EP 110: Spam Botnets

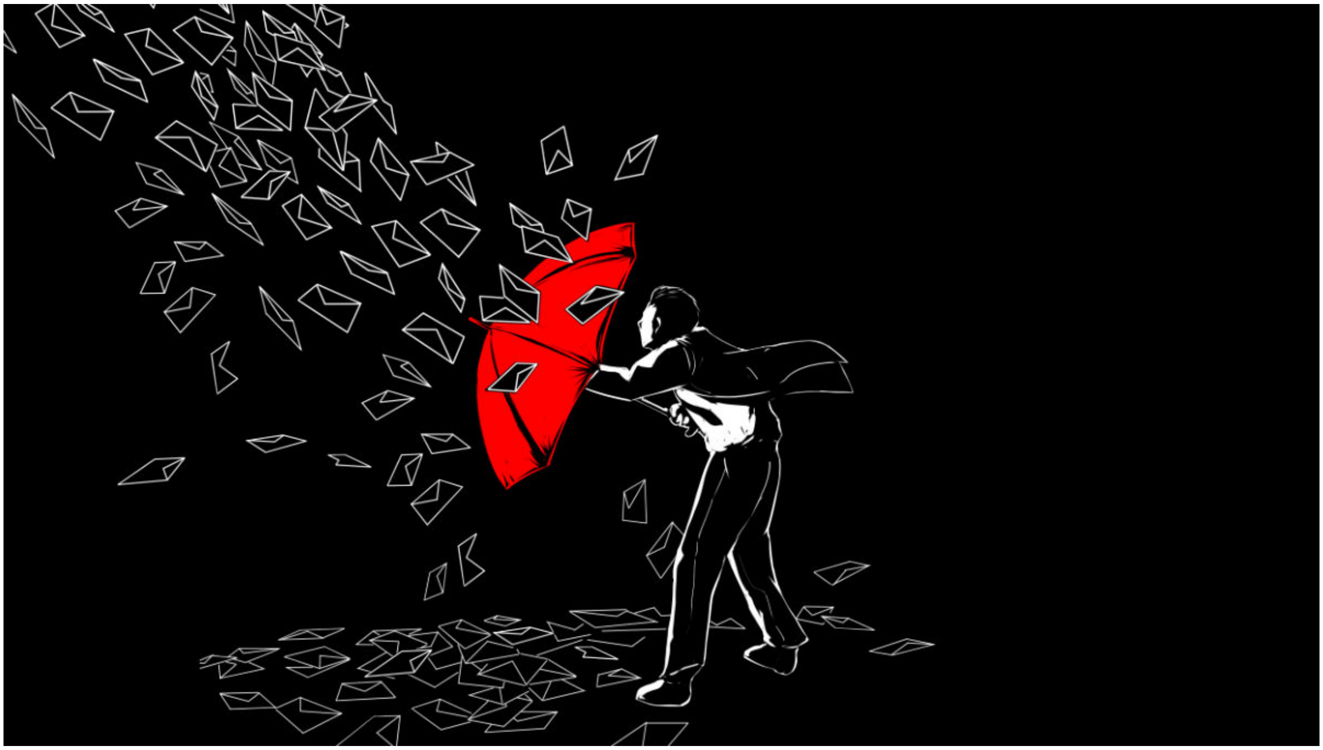
darknetdiaries.com/episode/110/

cybercrime

botnet

08 February 2022 | 69:09

Full Transcript



This episode tells the stories of some of the worlds biggest spamming botnets. We'll talk about the botnets Rustock, Waledac, and Cutwail. We'll discover who was behind them, what their objectives were, and what their fate was.

Sponsors

Support for this show comes from Juniper Networks. Juniper Networks is dedicated to simplifying network operations and driving superior experiences for end users. Visit juniper.net/darknet to learn more about how Juniper Secure Edge can help you keep your remote workforce seamlessly secure wherever they are.

Sources

- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/samosseikovb2009paper.pdf?la=en.pdf?dl=true
- https://cseweb.ucsd.edu/~apitsill/papers/UsenixSec12.pdf
- https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/
- https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/cutwail
- https://krebsonsecurity.com/tag/0bulk-psyche-evolution/
- https://www.researchgate.net/publication/284219242_Master_of_Puppets_Analyzing_And_Attacking_A_Botnet_For_Fun_And_Profit
- https://www.wired.co.uk/article/infoporn-rise-and-fall-of-uks-biggest-spammer
- https://www.trendmicro.co.uk/media/wp/botnet-chronicles-whitepaper-en.pdf
- https://www.nominet.uk/the-cutwail-spam-delivery-service/
- https://krebsonsecurity.com/2012/01/pharma-wars-google-the-cutwail-botmaster/
- https://www.researchgate.net/publication/228415809_The_Underground_Economy_of_Spam_A_Botmaster’s_Perspective_of_Coordinating_Large-Scale_Spam_Campaigns
- https://slate.com/technology/2014/11/spam-nation-meet-the-russian-cybercrooks-behind-the-digital-threats-in-your-inbox.html
- https://www.networkworld.com/article/2260053/experts-link-flood-of–canadian-pharmacy–spam-to-russian-botnet-criminals.html
- https://www.m86security.com/newsimages/trace/m86_labs_report_jan2010.pdf
- https://www.ftc.gov/news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn
- https://www.theregister.com/2011/03/23/rustock_takedown_analysis/
- https://en.wikipedia.org/wiki/Rustock_botnet
- https://www.fireeye.com/blog/threat-research/2010/10/silent-rustock.html
- https://www.wsj.com/articles/BL-DGB-22173
- https://arstechnica.com/information-technology/2011/03/how-operation-b107-decapitated-the-rustock-botnet/
- https://shop.sourcebooks.com/spam-nation.html
- https://phys.org/news/2012-08-usenix.html
- https://www.politico.com/magazine/story/2014/12/pharma-spam-113562
- https://securelist.com/the-botnet-business/36209/
- https://www.wired.com/2006/08/spamking/
- https://www.wuwm.com/post/how-feud-between-two-russian-companies-fueled-spam-nation

- https://www.bloomberg.com/quicktake/drug-prices
- https://www.theatlantic.com/entertainment/archive/2018/03/20-years-of-viagra/556343/#:~:text=Formally%20approved%20by%20the%20Food,aired%20during%20mass%2Dtelevised%20sporting
- http://www0.cs.ucl.ac.uk/staff/g.stringhini/papers/saito_botnet.pdf
- https://www.secureworks.com/research/pushdo
- https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/CUTWAIL
- https://www.techrepublic.com/blog/it-security/pushdo-cutwail-botnet-second-to-none-when-it-comes-to-spamming/
- https://www.darkreading.com/attacks-breaches/which-botnet-is-worst-report-offers-new-perspective-on-spam-growth/d/d-id/1132055?
- https://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/#more-13518
- http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf
- https://www.techrepublic.com/article/spam-nation-cybercrime-and-spam-are-far-bigger-security-threats-than-you-think/
- https://securelist.com/spam-report-june-2011/36375/
- https://www.csoonline.com/article/2123967/botnets–4-reasons-it-s-getting-harder-to-find-and-fight-them.html
- http://www.bbc.co.uk/news/mobile/technology-15776973
- https://www.darkreading.com/risk/inside-one-of-the-worlds-biggest-botnets/d/d-id/1135416
- https://www.darkreading.com/attacks-breaches/major-disruption-of-pushdo-botnet-wasnt-the-original-goal/d/d-id/1134253
- https://www.researchgate.net/publication/224110468_Malware_authors_don’t_learn_and_that’s_good/download
- https://www.secureworks.com/research/waledac-kelihos-botnet-takeover
- https://www.fireeye.com/blog/threat-research/2009/06/killing-the-beast.html
- https://www.fireeye.com/blog/threat-research/2012/07/killing-the-beast-part-5.html
- https://www.wired.com/story/what-is-sinkholing/
- http://news.bbc.co.uk/1/hi/business/6298641.stm
- https://doi.org/10.2147/DHPS.S46232
- https://threatpost.com/waledac-botnet-now-completely-crippled-experts-say-031610/73694/
- https://docs.microsoft.com/en-us/archive/blogs/microsoft_on_the_issues/cracking-down-on-botnets
- https://blogs.microsoft.com/blog/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet/
- https://blogs.microsoft.com/on-the-issues/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet/
- https://www.crn.com/news/security/223100744/microsoft-takes-down-277-waledac-botnet-domains.htm?itc=refresh

- https://www.wsj.com/articles/SB10001424052748704240004575086523786147014
- https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/harvesters-asiaccs2014.pdf
- https://www.fireeye.com/blog/threat-research/2010/08/infiltrating-pushdo-part-2-2.html
- https://www.fireeye.com/blog/threat-research/2010/08/chasing-cncs-part1.html
- https://www.fireeye.com/blog/threat-research/2008/11/rustocks-new-home.html
- https://www.fireeye.com/blog/threat-research/2008/11/mccolo-up-again.html
- https://www.theregister.com/2011/06/27/chronopay_arrests/
- https://krebsonsecurity.com/2013/08/pavel-vrublevsky-sentenced-to-2-5-years/
- https://www.theregister.com/2014/06/04/hacker_hired_to_build_russias_national_payment_system_report/
- https://www.nytimes.com/2010/10/27/business/27spam.html
- https://www.forbes.ru/sp_data/2014/sex_drugs_and_rockn_roll/#gl_1
- https://www.cnews.ru/news/top/spamer_1_schitaetchto_ego_travit
- https://safe.cnews.ru/news/top/russkaya_spamset_glavmed_zarabotala
- https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rx-partners-09192017
- https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/glavmed-09192017
- https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/rx-partners-06082015
- http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened
- https://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html
- https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/
- https://www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime
- https://nabp.pharmacy/wp-content/uploads/2020/05/Rogue-Rx-Activity-Report-May-2020.pdf
- https://www.safemedicines.org/2020/06/nabp-fake-pharmacies-and-covid-19.html

Videos:

- Bringing Down a Spam King: The Rustock Botnet Takedown
- What is a Botnet?
- BlackHat 2011 - Affiliate Programs: Legitimate Business or Fueling Cybercrime ?
- BlackHat 2011 – The Rustock Botnet Takedown, Operation B107
- World Business: Botnets – 01/04/2011
- Taking Down the Waledac Botnet: The Story of Operation b49
- Interpol Operation Pangea 2012 Video Report
- Lab Matters - The State of Spam
- Lab Matters - The Ups and Downs of Mitigating Botnets

- Lab Matters – The threat from P2P botnets
- 24C3 Cybercrime 2.0 [Storm Botnet]
- FDA to CNN Many online pharmacies selling fake medicine
- Fake Prescription Drugs are Dangerous
- Is Your Online Pharmacy Safe
- Cheaper Rx Drugs Are As Close As Canada
- Fake Online Pharmacies for COVID-wild

Attribution

Darknet Diaries is created by Jack Rhysider.

Episode artwork by odibagas.

Audio cleanup by Proximity Sound.

Theme music created by Breakmaster Cylinder. Theme song available for listen and download at bandcamp. Or listen to it on Spotify.

Equipment

Recording equipment used this episode was the Shure SM7B, Zoom Podtrak P4, Sony MDR7506 headphones, and Hindenburg audio editor.

Embed Episode

Add this episode of Darknet Diaries to your own website with the following embed code:

```
<iframe frameborder="0" height="200" scrolling="no"
src="https://playlist.megaphone.fm?e=ADV1493915926" width="100%"></iframe>
```

Transcript

[START OF RECORDING]

JACK: I grew up in the US, close to my grandma. She was old and needed medicine, and often she'd buy her medicine in Mexico. I have many fond memories of taking an all-day road trip to Mexico, getting across the border, trying to find la farmacia, hoping we'd get the right medicine there, figuring out a way to get it back over the border, and then driving home. The thing is, here in the US, medicine is crazy expensive, so making the trip down to Mexico for medicine was worth it to us. [MUSIC] My grandma was just someone looking for deals and trying to save money. But this is a common story I've heard from other people in the US, too. Yeah, it's often illegal to do this, because the US doesn't want people importing drugs that aren't FDA-approved, but still, people do it. But then, another option landed on the table; pharmacies began to appear online. Suddenly, you could order your medicines from your computer and get it delivered right to your front door, and that changed everything.

Read Full Transcript

Previous Episode Next Episode