Windows. Работа программы состоит из следующих этапов: посредством функций WinAPI она может скрывать, развернуть, закрывать окна приложений и программ, открытых и работающих в операционной системе Windows, а также отключить, восстановить список их объектов, элементов и компонентов.

Список использованных источников

1. M. Çüriýew. Intellektual ulgamlar. Ýokary okuw mekdepleri üçin okuw kitaby.- A.: „Ylym“ neşirýaty, 2014.
2. А.Я.Архангельский. Программирование в Delphi. М., Издательство БИНОМ, 2008.

УДК 681.3:553.98(574.4)

М.М. Чуриев, Д. Тедженов, М.Р. Отузов, С.О. Гелдиев
Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

РАЗРАБОТКА ПРОГРАММ СИМУЛЯТОРОВ КИБЕРУГРОЗ

Аннотация. *В статье рассматриваются программы симуляторов различных киберугроз в учебном процессе при подготовке специалистов и бакалавров по направлению информационной и кибербезопасности. Использование данных разработок в практических и лабораторных занятиях, позволят создавать условия, максимально приближенные к реальным условиям атак.*

M.M. Churiyev, D. Tejenow, M.R. Otuzov, S.O. Geldiyev
Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

DEVELOPMENT OF CYBER THREAT SIMULATOR PROGRAMS

Abstract. *The article discusses the features of the use of developed simulators of various cyber threats in the educational process when training specialists in the field of information and cyber security. The use of these developments in practical and laboratory exercises will create conditions that are as close as possible to real attack conditions.*

Решение проблемы кибербезопасности в современном мире невозможно без подготовки квалифицированных специалистов, бакалавров и магистров в области информационной и кибербезопасности. А это в свою очередь уже другая проблема. В

большинстве высших и других учебных заведениях осуществляется подготовка хотя бы по одному из направлений информационной и кибербезопасности. В крайнем случае, в рамках существующих специальностей по IT технологиям преподаются дисциплины или группы дисциплин по информационной безопасности. Однако выпускники, выходя из университетских пенатов, сталкиваются в реальных условиях с изощренными киберугрозами и кибератаками. Исход этих противостояний не всегда в пользу молодых специалистов.

Это можно объяснить следующими факторами:

1. Студенты готовятся по заранее известным технологиям, злоумышленники прекрасно осведомлены об этих технологиях.

2. Подготовка ведется академически, а зачастую атака производится хаотично, «хулиганскими методами».

3. Контроль знаний зачастую производится теоретическими методами, тестирование, собеседование.

Таким образом не всегда удается не только подготовить студента к реалиям современных угроз, но и проверить и дать объективную оценку его навыкам.

Не стоит забывать, что дисциплины по информационной и кибербезопасности должны дать не только необходимые и актуальные знания, но в большей степени они должны обеспечить усвоение студентами компетенций и навыков по выявлению и обнаружение, предупреждению и предотвращению, противостоянию кибернетическим и другим угрозам.

Дается много рекомендаций, разрабатываются стратегии и политики обеспечения кибербезопасности. Можно с уверенностью сказать, что ни одну из них нельзя воплотить в жизнь без тщательного изучения и анализа источника киберугроз, без изучения природы самой кибератаки.

В данной статье опишем процесс разработки симулятора многоволновых кибератак и выработаем рекомендации по применению данного симулятора на практических и лабораторных занятиях.

На языке объектно-ориентированного программирования Delphi создаем новый проект. Размещаем компонент слежения за временем TTimer. Для того чтобы скрыть наш симулятор, в процедуре слежения компонента Timer (Timer1.Timer) запишем следующий код:

```
procedure TForm1.Timer1Timer(Sender: TObject);
begin
if timetostr(time)<>'10:00:00' then
begin
hide;
```

```
timer1.Enabled:=false;
end
else
begin
Timer2.Enabled:=false;
show;
end;
```

Суть данного программного кода заключается в том, что до 10:00 (по местному времени) программа будет работать резидентно. Можно указать любое другое время, например до завершения занятий.

Чтобы скрыть следы автоматической загрузки нашего симулятора, чтобы нельзя было найти размещения его файла, а также способ его самостоятельной загрузки в процедуре загрузки программы (OnShow) добавим следующий код:

```
Reg := nil;
try
 reg := TRegistry.Create;
reg.RootKey := HKEY_CURRENT_USER;
reg.LazyWrite := false;
reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Run',fal
se);
if reg.ValueExists('Gizlin1')=true then reg.DeleteValue(' Gizlin1');
if reg.ValueExists(' Gizlin2')=true then reg.DeleteValue(' Gizlin2');
reg.CloseKey;
reg.OpenKey('\Software\Microsoft\Windows\CurrentVersion\'
+'Explorer\Shell Folders', True);
Maksat:=reg.ReadString('Personal');
reg.CloseKey;
except if Assigned(Reg) then Reg.Free;
end;
```

Используя данный код в момент своей загрузки в оперативную память симулятор удаляет записи своей автоматической загрузки в реестре. Таким образом, для будущих специалистов будет очень проблематично провести профилактику данной кибератаки и обнаружить место размещения файла симулятора.

Он позволяет скрытно скопировать файл симулятора и запустить его. Таким образом, помимо главной программы симулятора dllhost.exe, будет действовать параллельный модуль под названием svchost.exe. Название процессов данных двух модулей специально подобраны так, чтобы запутать пользователя, так-как данные названия

также соответствуют системным службам системы.

Теперь возникает другой вопрос, как будут загружаться данные параллельные модули симулятора после выключения или перезагрузки операционной системы (ведь запись автозагрузки была удалена).

Создается процедура, которая позволяет перехватить сообщение о завершении работы операционной системы и записать в системный реестр записи об автозагрузке наших резидентных модулей.

В итоге, операционная система выключится с уже записанными записями автоматической загрузки. После загрузки операционной системы и вместе с ней резидентных модулей, данные записи будут стерты и так будет продолжаться до тех пор пока каким-то образом не будут удалены резидентные модули.

Значит, попробуем их защитить. В процедуре слежения за временем компонента Timer2 (Timer2.Timer) запишем следующий код:

```
procedure TForm1.Timer2Timer(Sender: TObject);
var
i:integer;
begin
ProcArr := TLpModuleInfoArray(unit1.GetAllProcessesInfo);
svchost:=false;
project1:=false;
for i := Low(ProcArr) to High(ProcArr) do
begin
if ProcArr[i].ModuleName='svchost.exe' then svchost:=true;
if ProcArr[i].ModuleName='dllhost.exe' then project1:=true;
end;
if svchost=false then
winexec(pansichar(ansistring(Maksat+'\svchost.exe')),Sw_shownorm
al);
if project1=false then
winexec(pansichar(ansistring(Personal+'\dllhost.exe')),Sw_shownor
mal);
end;
```

Суть данной процедуры заключается в том, что наши процессы (dllhost.exe и svchost.exe) будут мониторить друг друга оперативной памяти и в момент времени когда по каким-то причинам не обнаружат соседний процесс (при удалении пользователем или программой) мгновенно восстановят его. Таким образом, отдельно удалить резидентные процессы не получится, нужно будет достаточно мощное программное средство удаления данной параллельной угрозы.

А для того чтобы приблизить симуляцию к реальным условиям

киберугрозы и усложнить «жизнь» будущим специалистам по кибербезопасности, можно через компонент TTimer через определенное время расставить разные ловушки, например отключение дисплея, клавиатуры и мыши, манипуляция с текстовым фокусом, когда на месте курсора нужный текст автоматически замещался текстом из программы симулятора. Таким образом наш симулятор угроз будет искусно расставляет ловушки, препятствуя выполнению действий по устранению угроз, через определенные промежутки времени запускает новые волны атак, призванные запутать будущих специалистов по кибербезопасности.

Из всего выше сказанного следует, что симулятор обладает достаточно мощными средствами кибератаки, тем более он атакует первым и имеет возможность дезориентировать своих визави очередными волнами кибератак, действующих через определенные промежутки времени.

В стадии разработки данного симулятора, который несомненно будет очень полезен для подготовки специалистов в «боевых» условиях, был получены важный опыт, который будет полезен в дальнейшем для противодействия кибератак и который заключается в том, что в первую очередь нужно ликвидировать активную угрозу, т.е. резидентную программу (программы), иначе все предпринятые действия будут напрасными.

Поэтому применение данной и других подобного рода программ на практических и лабораторных занятиях, позволит студентам на ранней стадии как говорится «понюхать пороха», научиться ориентироваться и не паниковать в неизвестных условиях киберугроз, приспособиться к многоволновым кибератакам, поможет вырабатывать правильные, а главное своевременные решения по выявлению и предупреждению скрытой угрозы, а также обнаружению и устранению активной фазы кибератаки. На данное специальное программное обеспечение было получено в установленном порядке патентное свидетельство (№ 147 от 03.11.2023).

Список использованных источников

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: ИД. "Форум": ИНФРА - М. 2013-592с.
2. Karl Maria Michael de Leeuw, Jan Bergstra - The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007.

3. M.Çuriýew. Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. –A.: Türkmen döwlet neşirýat gullugy, 2013, 206 s.

УДК 681.3:553.98(574.4)

Б.С. Гафуров[1], М.А. Гельдыева[2], Г.Д. Базарова[2], А.Р. Аннаева[2]
[1]"Dragon Oil" (Turkmenistan) Ltd
[2]Международный университет нефти и газа имени Ягшыгельди Какаева
Ашхабад, Туркменистан

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В КИБЕРБЕЗОПАСНОСТИ

Аннотация. *Блокчейн - это распределённая цифровая электронная книга. Впервые об этой технологии стало известно с появлением криптовалюты биткойн. Эта статья описывает применение технологии блокчейн как безопасной цифровой инфраструктуры, в частности в аутентификации пользователей и управлении личных данных.*

B.S. Gafurov[1], M.A. Geldiyeva[2], G.D. Bazarova[2], A.R. Annayeva[2]
[1]Dragon Oil" (Turkmenistan) Ltd
[2]Yagshigeldi Kakaev International University of Oil and Gas
Ashgabat, Turkmenistan

FEATURES OF USING BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY

Abstract. *Blockchain is a distributed digital ledger. This technology first made headlines with the emergence of the bitcoin cryptocurrency. This article describes the application of blockchain technology as a secure digital infrastructure, particularly in user authentication and personal data management.*

В современном цифровом веке информация свободно и быстро распространяется по просторам глобальной сети Интернет. При этом, такие технологии как блокчейн имеют особую важность в такой быстроразвивающейся среде. При этом, технология блокчейн находит множество применений в сфере кибербезопасности. Эти два понятия, кибербезопасность и блокчейн, подобны стражам цифровой сферы, неустанно работающим над обеспечением безопасности и целостности наших данных и транзакций.

Технология блокчейн является основой многих цифровых инноваций, и ее значение в обеспечении безопасности данных имеет первостепенное значение. Блокчейн - это децентрализованная,