Date: 3rd May, 2021
Problem ID & Name: DearCry Ransomware Attack
Severity: Medium - High

Executive Summary

A new patch of exploits in on-premises variants of Microsoft Trade Server has been effectively misused for more than two months. The adventure, at first ascribed to a Chinese state-supported entertainer, has now been embraced for a scope of cybercrime exercises the most recent being ransomware called DearCry. The DearCry ransomware gives off an impression of being made by an amateur—it is unsophisticated, and does little to conceal itself from identification. Its most remarkable component is that the encryption header that DearCry adds to the assaulted records appears to be like the header-utilised by the famous WannaCry ransomware, which appears to be in excess of a fortuitous event.

The bugs utilised in the adventure CVE-2021-26855 and CVE-2021-27065. The bugs together made a functional pre-validation distant code execution abuse as "ProxyLogon," as it misuses bugs in Return's intermediary design and logon instrument. The wild misuse seems to have begun from 2021. The aggressor composing webshell (ASPX documents) to circle and leading further tasks to dump accreditations, add client accounts, take duplicates of the Dynamic Index information base, and move along the side to different frameworks and conditions subsequent to crediting this mission with high certainty a gathering surveyed to be state-supported and working out of China, in light of noticed victimology, strategies and methodology. The abused way in the endeavour assaults is comparative (/ecp/<single char>.js) and the webshell secret key is "orange"

CVE-2021-26855 & CVE-2021-27065: The Microsoft Trade Server assault chain creatures with the investigation of this blemish, otherwise called a server-side request forgery (SSRF) exploit. At the point when misused, HTTPS associations are set up to verify client access other than introducing every compulsory patch, such untrusted associations can be forestalled by putting the Trade worker inside a VPN to isolate port 443 from outside association demands. Since CVE-2021-26855 is the section point for abusing every one of the other three weaknesses illustrated underneath, remediation endeavours ought to be centred around this openness first. Thus, any remaining auxiliary dangers could be shielded from abuse.
Functionality of DearCry Ransomware

The DearCry ransomware utilizes AES-256 encryption and during its encryption routine to scramble focus on records and afterward utilises an RSA-2048 key to encode the AES key for additional harm. Muddling things further, the public-key cryptosystem used to encode these records has its public encryption key implanted in the ransomware double, which implies that DearCry doesn’t have to contact the aggressor’s order-and-control worker to scramble documents on the worker. Therefore, even Trade Workers arrangement to just permit web admittance to the Trade administrations will in any case get scrambled. Without the unscrambling key, which is held by the aggressors, decoding is absurd.

Two examples of DearCry for this investigation. In both cases, the doubles were unsigned, and showed no proof of form control or other expert advancement rehearsals. The parallels had no safeguard against hostile to infection marks, they were not pressed or muddled, so all ransomware text strings are on display for recognition by experts and mark-based malware insurance. The shortfall of these qualities persuades that the ransomware creator is a fledgling, or that this is an early model. The two examples contained an indistinguishable PDB reference to the machine and source document used to arrange the malware paired:

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

Every binary had all the earmarks of being made exceptionally to be conveyed to the person in question. DearCry utilises a completely independent encryption technique, with the public key implanted inside the ransomware attack, so it doesn’t need to contact a C2 server to start scrambling records. The two examples contemplated were shipped off various casualties and had diverse exceptional identifiers in their payoff notes and utilised various keys. Prior to scrambling a record, DearCry first makes another record with a filename depending on the name of the archive it assaults, however adds a. CRYPT document expansion. Once made, DearCry begins perusing the substance of the first document and composes it back, encoded, into the. CRYPT record. There are two distinctive encryption techniques utilised by DearCry. Documents are scrambled utilising the AES-256 symmetric encryption calculation, utilising an OpenSSL library implanted in the ransomware as stated above.

The AES key itself is scrambled by the assailant with a RSA public-key calculation. A public key for decoding the AES key is installed in the code, however, the private key is held by the assailant. Utilising the RSA encryption of the AES key permits the entertainer to convey the ransomware without requiring an order and control worker to
send the key. Furthermore, the DearCry entertainer can make a ransomware parallel for every casualty, with an extraordinary, casualty explicit public encryption key. Notwithstanding, in view of our discoveries, the entertainer has endeavoured to convey similar pairs to different casualties. Strangely, the rundown of record types the ransomware targets can contrast per casualty. For instance, mainstream picture documents (like JPG), computer aided design drawings, programs (EXE) and dynamic connection libraries (DLL) were not focused in example as demonstrated underneath, which appears to be prior conveyed by the compiler timestamp. Most other ransomware families prohibit projects and DLLs from their rundown of encryption targets on the grounds that encoding some unacceptable documents can bring about the PC getting unbootable, which makes it a lot harder for the casualty to peruse the ransom note.


Taking a gander at these record types, DearCry likewise targets ASPX documents. This would mean the assailant could scramble a Trade webshell that permitted active console from far off. This persuades that the ransomware may not be conveyed through a webshell or that the assailant has no interest in keeping webshell-access.

**DearCry and WannaCry**

Intriguingly, the encryption header that DearCry adds to the assaulted records seems to be like the header utilised by the infamous WannaCry. From an enemy of ransomware point of view, taking a gander at DearCry’s record framework practices uncovers additional fascinating subtleties. DearCry is the thing that is called a Duplicate ransomware. It makes scrambled duplicates of the assaulted records and erases the firsts. This makes the encoded records be put away on various consistent areas, regularly permitting casualties to recuperate perhaps some information – relying upon whether Windows reuses the liberated sensible areas.

Contrasted with DearCry, more infamous human-worked ransomware like Ryuk, REvil, BitPaymer, Labyrinth and Clop, are set up ransomware, where the assault quickly makes the encoded record be put away on intelligently similar areas as the first report, making recuperation through undelete apparatuses unimaginable. In any case, DearCry has an additional stunt to make recuperation unthinkable. Prior to erasing the first report and subsequent to shutting the encoded duplicate, it additionally overwrites the first archive. This implies DearCry has a half and half encryption
approach: it performs both a Duplicate and Set up encryption assault. To educate casualties about what occurred and who they should contact, a record ‘readme.txt’ is dropped in each envelope containing the word ‘desktop’ and in the root organizer of the framework plate. This ransom note contains two email addresses and a hash. This hash is an identifier, so the aggressor understands what unscrambling key is related with the particular assault.

While analysing the IOC, beneath information encountered:

**FileHash-MD5**

*0e55ead3b8fd305d9a54f78c7b56741a*

- MD5:0e55ead3b8fd305d9a54f78c7b56741a
- SHA-1:f7b084e581a8dceaa450c2652f8058d93797413c3
- SHA-256:2b9838da7edboedcd32b086e47a31e8f57333b5981ad8247a2f9508e232589b
- Vhash:016056756d55555173z72z67nz35z67z
- Authenticash:a19ed23411cd99c0427370728563d3dc309130c8d75b124f569155bfb928fa18
- Imphash:f8b8e20e844cc060a58eb73c2fca3626d
- Rich PE header hash:be78f27ebeabcb0f8dec8f6b28e0a6b
- SSDEEP:24576:LU5NX2yJoIXx2wAP0NizkQM+KpPRQ9StUDpl1fpKHKZgMCS+:L7XP7P9o5QzUt1fpKHXZgMC3

*5544ba9ad1b56101b5d52b5270421d4a*

- MD5:5544ba9ad1b56101b5d52b5270421d4a
- SHA-1:fc6f5ece56166d9b4516ba207f3a653b722e1a8df
- SHA-256:511df0e2df9bafa5521b588cc4bb5f8c5a321801b803394ebc405c7db1ef3c78fa1
- SSDEEP:6:aEmAEH2vaW9tuc90GdZLtbNOaL41jEOaDpA0k1gbn:uehSW9tHjbNxyEbnx

*4ef04cba6bec2c3a164b9755efbeb1c*

- MD5:4ef04cba6bec2c3a164b9755efbeb1c
- SHA-1:49644cbbb9d234bd4f7a47ed596c8bbfe2d39065
- SHA-256:8e90ed33c7ee82c0b64078ea36ec95f7420ba435c693b3b3dd728b494abf7d
- Vhashhttm:878fd1c82017ae3a0d1c7fe9a68ed344
- SSDEEP:384:CkswiYDJ439mo+fvF3c7I7p/DNKBIj21WvY51ZD/Dy0fgy:qNb9mo+XFulvWf1Wkyc
By the end, after the above discussion the recommendation and mitigation are as follows:

Promptly introducing the accessible patches on Trade Server, to be prescribed as to confining untrusted associations or setting up a VPN to isolate the Trade Server from outside access. Utilising this relief will just secure against the underlying part of the assault, be that as it may. Different parts of the chain actually can be set off if an aggressor as of now approaches or can persuade an overseer through friendly designing strategies to open a pernicious document. On account of DearCry, no outside association is needed to start encoding documents once the malware has been stacked.

Because of the simplicity of interruption and potential for harm to everyday tasks, notoriety and undesirable arrival of by and by recognizable data (PII) and so forth, it is imperative to keep all AV and IPs marks exceptional. It is additionally imperative to guarantee that all known seller exploits inside an association are tended to and refreshed to secure against aggressors building up a traction inside an organisation.
### References

- [https://www.fortinet.com/blog/threat-research/new-dearcry-ransomware-targets-microsoft-exchange-server-vulnerabilities](https://www.fortinet.com/blog/threat-research/new-dearcry-ransomware-targets-microsoft-exchange-server-vulnerabilities)

### Revision Note:

<table>
<thead>
<tr>
<th>VERSION</th>
<th>DESCRIPTION</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Public Release</td>
<td>Final</td>
</tr>
</tbody>
</table>

### Issued by

Research wing: CyberPeace Foundation

Research Wing, Autobot Infosec Private Ltd.