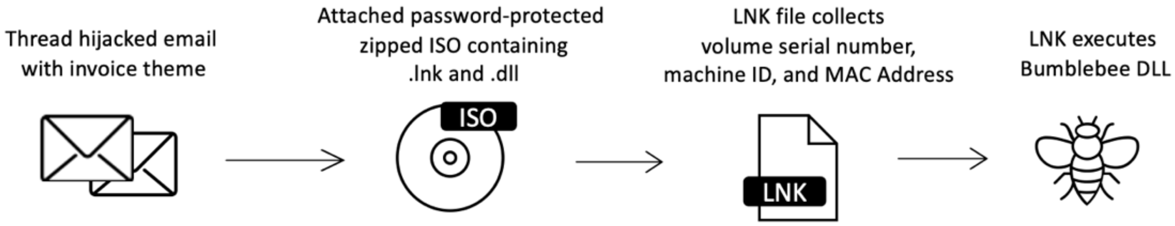
The URL embedded in the HTML file used a redirect service that relies on the Prometheus TDS (traffic distribution service) that filters downloads based on the victim's timezone and cookies. The final destination was also the malicious ISO hosted on OneDrive.

Proofpoint researchers attributed this campaign with high confidence to the cybercriminal group TA579. Proofpoint has tracked TA579 since August 2021. This actor frequently delivered BazaLoader and IcedID in past campaigns

In March, Proofpoint observed a campaign that delivered Bumblebee through contact forms on a target's website. The messages claimed that the website used stolen images and included a link that ultimately delivered an ISO file containing the malware.

Proofpoint attributes this campaign to another threat actor that the company tracks as TA578 since May 2020 and uses email campaigns to deliver malware like Ursnif, IcedID, KPOT Stealer, Buer Loader, and BazaLoader, as well as Cobalt Strike.

The researchers detected another campaign in April that hijacked email threads to deliver the Bumblebee malware loader in replies to the target with an archived ISO attachment.


Thread hijacked email with invoice theme
Attached password-protected zipped ISO containing .lnk and .dll
ISO
LNK file collects volume serial number, machine ID, and MAC Address
LNK
LNK executes Bumblebee DLL

*source: Proofpoint*

Although it has not found undeniable evidence, Proofpoint believes that the threat actors deploying Bumblebee are initial network access brokers working with ransomware actors.

## Highly-complex malware

Researchers agree that Bumblebee is a "new, highly sophisticated malware loader" that integrates intricate elaborate evasion techniques and anti-analysis tricks that include complex anti-virtualization methods.

In a technical analysis on Thursday, Eli Salem shows that Bumblebee's authors used the entire anti-analysis code from the publicly available al-khaser PoC 'malware' application.

Salem's code examination revealed that the malware searches for multiple tools for dynamic and static analysis, it tries to detect "any kind of virtualization environment" by looking for their processes, and by checking registry keys and file paths.

The researcher notes that one of the most interesting things he found in Bumblebee's core loader component is the presence of two 32/64-bit DLL files called RapportGP.dll, a name used by the Trusteer's Rapport security software for protecting sensitive data like credentials.

In its separate technical analysis, Proofpoint found that the Bumblebee loader supports the following commands:

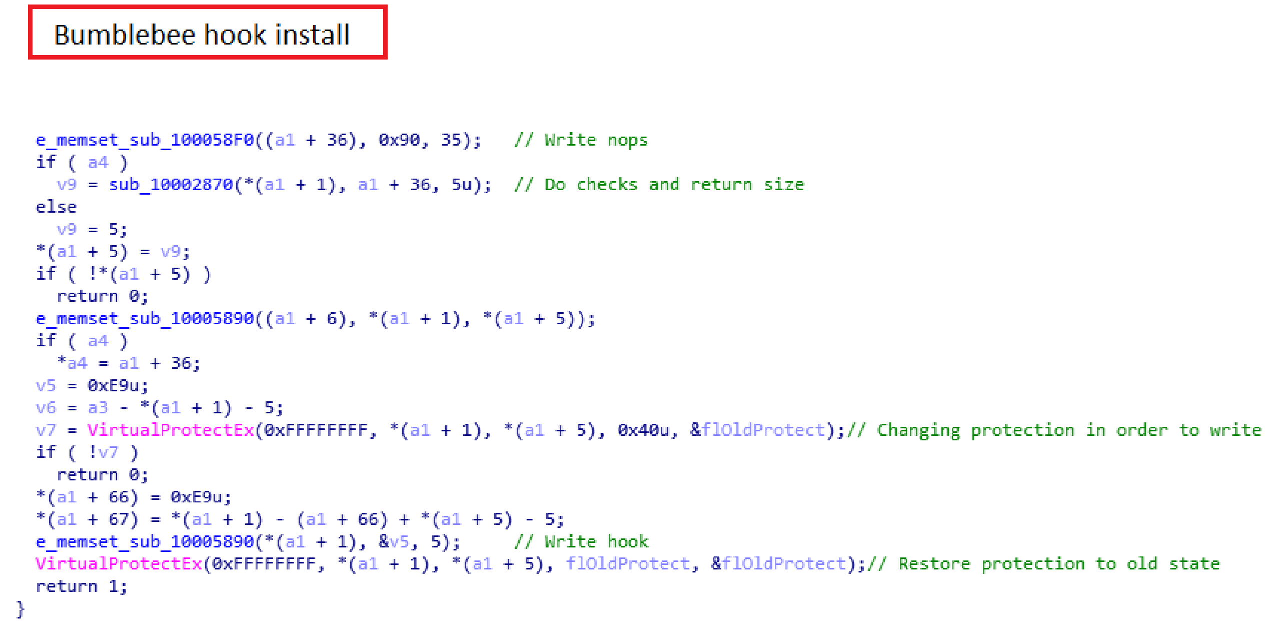
- Shi: shellcode injection

- Dij: DLL injection in the memory of other processes
- Dex: Download executable
- Sdl: uninstall loader
- Ins: enable persistence via a scheduled task for a Visual Basic Script that loads Bumblebee

## Bumblebee uses TrickBot code

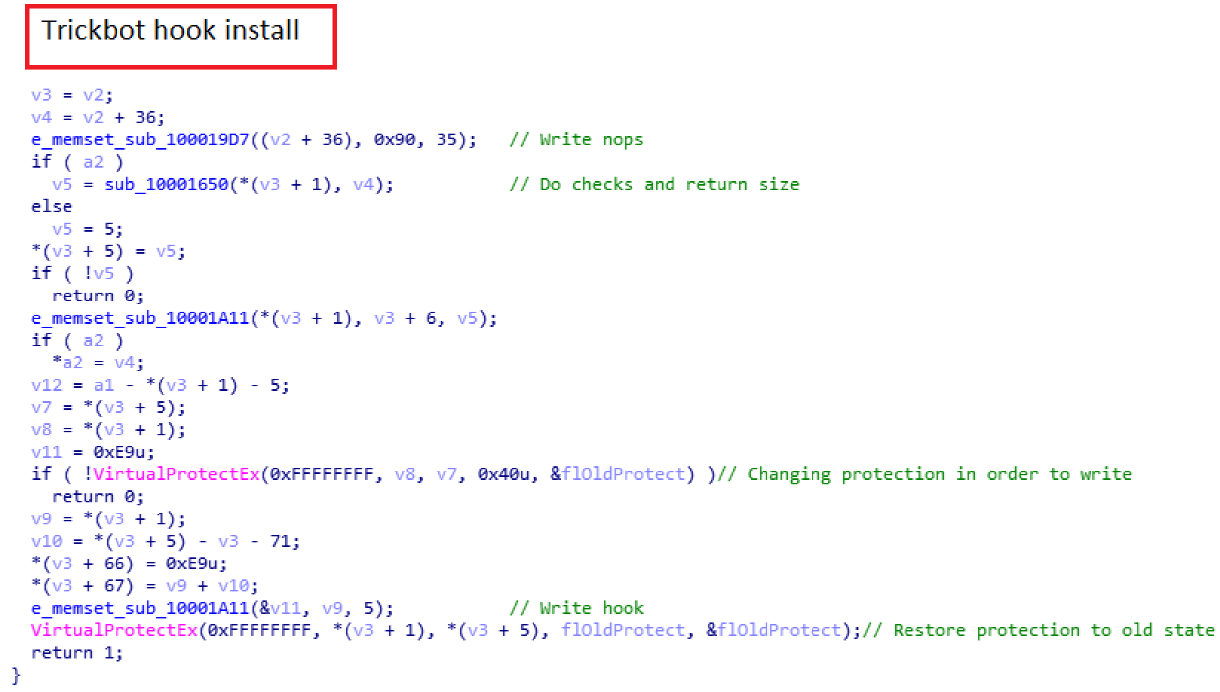
Malware researchers at cybersecurity companies Proofpoint and Cybereason analyzed Bumblebee and noticed similarities with the TrickBot malware in code, delivery methods, and dropped payloads.

Salem established a connection between Bumblebee to TrickBot after seeing that both malware pieces rely on the same installation mechanism for the hooks.



Bumblebee hook install

```
  e_memset_sub_100058F0((a1 + 36), 0x90, 35);   // Write nops
  if ( a4 )
    v9 = sub_10002870(*(a1 + 1), a1 + 36, 5u);  // Do checks and return size
  else
    v9 = 5;
  *(a1 + 5) = v9;
  if ( !*(a1 + 5) )
    return 0;
  e_memset_sub_10005890((a1 + 6), *(a1 + 1), *(a1 + 5));
  if ( a4 )
    *a4 = a1 + 36;
  v5 = 0xE9u;
  v6 = a3 - *(a1 + 1) - 5;
  v7 = VirtualProtectEx(0xFFFFFFFF, *(a1 + 1), *(a1 + 5), 0x40u, &flOldProtect);// Changing protection in order to write
  if ( !v7 )
    return 0;
  *(a1 + 66) = 0xE9u;
  *(a1 + 67) = *(a1 + 1) - (a1 + 66) + *(a1 + 5) - 5;
  e_memset_sub_10005890(*(a1 + 1), &v5, 5);     // Write hook
  VirtualProtectEx(0xFFFFFFFF, *(a1 + 1), *(a1 + 5), flOldProtect, &flOldProtect);// Restore protection to old state
  return 1;
}
```



Trickbot hook install

```
  v3 = v2;
  v4 = v2 + 36;
  e_memset_sub_100019D7((v2 + 36), 0x90, 35);   // Write nops
  if ( a2 )
    v5 = sub_10001650(*(v3 + 1), v4);           // Do checks and return size
  else
    v5 = 5;
  *(v3 + 5) = v5;
  if ( !v5 )
    return 0;
  e_memset_sub_10001A11(*(v3 + 1), v3 + 6, v5);
  if ( a2 )
    *a2 = v4;
  v12 = a1 - *(v3 + 1) - 5;
  v7 = *(v3 + 5);
  v8 = *(v3 + 1);
  v11 = 0xE9u;
  if ( !VirtualProtectEx(0xFFFFFFFF, v8, v7, 0x40u, &flOldProtect) )// Changing protection in order to write
    return 0;
  v9 = *(v3 + 1);
  v10 = *(v3 + 5) - v3 - 71;
  *(v3 + 66) = 0xE9u;
  *(v3 + 67) = v9 + v10;
  e_memset_sub_10001A11(&v11, v9, 5);           // Write hook
  VirtualProtectEx(0xFFFFFFFF, *(v3 + 1), *(v3 + 5), flOldProtect, &flOldProtect);// Restore protection to old state
  return 1;
}
```

*source: Eli Salem*

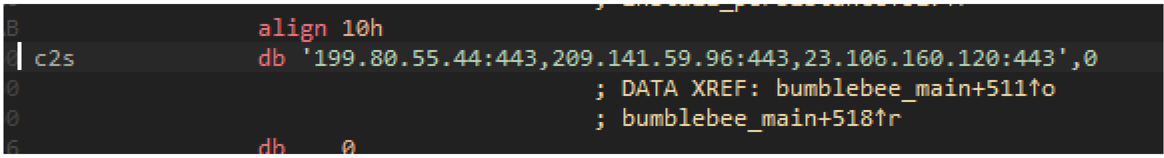
The similarities go even further, as Bumblebee uses the same evasion technique for RapportGP.DLL as TrickBot for its web-inject module.

Additionally, both malware pieces try to use the LoadLibrary and get the address of the function they want to hook, the researcher found.

Salem says that while there isn't sufficient evidence to say that Bumblebee and TrickBot have the same author it is plausible to assume that Bumblebee's developer has the source code for TrickBot's web-inject module.

## Rapid malware development

Bumblebee is actively developed, gaining new capabilities with each update. The most recent one Proofpoint observed is from April 19 and it supports multiple command and control (C2) servers.

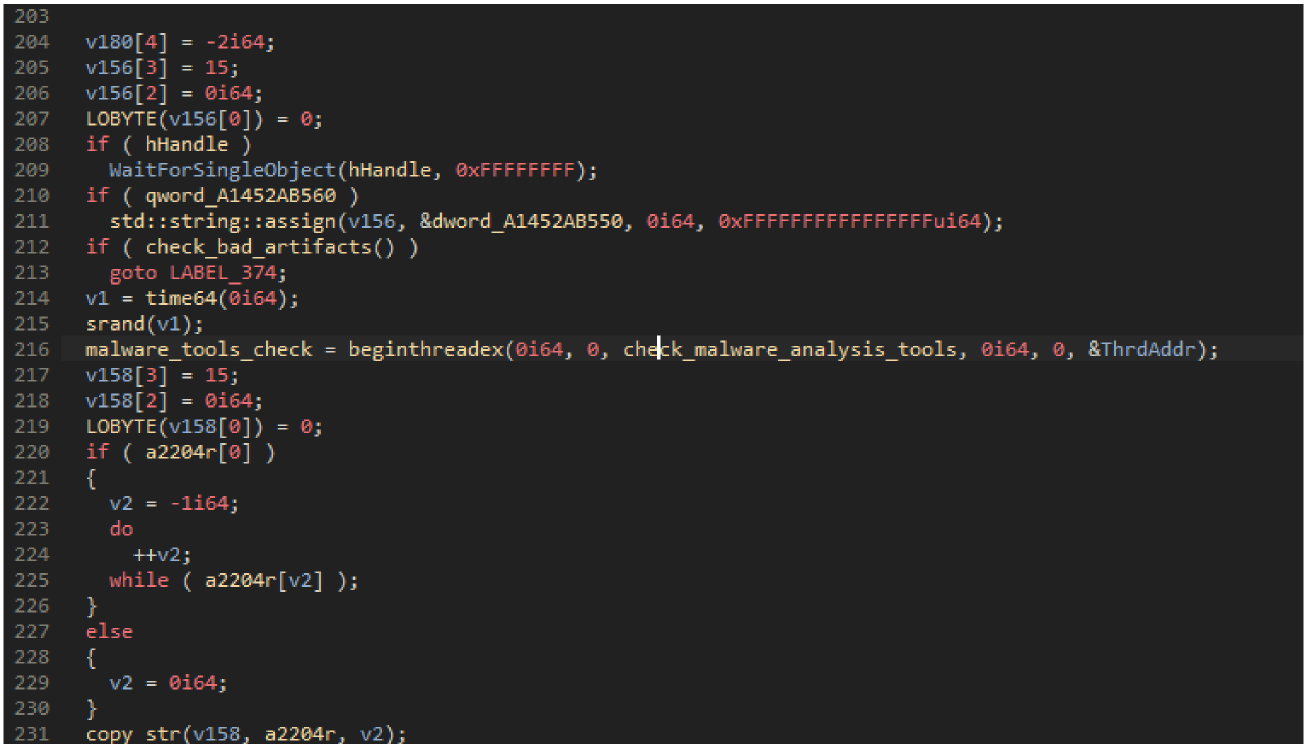


```
                  align 10h
c2s               db '199.80.55.44:443,209.141.59.96:443,23.106.160.120:443',0
                                             ; DATA XREF: bumblebee_main+511↑o
                                             ; bumblebee_main+518↑r
                  db    0
```

*source: Proofpoint*

However, Proofpoint says that the most significant development is the addition of an encryption layer via the RC4 stream cipher for network communications, which uses a hardcoded key to encrypt requests and decrypt responses from the C2.

Another modification appeared on April 22 when researchers noticed that Bumblebee integrated a thread that checks for common tools used by malware analysts against a hardcoded list.



```
  v180[4] = -2i64;
  v156[3] = 15;
  v156[2] = 0i64;
  LOBYTE(v156[0]) = 0;
  if ( hHandle )
    WaitForSingleObject(hHandle, 0xFFFFFFFF);
  if ( qword_A1452AB560 )
    std::string::assign(v156, &dword_A1452AB550, 0i64, 0xFFFFFFFFFFFFFFFFui64);
  if ( check_bad_artifacts() )
    goto LABEL_374;
  v1 = time64(0i64);
  srand(v1);
  malware_tools_check = beginthreadex(0i64, 0, check_malware_analysis_tools, 0i64, 0, &ThrdAddr);
  v158[3] = 15;
  v158[2] = 0i64;
  LOBYTE(v158[0]) = 0;
  if ( a2204r[0] )
  {
    v2 = -1i64;
    do
      ++v2;
    while ( a2204r[v2] );
  }
  else
  {
    v2 = 0i64;
  }
  copy_str(v158, a2204r, v2);
```

*source: Proofpoint*

Proofpoint believes that Bumblebee is a multifunctional tool that can be used for initial access to victim networks to later deploy other payloads such as ransomware.

Sherrod DeGrippo, Vice President of Threat Research and Detection at Proofpoint, says that “the malware is quite sophisticated, and demonstrates being in ongoing, active development introducing new methods of evading detection.”

The reports [1, 2] from Cybereason's Eli Salem and Proofpoint came one day apart and include a detailed technical analysis of Bumblebee malware's most significant aspects.

## Related Articles:

Google exposes tactics of a Conti ransomware access broker

AstraLocker 2.0 infects users directly from Word attachments

Google Drive now warns you of suspicious phishing, malware docs

Fake copyright infringement emails install LockBit ransomware

The Week in Ransomware - June 24th 2022 - Splinter Cells

- BazarLoader
- Bumblebee
- Cobalt Strike
- Conti
- ISO
- Meterpreter
- Phishing
- Ransomware
- Sliver
- TrickBot

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: