Trickbot Expands Global Targets Beyond Banks and Payment Processors to CRMs

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

byline

August 1, 2017

The financial trojan TrickBot has been updating its campaigns and targets since F5 malware researchers started following it in September 2016. This is expected behavior because attackers need to continually update their targets and methods to evade detection. Previously, TrickBot, the successor to Dyre, targeted financial institutions in Europe, Australia, New Zealand, and Canada. TrickBot's May 2017 campaigns targeted banks in the UK, Australia, US, Canada, New Zealand, Ireland, France, Germany, Switzerland, the Netherlands, Bulgaria, India, Singapore, and Hong Kong.

In the 26 TrickBot configurations F5 researchers analyzed that were active in May 2017, targets expanded beyond banks to include two payment processing providers and two Customer Relationship Management (CRM) SaaS providers. The fact that payment processors were targets was a notable change that we also observed in Marcher, an Android banking trojan in March of 2017. It appears now that CRMs are a new target of attackers; is it because of their potential for collecting valuable user data that could enhance phishing campaigns?

What's also notable (and expected) is that all command and control (C&C) servers tied to the most recent campaigns reside within web hosting provider networks and were communicating with their infected hosts over port 443. We know attackers hide their exploits in encrypted traffic; this is just another point of reference to prove it is a consistent and common method being used. Additionally, none of the C&Cs we observed in May 2017 were the same C&Cs we tracked in late 2016.

May 2017 Campaigns

This analysis focuses on the activities of two separate campaigns of different sizes identified in the 26 configurations analyzed, versions "1000018" and "1000019." The smaller campaign detected included 210 URL targets focused on banks in Australia, UK, Canada, New Zealand, Singapore, India, and Ireland, and a payment

processor in the US. The larger campaign detected included 257 URLs for banks in the UK, Australia, US, Canada, Ireland, France, Germany, Switzerland, Hong Kong, the Netherlands, and Bulgaria. The same US payment processor was targeted across both campaigns, however, the CRM targets only appeared in the second campaign.

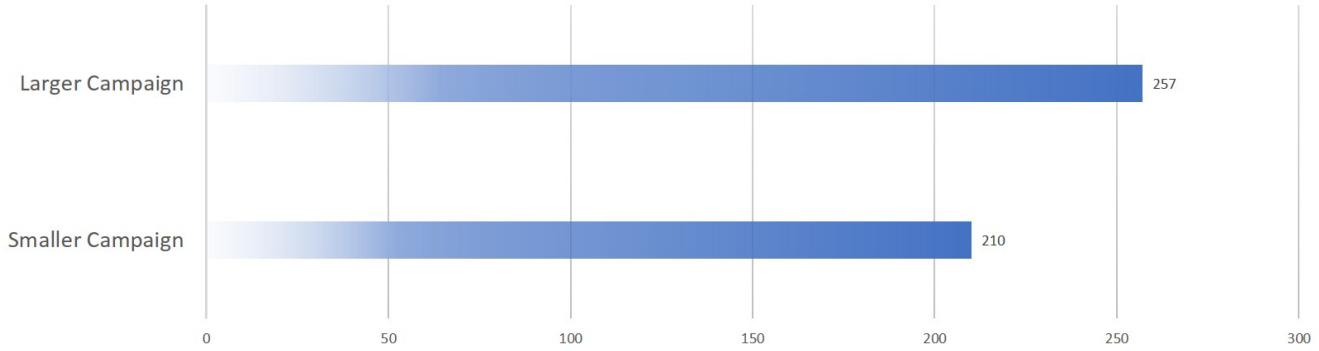

Figure 1: Smaller campaign and larger campaign with count of URL targets

Figure 1: Smaller campaign and larger campaign with count of URL targets

TrickBot May Targets by Industry and Country

When looking at TrickBot's URL targets, we attributed the country target based on the country code in the URL rather than the global headquarters of the targeted business. For instance, https://www.citibank.com.sg is attributed to Singapore, and https://online.citi.eu/GBIPB is attributed to the UK, even though CitiBank is headquartered in the US. (Refer to Appendix A for specific targets by country.)

The smaller campaign focused on targeting banks (83% of URL targets) in Australia, UK, Canada, New Zealand and Singapore, and a payment processor (PayPal) attributed to the US (although PayPal users are global).

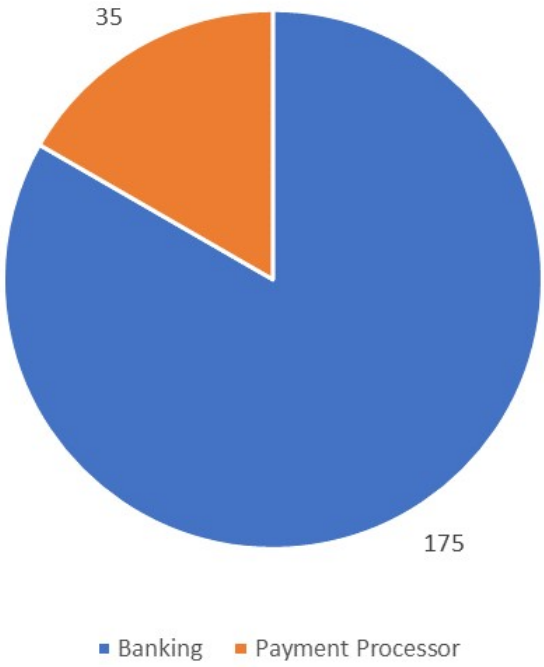

Figure 2: URL targets by industry in the smaller campaign

Figure 2: URL targets by industry in the smaller campaign

The map in Figure 3 shows the number of URLs targeted by country in the smaller campaign. All targets in every country except the US were banks. No US banks were targeted in this campaign, only the payment processor, PayPal. The 35 unique PayPal URLs targeted were the exact same URLs targeted in both campaigns.

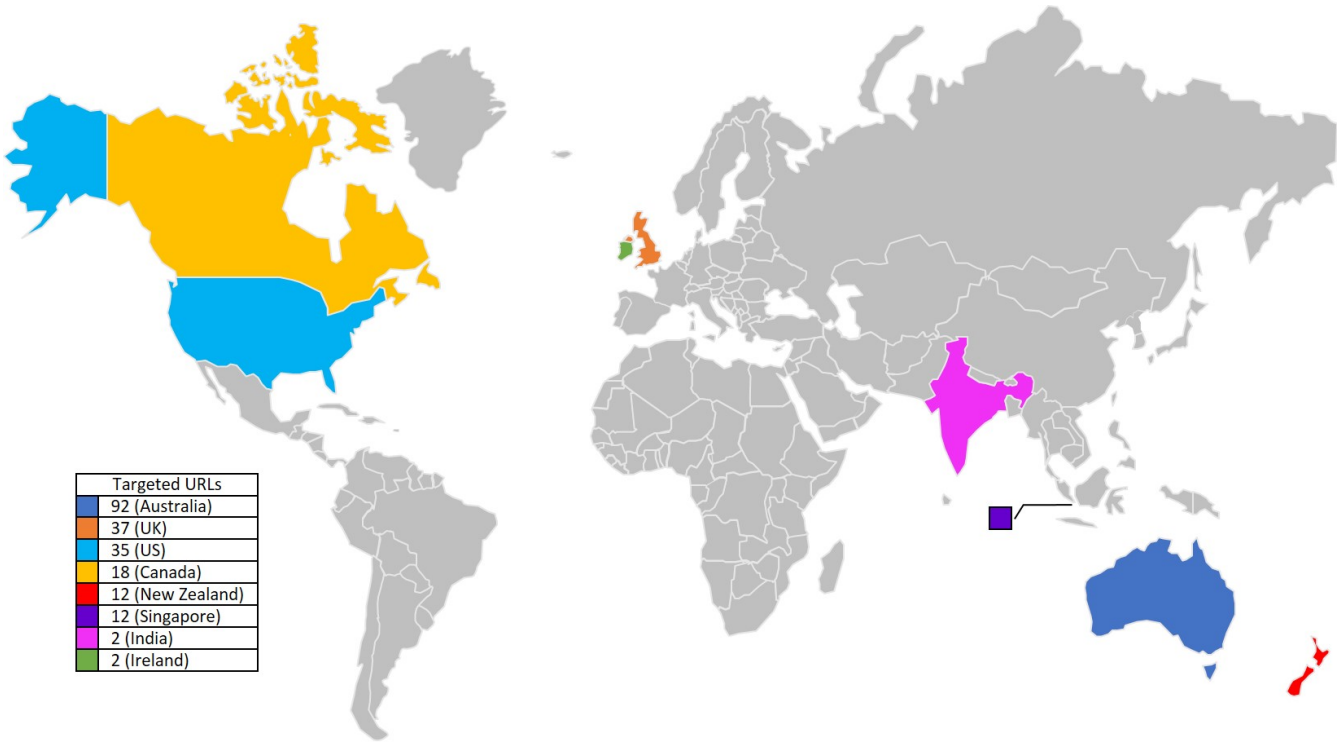

Figure 3: Targeted Countries in the smaller campaign

Figure 3: Targeted Countries in the smaller campaign

Figure 4 shows unique URLs targeted in comparison to unique businesses, because there were often multiple URL targets within one business. (For additional details on the businesses targeted by industry and country, see Appendix A.)

Figure 4 shows unique URLs targeted in comparison to unique businesses, because there were often multiple URL targets within one business. (For additional details on the businesses targeted by industry and country, see Appendix A.)

Smaller Campaign: URL Quantity to Business Entities, by Country		
	URLs	Businesses
Australia	92	32
UK	37	17
US	35	1
Canada	18	5
New Zealand	12	9
Singapore	12	8
India	2	2
Ireland	2	1

Figure 4: Unique URLs to unique businesses in the smaller campaign

The larger campaign expanded its scope of targeted banking URLs and payment processors by adding one new payment processor URL in the UK and introducing CRMs as new targets. The specific CRMs targeted were Salesforce.com and an auto sales CRM developed by Reynolds & Reynolds in the US.

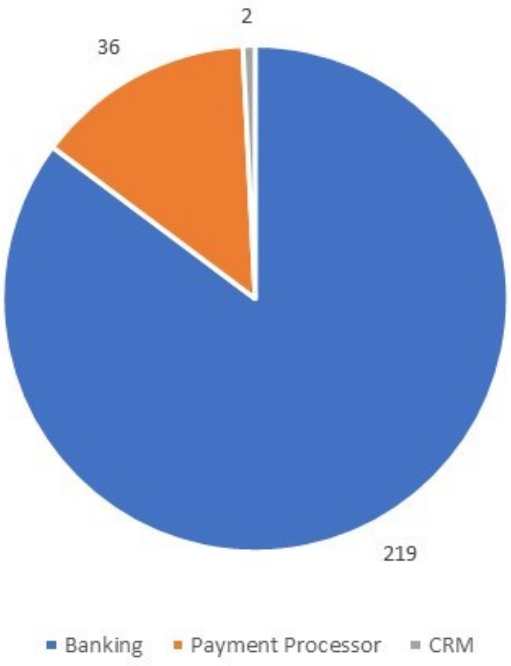

Figure 5: URL targets by industry in the larger campaign

Figure 5: URL targets by industry in the larger campaign

The larger campaign was mainly focused on banks in the UK (47% of targets, up from 18% in the smaller campaign), followed by Australia, then the US. All Australian targets were banks again. PayPal was the leading US target (exactly the same PayPal URLs in both campaigns), followed by 9 other US banks that were not targeted in the smaller campaign, and with the addition of new CRM providers. Additional European companies were targeted in the larger campaign, including banks in France, Germany, Switzerland, the Netherlands, and Bulgaria. A bank in Hong Kong was the new Asia target in this campaign, however, the banking targets in Singapore and India from the smaller campaign were not included.

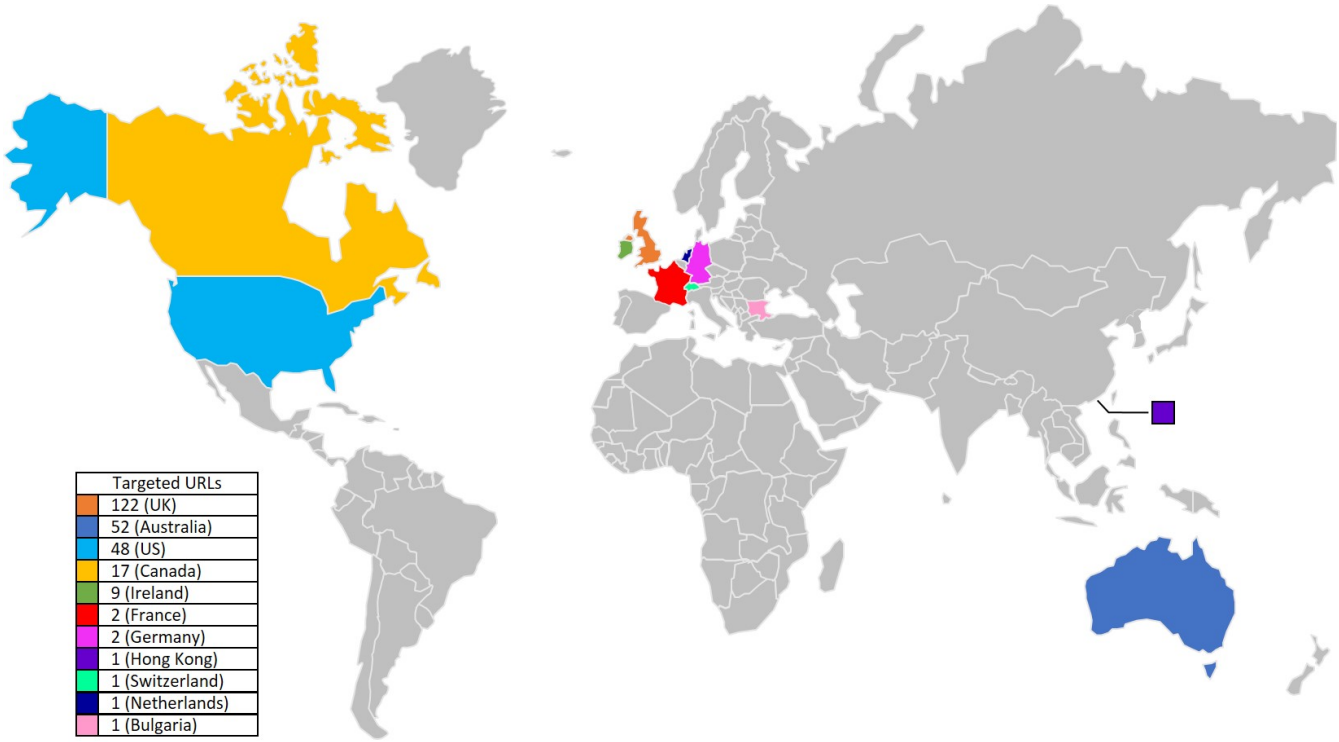

Figure 6: Targeted countries in the larger campaign

Figure 6: Targeted countries in the larger campaign

The chart below shows the same data as that shown in Figure 4 for the larger campaign. (For details, see Appendix A.)

Larger Campaign: URL Quantity to Business Entities, by Country		
	URLs	**Businesses**
UK	122	74
Australia	52	8
US	48	13
Canada	17	6
Ireland	9	6
France	2	2
Germany	2	1
Switzerland	2	2
Hong Kong	1	1
Netherlands	1	1
Bulgaria	1	1

Figure 7: Unique URLs to unique businesses in the larger campaign

C&C Servers in Europe

When analyzing the two campaigns, six C&C IP addresses were identified, all of which exist within European web hosting provider networks. As shown in the table below, three of the six are operated by hosting firms in Asia that use these European web hosting companies' services. All of them used port 443 / HTTPS as a connection method from the infected machine back to the C&C host, a method commonly used by malware authors to evade detection from network security devices that don't inspect encrypted traffic.

C&C IP Address	Network Name	ASN	Country	Industry	Hosting Customer	City	Country
149.202.30.126	OVH	AS16276	France	Web Hosting Provider	MAXSERVER CO.	Hanoi	Vietnam
151.80.84.1	OVH	AS16276	France	Web Hosting Provider	Premium Cheap Hosting	Bandung	Indonesia
195.133.196.129	RUCLOUD	AS48347	Russia	Web Hosting Provider	JSC Mediasoft ekspert	Moscow	Russia
37.1.205.43	INFERNO-NL-DE	AS50673	Netherlands	Web Hosting Provider	3NT Hosting Network	London	UK
88.99.246.23	Hetzner Online GmbH	AS24940	Germany	Web Hosting Provider	MAXSERVER CO.	Hanoi	Vietnam
91.247.36.15	FRIENDHOSTING	AS59729	Bulgaria	Web Hosting Provider	—	—	—

Samples Analyzed

The following MD5 samples, active in May 2017, were analyzed for this report:

- a21c6369738446afa16bf5e70da6ccfa
- 8bf6ee81794c965f38484c0570718971
- b4195cf20d59be307a4d7125d51150b7
- ad8783a32b43f8fa50c5279b712255dc
- 143b01d3edc77ed82c5e5a4ae4d92b5a
- 5376a68fe2e9899515b4ea0e531f4d4d
- 645a229bfa994e79286537ea8f0c9381
- 7a3ecbf2fefa5c329d9d659cbbf7a58d
- d4a2a049fe6c23cb1a2e19f804eb4ba8
- 2073224eda2e5e6bd9e782d6be4d28cb
- 830ebf2cefb1f6bad8587978b252d0b7
- 45160aa23d640f8d1bcb263c179f84f9
- 9d166a822439a47eb2dfad1aeb823638
- a9bdbd097b9757c23d5600ecfb0e8b45
- ddf408ce7c4b5df1a57a3ca45197f18e
- d5aa87b9f44575c00d6bc803ac31f18b
- 8cb0af444e90da3b0d9de00e7db0f4f7
- fe2d9595a96046e441e43f72deac8cb0
- 14ffdcecdd3c6056460cc622fef3b061
- 1082f5c74019f2122bade2dac71f693f

- 5a137c1dd4a55c06531bdbfeaf15c894
- 18056207edc1a3384c2c84531fa2817c
- 1d004f708748b4ce5aa095fd5a42e0ce
- eb7d15c945324529e28e72ad76f387a4
- 3ec07fee718360ad1f1a450f7aaa19db
- 1d3a3922bdcea3a6bca3c8b2f4b40e48

Conclusion

It seems the success of TrickBot thus far has influenced the authors to not only repeat their previous target list of banks from previous campaigns but to expand those targets to include new banks globally as well as CRM providers. The fact that C&C servers in these two most recent campaigns reside within web hosting companies is also significant, along with the fact that the C&C servers were different from those used in previous campaigns. Given the changes we've witnessed with each successive campaign, F5 Labs researchers expect to see further evolution in both the targets and methods used by TrickBot authors, and we will continue to monitor and report on this evolving threat. TrickBot's consistent initial attack pattern is to use email spam campaigns, so users are advised not to open suspicious files received by email.

Appendix A

The following list shows the actual banks targeted by country, and the number of unique URLs per bank as an indication of their importance to the malware authors.

Bank (By Country)	URLs Targeted Smaller Campaign	URLs Targeted Larger Campaign
Australia		
Adelaide Bank	1	
AMP Bank	1	
Arab Bank Australia	1	
Australia and New Zealand Banking Group Ltd	8	5
Bank of Melbourne	4	3
Bank of Queensland	2	
Bank of South Australia	4	3
Bank of Sydney	1	
Bankwest	1	
Bendigo Bank	1	
Beyond Bank	1	
Commonwealth Bank of Australia	13	12
Credit Union Australia	1	
Defence Bank	1	
Greater Bank	1	
HSBC Bank	1	

Hume Bank	1	
IMB Bank	1	
Macquarie	2	
Members Equity Bank	1	
MyState Bank	1	
National Australia Bank Limited	6	3
Newcastle Permanent	1	
QT Mutual Bank	1	
Rabobank	2	
Rural Bank	1	
St. George Bank	4	3
State Bank of India (AU site)	1	
Suncorp Metway Limited	10	9
Teachers Mutual Bank	1	
TSWG	1	
Westpac Banking Corporation	16	14
Bulgaria		
UniCredit Bulbank		1
Canada		
Bank of Montreal	7	6
Banque Nationale du Canada		1
Canadian Imperial Bank of Commerce	1	
Peace Hills Trust		1
Royal Bank of Canada	4	4
Scotiabank	2	1
TD Canada Trust	4	3
France		
BNP Paribas		1
Societe Generale		1
Germany		
Deutsche Bank		2
Hong Kong		
HSBC Bank		1

India		
ICICI Bank	1	
State Bank of India	1	
Ireland		
Allied Irish Banks		2
Bank of Ireland		2
EBS		1
Ireland Bank		1
Open24		1
Ulster Bank	2	2
Netherlands		
ING		1
New Zealand		
ASB Bank	1	
Australia and New Zealand Banking Group Ltd	2	
Bank of New Zealand	1	
Heartland Bank	1	
HSBC Bank	1	
Kiwi Bank	1	
Rabobank	2	
SBS Bank	1	
Westpac Banking Corporation	2	
Singapore		
CIMB Bank	1	
Citibank	2	
DBS Bank	2	
HSBC Bank	1	
Maybank	1	
OCBC Bank	2	
Standard Chartered	1	
United Overseas Bank	2	
Switzerland		

Julius Baer		1
UBS		1
UK		
Adam and Company		1
Airdrie Savings Bank		1
AJ Bell		1
Al Rayan Bank		1
Aldermore Bank		1
Arbuthnot Latham		1
Bank Leumi	1	1
Bank of Cyprus		1
Bank of Scotland	3	4
Barclays Bank	3	7
Buckinghamshire Building Society		1
Butterfield Bank		1
C. Hoare & Co		1
Cambridge and Counties Bank		1
CardOne Banking		2
Cashplus		1
Cater Allen		1
Chorley Building Society		1
Citibank		1
Close Brothers Asset Management		1
Clydesdale Bank		1
Coutts	1	2
Coventry Building Society		1
Cumberland Building Society		1
Danske Bank		2
Duncan Lawrie		1
First Direct		1
First Trust Bank		1
Gerrard Investment Management		1
GT Bank		1

Halifax		1
Hampshire Trust Bank		1
Hargreaves & Lansdown		1
HSBC Bank	1	5
ICICI Bank		1
Investec		2
Isle of Man Bank	2	3
J.P. Morgan		1
Kleinworth Benson		1
Lloyd's Banking Group PLC	5	8
Metro Bank	2	2
National Westminster Bank	5	6
Nationwide Building Society	1	1
NatWest	1	1
Nedbank		2
Newbury Building Socety		1
Paragon Bank		1
Rathbone Brothers		1
RCI Bank		1
Reliance Bank		1
Royal Bank of Scotland	3	10
Santander Bank	1	4
Secure Trust Bank		1
Shawbrook Bank		1
St. James's Place Bank		1
Standard Bank		1
Standard Chartered	1	
Standard Life Savings Limited		1
Tesco Bank		1
The Access Bank		1
The Bank of East Asia		1
The Co-operative Bank	2	5
Tilney		1

Toronto-Dominion Bank		1
Triodos Bank		2
TSB Bank	2	2
Turkish Bank		1
Ulster Bank	3	3
United Bank UK		1
Unity Trust Bank		1
Virgin Money		1
Yorkshire Bank		1
Yorkshire Building Society		1
Zenith Bank		1
US		
GE Capital		1
J.P. Morgan		2
Merrill Lynch		1
Northrim Bank		1
Paragon Bank		1
Royal Bank of Canada		1
Silicon Valley Bank		1
State Street		2
US Bank		1
Voya Financial		1

Payment Processor Targets by Country

Payment Processors (By Country)	URLs Targeted Smaller Campaign	URLs Targeted Larger Campaign
UK		
[Redacted]		1
US		
PayPal	35	35

CRM Targets by Country

CRMs (By Country)	URLs Targeted Smaller Campaign	URLs Targeted Larger Campaign
US		

Salesforce (login page)		1
Reynolds & Reynolds (login page)		1