Battling the Rustock Threat

Microsoft | Security Intelligence Report

Special Edition

January 2010 through May 2011

Authors

David Anselmi – Microsoft Digital Crimes Unit
Richard Boscovich – Microsoft Digital Crimes Unit
T.J. Campana – Microsoft Digital Crimes Unit
Samantha Doerr – Microsoft Digital Crimes Unit
Marc Lauricella – Microsoft Trustworthy Computing
Oleg Petrovsky – Microsoft Malware Protection Center
Tareq Saade – Microsoft Malware Protection Center
Holly Stewart – Microsoft Malware Protection Center

Program Manager

Frank Simorjay – Microsoft Trustworthy Computing

Introduction

This document provides an overview of the Win32/Rustock family of rootkit-enabled backdoor trojans. The document examines the background of Win32/Rustock, its functionality, how it works, and provides threat telemetry data and analysis from calendar year 2010 through May 2011. In addition, this document details the legal and technical action used to takedown the Rustock botnet and how to detect and remove the threat using Microsoft antimalware products.

For updates, and current activities on Rustock botnet visit:
http://blogs.technet.com/b/microsoft_on_the_issues/

Foreword

Microsoft and the Rustock Botnet

On March 16, 2011, Microsoft announced that the Microsoft Digital Crimes Unit (DCU), in cooperation with industry and academic experts, had successfully taken down the Win32/Rustock botnet. At the time of the takedown, Rustock was estimated to have had approximately a million infected computers operating under its control and was known to be capable of sending billions of spam email messages every day, including fake Microsoft lottery scams and offers for fake – and potentially dangerous – prescription drugs.

The Rustock takedown was the second botnet takedown orchestrated by Microsoft through a joint effort between DCU, Microsoft Malware Protection Center (MMPC), and Microsoft Trustworthy Computing known as Project MARS (Microsoft Active Response for Security). Project MARS was started as a way to target and disrupt botnets and the criminal infrastructure they support, as well as to help victims regain control of their infected computers. The first botnet takedown in Project MARS was in the spring of 2010 - a takedown codenamed "Operation b49" which disabled the Waledac botnet. Operation b49 was a proof-of-concept case for the Microsoft botnet takedown approach, and it was then followed by the takedown of a larger, more notorious botnet known as Rustock in March 2011. Like Waledac, the Rustock takedown (codenamed Operation b107) relied on the novel application of both legal and technical measures to sever the connection between the command and control structure of the Rustock botnet and the malware-infected computers operating under its control to stop the ongoing harm caused by the botnet.

Large scale botnet takedowns like these cannot be accomplished alone. They require collaboration between industry, academic researchers, law enforcement agencies, and governments worldwide. In this specific case, Microsoft worked with Pfizer, the network security provider FireEye, and security experts at the University of Washington. FireEye provided significant technical assistance with the technical analysis of Rustock, and all three provided declarations in federal court on the dangers posed by the Rustock botnet and its impact on the Internet community. Microsoft also worked with the Dutch High Tech Crime Unit within the Netherlands Police Agency to help dismantle part of the command structure for the botnet operating outside of the United States. In addition, Microsoft worked with CN-CERT in blocking the registration of domains in China that Rustock could have used for future command and control servers.

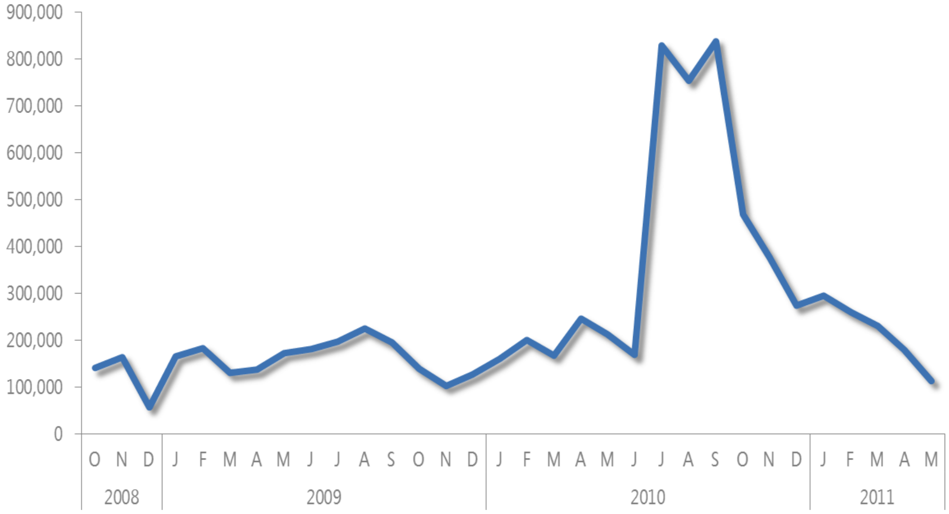
The central lesson that we have learned from all our efforts to fight botnets has been that cooperation in the execution of proactive disruptive efforts is the key to success.

Richard Boscovich
Senior Attorney, Microsoft Digital Crimes Unit

How Win32/Rustock Works

Win32/Rustock is a multi-component family of rootkit-enabled backdoor trojans that were historically developed to aid in the distribution of spam email. Detections of Rustock were first discovered in early 2006. By 2008, Rustock began appearing in significant numbers and by mid 2010 had grown to become one of the most prevealent and pervasive computer threats in the world as seen in Figure 1. Recent variants seemed to be associated with rogue security programs.

Figure 1. Detections of Win32/Rustock by Microsoft antimalware solutions, October 2008–May 2011



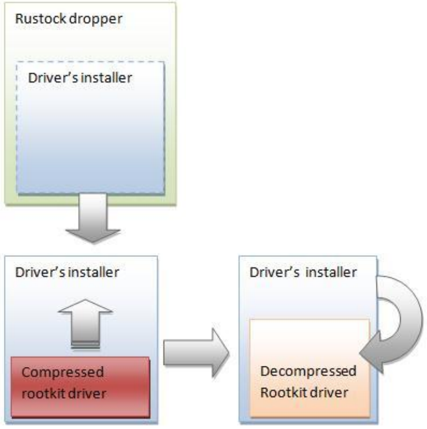
Components and Installation

Rustock consists of three distinct components that are encrypted using both custom and third-party technologies. Although Rustock has evolved over the past five years, it has relied heavily on code compression and obfuscation utilities such as aPLib and UPX, as well as the RC4 encryption algorithm.

The three components and their involvement in the Rustock infection process are described in the following paragraphs:

1. The dropper component runs in user mode and is responsible for decrypting and dropping the rootkit driver component. (The dropper component was also responsible for contacting a Rustock command-and-control C&C server to determine whether any updates were available.)

Figure 2. Win32/Rustock schematic diagram



Before attempting to infect the computer, the dropper component checks the registry to determine whether the Rustock rootkit is already present. It accomplishes this by seeking out the presence of certain "global events" keys that Rustock adds to a computer's registry when fully installed.If the rootkit is present and active, the dropper does not attempt to reinfect the computer.

The code of the dropper component is complex; it's deliberately messy and unoptimized, employing polymorphic jumps and no static strings. It's encrypted with the RC4 algorithm, and then packed with the aPLib compression library.

2. The driver installer component runs in kernel mode, disguised as a Windows system driver. This component attempts to hide itself by replacing a driver such as beep.sys or null.sys with a copy of itself, then replacing it after it has started. If this attempt is unsuccessful, the dropped installer typically uses a filename that is either hard-coded or randomly-generated, depending on the Rustock variant. Sample hard-coded filenames have included glaide32.sys and lzx32.sys; 7005d59.sys is a typical random filename that researchers have observed.

Older variants of Rustock employed many alternate techniques to get themselves installed as a system driver to evade detection. researchers have observed variants attempting to install themselves to null shares (for example, \\127.0.0.1\admin$\system32\drivers\*drivername*.sys) and dropping the installer as an alternate data stream (such as System:lzx32.sys), among others. Modern versions of Rustock use system service hooking to covertly load this component.

3. The rootkit driver component runs in kernel mode, like the driver installer. This component represents the kernel-mode side of the Rustock payload. The user-mode bot client communicates with the rootkit using INT 2Eh interrupts.

   This component contains all the code that managed the backdoor functionality, such as communicating with the C&C server and executing instructions sent by the Rustock operators (which typically involved sending spam messages).

   Like the others, this component begins by decrypting itself and then injects a copy of its decrypted code into itself before transferring control over to the newly instantiated copy.

   To hide its presence, the rootkit component hooks a variety of functions in the System Service Dispatch Table (SSDT), including ZwCreateEvent, ZwCreateKey, and ZwOpenKey, to filter itself out of any requests that contain its own name. It also hides its disk and network operations by hooking functions in ntoskrnl.dll and ntdll.dll, as well as network drivers such as tcpip.sys and wanarp.sys.

   In addition to the previously described protection techniques (RC4 encryption, unoptimized and jump-laden code), Rustock checks for the presence of kernel debuggers such as WinDBG, Syser, and SoftICE. It also tries to maintain code integrity by constantly checking itself for modifications using CRC32 checksums, and by scanning itself for software breakpoints (0xCC).

Spam

After Rustock is installed and carefully disguised on a user's computer, it is ready to connect to and communicate with its C&C servers. Before the takedown, these servers sent Rustock-infected computers information and instructions to send out spam messages without the knowledge, approval, or involvement of the users.

The structure of the spam component has varied. In some cases, it is integrated into the kernel-mode rootkit component; in others, researchers found that the rootkit component drops it onto a disk separately, where it executes in a user context.

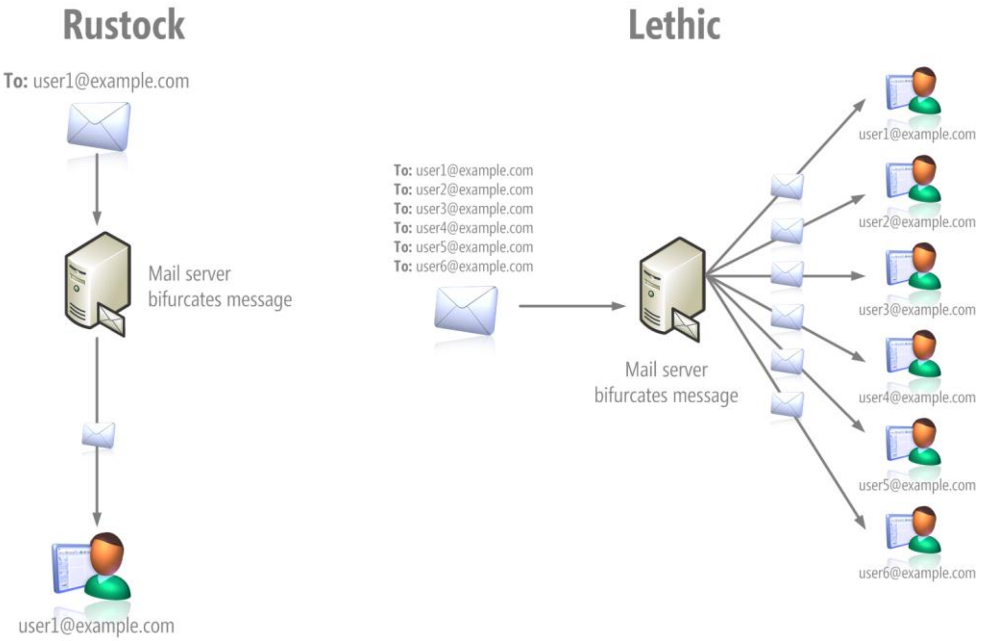
Early versions of Rustock used a custom-built SMTP client engine named “botdll.dll” to send out spam email. In 2008, Rustock was modified to send spam through Windows Live Hotmail using credentials supplied by the C&C server. Sending email directly from a user’s computer is often a telltale sign of a malware infection, and risks being detected as malicious activity by firewalls and other network monitoring technologies. By using a web-based email client, Rustock was more likely to avoid detection.

Moving to Hotmail also allowed Rustock to take advantage of SSL. Whereas traditional email messages are delivered in cleartext, Rustock was now able to encrypt its outgoing traffic using DHTTPS, thus further evading detection.

The spam sent out by infected computers is based on “spam templates,” or resource files, that the user’s computers received from the C&C servers. The infected computers used these templates, some of which unlawfully contain Microsoft trademarks, to generate the spam that they sent out. The Rustock operators could manage how aggressively a compromised computer sent spam by specifying the number of threads the computer used to send messages, up to a maximum of 100.

Some other mass-mailer malware threats, such as Win32/Lethic, include several addresses on the “To” line. Unlike these threats, Rustock sent spam messages to recipients one at a time.

Figure 3. Comparison of the Rustock and Lethic spam distribution models



Deployment and Payload

As Rustock evolved, so too did its payload. It was initially designed to send out spam email, and was originally associated with the McColo infrastructure and the Russian Business Network (where installers had been seen being hosted). Typical spam messages that it sent often related to pharmaceutical products or fake pharmacy sites, or linked to pages that occasionally hosted additional malware.

Rustock was also observed directing traffic to rogue security software sites that duped unsuspecting users into purchasing and installing phony antivirus products using social engineering techniques. In addition, Rustock was known to install rogue security software and other malware onto infected computers directly and through drive-by exploits.

The DCU performed an experiment in conjunction with the MMPC in which a closely monitored host was infected with Win32/Harnig (a known Rustock dropper) to determine what additional malware would get installed. Within five interaction-free minutes of infection, a wide variety of additional malware and potentially unwanted software had been downloaded and installed onto the infected computer, as shown in the following figure:

Figure 4. Threats installed by Win32/Harnig within five minutes of infection

Threat Name	MD5
Adware:Win32/Zugo	5a77b40c7e9de96a4183f82da0836a19
Backdoor:Win32/Kelihos.A	1454b22c36f1427820b24b564efb2e39
TrojanDownloader:Win32/Stasky.A	19616154d6d63a279d77ae11f7b998e9
TrojanDownloader:Win32/Bubnix.A	8e159ff1bbd5a470f903d0e32979811c
Rogue:Win32/FakeSpypro	76f4c35d23b7363fcf6d1870f0169efe
Trojan:Win32/Malagent	7d6ead50862311242902df065c908840
Trojan:Win32/Harnig.gen!D	d0556114e53bae781a5870ef4220e4fc
Trojan:Win32/Hiloti.gen!D	1c8cb08d2841f6c14f69d90e6c340370
Trojan:Win32/Hiloti.gen!D	444bcb3a3fcf8389296c49467f27e1d6
TrojanDownloader:Win32/Renos.MJ	5571a3959b3bd4ecc7ae7c21d500165f
TrojanDownloader:Win32/Renos.MJ	89f987bdf3358e896a56159c1341f518
TrojanDownloader:Win32/Small.SL	ccd08d114242f75a8f033031ceeafb88
Trojan:Win32/Meredrop	23472a09a1d42dc109644b250db0ca1e
TrojanDownloader:Win32/Waledac.C	b7030bdf24d6828c6a1547dc2eece47d
TrojanDownloader:Win32/Waledac.C	de5bd40cb5414a5d03ffd64f015ffacc
Backdoor:Win32/Cycbot.B	86d308e7a03e9619dbf423e47ac39c50
TrojanDownloader:Win32/Small.SL	2664b0abf4578d0079e3ad59ab697554
Worm:Win32/Skopvel	331fe9a906208ce29ba88501d525356b
Rogue:Win32/Winwebsec	e4a9504875c975b8053568120c56743b

Many of the threats listed in Figure 4 are themselves designed to download yet more threats at various intervals.

Multiple layers of trojan downloaders form complex chains of relationships between the owners of different malware networks. Botnet access is often cited as being available for rent, but so too is access to downloader locations. This access is evident by the fact that the files pointed to by downloaders constantly change—sometimes they are swapped out for newer versions of the malware or versions that were obscured in different ways, and other times they're swapped out for something different altogether.

It should be noted that Rustock employs a modular payload architecture: the user-mode bot client known in earlier versions as botdll.dll could easily be replaced with any other payload. Although Rustock spent most of its time sending spam, it could have easily been used for virtually any nefarious purpose with very minor modification.

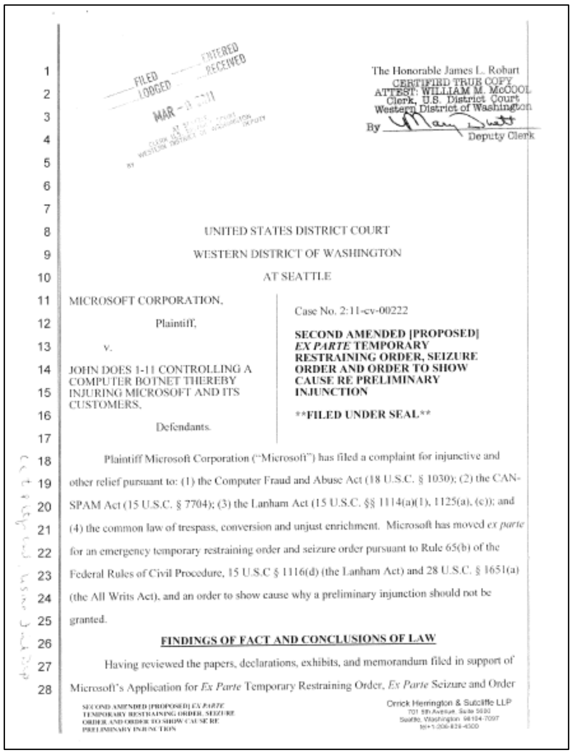
Backup Control Mechanism

When the C&C servers were unreachable, Rustock had a fallback mechanism it relied on to re-establish communications. The malware includes an algorithm that generates 16 new domain names daily, consisting of nonsense strings of characters such as *jvwyqarglgwqvt.info* and *hy38la8rwpaqlpiy.com*. Infected computers then attempt to contact each of these domains. The Rustock operators would use the same algorithm to generate the domain names in advance and use them as command-and-control points. Rustock variants have been identified as using six different algorithms that each generate different domain name lists, for a total of 96 new domain names each day. As explained in the "Rustock Statistics" section later in this report, Microsoft researchers have been able to take advantage of this mechanism to obtain valuable information about the spread and scope of the Rustock botnet.

Defeating Rustock In the Courts

The Rustock takedown was the second major botnet takedown Microsoft has spearheaded within the last two years. In 2010, Microsoft asked for and received a court order that shut down a number of malicious domains used by the Waledac botnet. (See the *Security Intelligence Report* website for more information.) As part of that effort, Microsoft filed a John Doe lawsuit against the anonymous operators of the Rustock botnet, based in part on the abuse of Microsoft trademarks in the bot's spam.

Figure 5. The temporary restraining order (TRO) granted against the operators of the Rustock botnet.



FILED — ENTERED
LODGED — RECEIVED
MAR - 3 2011
AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

The Honorable James L. Robart
CERTIFIED TRUE COPY
ATTEST: WILLIAM M. McCOOL
Clerk, U.S. District Court
Western District of Washington
By ______
Deputy Clerk

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,
Plaintiff,
v.
JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,
Defendants.

Case No. 2:11-cv-00222

SECOND AMENDED [PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

****FILED UNDER SEAL****

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the Lanham Act) and 28 U.S.C. § 1651(a) (the All Writs Act), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order

SECOND AMENDED [PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

However, Rustock's infrastructure was much more complicated than Waledac's, relying on hard-coded IP addresses rather than domain names and peer-to-peer command and control (C&C) servers to control the botnet. In an attempt to prevent the bot from being quickly shifted to new infrastructure, Microsoft sought and was granted on March 9, 2011 a court order that incorporated a seizure order. This order allowed the company, escorted by the U.S. Marshals Service, to physically capture evidence onsite and, in some cases, take the affected servers from hosting providers for analysis. (This order, and other legal documents in the case, are posted at www.noticeofpleadings.com.)

Figure 6. Hard disks confiscated from Rustock C&C servers

On March 16, 2011, servers were seized from five hosting providers operating in seven cities in the U.S., including Kansas City, MO; Scranton, PA; Denver, CO; Dallas, TX; Chicago, IL; Seattle, WA; and Columbus, OH. With help from the upstream providers, Microsoft successfully severed the IP addresses that controlled the botnet, cutting off communication and disabling it.

Microsoft subsequently conducted a forensic investigation on 20 of the seized hard drives, which uncovered some important information about the operation of the botnet:

- Evidence of spam dissemination found on one of the drives included custom-written software that relates to assembly of spam email messages and text files that contain thousands of email addresses and username/password combinations. One text file alone contained more than 427,000 email addresses. Several of the spam templates provided evidence of abuse of trademarks that belong to Microsoft and pharmaceutical companies.

- Another drive included data that indicated the server from which the drive was taken was used as the starting point for cyber-attacks into Russian IP space.

- The other 18 drives all exhibited common characteristics that indicated the associated servers were used as nodes in a network that provides anonymized Internet access. These servers were likely used to provide the operators with anonymous access to Rustock systems such as the one described earlier that stored email templates, trademarks, and email addresses.

The forensic analysis of the drives also uncovered several email addresses that were likely used by the operators in the course of testing the system.

Through investigation of the hosting arrangements made for the servers, Microsoft determined that the Rustock C&C servers were paid for through an online payment service account associated with an address in the Moscow, Russia area. Similarly, a number of the C&C servers were established by an individual or individuals using the nickname "Cosma2k," which has been connected to a number of different names.

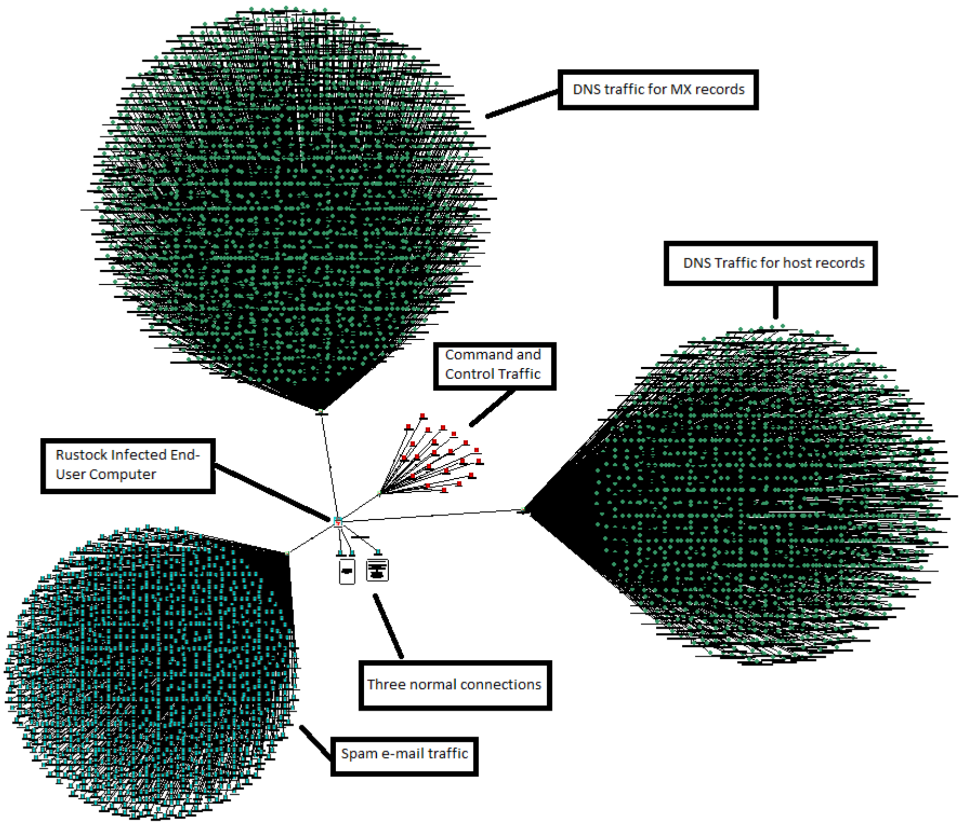
Microsoft continues to investigate all of these names, email addresses, and other evidence in an effort to locate the individuals responsible for implementing and operating the Rustock botnet, so that appropriate legal actions can be taken.

Rustock Statistics

Between January 22, 2011 and February 4, 2011, Microsoft detected that Rustock-infected computers connected to the Internet from more than 1,300,000 unique IP addresses around the world. The infection tier in the Rustock architecture is made up of a large number of Rustock-infected computers such as those found in businesses, living rooms, schools, libraries, and Internet cafes around the world.

The following figure depicts the very large number of Internet connections made within 24 minutes by a single Rustock-infected computer. This computer made three normal connections, but it also performed 1,406 unique lookups for various DNS A hosts on the Internet and 2,238 unique lookups for DNS MX records for mail servers on the Internet. In addition, it attempted to send spam e-mail to 1,376 email servers on the Internet, including to a number of Hotmail and MSN email account customers, and made 22 connections to C&C servers or other servers on the Internet.

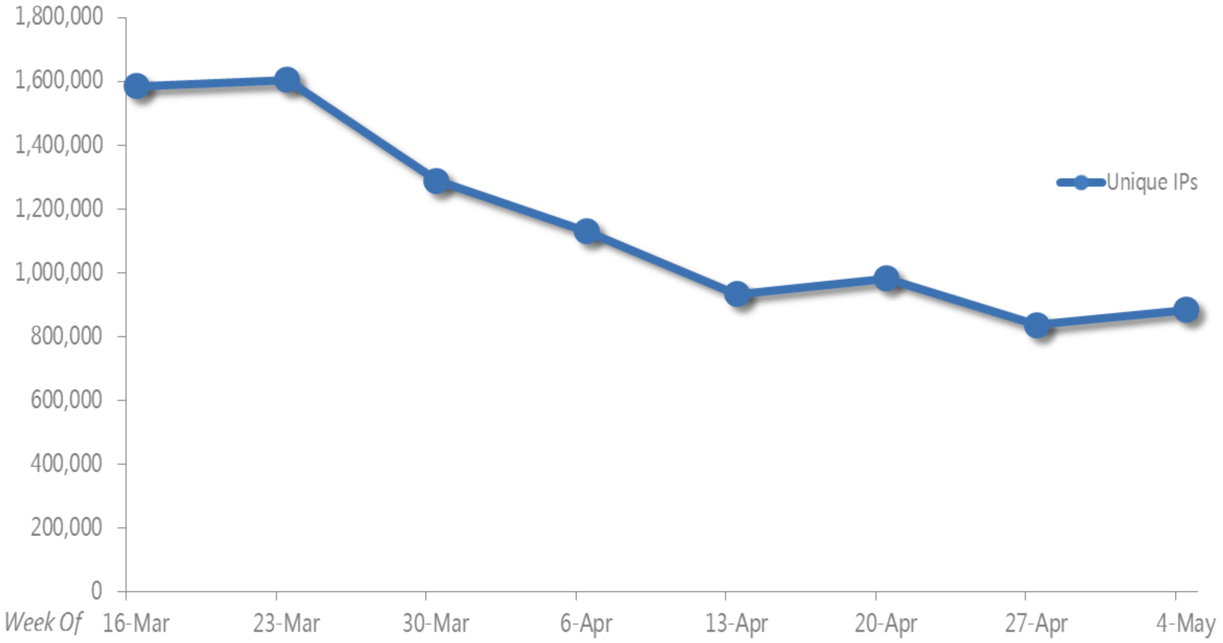
Figure 7. Visual representation of the activity of a single Rustock-infected computer within a 24-minute timeframe.


DNS traffic for MX records
DNS Traffic for host records
Command and Control Traffic
Rustock Infected End-User Computer
Three normal connections
Spam e-mail traffic

Infection Statistics

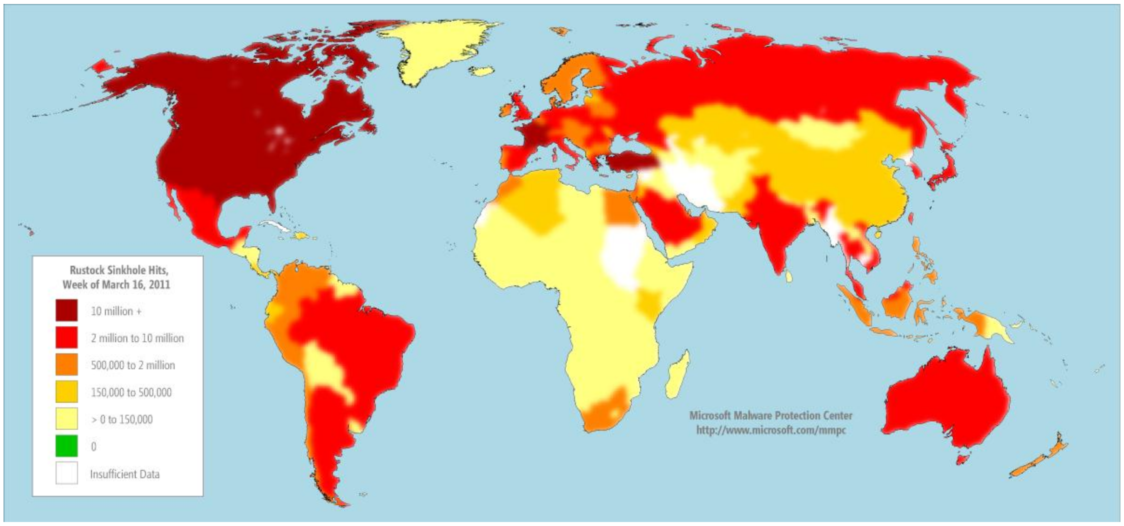
As explained in the “How Win32/Rustock Works” section earlier in this report, Rustock variants are designed to contact a number of algorithmically generated domain names for instructions if the primary C&C servers are unavailable. Microsoft researchers successfully reverse-engineered the Rustock domain name generation algorithms prior to the March 16 takedown, which enabled them to register many of the domain names themselves to prevent the Rustock operators from gaining control of them. These domain names were assigned to *sinkholes* (server complexes designed to absorb and analyze malware traffic) operated by Microsoft so botnet traffic could be observed and studied. The telemetry generated by the sinkhole servers has provided valuable information about the geographic scope of the Rustock botnet.

Figure 8. Unique IP addresses contacting the Rustock sinkhole during the first 8 weeks after the takedown, by week



Like most malware families, Rustock does not affect all parts of the world equally. The following figure shows the number of hits received by sinkhole servers from Rustock-infected computers during the first week after the takedown.

Figure 9. Worldwide distribution of Rustock traffic during the first week after the takedown


Rustock Sinkhole Hits, Week of March 16, 2011
10 million +
2 million to 10 million
500,000 to 2 million
150,000 to 500,000
> 0 to 150,000
0
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Infected computers in the United States generated the most sinkhole traffic during week 1, with 55.8 million hits. Following the United States were France (13.7 million hits), Turkey (13.4 million), Canada (11.4 million), India (7.3 million), and Brazil (7.1 million). Some locations with large numbers of computers nevertheless generated relatively few hits, including China (423,078 hits in week 1), Chile (500,925), Denmark (539,577), and Norway (581,263).

The number of IP addresses contacting the sinkhole decreased 44.2 percent between the 1st and 8th week after the takedown, as Rustock variants were removed from affected computers by antivirus software and through other means such as scripts, removal tools and computer reinstallation. As with the initial infections, this decrease did not affect all parts of the world equally. Figure 10 and Figure 11 show the percentage decrease in unique IP addresses contacting the Rustock sinkhole between the 1st and 8th weeks after the March 16 takedown in different locations around the world, and for the most affected Autonomous System Numbers (ASNs).

Figure 10. Decreases in IP addresses contacting the Rustock sinkhole during the first eight weeks after the takedown, by location

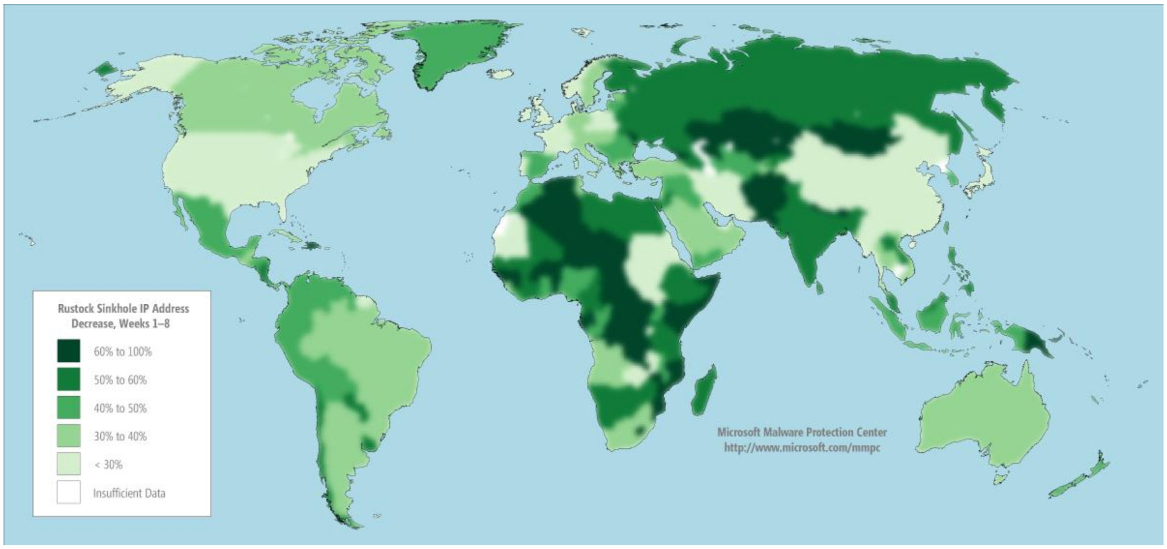

Rustock Sinkhole IP Address Decrease, Weeks 1–8
60% to 100%
50% to 60%
40% to 50%
30% to 40%
< 30%
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

Figure 11. Rustock traffic decrease from the 15 most-affected ASNs between March 16 and May 17

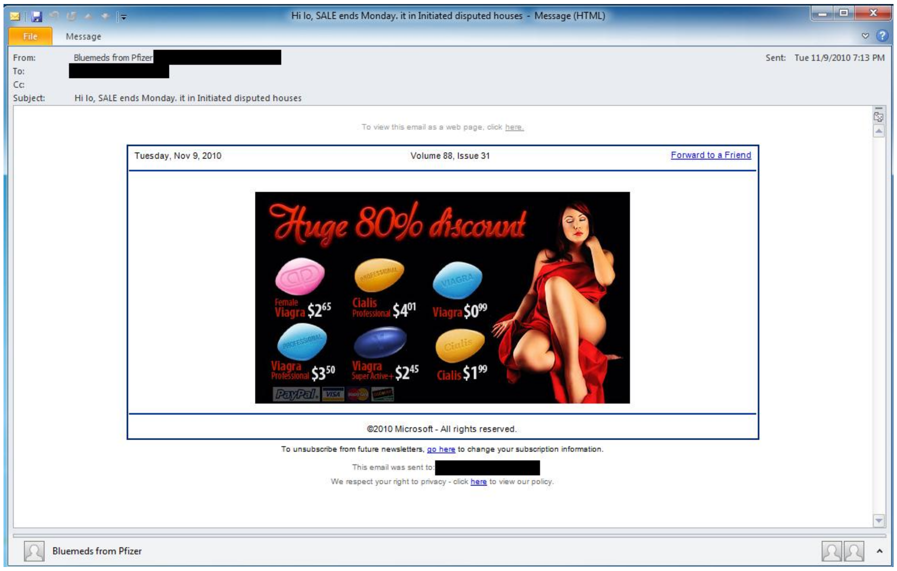
ASN Rank	Continent	Unique IPs – Week 1	Unique IPs – Week 9	Decrease
Affected ASN 1	Asia	117,480	42,109	64.2%
Affected ASN 2	Asia	73,751	43,745	40.7%
Affected ASN 3	Asia	33,303	12,015	63.9%
Affected ASN 4	North America	31,405	17,611	43.9%
Affected ASN 5	Asia	28,890	11,785	59.2%
Affected ASN 6	Asia	28,829	11,646	59.6%
Affected ASN 7	Asia	28,738	13,472	53.1%
Affected ASN 8	Asia	24,709	13,480	45.4%
Affected ASN 9	Europe	23,440	15,006	36.0%
Affected ASN 10	Asia	22,723	7,839	65.5%
Affected ASN 11	Asia	21,680	6,242	71.2%
Affected ASN 12	Europe	21,543	9,982	53.7%
Affected ASN 13	Europe	20,239	13,551	33.0%
Affected ASN 14	Asia	18,955	11,632	38.6%
Affected ASN 15	Europe	17,878	9,974	44.2%

Spam Statistics

Although its behavior fluctuated over time, Rustock was reported to be among the world's largest spambots, at times capable of sending 30 billion spam email messages per day. DCU researchers observed a single Rustock-infected computer send **7,500** spam email messages in just **45 minutes –** a rate of **240,000** spam messages **per day**. Moreover, much of the spam observed coming from Rustock posed a danger to public health, advertising counterfeit or unapproved knock-off versions of pharmaceuticals.

As mentioned previously, because Rustock propagated a market for these fake drugs, drug maker Pfizer served as a declarant in this case. Pfizer conducted test purchases of the drugs advertised by Rustock and included the results of their analysis in their declaration. Pfizer's declaration provided evidence that the kind of drugs advertised through this type of spam often contained the wrong active ingredients, incorrect dosages, or worse, because of the unsafe conditions in which they are often produced. Fake drugs are often contaminated with substances including pesticides, lead-based highway paint, and floor wax, to name just a few examples.

Figure 12. A spam message sent through the Rustock botnet



Hi lo, SALE ends Monday. it in Initiated disputed houses - Message (HTML)
File
Message
Huge 80% discount
Female Viagra $2^{65}
Cialis Professional $4^{01}
Viagra $0^{99}
Viagra Professional $3^{50}
Viagra Super Active+ $2^{45}
Cialis $1^{99}
PayPal
VISA
Bluemeds from Pfizer

From: Bluemeds from Pfizer [redacted]

To: [redacted]

Cc:

Subject: Hi lo, SALE ends Monday. it in Initiated disputed houses

Sent: Tue 11/9/2010 7:13 PM

To view this email as a web page, click here.

Tuesday, Nov 9, 2010 | Volume 88, Issue 31 | Forward to a Friend

©2010 Microsoft - All rights reserved.

To unsubscribe from future newsletters, go here to change your subscription information.

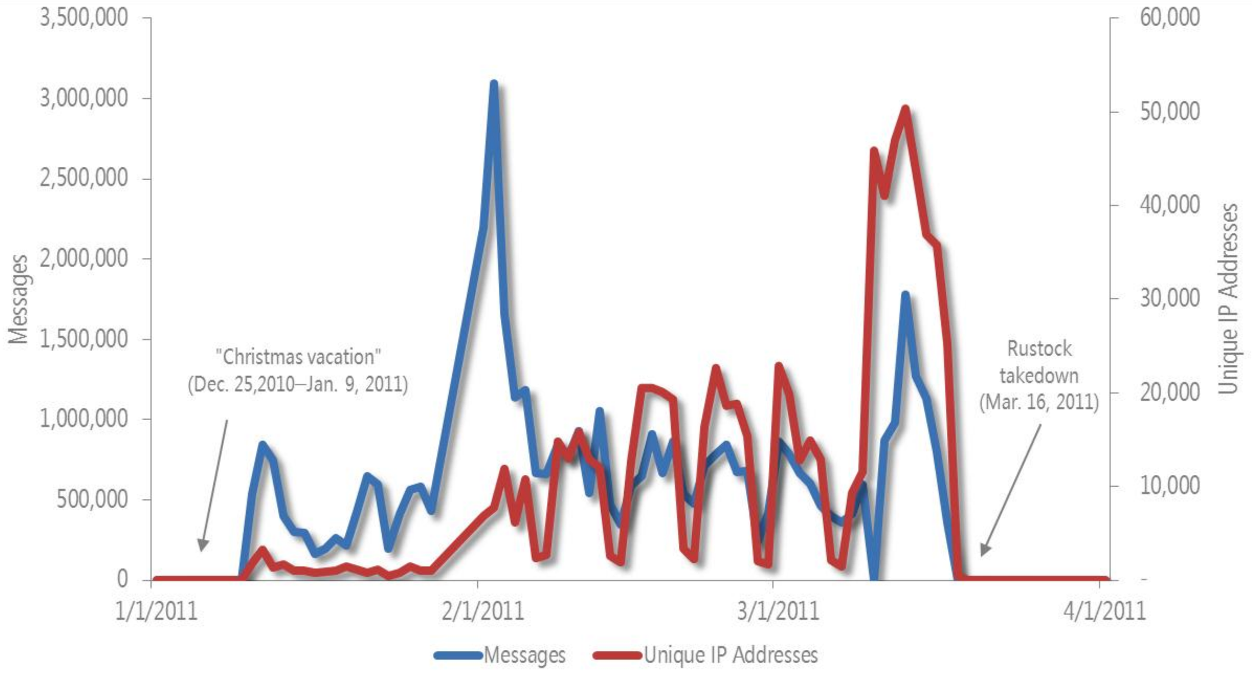
This email was sent to: [redacted]

We respect your right to privacy - click here to view our policy.

Rustock Spam Activity Detected by Microsoft Technology

Large volumes of spam from Rustock was detected using Microsoft® Forefront® Online Protection for Exchange (FOPE). FOPE provides a layered technologies to actively help protect organizations' inbound and outbound email from spam, viruses, and phishing scams in violation of email policy violations. The following figure shows the spam activity of the Rustock botnet from January through April 2011 as detected by FOPE, by messages received and distinct IP addresses used.

Figure 13. Rustock botnet activity detected by FOPE in 1Q11, by messages received and IP addresses used



The Rustock botnet was almost completely inactive between December 25, 2010 and January 9, 2011, for reasons that are not entirely clear but may reflect a pause for Christmas vacation. The botnet resumed normal operation after this break concluded, and by early February was exhibiting a typical stable pattern of activity. Botnet activity dropped abruptly to almost zero in mid-March following the takedown.

Conclusion

The Rustock botnet was once reported to be among the world's largest spambots, at times capable of sending 30 billion spam email messages per day. Through the combined efforts of Microsoft,the judicial system, and the industry, Rustock was successfully taken down on March 16, 2011.

The actions taken against large scale botnets like Waledac and Rustock may have been the first of their kind, but they won't be the last. As cybercriminals continue to use botnets as the backbone for cybercriminal activity, Microsoft, industry partners, academia and law enforcement around the world remain commited to fighting them. Together, we can stop criminals from using botnets to wreak havoc online and create a safer more trusted Internet for everyone.

Guidance: Defending Against Malicious and Potentially Unwanted Software

Effectively protecting users from malware requires an active effort by both organizations and individuals. It’s important to maintain up-to-date antimalware defenses and to stay informed about the latest developments in malware propagation techniques, including social engineering.

For in-depth guidance, see the following resources in the “Mitigating Risk” section of the Microsoft Security Intelligence Report website:

- Promoting Safe Browsing
- Protecting Your People

If you believe your computer may be infected by Rustock or other type of malware, we encourage you to visit support.microsoft.com/botnets for free information and resources to clean your computer.

For updates, and current activities on Rustock botnet visit: http://blogs.technet.com/b/microsoft_on_the_issues/

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security