Delaware Information & Analysis Center
Cyber Alert
July 26, 2018
Captain William Crotty, Director • DIAC@state.de.us • Phone: (302) 739-5996 • Fax: (302) 739-1609

TLP: GREEN

SLTT Governments Receiving Suspicious Envelopes with Malware Infected CDs

Summary
The Delaware Information and Analysis Center (DIAC) is providing the following information for situational awareness. On 07/26/18, the Multi-State Information and Analysis Center (MS-ISAC) advised that several state, local, tribal, and territorial (SLTT) governments reported receiving suspicious envelopes, which contained malware infected CDs that originated from China. To date State Archives, State Historical Societies, and State Departments of Cultural Affairs offices in several states (Delaware included) reported having all received letters addressed specifically to that agency. Key identifiable features of the package include:

- Chinese postmarked envelope
- Confusingly worded typed letter with occasional Chinese characters
- SOCKO brand CD-Rs contained in the envelope

Images of the letter, CD, and envelopes are attached.

Preliminary analysis of the CDs indicate that they contained Mandarin language word (.doc) files, some of which may contain Visual Basic Scripts (VB Script). VB Script is based in part on Microsoft's programming language, Visual Basic. This is used to give functionality and interaction to web pages.

Recommendations
If any agency receives one of these letters, please report it to DIAC. Do not insert the CD into a government computer. If you believe that the CD may have been inserted into a government system:

- Isolate the machine from the network and begin initial triage;
- Contact MS-ISAC CERT for assistance at 1-866-787-4722, or by email at SOC@msisac.org.

DIAC recommends state and local agencies and mail handlers to be on the look out for, and report these envelopes to DIAC at diac@state.de.us

Source
MS-ISAC

TLP: GREEN

Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community. http://www.us-cert.gov/tlp

How are you:

The subject of this letter is to provide scripts, materials, and engineering documents for free.

First of all, on November 11th, 2018, the United States national military parade activities, put forward the use of artificial intelligence for on-site improvised command and dispatch methods, detailed in the attachment, for artificial intelligence professionals, without further questions, can be implemented. This system is suitable for flash entertainment, for Olympic performances, for military operations, etc. It is groundbreaking. The basis is a very mature, existing engineering technology that measures the spatial location of cluster objects.

The <Parade 阅兵> document is immediately filed, and the input database is saved. Parade parade documents are immediately publicized. Whether to delete the public part or not must be accompanied by soliciting opinions from the Chinese Embassy in the United States.

Then, because the fireworks that were set off on the Independence Day of the United States were traditional varieties that had a history of more than 100 years, they remained unchanged and they were not creative. Guided fireworks were proposed to improvise stereoscopic, dynamic, and changing space fireworks. The basis is an existing warhead fuse that injects instructions into the muzzle.

The above two items have opened up a new commercial space, which is the integrated application and comprehensive application of the existing engineering technology. It is the integration of artificial intelligence. This can be used to film new themes. The most prominent feature is that all the new technologies in the film are not fiction and dreams. They are the first to be fully demonstrated in the scenes, props and performances of the film. Application, and, after the film screening, commercial applications are fully carried out.

Unlike the traditional Hollywood fantasy science and technology blockbusters, it is no longer an additional sale of props, costumes, designs, models, ideas, but rather a specific, novel, practical device for sale.

<Guidance fireworks 烟花汇编> File immediately

Ref # 777dd049-6597-4ff4-9484-c7f1f1165e3e

2018-777dd049

archive, immediately enter the database to save, immediately open, and whether to delete the public part, to solicit the review opinions of the Chinese Embassy in the United States, in particular, to point out that people reading this document, in advance To sign this document must not be used to endanger public safety.

In the attachment, many of the documents in the English name <similar-类似-相近>, explain the subject, are abstracts, and have many brief introductions. These descriptions are partially repetitive.

The <similar-类似-相近> document will not be open for 10years.

The <Confidentiality important 临时保密 Report terrorists 举报恐怖分子>/< Report terrorists 举报恐怖分子> document will not be open for 15 years.

All the files on this CD-ROM were immediately disclosed to the U.S. government departments and were immediately made public to large U.S. companies. They immediately immediately disclosed the U.S. university tenured professors. The author gave up the right of authorship, gave up the copyright, and was free to use it.

<Confidentiality important 保密> The document is not open to the general public and is only open to the general public after 30 years.

If you refuse to collect these documents, please transfer them to any individuals, organizations or organizations that are willing to collect these documents. Please do not discard! ! ! !

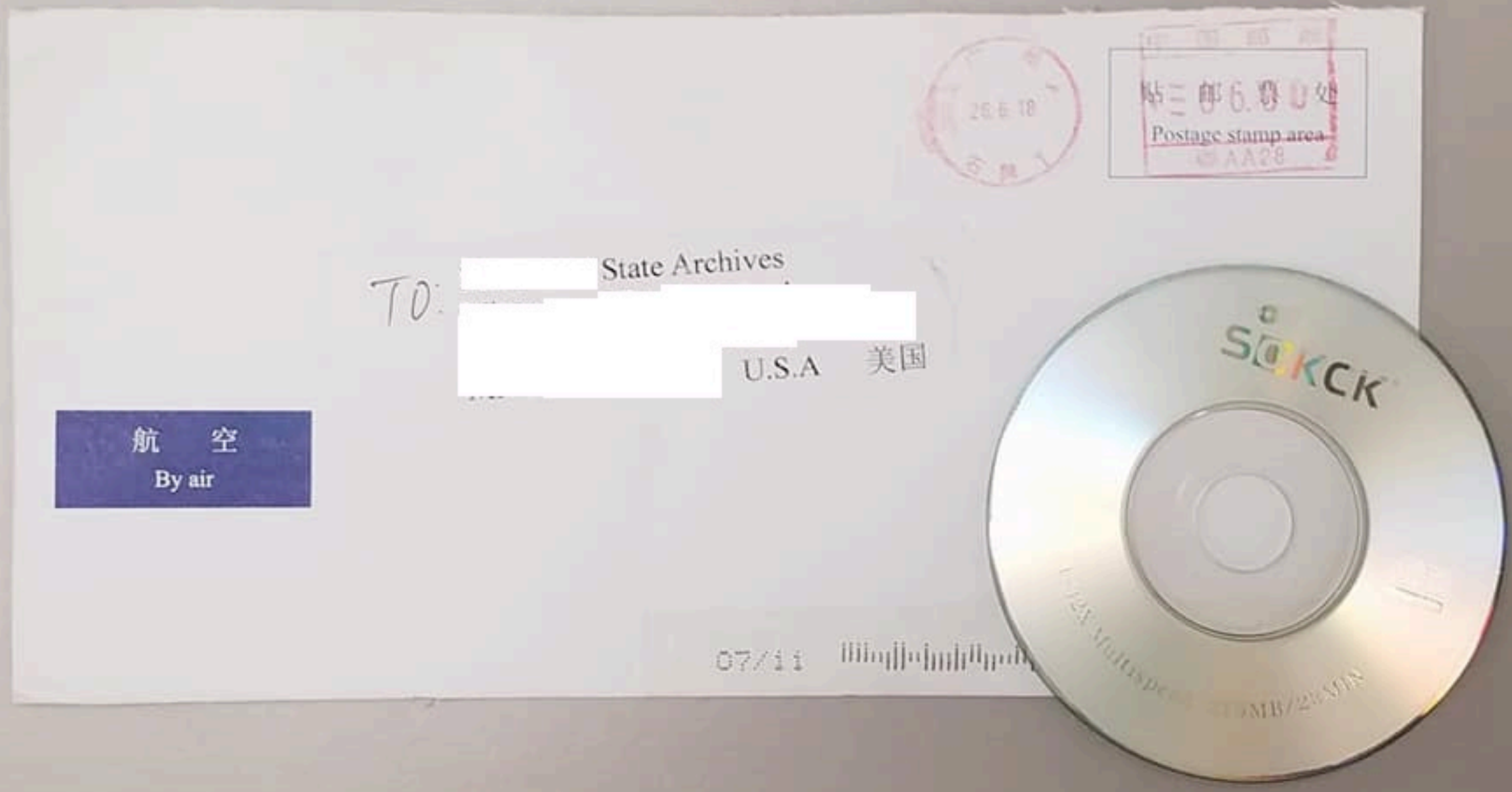
If you want to be public on the Internet, you must seek the opinions of the Chinese Embassy and the Chinese Consulate in advance. Remember, don't go wrong!

Note that the file's requirement is to preserve the original text in its entirety. It cannot be deleted or deleted. There are other requirements for disclosure.

The files and file names of the attached CD are basically Chinese, and only a small part of the content of the file is translated into English. You need to edit, catalog, and organize your computer on a Chinese system.

This article uses computer translation without manual proofreading.

Ref # 777dd049-6597-4ff4-9484-c7f1f1165e3e


Postage stamp area
TO:
State Archives
U.S.A 美国
航 空
By air
07/11