

Advanced Malware Analysis

PERFORMING SAFE DYNAMIC ANALYSIS



Dr. Jared DeMott

SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com



Overview



Goals of Malware Analysis

Another example

Common Malware Types

Runtime Malware Analysis





Goals

- Signatures



Indicators of Compromise





Understanding communications





Anti-analysis





Research


- <http://cyberthreatalliance.org/cryptowall-report.pdf>
- <http://labs.lastline.com/a-peek-behind-the-cryptowall>
- <http://blogs.cisco.com/security/talos/teslacrypt>

Internet Explorer Malware


SEVERITY: HIGH


ISOLATED 

LAVA has identified malicious activity targeting Internet Explorer. vSentry has successfully isolated the threat and generated a detailed profile of the malicious activity.


 **Computer**
WIN-6FA51D049IN

 **User**
jared

 **Resources**
<http://alexu.edu.eg/index.php/ar/>

 **Action set**
Continued

Generate Report 

Threat Information 

Geolocations




Alexandria University Faculty Of Science


جامعة الاسكندرية




Threat Behavioral Graph

BEHAVIORAL EVENTS

 17:16:12 Internet Explore...

 17:16:12 Network

 17:16:12 Network

BEHAVIORAL DETECTION GRAPH



Uncategorized

Persistence 2

Privilege Escalations 5

Updating OS Setting 4

Anti-Forensic 1

Code-Injection 1

Crypto M



Network

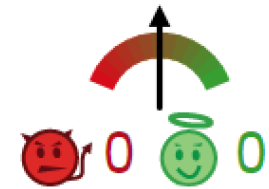
Feb 27, 2016, 17:16:13



URL: <http://alexu.edu.eg/index.php/ar/>

Detection ratio: 0 / 67

Analysis date: 2016-02-28 18:34:58 UTC (0 minutes ago)



Analysis Additional information Comments Votes

URL Scanner	Result
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira	Clean site
Baidu-International	Clean site
BitDefender	Clean site
Blueliv	Clean site









File not found

The file you are looking for is not in our database.

[Take me back to the main page](#)[Try another search](#)

 B4CD.tmp.exe	2/28/2016 1:25 PM	Application	360 KB
 EE93.tmp.exe	2/28/2016 1:26 PM	Application	360 KB
 massxfynhcd.exe	2/28/2016 1:24 PM	Application	360 KB
 vdespohcfeyy.exe	2/28/2016 1:25 PM	Application	360 KB

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files ?

All of your files were protected by a strong encryption with AES

More information about the encryption keys using AES can be found here: <http://en.wikipedia.org/wiki/AES>

How did this happen ?

!!! Specially for your PC was generated personal AES KEY, both public and private.

!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.

!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?

So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way.

If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://gwe32fdr74bhfsyujb34gfszfv.zatcurr.com/7B95F5D082869DF8>

2. <http://tes543berda73i48fsdfs.kerataadze.at/7B95F5D082869DF8>

3. <http://tt54rfdjhb34rfbnknaerg.milerteddy.com/7B95F5D082869DF8>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>

2. After a successful installation, run the browser

3. Type in the address bar: xlowfznrg4wf7dli.onion/7B95F5D082869DF8

4. Follow the instructions on the site.

----- IMPORTANT INFORMATION -----

--* Your personal pages:

<http://gwe32fdr74bhfsyujb34gfszfv.zatcurr.com/7B95F5D082869DF8>

<http://tes543berda73i48fsdfs.kerataadze.at/7B95F5D082869DF8>

<http://tt54rfdjhb34rfbnknaerg.milerteddy.com/7B95F5D082869DF8>

--* Your personal page Tor-Browser: xlowfznrg4wf7dli.ONION/7B95F5D082869DF8



 EN  IT  FR  ES  DE

Service to decrypt the files.

To continue please enter the code from the picture in the input field.



Code of picture:

Enter to decrypt service



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **05/03/16** the cost of decrypting files will increase **2** times and will be **1000 USD**

Prior to increasing the amount left:

First connect IP: 12.226.95.51

[Refresh](#)[Payment](#)[FAQ](#)[Decrypt 1 file for FREE](#)[Support](#)

We present a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.



2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods of creating wallet](#))

3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [bitquick.co](#) - Good service for United States.
- [localbitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly (WU, Cash, SEPA, Paypal and many others).
- [cex.io](#) - Buy Bitcoins with Visa/Mastercard or Wire Transfer.
- [coincafe.com](#) - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order.



- bitstamp.net - Old and trusted Bitcoin dealer.
- btc-e.com - BTC dealer, Visa/Mastercard and etc.

Couldn't find BTC in your location? Try searching these directories:

- buybitcoinworldwide.com - An international directory of bitcoin exchanges.
- bitcoin-net.com - One more BTC dealer directory.
- howtobuybitcoins.info - An international directory of bitcoin exchanges.
- bittybot.co/eu/ - EU countries directory.

4. Send **1.2 BTC** to Bitcoin address: **17VcjEhFwQtGM4kwEVRMAArnQUvTKBJL3D**

5. Enter the Transaction ID and chose payment option:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

6. Please check the payment information and click "PAY".

PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status
-----	------------	--------------------------------	--------	--------

Your payments not found.

0 valid drafts are put, the total amount of 0 USD.



5. Enter the Transaction ID and chose payment option:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

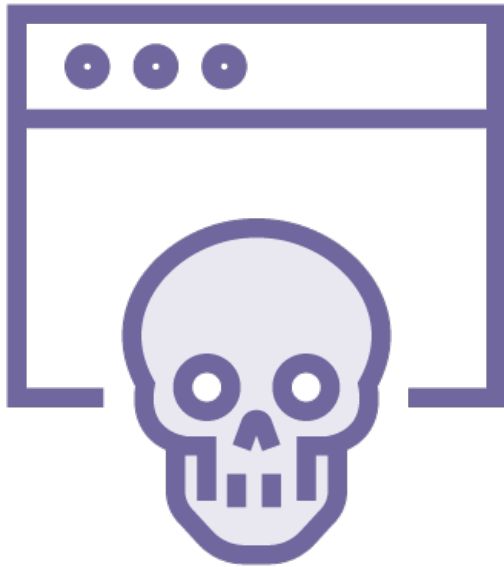
6. Please check the payment information and click "PAY".

PAY

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status
1	Bitcoin	KISSMYA\$\$I\mBromiumprotected	0	Pending

0 valid drafts are put, the total amount of 0 USD.





Malware

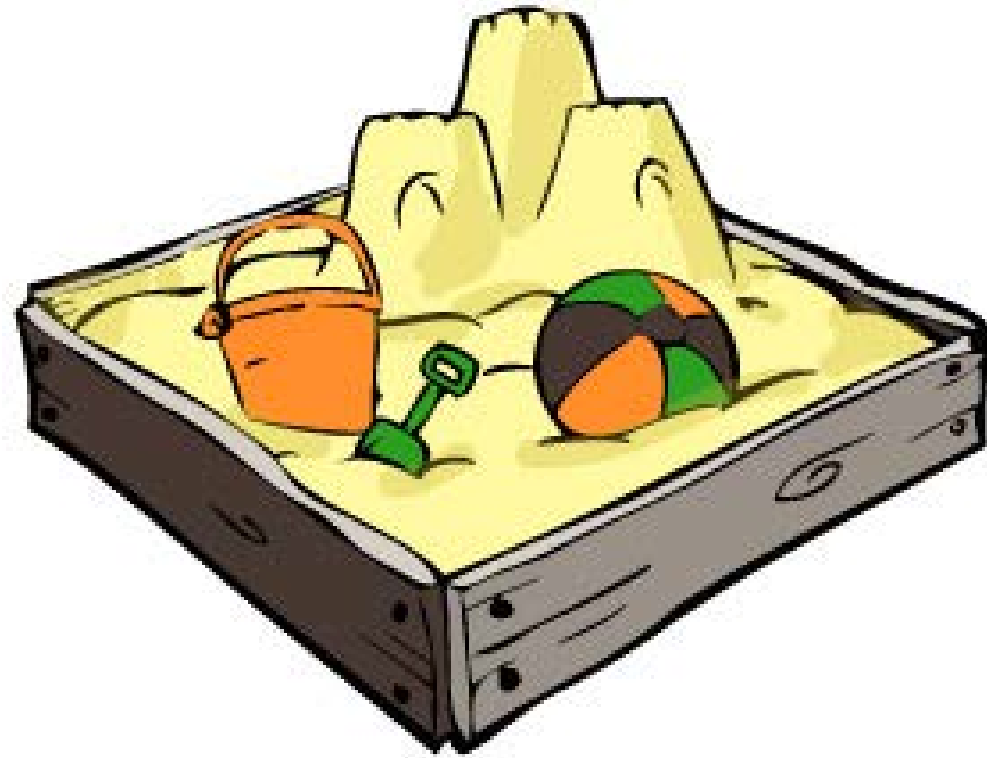
- PUP
 - Adware
- Downloaders
- Bots
- RATs
- Ransomware
- Banking Trojan
- Targeted or blended threats



Approach?

- VT
- Runtime analysis

Dynamic Analysis





File Details

FILE NAME	vdespohcfeyy.exe
FILE SIZE	368640 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5	9ce01dfbf25dfea778e57d8274675d6f
SHA1	1bd767beb5bc36b396ca6405748042640ad57526
SHA256	5343947829609f69e84fe7e8172c38ee018ede3c9898d4895275f596ac54320d
SHA512	d6ba89c1f221a94e3061bc4da896760d99935a7c766b8e4e30146266cf3356acd883835e75dbb86574bc869c83d381c8f
CRC32	4A1FAD43
SSDEEP	6144:4qZbqZToxlizLBZ6R56VkGM4ceLJ5vs5JGJceO/QCErliuNAvwu:4qZb8oR3D6R5QHXYZJy/Q50imAvB
YARA	None matched



Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

Comment Board (0)

PE Imphash

c00702bdb5e1419c3dc899a74a60a37d

Version Infos

LEGALCOPYRIGHT	\xa9nah nah Corporation. All rights reserved.
INTERNALNAME	nah nah
FILEVERSION	1.600.5512
COMPANYNAME	nah nah Corporation
PRODUCTNAME	nah nah\xae
PRODUCTVERSION	1.9.0
FILEDESCRIPTION	nah nahApp
ORIGINALFILENAME	nah nah
TRANSLATION	0x0409 0x04b0



Static Analysis

Behavioral Analysis

Network Analysis

Dropped Files

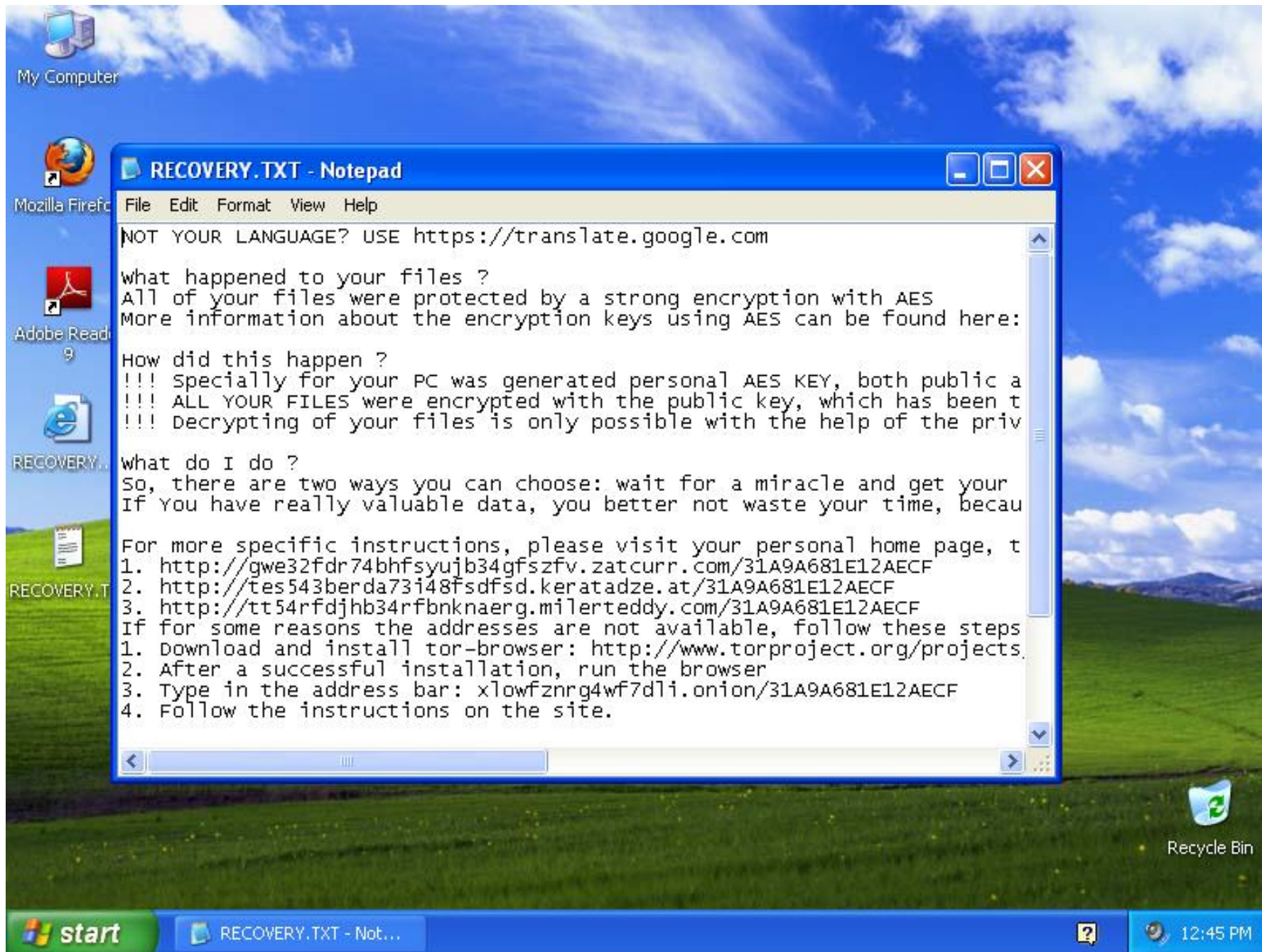
Comment Board (0)



- X-axis by: [event](#)
- Y-axis by: [category](#)

- **vdespohcfeyy.exe** 1332
 - **fdocgpiqrtnt.exe** 1708
 - **NOTEPAD.EXE** 1800
 - **iexplore.exe** 1796
 - **Rundll32.exe** 1964
 - **rundll32.exe** 1784
 - **cmd.exe** 260





Hosts

IP
192.185.39.66
62.210.141.228

Domains

DOMAIN	IP
biocarbon.com.ec	192.185.39.66
imagescroll.com	62.210.141.228

Summary

- Files
- Registry Keys
- Mutexes

```
C:\WINDOWS\system32\msctfime.ime
C:\DOCUME~1\User\LOCALS~1\Temp\vdespohcfeyy.exe:Zone.Identifier
C:\DOCUME~1\User\LOCALS~1\Temp\vdespohcfeyy.exe
C:\WINDOWS\vdespohcfeyy.exe
C:\WINDOWS\fdocgpiqrtnt.exe
C:\WINDOWS\fdocgpiqrtnt.exe:Zone.Identifier
PIPE\wkssvc
PIPE\svrsvc
C:\WINDOWS\system32\rsaenh.dll
C:\Documents and Settings\User\My Documents\recover_file_fkdemquae.txt
C:\Documents and Settings\User\Local Settings\Temporary Internet Files
```



Deepviz - Malware Analyzer



Behaviours

#	Description
1	Creates autorun registry key
2	Attempts connections to suspicious countries
3	Steals local browser data
4	Injects code into other processes
5	Searches for digital certificates
6	Drops EXE file
7	Manipulates Internet Explorer settings
8	Loads dropped image
9	Injects dropped images in already existing process
10	Runs dropped executable
11	Runs existing executable
12	Deletes itself
13	Automatically unpack its own code
14	Suspicious delay
15	Creates an executable into the startup folder
16	Gathers system data

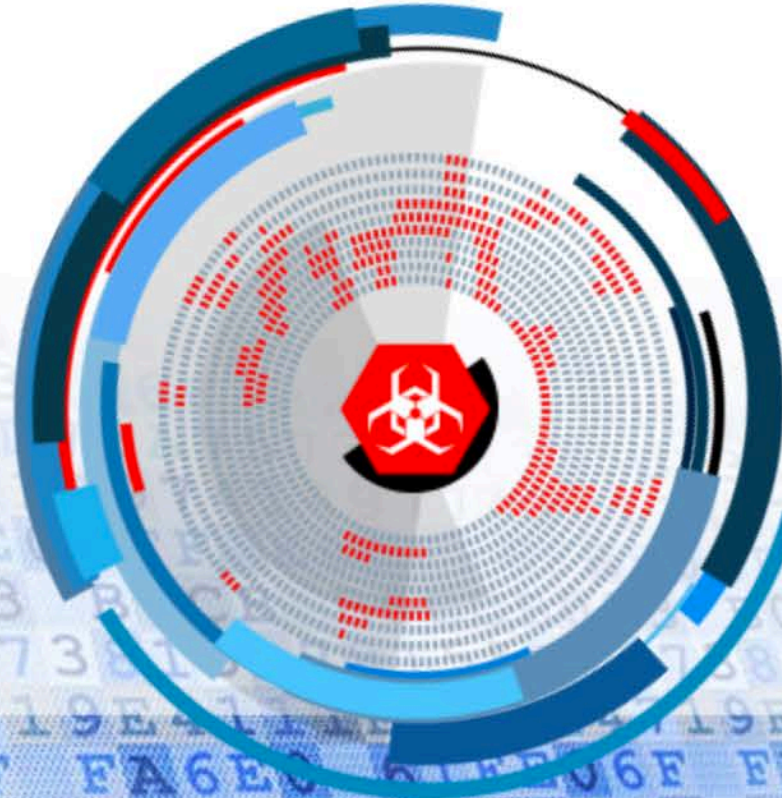
Host resolved	Alias chain	Addresses
worldisonefamily.info		23.229.4.214
surrogacyandadoption.com		185.26.122.59
imagescroll.com		62.210.141.228
stacon.eu		188.116.9.2
music.mbsaeger.com		76.125.213.205
biocarbon.com.ec		192.185.39.66





data	type	process	address	url	referer	dataSize
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	192.185.39.66:80			899
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	62.210.141.228:80			897
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	76.125.213.205:80			893
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	188.116.9.2:80			873
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	185.26.122.59:80			888
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	23.229.4.214:80			898
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	192.185.39.66:80			899
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	62.210.141.228:80			897
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	76.125.213.205:80			893
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	188.116.9.2:80			873
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	185.26.122.59:80			888
🚩	send	C:\Windows\uppqxgrkgjgm.exe (v. 5.1.2600.5512)	23.229.4.214:80			898

<http://bit.ly/20YE3Ds> pic.twitter.com/kGTd3EDifc — 2nd: The C-code generation when combined with the execution graphs allows the analyst to quic

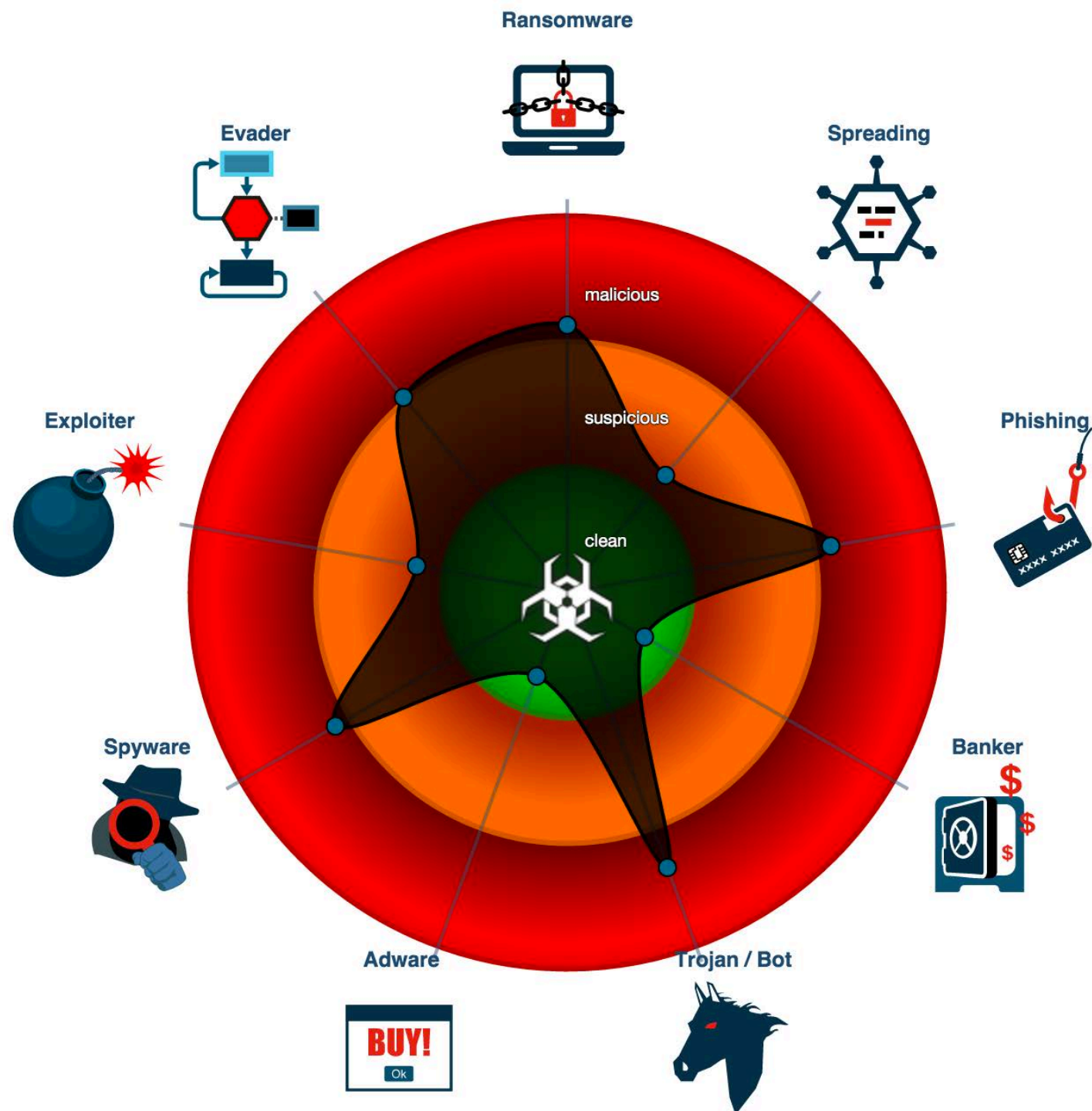
Prepared to fight evasive cyber threats?

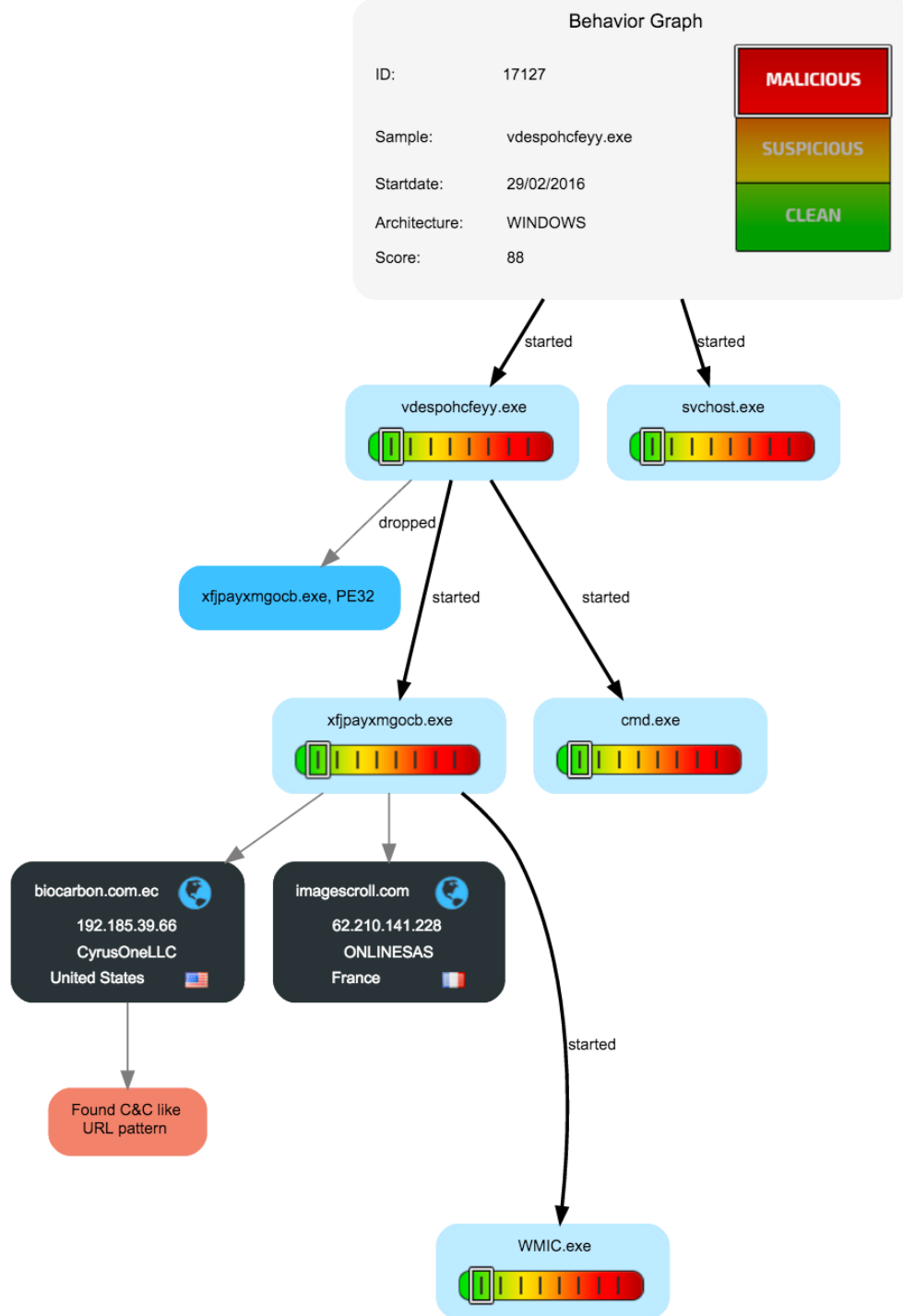
Open and agile malware analysis tools to deeply understand malicious codes.



-  Deletes Windows files
-  Executes code after phone reboot
-  PE file contains an invalid checksum
-  Queries SIM card contact information







Show sourcesShow sources

Execution Coverage



Dynamic/Packed Code Coverage



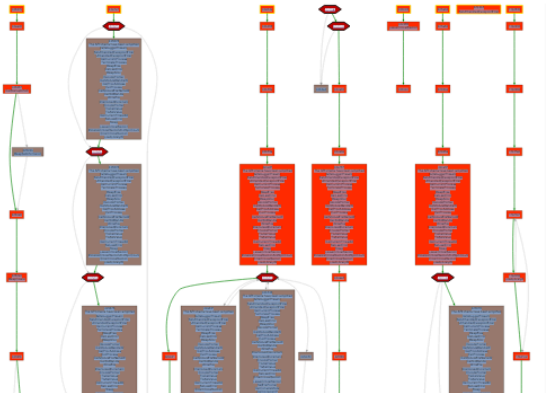
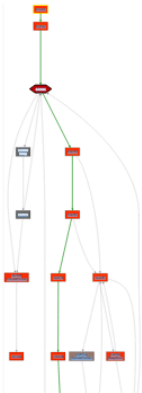
Signature Coverage



Execution Coverage:	3.4%
Dynamic/Decrypted Code Coverage:	100%
Signature Coverage:	5.2%
Total number of Nodes:	2000
Total number of Limit Nodes:	53

Hide Nodes/Edges

Show legend



- **API Calls:**
 - The API chains have been simplified
 - IsDebuggerPresent
 - SetUnhandledExceptionFilter
 - UnhandledExceptionFilter
 - GetCurrentProcess
 - TerminateProcess
 - HeapFree
 - GetLastError
 - HeapAlloc
 - DecodePointer

Summary



Analyze

- Report
 - Dynamic runtime
 - Static file analysis
 - Static code review
 - Debugging code