DearCry ransomware attacks Microsoft Exchange with ProxyLogon exploits

bleepingcomputer.com/news/security/new-dearcry-ransomware-is-targeting-microsoft-exchange-servers/

Lawrence Abrams

By
Lawrence Abrams

- March 11, 2021
- 07:39 PM
- 1

Threat actors are now installing a new ransomware called 'DEARCRY' after hacking into Microsoft Exchange servers using the recently disclosed ProxyLogon vulnerabilities.

Since Microsoft revealed earlier this month that threat actors were compromising Microsoft Exchange servers using new zero-day ProxyLogon vulnerabilities, a significant concern has been when threat actors would use it to deploy ransomware.

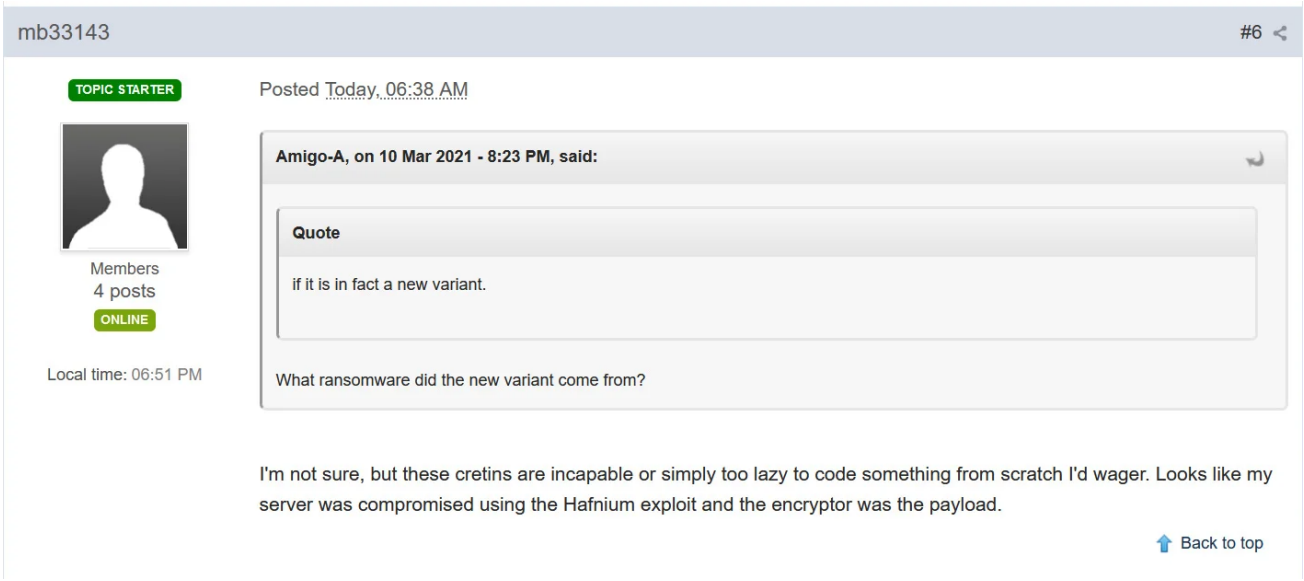
Unfortunately, tonight our fears became a reality, and threat actors are using the vulnerabilities to install the DearCry ransomware.

Attacks started March 9th

According to Michael Gillespie, the creator of the ransomware identification site ID-Ransomware, starting on March 9, users began submitting a new ransom note and encrypted files to his system.

After reviewing the submissions, Gillespie discovered that users submitted almost all of them from Microsoft Exchange servers.

On March 9, a victim also created a forum topic in the BleepingComputer forums where they state their Microsoft Exchange server was compromised using the ProxyLogon vulnerabilities, with the DearCry ransomware being the payload.

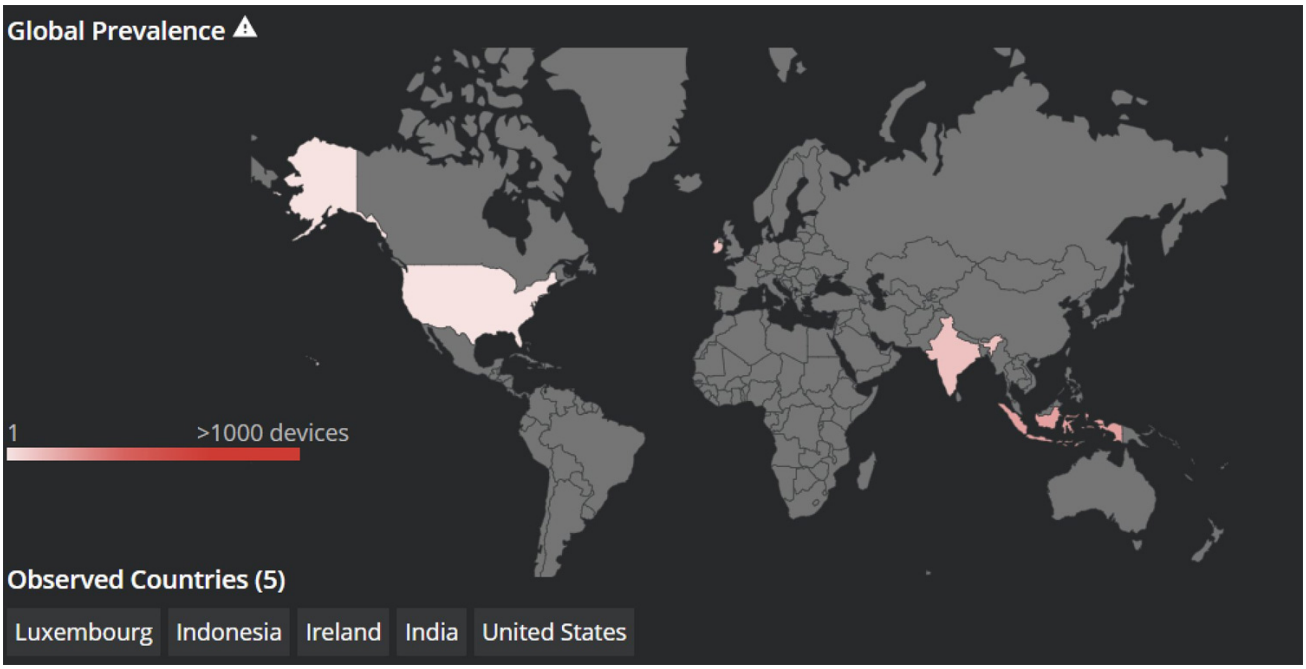


Post about DearCry on BleepingComputer forums

After we broke the news about this attack, Microsoft security researcher Phillip Misner confirmed that the DearCry, or what they call **DoejoCrypt**, is installed in human-operated attacks using the new Microsoft Exchange exploits.

> Microsoft observed a new family of human operated ransomware attack customers – detected as Ransom:Win32/DoejoCrypt.A. Human operated ransomware attacks are utilizing the Microsoft Exchange vulnerabilities to exploit customers. #DearCry @MsftSecIntel
>
> — Phillip Misner (@phillip_misner) March 12, 2021

Today, McAfee's Head of Cyber Investigations John Fokker told BleepingComputer that they are seeing victims in United States, Luxembourg, Indonesia, Ireland, India, and Germany.



Global DearCry heatmap of victims
Source: McAfee Insights

While the detections are still low, Fokker states that the detections are continuing to grow.

AV vendors are currently detecting DearCry using a variety of generic ransomware detections. Below we have listed the more specific detections:

- Ransomware/Win.DoejoCrypt [**AhnLab**]
- Win32/Filecoder.DearCry.A [**ESET**]
- Win32.Trojan-Ransom.DearCry.B [**GDATA**]
- Ransom-DearCry [**McAfee**]
- Ransom:Win32/DoejoCrypt.A [**Microsoft**]
- Ransom.DearCry [**Rising**]
- Ransom/W32.DearCry [**TACHYON**]
- Ransom.Win32.DEARCRY [**TrendMicro**]
- W32.Ransomware.Dearcry [**Webroot**]

How the DearCry ransomware encrypts computers

MalwareHunterTeam was able to find three samples of this ransomware on VirusTotal [1, 2, 3], with addition hashes below, all of which are MingW-compiled executables. The one analyzed by BleepingComputer includes the following PDB path:

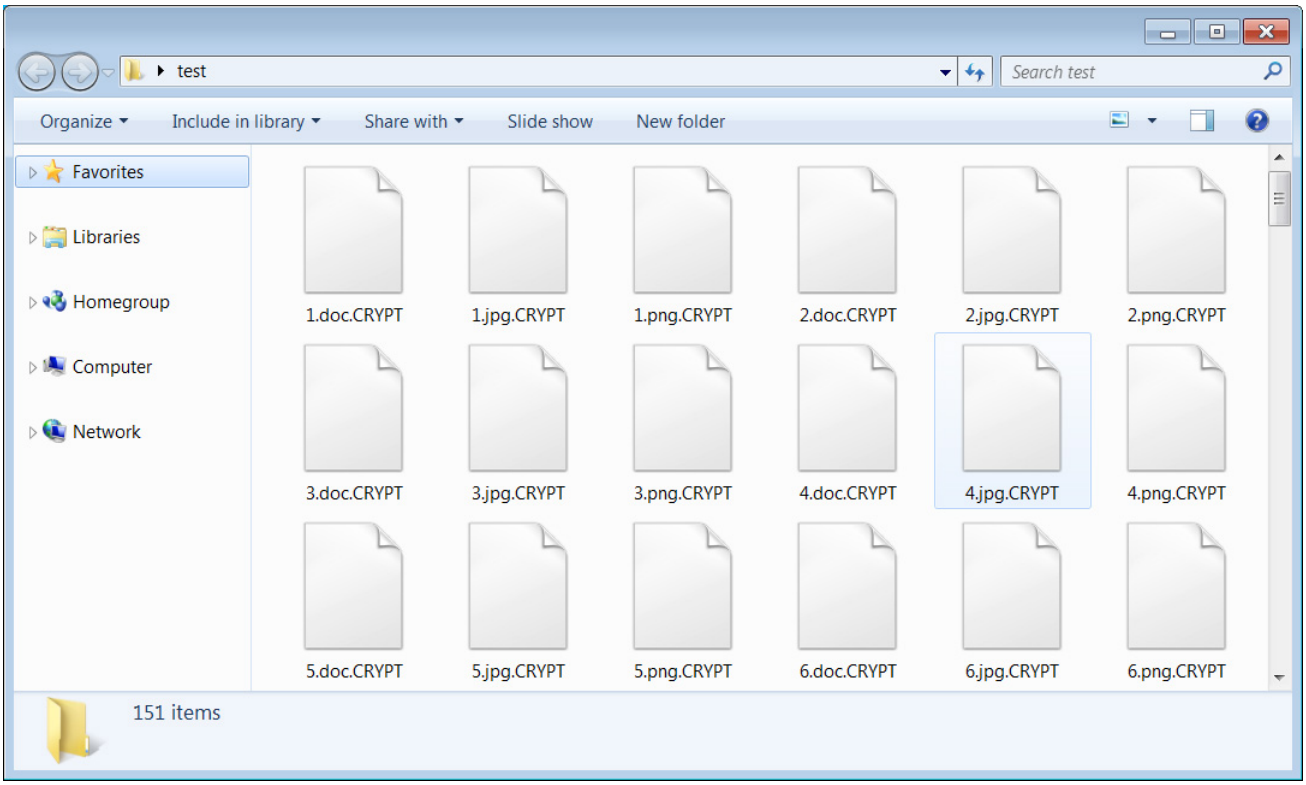
```
C:\Users\john\Documents\Visual Studio 2008\Projects\EncryptFile -
svcV2\Release\EncryptFile.exe.pdb
```

When launched, the DearCry ransomware will create a Windows service named 'msupdate' that is started to perform the encryption. This Windows service is later removed when the encryption process is finished.

The ransomware will now begin to encrypt files on the computer if they match the following extensions:

```
.TIF .TIFF .PDF .XLS .XLSX .XLTM .PS .PPS .PPT .PPTX .DOC .DOCX .LOG .MSG .RTF .TEX
.TXT .CAD .WPS .EML .INI .CSS .HTM .HTML  .XHTML .JS .JSP .PHP .KEYCHAIN .PEM .SQL
.APK .APP .BAT .CGI .ASPX .CER .CFM .C .CPP .GO .CONFIG .PL .PY .DWG .XML .JPG .BMP
.PNG .EXE .DLL .CAD .AVI .H.CSV .DAT .ISO .PST .PGD  .7Z .RAR .ZIP .ZIPX .TAR .PDB
.BIN .DB .MDB .MDF .BAK .LOG .EDB .STM .DBF .ORA .GPG .EDB .MFS
```

When encrypting files, it will append the **.CRYPT** extension to the file's name, as shown below.



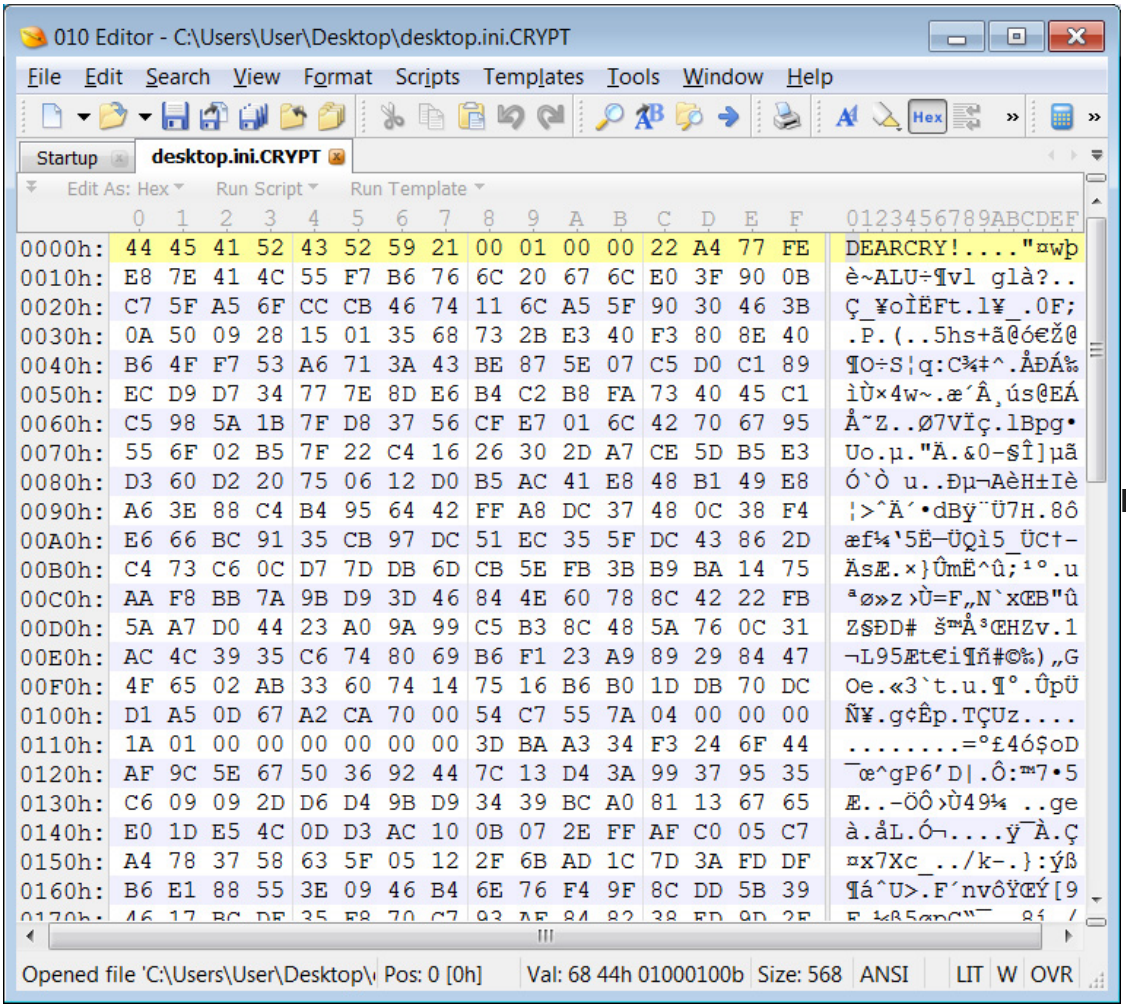
DearCry encrypted files

Embedded in each sample of DearCry is a public RSA-2048 key.

```
13576 zc%C1
13577 NKeb
13578 -----BEGIN·RSA·PUBLIC·KEY-----
13579 MIIBCAKCAQEAyLBClz9hsFGRf9fk3z0zmY2rz2J1qqGfV48DSjPV4lcwnhCi4/5+
13580 C6UsAhk/dI4/5HwbfZBAiMySXNB3DxVB2hOrjDjIeVAkFjQgZ19B+KQFWkSolube
13581 VdHjwdv74evE/ur9Lv9HM+89iZdzEpVPO+AjOTtsQgFNtmVecC2vmw9m60dgyR/1
13582 CJQSg6Moblo2NVF50AK3cIG2/lVh82ebgedXsbVJpjVMc03aTPWV4sNWjTO3o+aX
13583 6Z+VGVLjuvcpfLDZb3tYppkqZzAHfrCt7lV0qO47FV8sFCltuoNiNGKiP084KI7b
13584 3XEJepbSJB3UW4o4C4zHFrqmdyOoUlnqcQIBAw==
13585 -----END·RSA·PUBLIC·KEY-----
13586 dear!!!
13587 .TIF·.TIFF·.PDF·.XLS·.XLSX·.XLTM·.PS·.PPS·.PPT·.PPTX·.DOC·.DOCX·.LOG
13588 WINDIR
13589 TEMP
```

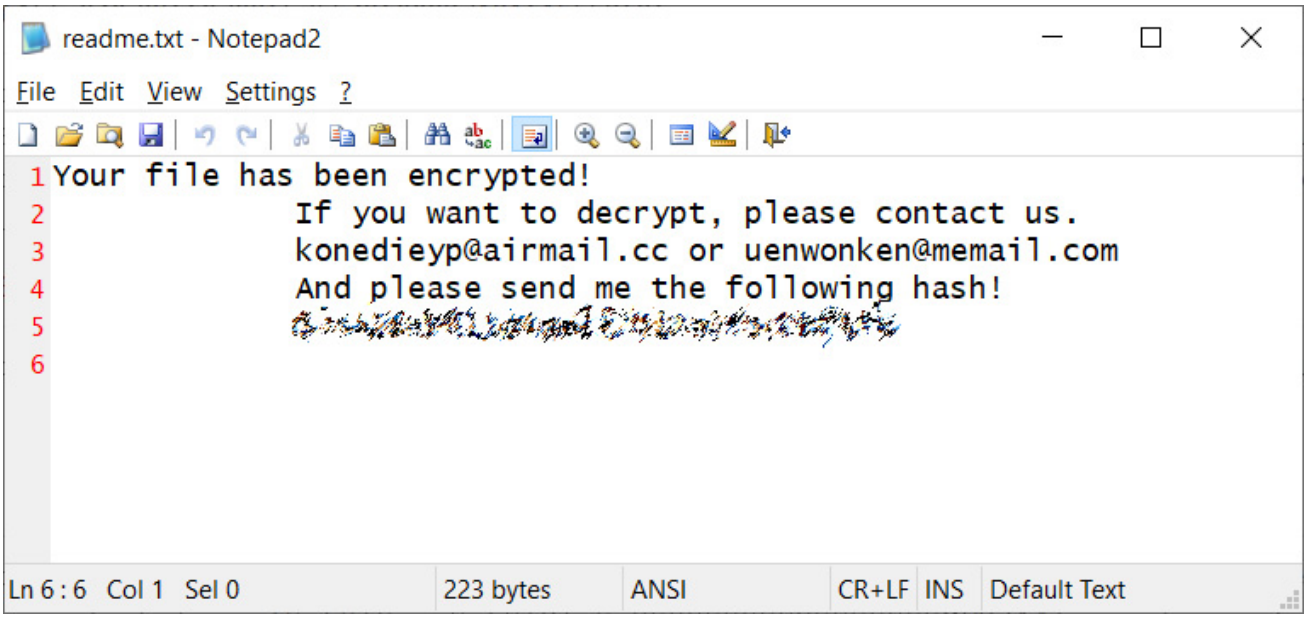
Embedded public RSA key

Gillespie told BleepingComputer that the ransomware uses AES-256 to encrypt the files and the RSA-2048 public key to encrypt the AES key. The ransomware will also prepends the 'DEARCRY!' string to the beginning of each encrypted file.



DEARCRY file marker in encrypted file

When done encrypting the computer, the ransomware will create a simple ransom note named 'readme.txt' on the Windows desktop. This ransom note contains two email addresses for the threat actors and a unique hash, which Gillespie states is an MD4 hash of the RSA public key embedded in the malware.



DearCry ransom note

For at least one of the victims, the ransomware group demanded a $16,000 ransom.

Unfortunately, the ransomware does not appear to have any weaknesses that would allow victims to recover their files for free.

Patch now!

According to new data shared by cybersecurity firm Palo Alto Networks with BleepingComputer, tens of thousands of Microsoft Exchange servers have been patched over the last three days.

Unfortunately, Palo Alto Networks states that there are still approximately 80,000 older servers that cannot directly apply the recent security updates.

“I’ve never seen security patch rates this high for any system, much less one as widely deployed as Microsoft Exchange,” said Matt Kraning, Chief Technology Officer, Cortex at Palo Alto Networks. “Still, we urge organizations running all versions of Exchange to assume they were compromised before they patched their systems, because we know attackers were exploiting these zero-day vulnerabilities in the wild for at least two months before Microsoft released the patches on March 2.”

All organizations are strongly advised to apply the patches as soon as possible and to create offline backups of their Exchange servers.

Not only to protect your mailboxes from being stolen but now to prevent them from being encrypted.

DearCry / DoejoCrypt IOCs

Associated DearCry hashes:

```
SHA256: 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
SHA256: e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
SHA256: feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
SHA256: FDEC933CA1DD1387D970EEEA32CE5D1F87940DFB6A403AB5FC149813726CBD65
SHA256: 10BCE0FF6597F347C3CCA8363B7C81A8BFF52D2FF81245CD1E66A6E11AEB25DA
```

Associated DearCry file names:

```
readme.txt
```

Associated DearCry emails:

```
konedieyp@airmail.cc
uenwonken@memail.com
```

DearCry ransom note text:

```
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp@airmail.cc or uenwonken@memail.com
And please send me the following hash!
[victim id]
```

Update 3/11/21: Updated article after confirmation from Microsoft that it is installed via ProxyLogon vulnerabilities. Added list of targeted extensions and heatmap/victim info from McAfee.
Update 3/12/21: Added AV detection information.
Update 3/13/21: Added IOCs section

Related Articles:

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Microsoft May 2022 Patch Tuesday fixes 3 zero-days, 75 flaws

The Week in Ransomware - May 6th 2022 - An evolving landscape

Magniber ransomware gang now exploits Internet Explorer flaws in attacks

Fake Windows 10 updates infect you with Magniber ransomware

- DearCry
- Exchange
- Microsoft
- ProxyLogon
- Ransomware

- Vulnerability

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

xXHelperXx - 1 year ago

-
-

This is crazy how people can exploit the venerability so quickly

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: