The Rustock Botnet Takedown: A High-Level Overview

Julia Wolf <julia@fireeye.com>
Alex Lanstein <alex@fireeye.com>

July 12, 2011 (Draft Copy)

Abstract

The Rustock botnet operated for several years sending spam emails, and at several times was the largest spamming botnet on Earth. This paper covers the history of the botnet, and the most recent shutdown of it instigated by researchers (Operation b107). These techniques used could be generalized to the takedown of other botnets.

Introduction

The Rustock botnet has evolved over time, from a fairly simple spambot, into a much more advanced spambot. The most recent versions used several techniques to prevent the [easy] takedown of the botnet's central command and control [C&C] infrastructure (typically a botnet's weakest point), and to allow the botnet operator(s) to recover the bots should a command and control takedown be successful. The most recent, and successful, takedown of Rustock's command and control utilized a new legal technique to physically seize the C&C servers; The Lanham Trademark Act (15 U.S.C.), which allows for the seizure of counterfeit goods. (This of course only applies within the jurisdiction of the United States, but fortunately, all but two of Rustock's C&C servers where hosted within the United States.)

Timeline

2006

The name "Rustock" was first used in early 2006 by Symantec[1] to describe a fairly ordinary spam bot. In the long tradition of no two Anti-Virus companies

[1] `http://www.symantec.com/security_response/print_writeup.jsp?docid=2006-011309-5412-99`

ever using the same name for the same malware, it has also been known by the names: "RKRustok", "Costrat[2]", and a bunch of generics like "Meredrop", or "Spambot". Initially, Rustock used the IRC protocol for C&C Communications[3]. The C&C servers were hosted at the notorious Russian Business Network[4]. These early versions opened a remote proxy on the victim computer, through which the C&C server would send SMTP directly to deliver spam. It used all the standard Windows Rootkit tricks to hide (SSDT, hooking ZwOpenKey, ADS, etc.) Rustock would also download an ICQ Client.

2007

I wasn't long before Rustock switched to using the more efficient template based spam technique, and began using HTTP for its C&C communications. It was mostly propagated through drive-by exploits, or through spam email with sensational subject lines, enticing users to run the attached [EXE] file. One of the more interesting campaigns this botnet was used for, was inflating penny stocks[5]. It was also around this time that the Rustock botnet was first being used to sell counterfeit Pfizer pharmaceuticals, and to perform advance-fee[6] fraud using Microsoft's trademark.

2008

After the demise of the Russian Business Network, Rustock, along with many other botnets, migrated it's C&C servers to Atrivo/Intercage[7]. Then after the shutdown of Atrivo[8] in September, Rustock's C&C servers were migrated to McColo.

McColo was de-peered in early November; Several botnets were simultaneously crippled by this – FireEye seized this sudden opportunity to hijack the Srizbi botnet[9], but that's another story. However, the technique we used then has also been used in this most recent Rustock takedown. (But I'm getting ahead of myself.)

McColo regained connectivity for about twelve hours, on a weekend, through a backup peering agreement with TeliaSonera. This was enough time for the

[2] http://www.m86security.com/labs/spambotitem.asp?article=902

[3] http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars

[4] http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html

[5] http://www.secureworks.com/research/blog/research/21041/

[6] http://en.wikipedia.org/wiki/Advance-fee_fraud

[7] http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

[8] http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html

[9] http://blog.fireeye.com/research/2008/11/srizbi-100000-strong-part-1.html

Rustock C&C's to push out a new update to a large percentage of the drones, pointing their new C&Cs to a server in Russia[10].

At that time, Rustock used hard-coded IP addresses for finding its C&Cs. There were some versions of Rustock which had a short list of hard-coded DNS names to lookup, should all of the C&C IP addresses no longer respond[11]. If McColo had remained down, a very large portion of the botnet would have been lost to the herder.

After McColo, all versions of Rustock had a DNS backup should the C&C servers become unreachable.

Joe Stewart estimated that there were approximately 130,000 computers infected with Rustock at the time[12].

2009

During this time, Rustock was propagated via Pay-Per-Install [Piptea] malware, and regular drive-by-download attacks. It sent out a lot of Pharmaceutical spam, and more of everything else that it had been spamming for the previous few years. Rustock was also now the source of over 50% of all spam on Earth.

Example Spam

```
Dear lucky winner,
This is to inform you that your email has won a consolation prize of the
     Microsoft Corporation EMAIL DRAW Today. Your email has won you
     1,000.000.00 (One Million Great british Pounds) To claim your prize,
     please contact your fiduciary agent Barr.Arthur James Esq with your
     Batch #:409978E and Reference No:FL/668530092 and contact him via email
     immediately within 24hrs.with the information below.
Barr Arthur James Esq
Email:barr.arthurjamesesq01@hotmail.com.hk
Tel: +44-792-404-9532
Tel: +44-703-192-4594
You are to send the below required details;
1.Full Name:.............
2.Address:..............
3..Occupation :.............‘
4.Age:.............
5.Sex:..............
6.Tel:.............
Sincerely,
Mrs Marilyn Berger Head Customercare Service
Microsoft Promotion.
```

[10] http://blog.fireeye.com/research/2008/11/rustocks-new-home.html

[11] http://blog.fireeye.com/research/2008/11/rustock-and-megad-fallback-domains.html

[12] http://www.secureworks.com/research/threats/botnets2009/

2010

Rustock had been using SMTP over TLS [SSL], but dropped support for TLS, presumably for performance reasons. The C&C servers, mostly hosted within the US, were fast-fluxed behind innocuous DNS names like "go-thailand-now.com" or "hollyjesus.com", and the URIs were also rather unremarkable, with names like "login.php", "main.php", "data.php". Most people just glancing at this in a packet capture might just think it's some web bulletin board and not investigate further.

One of the other things that Rustock would do, is pull in random text from Wikipedia [via /wiki/Special:Random] and add it to the end of the Subject line.

Example Spam Subjects

```
From: Super Offers onViagra <ibabuyaz9927@comcastbusiness.net>
Subject: julia, cut prices all week. Roman a Planet present Forest

From: Super Offers onViagra <pesipabep8888@vt.edu>
Subject: julia, cut prices all week. the rates received

From: Super Offers onViagra <uxupeidi1999@alicedsl.de>
Subject: julia, cut prices all week. d The

From: Super Offers onViagra <okysoy7918@charter.com>
Subject: julia, cut prices all week. Executive

From: Super Offers onViagra <yavehawygo7373@rr.com>
Subject: julia, cut prices all week. the the

From: Super Offers onViagra <nuufuigu2455@comcast.net>
Subject: julia, cut prices all week. as sequential The After

From: "Pfizer PillsTrader" <seruky3597@mchsi.com>
Subject: Hi julia, Sale-Over Reminder. area volcanic Movies

From: "Pfizer PillsTrader" <iliowi9398@comcast.net>
Subject: Hi julia, Sale-Over Reminder. is the b IB on

From: "Pfizer PillsTrader" <pocisyxu4643@2sex899.com>
Subject: Hi julia, Sale-Over Reminder. more Please the A members
```

Christmas Vacation

For reasons not yet known, Rustock stopped sending spam completely between Dec 25, 2010 and Jan 9, 2011. There has been much speculation as to the cause. One hypothesis holds that this was related to "SpamIt/Glavmed" going down in October. Or perhaps someone involved got arrested, or just wanted to take a vacation over the holidays. Maybe the botnet herder was abducted by space aliens.

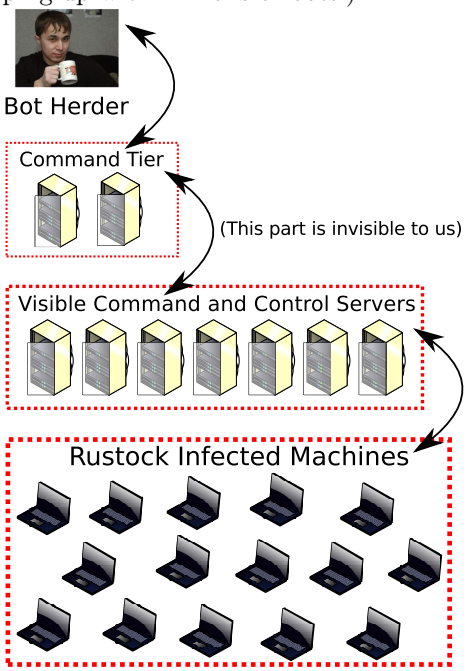
Technical Advancements

Rustock had begun using pseudo-random DNS names for C&C backup 16 fall-back names per day (after a static name or two like "gbsup.com"). It used a slight

variation of RC4 to encrypt communications, obscuring some of its updates as fake RAR files.

The DNS lookups for C&Cs would return an obfuscated IP address, which Rustock would then transform into the real thing $1.2.3.4 \Longrightarrow 5.6.7.8$

And a hierarchal C&C Server structure was created. The infected drones would connect to several dozen C&C servers to receive their spam templates, and binary updates. And those several dozen C&C servers would in turn receive their instructions from another smaller set of C&C servers – the identities of which are only know to the C&C servers themselves. Most of the visible C&C servers could be takendown, wiped, moved, or recreated by the bot herder easilly, and as long as at least one of them remained up, the botnet could be updated to point to a fresh set of C&C servers. I imagine there's probably also a performance benefit for the bot herder using the architecture, since it must be able to handle millions of incoming web connections at a time. (This is also probably why hosting was done in the United States and Netherlands, large amounts of bandwidth for keeping up with millions of bots.)



2011

March 16, 2011: US Federal Marshals and the Dutch High Tech Crime Unit seize all Rustock C&C physical servers.

All of the static backup DNS names ("incolonix.com", etc.) and psudeo-random DNS names out to the end of June are registered.

Operation b107

The Waledac takedown in 2010, Operation b49, involved the transfer of botnet DNS names to Microsoft control, by court order. This is not applicable to Rustock's C&C infrastructure.

Richard Boscovich had a great idea! Use the Lanham Trademark Act (15 U.S.C.) [And also, Computer Fraud and Abuse Act (18 U.S.C) and CAN-SPAM Act (15 USC ss 7704 and 7706) (via Microsoft's Hotmail) (trespass to chattels, conversion, unjust enrichment, etc.)] to...

> Enter a preliminary and permanent injunction isolating and securing the botnet infrastructure, including the software operating from and through the Command and Control IP Addresses/Domains and placing that infrastructure outside of the control of the Defendants or their representatives or agents.

Lanham TradeMark Act

This law allows companies to seize [alleged] counterfeit goods and trademark infringing materials.

The Rustock C&C servers [are believed to] contain spam templates for emails claiming to be from Microsoft, and for counterfeit Pfizer pharmaceuticals...

... Which are all fraudulently using Microsoft and Pfizer's trademarks.

> In the case of a civil action arising under section 32(1)(a) of this Act (15 U.S.C. 1114) [15 USC 1114(1)(a)] or section 220506 of title 36, United States Code, with respect to a violation that consists of using a counterfeit mark in connection with the sale, offering for sale, or distribution of goods or services, the court may, upon ex parte application, grant an order under subsection (a) of this section pursuant to this subsection providing for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacturer, sale, or receipt of things involved in such violation.

Since March

Brian Krebs may have found at least one person behind the operation of the Rustock Botnet: Vladimir Alexandrovich Shergin (who doesn't pay his hosting bills).

Another suspect associated with SpamIt goes by "Cosma2k" possibly named Dmitri A. Sergeev, Artem Sergeev, or Sergey Vladomirovich Sergeev. (Note, this is kind of the Russian equivalent of "John Smith").

Microsoft have been running large advertisements in two Russian newspapers, in the areas where the suspects are suspected to be, stating what they seized, and if anyone believe this to be in error, to contact them.

So far, no one has contacted Microsoft complaining about their servers being sized.

> "No Customers of the IP addresses in question, or the domains in question have requested that the IP addresses and domains be reinstated."

Botnet Size, Measured By Microsoft Sinkhole

- Mar 20-26, 2011: 1,601,619
- June 12-18, 2011: 702,860 [13]

Related News

Similar tactics were used to takedown CoreFlood botnet [14]

Conclusion

1. Researcher's need to share information. [Specifics go here]
2. Takedowns are mostly whack-a-mole if law enforcement is not involved. Also allows for the collection of evidence/data which may be lost (like where the top level C&Cs are).
3. DNS is a weak spot for botnet backup, now that it's possible to work with registrars and registries to just hand them a giant list of domain names, and have them quickly suspended/blacklisted/flagged/sinkholed. (This would have been so nice back during Srizbi.)
4. Jurisdictional stuff.
5. New legal tactics - it has its Pros and Cons.
6. Success!

Thanks and Credits

- Microsoft DCU did most of the work
- FireEye [mostly just Alex] just double-checked the data and wrote a declaration

[13] http://blogs.technet.com/b/microsoft_blog/archive/2011/07/05/microsoft-releases-new-threat-data-on-rustock.aspx

[14] http://blogs.technet.com/b/security/archive/2011/04/14/fbi-and-doj-legal-and-technical-action-against-coreflood-botnet.aspx

- David Dittrich at University of Washington
- Patrick Ford of Pfizer Global Security
- ...

Draft Status

- I still need to include the raw technical data, with charts and graphs.
- Improve the bibliographic citations.
- Edits based upon commentary/review of other researchers involved.

References

[This needs to be cleaned-up.]

Lanham (Trademark) Act (15 U.S.C.) http://www.bitlaw.com/source/15usc/

Lanham Act (15 U.S.C. §1114) http://www.bitlaw.com/source/15usc/1114.html

Lanham Act (15 U.S.C. §1125) http://www.bitlaw.com/source/15usc/1125.html

CAN-SPAM http://uscode.house.gov/download/pls/15C103.txt

Messagelabs 2009 Report http://de.messagelabs.com/mlireport/2009MLIAnnualReport_Final_EN-DE.pdf

Messagelabs Anual Security Report 2010 http://www.symanteccloud.com/mlireport/MessageLabsIntelligen

Messagelabs August 2010 http://www.symanteccloud.com/download.get?filename=MLI_2010_08_August

Messagelabs April 2010 http://www.messagelabs.com/mlireport/MLI_2010_04_Apr_FINAL_EN.pdf

Oct 6, 2010 http://www.symantec.com/connect/blogs/recent-drop-global-spam-volumes-what-happened

Jul 23, 2010 http://www.m86security.com/labs/traceitem.asp?article=1362

–

Jan 9, 2007 Joe Stewart http://www.secureworks.com/research/blog/research/21041/

Jun 20, 2007 http://isc.sans.org/diary.html?storyid=3015 (The bit about RBN)

Apr 8, 2008 Joe Stewart http://www.secureworks.com/research/threats/topbotnets/

Nov 16, 2008 Alex Lanstein, et al. http://blog.fireeye.com/research/2008/11/fallback-cc-channels-part-deux.html

Nov 18, 2008 Nick Chapman http://www.secureworks.com/research/blog/spam/50557/

Nov 18, 2008 http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/

Sep 29, 2009 Kevin Stevens http://www.secureworks.com/research/threats/ppi/

Dec 7, 2010 http://www.symantec.com/about/news/release/article.jsp?prid=20101207_01

Feb 15, 2011 SecureWorks http://www.secureworks.com/research/threats/spambot-evolution/

Mar 17, 2011 http://blogs.technet.com/b/security/archive/2011/03/18/microsoft-takedown-of-rustock-botnet.aspx

Mar 17, 2011 http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx

Mar 18, 2011 http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html?mod=V

Mar 21, 2011 http://blogs.iss.net/archive/RustockSpam.html

Mar 22, 2011 http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars

Mar 23, 2011 http://www.theregister.co.uk/2011/03/23/rustock_takedown_analysis/

Mar 2011 http://www.symanteccloud.com/mlireport/MLI_2011_03_March_Final-EN.pdf

Jul 25, 2008 http://www.scmagazineus.com/the-rustock-botnet-spams-again/article/112940/

–

http://voices.washingtonpost.com/securityfix/2007/10/mapping_the_russian_business_n.html

http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html

http://voices.washingtonpost.com/securityfix/2008/10/spam_volumes_plummet_after_atr.html

Nov 11, 2008 http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.h

Nov 13, 2008 http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html

Nov 12, 2008 http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.h

Nov 18, 2008 http://www.washingtonpost.com/wp-dyn/content/article/2008/11/19/AR2008111903075_pf

http://voices.washingtonpost.com/securityfix/2009/01/meet_the_new_bots_will_we_get.html

Jan 5, 2011 http://krebsonsecurity.com/2011/01/taking-stock-of-rustock/

May 25, 2011 http://arstechnica.com/microsoft/news/2011/05/microsoft-fingers-russians-over-rustock-spam-botnet.ars

Mar 23, 2011 http://www.v3.co.uk/v3-uk/analysis/2036894/microsoft-fireeye-inside-story-rustock-botnet-shutdown

Mar 23, 2011 http://www.v3.co.uk/v3-uk/analysis/2036894/microsoft-fireeye-inside-story-rustock-botnet-shutdown/page/2

–

Jun 2011 http://download.microsoft.com/download/8/A/F/8AF98F57-8111-44EC-8E82-53E9404B211E/Battling%20the%20Rustock%20Threat_English.pdf

Jul 5, 2011 http://blogs.technet.com/b/microsoft_blog/archive/2011/07/05/microsoft-releases-new-threat-data-on-rustock.aspx

Oct 6, 2010 http://blog.fireeye.com/research/2010/10/silent-rustock.html

Aug 30, 2010 http://blog.fireeye.com/research/2010/08/infiltrating-pushdo-part-2.html

Mar 19, 2011 http://blog.fireeye.com/research/2011/03/an-overview-of-rustock.html

Oct 28, 2008 http://blog.fireeye.com/research/2008/10/mccolo-still-hosting-rustock-cc.html

Aug 22, 2008 http://blog.fireeye.com/research/2008/08/srizbi-and-ru-1.html

Nov 24, 2008 http://blog.fireeye.com/research/2008/11/rustock-selling-pills-again.html

Nov 16, 2008 http://blog.fireeye.com/research/2008/11/rustocks-new-home.html

Aug 17, 2008 http://blog.fireeye.com/research/2008/08/srizbi-and-rust.html

Mar 22, 2011 http://blog.fireeye.com/research/2011/03/a-retreating-army.html

Nov 18, 2008 http://blog.fireeye.com/research/2008/11/rustock-and-megad-fallback-domains.html

http://blog.fireeye.com/research/rustock-cnc-servers.html

Nov 7, 2008 http://blog.fireeye.com/research/2008/11/quick-nugget-on-the-russiarustock-connection.html

–

Apr 8, 2010 http://florensik.wordpress.com/2010/04/08/windbg-rustock-2010-blobs/

Oct 29, 2008 http://www.threatexpert.com/report.aspx?md5=abb9a2630e25c5511de2c7ebe694660f

Feb 8, 2011 http://www.threatexpert.com/report.aspx?md5=60f7ae2098b2d58869d021e441d2c90e

Mar 29, 2009 http://www.threatexpert.com/report.aspx?md5=73f9be140abee3f43fdd2b9ed5beb401

2007 http://www.usenix.org/event/hotbots07/tech/full_papers/chiang/chiang_html/

Jan 13, 2006 http://www.symantec.com/security_response/print_writeup.jsp?docid=2006-011309-5412-99

Jun 1, 2006 http://www.naked-security.com/malware/Backdoor.Rustock.A/

Mar 20, 2009 http://www.m86security.com/labs/spambotitem.asp?article=902

Mar 5, 2009 http://www.m86security.com/labs/traceitem.asp?article=882

Jan 18, 2007 http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%

Sep 2, 2009 http://www.sunbeltsecurity.com/ThreatDisplay.aspx?tid=45547&cs=DC9E4149B3D49F2FCEI

–

Mar 11, 2011 http://www.noticeofpleadings.com/

http://en.wikipedia.org/wiki/Rustock_botnet

–

Sep 8, 2010 http://blogs.technet.com/b/microsoft_blog/archive/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet.aspx

–

Apr 14, 2011 http://blogs.technet.com/b/security/archive/2011/04/14/fbi-and-doj-legal-and-technical-action-against-coreflood-botnet.aspx

Legal Pedantary