Goznym Indictments – action following on from successful Avalanche Operations

shadowserver.org/news/goznym-indictments-action-following-on-from-successful-avalanche-operations/

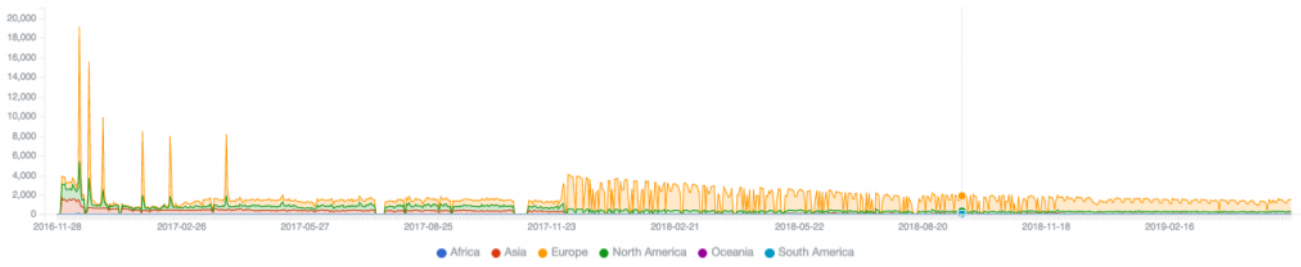
May 16, 2019

We have previously reported on multiple phases of the operations against the Avalanche platform, in late November 2016, 2017 and 2018. To recap: **Avalanche** was a long running criminal malware delivery platform that was used to provide difficult to disrupt, fast flux botnet command and control (C2) capabilities, to over 20 different malware strains. During the past 3 years, the Shadowserver Foundation has been supporting multiple international Law Enforcement Agencies in helping to keep roughly 2 million unique IP addresses of the victims of one or more of these strains protected from cybercrime every day, through court ordered and voluntary sinkholing of malicious C2 domains and victims remediation via our free daily network reporting,

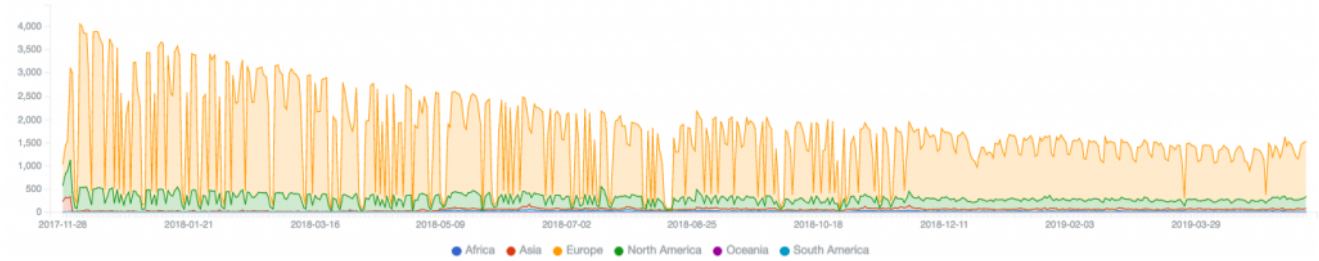
As part of ongoing investigations into the operators and customers of the Avalanche platform, the US Department of Justice (DoJ) and Federal Bureau of Investigations (FBI), together with Europol, Eurojust and many Law Enforcement partners in Germany, Georgia, Ukraine, Moldova and Bulgaria, today announced a significant new case development. The malware known as **Goznym** was one of the malware strains being controlled through the Avalanche platform at the time of the takedown. The Pittsburgh FBI Field Office and LE partners have now reached a point in their investigation into Goznym where they can reveal their work to the world. The Goznym malware and the criminal actors behind it were allegedly responsible for over 41,000 infected computers used in $100 million USD of attempted fraud. So far 10 suspects have been indicted, with 5 arrested internationally and 5 still at large.

You can view a helpful DoJ/Europol infographic explaining the alleged Avalanche Goznym crimes here, as well as a map showing the location of the indicted defendants. The defendants join the FBI's wanted list. You can view the full DoJ indictment here

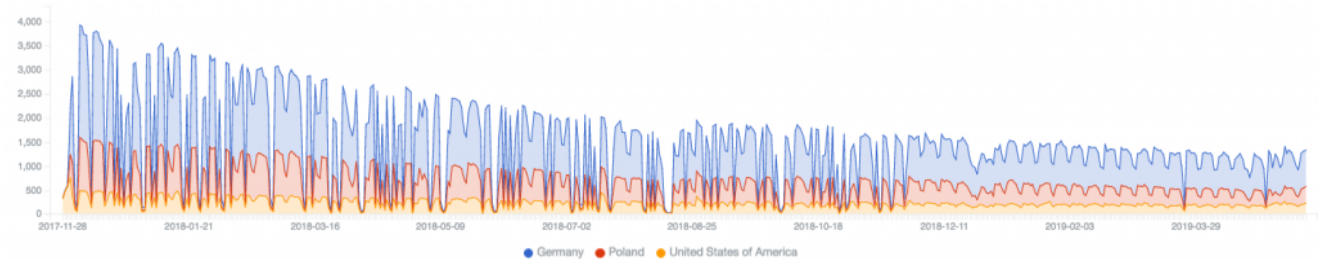
The graph below shows the number of unique IP addresses connecting each day to the Avalanche sinkhole for active Goznym infections:



Seen from year two onwards:

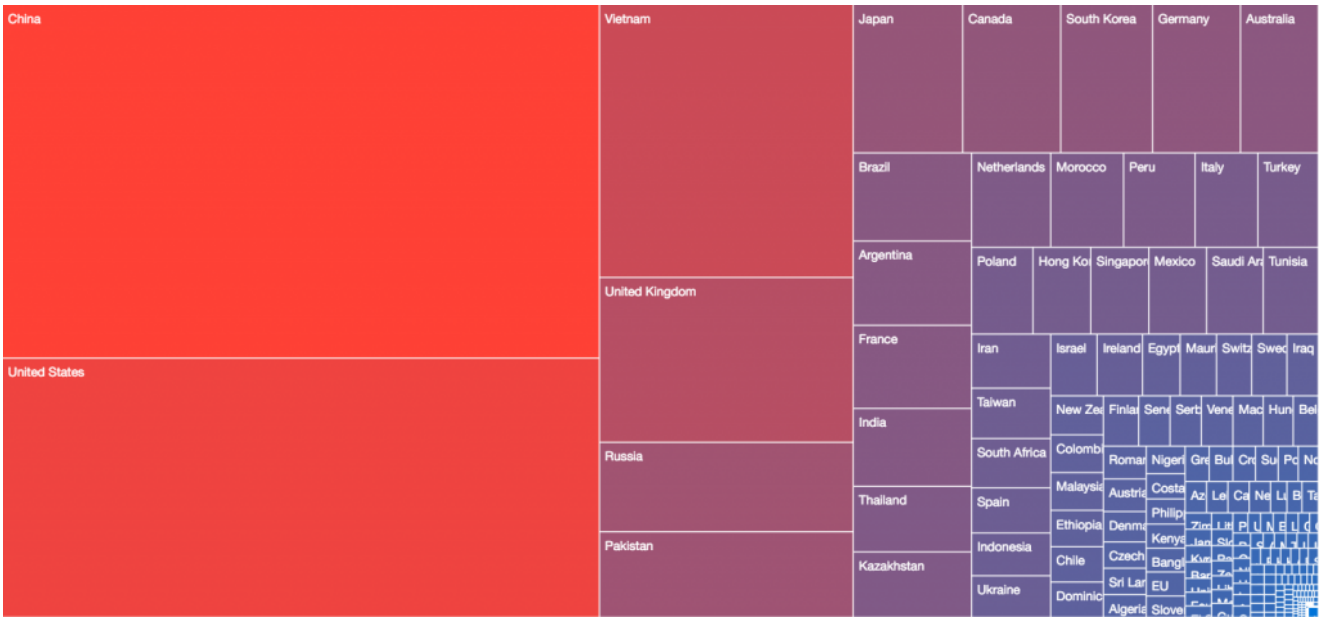


And focusing on the top three countries with victims – Germany, Poland and the United States from year two onwards:

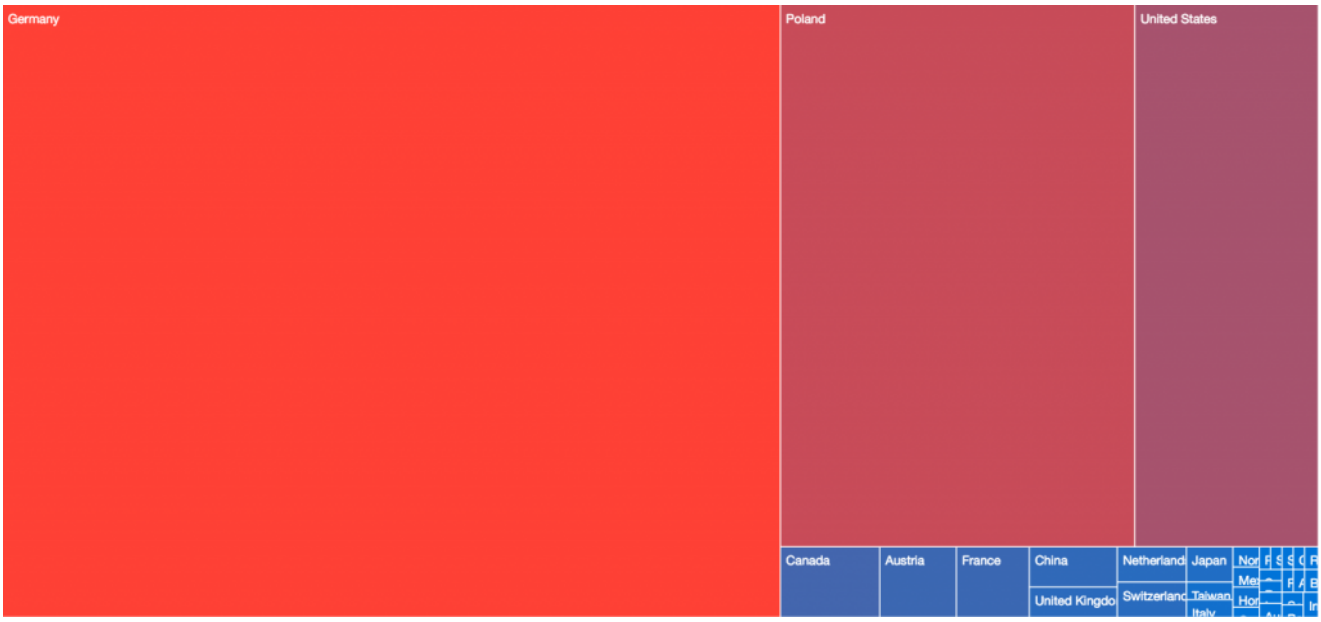


The treemaps below show the relative distributions of victim populations globally on various dates:

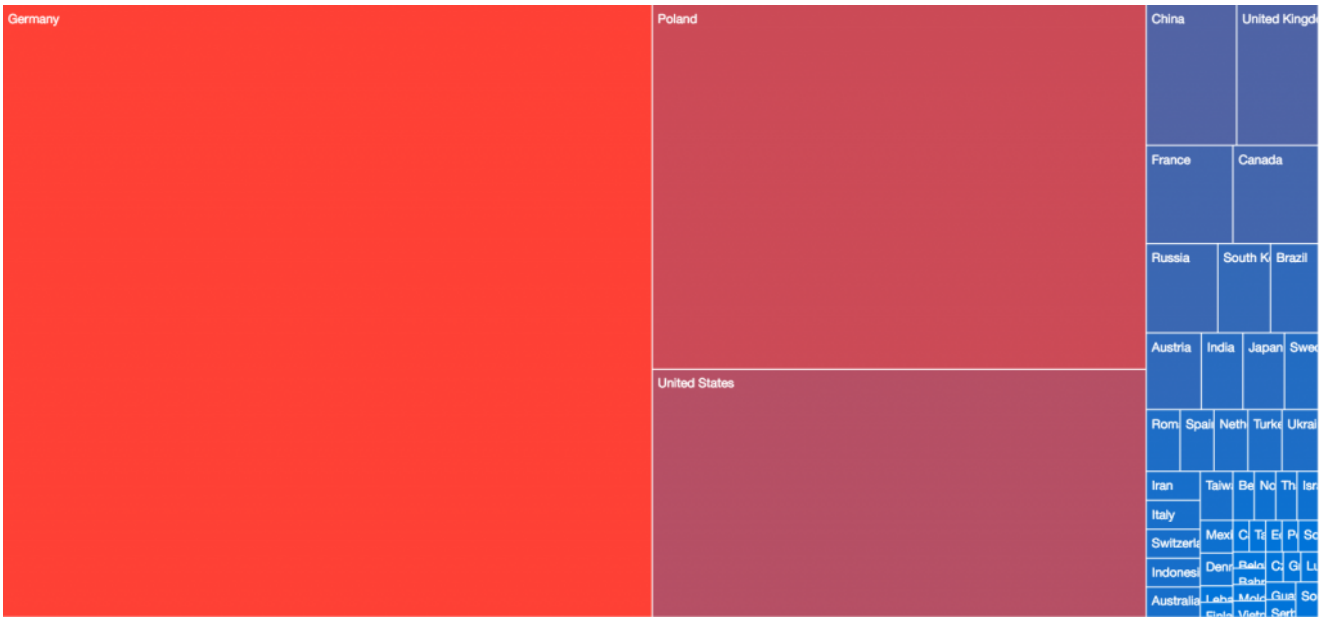
20161131 – Year One, initial operation



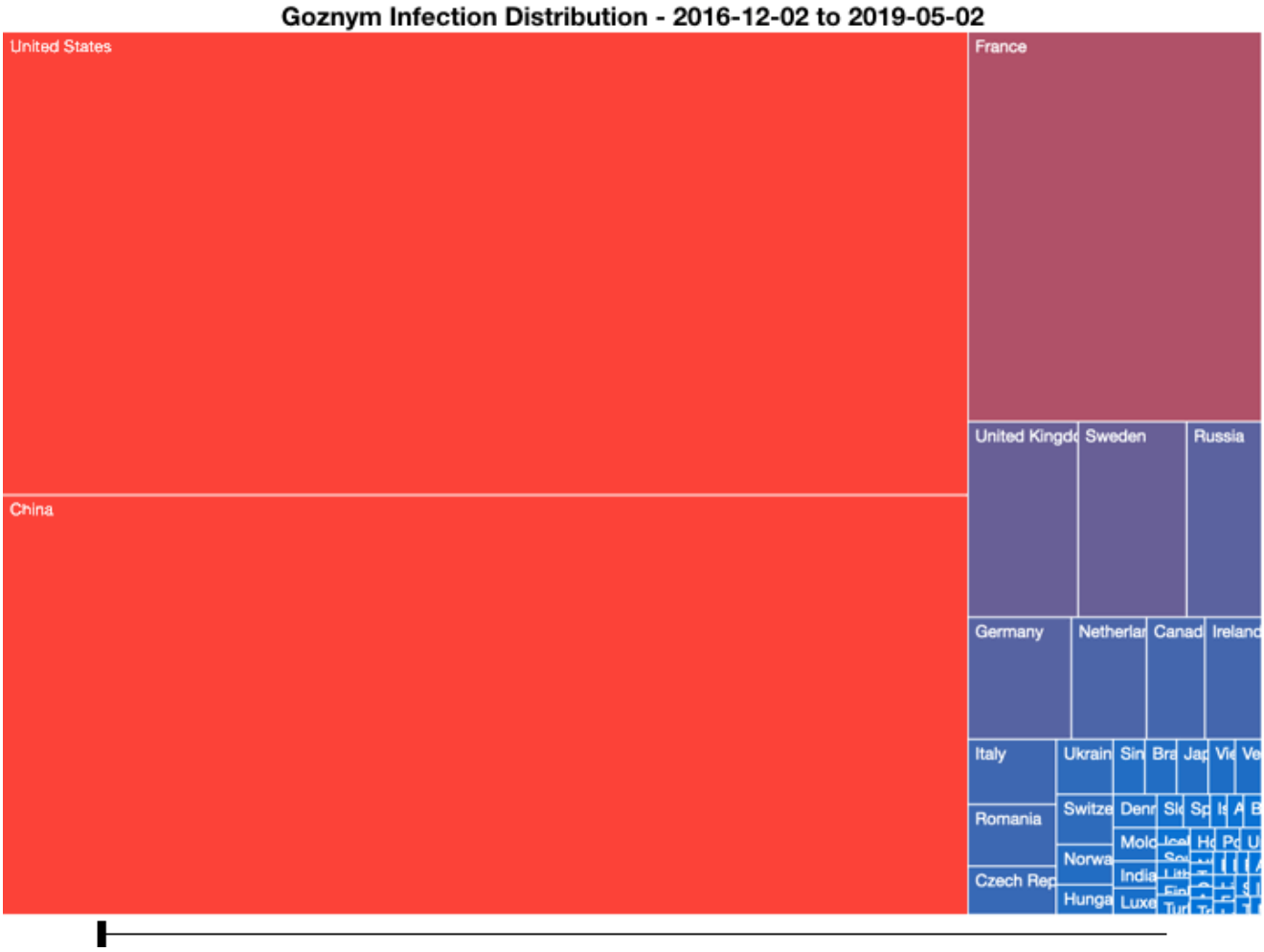
20171201 – Year Two, first anniversary



20190515 – Point of Goznym Indictment



The animation below shows the changing international locations of Goznym victims globally each month since the November 2016 initial Avalanche takedown to the May 2019 US DoJ/FBI indictments:



We often find that major cybercrime investigations require effective collaboration and partnerships on a truly international scale. Whilst the Internet spans international borders as if they were irrelevant, Law Enforcement Agencies still have to work within nation-state legal frameworks. These factors provide considerable logistical and legal challenges. So congratulations to all involved in this case for using all of the available tools to best effect. No one should underestimate the scale of the achievement here.

We can't say it any better than the FBI Pittsburgh Field Office Special Agent in Charge – Robert Jones: "*Successful investigation and prosecution is only possible by sharing intelligence, credit and responsibility. Our adversaries know that we are weakest along the seams and this case is a fantastic example of what we can accomplish collectively.*" We salute the work in this case and we're happy to have been able to support this investigation.

In turn, we would also like to thank all those who support the work of the The Shadowserver Foundation. Your continued support means we can quietly provide Law Enforcement with impartial, free specialist advice and assistance to help them achieve these major successes and reduce the exposure to risk faced by Internet users.

- Botnets
- Bots

- Malware
- Takedowns

« Back to News & Insights