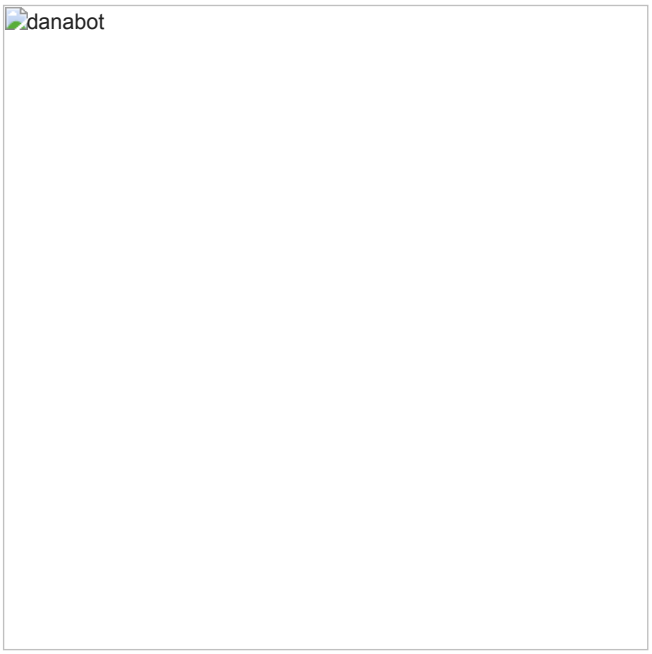
Danabot's Travels, A Global Perspective

asert.arbornetworks.com/danabots-travels-a-global-perspective/

- Banker
- Credtheft
- danabot
- Infostealer



Executive Summary

First discovered in May of 2018, Danabot is a Delphi written banking trojan that has been under active development throughout the year. This malware's early success can be attributed to its modular structure and mature distribution system. Throughout the year, NETSCOUT Threat Intelligence has observed the growth in distribution and global coverage of Danabot.

NOTE: *NetScout AED/APS enterprise security products detect, and block activity related to Danabot using our ATLAS Intelligence Feed (AIF).*

Key Findings

- Danabot is an actively supported banking trojan **steadily approaching the sophistication of mature crimeware** families such as Dridex and Trickbot.
- Danabot leverages a centralized command and control infrastructure that **allows third party actors as affiliates**. This is a proven model that we have seen work well with other banking trojans like the mature families noted previously.
- Danabot's affiliate program has **gradually expanded to target numerous geographical regions** including: Australia, Austria, Canada, Germany, Italy, Poland and the United States.

Overview of Danabot

Danabot is a modular banking trojan that utilizes several DLL files to aid in credential theft using various mechanisms, most notably web injects. In addition to credential theft and information stealing operations, Danabot supports remote access from an infected system to malicious actors through the VNC and RDP modules distributed from the command and control server. Danabot is typically distributed by spam email through malicious documents or Hancitor malware. Once the initial Danabot payload (loader) is executed it will reach out to the C2 to download additional DLL modules which can perform credential theft or remote access tasks.

Command and Control Centralization

Danabot uses a centralized command and control (C2) infrastructure which appears to be copied across various servers. All malware samples connect to the same set of C2 IP addresses which are presumably managed by one entity as opposed to each Danabot actor managing their own C2 infrastructure. We observed this centralization becoming a trend among mature information stealing and banking type malware families. When an infected machine connected to the Danabot C2 it provides information about its affiliate ID allowing the C2 to provide the machine the correct payloads, configuration files, and web injects. Samples with the same affiliate ID can have different hardcoded C2 IPs, however in our observations each affiliate ID will get the same data despite which C2 it connects to. This means that the data for each affiliate ID is hosted on every Danabot C2 server. Our research identified the same webinject targets and configuration files being used for multiple affiliate IDs. This overlap suggests the affiliates of Danabot may be separate third-party entities who may have the same targets.

New Affiliate IDs

As of December 14th, we identified 12 different affiliate IDs targeting various regions and sectors globally. This included 3 additional affiliates (10, 14, 15) added since the last public reporting in September by Proofpoint. The following sections break down these affiliate IDs into clusters to showcase regional targeting. **Appendix A** represents the primary websites targeted by Danabot.

Affiliate 10

Although we observed numerous malware samples coded with the affiliate ID "10", we have been unable to recover live C2 communications to retrieve infects and confirmation files. This could mean the affiliate ID is no longer being serviced by the Danabot operators.

Affiliate 14

Affiliate ID "14" first surfaced in early November and we observed it in more than 50 malware samples. The C2 communication for this affiliate ID contained the following configuration, consistent with other campaigns we are tracking:

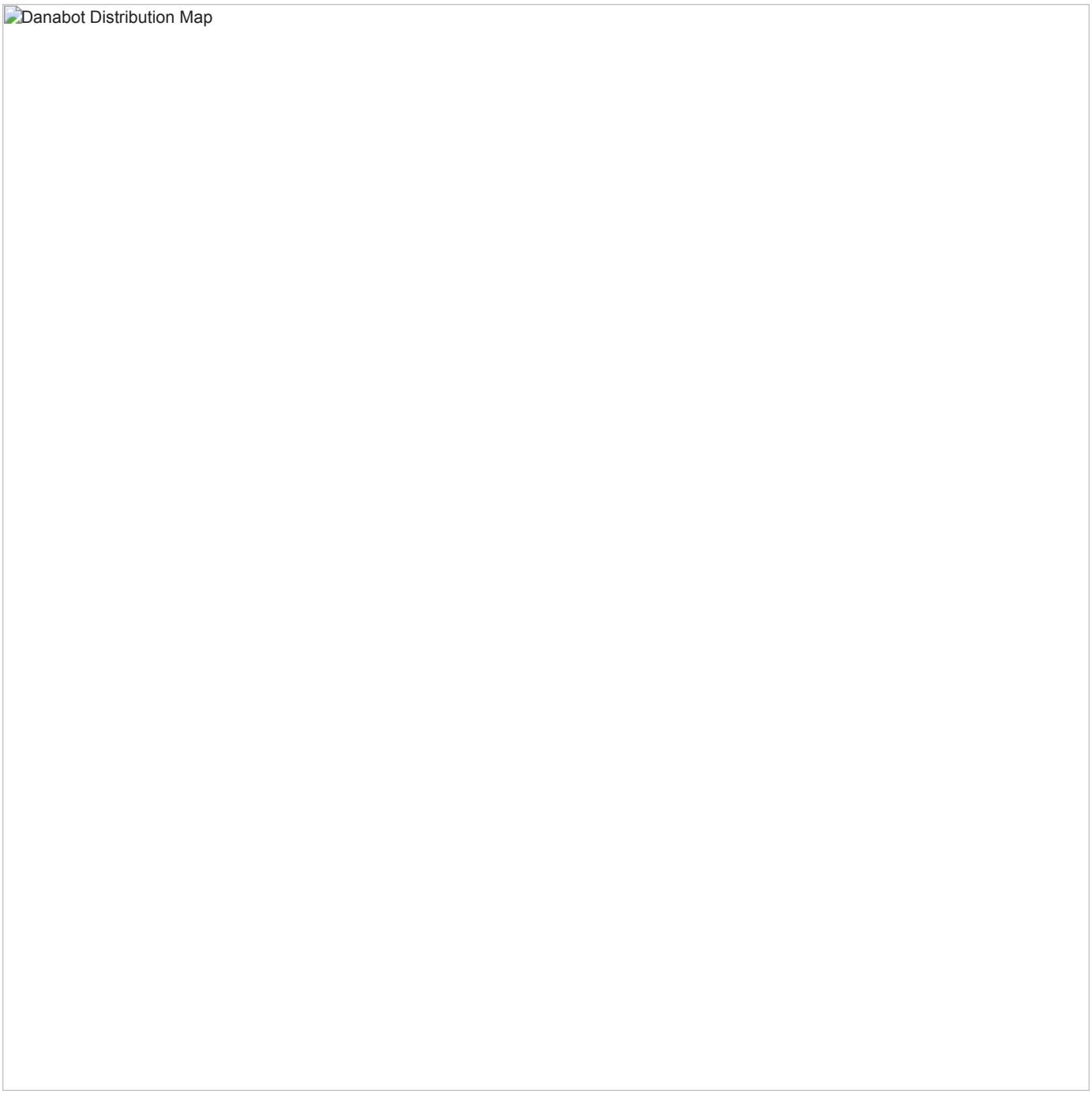
- BitVideo
- KeyBit
- PostWFilter
- BitFilesZ

No webinjects were captured during our observations of affiliate ID "14" traffic. However, the configuration files offer the capability to steal cryptocurrency wallets, files, and account credentials.

Affiliate 15

Affiliate ID "15" started appearing in late November and is the most recent affiliate discovered. We managed to collect configuration files and webinjects from the C2 servers. These files and infects contained different names compared to those of previous affiliate IDs. The injects retrieved primarily targeted Polish banking institutions, but also one U.S. financial organization.

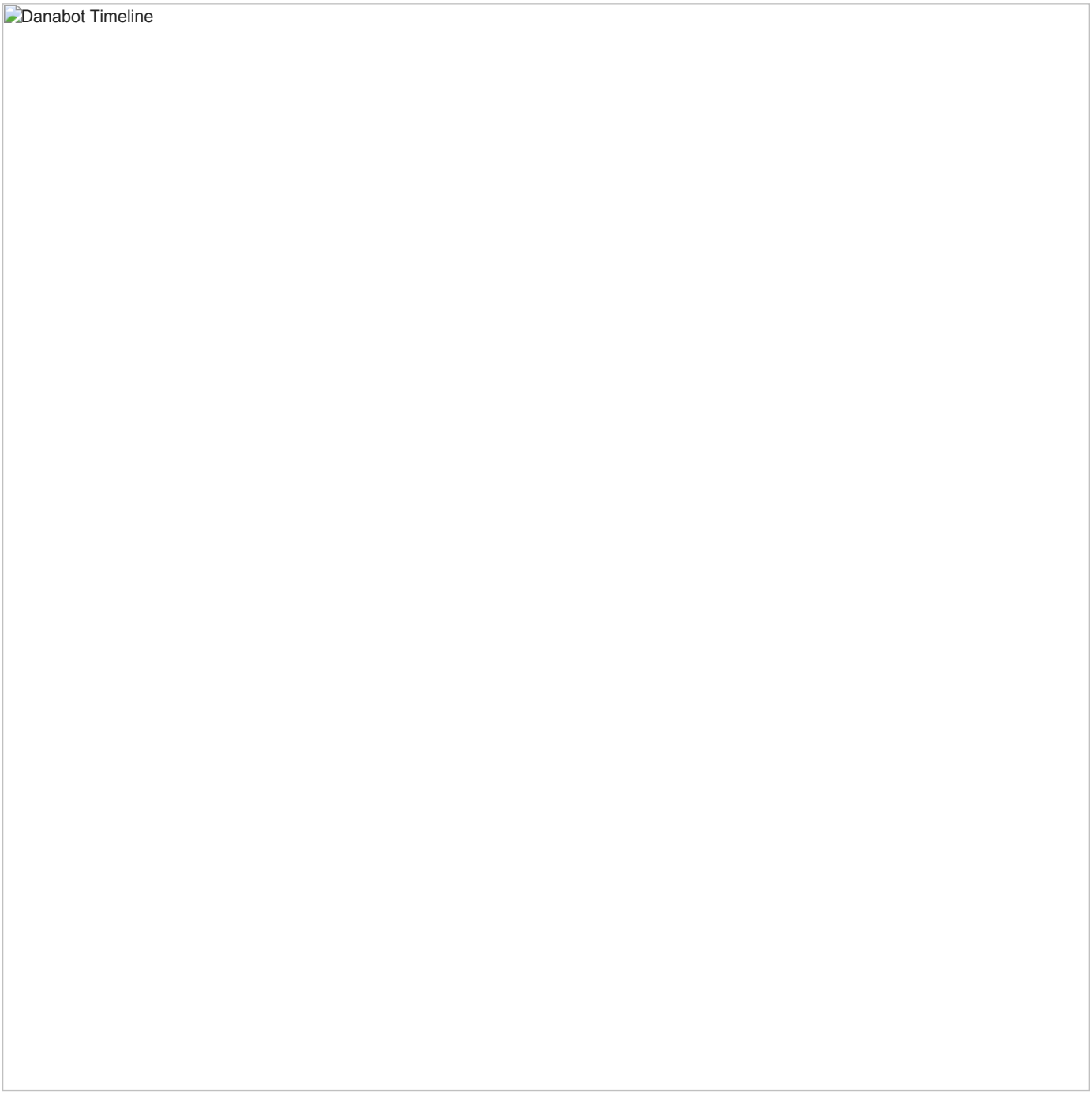
Current Affiliate ID Distribution by Region



Affiliate ID	Targeted Countries	First Seen
3	AustriaItaly	September 06, 2018
4	Australia	September 24, 2018
5	None	September 18, 2018
8	CanadaUnited States	September 11, 2018
9	AustriaGermanyItalyPolandUnited States	September 15, 2018
10	None	October 29, 2018
11	None	September 26, 2018
12	Australia	September 29, 2018

13	**Germany**	**September 29, 2018**
14	**None**	**November 08, 2018**
15	**PolandUnited States**	**November 21, 2018**
20	**None**	**September 29, 2018**

Affiliate ID Timeline



Conclusion

Danabot is an active banking trojan that has adopted a centralized command and control infrastructure to provide its services for third party actors. We continue to see this malware operation expanding its global coverage around the globe. Based on the overlap in targeting between various affiliate IDs, Danabot appears to have multiple third parties using their platform. The modular nature of Danabot, the

centralized infrastructure, and increasing number of affiliate IDs suggest this operation is streamlined, well-managed, and likely to grow beyond the seven countries currently impacted.

Appendix A: Domains/URLs Targeted by Danabot

This is a list of URLs observed in captured web injects and configuration files

- .it
  - unicredit.it
  - bancagenerali.it
  - banking4you.it
  - credit-agricole.it
  - unipolbanca.it
  - credem.it
  - inbank.it
  - relaxbanking.it
  - Tim.it
  - credem.it
  - bancaeuro.it
- .pl
  - ingbank.pl
  - neobank24.pl
  - centrum24.pl
  - ingbusinessonline.pl
  - aliorbank.pl
  - ideabank.pl
  - pocztowy24biznes.pl
  - bosbank24.pl
  - credit-agricole.pl
  - sgcib.pl
  - cui.pl
  - bgzbnpparibas.pl
  - ipko.pl
  - ebusinessbank.db-pbc.pl
  - e25.pl
  - e-skok.pl
  - t-mobilebankowe.pl
- .at
  - sparkasse.at
  - raiffeisen.at
- .com/.net
  - raiffeisenpolbank.com
  - chebanca.net
  - Intesasanpaolo.com
  - bittrex.com
  - bitbay.net
  - poloniex.com
  - citidirect.com
  - ubibanca.com
- .au
    commbank.com.au
- .de
  - deutsche-bank.de
  - sparda.de
  - commerzbank.de
  - comdirect.de
  - berliner-bank.de
  - norisbank.de
  - targobank.de
- .ch
    bluewin.ch