Conficker and Beyond: A Large-Scale Empirical Study

SUCCESS LAB



Contents

- Background
- Introduction
- Measurement Results
- Limitation
- Summary



Background

- Botnet
 - Collection of bots, which runs automatically to perform malicious operations
 - Most serious threat
- Why is it serious?
 - Bot-master (owner of the Botnet)
 - has Power
 - to control huge amount of machines
 - has Motivation
 - to earn some money



Image from wikipedia



Understanding Botnet

• Why is it needed?

 If you know the enemy and know yourself, you need not fear the result of a hundred battles.

from Art of War

- If we know Botnet, we can
 - Discover its current trend
 - Predict its future trend
- This will give us clues to detect/prevent botnet
- Main goal of this paper
 - To understand current powerful Botnet



Our Target

Conficker

- Why?
 - The most recent and powerful
 - Nov. 2008
 - Known as infected more than 10 million PCs
 - They are still active
 - Several companies/organizations are trying to remove it

February 13, 2009

Microsoft's \$5,000,000 Reward for Microsoft Collaborates With Industry to D By JOHN MARKOFF Published: January 22, 2009



By Richard Grigonis Executive Editor, IP Communications Gro

Back in 2003, Microsoft (News - Alert) est: capture renegade programmers of compl helped finger 18-year old German compu Sasser worm - so named because it sp the German authorities

Conficker Worm

Microsoft offers \$250,000 reward for Conficker arrest and conviction.

REDMOND, Wash. - Feb. 12, 2009 - Today, Microsoft Corp. announced a pa technology industry leaders and academia to implement a coordinated, global re Related Conficker (aka Downadup) worm. Together with security researchers, Internet (Do We Need a New Internet? Assigned Names and Numbers (ICANN) and operators within the Domain Name (February 15, 2009) coordinated a response designed to disable domains targeted by Conficker. Micr announced a \$250,000 reward for information that results in the arrest and conv

responsible for illegally launching the Conficker malicious code on the Internet. Service) component of Windows XP and Windows 2000 operating systems — who was ultimately arrested and sentenced by

SUCCESS LAB, Texas A&M University

Top News

Virus strikes 15 million PCs

Published: Jan. 26, 2009 at 10:34 AM

Artide Listen



WASHINGTON, Jan. 26 (UPI) -- A virulent computer virus has infected as many as 15 million computers around the world so far, according to various estimates.

The virus -- a self-replicating computer worm known as Downadup, Conficker or Kido -- spreads across computer networks using Microsoft Windows software which have not been patched or updated properly. Microsoft issued a patch that fixes the vulnerability the virus exploits last

Worm Infects Millions of Computers Worldwide

E TWITTER

A new digital plague has hit the Internet, infecting millions of personal and business computers in what seems to be the first step of a multistage attack. The world's leading computer security experts do not yet know who programmed the infection, or what the next stage will be.

> In recent weeks a worm, a malicious software program, has swept through corporate, educational and public computer networks around the world.

Known as Conficker or Downadup, it is spread by a

recently discovered Microsoft Windows vulnerability, by guessing network passwords and by hand-carried consumer gadgets like USB keys.





Related Work

- Conficker binary analysis
 - SRI [porras et al.,]
 - Analyze several variants of Conficker binary
 - Reveal how it,
 - infects victims, evades detection, updates itself and etc.
 - Honeynet Project [watson et al.,]
 - Analyze Conficker binary
 - Provide scanning tools for detecting Conficker victims
- Conficker victim analysis
 - CAIDA [<u>http://www.caida.org/research/security/ms08-067/conficker.xml</u>]
 - Show Conficker victim's propagation (location)
 - Cymru [kristo et al.,]
 - Display Conficker victim's distribution on the Internet



What We Want To Provide

- What we want to provide in this work
 - Large-Scale analysis of Conficker victims
 - around **25,000,000 victims**
 - More detailed analysis of Conficker victims
 - *Cross-comparison* with previous popular bots/worms
 - Cross-checking current detection systems
 - Other notable characteristics of Conficker victims



Data Collection

Our Collection : 24,912,492 unique IP address of Conficker victims

Malware	Туре	Data source	Collection time
Conficker	Bot	Sinkhole server Shadowserver.org	Jan.1, 2010 - Jan.8, 2010

ACKNOWLEDGEMENT : We thank Shadowserver.org and Chris Lee for providing the data of Conficker

Previous Data for Comparison

Malware	Туре	Data source	Collection time
Botnet 1 [Ramachandran et al.,]	Bot	Sinkhole server	Aug. 2004 - Jan. 2006
Botnet 2 [Xie et al.,]	Bot	Hotmail	Jun. 2006 - Sep. 2006
Botnet 3 [Xie et al.,]	Bot	Spamhaus	Nov. 2006 - Jun. 2007
Waledac [Stock et al.,]	Bot	Infiltration into Waledac	Aug. 2008 - Sep. 2009
CodeRed [Moore et al.,]	Worm	Measurement	Jul. 2001 - Oct. 2001
Slammer [Moore et al.,]	Worm	Measurement	Jan. 2003
Witty [Shannon et al.,]	Worm	Measurement	Mar. 2004

Who Are Victims ?



Distribution Over IP Address Space



Result : Conficker victims are concentrated in several specific IP address spaces

Insight : We may need to monitor a limited number of specific ranges of network, not the whole network, and it might be more efficient



Distribution Over ASes - 1

ASN	# Host	AS Name	Country
4134	2,825,403	CHINA-BACKBONE	China
4837	1,435,411	CHINA169-BACKBONE	China
7738	385,672	TELECOMUNICACOES	Brazil
3462	280,957	HINET	Taiwan
45899	273,577	VPNT-AS-VN	Vietnam
27699	260,848	TELECOMUNICACOES	Brazil
9829	248,444	BSNL-NIB	India
8167	237,465	TELESC	Brazil
3269	231,020	ASN-IBSNAZ	Italy
9121	207,849	TTNET	Turkey

Result : Top 2 ASes account for 28.37% of all victims and top 20 ASes cover 52.16% Insight : Focusing on specified ASes may be an efficient way to detect malware



Distribution Over ASes - 2

Conf	icker	Bonet 1		Botnet 2		Botnet 3	
ASN	Country	ASN	Country	ASN	Country	ASN	Country
4134	China	766	Korea	4134	China	4766	Korea
4837	China	4134	China	4837	China	19262	USA
7738	Brazil	1239	USA	4776	Australia	3215	France
3462	Taiwan	4837	China	27699	Brazil	4837	China
45899	Vietnam	9318	Japan	3352	Spain	4134	China
27699	Brazil	32311	USA	5617	Poland	No info.	No info.
9829	India	5617	Poland	19262	USA	No info.	No info.
8167	Brazil	6478	USA	3462	Taiwan	No info.	No info.
3269	Italy	19262	USA	3269	Italy	No info.	No info.
9121	Turkey	8075	USA	9121	Turkey	No info.	No info.

Result : Top 2 ASes were also sources of previous botnets, but other ASes are newly emerged

Insight: Infection Trend is changing

SUCCESS LAB, Texas A&M University





Distribution Over Domain Names

Con	ficker	ker CodeRed		Slammer		Witty	
Top Level	Percentage	Top Level	Percentage	Top Level	Percentage	Top Level	Percentage
unknown	48.81	unknown	47.22	unknown	59.49	net	33
br	8.83	net	18.79	net	14.37	com	20
net	8.65	com	14.41	com	10.75	unknown	15
cn	6.94	edu	2.37	edu	2.79	fr	3
ru	5.01	tw	1.99	tw	1.29	са	2
it	2.36	јр	1.33	au	0.71	јр	2
ar	1.54	са	1.11	са	0.71	au	2
in	1.35	it	0.86	јр	0.65	edu	1
com	1.21	fr	0.75	br	0.57	nl	1
mx	1.16	nl	0.73	uk	0.57	ar	1

Result : .net domain is still prevalent, but new CC (country code) domains have recently emerged Insight : Watch out ! Newly registered domains

SUCCESS LAB, Texas A&M University



Distribution Over Bandwidth



Result : Most victims use ADSL or Modem, and low bandwidth networks are more likely to have more Conficker victims Insight : Hosts with ADSL or Modem connections are still vulnerable

SUCCESS LAB, Texas A&M University

Reputation-based Detection Systems



Reputation-Based Detection Systems

- Reputation-based detection system
 - Detect malicious hosts or networks based on their reputation
 - How to get the reputation
 - By using their previous records
 - Did they host malicious web sites ?
 - Did they send spam emails ?
 - Did they try to scan network ?
 - E.g.,
 - DNS blacklist
 - FIRE [http://maliciousnetworks.org/]
 - Dshield [<u>http://www.dshield.org/</u>]
- Question
 - How well do they detect Conficker infected hosts ?



DNS Blacklist

- What we have tested
 - DNSBL, SORBS, Spamhaus, and SpamCop
 - Query all 24,912,492 hosts to them
 - 4,281,069 hosts are on blacklists (only 17.18%)

Insight : Unfortunately, DNS blacklists are not enough to detect Conficker victims



FIRE And Dshield

- FIRE
 - Detect malicious ASes
 - Most heavily infected ASes by Conficker are not shown in the top 500 malicious ASes of FIRE
- Dshield
 - Detect malicious hosts or ASes
 - 82,856 (only 0.33%) hosts and 83 ASes (only cover 0.2% of victims) are reported by Dshield as malicious

Insight : FIRE and Dshield did not detect large portions of Conficker victims as well. We may need other complementary detection approach such as anomaly detection

Watch Your Neighbor



Infection Preference

- Conficker infection vectors
 - Infecting random hosts by
 - Random network scanning
 - Infecting nearby hosts by
 - Scanning local subnets
 - Infecting portable storage (USB storage)
- Which approach is more effective ?
 - Some research points out "infecting nearby hosts" is more dominant [Krishana et al.,] [Porras et al.,]
- Question
 - Is "infecting nearby hosts" really dominant ?



Test For Neighborhood Infection - 1

- Definition
 - *Camp*: group of /24 subnets whose /16 subnet is the same and locations are close together
 - Neighbor: each /24 subnet in the same Camp is a "Neighbor" to each other





Test For Neighborhood Infection - 2



and this represents each /24 network in the Camp has similar number of infected victims



Test Results

Within distance	# of all "Camps"	# of "Camps" whose /24 subnet members are similar to each other (VMR < 1)
~ 100km	85,246	62,121 (72.87%)
~ 200km	65,748	44,633 (67.88%)
~ 300km	54,415	36,495 (67.06%)

Insight : From this result, we think that a large portion of victims are infected by their neighbor hosts



Can We Use This More ?

- Based on this knowledge, we propose a *Conficker prediction approach*
 - Employ K-NN (K-Nearest Neighbor) (K = 3, in this experiment)
 - Detection granularity
 - /24 subnet
 - Define class
 - Benign : /24 subnet which does not have any infected hosts
 - Malicious : /24 Subnet which has Conficker infected hosts
 - How to define nearest
 - Physical Distance between each subnet





Detection Result

- Data for training and evaluation
 - 20 % for training (randomly selected)
 - Other 80 % for evaluation

Detection Accuracy	TP rate	FP rate	
91.59 %	91.65 %	8.5 %	

Insight : Watching neighborhood can help us predict unknown malicious networks

And this insight implies that further research is needed for developing new detection/defending approaches based on co-operated/shared information



Limitation And Discussion

- Dynamic IP address or NAT(Network Address Translation)
 - Each reported IP may not represent unique victims
 - However, we believe that our observation can show overall characteristics or statistics of Conficker victims



Summary And Future Work

- Summary
 - Observe around 25,000,000 Conficker victims data to show their identities
 - Compare previous bots/worms and show the difference among them
 - Check current reputation-based detection systems
 - Propose a prediction/early warning approach of Conficker infected networks
- Future Work
 - Analyze more Conficker data
 - Compare with more data (other recent bots)



Q & A





References

- [1] SRI-International. An analysis of Conficker C. <u>http://mtc.sri.com/Conficker/addendumC/</u>
- [2] D. Watson. Know Your Enemy: Containing Conficker. http://www.honeynet.org/papers/conficker
- [3] CAIDA. Conficker/Conficker/Downadup as seen from the UCSD Network Telescope. <u>http://www.caida.org/research/security/ms08-067/conficker.xml</u>
- [4] J. Kristo et al., Experiences with Conficker C Sinkhole Operation and Analysis. In Proceedings of Australian Computer Emergency Response Team Conference, May 2009
- [5] A. Ramachandran and N. Feamster. Understanding the Network-Level Behavior of Spammers. In Proceedings of ACM SIGCOMM, Sep. 2006
- [6] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldzmidt, and T. Wobber. How Dynamic are IP Addresses? In Proceedings of ACM SIGCOMM, Aug. 2007
- [7] Y. Xie, F. Yu, K. Achan, R. Panigraphy, G. Hulte, and I. Osipkov. Spamming Botnets: Signatures and Characteristics. In Proceedings of ACM SIGCOMM, Aug. 2008
- [8] B. Stock, M. E. Jan Goebel, F. C. Freiling, and T. Holz. Walowdac Analysis of a Peer-to-Peer Botnet. In Proceedings of European Conference on Computer Network Defense (EC2ND), Nov. 2009
- [9] D. Moore, C. Shannon, and K. Calffy. Code-red: a case study on the spread and victims of an internet worm. In Proceedings of ACM SIGCOMM Workshop on Internet Measurement, Nov. 2002
- [10] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. Inside the Slammer Worm. In Proceedings of IEEE Security and Privacy, May 2003
- [11] C. Shannon and D. Moore. The Spread of the Witty Worm. In Proceedings of IEEE Security and Privacy, May 2004
- [12] S. Krishnan and Y. Kim. Passive identification of Conficker nodes on the Internet. In University of Minnesota -Technical Document, 2009.
- [13] P. Porras, H. Saidi, and V. Yegneswaran. A Foray into Conficker's Logic and Rendezvous Points. In *Proceedings of USENIX LEET, Apr. 2009*