

# SECURITY RESPONSE

## Dridex: Tidal waves of spam pushing dangerous financial Trojan

Dick O'Brien

Version 1.0 – February 16, 2016

“ *Even organizations who are well protected against the group's malware can often struggle to cope with the sheer volume of spam the attackers send.* ”

# CONTENTS

OVERVIEW.....	3
Key findings.....	5
Background.....	7
2015 takedown operation.....	7
Prevalence.....	9
Victims.....	10
Infection vector: Spam campaigns.....	12
Malicious attachments.....	17
Dridex in action.....	20
Dridex: Technical analysis.....	22
Loader module.....	22
Main module.....	22
VNC module.....	24
SOCKS module.....	24
mod4 module.....	25
mod6 module.....	25
Attribution.....	27
Protection.....	27
Mitigation strategies.....	28

## OVERVIEW

The Dridex financial Trojan has emerged as one of the most serious online threats facing consumers and businesses. The attackers operating the Dridex botnet have continually refined the Trojan, which is now capable of harvesting banking credentials from customers of approximately 300 banks and other financial institutions in over 40 countries.

Dridex's operators are disciplined and highly active, pushing out in the malware through massive spam campaigns that run to millions of emails per day. Even organizations who are well protected against the group's malware can often struggle to cope with the sheer volume of spam the attackers send.

Law enforcement operations against Dridex have led to some arrests but have had a limited effect on the group's overall activity. On the evidence of recent months, Dridex will continue to be one of the main financial threats during 2016.

## KEY FINDINGS

“ These spam campaigns operate on a massive scale.

During one 10-week period, at least 145 spam campaigns were observed.


”

## Key findings

---

- The number of Dridex infections detected by Symantec increased during 2015. Between January and April, there were less than 2,000 infections per month. Infection numbers spiked considerably in the following months, before dropping and stabilizing at a rate of 3,000 to 5,000 per month in the final quarter.
- Dridex is configured to attack the customers of selected banks and other financial institutions by stealing their credentials during online banking sessions. The malware can now target nearly 300 different organizations in over 40 regions.
- Dridex is heavily focused on financial institutions in wealthy, English-speaking nations, with the majority of targets located in these regions. The attackers also prioritize other European nations and a range of Asia-Pacific states.
- Dridex has been almost exclusively distributed through spam email campaigns. These spam campaigns operate on a massive scale. During one 10-week period, at least 145 spam campaigns were observed. The average number of emails blocked by Symantec per campaign was 271,019.
- Almost three quarters (74 percent) of Dridex spam campaigns used real company names in the sender address and frequently in the email text. Where real company names were used, the attackers usually used a top level domain in the sender address that matched the region of origin, e.g. “co.uk” in the case of UK companies.
- The vast majority of spam campaigns were disguised as financial emails, e.g. invoices, receipts, and orders. During the period analyzed, spam was heavily focused on English-speaking regions, with the majority of emails purporting to come from English-speaking senders.
- Dridex’s operators are quite professional in their approach, usually following a Monday-to-Friday working week and even taking time off for Christmas. The malware is continually refined and some degree of effort is applied to its spam campaigns in order to make them appear as authentic as possible.

## BACKGROUND

A person is walking through a complex maze of interlocking gears. The scene is dimly lit, with a bright light source from the left casting long shadows and highlighting the textures of the gears. The person is seen from behind, walking away from the viewer into the depths of the maze.

“ The attackers using Dridex have moved away from self-propagation as an infection vector and the malware is now spread through massive spam campaigns. ”

## Background

The original version of Dridex first appeared in 2012. Known as Cridex (detected by Symantec as [W32.Cridex](#)), the malware added the infected computer to a botnet and stole banking credentials by intercepting online banking sessions. The original Cridex acted as a worm and spread by copying itself to network drives and attached local storage devices, such as USB keys.

The current version, known as Dridex, first appeared in 2014. Like earlier versions, its primary function is to add the victim's computer to a botnet and harvest banking credentials using man-in-the-browser (MITB) attacks. The attackers using Dridex have moved away from self-propagation as an infection vector and the malware is now spread through massive spam campaigns. By 2015, it had become one of the most prevalent financial Trojans.

The Dridex botnet received a significant update in November 2014, when command and control (C&C) communications were switched to a peer-to-peer (P2P) format. The move decentralized Dridex's infrastructure and made the botnet more resilient to takedown operations. P2P communications made it more likely that the botnet would stay live should key pieces of infrastructure be taken offline.

In addition to this, Dridex is segregated into a number of subsidiary botnets, known as subnets. These subnets are identified by three digit numbers, e.g. 120, 220 etc. It appears likely that different teams of attackers are operating each subnet.

## 2015 takedown operation

Dridex's high level of activity has attracted the attention of police forces in a number of regions. In October 2015, [an international law enforcement operation against the botnet](#) saw one man charged alongside a coordinated effort to sinkhole thousands of compromised computers, cutting them off from the botnet's control. The operation involved [the FBI in the US](#), the [UK National Crime Agency](#) and a number of other international agencies.

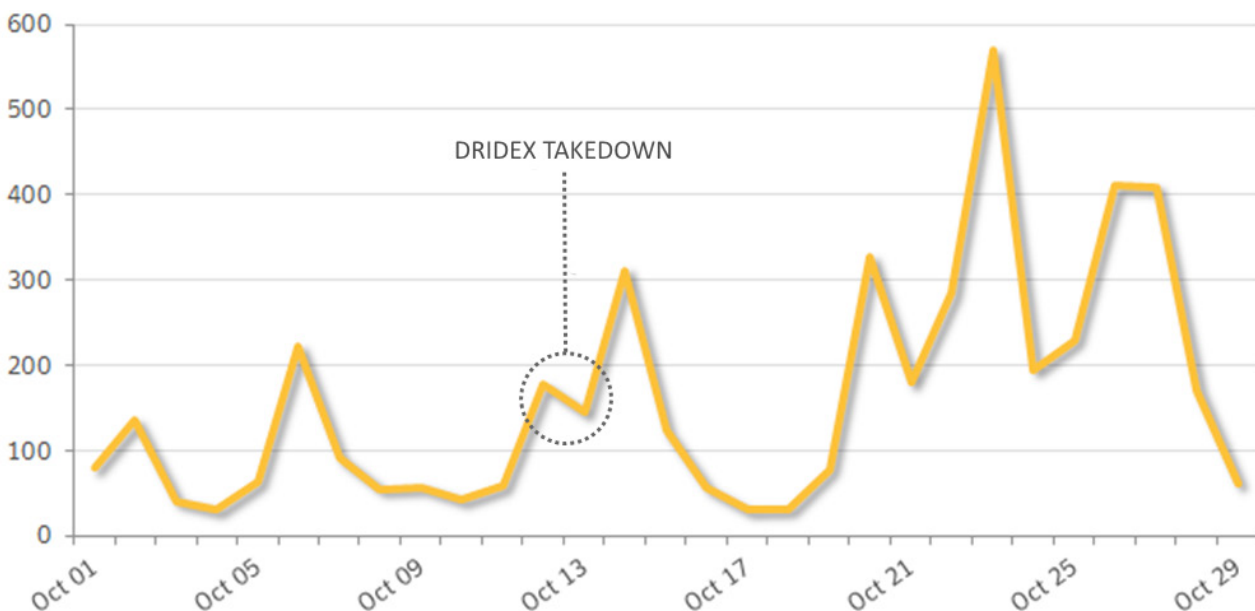



Figure 1. Takedown operation during October 2015 had little impact on Dridex infections

It appears this may have only been a partial success as Dridex continues to propagate, indicating many key elements of the operation are still functioning. As illustrated in Figure 1, the operation had little impact on overall infection numbers.

## PREVALENCE



“ Dridex was one of the most active financial Trojan threats during 2015. When compared with similar threat groups, it accounted for almost half of all infections in 2015. ”



## Prevalence

The number of Dridex infections detected by Symantec increased during 2015. Between January and April there were less than 2,000 infections per month. Infection numbers spiked considerably in the following months, hitting almost 16,000 in June before dropping and stabilizing at a rate of 3,000 to 5,000 per month in the final quarter.

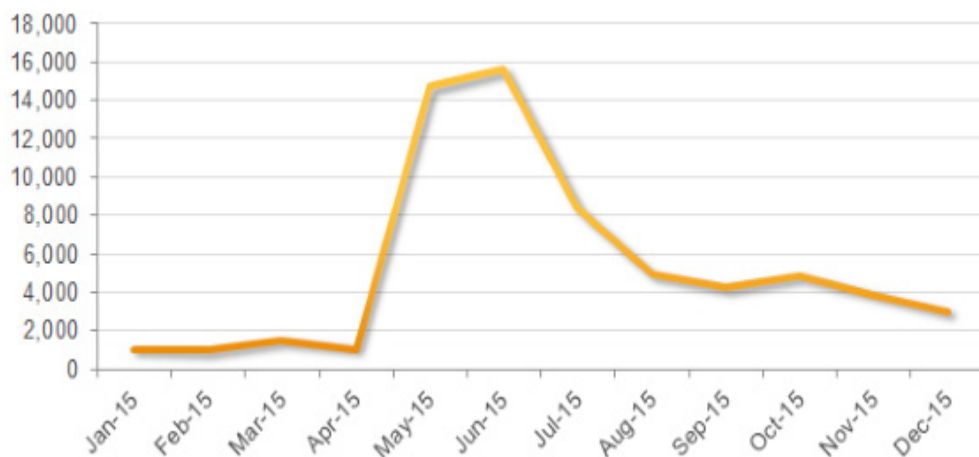


Figure 2. Dridex infections detected during 2015

Dridex infections were detected in a wide range of regions during 2015. While the largest infection numbers in 2015 occurred in Germany, this statistic was inflated by a wave of attacks from a group unrelated to Dridex, using a different variant of the original Cridex malware. The Dridex group itself has also been seen to attack Germany, albeit on a smaller scale.

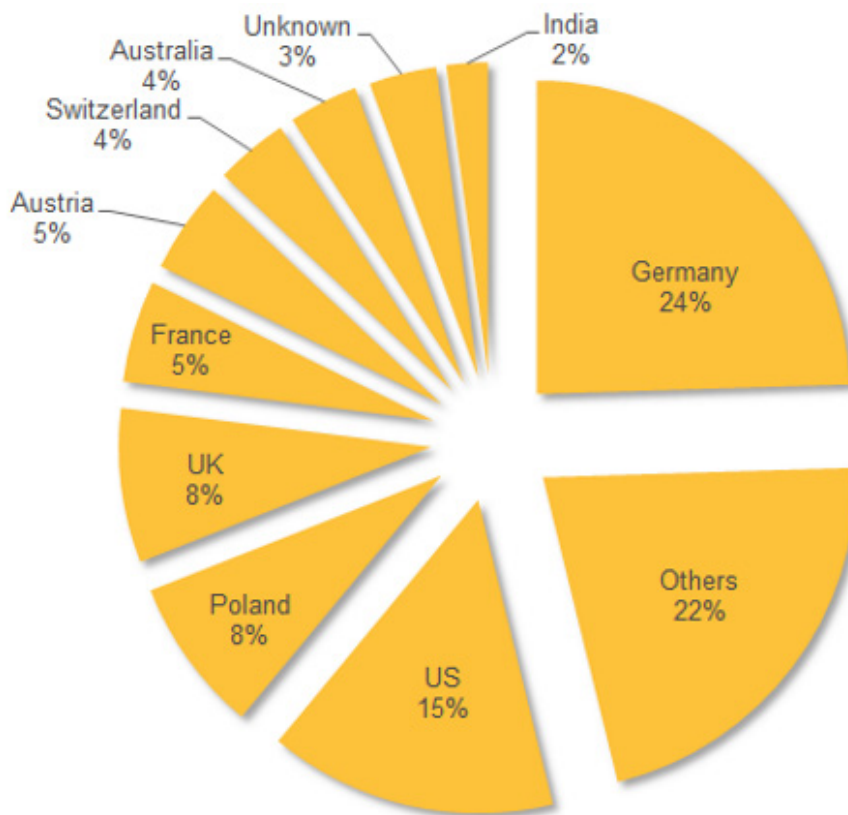


Figure 3. Dridex infections by region during 2015

English-speaking regions including the US, UK, and Australia experienced high infection rates, which reflected the high number of banks in these nations that the attackers have configured the malware to attack and the number of English-language spam campaigns spreading the Dridex Trojan.

Dridex was one of the most active financial Trojans during 2015. When compared with similar threat groups, it accounted for almost half of all infections in 2015. Of its peers, only Dyre (detected by Symantec as [Infostealer](#)).

[Dyre](#)) came close in terms of infection numbers.

Both Zeus (detected by Symantec as [Trojan.Zbot](#)) and Ramnit (detected by Symantec as [W32.Ramnit](#)) have significantly higher infection numbers than Dridex, but it is difficult to make a direct comparison with Dridex and similar groups. Zeus has multiple variants, is operated by disparate groups and cannot really be regarded as a single attacker group. Ramnit was subject to a [major takedown operation in February 2015 and does not appear to be actively in use](#). High infection numbers persist due to the virulent nature of some versions of the malware, which propagate by infecting files on the compromised computer and any attached drives.

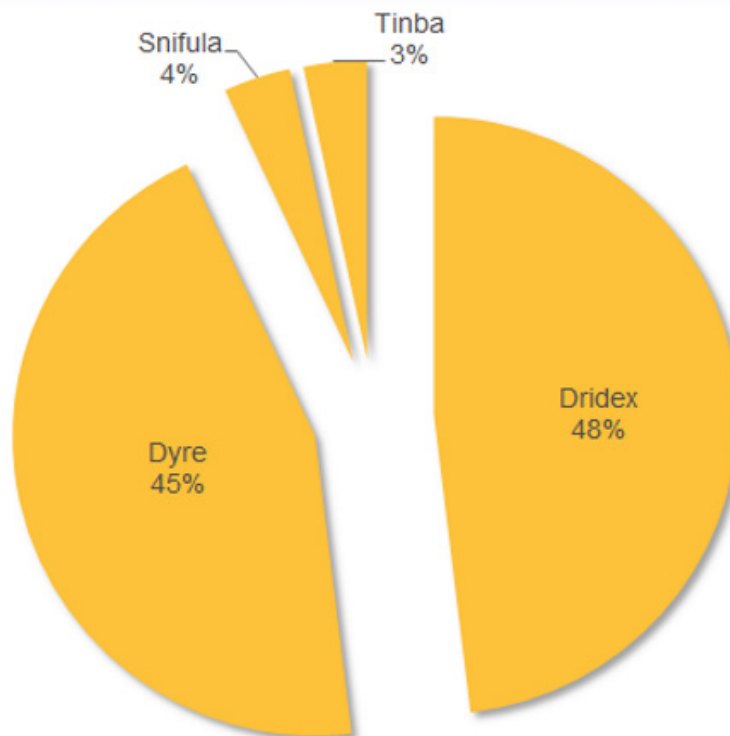


Figure 4. Dridex infections in 2015 compared with similar financial Trojan threats

## Victims

Dridex is configured to attack the customers of selected banks and other financial institutions by stealing their credentials during online banking sessions. The malware has been configured to target the customers of nearly 300 different organizations in over 40 regions.

Dridex is heavily focused on the customers of financial institutions in wealthy, English-speaking regions, with the majority of targeted organizations located in these places. The attackers also prioritize other European nations, along with a range of Asia-Pacific states.

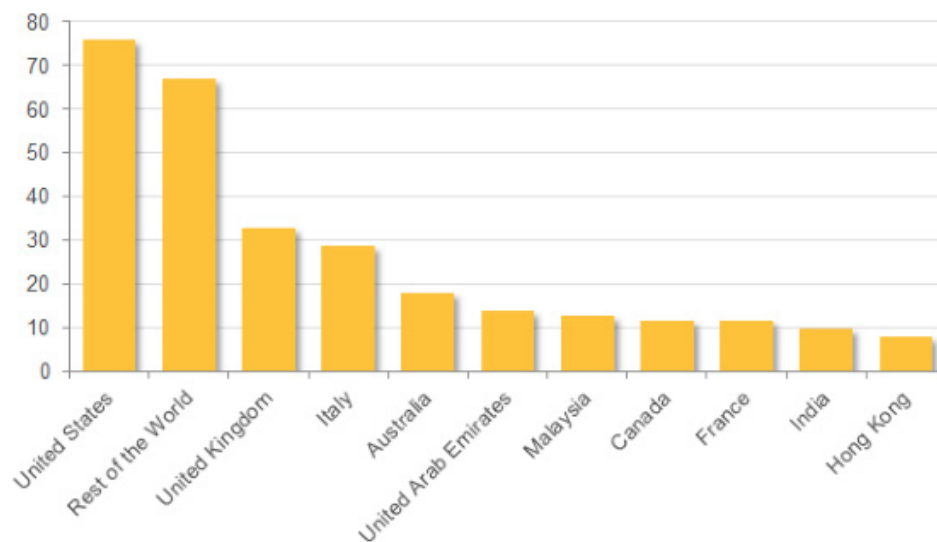


Figure 5. Number of organizations whose customers are targeted by Dridex, per region

## INFECTION VECTOR: SPAM CAMPAIGNS

“The attackers behind Dridex regularly send millions of spam emails in the course of one day.”

## Infection vector: Spam campaigns

Since 2014, Dridex has been almost exclusively distributed through spam email campaigns. These email campaigns are notable for their massive scale, frequency, and professionalism. The attackers behind Dridex regularly send millions of spam emails in the course of one day.

Analysis of 145 known Dridex spam campaigns logged between November 1, 2015 and January 15, 2016 revealed a number of clear trends:

- Dridex spam campaigns operate on a massive scale. The average number of emails blocked by Symantec per campaign was 271,019. The largest campaign seen by Symantec resulted in 982,832 emails being blocked.
- Almost three quarters (74 percent) of spam campaigns used real company names in the sender address and frequently in the email text.
- Where real company names were used, the attackers usually used a top level domain in the sender address that matched the region of origin, e.g. “co.uk” in the case of UK companies.
- Spam campaigns during the period analyzed were heavily focused on English-speaking regions, with the majority of emails purporting to come from English-speaking senders.
- The vast majority of spam campaigns were disguised as financial emails, e.g. invoices, receipts, and orders.

During the period analyzed, Dridex mounted a consistent series of massive spam campaigns. The attackers operated on a Monday-to-Friday working week, with no spam campaigns detected on Saturdays or Sundays. They also ceased all activity between December 24, 2015 and January 6, 2016. The sole exception to this pattern was Wednesday November 25, when no spam campaigns were detected. The reason for this aberration is unknown.

On the weekdays when the attackers were active, an average of three spam campaigns were launched per day. The lowest number of campaigns launched in a day was one and the highest number seen was eight in one day.

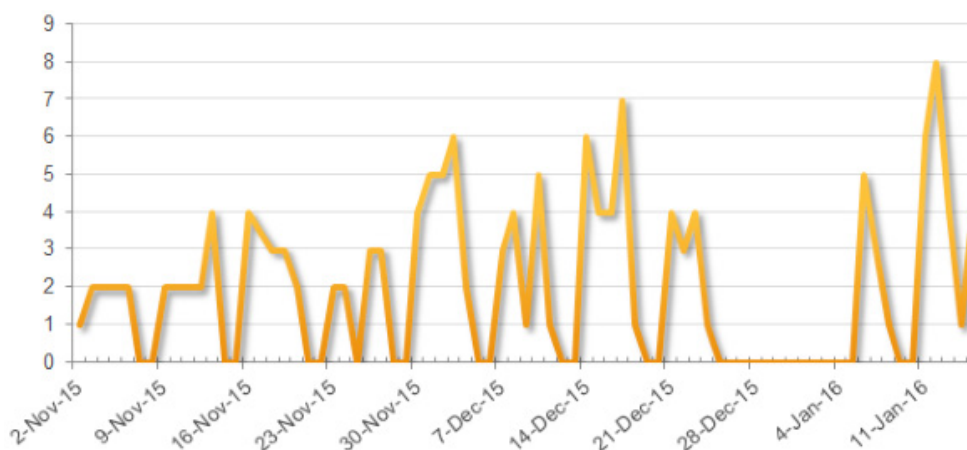


Figure 6. Number of known Dridex spam runs per day, November 1 2015 to January 15 2016

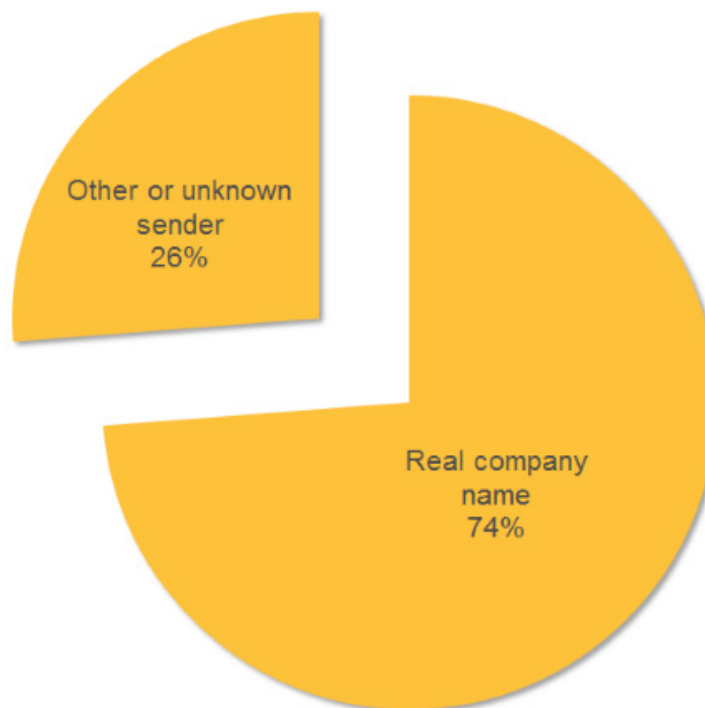


Figure 7. Proportion of Dridex spam campaigns using real company names

The attackers behind Dridex have gone to some lengths to make their spam emails appear more authentic. During the period analyzed, the majority of spam campaigns used real company names in the body text, subject line, and/or sender address.

Furthermore, when real company names were used, the attackers frequently included top level domains in the sender address that matched the company's region of origin, e.g. "co.uk" in the case of UK companies.

Despite generally having good attention to detail, the attackers did make occasional mistakes. In some instances the sender address, subject line, and/or email body contained contradictory information, likely resulting from the attacker entering the wrong details into one or more fields of the email.

On occasion, attachments or malware payloads were malformed, meaning that the malicious attachment would fail to install Dridex on the victim's computer.

The vast majority of Dridex spam campaigns during the period analyzed involved emails disguised as some sort of financial statement. Invoices were by far the most popular choice of subject, with a number of other financial themes being used on a less frequent basis.



Figure 8. Dridex spam email containing contradictory information about who the sender is. The sender address and signature mention TopSource, the subject line mentions British Gas, and the signature mentions Trinity Restaurants.

# Invoice

Statement

Message Documentation

Scan Order Receipt

Shipping Payment

Figure 9. Most popular keywords seen in subject lines of Dridex spam campaigns

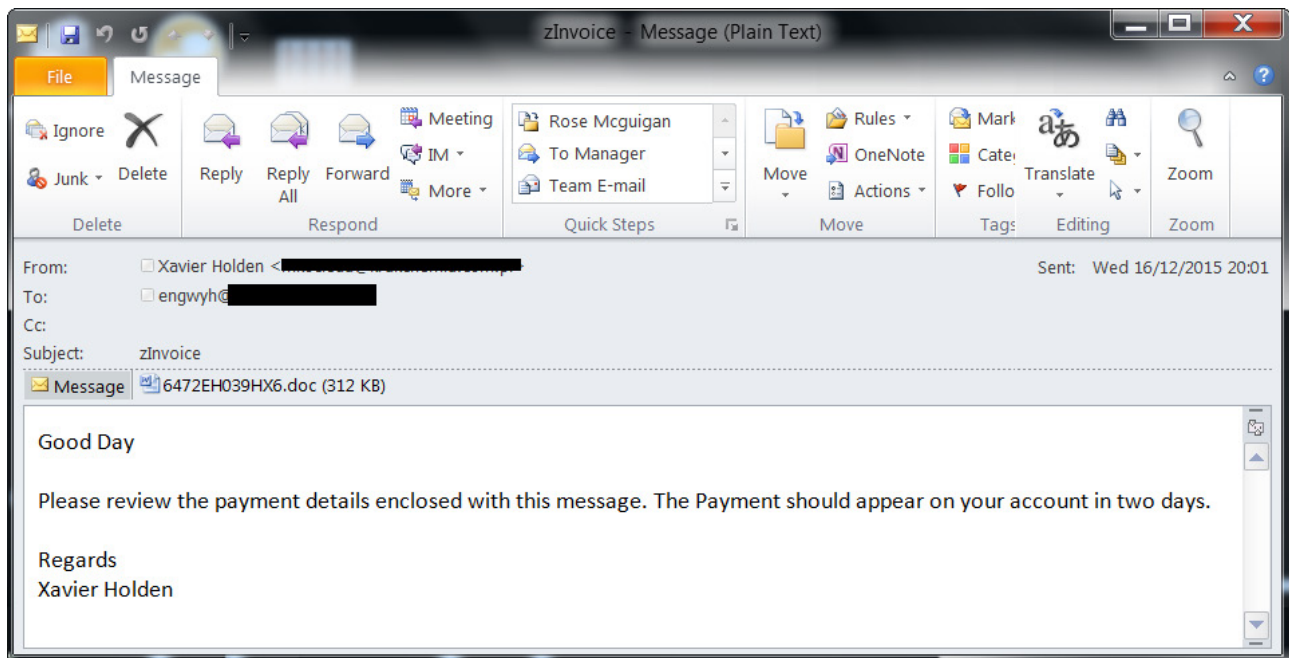


Figure 10. Example of Dridex-related spam email disguised as a financial document.

The fact that financial themes are so heavily favored indicates that the attackers have had a high degree of success with this tactic. It is likely that some consumers are tricked into opening attachments over concerns that they have been charged for goods they didn't order. In the case of businesses, employees in accounts departments are often used to receiving high volumes of emails from a diverse range of suppliers and customers. They may open one of these spam emails in the belief that it contains a legitimate document.

Aside from financial data, the only other frequently observed theme involved emails purporting to contain scanned documents (usually claiming to be sent by a network-connected scanner) and emails claiming to have some form of message attached.

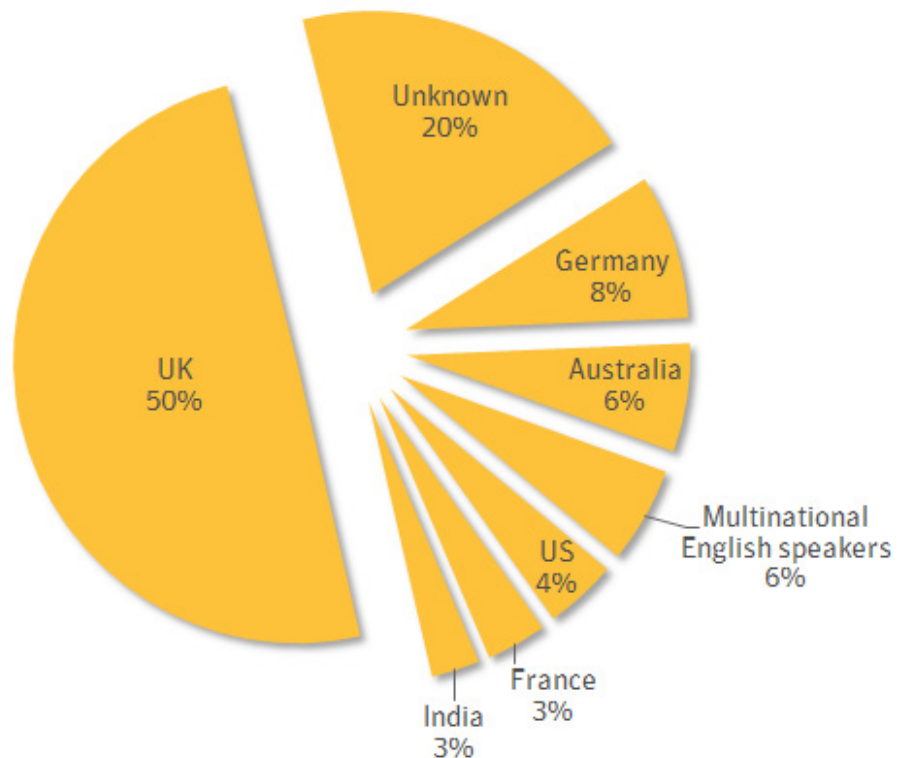


Figure 11. Dridex spam campaigns by target region

During the six-week period analyzed, Dridex spam campaigns appeared to be heavily focused on English-speaking regions. Half of all email campaigns were primarily directed at the UK, using emails that appeared to come from UK-based organizations. The other English-speaking regions targeted during this period included the US, Australia, and India (where English is the main language of business).

A small proportion of emails (six percent) purported to come from large, English-speaking multinational companies, which could trick recipients in a range of different regions.

The non-English speaking regions targeted during this period were Germany and France. Once again, a significant proportion of spam emails purported to come from real companies and the emails themselves were composed in German and French. The attackers occasionally made mistakes, such as spelling the German word Rechnung (Invoice) as “Rechung”.

Dridex activity is divided out into several distinct botnets, known as “subnets”. Each is identified with a three-digit number. Of the spam campaigns where a subnet was identified, Subnet 220 was the most prolific during the period analyzed, as it was responsible for 40 percent of campaigns. Subnets 223 and 120 were also highly active during this period.

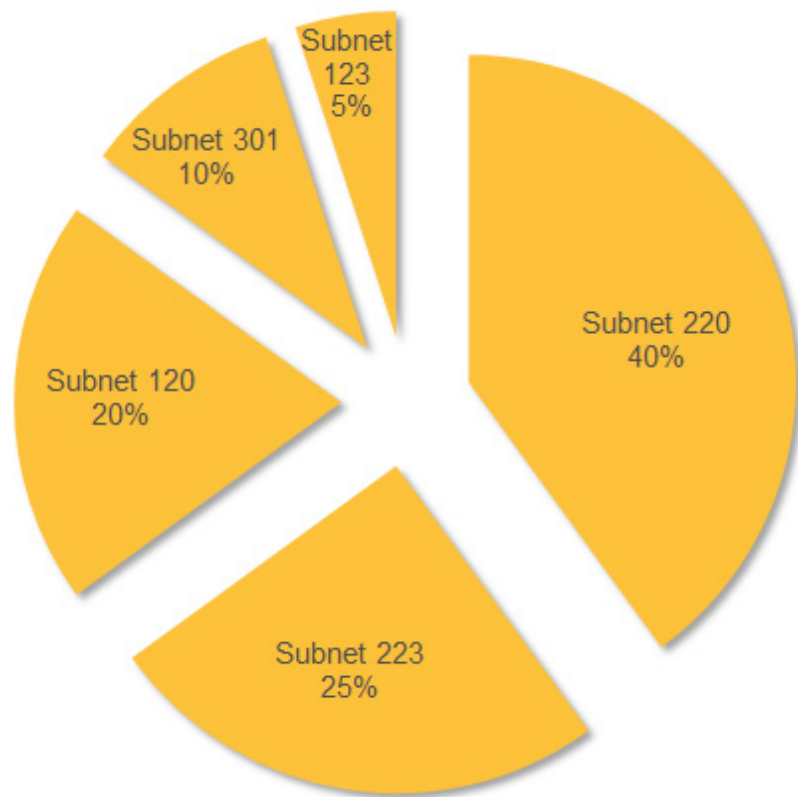


Figure 12. Dridex spam campaigns by botnet number

# MALICIOUS ATTACHMENTS



“Virtually all spam campaigns spreading Dridex do so using attached Word documents containing a malicious macro.”



## Malicious attachments

Most spam campaigns spreading Dridex do so using attached Word documents containing a malicious macro. Symantec detects these malicious attachments as [W97M.Downloader](#). If this macro is allowed to run, a malicious .vbs file is dropped and executed. This file is detected as [VBS.Downloader.Trojan](#). This malicious .vbs file will in turn download and install Dridex on the victim's computer.

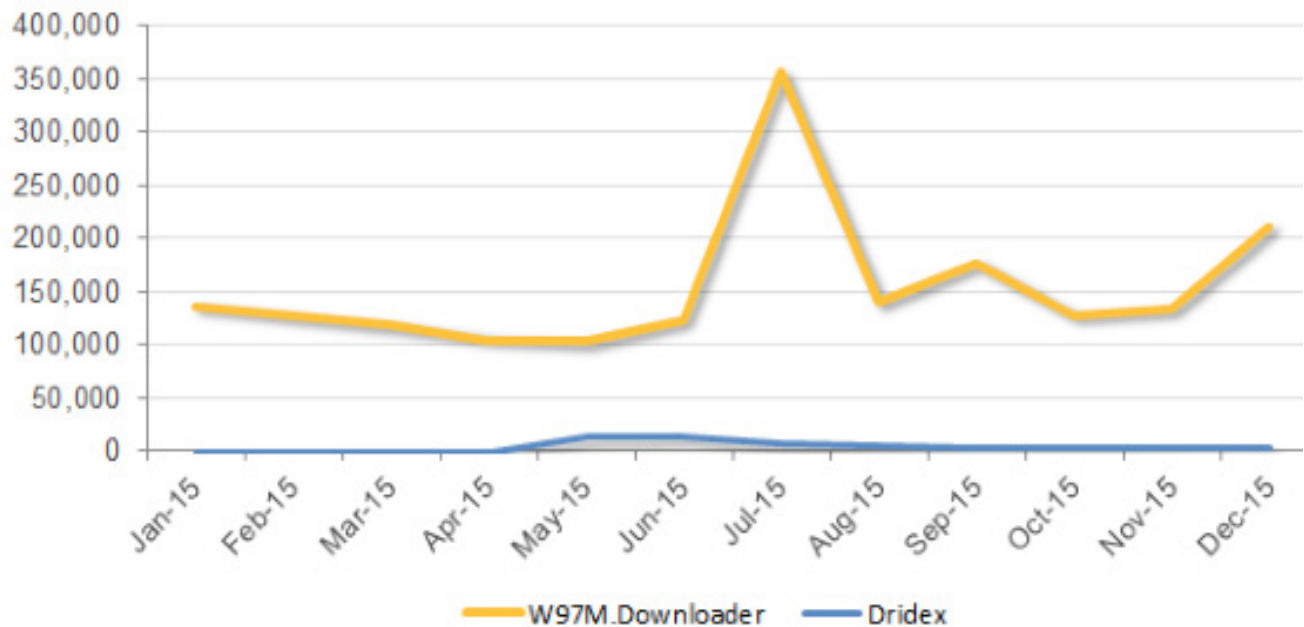


Figure 13. Dridex infections compared to W97M.Downloader infections by month during 2015

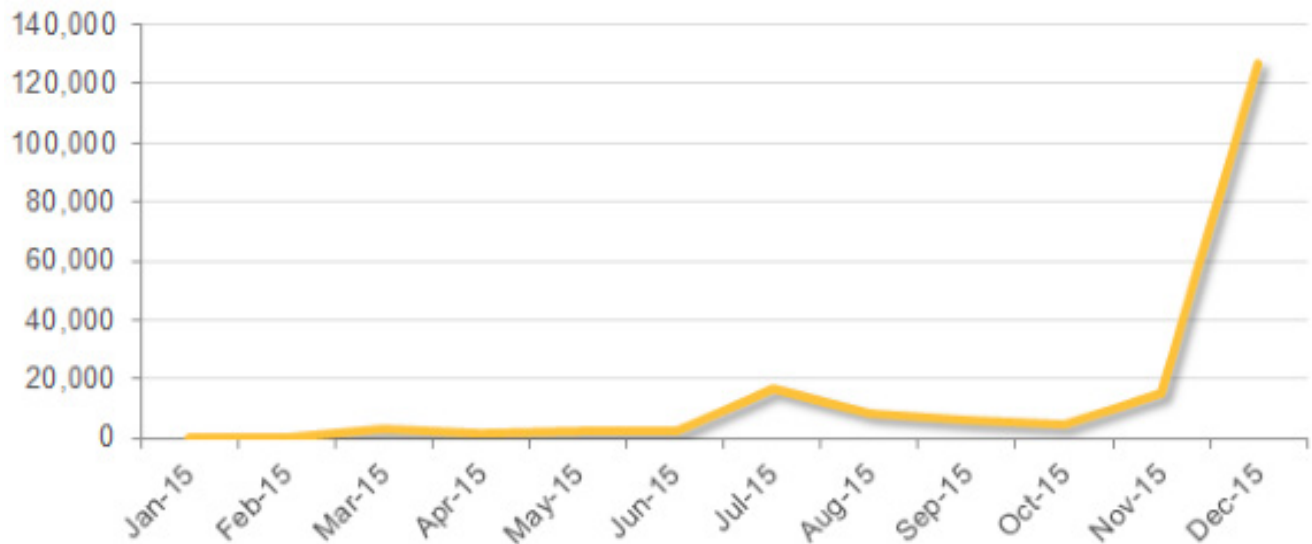


Figure 14. JS.Downloader infections detected during 2015

The number of W97M.Downloader infections increased during the second half of 2015. Following a surge in July, infection numbers slipped back in subsequent months before another notable uptick during December.

The level of W97M.Downloader infections seen during 2015 greatly exceeds the numbers of Dridex infections seen during the same period, with the latter averaging 5,400 infections a month. Two main factors account for this trend. In most cases, a downloader such as W97M.Downloader will be detected and deleted by antivirus software before it has a chance to install its payload onto a computer. Secondly, while Dridex is one of the main threats currently using W97M.Downloader, it is not the only one.

While the Dridex group has largely relied on malicious Word document attachments, in recent weeks it has been observed to vary its tactics and, in some spam campaigns, use malicious JavaScript attachments (detected by Symantec as [JS.Downloader](#)).

Interestingly, the number of JS.Downloader infections detected by Symantec jumped significantly during December 2015.

## DRIDEX IN ACTION

“Dridex is capable of injecting itself into the three most commonly used Windows web browsers every time they are opened and monitoring them for online banking sessions.”

## Dridex in action

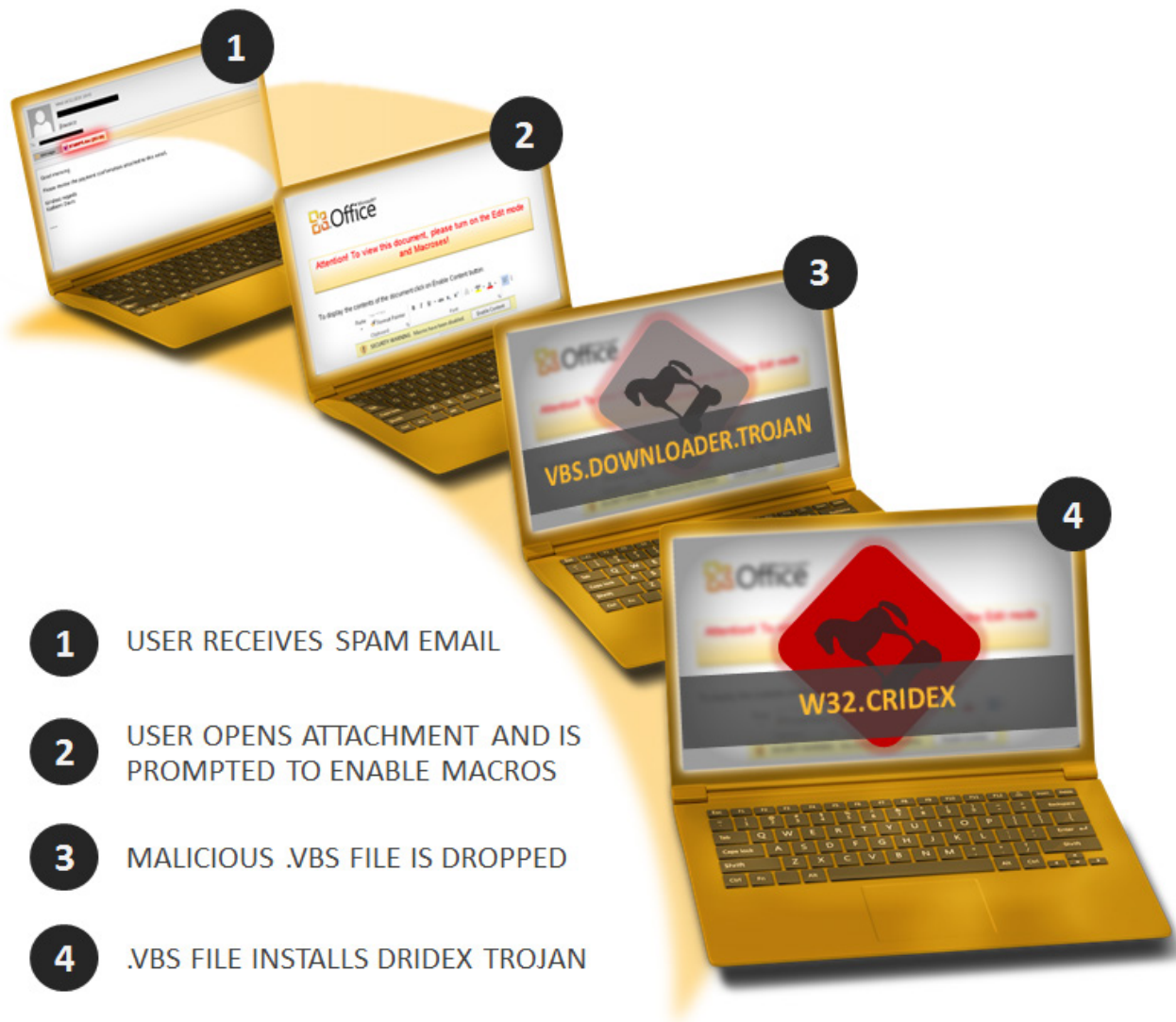


Figure 15. The Dridex infection process.

While the Dridex Trojan has a broad range of functions, it is mainly employed to steal the victim's banking credentials and add their computer to the Dridex botnet.

Credentials are stolen primarily through man-in-the-browser (MITB) attacks. Dridex is capable of injecting itself into the three most commonly used Windows web browsers (Internet Explorer, Chrome, and Firefox) every time they are opened. The Trojan then monitors browser activity for online banking sessions. If the user logs into one of a configured list of almost 300 websites (mostly banks), Dridex will attempt to steal their credentials using a variety of methods, such as capturing data input into online forms, logging keystrokes, or taking screenshots.

Stolen data is transmitted back to attacker-controlled C&C servers using encrypted communications.

## DRIDEX: TECHNICAL ANALYSIS

“Dridex has a number of core modules, used to handle the main functionality of malware, in addition to a number of additional features.”

## Dridex: Technical analysis

Dridex has a modular architecture—it can download and install additional modules after initial infection. This makes the Trojan relatively straightforward for its authors to add and refine its features. Dridex has a number of core modules that are used to handle its main functionality, in addition to a number of extra modules that provide additional features.

### Loader module

The Loader module is responsible for downloading and installing the Main module. The Loader communicates through HTTPS and uses RC4 to encrypt XML messages which are exchanged with the control servers found in the embedded configuration.

*Table 1. Dridex Loader module information*

<b>File name</b>	1111.exe
<b>MD5</b>	6f9ec4ffa07bcade346b04317dfb6f1c
<b>SHA1</b>	c4a5ad53737df1087f1bce594bd20554345ac335
<b>SHA256</b>	a497de7f2488f093aa74562695a2ce705cbddbd2c4a357f5c785f23ea7450f43
<b>Size</b>	324608
<b>PE timestamp</b>	2015-10-01 10:52:51
<b>Purpose</b>	Loader – (install Main module and associated configuration)

*Table 2. Load point registry key created by Loader module*

<b>Key</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
<b>Name</b>	b5V9
<b>Data</b>	rundll32.exe %AppData%\1.tmp [RANDOM LETTERS AND NUMBERS]

The Loader module creates a registry key to act as a load point for the Main module.

*Table 3. Main module configuration registry key created by Loader module*

<b>Key</b>	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\[GENERATED CLSID]\ShellFolder
<b>Name</b>	0
<b>Data</b>	[ENCRYPTED MAIN CONFIGURATION]

The Loader also creates the registry key containing configuration information for the downloaded Main module.

The Loader exchanges RC4 encrypted XML messages over HTTPS with a C&C server. The Loader contains the following hard-coded RC4 key:

- 560re2DobsPZGdq4yEbwKlpY9ZJqyvHjRA

The Loader will request the Main module binary and the Main module configuration from one of the servers in its embedded configuration.

### Main module

The Main module is

*Table 4. Dridex Main component information*

<b>File name</b>	1.tmp
<b>MD5</b>	5779e8f68f4d06fa3b6a73023ee7d552
<b>SHA1</b>	90842a7540df9b1c3cf9fbf0b0c751724ae81124
<b>SHA256</b>	cd1b462be0821eed24a97523206399b9e83266e6675a26a2b070edfe9dcd2b5a
<b>Size</b>	498152
<b>Purpose</b>	Main – (backdoor/MITB attacks)

responsible for the majority of Dridex's functionality. Network communication with peers and remote servers uses HTTPS or raw TCP. The data sent over the network is XOR encrypted, uses asymmetric encryption, and is compressed using gzip. The Main module will create its own public and private key pair.

The Main module is injected into the explorer.exe process. The module will also inject itself into web browser processes such as Firefox and Chrome to perform MITB attacks.

The Main module can perform the following core functions:

- Steal information from forms
- Take screenshots
- Redirect HTTP requests
- Inject code into web applications
- Log keystrokes
- Steal password
- Virtual network computing (VNC)
- Back connect
- Act as a mini server (peer node)
- Delete files
- Download other modules
- Steal cookies

The module performs these functions by sending and receiving commands, modules, and configuration information over the P2P network. XML messages are used to communicate over the P2P network. The module uses RC4 to encrypt network traffic with a key generated at runtime using the CryptGenKey API. Earlier variants of Dridex used XOR instead of RC4 to encrypt network traffic.

### Main module settings

The Main module is configured to perform man-in-the-browser attacks by a "settings" configuration, which is stored encrypted in the registry.

**Table 5. Dridex "settings" configuration's high level elements**

Basic element	Purpose
<b>Root</b>	Contains all following elements
<b>Nodes</b>	Public nodes available for the bot to connect to
<b>Settings</b>	Options and data for web injects
<b>Commands</b>	Additional commands to be executed

These contain the method of data ex-filtration and properties associated with that method.

**Table 6. Dridex "settings" configuration method elements**

Method	Purpose
<b>httpshots</b>	Take screenshots for the requested sites that match a URL regex
<b>httpinblock</b>	Block injections for the requested sites that match a URL regex
<b>httpblock</b>	Block/allow access for the requested sites that match a URL regex
<b>formgrabber</b>	Grab data from forms for the requested sites that match a URL regex
<b>clickshots</b>	Take screenshots when clicking in a site that matches a URL regex. Useful in case of a virtual keyboard input
<b>redirects</b>	Redirections used for additional actions, usually used with httpinjects to fetch remote scripts. Modules VNC and SOCKS may also be used for that action
<b>smartcard</b>	Similar to redirects, URL patterns indicate possible smart card related functionality
<b>httpinjects</b>	Patters of HTML code to be searched and replaced for the requested sites that match a URL regex
<b>httpcookiescut</b>	Related to cookie data fetch for the requested sites that match a URL regex

## VNC module

The VNC module acts as a virtual network computing (VNC) server. There is an x86 and x64 module available, both containing similar functionality.

The module provides a graphical user interface (GUI) to remotely control the computer and contains two basic functions, starting and stopping the VNC server. The domain and port to connect to are passed as input arguments to the VncStartServer function.

The following operations are supported:

- Command Prompt
- Computer Management
- Control Panel
- Device Manager
- Disk Management
- Event Viewer
- File Explorer
- Logoff
- Task Manager
- Programs and Features
- Power Options
- Restart
- Shutdown
- System

File name	VncDll.dll
<b>MD5</b>	11240b94722da140b2709bdd5e3da118
<b>SHA1</b>	a1b7ceede38d1ff52f60f1c4ed0e7a1b02e3fc09
<b>SHA256</b>	0cafdbc2d8ec175ccf605ae898ef1fd5f775e933370e40f3a2c9e3f22c1377
<b>Size</b>	203264
<b>Purpose</b>	VNC module (x86)

## SOCKS module

The SOCKS module supports remote command execution, search, and download functionality on the compromised computer. There is an x86 and x64 module available, both containing similar functionality.

File name	socks_x32.dll
<b>MD5</b>	9b94506dbebb8e3f8fb8468583b1a185
<b>SHA1</b>	38a56cdeb970aa9e767ee74c1669b5328b2154c8
<b>SHA256</b>	68a18b59e551beb98d00dea39eb492f5cd588bbb487250aa69e96211d45f8016
<b>Size</b>	91136
<b>Purpose</b>	SOCKS module (x86)

The SOCKS module provides the following functionality on a compromised computer:

- Remote command execution
- File system search
- File download
- Command and control



The module also acts as a server interpreting commands as HTTP requests to remotely control the compromised computer. The remote address is passed as an argument to the module.

## mod4 module

The mod4 module is an additional Dridex module used to create a new process. There is an x86 and x64 module available, both containing similar functionality. The process to create is parsed from the <lpCommandLine> command line, where <lpCommandLine> is the first argument passed to the currently running process.

**Table 9. Dridex SOCKS commands available**

Command	Description
<b>exec</b>	Remote command execution using cmd.exe
<b>search</b>	Enumerate drives/folders/files
<b>download</b>	Download files from victim

**Table 10. Dridex mod4 module information**

File name	Unknown
<b>MD5</b>	4530ae1c3d786edcbfac0244b4954c32
<b>SHA1</b>	42b8fbc0bba2d0576f38cce75e7bb30189809771
<b>SHA256</b>	bbaba6808a69a9a4de1a66de91637337f96f167831fb69890b9a20a20e3e2dfd
<b>Size</b>	3072
<b>Purpose</b>	mod4 module (x86)

## mod6 module

Another additional Dridex module is mod6. It is used to send emails using Outlook. There is an x86 and x64 module available, both containing similar functionality. It essentially functions as a spam module, using Outlook to send email to existing contacts.

The module functionality is available from two exported functions.

The GetContacts export is used to extract email addresses from Outlook. It uses the Component Object Model (COM) which is initialized using the following Outlook CLSID:

- 0006F03A-0000-0000-C000-000000000046

The SendMail export is used to send files using Outlook. The name, size, and data to be written to the file are passed as input arguments by this export.


**Table 11. Dridex mod6 module information**

File name	spammer_x32.dll
<b>MD5</b>	79d1378b6a1bf5636880cc0a7631a33e
<b>SHA1</b>	e29be9d8a16ae7ee950be2d1ae12b542313fac0b
<b>SHA256</b>	83d6e57210e3c7d6813730170d6f1cf2d42cb6dbee4756d7afe2904679aaa9f5
<b>Size</b>	23552
<b>Purpose</b>	mod6 module (x86)

**Table 12. Dridex mod6 exports**

Export	Description
<b>GetContacts</b>	Get contacts from Outlook
<b>SendMail</b>	Send email using Outlook

# ATTRIBUTION

The background features a 3D perspective of numerous translucent cubes, each displaying binary code (0s and 1s) on its faces. The cubes are arranged in a grid-like pattern that recedes into the distance, creating a sense of depth. The overall color palette is a gradient of dark blues and greys, with light rays emanating from behind the cubes, giving the scene a digital, ethereal atmosphere.

“ Interestingly, Dridex largely ceased operations on December 24, 2015 and resumed again on January 6, 2016. ”

## Attribution

---

The level of activity surrounding Dridex indicates that a large cybercrime group is behind the botnet. As mentioned earlier, Dridex is segregated into a number of subsidiary botnets, known as subnets. It appears likely that different teams of attackers are operating each subnet. It is unknown whether these groups act in loose association or whether they have a centralized organization. The US Department of Justice [has said that the botnet is “run by criminals in Moldova and elsewhere.”](#)

Dridex’s operators are quite professional in their approach, usually following a Monday to Friday working week. The malware is continually refined and some degree of effort is applied to its spam campaigns in order to make them appear as authentic as possible.

Interestingly, Dridex largely ceased operations on December 24, 2015 and resumed again on January 6, 2016. The attackers appeared to have taken an extended break over the holiday period, much like any other professional organization would do.

Given the extremely high level of activity surrounding Dridex in late 2015, it would be reasonable to assume that, barring a comprehensive takedown, the group will continue to pose a threat throughout 2016.

## Protection

---

Symantec and Norton products have the following protections against Dridex:

### Email protection

- Adopting a multi-layered approach to security minimizes the chance of infection. Using an email security solution should remove the chance of you accidentally opening malicious email and malicious attachments in the first place.
- Email-filtering services such as [Symantec Email Security.cloud](#) can help to filter out potential targeted attack emails before they can reach users.
- [Symantec Messaging Gateway](#)’s Disarm technology can also protect computers from this threat by removing the malicious content from the attached documents before they even reach the user.

### Antivirus

- [W32.Cridex](#)
- [W32.Cridex!gen1](#)
- [W32.Cridex!gen2](#)
- [W32.Cridex!gen4](#)
- [W32.Cridex!gen5](#)
- [W32.Cridex.B](#)
- [W64.Cridex](#)
- [Trojan.Cridex](#)
- [VBS.Downloader.Trojan](#)
- [W97M.Downloader](#)

### Intrusion prevention system

- [System Infected: Trojan.Cridex Activity](#)
- [System Infected: Trojan.Cridex Activity 2](#)
- [System Infected: Trojan.Cridex Activity 3](#)
- [System Infected: Trojan.Cridex Activity 5](#)
- [System Infected: Trojan.Cridex Activity 6](#)
- [System Infected: W32.Cridex Worm Activity 4](#)
- [System Infected: W32.Cridex Worm Activity 6](#)
- [System Infected: W32.Cridex Worm Activity 8](#)
- [System Infected: W64.Cridex Activity](#)
- [Web Attack: Cridex.B Activity](#)

## Mitigation strategies

---

- Always keep your security software up to date to protect yourself against any new variants of this malware.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Exercise caution when conducting online banking sessions, in particular if the behavior or appearance of your bank's website changes.
- Delete any suspicious-looking emails you receive, especially if they contain links and/or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- If you suspect Dridex infection, immediately change your online banking account passwords using an uninfected system, contact your bank to alert them to look for any potentially fraudulent transactions.




**Author**  
**Dick O'Brien**  
Sr Information Developer

## About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings -- anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of \$6.5 billion.

To learn more go to [www.symantec.com](http://www.symantec.com) or connect with Symantec at: [go.symantec.com/social/](http://go.symantec.com/social/).

 Follow us on Twitter  
[@threatintel](https://twitter.com/threatintel)

 Visit our Blog  
<http://www.symantec.com/connect/symantec-blogs/sr>

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters  
350 Ellis St.  
Mountain View, CA 94043 USA  
+1 (650) 527-8000  
1 (800) 721-3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2016 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY . The technical information is being delivered to you as is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.