Sinkholing the Backoff POS Trojan

SL securelist.com/sinkholing-the-backoff-pos-trojan/66305/

Authors

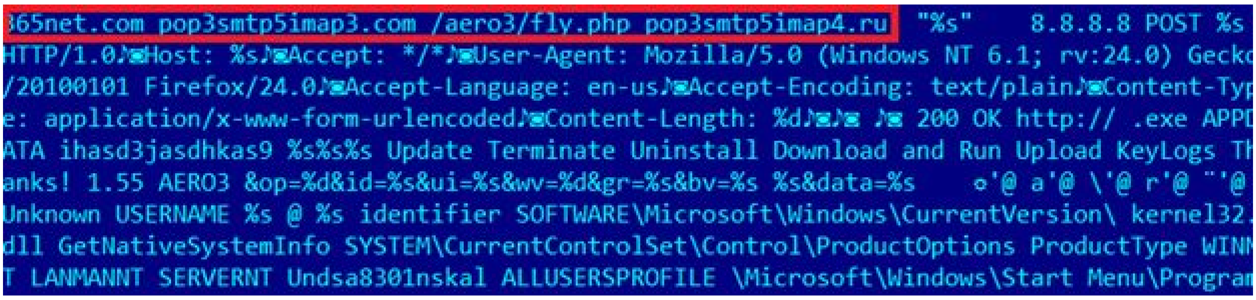
- Costin Raiu
- Roel Schouwenberg
- Ryan Naraine

Victim data paints sorry picture of PoS security

There is currently a lot of buzz about the Backoff point-of-sale Trojan that is designed to steal credit card information from computers that have POS terminals attached.

Trustwave SpiderLab, which originally discovered this malware, posted a very thorough analysis in July. The U.S. Secret Service, in partnership with DHS, followed up with an advisory.

Although very thorough, the existing public analyses of Backoff are missing a very relevant piece of information: the command-and-control (C&C) servers. However, if you have access to the samples it isn't hard to extract this information. At the end of this document, you can find a full list together with other IOCs (indicators of compromise).

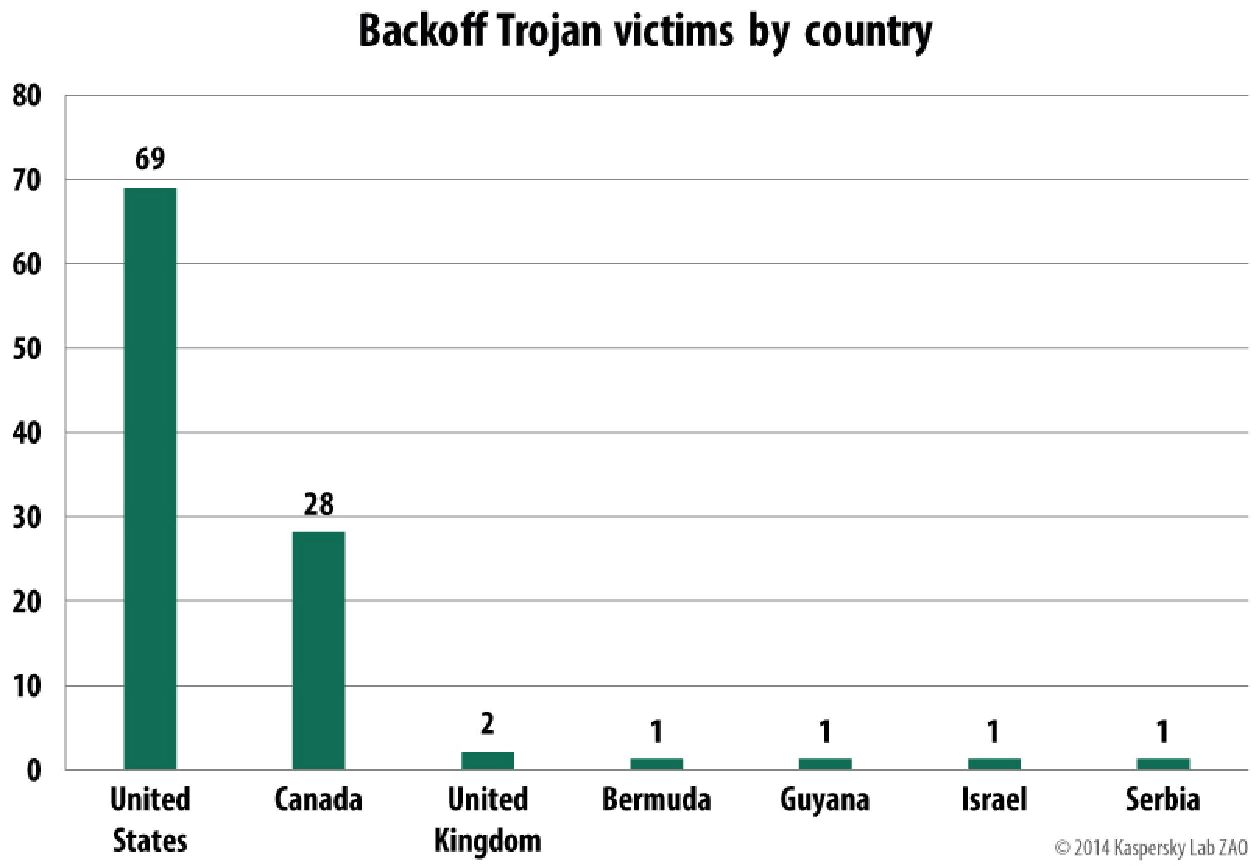


```
365net.com pop3smtp5imap3.com /aero3/fly.php pop3smtp5imap4.ru  "%s"   8.8.8.8 POST %s
HTTP/1.0♪◙Host: %s♪◙Accept: */*♪◙User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko
/20100101 Firefox/24.0♪◙Accept-Language: en-us♪◙Accept-Encoding: text/plain♪◙Content-Typ
e: application/x-www-form-urlencoded♪◙Content-Length: %d♪◙♪◙ ♪◙ 200 OK http:// .exe APPD
ATA ihasd3jasdhkas9 %s%s%s Update Terminate Uninstall Download and Run Upload KeyLogs Th
anks! 1.55 AERO3 &op=%d&id=%s&ui=%s&wv=%d&gr=%s&bv=%s %s&data=%s    ○'@ a'@ \'@ r'@ "'@
Unknown USERNAME %s @ %s identifier SOFTWARE\Microsoft\Windows\CurrentVersion\ kernel32.
dll GetNativeSystemInfo SYSTEM\CurrentControlSet\Control\ProductOptions ProductType WINN
T LANMANNT SERVERNT Undsa8301nskal ALLUSERSPROFILE \Microsoft\Windows\Start Menu\Program
```

Backoff malware configuration, with C&Cs

We sinkholed two C&C servers that Backoff samples used to communicate with their masters. These C&C servers are used by certain samples that were compiled from January – March 2014. Over the past few days, we observed over 100 victims in several countries connecting to the sinkhole.

Statistics:



There were several interesting victims among them:

- A global freight shipping and transport logistics company with headquarters in North America.
- A U.K.-based charitable organization that provides support, advice and information to local voluntary organizations and community groups.
- A payroll association in North America.
- A state institute connected with information technology and communication in Eastern Europe.
- A liquor store chain in the U.S.
- An ISP in Alabama, U.S.
- A U.S.-based Mexican food chain.
- A company that owns and manages office buildings in California, U.S.
- A Canadian company that owns and operates a massive chain of restaurants.

There are also a lot of home user lines, mostly in the U.S. and Canada, connecting to the sinkhole. This is to be expected as many smaller businesses generally tend to run those rather than dedicated corporate connections.

Conclusions

The success of Backoff paints a very bleak picture of the state of point-of-sale security. Our sinkhole covers less than 5% of the C&C channels and the sinkholed domains only apply to certain Backoff samples that were created in the first quarter of this year. Yet, we've seen more than 85 victims connecting to our sinkhole.

Most of these victims are located in North America and some of them are high profile. Taking into account the U.S. Secret Service statement, it's a pretty safe bet that the number of Backoff infections at businesses in North America is well north of 1,000.

Since its appearance last year, Backoff has not changed dramatically. The author created both non-obfuscated and obfuscated samples. This was likely done to defeat the security controls on the targeted networks. However, the defenses running on a PoS terminal and/or network should not have been affected by this. This speaks volumes about the current state of PoS security, and other cybercriminals are sure to have taken note.

It's very clear that PoS networks are prime targets for malware attacks. This is especially true in the US, which still doesn't support EMV chip-enabled cards. Unlike magnetic strips, EMV chips on credit cards can't be easily cloned, making them more resilient. Unfortunately, the US is adopting chip and signature, rather than chip and PIN. This effectively negates some of the added security EMV can bring.

This may prove another costly mistake. Not adopting EMV along with the rest of the world is really haunting retail in the U.S. and the situation is not likely to change anytime soon.

IOCs / C&Cs:

Trojan file paths:

```
%APPDATA%\AdobeFlashPlayer\mswinsvc.exe
%APPDATA%\AdobeFlashPlayer\mswinhost.exe
%APPDATA%\AdobeFlashPlayer\Local.dat
%APPDATA%\AdobeFlashPlayer\Log.txt
%APPDATA%\mskrnl
%APPDATA%\nsskrnl
%APPDATA%\winserv.exe
%APPDATA%\OracleJava\javaw.exe
%APPDATA%\OracleJava\javaw.exe
%APPDATA%\OracleJava\Local.dat
%APPDATA%\OracleJava\Log.txt
```

Kaspersky names for the Trojans:

```
HEUR:Trojan.Win32.Invader
HEUR:Trojan.Win32.Generic
Backdoor.Win32.Backoff
Trojan.Win32.Agent.ahhia
Trojan.Win32.Agent.agvmh
Trojan.Win32.Agent.aeyfj
Trojan-Spy.Win32.Recam.qq
Trojan-Dropper.Win32.Sysn.ajci
Trojan.Win32.Bublik.covz
Trojan-Dropper.Win32.Dapato.dddq
Trojan.Win32.Agent.agufs
Trojan.Win32.Agent.ahbhh
Trojan.Win32.Agent.agigp
Trojan.Win32.Agent.aeqsu
Trojan.Win32.Agent.ahgxs
Trojan.Win32.Inject.mhjl
Trojan.Win32.Agent.ahbhh
Trojan.Win32.Agent.ahhee
Trojan.Win32.Agent.ahgxs
```

MD5s:

```
 684e03daaffa02ffecd6c7747ffa030e
3ff0f444ef4196f2a47a16eeec506e93
12c9c0bc18fdf98189457a9d112eebfc
14cca3ad6365cb50751638d35bdb84ec
d0f3bf7abbe65b91434905b6955203fe
38e8ed887e725339615b28e60f3271e4
7b027599ae15512256bb5bc52e58e811
5cdc9d5998635e2b91c0324465c6018f
821ac2580843cb0c0f4baff57db8962e
b08d4847c370f79af006d113b3d8f6cf
17e1173f6fc7e920405f8dbde8c9ecac
874cd0b7b22ae1521fd0a7d405d6fa12
ea0c354f61ba0d88a422721caefad394
6a0e49c5e332df3af78823ca4a655ae8
8a019351b0b145ee3abe097922f0d4f6
337058dca8e6cbcb0bc02a85c823a003
842e903b955e134ae281d09a467e420a
d1d544dbf6b3867d758a5e7e7c3554bf
01f0d20a1a32e535b950428f5b5d6e72
fc041bda43a3067a0836dca2e6093c25
4956cf9ddd905ac3258f9605cf85332b
f5b4786c28ccf43e569cb21a6122a97e
cc640ad87befba89b440edca9ae5d235
0b464c9bebd10f02575b9d9d3a771db3
d0c74483f20c608a0a89c5ba05c2197f
b1661862db623e05a2694c483dce6e91
ffe53fb9280bf3a8ceb366997488486e
c0d0b7ffaec38de642bf6ff6971f4f9e
05f2c7675ff5cda1bee6a168bdbecac0
9ee4c29c95ed435644e6273b1ae3da58
0607ce9793eea0a42819957528d92b02
97fa64dfaa27d4b236e4a76417ab51c1
82d811a8a76df0cda3f34fdcd0e26e27
```

```
0b7732129b46ed15ff73f72886946220
30c5592a133137a84f61898993e513db
aa68ecf6f097ffb01c981f09a21aef32
bbe534abcc0a907f3c18cfe207a5dfca
29e0259b4ea971c72fd7fcad54a0f8d0
```

C&C domains and hostnames:

```
 00000000000.888[.]ru
10000000000.888[.]ru
adobephotoshop11111[.]com
adobephotoshop22222[.]com
domain12827312[.]com
helloflashplayers12345[.]com
hellojavaplayers12345[.]com
ilovereservdom213ada2[.]ru
iownacarservice[.]ru
iownacarservice1[.]com
msframework1[.]com
msframework1[.]ru
msframeworkx64[.]com
msframeworkx86[.]com
msframeworkx86[.]ru
msoffice365net[.]com
nullllllllllll[.]com
ollygo030233[.]com
ollygo030233[.]ru
pop3smtp5imap2[.]com
pop3smtp5imap3[.]com
pop3smtp5imap4[.]ru
reservedomain12312[.]ru
total-updates[.]com
```

C&C IPs:

```
 146.185.233.32
81.4.111.176
95.211.228.249
217.174.105.86
```