ARTICLE

TrickBot Focuses on Wealth Management Services from Its Dyre Core

Written by: Doron Voolf, Sara Boddy

Date: July 27, 2017

In this article, we explore TrickBot targets in configuration version 1000024 ("v24"), which was operating in June 2017. F5 Security Operations Center (SOC) researchers continually track TrickBot target and publish reports in conjunction with F5 Labs researchers. Our efforts are to understand the malware author's behavior and notify the targeted institutions so they can be on alert for TrickBot fraud within their environments.

Key data points from v24 analysis:

- 95% of TrickBot v24 URLs were identical to those targeted by Dyre in 2015, adding to the growing list of commonalities between Dyre and TrickBot.
- 62% of the targets in v24 were also targeted in v18 and v19, which were active in May, suggesting the target list always started from Dyre targets.
- v24 included a spike in Nordic targets—primarily UK, Sweden, Switzerland, Finland and Norway targets, as well as a large reduction in URLs in Australia and New Zealand.
- Clear focus on wealth management financial institutions that service individuals and businesses.
- Targeting both retail (personal accounts) and commerce (business accounts) banks.
- Targeting Islamic banks in UAE, UK, and Jordan.

TrickBot 101

TrickBot infects its victims much like any other banking trojan that begins with social engineering attacks, such as phishing or malvertizing, to trick unassuming users into clicking malware links or downloading malware files. Once a user engages with the malware and it's able to exploit the user's system (because of out-of-date patches and AV software—the exception would be zero-day malware), the malware installs and controls the host via commands from its command and control (C&C) server.

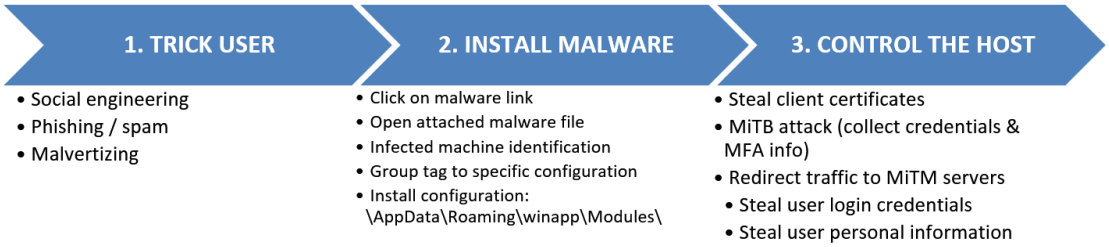

Figure 1: Initial TrickBot attack path

TrickBot's Dynamically Updating DLL Module

TrickBot has a basic configuration file that is written when the malware initially infects a victim's system. This configuration file specifies the malware's version, its C&C servers (that are set up on compromised IoT devices, specifically wireless routers[1]), and **modules** to be fetched and installed by the malware.

"**injectDll**" module is the core banking module that contains the malware's banking functionality, the list of targeted URLs, and servers to which the legitimate bank content is sent for modification upon receipt by the user. These files are updated frequently by the malware authors and dynamically deployed to TrickBot's infected systems.

These configuration versions and the URL targets within them are what the F5 SOC and Labs researchers analyze to understand the malware author's targets. There have been at least 29 new configuration files in the DLL module since September of 2016.

[1] https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/

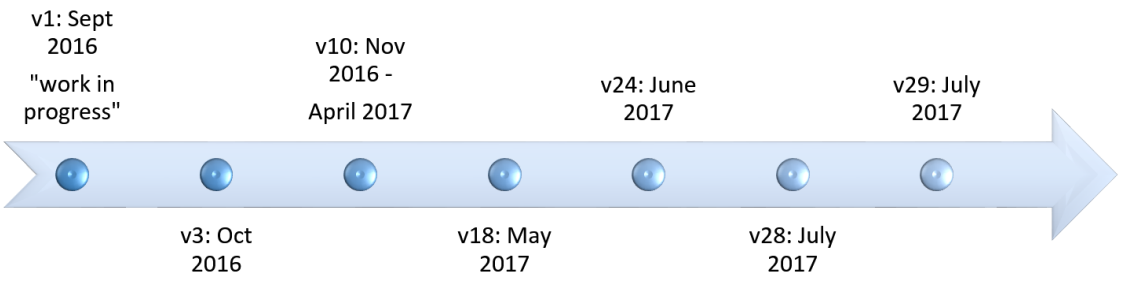

Figure 2: TrickBot configuration versions since September 2016

Once a user's host is infected with TrickBot, and the unassuming user browses to their banking site (a TrickBot-targeted URL), the malware injects malicious javascripts and redirects the session to fake pages that collect the user's data, including user credentials. The data collected is sent to "drop zone" servers, which the malware authors then uses to process fraudulent transactions on the accounts they have now have access to.

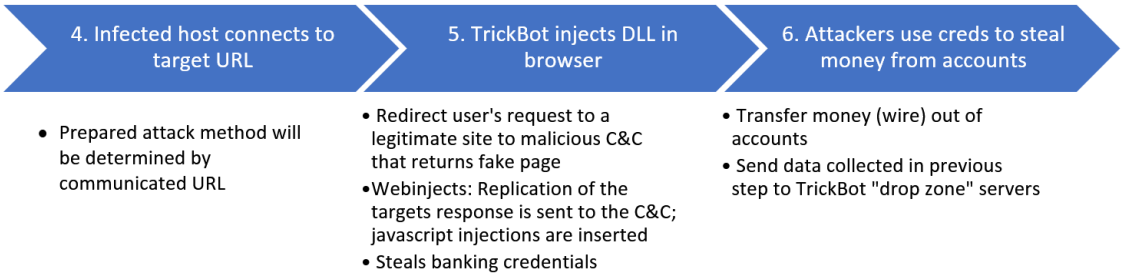

Figure 3: TrickBot post-infection attack path

TrickBot v24 Targets

There was a large expansion in targets from the previous configurations (v18 and v19) we analyzed[2] that were active in May. Configurations v18 and v19 included 210 and 257 targeted URLs across 13 countries and 155 businesses. Configuration v24 targeted 618 URLs, a 240% growth in target URLs over v19, across 34 countries and 177 businesses (see Appendix A for list of target businesses).

[2] https://f5.com/labs/articles/threat-intelligence/malware/trickbot-expands-global-targets-beyond-banks-and-payment-processors-to-crms

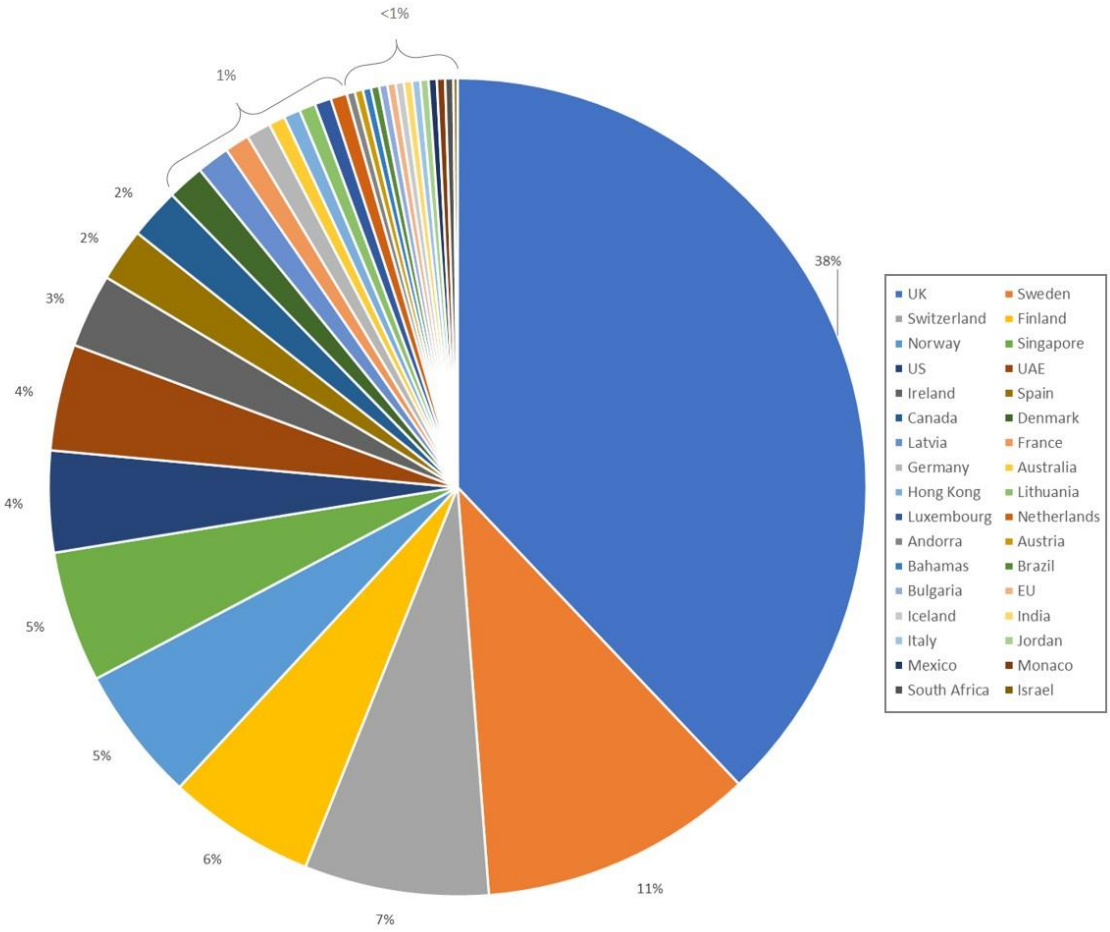

Figure 4: v24 country targets by URL count

European banks were the focus of TrickBot's targets in v24, comprising 81% of the URL targets. The primary targets were in the UK, Switzerland, and the Scandinavian countries of Sweden, Finland, and Norway; the UK and Sweden were collectively nearly 50% of the targets. Some of the banks targeted in those countries are foreign banks where the localized country domain was targeted, indicating the attackers are going after customers of those banks in those countries rather than targeting every country in which the bank operates.

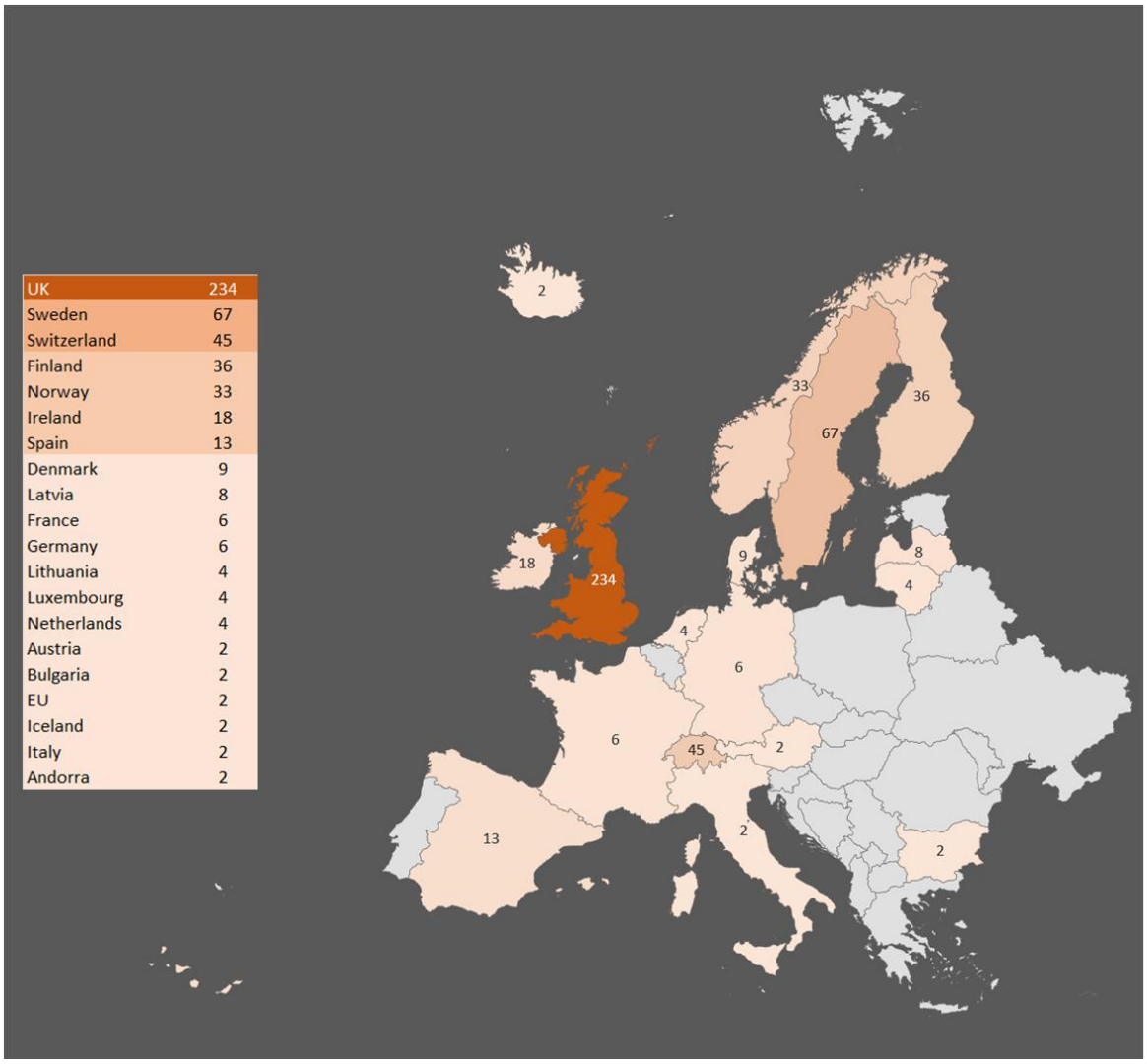

Figure 5: v24 European targets: URL count by country

Ninety-eight percent of the targets were financial institutions, including public and private banks focusing on both retail and commerce, wealth management services, retirement and investment firms, co-ops, internet banking, Islamic banking, savings banks, loan providers and clearing banks. The CRMs and payment processors are consistent from previous configurations, the insurance brokers are new since v18 and v19, however, those insurance brokers had banking divisions in the past. It could be that since these targets were pulled from Dyre circa 2015, it's likely they were targeting the banking division.

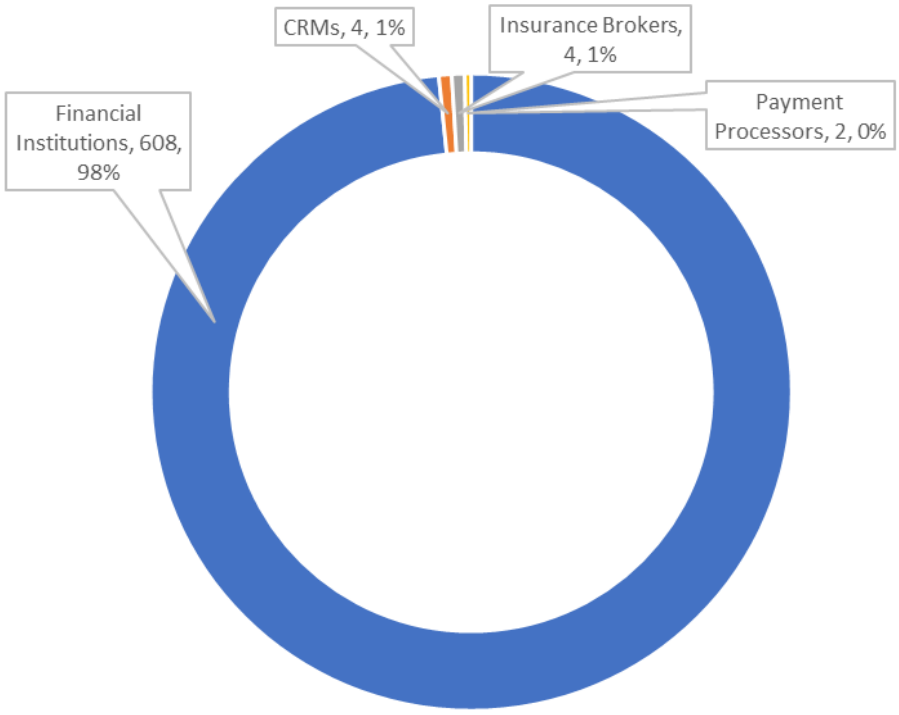

Figure 6: Targets by Industry

Notable Target Drops

European banks have continually been a top target of TrickBot, and although there was growth in targets in that region, Europe stands out more in this configuration because Australia and New Zealand targets dropped off, thereby boosting Europe's portion of the pie. There were no New Zealand targets in this configuration, and only four in Australia.

Another notable drop was PayPal, which drove a significant portion of US interest in previous configurations. Because PayPal was not targeted this time, the US dropped in overall % of targets.

TrickBot Targets are Directly from Dyre Circa 2015

What's most interesting about the URL targets is that they replicate Dyre's targets from 2015.[3] Ninety-five percent of the URLs in TrickBot v24 were also targeted by Dyre in 2015. It is widely

[3] https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/tspy_dyre.yysnz

believed that TrickBot and Dyre were written by the same authors because of code similarities. Specifically, they have the same loaders, encryption and decryption routines, structure of configuration files, and inter-process communication. The fact that both trojans target the same URLs just adds to the parallels and resulting conclusion that the same actors are likely behind both trojans.

Although almost all of TrickBot's URLs came from Dyre, not all of the Dyre URLs are present in this TrickBot configuration. In fact, TrickBot has some URL formulations that target a specific subdomain of a bank, but it doesn't use *all* the URLs for that subdomain. This suggests someone is selectively choosing which URLs from the Dyre list to use.

In researching the Dyre–TrickBot connection, we noticed that Salesforce and Reynolds & Reynolds appeared on the Dyre target list in the same formulation. Therefore, it's not actually surprising that TrickBot "expanded" into CRMs. This has been a behavior of financial malware for quite some time.

Some URLs in the TrickBot list do not appear on any published Dyre list that we found. Most of these are variations on URLs that *can* be found in the Dyre list. This suggests that the TrickBot authors are attempting to improve at least some of the Dyre URLs—although there are still many URLs that don't resolve anymore. Most of the "improvements" from Dyre to TrickBot are to UK and Swedish banks.

Almost Thirty Percent of Targets Have Wealth Management Specialties

Fifty of the 177 businesses targeted specialize in or offer wealth management services. Wealthy individuals are more likely to have multiple card holders on one account (who could be in multiple global positions at the same time), and process high value transactions frequently. These types of customers also have low patience for fraud holds. This type of behavior profile makes it more difficult for banks to implement the standard behavioral-based fraud controls that most financial institutions rely on now. This could make them a great target for attackers, and perhaps is one of the reasons why the targets have remained consistent over the years, beginning with Dyre in 2015.

Institutions with a Wealth Management Focus and/or Services	Country
Andbank	Andorra
Aktia Bank	Finland
Danske Bank	Global
Arab Bank	Jordan
Baltic International Bank	Latvia
Medicinos Bankas	Lithuania
DBS Bank	Singapore
OCBC Bank	Singapore
Investec	South Africa
Banca March	Spain
Banco Mediolanum	Spain
Carnegie	Sweden
Catella	Sweden
DNB Bank	Sweden
Erik Penser Bank	Sweden
Bank Cler	Switzerland
Bank von Roll	Switzerland
Barclays Bank	Switzerland
BHF-Bank	Switzerland
Julius Baer	Switzerland
Neue Helvetische Bank	Switzerland
Valiant	Switzerland
Abu Dhabi Islamic Bank	UAE
Mashreq Bank	UAE
United Arab Bank	UAE
Adam and Company	UK
Aldermore Bank	UK
Arbuthnot Latham	UK
Barclays Bank	UK
Butterfield Bank	UK
C. Hoare & Co	UK
Cater Allen	UK
Close Brothers Asset Management	UK
Coutts	UK
Credit Suisse	UK
Gerrard Investment Management	UK
Hargreaves & Lansdown	UK
HSBC Bank	UK

Investec	UK
J.P.Morgan	UK
Kleinworth Benson	UK
Rathbone Brothers	UK
St. James's Place Bank	UK
Standard Life Savings Limited	UK
Tilney	UK
Toronto-Dominion Bank	UK
Triodos Bank	UK
Yorkshire Bank	UK
Merrill Lynch	US
Voya	US

Figure 7: Financial institutions targeted that specialize in wealth management

Islamic Bank Targets

Twelve Islamic banks were targeted in the Middle East and UK, all of which were also targeted by Dyre.

Financial Institution	Country
Al Rayan Bank	UK
Arab Bank	Jordan
CBI	UAE
Commercial Bank of Dubai	UAE
Dubai Islamic Bank	UAE
Emirates NBD Bank	UAE
Invest Bank	UAE
Mashreq Bank	UAE
Noor Bank	UAE
RAK Bank	UAE
United Arab Bank	UAE
United Bank UK	UK

Figure 8: Islamic banking targets

C&C Servers

Over 50% of the C&C addresses being used are owned by two ASNs: OVH (in France and Canada), and JSC in Russia.

C&C Address	Port	Service	Location	ASN Owner
147.135.185.124	449	TCP?	France	OVH SAS
149.56.35.205	443	HTTPS	Canada	OVH SAS
163.53.206.187	443	HTTPS	India	Rainbow Communications
185.208.170.211	443	HTTPS	UK	Hydra Communications Ltd
186.103.161.204	443	HTTPS	Chile	Telefonica Empresas
190.34.158.250	443	HTTPS	Panama	Cable & Wireless Panama
191.7.30.30	443	HTTPS	Brazil	NEMESIS
193.124.117.102	449	TCP?	Russia	JSC Mediasoft
194.87.102.151	445	SMB	Russia	JSC Mediasoft
195.133.144.100	443	HTTPS	Russia	JSC Mediasoft
195.133.48.128	449	TCP?	Russia	JSC Mediasoft
195.62.52.55	443	HTTPS	Russia	IT Expert LLC
37.59.183.143	443	HTTPS	France	OVH SAS
46.160.165.31	443	HTTPS	Russia	UGMK-Telecom LLC
5.196.116.238	443	HTTPS	France	OVH SAS
91.247.37.9	443	HTTPS	Bulgaria	ITL Company
93.95.97.20	449	TCP?	Russia	JSC Mediasoft
93.99.68.140	443	HTTPS	Czech Republic	Liberty Global Operations B.V
95.213.251.135	443	HTTPS	Russia	OOO "Network of data-centers "Selectel"
hxxp://194.87.238.88/response.php			Russia	JSC Mediasoft
hxxp://66.70.172.120/response.php			Canada	OVH SAS

Conclusion

Banking trojan authors rely on social engineering to trick banking customers into opening phishing emails and malicious files, clicking on malicious links in text messages, or clicking on malvertizing ads. Yet, it's still not common practice for banks to provide security awareness training to their customers. This is likely due to legal concerns and the potential flood of costly customer service calls. In reviewing TrickBot's banking targets in this configuration, it's clear that some banks, especially Islamic banks, have overcome the hurdle of offering security advice to customers on their websites. Security professionals within banks who are trying to fight the good fight should use these banks as examples in conversations with their legal teams and continue to push for security awareness training to their customer base. That includes the need for security controls on systems like anti-virus and patching, not just general social engineering or phishing awareness.

Security awareness, however, is a double-edged sword. It's very important to educate the largely uninformed public on modern-day cyber fraud, but studies and real-world experience will both tell you that it's not going to *solve* your problem, it will just help. No matter how much you train users, they will still click on spear-phishing emails. This is where advanced web protection services come in, especially for banks, where specialty services understand the specifics of how each banking strojan works, and offer customized detection and mitigation for customers. The customer's device might be infected, but their session isn't going to get hijacked, and their credentials aren't going to get collected. For financial institutions who don't want to invest in these types of experts in-house, outsourcing these types of services are a good idea.

MD5s Reviewed

- 1c1fb7eda90ac98f97d76c61080783b5
- a2bbe6d113a8c67dede3b2aa91fe173a
- 8a86bec792b5341347bb6a63f4ffc9b9

Appendix A: All Businesses Targeted by v24

Financial Institution	URL Count	Country
Credit Suisse	36	Australia, Austria, Bahamas, Brazil, France, Hong Kong, Italy, Luxembourg, Mexico, Monaco, Singapore, Spain, Switzerland, UK, US
Nordea	35	Denmark, Finland, Luxembourg, Norway, Singapore, Sweden, Switzerland
Danske Bank	32	Denmark, Finland, Lithuania, Norway, UK
SEB	18	Finland, Germany, Norway, Sweden
Barclays Bank	15	UK, Switzerland
Lloyd's Banking Group PLC	14	UK
HSBC Bank	13	Hong Kong, Singapore, UK
The Co-operative Bank	10	UK
Ulster Bank	10	Ireland, UK
NatWest	9	UK
Royal Bank of Scotland	9	UK
Bank of Scotland	8	UK
OP	8	Finland
Resurs Bank	8	Sweden
Santander Bank	8	UK

Citibank	6	EU, Singapore
J.P.Morgan	6	UK, US
Swedbank	6	Latvia
Isle of Man Bank	5	UK
Skandiabanken	5	Norway
Allied Irish Banks	4	Ireland
Bank of Ireland	4	Ireland
Banque Cantonale Vaudoise	4	Switzerland
Carnegie	4	Sweden
Coutts	4	UK
DBS Bank	4	Singapore
Deutsche Bank	4	Germany
ICICI Bank	4	India, UK
Investec	4	South Africa, UK
Marginalen Bank	4	Sweden
Metro Bank	4	UK
Nedbank	4	UK
OCBC Bank	4	Singapore
Paragon Bank	4	UK, US
Royal Bank of Canada	4	Canada, US
Standard Chartered	4	Singapore
TSB Bank	4	UK
United Overseas Bank	4	Singapore
Aktia Bank	3	Finland
Banco Pastor	3	Spain
Bank Cler	3	Switzerland
Bank Norweigian	3	Norway
CardOneBanking	3	UK
Scotiabank	3	Canada
State Street	3	US
The Bank of East Asia	3	UK
Triodos Bank	3	UK
Volvofinans Bank	3	Sweden
Abu Dhabi Commercial Bank	2	UAE
Abu Dhabi Islamic Bank	2	UAE
Adam and Company	2	UK
Airdrie Savings Bank	2	UK
AJ Bell	2	UK
Al Rayan Bank	2	UK

Aldermore Bank	2	UK
Amfa Bank	2	Sweden
Andbank	2	Andorra
ANZ	2	Australia
Arab Bank	2	Jordan
Arbuthnot Latham	2	UK
Baloise Bank	2	Switzerland
Baltic International Bank	2	Latvia
Banca March	2	Spain
Banco Mediolanum	2	Spain
Bank of Cyprus	2	UK
Bankia	2	Spain
Banque Nationale du Canada	2	Canada
Berner Kantonalbank	2	Switzerland
BHF-Bank	2	Switzerland
Blue Orange Bank	2	Latvia
BNP Paribas	2	France
*REDACTED	2	UK
Buckinghamshore Building Society	2	UK
Butterfield Bank	2	UK
C. Hoare & Co	2	UK
Cambridge and Counties Bank	2	UK
Cashplus	2	UK
Catella	2	Sweden
Cater Allen	2	UK
CBI	2	UAE
Cembra	2	Switzerland
Cetelem	2	Spain
Chorley Building Society	2	UK
CIMB Bank	2	Singapore
Close Brothers Asset Management	2	UK
Clydesdale Bank	2	UK
Commercial Bank of Dubai	2	UAE
Coventry Building Society	2	UK
Cumberland Building Society	2	UK
DNB Bank	2	Sweden
Dubai Islamic Bank	2	UAE
Duncan Lawrie	2	UK

EBS	2	Ireland
Ekobanken	2	Sweden
Emirates NBD Bank	2	UAE
Erik Penser Bank	2	Sweden
EVRY	2	Norway
First Direct	2	UK
First International Bank of Israel	2	Israel
First Trust Bank	2	UK
Folksam	2	Sweden
Forex Bank	2	Sweden
GE Artesia Bank	2	Netherlands
GE Capital	2	US
Gerrard Investment Management	2	UK
GT Bank	2	UK
Halifax	2	UK
Hampshire Trust Bank	2	UK
Hargreaves & Lansdown	2	UK
ING	2	Netherlands
Invest Bank	2	UAE
Ireland Bank	2	Ireland
Julius Baer	2	Switzerland
Kaupthing Bank	2	Iceland
Kleinworth Benson	2	UK
Luzerner Kantonalbank	2	Switzerland
Mashreq Bank	2	UAE
Max Matthiessen	2	Sweden
Maybank	2	Singapore
Medicinos Bankas	2	Lithuania
Merrill Lynch	2	US
National Bank of Abu Dhabi	2	UAE
NBAD	2	UAE
Netfonds Bank	2	Norway
Nettkonto	2	Norway
Neue Aargauer Bank	2	Switzerland
Neue Helvetische Bank	2	Switzerland
Newbury Building Socety	2	UK
Noor Bank	2	UAE
Northrim Bank	2	US
Norvik Banka	2	Latvia

Open24	2	Ireland
POP Pankki	2	Finland
PostFinance	2	Switzerland
Raiffeisen	2	Switzerland
RAK Bank	2	UAE
Rathbone Brothers	2	UK
RCI Bank	2	UK
Re:member	2	Norway
Reliance Bank	2	UK
Reynolds & Reynolds	2	US
Saastopankki	2	Finland
Salesforce	2	US
S-Bank	2	Finland
Secure Trust Bank	2	UK
Shawbrook Bank	2	UK
Silicon Valley Bank	2	US
Societe Generale	2	France
Sparebanken Møre	2	Norway
St. James's Place Bank	2	UK
Standard Bank	2	UK
Standard Life Savings Limited	2	UK
State Bank of India	2	Singapore
Steinbach Credit Union	2	Canada
Storebrand Bank	2	Norway
Tesco Bank	2	UK
The Access Bank	2	UK
Tilney	2	UK
Toronto-Dominion Bank	2	UK
Turkish Bank	2	UK
UBS	2	Switzerland
UniCredit Bulbank	2	Bulgaria
United Arab Bank	2	UAE
United Bank UK	2	UK
Unity Trust Bank	2	UK
US Bank	2	US
Valiant	2	Switzerland
Virgin Money	2	UK
Voya	2	US
Yorkshire Bank	2	UK

Yorkshire Building Society	2	UK
Zenith Bank	2	UK
Zuger Kantonalbank	2	Switzerland
Zurcher Kantonalbank	2	Switzerland
Bank Leumi	1	UK
Bank von Roll	1	Switzerland
Nationwide Building Society	1	UK

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119| 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan:f5j-info@f5.com