“SandStorm” –attack

*“The ~~answer~~ **problem** is not in the box, it’s in the band.” – AntiTrust*

Author: Dennis Rand – 2012

Table of Contents

Introduction

Although the malware sandboxes have been demonstrated attacked in several ways, this paper will show new attack concept named "SandStorm".

The first generation of Sandbox[1] technologies for analyzing malware was a very strict and run in closed environment, where the actual malware execution often was done on emulated OS and services rather than on real systems.

The threats have evolved over the years and malware is becoming more and more dependent on internet access to communicate with a C&C server either to download additional components or configurations, and without this information the analyst will be missing a big piece of the puzzle. The sandbox technology has evolved to cope with the new malware threats.

This paper will have primary focus on binary analysis systems, however the attack sources are much wider, and a solution will come with a price.

[1] Read "Appendix Sandboxing history"

SandStorm - the concept

The SandStorm –attack is concept of attacking sources on the internet by using various online systems, such as unknown binary analysis system as also will be demonstrated in this paper however the attack sources are much wider, and the concept are on using online available systems to perform the attacks towards the internet.

In short malware analysis/behavior sandboxes used to give a fast indication on what a given binary are doing are begin used as the attack platform towards an arbitrary target chosen by the attacker.

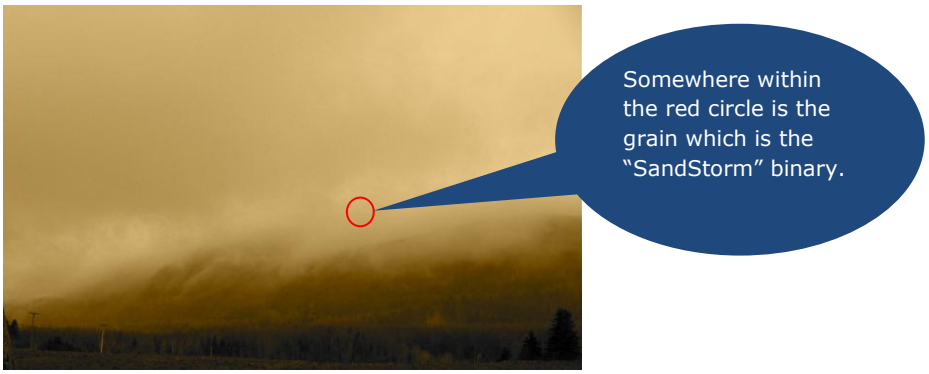
This also results in all traces going back towards the company owning the IP address space from where the binary was executed; Looking at this from an attackers perspective can in some cases be an advantage in case that the company being targeted has implemented a reputation filter in some sort of network filtering device, It would be unlikely that reputation filters have added e.g. large security companies on a block list, and there could even be a possibility that some are whitelisted.

It is vital that companies implementing solutions either public or none public for analyzing e.g. unknown binaries have done a risk assessment on consequences if their company was targeted by a "SandStorm" –attack, looking at it both from a reputation and economical point of view.

It is common that sandboxes should protect and filter outgoing attacks however as the "Proof of Concept" will show this is not a point that are often implemented, resulting in attacks being executed.

Why "SandStorm"

The analogy are that the online systems used as relays in the attacks receive a Sand Storm of samples/url's/etc. every day, and trying to filter out the ones with a different purpose than what the system was designed to analyze are more or less impossible; and that was why it is dubbed "SandStorm" –attack.



Sources of attacks

SandStorm can be performed by relaying from a various set of solution as the attack platform.

- **Online Antivirus Scanners (*Jump station*)**
  - Online AV-systems are interesting since they tend to share wide on the samples they scan, meaning that the SandStorm –attack could/will be executed from none public sandboxes.

- **Mail submission (*Jump station*)**
  - The attack can be used towards companies where it is likely that the binary will be executed in a sandbox environment, in itself it is not executing binaries or URL's but more looked upon as a jump-station.

- **Online Malware/Unknown binary analysis systems**
  - PE (Microsoft) [2]
  - ELF (*nix)
  - APK (Android)
  - CCI (iOS)

- **Online URL Scanners**
  - URL Scanners who are created to detect malicious content on a site can be used to perform attacks.

[2] PE Binaries are used in the test cases shown later in the paper.

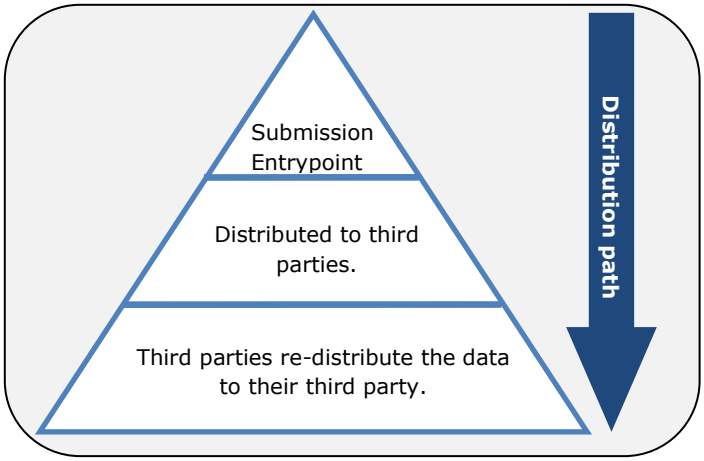
Attack scenarios

This paper will focus on 2 types of attack scenario these are "Stand-alone" and "Distributed"

Jump Station - Mail/Online submission

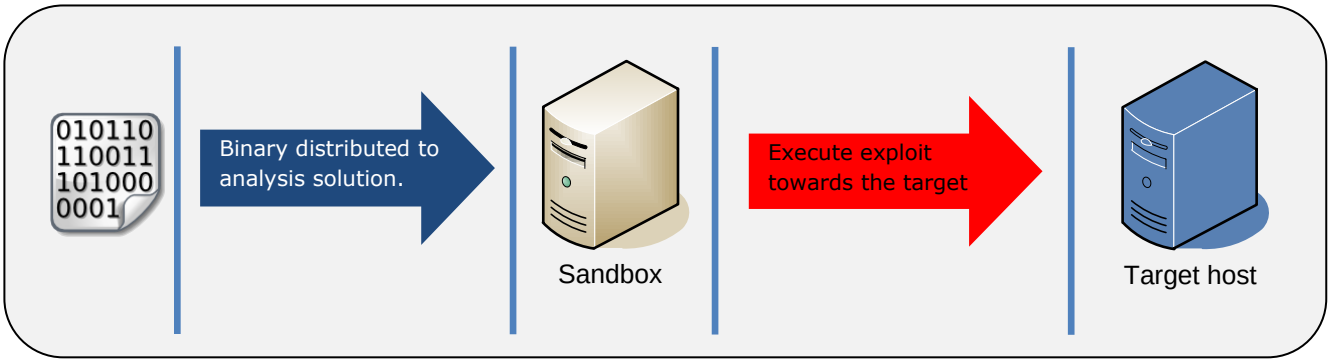
The usage of Mail or Online submission systems that are not directly executing the sample but more a jump station to binary or web scanning technologies.

The advantage of using a jump station are that you enter either you binary or URL in one location and it will be distributed wide depending on the system of choice.



Scenario 1 (Stand-alone - Sandbox)

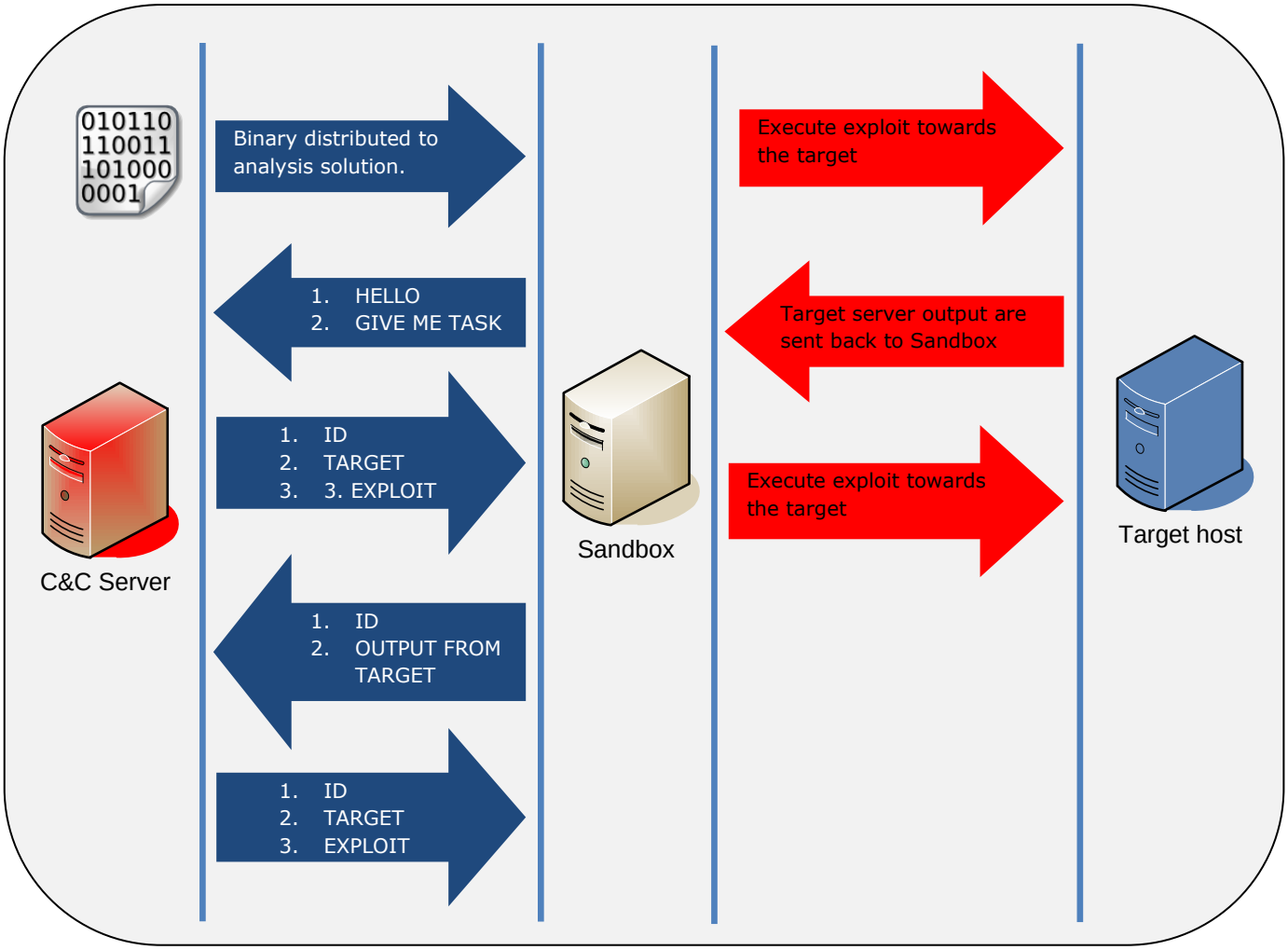
All information are included in the binary created for the attack, so there are no need for any infrastructure from the attackers point of view, it is a "fire-and-forget" type of attack, this means that unless there is a specific IPS rule to stop the specific attack it will be successful.



Scenario 2 (Distributed - SandBox)

The second way is to build a distributed scanning/attack vector where the binary are only acting as a "Relay" meaning it will fetch information on what to do from a Command & control server that will provide:

- Target
- Exploit



Proof of Concept

While the "SandStorm" –attack concept is interesting in theory, It was also vital go gain knowledge if this was possible to perform in a real world scenario.

In the Proof-of-Concept I decided to only test PE supported systems focusing on Windows executables, no vendors will be named in this paper.

Test cases

The Proof-of-Concept was divided into 4 test cases

Test case	Description
1	Loop connection request every 10 seconds
2	Loop connection request every second.
3	Stand-alone attack
4	Distributed attack

3 types of entry points was chosen for the binaries all-in-all **46** unqiue entry points was attempted at the beginning of the tests, and the only systems who "passed" meaning connected out were allowed to pass on to the next level of test case.

Amount	Description
12	Online sandbox systems
15	Online antivirus scanning systems (Single and Multi scanners)
19	Mails to Malware submission systems

Some of the systems are protected with Captcha meaning that it would not directly be possible to push a massive amount of "SandStorm" binaries onto the system, however the stand-alone attacks would still be possible for a successful run, due to the "one-shot-one-kill".

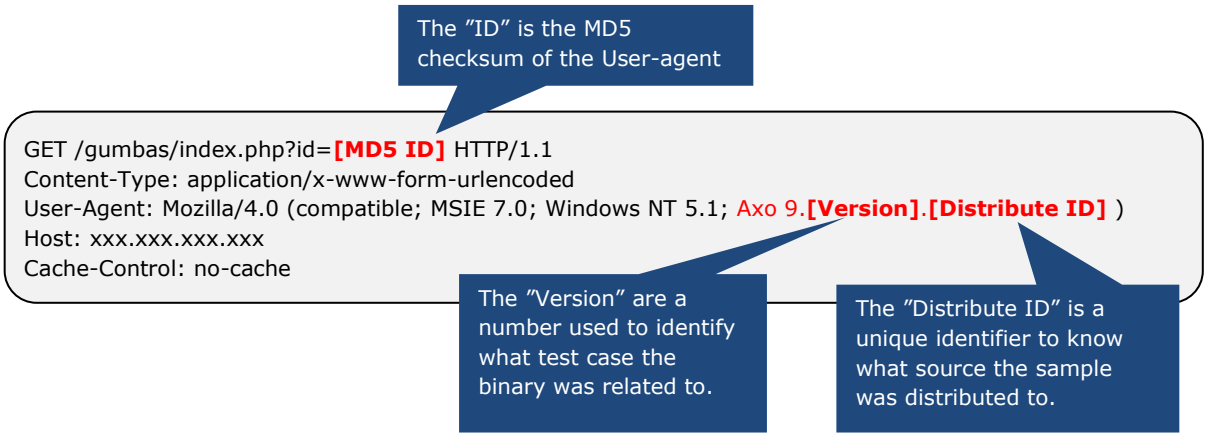
Every binary in the tests was tagged in an attempt to be able to identify where it originally was distributed to and what variant.

Attack scenario 1 – Anyone home

The first "SandStorm" –attack test was performed with a simple HTTP GET request that was looped every 10 seconds with the below request.

Data flow description of binary in test case 1

The packets looked like the below



The samples were distributed to all 46 sources that were pre-chosen before the test started.

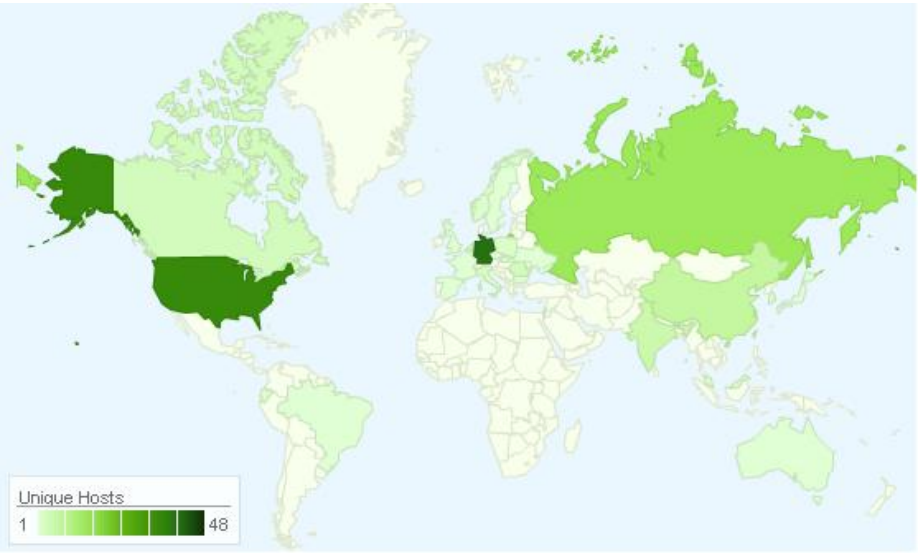
Who came back

During the run 18 binaries of the 46 that was distributed was seen connecting back to the C&C server. The binaries was executed in both raw un-manipulated for as well as in many cases a manipulated "replay".

Unique ID	AV scanner	Sandbox	(M)ail/(W)eb submission	Unmanipulated	Manipulated
1	X		W	X	X
2		X	W		X
3		X	W		X
4		X	W	X	X
5		X	W	X	
6	X		W	X	
7		X	W	X	X
10	X		W	X	
17		X	W	X	X
25		X	W	X	X
26		X	W	X	
27		X	W	X	
29	X		M	X	X
31	X		M	X	X
32	X		M	X	
33	X		M	X	
36	X		M	X	X
45	X		M	X	X

Unique IP's connections

During the run[3] 173 unique IP's was seen connecting back to the C&C server[4], distributed over 28 different geographical locations.



Country	Unique IP's
DE	48
US	41
RU	18
A1	11
CN	8
IN	6
NL	5
RO	4
CA	4
IT	3
NO	2
TW	2
PL	2
EC	2
MY	2
SK	2
KR	2
FR	1
BG	1
JP	1
BR	1
CZ	1
AU	1
GB	1
ES	1
UA	1
SE	1
IL	1

Unique IP's seen

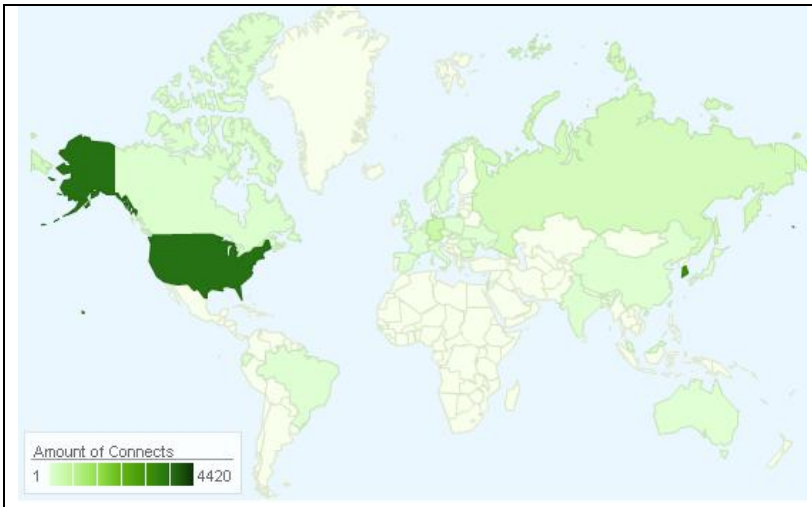
The binary code executed on the sandboxes had a build in delay timer looping every 10 seconds, interestingly there was seen some executions where the loop timer was removed, making the code executed in a fast stream this could lead to a DoS and DDoS depending on how many that use this vector.

[3] First seen connections 2012-04-14 00:02:41 (UTC+2) C&C shutdown on 2012-05-23 02:41:38 (UTC+2)

[4] 11 of the IP's were not possible to geo-locate and are marked as A1(Anonymous proxy entries) from the MaxMind DB

Connections received

During the attack with "binary 1" the server received 9316 connections over a timespan of little less than 40 days; however the primary connections were based on the day where the binary was uploaded and the main amount of connections are from US and Korea.



Country	Connections
US	4420
KR	3630
DE	497
RU	295
A1	85
CA	73
RO	69
BG	53
MY	53
NL	35
CN	20
IN	20
NO	15
SK	13
PL	8
FR	7
CZ	4
BR	3
TW	3
IT	3
EC	2
ES	2
JP	1
AU	1
IL	1
UA	1
SE	1
GB	1

Total connection based on country

Connections	Day	Month
4701	14	April
211	15	April
874	16	April
411	17	April
343	18	April
46	19	April
763	20	April
222	21	April
11	22	April
3	23	April
1	24	April
8	25	April
61	26	April
17	27	April
26	28	April
40	29	April
787	30	April

Connections a day

Connections	Day	Month
5	1	May
12	2	May
386	3	May
2	4	May
2	5	May
4	6	May
3	7	May
16	8	May
2	9	May
17	10	May
31	11	May
3	12	May
3	13	May
3	14	May
2	15	May
4	16	May
237	17	May
19	18	May
2	19	May
33	20	May
2	21	May
2	22	May
1	23	May

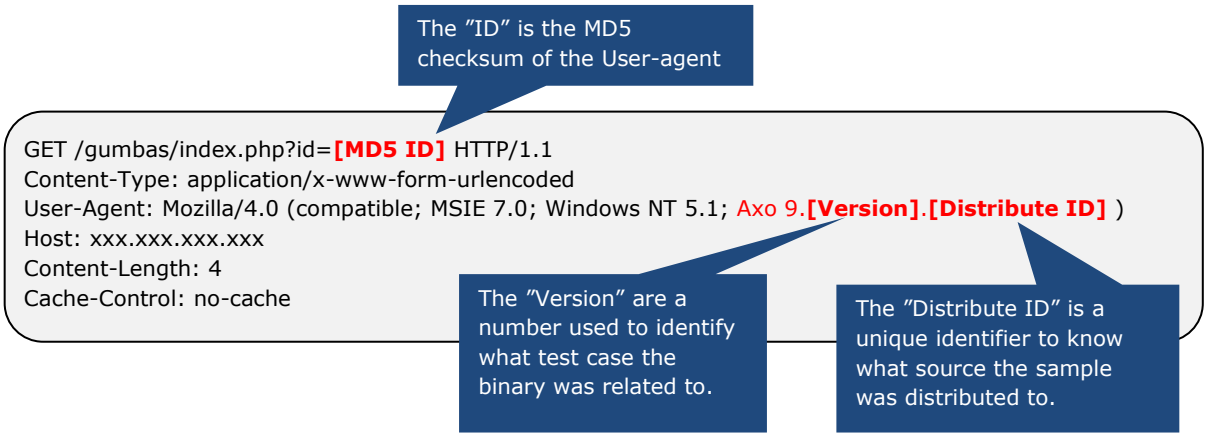
Connections a day

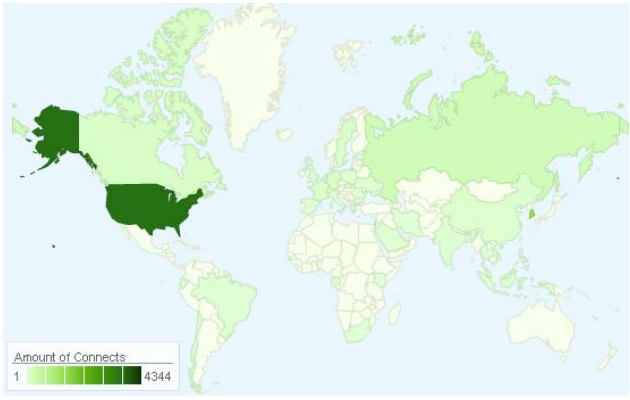
Attack scenario 2 – How many will you play with

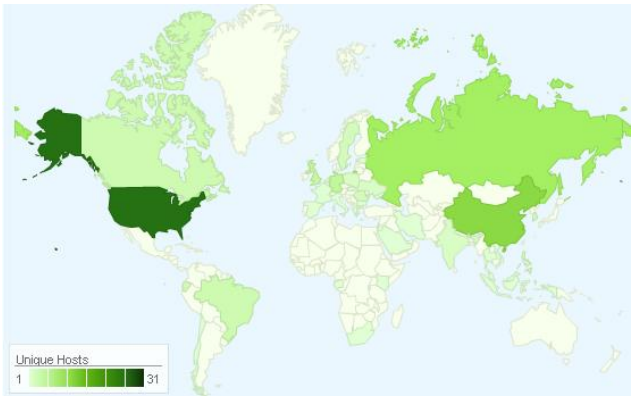
The second test case was to attempt to identify if there were any filters in sandbox solutions that would filter out Denial-of-Service (DoS) attacks.

Data flow description of binary in test case 2

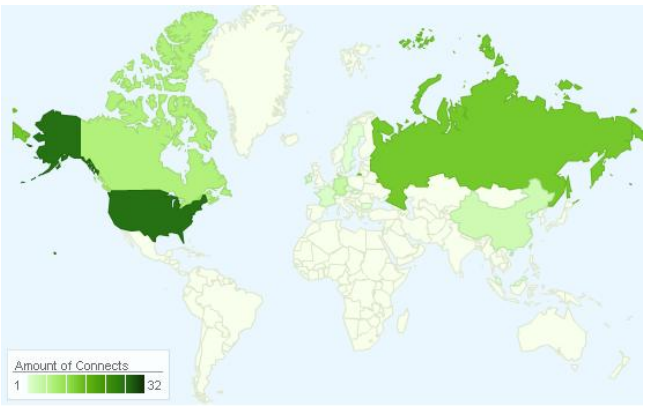
The packets looked like the below

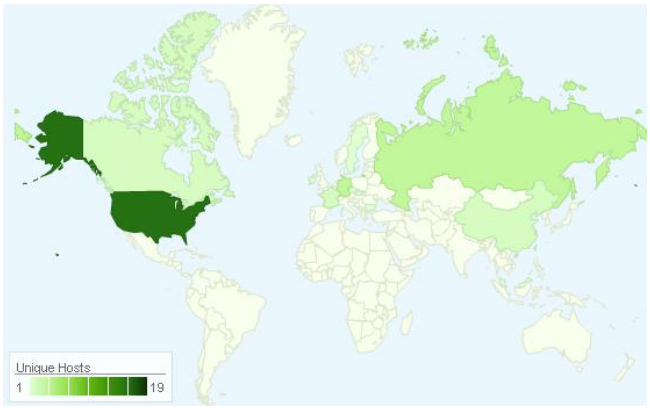




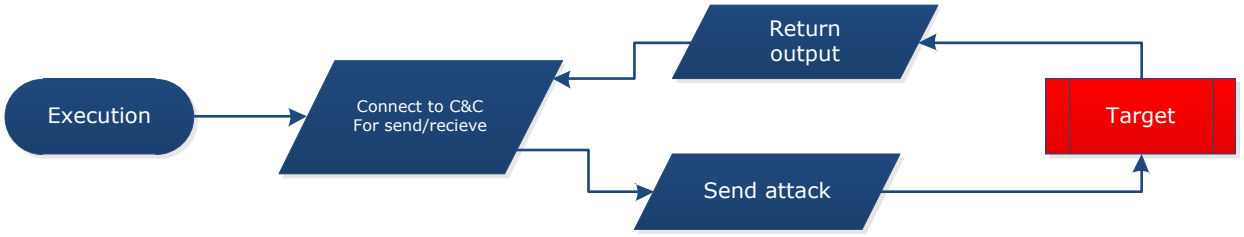


Attack scenario 3 – Fast in fast out





Attack scenario 4 – What are thy bidding, my master?



Appendix

Sandboxing history

Online sandboxes and services for analyzing unknown binaries are widely used to do an dynamic analysis of the binary to identify the run-time behavior as well as being used to attempt to detect a possible malware family, this is a faster way to "scratch" the surface of a binary to identify if it is possible or malicious or somewhere in between.

Many of the online services lets the binary be executed in a real operating system environment either on virtual or physical hardware and are open to the internet, meaning that if the file attempts to connect to a service on the internet this is allowed to also capture the internet traffic connected to. The original thought on a sandbox was a closed environment that would keep the malware inside to ensure that it did not propagate outside the analysis network.

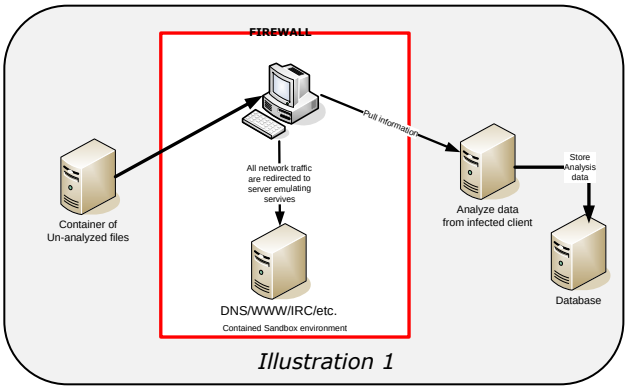


Illustration 1

The threats have evolved over the years and malware is becoming more and more dependent on internet access to communicate with a C&C server either to download additional components or configurations, and without this information the analyst will be missing a big piece of the puzzle. To comply to the new scenario more and more sandboxes allows the unknown binary to be executed and connect out on the internet however adding some form of filtering. The level of filtering is managed by the owners of the sandbox.

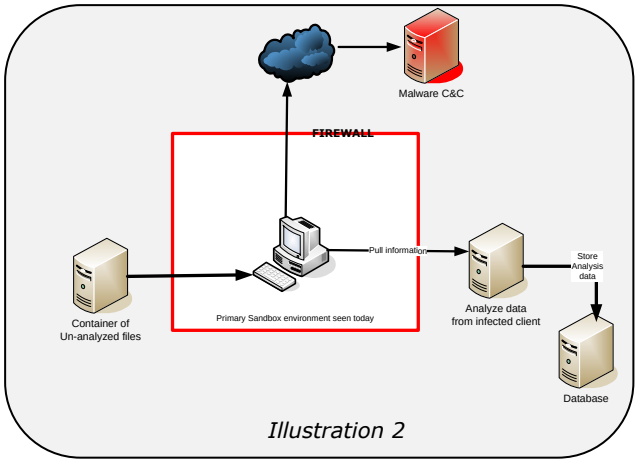


Illustration 2

Binaries used in test cases

Below is a list of the binaries distributed throughout this research paper, these binaries was ONLY designed to connected/attacked IP/Domains owned by the researcher of this paper.

MD5's for attack scenario 1

3DCD60225256BB03B3ED5D82A4949A9E
230576DB1B5811821B72417725C21855
B04864886B2E0425C2461F8C06F9DEDA
D2CAF524D8969CFF1A4A3AF8B58FD449
8DE95BBFA2B1DCEA1DB648BF0FF13AA2
35F9DC35955144EC2E7BA79108B8087F
826AD164580566626EC10F655D4697D6
D1B5548573C62B168B8893E89534FD69
7B39187BA330417C68BD0E119106D621
0412FD6DA9E4B64B95A76DED58E76255
0E83AD789CE672AF566BE0388AB2AB1E
48DEDCC4D71B5FFB4C2C413FFBA92B99
3378FDB38D1FE18D0E776AB3BFCBBF11
14C5C10B31917A37FC2312D3017EA030
3CE65E9D45277093E5C3E3A5FCD12949
B200146DAD053111C8FDB7A655B37F0A
3A69F1F422C2CBC976F727587264C63A
BCEA1BF49AF0C57BA462F604F8EED094
0CF9F278E6EDDED3D25DB3AE8FB79C6E
4BE63E2848B5A7E1F7E065F8E250DE2B
A3E0C7BE36983BA04CEA2792E2E45D55
9D401627294E4659981C58347EF63AFE
14103F58778D8D8C4C8A5E9FE8260958

549FA9379DD7C23F2B7DC403389B039C
2741346B5DEF1E580491D2E4F1B05A38
CC4F7F6A0E728F51EDDD8DC0F1B8A1A5
F4E19A465C147CCFE8116EF7D54BFA76
994BF9EFEA18D81BB737107411A05673
2254F7DACCFF65ADB28787811FD80D35
D77439D58060D00CF10DF0355E2EDB68
8708D9C93FCBA87898BAC2FE74A79035
3C72B5DC8C7023D3ED7D5D6182BC7961
F4BC81852ED8D27D512734E512C676F9
99536F42F46E071016A9D8555286ACAD
C4610E7C2A78E13F44E10CA0B5A6747C
4DB53418F8D77D26DEA82E5165F14B2B
0EDA70D279804E3AD0BCCD8A264F2C68
81AFD2237CC6C8E7B3495319CD0B3AB6
E502BF425329DAB1D0F5DCD8D3D93274
414795801C87C8F0E812C751C885FE4E
680C12EF942DF9E03C7C8C31CACA8D04
FD3302DF720A9BDB75D5111CB0147BC4
31081047F4F17FE1A9BDB072FB21897E
E960448B20BA444B93B814D42B60E5BE
C62F0A390579189E317F9AB44B73732D
BA6D59EEEC1FB20FF7B9FDCE9E5B9B4F

MD5's for attack scenario 2

B247556BF79ECA35B59C2996C06DE76E
DF22028C2EC1081178F755099176927D
2F7C1A7A0656CA3B724964C898BB162C
74961F7A177DB148039B3CAE6E07330C
A48F4BA16FB13B9FD0DB1391192018E3
0C8585F8B2713CF03DA01CD4F8C0994C
39BF5009607181B2AADDF929D07B5AC7
1B95AF5E941C78CAEA5B5CC7F0FDE96E
F020882D300A4E4FB12F503171AF17EC

95DB58808F5CF64420CE8993DFE681A0
40586E6ED57D631B57E4360E0BE9F87F
1699A43AD86419BD10B94C1A5BF49F69
63E6A831C1A52E72D3980A3D8A27DC5D
31D33F0C2B903729F855BF295B2EABCD
7129F9DA7D6527E7DCE24FCE4224F377
0D259F95F521A655F588781CAD7530AB
247F7433BEB232512CE120D93B95E93F
2F0B66C3F53AC5816841504D98BB0EC

MD5's for attack scenario 3

71AE08C20287BE717F1D5BA1E5311F55
BE43E2753B054A2EDBC9555D97A67C88
946D6656A1BE4CE0A71F01603A0B0526
8BEB888268B7E88B3FDC7483BE5138FB
CC87FB968CBF37B15C97660A8C7154EF
B73C2B5AC514018BDA3B2A572D95C53A
F772DCB72CBEEB19A312C0A30A41389C
87316E4F965677AD880F04C2F731A4E2
2274B1E50D135CDC0719C0DBAFC316B8

416B695742DE57C8EED6E4A706B1D2A3
03D7025D6351DB9B35441E2A99AE1263
2146BF8C4828CE2E6124534707F27A3F
DBE5DEAD6C9E4744BF14D01776936CAB
0B918DCF545AA3554EC298DBEC5F30FC
29F5DB33EB0327E89379F733B6F4A26A
863B0A5A8DDC4A9CA1E2EE84E637E34C
28C4F01704C69DC5A76F30E684DE3E2A
1DBEEB581F701810D880F497A17CB2D2

MD5's for attack scenario 4

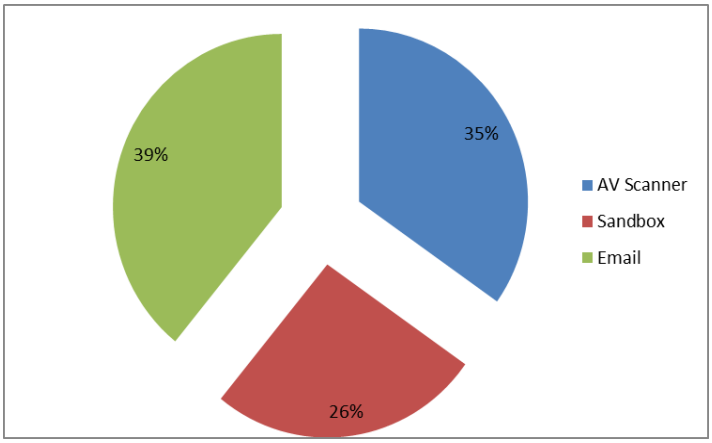
08A54E2B51706B5BF0F10216B4EE08D1
0D2A49B2BCFFDA779AE96137A1C971E9
1756CC6C0412EBB4338D3CD2685540AF
3349042C7B3B237066107589076A769E
3C876680C8653EA45B06E1DC0979EF7F
3F70F1E32DA7D6DA11265635507F2C46
4B13A5E30EE37B09FCD44EB6C0ACFEEE
580DFEB862F30DEE539AF18E57F4D588
5DB7FD777AF348E2DC86B167302CDDBD

6F39730F2A2835AE4C7B6F01AC0C8308
94F614D506C01FAE0D5B24FE15C23328
974EFA10674D27D30A0840D59CAAAEC2
CCCA2F329B506A878796EF2A036BEA4C
D00DA5BDE1FC33622B81A2BF4CC8D630
D35B173ECA526578684CC34E40E617AF
EBA57E8D19ABB029A28C3FF484BEA14C
EDDA98AE26D23381E70F030221373339
F8D4812980C6474A61C570E4D8DA02DE

Sources defined

Every source choosen are mentioned as a number below + adding if it is an "Online AV Scanner", "Online sandbox" or through "Email" distribution.

Unique ID	AV scanner	Sandbox	Mail
1	x		
2		x	
3		x	
4		x	
5		x	
6	x		
7		x	
8	x		
9	x		
10	x		
11	**x**		**← DEAD**
12	x		
13	x		
14		x	
15		x	
16		x	
17		x	
18	x		
19	x		
20	x		
21	x		
22	x		
23	x		
24	x		
25		x	
26		x	
27		x	
28	x		
29	x		
30			x
31			x
32			x
33			x
34			x
35			x
36			x
37			x
38			x
39			x
40			x
41			x
42			x
43			x
44			x
45			x
46			x
47			x



Acknowledgements

A special thanks to the following people for helping with ideas, review, thoughts and insights:

- Tonny Bjørn
- Mikael Vingaard
- 364K

References

[1] Execution Context in Anti-Malware Testing, David Harley BA CISSP FBCS CITP – ESET

[2] Man, Myth, Malware and Multi-Scanning
David Harley, ESET N. America
Julio Canto, VirusTotal/Hispasec Sistemas

[3] Creating a Malware analysis Laboratory
Francisco Jesus Monserrat Coll
IRIS-CERT / RedIRIS
FIRST TC /COLARIS ,Montevideo UY. NOV 2008

[4] A Survey on Automated Dynamic Malware Analysis Techniques and Tools
MANUEL EGELE
Vienna University of Technology
THEODOOR SCHOLTE
SAP Research, Sophia Antipolis
ENGIN KIRDA
Institute Eurecom, Sophia Antipolis
and
CHRISTOPHER KRUEGEL
University of California, Santa Barbara

[5] Vulnerability in Public Malware Sandbox Analysis Systems
E-ISBN : 978-0-7695-4107-5
Print ISBN: 978-1-4244-7526-1

[6] Sandbox Analysis with Controlled Internet Connection for Observing Temporal Changes of Malware Behavior
Katsunari Yoshioka , Takahiro Kasama, and Tsutomu Matsumoto
Yokohama National University,
Tokiwadai, Hodogaya,
Yokohama, Kanagawa 240-8501, Japan
yoshioka@ynu.ac.jp

[7] Toward Automated Malware Response for Trustable Network
Katsunari Yoshioka
Yokohama National University

http://ec.europa.eu/information_society/activities/foi/research/eu-japan/eujapan3/docs/yoshioka.pdf

[8] SQL injection: More of the same
by Johannes Ullrich (Version: 1)
http://isc.sans.edu/diary.html?storyid=4565

[9] inj3ct0r
http://www.1337day.com/
http://www.1337day.com/exploits/18141
http://www.1337day.com/exploits/18135
http://www.1337day.com/exploits/18125
http://www.1337day.com/exploits/18033
http://www.1337day.com/exploits/17984
http://www.1337day.com/exploits/18071
http://www.1337day.com/exploits/16861

[10] A Year in Review: Statistics on attacks against Hawaii companies
http://www.issahawaii.org/download.cfm?ID=31551