National College of Ireland

Malware Analysis: rainbowmagic

FileVersion 1.0.0.1
Report

for
Niall Heffernan

by
Rohan Bhangale (x18147119)

Contents

01 Executive Summary

From the time of inception of Trojan Malware, there has been development in many variants and types of Trojan. A trojan is a malware which is disguised as legitimate software, in order to bypass defense mechanism against malware. Once Trojan is activated, it can block, delete, modify, copy and disrupt computing and network performance.

In this report, analysis of Rainbow Magic malware is conducted, demonstrating how the malware affects system (Windows) by using techniques such as bypassing OS protections, using anti-reversing tricks, stealing sensitive information such as documents and login credentials and encrypting data on the system for ransom. Analysis is drafted using malware analysis tools such as Cuckoo Sandbox, JoeSandbox, VirusTotal and Any.run also the report contains analysis of network traffic(*pcap file*) obtained from a passive network tap using Wireshark, PacketTotal. Furthermore, report specifies recommendations for defenses against the malware. Lastly the Appendix holds screenshots from analysis supporting the report.[6]

02 Identification

Sample Analyzed: Unknown.exe @ 2019_NCI_Project_infected.zip

File Metadata File Name: Unknown.exe

File Type :PE32 executable (console) Intel 80386, for MS Windows, UPX compressed

File Size : 368.0KB

MD5: 25d562f46c14c5267d56722f6a43b8ed

SHA1: 7cd4d6f44bdb71d24574d0b4bc326abd006eb510

SHA256:a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615

SHA512:02f4829f913fcc4d93d8bcf80f1be95fed7249351ec8022fe99ded7c6437e62e0a224db86411717d35db7c8e497933e4633970c46205622358d75172a95ae7ae
File Type: 32-bit Windows executable

CRC32: 30DC4FAC

ssdeep:6144:XR/o988gWaraDqRrgwKzBe31i4SgfHysWTx92ltFc87t1VEaj:B+lmRrg wK0lRysiG+Utt

Name	AV
TROJ_DROPPER.XXTXG	TrendMicro
Mal/Generic-S	Sophos AV
Ransom.TeslaCrypt	Symantec
Generic.ml	Palo Alto Networks
Trojan:Win32/Tiggre!rfn	Microsoft
Ransom.FileCryptor	Malwarebytes
Trojan-Ransom.Win32.Blocker.jyqs	Kaspersky
W32/Blocker.JYQS!tr	Fortinet
Ransom:Win32/Blocker.a3d3eaf9	Alibaba

Source: VirusTotal [7]

Yara: UPX - (no description)

- suspicious_packer_section - The packer/protector section names/keywords
- UPX - (no description)
- win_registry - Affect system registries
- Str_Win32_Wininet_Library - Match Windows Inet API library declaration
- Str_Win32_Internet_API - Match Windows Inet API call

Source: Cuckoo Sandbox [4]
As per the classification of malware, it is a possible case of Evader, Ransomware or Spyware.

03 Setup

Malware Lab Setup

Introduction

Analysis of a Malware requires an isolated lab, in order to study the execution and behaviour of the Malware in a contained environment, as not to infect the production system. In order to do this, virtualization software is used. Added advantage of snapshots is achieved i.e. basically images of VM in a given point of time to which it can be restored.

Setting up Virtual Machine (VMware)

Given the variety of Virtualization tools available, VMware was chosen by me because of user-friendly GUI Console and the ability to take multiple snapshots. During the analysis of the Malware, execution of the Malware will take place on the Windows Virtual Machine, use of VM because it can be reverted back to a clean state while it would not be possible to achieve the same using a physical machine.

Step 1: VM Setup

Victim VM: Windows 7 x86

- Here Windows 7 OS is chosen as the subject malware(Petya) affects Windows Platform.
- Configuration: Windows 7 x86 (32 bit); 4GB RAM
- Snapshot: For restoring stable state after a malfunction. A Snapshot is taken of the fresh installation while it is still clean, it looks at the state of registry and file system.

REMnux VM

- For reverse-engineering malicious software, as it has various tools for malware analysis, for external analysis.
- Simulating Virtual Network Gateway for Victim Machine for monitoring network behaviour of the malware
- Updating tools present in REMnux

```
sudo update-remnux full
sudo reboot now
```

- Snapshot is taken for regressing to stable state
- Configuring **inetsim.conf** with sudo privileges for starting DNS service and binding IP address

Flare VM

- For local tools on Windows 7(Victim) Machine, for local analysis
- On IE, script is executed using ActiveX or using Powershell for downloading repository from Fireeye.

Step 2: Network Setup

- ➔ Blocking Host System's communication with the Virtual Machine(i.e isolating the virtual machine from the production machine) by using dedicated network for managing acquisition of malware in the system.
- ➔ Setting up isolated network by creating a custom network (Static IP) with a dedicated network adaptor, assigning both Windows 7 and REMnux VM to it.
- ➔ Configuring network adaptor on Windows 7 to REMnux IP address for Default Gateway IP and Preferred DNS IP.

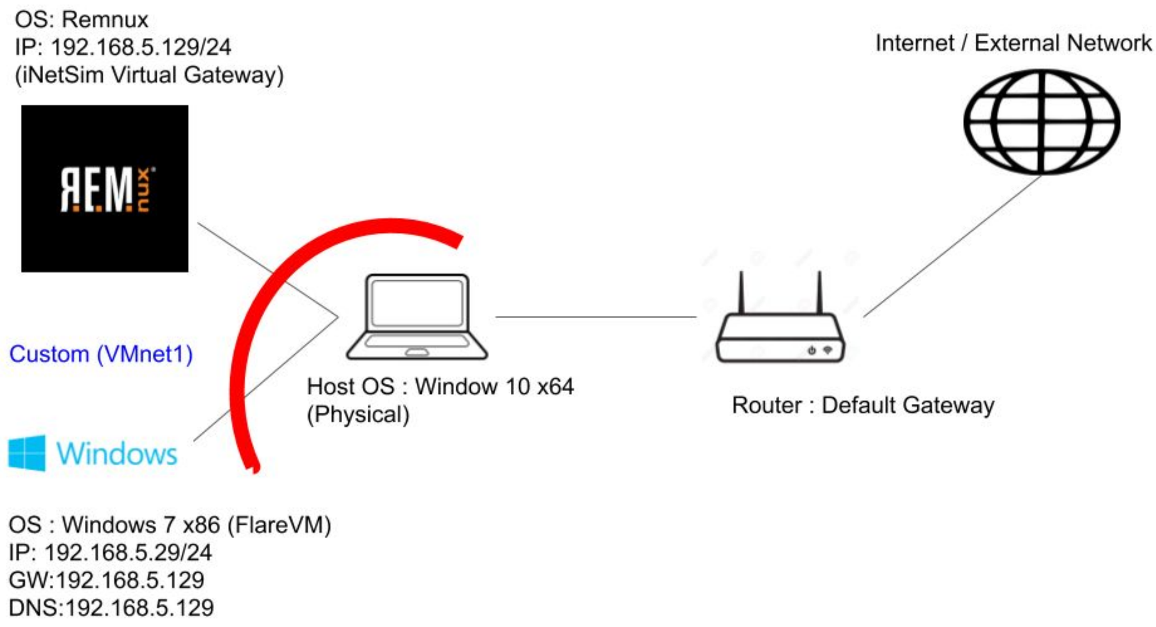


Figure : Network Diagram for Malware Lab

Step 3: Lab Testing

- ➔ Connectivity check using PING tool for Windows 7 and REMnux
- ➔ iNetSim status, check through victim browser
- ➔ Check for No Connectivity between the Host and Virtual Machine
- ➔ Turn off Firewall and Updates for Windows 7
- ➔ Make Hidden files visible and lower security measures

Step 4: Malware Analysis Tool

For learning behaviour of malware,

- ➔ Monitoring System Processes: For understanding the workflow of any execution during the process lifecycle, using tools such as Windows Process Explorer(for monitoring system resources),SysInternal suite, RegShot(for changes made to registry), Process Monitor(for real time changes made to file system) etc.

- ➔ Network Traffic Analysis: For analysing network traffic when malware communicates with external network, using tools such as Wireshark, netcat and FakeNet-NG.

- ➔ Detecting Local Changes: Basically for understanding what changes happen on the disk and the memory, using tools such as OSSEC, TRIPWIRE, AFICK.

- ➔ Debugger: For understanding state of execution within a program like changes made to memory locations, registers and arguments required, using tools such as OllyDbg, x64dbg, Windbg.

- ➔ Online Tools: VirusTotal,Malwr,ThreatMiner, Joe Sandbox. (for detail research)

04 Methodology

At the time of performing malware analysis, the malware lab was not attached to the external network except for the lab network. Malware was obtained from moodle.ncirl.ie. Malware lab was kept isolated from the host/production environment. Malware lab consists of Windows Client (Victim), Remote Linux Server(DHCP,DNS,tcpdump) and Cuckoo Sandbox(for the required tools for malware analysis). A baseline of the system was taken before executing the malware, in order to run comparison of the infected system with baseline system. Snapshot was taken ensuring Host-Only network.[8]

Static Analysis(Code):

Initial step of malware analysis was to run it against various AV scans. After scanning, malware was opened in Hex-Editor for identifying malware type and to determine if malware attempts to use packer application like UPX. UPX for unpacking applications and decompression of the file. A copy of malware was made as repacking the uncompressed file may not function properly. Applications (Wireshark,Windows Process Explorer, Process Monitor and RegShot) for monitoring system and network for insightful information such as protocols, ports, files, IP addresses, processes etc were used to understand the inner workings. Malware was then disassembled for reviewing calls made to DLL and system changes done by malware.

Dynamic Analysis(Behavioral):

For analysing the behavior of malware, it was executed on the system and the changes it made were monitored. It was made sure that patches and fixes were installed on the VM before execution. Tools such as *ResourceMonitor,TCPEye and WinPcap* are installed for understanding the flow of background processes, for monitoring if a new listener is installed on the system, if it tries to access tools such as telnet, netcat or browser. For monitoring if any backdoor is being installed. [8]

Internet Investigation(OSINT: Open Source Intelligence):

The Internet is a significant instrument for wide range of investigations and intelligence gathering. Which include research carried on Trojan, Ransomware and Extender, whitepapers by cybersecurity consultancies such as *SANS Institute, Cisco, Symantec, Norton*. Online Static and Dynamic analysis was carried out using online sandboxes such as *JoeSandbox, VirusTotal, CuckooOnline and Any.run*. Online sandbox provide safer environment and comprehensive reports from the publically submitted information.

05 Analysis

In this study of malware **RAINBOWMAGIC**, it was observed that malware is designed to work as a Trojan. The code is written is C/C++ programming language. Once the program is initiated it delays the analysis by 3x Sleep call for process. After that, the code runs GetAdaptersAddresses function to fetch addresses associated with adaptors present on the local machine. The malware then tries to load library which is not installed on the local machine. It has executable files which are compressed using UPX, which acts as a strategy to escape detection by AntiViruses. It contains functionality to download files from the internet. It contacts web servers via HTTP. Performs DNS lookups. It then adds an entry in the startup folder/Startup which are programs which get executed once the user logs, it gives persistence to the malware. The malware then deletes its own executable file and binaries, by being present on the RAM, as defense evasion. It then modifies the WPAD proxy for intercepting traffic by getting the listing of IP addresses that will be used by the malware for the lateral movement. The malware copies files from one system to another for placing adversary tools over a course of operation.These adversaries tools try to fetch security software, configurations, defensive tools installed on the system. These tools are controlled through the Control and Command channels to bring other tools into the victim network.Encryption standards are employed to conceal C&C traffic. Malware specifies some DLLs which take advantage of legitimate program which are vulnerable to side loaded malicious DLL. It also holds functionality to load and extract PE file embedded resources and ability to enumerate files inside a directory. Malware also holds functionality to check kernel debuggers. Also contains functionality to query CPU information and local system time.

For the dynamic analysis of the malware was done in an isolated environment, so that the malware does not affect the network and production/host machine. However given risk involved in the analysis. Hence for the analysis, JOE SANDBOX and CUCKOO SANDBOX were used. It was observed how the malware works and its propagation in the system and network. The malware file *Unknown.exe,* identified as rainbowmagic.exe and tries to connect with IP addresses, urls and domains. Then this IP address establishes connection with two communicating files(WIN32 Executable), for url opens and establishes connection to **http://definitely-not-evil.com/** and the contracted domains lead up to websites for downloading content.

On execution of the malware on a windows architecture, it initiates execution of unknown.exe, which later initiates processes to execute **dope.exe** (PE32) and

dope.exe:Zone.Identifier. Zone.Identifier is a type of file which is used by windows to manage security settings and generally kept hidden[5]. While the initiated dope.exe calls for **http://definitely-not-evil.com/** through a browser and simultaneously runs conhost.exe, after which dope.exe deletes itself. **Conhost.exe** is an important Windows process[1], related to **csrss.exe** (ClientServer Runtime System Service) and **cmd.exe** (Command Prompt) processes. The malware also imports libraries which are capable of obfuscating their behaviour, fetching variables from DLLs; conversion of formatted string into an array of bytes; closing handle of specified registry keys; freeing block of task memory; displaying message dialog box and functions initializing use of wininet for applications.

06 Network Traffic Investigation

The resultant traffic was stored in a pcap file which is a dump file for the traffic collected. The pcap file was analysed with wireshark and packettotal.
From the analysis, it can be seen that the sender IP is 192.254.234.118 and target IP is 192.168.122.62 which resolves to HTTP Hostname www.floridablueline.com which redirects to 46.30.45.65 which resolves to good.recycle2learn.com.The traffic observed is facilitating communication for network trojan which has alert signatures indicating 8x8 script; privacy violation; exploit URI; payload URI and cryptowall. An executable file is downloaded via 46.30.45.65 which remotely installs x-shockwave-flash which is used to pop malverts on the victim system, while various DNS are replicated from the sender IP for flashing various malvertises through the flash installed.

07 Recommendations

- URL filtering and use of defenders with comprehensive understanding and awareness of policies and controls.
- Disable remote registry services on all the systems in the organisation
- Keep software up-to-date with patches, fixes and updates.
- Use of Firewalls, AV, IDS and IDPS.
- Implementing Defense in depth and diversity
- Implementing the principle of least privilege to minimize exposure.
- Implementing Role Based Access Control
- Monitoring email attachments and scanning for viruses on them.
- Disable autoruns
- Frequently changing passwords
- Regular backups and recovery points
- Checking SSL for ecommerce sites
- Implementing Incident Response Plan as per SANS and NIST, for containment of the breach.

08 Conclusions

Various attack vectors are observed which revolve around the identified ***magicrainbow.exe*** malware which are extender, trojans, malvertising, ransomware. In future, for a more detailed understanding dynamic analysis on a redundant stand alone machine can be conducted to gain deep understanding over the malware. The approach used in this malware study is hybrid which involved running dynamic analysis on a sandbox environment over cloud and use of publically available data on the subject rainbow magic malware. It was learned that the malware is produced by **Rainbow Magic, Inc.** and has originated from domain **definitely-not-evil.com.**

09 References

[1]

"Conhost.exe: What Is It and Why Is It Running in My Task Manager," *Driver Easy*. [Online]. Available: https://www.drivereasy.com/knowledge/what-is-conhost-exe-in-task-manager/. [Accessed: 17-Aug-2019]

[2]
"Automated Malware Analysis Report for Unknown.exe - Generated by Joe Sandbox." [Online]. Available: https://www.joesandbox.com/analysis/163609/0/html. [Accessed: 17-Aug-2019]

[3]
"Free Automated Malware Analysis Service - powered by Falcon Sandbox." [Online]. Available:
https://www.hybrid-analysis.com/sample/4461dd9180efe2779ba2cdf3774b27f5d21ed5818b3957ae2c855f0276f838c3. [Accessed: 17-Aug-2019]

[4]
"Cuckoo Sandbox." [Online]. Available: https://cuckoo.cert.ee/analysis/1182866/summary/. [Accessed: 17-Aug-2019]

[5]
“File Extension .ZONE.IDENTIFIER Information.” [Online]. Available: https://pc.net/extensions/file/zone.identifier. [Accessed: 17-Aug-2019]

[6]
“Untitled.” [Online]. Available: https://www.kaspersky.com/resource-center/threats/trojans. [Accessed: 17-Aug-2019]

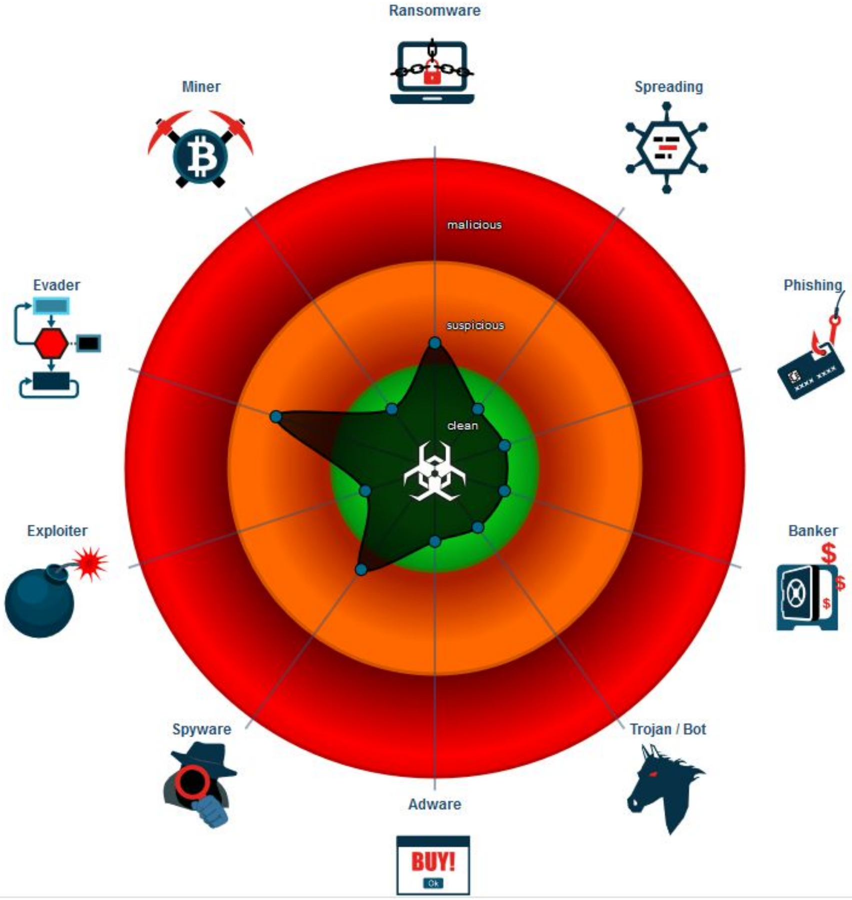
[7]

“VirusTotal.” [Online]. Available: https://www.virustotal.com/gui/file/a635f37c16fc05e554a6c7b3f696e47e8eaf3531407cac27e357851cb710e615/details. [Accessed: 17-Aug-2019]

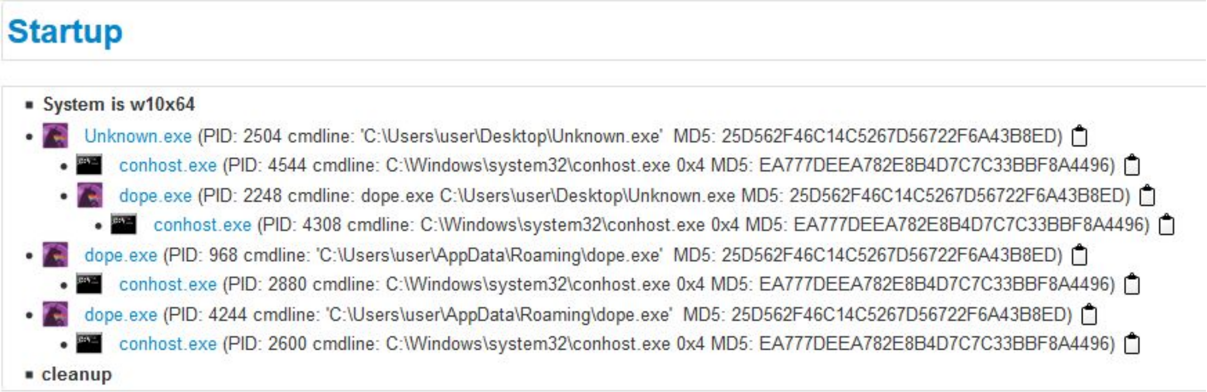
[8]

“SANS Institute: Reading Room - Malicious Code.” [Online]. Available: https://www.sans.org/reading-room/whitepapers/malicious/malware-analysis-introduction-2103. [Accessed: 17-Aug-2019]

10 Appendix



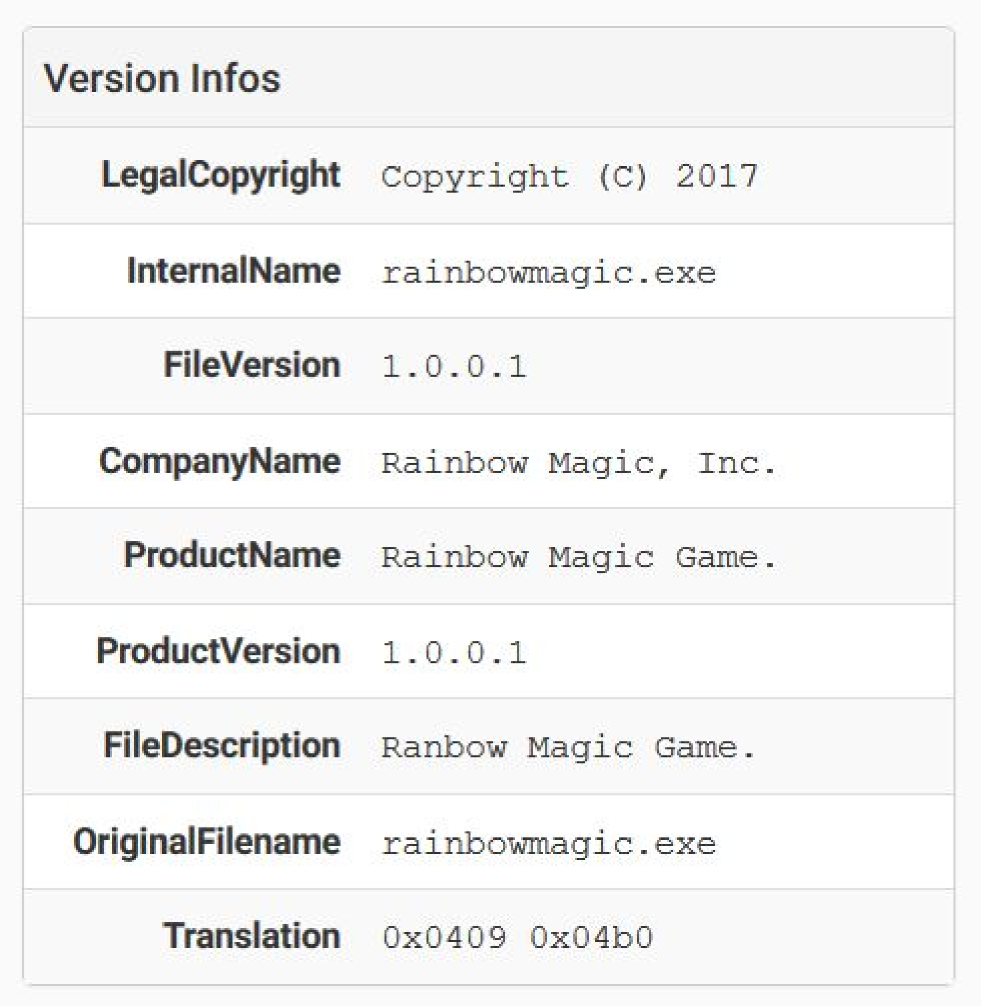
Classification of Malware Source: JoeSandbox



Startup

- System is w10x64
- Unknown.exe (PID: 2504 cmdline: 'C:\Users\user\Desktop\Unknown.exe' MD5: 25D562F46C14C5267D56722F6A43B8ED)
  - conhost.exe (PID: 4544 cmdline: C:\Windows\system32\conhost.exe 0x4 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dope.exe (PID: 2248 cmdline: dope.exe C:\Users\user\Desktop\Unknown.exe MD5: 25D562F46C14C5267D56722F6A43B8ED)
    - conhost.exe (PID: 4308 cmdline: C:\Windows\system32\conhost.exe 0x4 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dope.exe (PID: 968 cmdline: 'C:\Users\user\AppData\Roaming\dope.exe' MD5: 25D562F46C14C5267D56722F6A43B8ED)
  - conhost.exe (PID: 2880 cmdline: C:\Windows\system32\conhost.exe 0x4 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dope.exe (PID: 4244 cmdline: 'C:\Users\user\AppData\Roaming\dope.exe' MD5: 25D562F46C14C5267D56722F6A43B8ED)
  - conhost.exe (PID: 2600 cmdline: C:\Windows\system32\conhost.exe 0x4 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

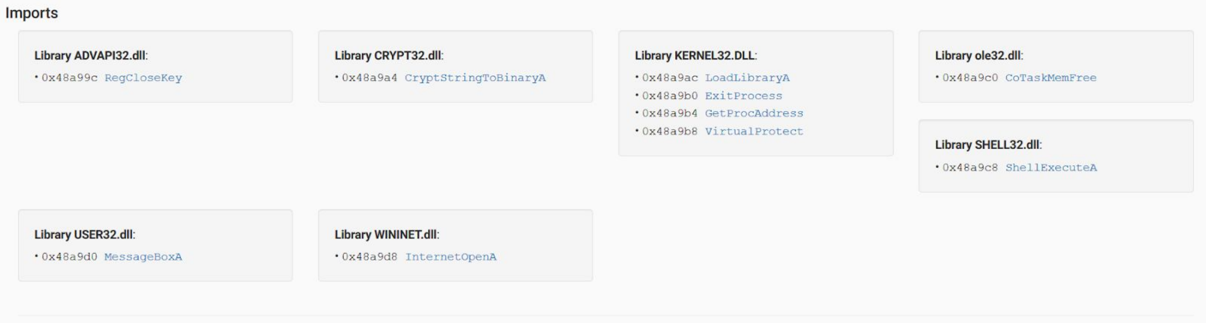
Process Execution Flow Source: JoeSandbox



Version Infos

LegalCopyright	Copyright (C) 2017
InternalName	rainbowmagic.exe
FileVersion	1.0.0.1
CompanyName	Rainbow Magic, Inc.
ProductName	Rainbow Magic Game.
ProductVersion	1.0.0.1
FileDescription	Ranbow Magic Game.
OriginalFilename	rainbowmagic.exe
Translation	0x0409 0x04b0

Malware Identification Source: Cuckoo Sandbox



Imports

Library ADVAPI32.dll:
- 0x48a99c RegCloseKey

Library CRYPT32.dll:
- 0x48a9a4 CryptStringToBinaryA

Library KERNEL32.DLL:
- 0x48a9ac LoadLibraryA
- 0x48a9b0 ExitProcess
- 0x48a9b4 GetProcAddress
- 0x48a9b8 VirtualProtect

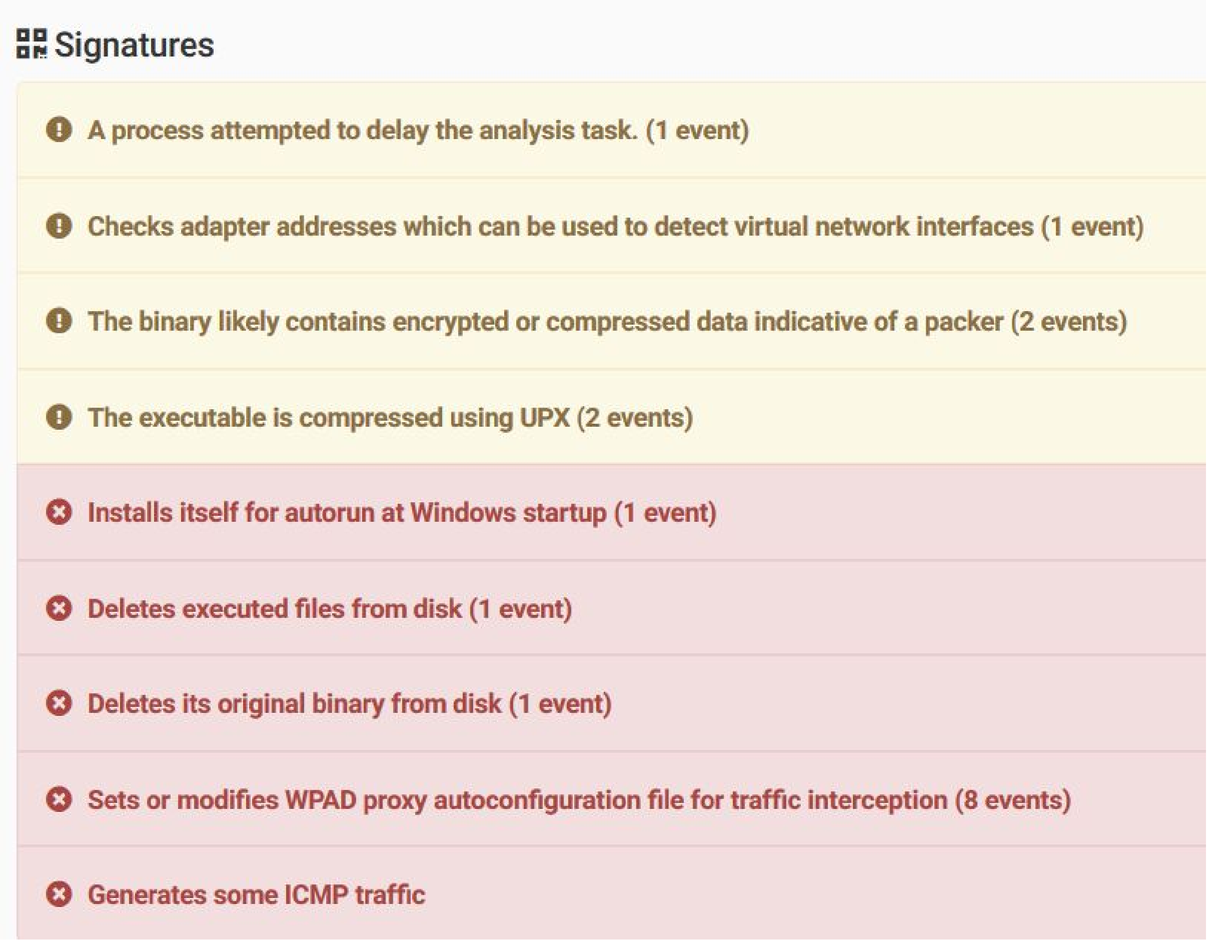
Library ole32.dll:
- 0x48a9c0 CoTaskMemFree

Library SHELL32.dll:
- 0x48a9c8 ShellExecuteA

Library USER32.dll:
- 0x48a9d0 MessageBoxA

Library WININET.dll:
- 0x48a9d8 InternetOpenA

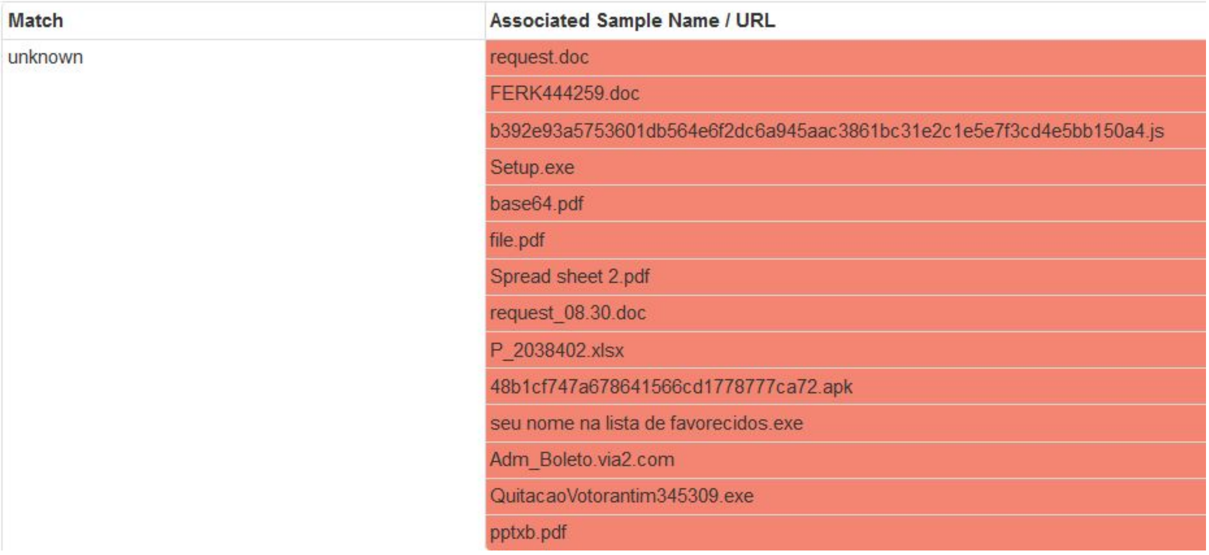
Library Imports Source: Cuckoo Sandbox



Signatures

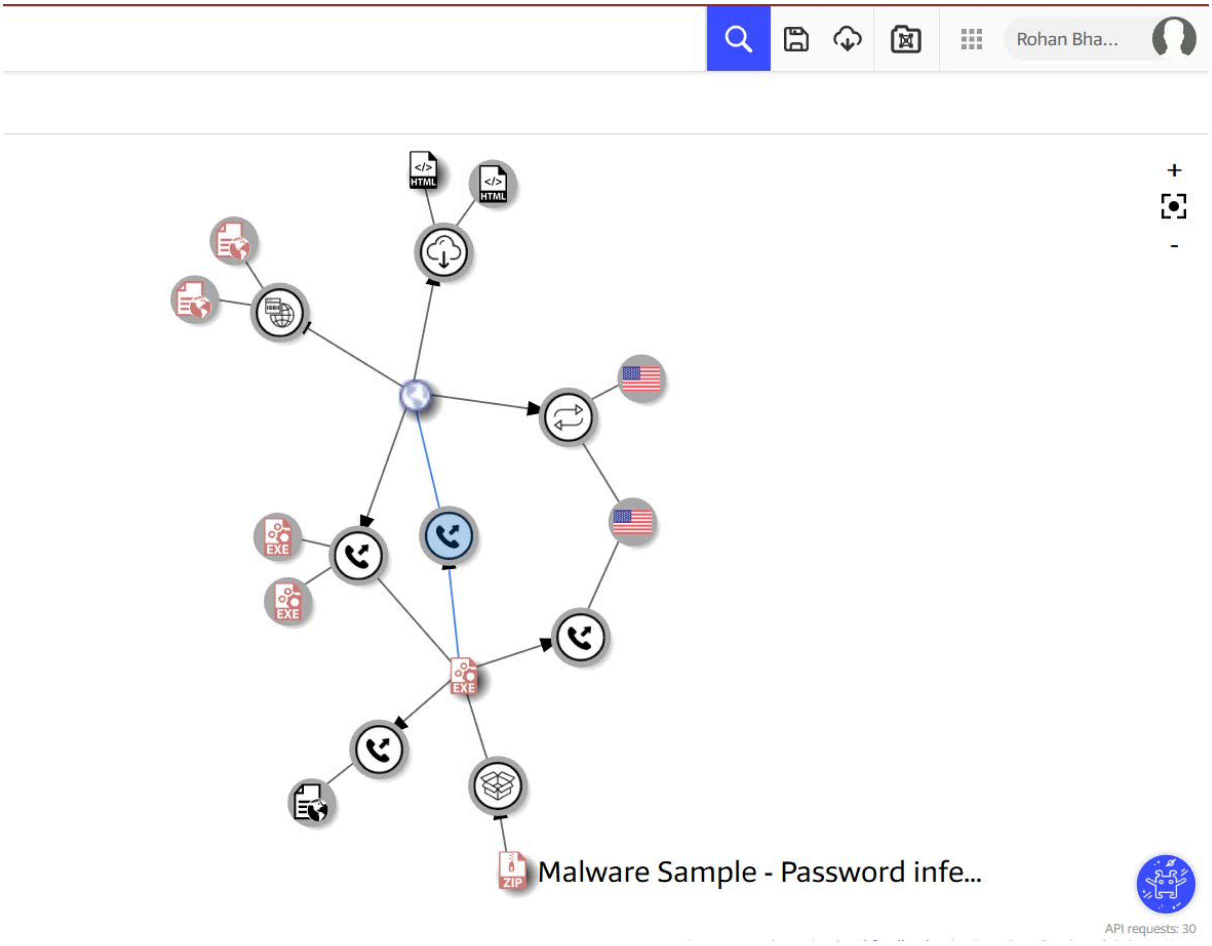
- A process attempted to delay the analysis task. (1 event)
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- The executable is compressed using UPX (2 events)
- Installs itself for autorun at Windows startup (1 event)
- Deletes executed files from disk (1 event)
- Deletes its original binary from disk (1 event)
- Sets or modifies WPAD proxy autoconfiguration file for traffic interception (8 events)
- Generates some ICMP traffic

Signature Activity Source: Cuckoo Sandbox

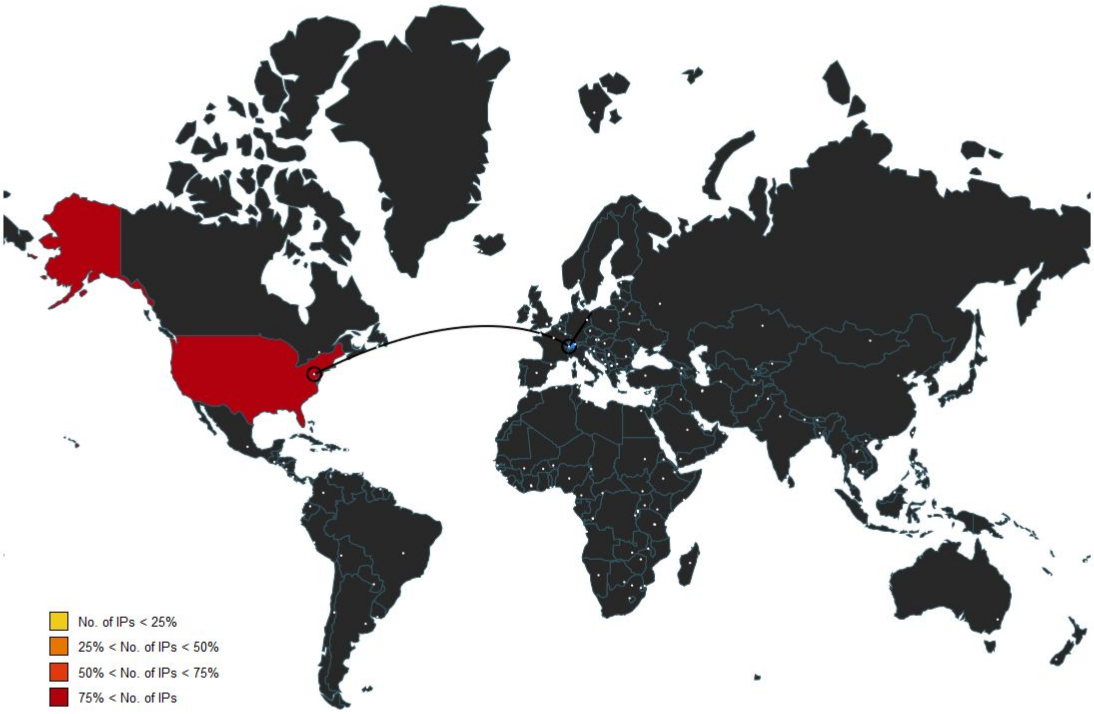


Match	Associated Sample Name / URL
unknown	request.doc
	FERK444259.doc
	b392e93a5753601db564e6f2dc6a945aac3861bc31e2c1e5e7f3cd4e5bb150a4.js
	Setup.exe
	base64.pdf
	file.pdf
	Spread sheet 2.pdf
	request_08.30.doc
	P_2038402.xlsx
	48b1cf747a678641566cd1778777ca72.apk
	seu nome na lista de favorecidos.exe
	Adm_Boleto.via2.com
	QuitacaoVotorantim345309.exe
	pptxb.pdf

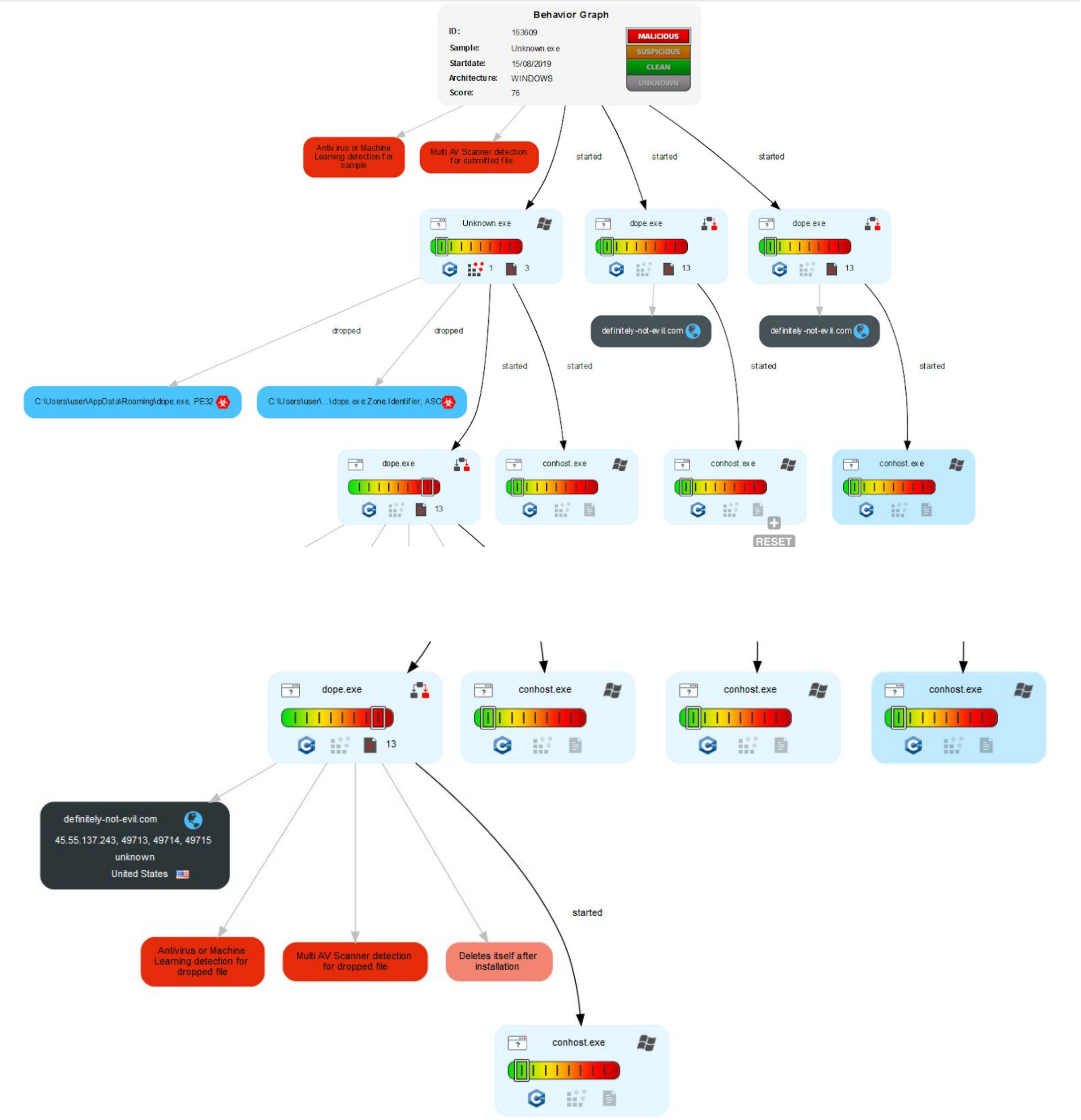
File Matches Source: Joe Sandbox



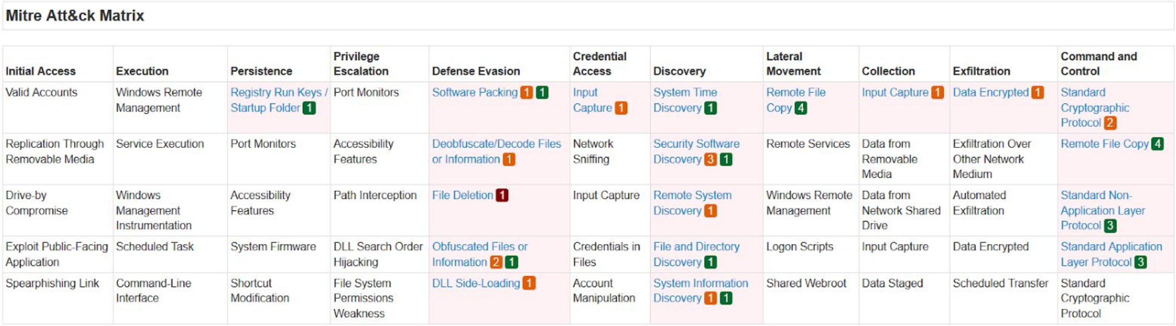
Malware Spread Graph Source: VirusTotal



Geographic Spread Map Source: JoeSandbox



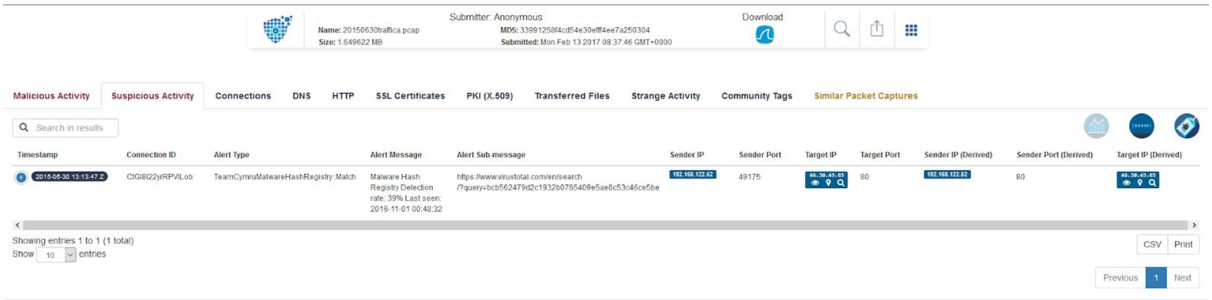
Behaviour Graph Source: Joe Sandbox



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Remote Management	Registry Run Keys / Startup Folder 1	Port Monitors	Software Packing 1 1	Input Capture 1	System Time Discovery 1	Remote File Copy 4	Input Capture 1	Data Encrypted 1	Standard Cryptographic Protocol 2
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Deobfuscate/Decode Files or Information 1	Network Sniffing	Security Software Discovery 3 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Remote File Copy 4
Drive-by Compromise	Windows Management Instrumentation	Accessibility Features	Path Interception	File Deletion 1	Input Capture	Remote System Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Non-Application Layer Protocol 3
Exploit Public-Facing Application	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information 2 1	Credentials in Files	File and Directory Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Standard Application Layer Protocol 3
Spearphishing Link	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	DLL Side-Loading 1	Account Manipulation	System Information Discovery 1 1	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol

Mitre Attack Matrix Source: Joe Sandbox



Submitter: Anonymous

Name: 20150630traffica.pcap **MD5:** 33991258f4cd54e30efff4ee7a250304

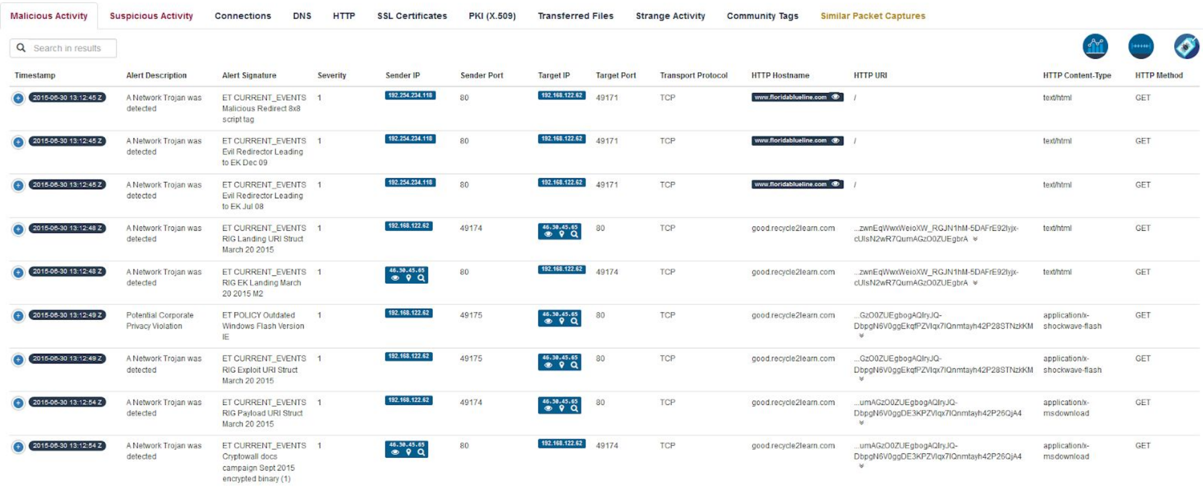
Size: 1.649622 MB **Submitted:** Mon Feb 13 2017 08:37:46 GMT+0000

Timestamp	Connection ID	Alert Type	Alert Message	Alert Sub-message	Sender IP	Sender Port	Target IP	Target Port	Sender IP (Derived)	Sender Port (Derived)	Target IP (Derived)
2015-06-30 13:13:47 Z	CtGI8I22yRPVILob	TeamCymruMalwareHashRegistry::Match	Malware Hash Registry Detection rate: 39% Last seen: 2016-11-01 00:48:32	https://www.virustotal.com/en/search /?query=bcb562479d2c1932b0765409e5ae8c53c46ce5be	192.168.122.62	49175	46.30.45.65	80	192.168.122.62	80	46.30.45.65

Showing entries 1 to 1 (1 total)

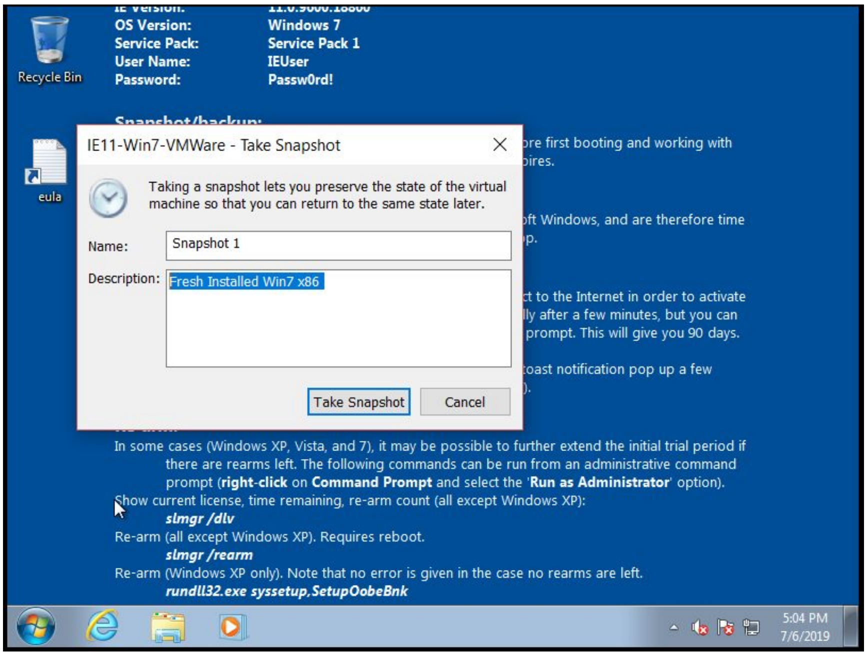
Show 10 entries

Suspicious Activity (Network) Source: PacketTotal



Timestamp	Alert Description	Alert Signature	Severity	Sender IP	Sender Port	Target IP	Target Port	Transport Protocol	HTTP Hostname	HTTP URI	HTTP Content-Type	HTTP Method
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Malicious Redirect 8x8 script tag	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com	/	text/html	GET
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Dec 09	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com	/	text/html	GET
2015-06-30 13:12:45 Z	A Network Trojan was detected	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 08	1	192.254.234.118	80	192.168.122.62	49171	TCP	www.floridablueline.com	/	text/html	GET
2015-06-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Landing URI Struct March 20 2015	1	192.168.122.62	49174	46.30.45.65	80	TCP	good.recycle2learn.com	...zwnEqWwxWeioXW_RGJN1hM-5DAFrE92lyjx-cUIsN2wR7QumAGzO0ZUEgbrA	text/html	GET
2015-06-30 13:12:48 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG EK Landing March 20 2015 M2	1	46.30.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com	...zwnEqWwxWeioXW_RGJN1hM-5DAFrE92lyjx-cUIsN2wR7QumAGzO0ZUEgbrA	text/html	GET
2015-06-30 13:12:49 Z	Potential Corporate Privacy Violation	ET POLICY Outdated Windows Flash Version IE	1	192.168.122.62	49175	46.30.45.65	80	TCP	good.recycle2learn.com	...GzO0ZUEgbogAQlryJQ-DbpgN6V0ggEkqfPZVlqx7IQnmtayh42P28STNzkKM	application/x-shockwave-flash	GET
2015-06-30 13:12:49 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Exploit URI Struct March 20 2015	1	192.168.122.62	49175	46.30.45.65	80	TCP	good.recycle2learn.com	...GzO0ZUEgbogAQlryJQ-DbpgN6V0ggEkqfPZVlqx7IQnmtayh42P28STNzkKM	application/x-shockwave-flash	GET
2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS RIG Payload URI Struct March 20 2015	1	192.168.122.62	49174	46.30.45.65	80	TCP	good.recycle2learn.com	...umAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4	application/x-msdownload	GET
2015-06-30 13:12:54 Z	A Network Trojan was detected	ET CURRENT_EVENTS Cryptowall docs campaign Sept 2015 encrypted binary (1)	1	46.30.45.65	80	192.168.122.62	49174	TCP	good.recycle2learn.com	...umAGzO0ZUEgbogAQlryJQ-DbpgN6V0ggDE3KPZVlqx7IQnmtayh42P26QjA4	application/x-msdownload	GET

Malicious Activity(Network) Source: PacketTotal



IE Version: 11.0.9600.18800
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:

re first booting and working with
ires.

ft Windows, and are therefore time
p.

t to the Internet in order to activate
lly after a few minutes, but you can
prompt. This will give you 90 days.

oast notification pop up a few
).

IE11-Win7-VMWare - Take Snapshot

Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.

Name: Snapshot 1

Description: Fresh Installed Win7 x86

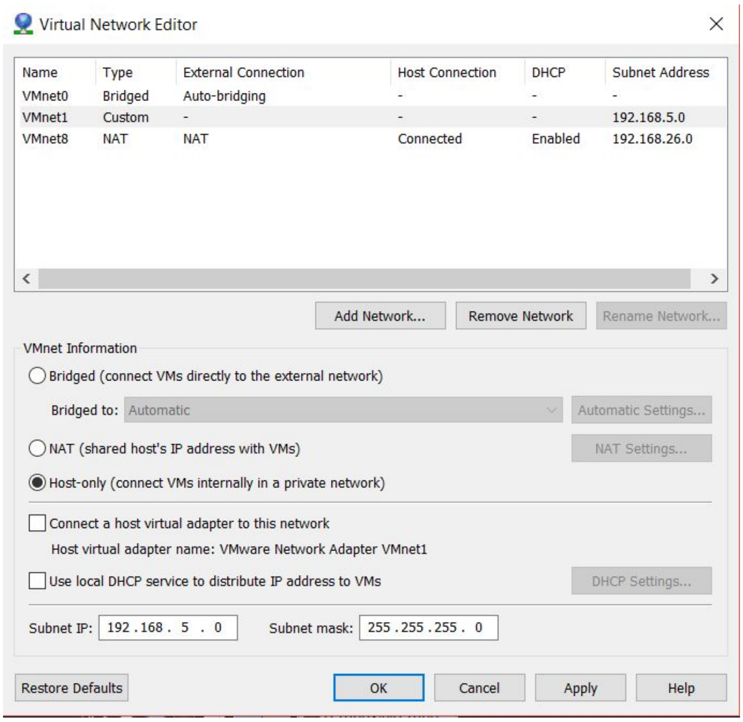
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).

Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv

Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

SNAPSHOT CREATED



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Custom	-	-	-	192.168.5.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.26.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

□ Connect a host virtual adapter to this network

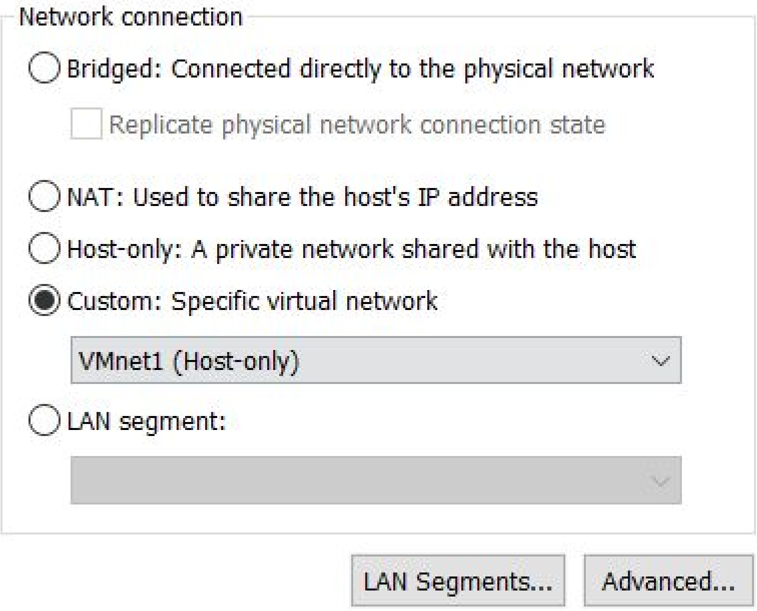
Host virtual adapter name: VMware Network Adapter VMnet1

□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 .168 . 5 . 0

Subnet mask: 255 .255 .255 . 0

VM SET TO HOST ONLY



Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

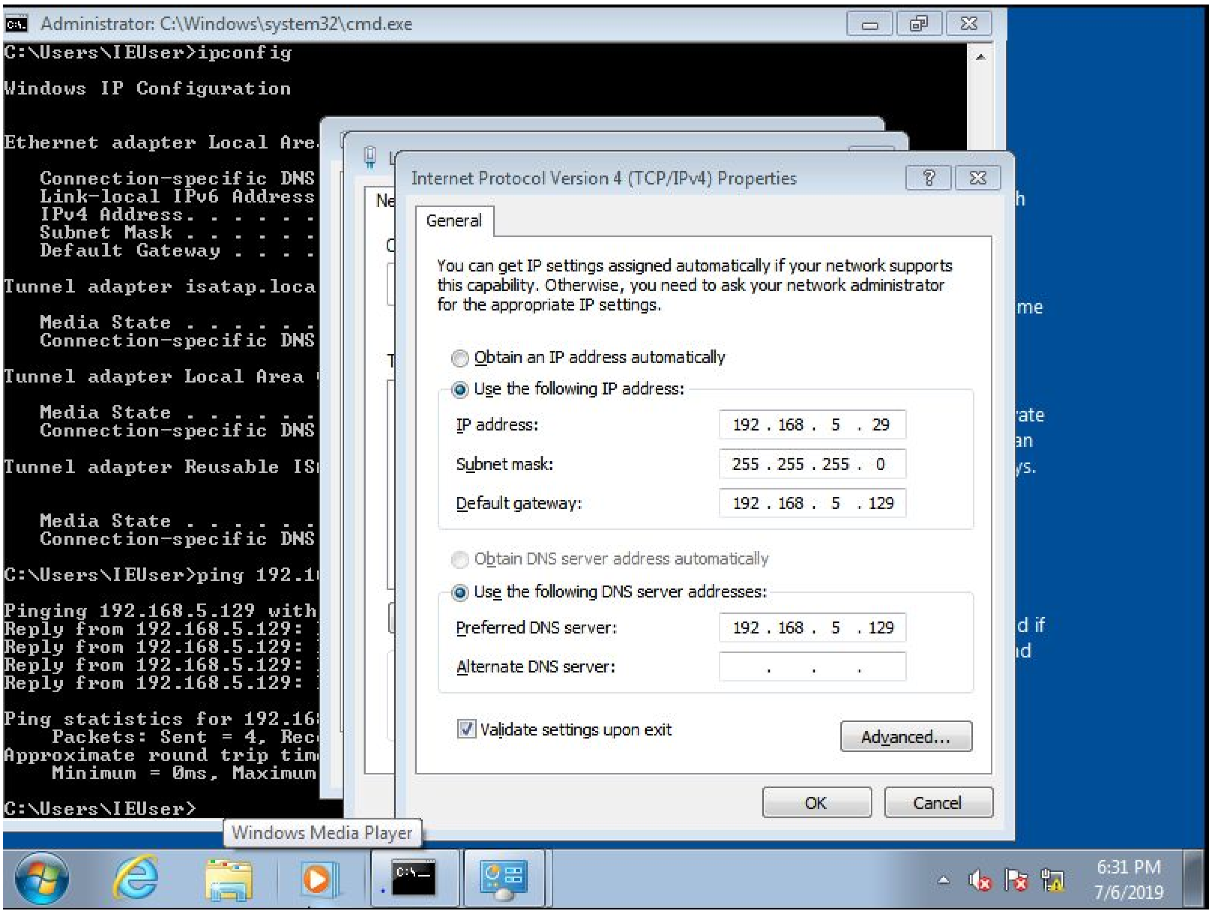
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet1 (Host-only)

○ LAN segment:

NETWORK ADAPTOR CONFIGURATION



```
C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Local Are

   Connection-specific DNS
   Link-local IPv6 Address
   IPv4 Address. . . . . .
   Subnet Mask . . . . . .
   Default Gateway . . . .

Tunnel adapter isatap.loca

   Media State . . . . . .
   Connection-specific DNS

Tunnel adapter Local Area

   Media State . . . . . .
   Connection-specific DNS

Tunnel adapter Reusable IS

   Media State . . . . . .
   Connection-specific DNS

C:\Users\IEUser>ping 192.1

Pinging 192.168.5.129 with
Reply from 192.168.5.129:
Reply from 192.168.5.129:
Reply from 192.168.5.129:
Reply from 192.168.5.129:

Ping statistics for 192.16
    Packets: Sent = 4, Rec
Approximate round trip tim
    Minimum = 0ms, Maximum

C:\Users\IEUser>
```

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

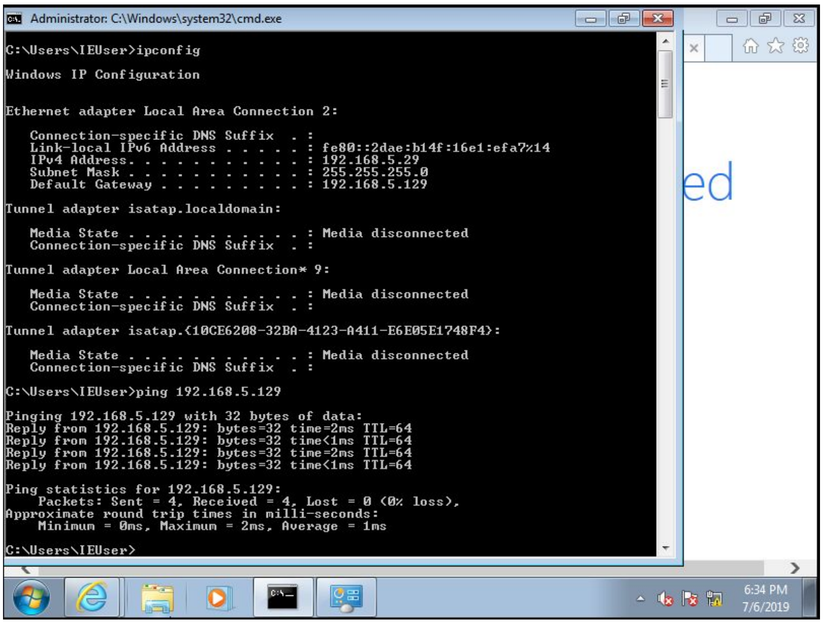
IP address: 192 . 168 . 5 . 29
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 5 . 129

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 5 . 129
Alternate DNS server: . . .

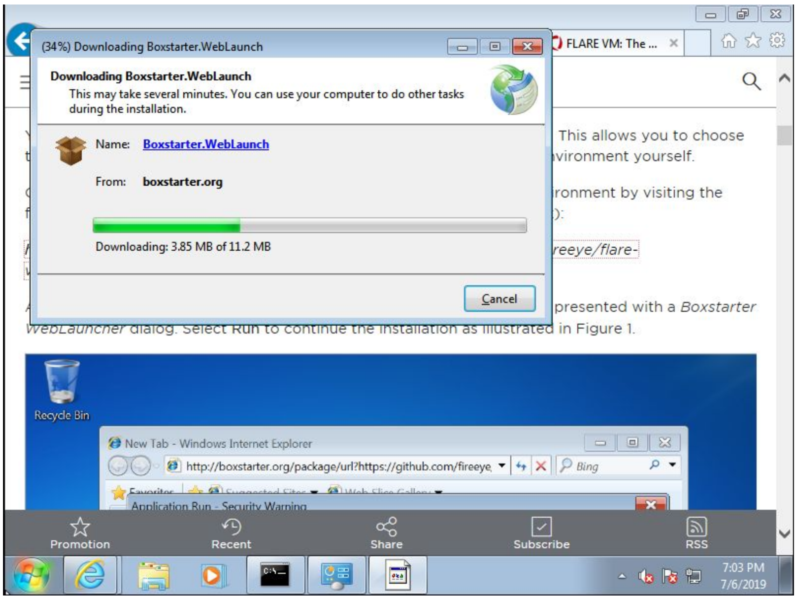
☑ Validate settings upon exit

STATIC IP ASSIGNED



```
C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2dae:b14f:16e1:efa7%14
   IPv4 Address. . . . . . . . . . . : 192.168.5.29
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.5.129

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{10CE6208-32BA-4123-A411-E6E05E1748F4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\IEUser>ping 192.168.5.129

Pinging 192.168.5.129 with 32 bytes of data:
Reply from 192.168.5.129: bytes=32 time=2ms TTL=64
Reply from 192.168.5.129: bytes=32 time<1ms TTL=64
Reply from 192.168.5.129: bytes=32 time=2ms TTL=64
Reply from 192.168.5.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.5.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\IEUser>
```

CONNECTION CHECK



(34%) Downloading Boxstarter.WebLaunch

Downloading Boxstarter.WebLaunch

This may take several minutes. You can use your computer to do other tasks during the installation.

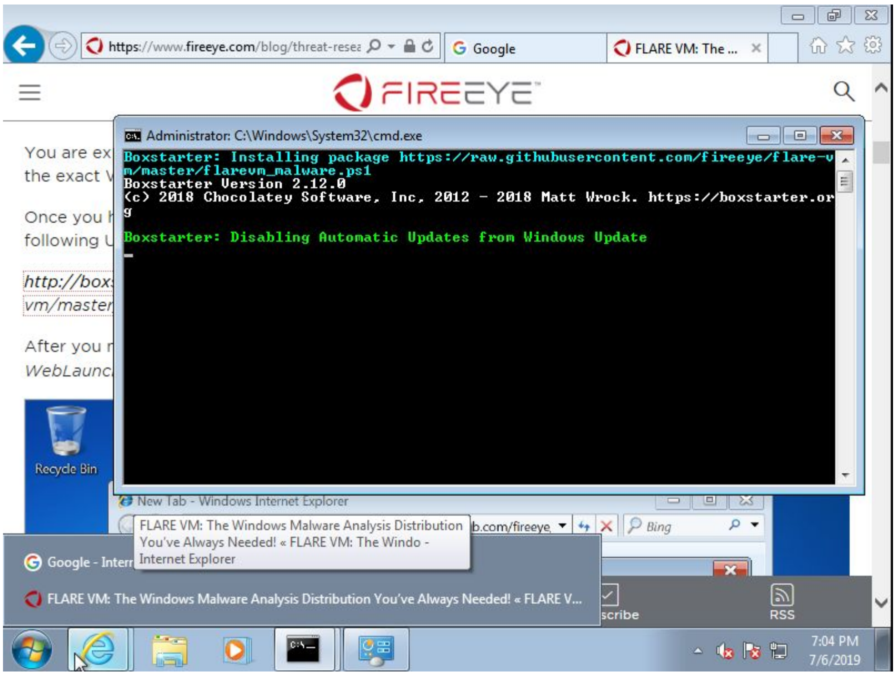
Name: Boxstarter.WebLaunch

From: boxstarter.org

Downloading: 3.85 MB of 11.2 MB

Cancel
FLARE VM: The ...
This allows you to choose
vironment yourself.
ronment by visiting the
):
reeye/flare-
presented with a Boxstarter
WebLauncher dialog. Select Run to continue the installation as illustrated in Figure 1.
Recycle Bin
New Tab - Windows Internet Explorer
http://boxstarter.org/package/url?https://github.com/fireeye
Bing
Application Run - Security Warning
Promotion
Recent
Share
Subscribe
RSS
7:03 PM
7/6/2019

FLARE SETUP

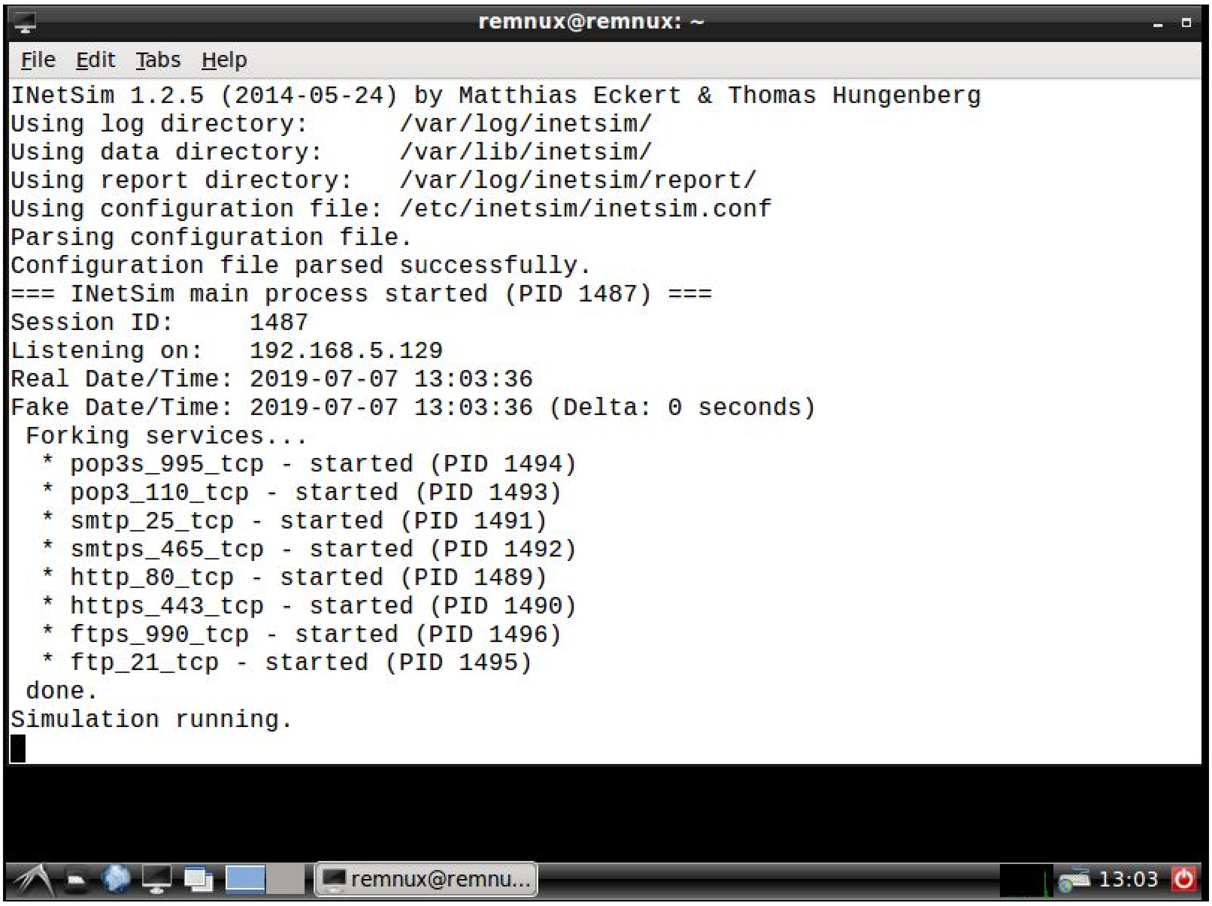


Administrator: C:\Windows\System32\cmd.exe

```
Boxstarter: Installing package https://raw.githubusercontent.com/fireeye/flare-v
m/master/flarevm_malware.ps1
Boxstarter Version 2.12.0
(c) 2018 Chocolatey Software, Inc, 2012 - 2018 Matt Wrock. https://boxstarter.or
g

Boxstarter: Disabling Automatic Updates from Windows Update
_
```

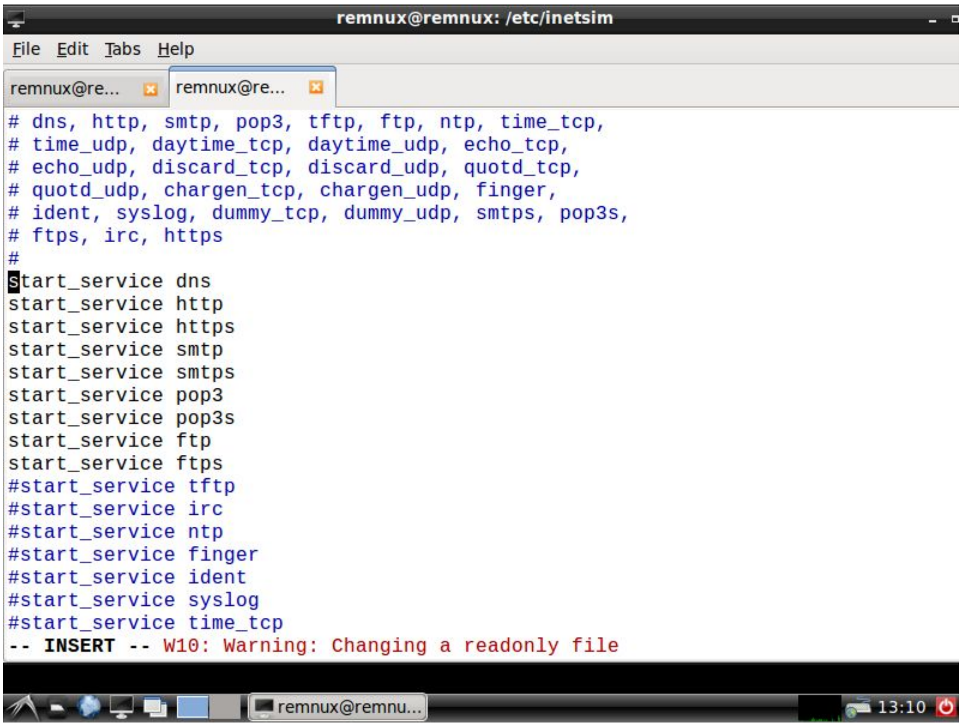
https://www.fireeye.com/blog/threat-resea
Google
FLARE VM: The ...
FIREEYE
You are ex
the exact V
Once you h
following U
http://box
vm/master
After you r
WebLaunc
Recycle Bin
New Tab - Windows Internet Explorer
FLARE VM: The Windows Malware Analysis Distribution You've Always Needed! « FLARE VM: The Windo - Internet Explorer
Google - Interr
FLARE VM: The Windows Malware Analysis Distribution You've Always Needed! « FLARE V...
scribe
RSS
7:04 PM
7/6/2019

FLARE VM RUNNING



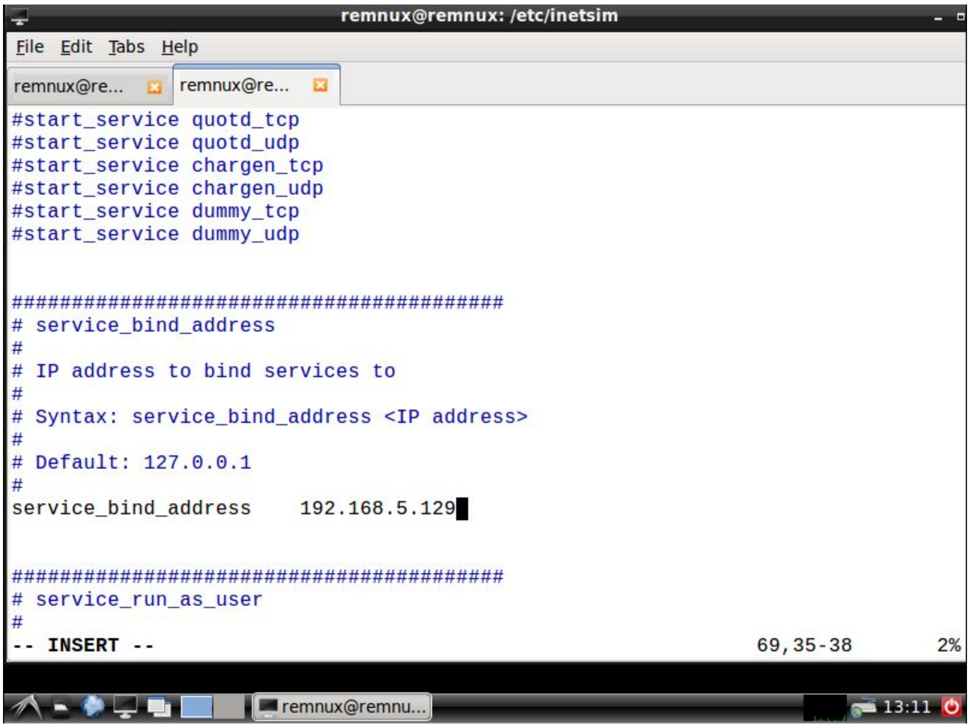
```
INetSim 1.2.5 (2014-05-24) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 1487) ===
Session ID:     1487
Listening on:   192.168.5.129
Real Date/Time: 2019-07-07 13:03:36
Fake Date/Time: 2019-07-07 13:03:36 (Delta: 0 seconds)
 Forking services...
  * pop3s_995_tcp - started (PID 1494)
  * pop3_110_tcp - started (PID 1493)
  * smtp_25_tcp - started (PID 1491)
  * smtps_465_tcp - started (PID 1492)
  * http_80_tcp - started (PID 1489)
  * https_443_tcp - started (PID 1490)
  * ftps_990_tcp - started (PID 1496)
  * ftp_21_tcp - started (PID 1495)
 done.
Simulation running.
```

INETSIM SIMULATION RUNNING



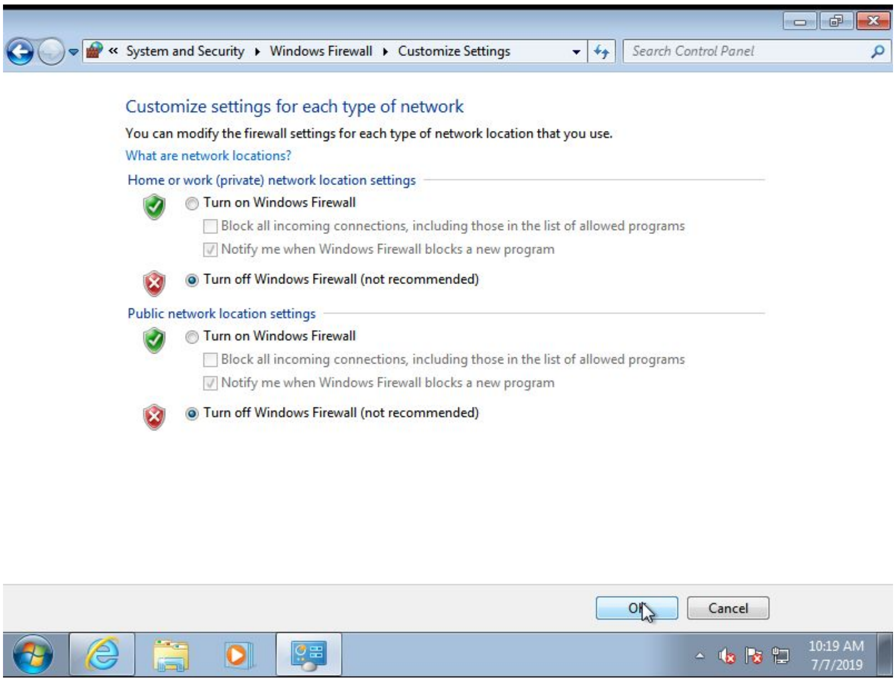
```
# dns, http, smtp, pop3, tftp, ftp, ntp, time_tcp,
# time_udp, daytime_tcp, daytime_udp, echo_tcp,
# echo_udp, discard_tcp, discard_udp, quotd_tcp,
# quotd_udp, chargen_tcp, chargen_udp, finger,
# ident, syslog, dummy_tcp, dummy_udp, smtps, pop3s,
# ftps, irc, https
#
start_service dns
start_service http
start_service https
start_service smtp
start_service smtps
start_service pop3
start_service pop3s
start_service ftp
start_service ftps
#start_service tftp
#start_service irc
#start_service ntp
#start_service finger
#start_service ident
#start_service syslog
#start_service time_tcp
-- INSERT -- W10: Warning: Changing a readonly file
```

DNS INETSIM



```
#start_service quotd_tcp
#start_service quotd_udp
#start_service chargen_tcp
#start_service chargen_udp
#start_service dummy_tcp
#start_service dummy_udp


#########################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address    192.168.5.129


#########################################
# service_run_as_user
#
-- INSERT --                                              69,35-38      2%
```

IP Binding INETSIM


« System and Security ▸ Windows Firewall ▸ Customize Settings
Search Control Panel
OK
Cancel
10:19 AM
7/7/2019

Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Firewall turned off

Note: *Same Malware Lab setup was used by me in my CA 1, thank you.*