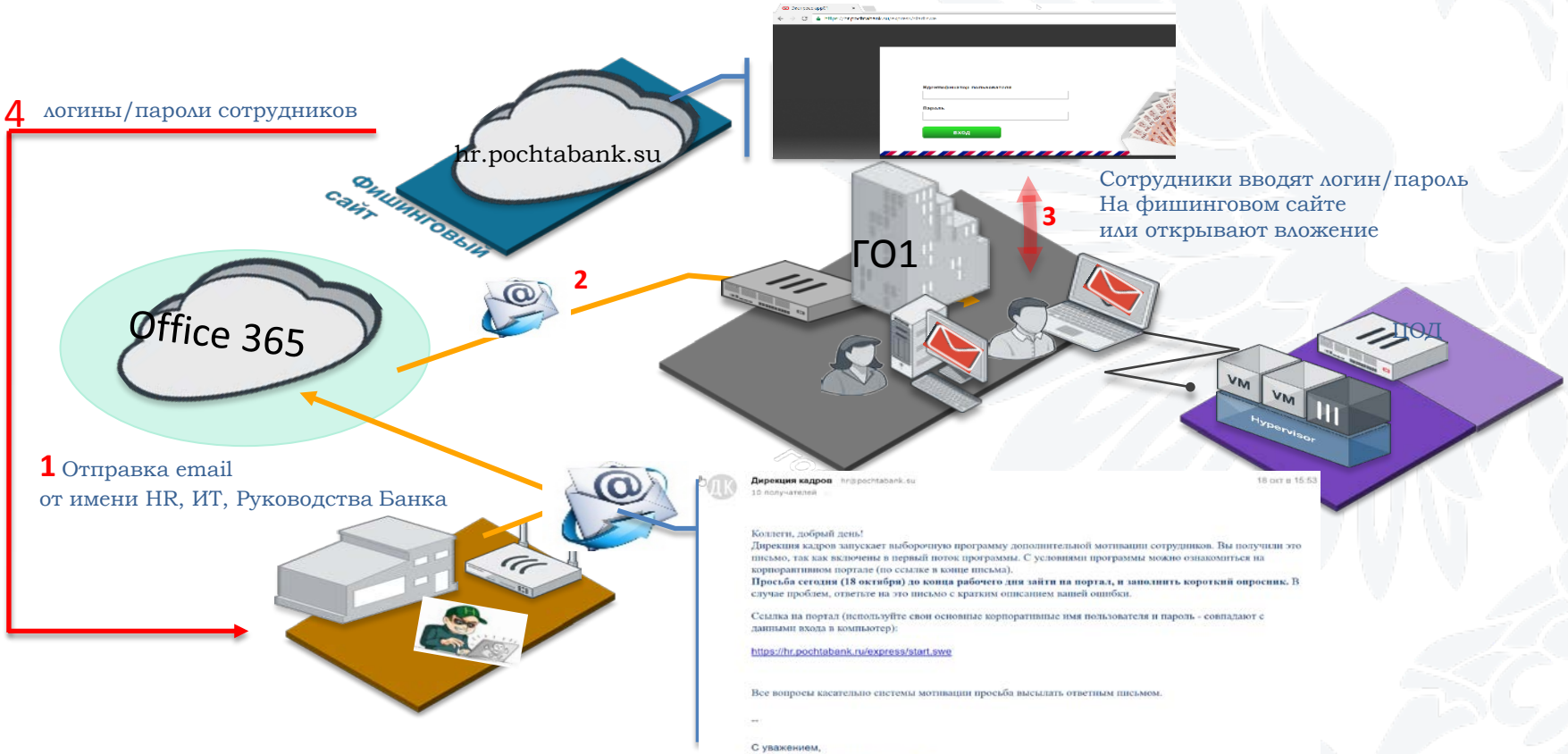
Практический опыт повышения осведомленности персонала с использованием методов социальной инженерии

Максим Лукин. Руководитель Дирекции информационной безопасности

2016

ПРОВЕРКА ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ



СЦЕНАРИИ ПРОВЕРКИ УРОВНЯ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ 1/2

№	Подразделение	Сценарий	Ожидаемый результат
1.	Отделения Банка	Запуск макроса из документа Word под предлогом распечатки документа. В качестве документа будет использовано письменное «обращение» в банк.	Получение удаленного доступа, скриншот рабочего стола.
2.	Клиентская служба	Звонок на общую линию, вопрос о возможности отзыва заявления об обработке персональных данных, отправка отзыва (формат doc со скриптом).	Получение удаленного доступа, скриншот рабочего стола.
3.	Клиентская служба	Звонок на общую линию, вопрос о возможности оставить претензию/благодарность, отправка «документа» (формат doc со скриптом).	Получение удаленного доступа, скриншот рабочего стола.
4.	Дирекция кадров и трудовых отношений	Рассылка, якобы от ИТ-службы о «новом hr-портале».	Получение доменных аккаунтов пользователя.
5.	Служба маркетинга и общественных связей	Звонок с переложением бесплатного продвижения в социальных сетях. или Звонок с предложением посреднических услуг в «Банки.ру». После звонка – отправка «предложения» (формат doc со скриптом).	Получение удаленного доступа, скриншот рабочего стола.
6.	Отдел сопровождения закупок	Дополнение к закупочному лоту, высланное по электронной почте (формат doc со скриптом). Закупочный лот выбирается с площадки zakupki.gov.ru	Получение удаленного доступа, скриншот рабочего стола.
7.	Служба бухгалтерского учета и отчетности	Рассылка с письмом о смене реквизитов. (формат xls со скриптом). В качестве контрагента выбирается: - контрагент из архивов zakupki.gov.ru - часто встречающиеся контрагенты (канцелярские товары, вода).	Получение удаленного доступа, скриншот рабочего стола.
8.	Юридическая служба	Письмо с «досудебной претензией» (формат doc со скриптом).	Получение удаленного доступа, скриншот рабочего стола.

СЦЕНАРИИ ПРОВЕРКИ УРОВНЯ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ 2/2

Этап 2. Рассылки без знания цели (имитация полностью неосведомленного внешнего злоумышленника, используются найденные в Интернет адреса).			
9.	Секретариат, фронт-офис[2]	Передача компакт-дисков с «важной информацией» для отдела закупок, руководства, и.т.д. (формат doc со скриптом).	Передача физического носителя через ресепшн.
10.	30 адресов, найденных из открытых источников. Подразделения неизвестны.	Рассылка с фишинговым письмом, о якобы обновленным «корпоративным hr-порталом», на котором находится информация о новой системе мотивации.	30 адресов, найденных из открытых источников.
11.	30 адресов, найденных из открытых источников. Подразделения неизвестны.	Рассылка «секретной информации», которая направлялась руководству, и «случайно» попала в ящик пользователя.	30 адресов, найденных из открытых источников.

Массовая рассылка/Письмо от службы кадров и мотивации (hr@pochtabank.ru).

Коллеги, добрый день!
Дирекция кадров запускает выборочную программу дополнительной мотивации сотрудников. Вы получили это письмо, так как включены в первый поток программы. С условиями программы можно ознакомиться на корпоравтивном портале (по ссылке в конце письма).
Просьба сегодня (18 октября) до конца рабочего дня зайти на портал, и заполнить короткий опросник. В случае проблем, ответьте на это письмо с кратким описанием вашей ошибки.

Ссылка на портал (используйте свои основные корпоративные имя пользователя и пароль - совпадают с данными входа в компьютер):

https://hr.pochtbank.ru/express/start.swe

Все вопросы касательно системы мотивации просьба высылать ответным письмом.

--

Массовая рассылка/Письмо от службы технической поддержки (support@pochtabank.ru).

Коллеги, добрый день!
Дирекция ИТ запускает новый единый информационный портал, на котором будут объединены все корпоративные сервисы. Портал пока работает в тестовом режиме, проводятся выборочные проверки работоспособности у пользователей. Просьба сегодня (18 октября) до конца рабочего дня зайти на портал, и проверить его работоспособность. В случае проблем, ответьте на это письмо с кратким описанием вашей ошибки.

Ссылка на портал (используйте свои основные корпоративные имя пользователя и пароль - совпадают с данными входа в компьютер):

https://portal-new.pochtabank.ru/express/start.swe

Все вопросы касательно портала просьба высылать ответным письмом.

--

С уважением,
Служба поддержки,
Дирекция развития и сопровождения информационных систем

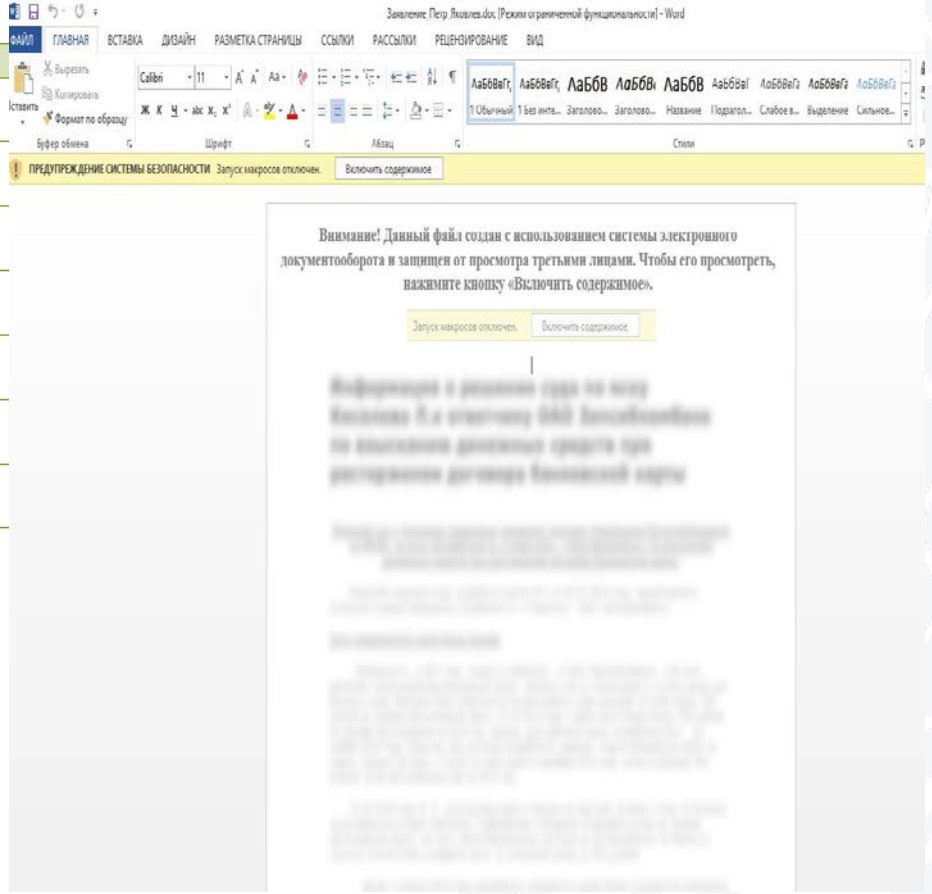
ЗАЯВЛЕНИЕ ПЕТРА ЯКОВЛЕВА ОБ ОТЗЫВЕ ПДн

This sample was found to be **malware** on this virtual machine.

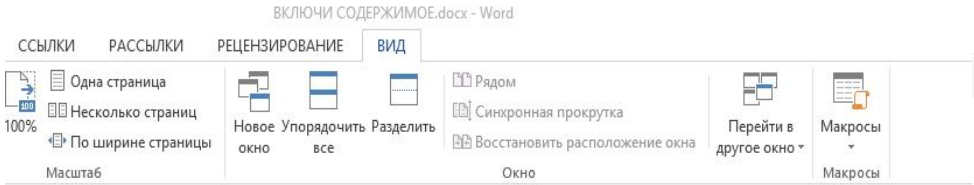
Behavior	Severity
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Started a process A process running on the system may start additional processes to perform actions in the background. This behavior is common to legitimate software as well as malware.	
Connected to an unregistered domain name Malware typically communicates back to an attacker via a command-and-control server. This command-and-control server is usually addressed in the malware as a domain name. To avoid easy identification of malicious domain names, the attacker may use a domain generation algorithm (DGA) to address a large number of dynamically generated domains, most of which are not registered.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	
Opened a Command Prompt window Command Prompt is the built-in Windows command-line interface. While it is common for users to open Command Prompt windows, legitimate applications rarely do so.	
Opened a Windows PowerShell window Windows PowerShell is an enhanced command-line interface and scripting environment for administrators. While it is common for users to open PowerShell windows, legitimate applications rarely do so.	
Enumerated running processes Malware often enumerates running processes before injecting malicious code into them.	

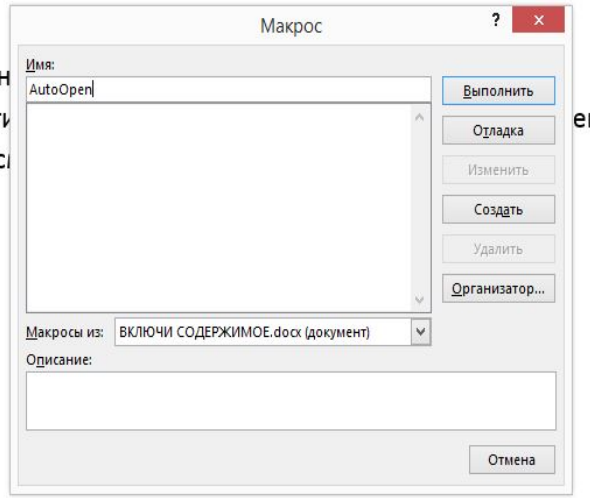
1 File Information

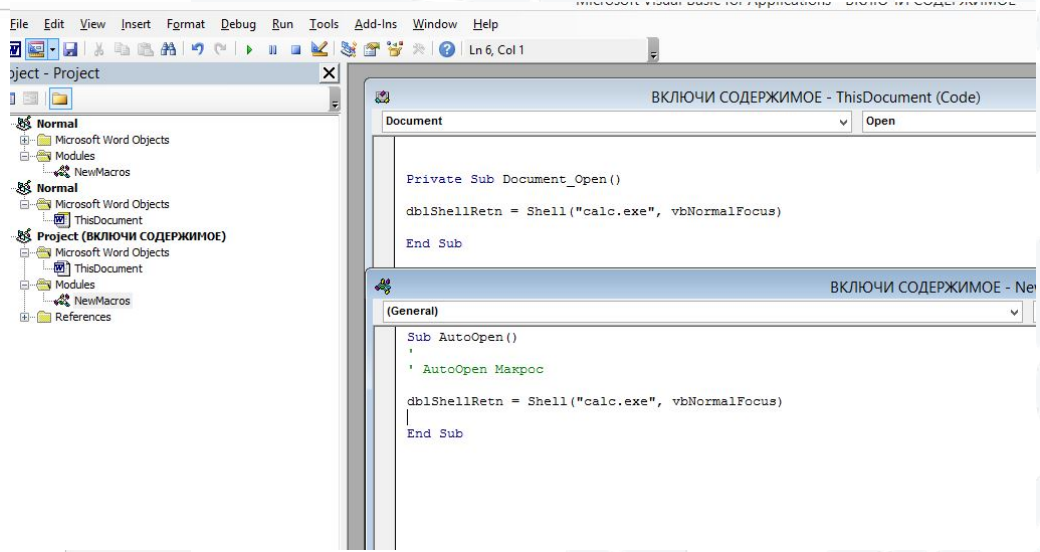
File Type	Microsoft Word 97 - 2003 Document
File Signer	None
SHA-256	1c5af5207b1ad7e4300af3aa9b4ed0ffe614375b8e16200530b2b6e6c114cf92
SHA-1	0742f94af0ac2555372d6f36f28d3f9975887287
MD5	0d91454b5698d21d4d35dec9e749188c
File Size	716288bytes
First Seen Timestamp	2016-10-17 16:34:13 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information



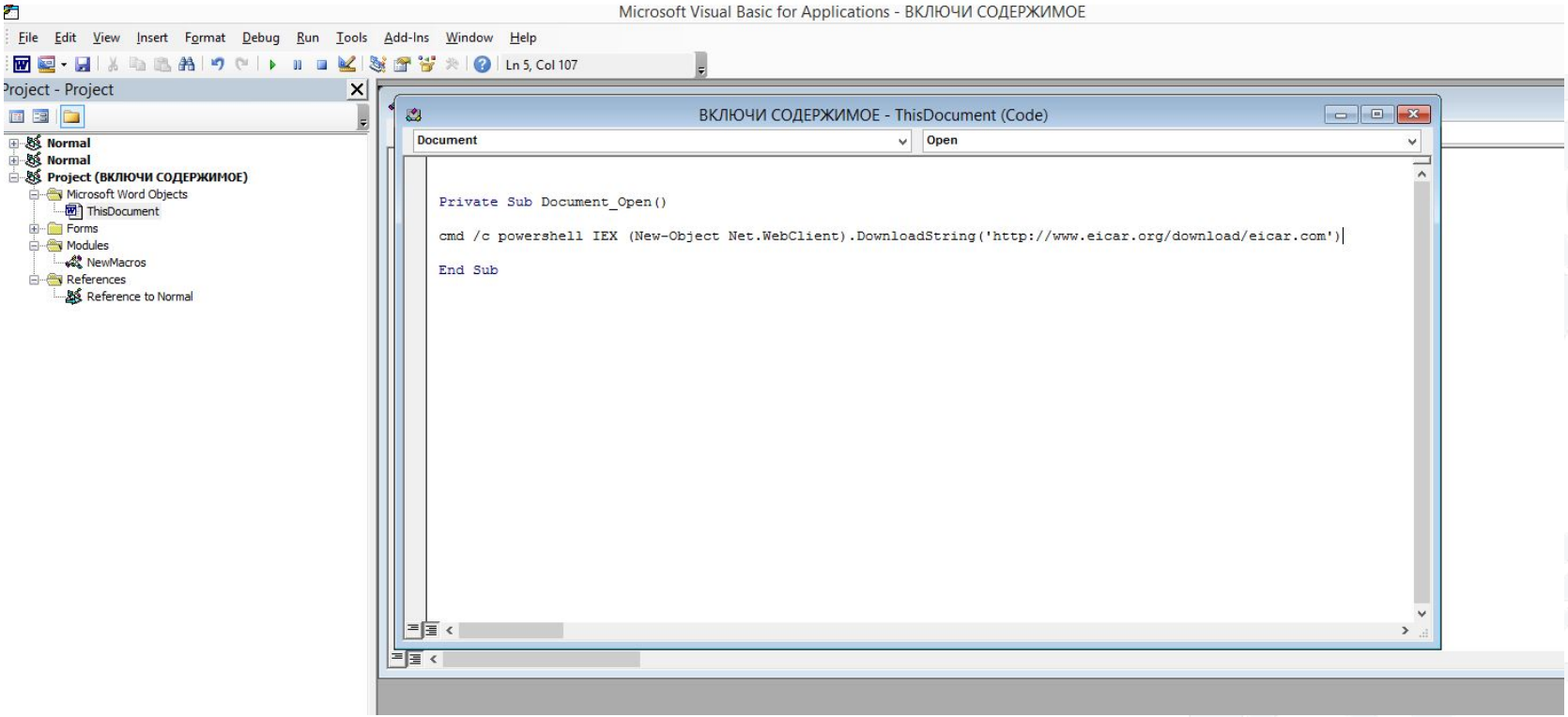
ПРИМЕР 1. СОЗДАЕМ DOC ЗАПУСКАЮЩИЙ ПО ПРИ ОТКРЫТИИ







ПРИМЕР 2. СОЗДАЕМ DOC ЗАГРУЖАЮЩИЙ ТРОЯН ИЗ СЕТИ ИНТЕРНЕТ



ПЛАН МЕРОПРИЯТИЙ ПО ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ 2017

- Внедрение автоматизированной системы проверки уровня осведомленности
- Использование интерактивных платформ
- Проведение деловых игр по информационной безопасности
- Обучение подразделений с учетом специфики бизнес процессов
- Оценка культуры безопасности и включение в KPI подразделений
- Реализация цикла непрерывного обучение и проверки

СПАСИБО ЗА ВНИМАНИЕ!