Octopus恶意软件分析

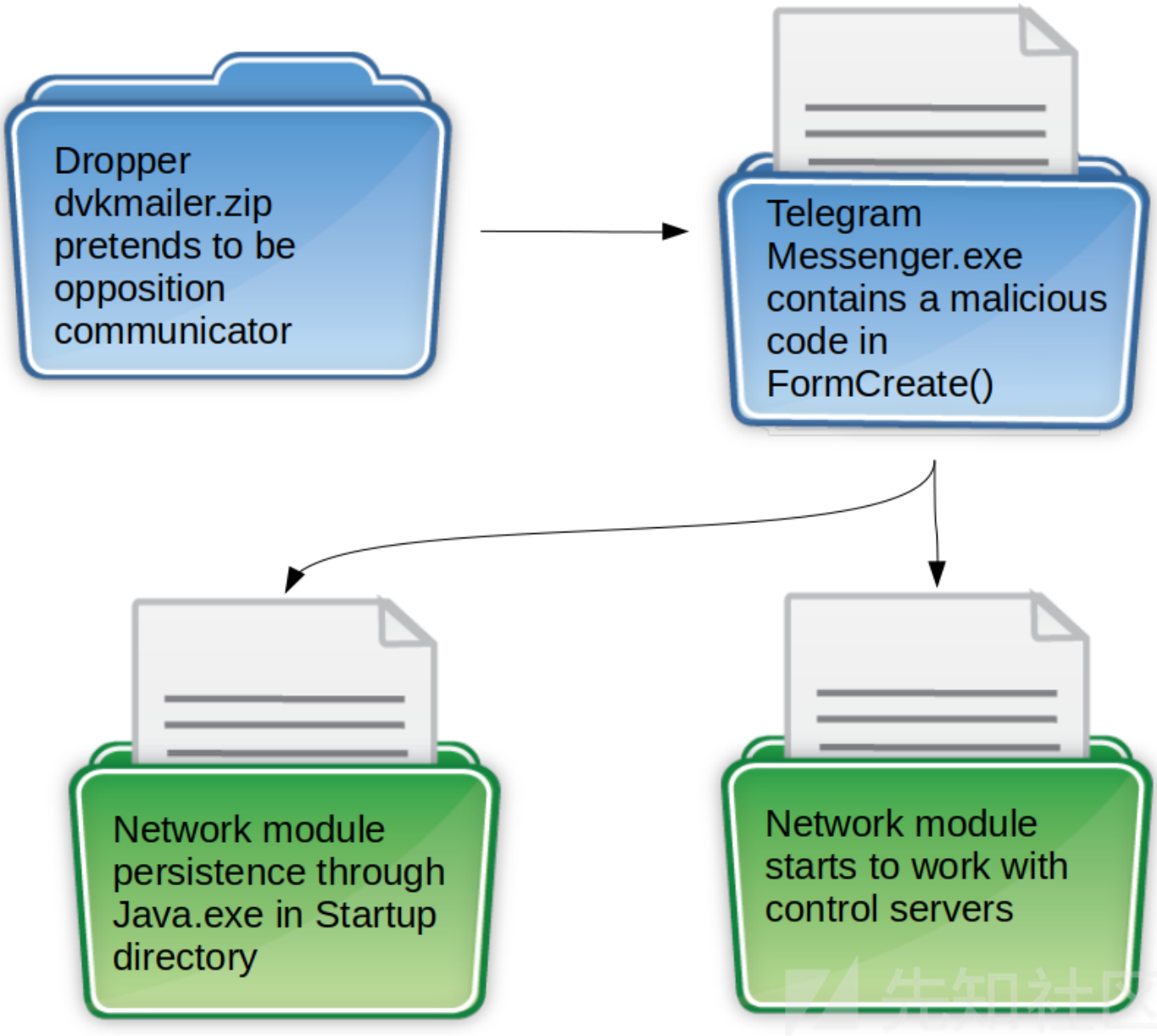
angel010 / 2018-10-16 00:15:27 / 浏览数 2093

本文翻译自：https://securelist.com/octopus-infested-seas-of-central-asia/88200/

2018年4月，研究人员发现一个新的Octopus样本，装扮成哈萨克反政府组织的通信软件。恶意软件打包成名为dvkmailer.zip的ZIP文件，时间戳显示为2018年2-3月。

技术细节

攻击者利用Kazakhstan（哈萨克斯坦）禁止使用Telegram来推送dropper，作为政治反对派可选的一种通信软件。



'Telegram messenger'以最简单的方式建立网络模块驻留，并启动模块

研究人员不能确认恶意软件的传播方式，但很明显恶意软件使用了社会工程技术。该攻击单元之前就使用过鱼叉式钓鱼攻击来传播恶意软件。

Dropper

MD5 hash	979eff03faeaeea5310df53ee1a2fc8e
Name	dvkmailer.zip

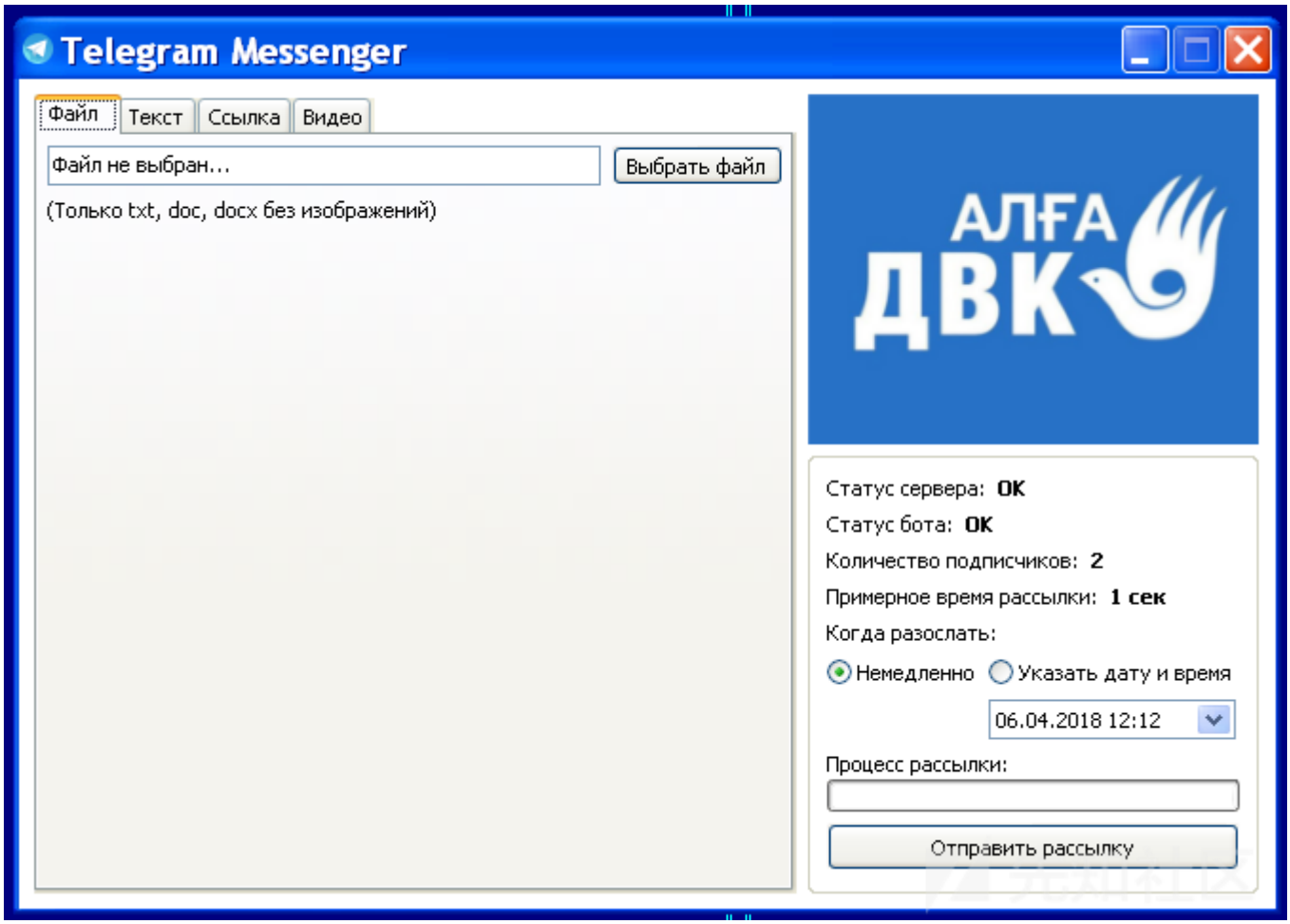
Archive contents

d6e813a393f40c7375052a15e940bc67	CsvHelper.dll	Legit .NET CSV files parser
664a15bdc747c560c11aa0cf1a7bf06e	Telegram Messenger.exe	Persistence and launcher
87126c8489baa8096c6f30456f5bef5e	TelegramApi.dll	Network module
d41d8cd98f00b204e9800998ecf8427e	Settings.json	Empty

Launcher

MD5 hash	664a15bdc747c560c11aa0cf1a7bf06e
File name	Telegram Messenger.exe
PE timestamp	2018.03.18 21:34:12 (GMT)
Linker version	2.25 (Embarcadero Delphi)

在用户交互前，FormCreate()函数中的启动器会检查相同目录中的TelegramApi.dll文件。如果文件存在，启动器就会将网络模块复制到开始菜单目录中（Java.exe），并运



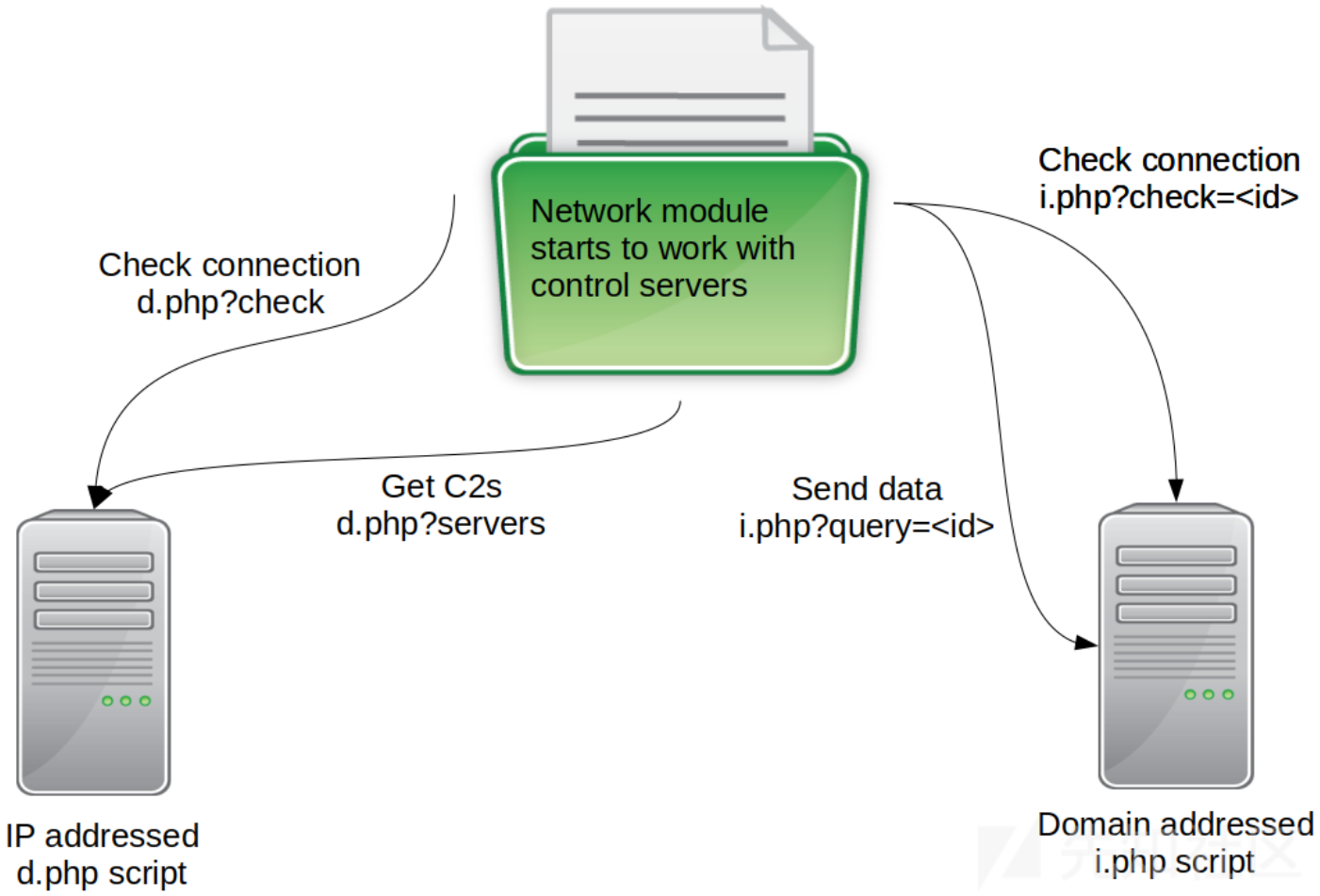
右下角的"发送邮件"按钮都没有handler函数

Delphi Visual Component Library
(VCL)程序是基于表单元素的事件处理器。这类程序一般都很大（大概有2.6MB，12000个函数），但所有的代码都是用来处理画面部分和运行时库的。但在Octopus启动器

函数名	功能
FormCreate()	在用户活动前以 constructor 运行。通过开始菜单目录确保网络模块驻留并运行。
Button1Click()	显示 explorer 对话窗口来选择“发送文件”。
DateTimePicker1Click()	显示日历来选择发送日期。

但“发送邮件”按钮没有handler，所以当加载器伪装成备选的通信软件时，而事实上并没有通信的功能。这可能是因为恶意软件还没有完成，毕竟发送的消息对攻击者来说还

网络模块



C2通信机制

MD5 hash	87126c8489baa8096c6f30456f5bef5e
File name	TelegramApi.dll
PE timestamp	2018.02.06 11:09:28 (GMT)
Linker version	2.25 (Embarcadero Delphi)

虽然扩展名是dll，但网络模块其实是一个自满足的可移动可执行文件，而非dll文件。第一个样本检查用户临时目录中名为1?????????.*的文件，并将找到的文件删除。然
Data）目录中创建.profiles.ini文件。

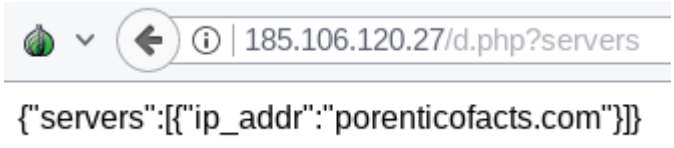
HTTP request	Response
GET /d.php?check	JSON “ok”
GET /d.php?servers	JSON domain name
GET /i.php?check=	JSON “ok”
POST /i.php?query=	JSON response code or command depends on POST data

```php
<?php
if(isset($_GET['check'])){echo(json_encode(array('status'=>'ok')));}
if(isset($_GET['servers'])){
    $arr_servers = array();
    array_push($arr_servers,array('ip_addr'=>'latecafe.in'));
    echo(json_encode(array('servers'=>$arr_servers)));
}
?>
```

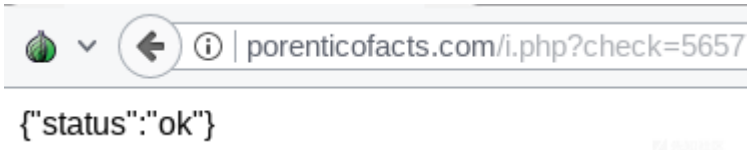
检查连接和获取c2域名的.php脚本

所有的网络模块都含有硬编码的IP地址，而IP地址都是不同国家的web主机服务。运营者简单地应用了一阶段的.php脚本，脚本会用HTTP GET请求检查真实的C2服务器域名。

在初始连接检查后，恶意软件会接收到JSON格式的真实C2域名，如下图所示：



然后网络模块会检查硬编码的受害者id，如下图所示：



网络模块会检查32个字母（数字）的硬编码的受害者id，并通过HTTP POST请求将收集的数据发送到C2服务器。从编程的角度看，该id很奇怪，因为恶意软件同时用系统数据的MD5哈希值对受害者计算指纹。

```
{"id":"dcb0f33785c12345f1b5da2414143b34",
    "act":0,
    "data":
        {   "cn":"here_goes_computer_name",
            "un":"here_goes_user_name",
            "wd":"C:\\Windows",
            "vl":
                {   "C|Local Disk (C:)":53580132352,
                    "<other disks data>"
                },
            "li":"here_goes_victim_ip",
            "pa":"full_path_to_TelegramApi.dll",
            "vr":"2.0",
            "dt":"185.106.120.27"
        }
}
```


将收集的JSON格式的数据以HTTP POST base64编码请求发送

所有与C2的通信都是基于JSON格式和HTTP协议的。开发者使用Indy Project (indyproject.org)公开的库和第三方urboPower Abbrevia (sourceforge.net/projects/tpabbrevia)进行压缩。

在初始HTTP GET请求后，恶意软件会开始收集JSON格式的系统数据。网络模块会保存磁盘名和大小、计算机名和用户名、Windows目录、host IP等。其中有一个域vr的值是2.0，应该是通信协议中编码的恶意软件版本。

Id域保存的是恶意软件用Windows Management Instrumentation机制制作的受害者指纹，木马会以以下参数运行WMIC.exe：

```
C:\WINDOWS\system32\wbem\WMIC.exe computersystem get Name /format:list
C:\WINDOWS\system32\wbem\WMIC.exe os get installdate /format:list
C:\WINDOWS\system32\wbem\WMIC.exe path CIM_LogicalDiskBasedOnPartition get Antecedent,Dependent
```

然后模块会将收集的ids连接起来来计算MD5哈希值，这就是受害者的最终`id`。`act`域表示通信的阶段，之后HTTP POST控制服务器会返回`JSON {"rt":"30"}`，客户端会在HTTP POST中继续下一个`act`：


```
{"id":"dcb0f33785c12345f1b5da2414143b34",
    "act":1
}
```


C2会发送一个JSON格式的命令来执行，包括上传和下载文件、截屏、找出`*.rar`格式的文件。

其他恶意软件

除了木马本身外，Octopus开发者还使用密码复制工具fgdump。

IOC
文件哈希

```
87126c8489baa8096c6f30456f5bef5e
ee3c829e7c773b4f94b700902ea3223c
38f30749a87dcbf156689300737a094e
6e85996c021d55328322ce8e93b31088
7c0050a3e7aa3172392dcbab3bb92566
2bf2f63c927616527a693edf31ecebea
d9ad277eb23b6268465edb3f68b12cb2
```

域名和IP

```
85.93.31.141
104.223.20.136
```

```
5.8.88.87
103.208.86.237
185.106.120.240
204.145.94.101
5.188.231.101
103.208.86.238
185.106.120.27
204.145.94.10
hovnanflovers.com
latecafe.in
certificatesshop.com
blondehairman.com
porenticofacts.com
```

上传和下载文件的URL:

```
www.fayloobmennik.net/files/save_new.html
http://uploadsforyou.com/download/
http://uploadsforyou.com/remove/
```

保存一阶段.php脚本的位置：

```
148.251.185.168
185.106.120.46
185.106.120.47
46.249.52.244
5.255.71.84
5.255.71.85
88.198.204.196
92.63.88.142
```

返回.php脚本的域名：

```
giftfromspace.com
mikohanzer.website
humorpics.download
desperados20.es
prom3.biz.ua
```


上一篇：[译] ptmalloc介绍 下一篇：Python中从服务端模板注入到沙...

1. 0 条回复
   - 动动手指，沙发就是你的了！