

MICHIGAN STATE
UNIVERSITY
Beta Presentation

Next Generation Malware Analysis
System

The Capstone Experience

Team Proofpoint

Brad Doherty

Crystal Lewis

Yash Patel

Graham Thomas

George Zhao



*From Students...
...to Professionals*

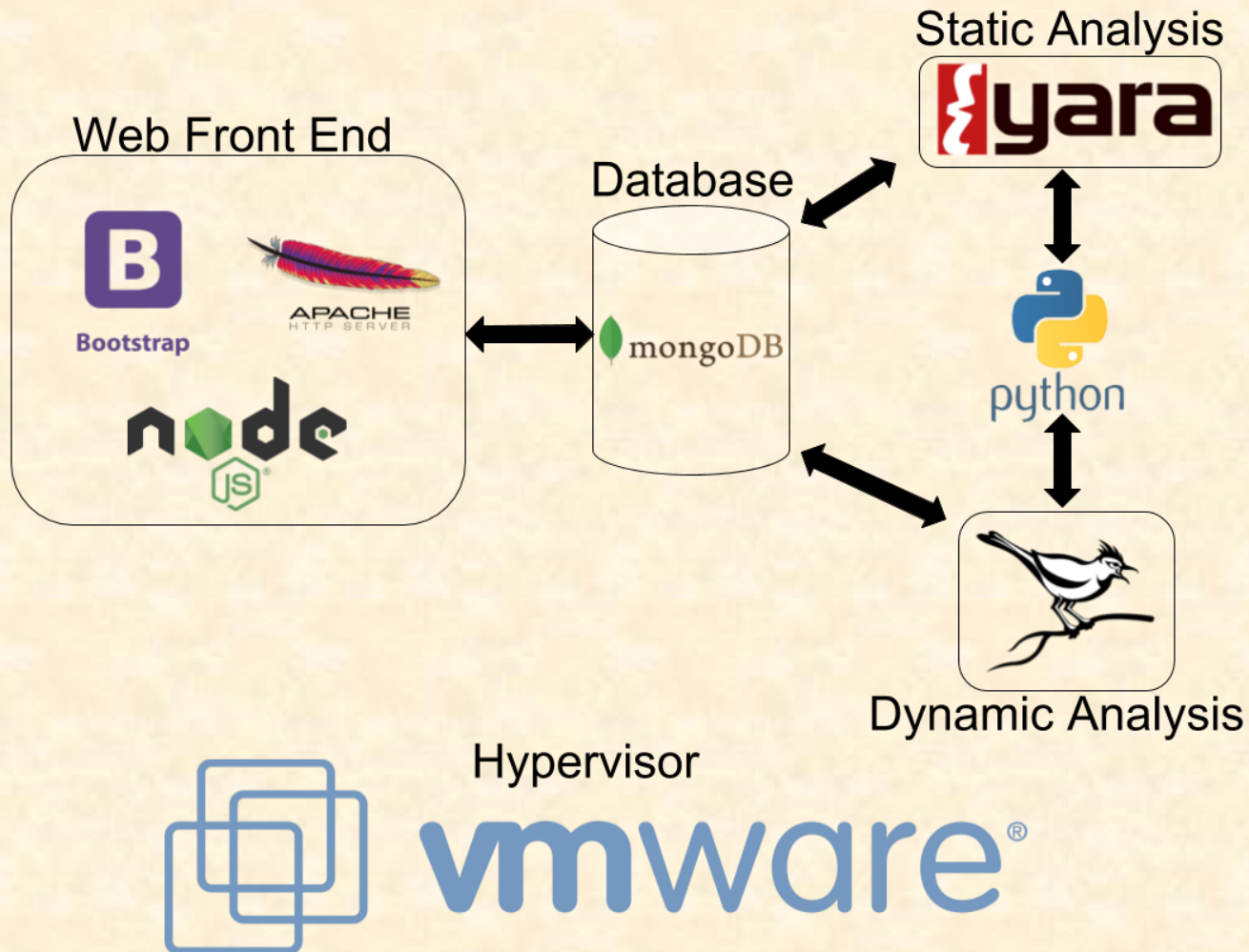
Department of Computer Science and Engineering
Michigan State University
Spring 2018

Project Overview

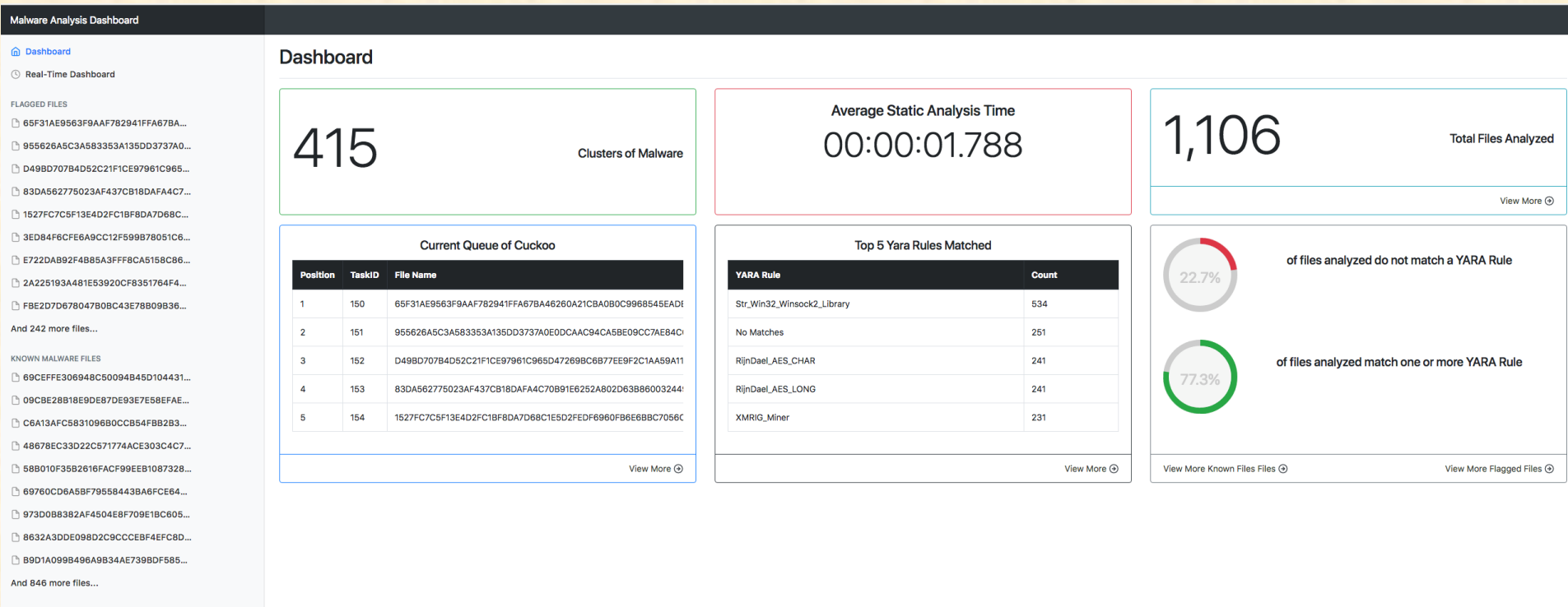
- Efficiently analyze different types of malware
- Cluster similar malware
- Provide dashboard for malware analysis data
- Provide framework for signature generation



System Architecture



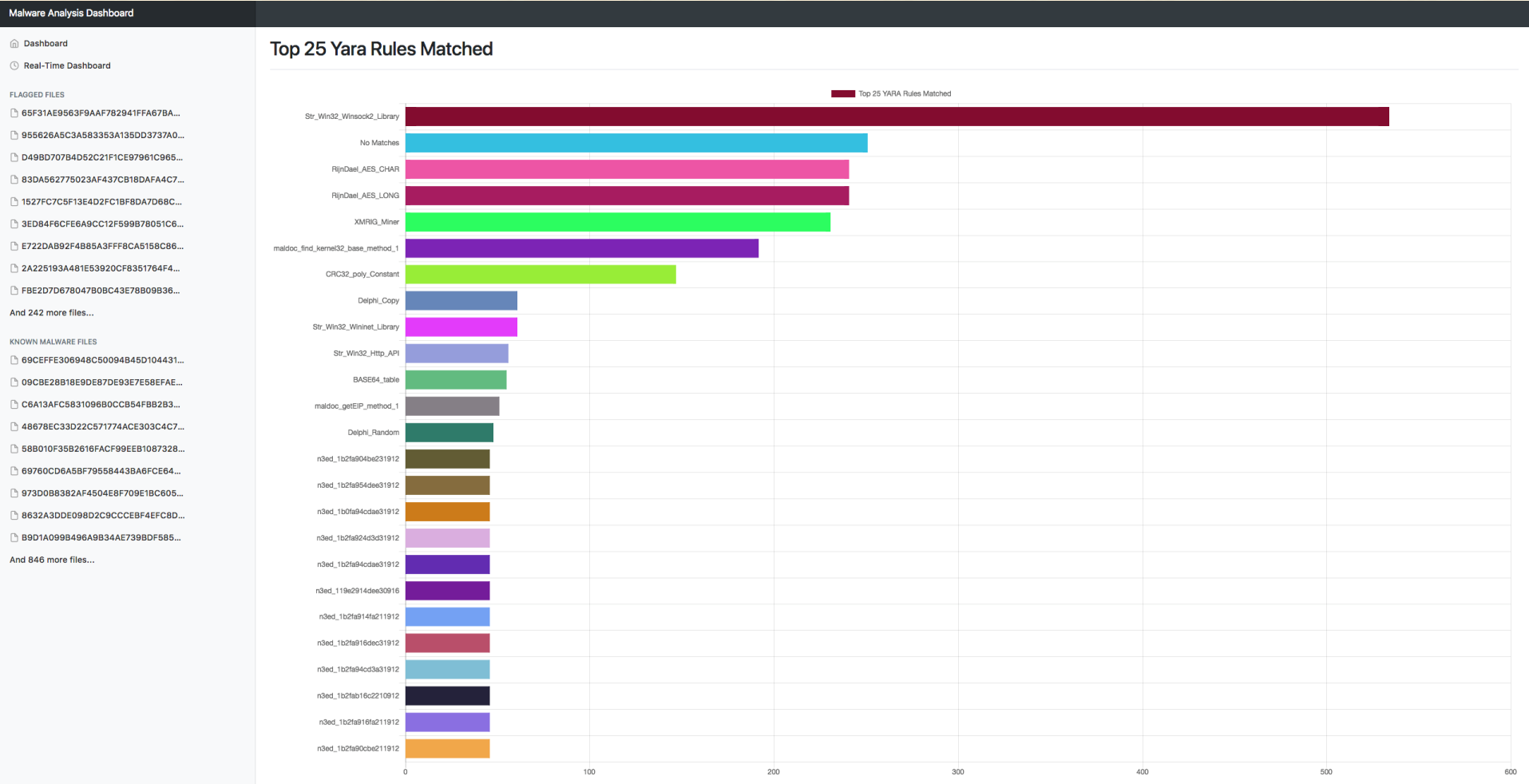
Main Page On Dashboard



All Malware Files Table

Malware Analysis Dashboard				
<div><div><div><div><div></div><div>Dashboards</div></div><div><div></div><div>Real-Time Dashboard</div></div></div><div>FLAGGED FILES</div><div><div>65F31AE9563F9AAF782941FFA67BA...</div><div>955626A5C3A583353A135DD3737A0...</div><div>D498D707B4D52C21F1CE97961C965...</div><div>83DA562775023AF437CB18DAFA4C7...</div><div>1527FC7C5F13E4D2FC1BF8DA7D68C...</div><div>3EDB4F6CFE6A9CC12F599B78051C6...</div><div>E722DAB92F4B85A3FF8CA5158C86...</div><div>2A225193A481E53920CF8351764F4...</div><div>FBE2D7D67804780B8C43E78809B36...</div></div><div>And 242 more files...</div><div>KNOWN MALWARE FILES</div><div><div>69CEFFE306948C50094B45D104431...</div><div>09C8E28B18E9DE87DE93E7E58EFAE...</div><div>C6A13AFC5831096B0CCB54FB82B3...</div><div>4867EC3D3D22C571774ACE303C4C7...</div><div>58B010F35B2616FACF99EEB1087328...</div><div>69760CD6A5BF79558443BA6FCE64...</div><div>973D0B8382AF4504E8F709E18C605...</div><div>8632A3DDE098D2C9CCCEBF4EFC8D...</div><div>B9D1A099B496A9B34AE7398BDF585...</div></div><div>And 846 more files...</div></div></div>				
All Malware Files				
<div><div>Show50entries</div><div>Search:</div></div>				
SID	File Name	File Type	# of YARA Matches	Flagged?
1	65F31AE9563F9AAF782941FFA67BA46260A21CBA0B0C9968545EADef4CE70E7	PE32 executable (GUI) Intel 80386, for MS Windows	0	Yes
2	955626A5C3A583353A135DD3737A0E0DCAAC94CA5BE09CC7AE84CCF5B461ACE	PE32 executable (GUI) Intel 80386, for MS Windows	0	Yes
3	D498D707B4D52C21F1CE97961C965D47269BC6B77EE9F2C1AA59A11AF8F39C3	PE32 executable (GUI) Intel 80386, for MS Windows	0	Yes
4	83DA562775023AF437CB18DAFA4C70B91E6252A802D63B86003244992ACA337	PE32+ executable (console) x86-64, for MS Windows	0	Yes
5	1527FC7C5F13E4D2FC1BF8DA7D68C1E5D2FEDF6960FB6E6BBC7056C4C372471	PE32+ executable (GUI) x86-64, for MS Windows	0	Yes
6	69CEFFE306948C50094B45D104431166AFB977AD75DA9F315B23E7EFBC08FB	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	2	No
7	09C8E28B18E9DE87DE93E7E58EFAED5C7B4CE36315068EE6A4E00444339B9E3	PE32 executable (GUI) Intel 80386, for MS Windows	36	No
8	C6A13AFC5831096B0CCB54FB82B3D14E4BA0E9C7A363C884B1383C5EE81FAA	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No
9	48678EC3D3D22C571774ACE303C4C771B46C8121FB646AFA807E54787671DE13	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No
10	58B010F35B2616FACF99EEB10873287844C1553D79880475CD5EC78F34351C	PE32+ executable (GUI) x86-64, for MS Windows	56	No
11	69760CD6A5BF79558443BA6FCE643F2F998E7E70B2FC9D0B180A66A7EE4D625	PE32 executable (GUI) Intel 80386, for MS Windows	9	No
12	973D0B8382AF4504E8F709E18C60578A8FD46DF8E8FA3A91CB4404078B95D55	PE32 executable (GUI) Intel 80386, for MS Windows	12	No
13	3EDB4F6CFE6A9CC12F599B78051C638E3E6A51453A0DFE8E3A3FFD6EA060DB7	PE32+ executable (GUI) x86-64, for MS Windows	0	Yes
14	8632A3DDE098D2C9CCCEBF4EFC8DEEBEFAA97978EE9D20D9CA992E295A802E9	PE32+ executable (GUI) x86-64, for MS Windows	1	No
15	B9D1A099B496A9B34AE7398BDF585297F50F548DCFFAE7BD	PE32 executable (GUI) Intel 80386, for MS Windows	11	No
16	879EBB0698CF93D4E8E90B79E6A4B1256AF425439226F13D6ED8644B8C2AA1	PE32 executable (native) Intel 80386, for MS Windows	20	No
17	A5072B34B8EF1C27ED440355D21566152895CDFA1D57CA9F731BD368C3004AF	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows	4	No

Top 25 Yara Rules Matched Graph



File Info Page

Malware Analysis Dashboard

Dashboard

Real-Time Dashboard

FLAGGED FILES

65F31AE9563F9AAF782941FFA67BA...

955626A5C3A583353A135DD3737A0...

D498D707B4D52C21F1CE97961C965...

83DA562775023AF437C818DAFA4C7...

1527FC7C5F13E4D2FC1BF8DA7D68C...

3ED84F6CFE6A9CC12F599B78051C6...

E722DAB92F4B85A3FF8CA5158C86...

2A225193A4481E53920CF8351764F4...

FBE2D7D678047B08C43E78B09B36...

And 242 more files...

KNOWN MALWARE FILES

69CEFFE306948C50094B45D104431...

09CBE28B18E9DE87DE93E7E58EFAE...

C6A13AFC583109680CCB54FB82B3...

48678EC33D22C571774ACE303CA7...

58B010F35B2616FACF99EEB1087328...

69760CD6A5B7F9558443BA6FCE64...

973D0B8382AF4504EBF709E1BC605...

8632A3DDE098D2C9CCCEBF4EFC8D...

B9D1A099B496A9B34AE739BD585...

And 846 more files...

PE Hash

SHA256

SHA1

MD5

3-N9K8gKRTeJ3HXKUQDZDhBMgR6mmWkWoPWW2zjUjVUn:N7TENXPQdHfzWf/W2Pf2+

13EE01EE8EA515C436D5110BE4612CEF3A41973439B7303356DCEFFA37B01901

F966381952994E7C2186E6AC1D1A213EA315D895

7C3AA34A2A8AAFDB8695325D3A5436FB

Similar Malware

Show10entries

Search:

File Name

PE Hash

052676CE939DE75433B97C6A87086FD6D69C734B24B64A4C4579899A6CE3B0A

3-N9K8gKRTeJ3HXKVCTSTg0BaoeRhQmSWVRndYm8eckqu:N7TENXfetg0lqnmwn

0C8CC948B56E1B84DEEC5E561951EA4FFBE8C0CFD0200C54E63D7D6E2C6C9D

3-N9K8gKRTeJ3HXKVqRgnklHggm1QYcBgYfLVUL5RhShGn:N7TENXT6KVWDJYTiVHShGn

10F04B166222635BD2938A57A5FC6032B7029BD13F1AC3C8C26338566FC2F8

3-N9K8gKRTeJ3HXKUJVwTXXXTXBcVmo2JJdsaaQmhn:N7TENXPbwH1Gmo2/dsaazh

119D4046B4ADAB0224C190D0D99D33FAF02F4ABA18CE342F879274E4A2CC4D7

3-N9K8gKRTeJ3HXKU1VRehyIKp9CkPgWPS9XmmJ:N7TENXP5eh6ikPgWOXmmJ

1EAC00FD1299F38CF964BA54B2ACBB154E98F46D4B4D6705D6E703ACF284808

3-N9K8gKRTeJ3HXKUgVJcqdnZyQnfgczhRnRtmb1J7kn:N7TENXPgbcqvtvnhzhlb1kn

2075A75B5C991BF65E1A48FBFCE8D4E07A87552C367EFB0D643FEC961683D1

3-N9K8gKRTeJ3HXKX4xbQtculjmmMGvQx/bvFwgc0RWhL:N7TENXLxbQRmMCQtxfw2WhL

241813A80ABB18FC8C09CEFAE0C292854898E06DFFCC86663C30D2002DED872

3-N9K8gKRTeJ3HXKXyefdqmq2mgjRgVmWdEdsEZhWLXunSzn:N7TENXBe1jq/zRgzidsOU+v

2F0EA548E40A95C2809F5A4800D3ACBF0CD2680C4FEF39C8A3A52AA42309F9

3-N9K8gKRTeJ3HXKXqY7UvVjkn0vzhXKajWz0kRXWEmn:N7TENXIM5Ky4o3/n

3439D421368F3EBF63687DDA5A3948BCE563C1777B57948D12D86BC520E8F

3-N9K8gKRTeJ3HXKWPR5jnmShbcnmbSglUhnXVgdlVn:N7TENXnrjntbcwJmXVQVn

3661B212690D0FAEFC9F053F2060BD6F0BB3952CC9E8D5E851B49036D696B2

3-N9K8gKRTeJ3HXKWWUXTqmS6KTVnFppm73nlUnphinx:N7TENXnwOTqzTVAJG

Showing 1 to 10 of 39 entries

Previous

1

2

3

4

Next

Yara Output

Show10entries

Search:

Rule

Namespace

Meta

maldoc_find_kernel32_base_method_1

rule13164

author: Didier Stevens (https://DidierStevens.com);

RijnDael_AES_CHAR

rule13149

date: 2016-06; description: RijnDael AES (check2) [char]; author: .pusher_;

RijnDael_AES_LONG

rule13149

date: 2016-06; description: RijnDael AES; author: .pusher_;

Str_Win32_Winsock2_Library

rule17

author: @adricnet; method: String match; description: Match Winsock 2 API library declaration;

XMRIG_Miner

rule54

Showing 1 to 5 of 5 entries

Previous

1


Next

The Capstone Experience

Team Proofpoint Beta Presentation

7

Signature Generation Page

 Dashboard Recent Pending Search

Submit

Import

Automated Signatures

DNS

Generated Signature

alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (www.msftncsi.com in DNS Lookup); dns_query; content:"www.msftncsi.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:88067683; rev:5; metadata: created_at 2018_3_28, updated_at 2018_3_28)
alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (dns.msftncsi.com in DNS Lookup); dns_query; content:"dns.msftncsi.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:87202183; rev:18; metadata: created_at 2018_3_28, updated_at 2018_3_28)
alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (teredo.ipv6.microsoft.com in DNS Lookup); dns_query; content:"teredo.ipv6.microsoft.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:98581784; rev:17; metadata: created_at 2018_3_28, updated_at 2018_3_28)

Generated Signature

alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (www.msftncsi.com in DNS Lookup); dns_query; content:"www.msftncsi.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:88067683; rev:5; metadata: created_at 2018_3_28, updated_at 2018_3_28)
alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (dns.msftncsi.com in DNS Lookup); dns_query; content:"dns.msftncsi.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:87202183; rev:18; metadata: created_at 2018_3_28, updated_at 2018_3_28)
alert dns \$HOME_NET any -> any any(msg:ETPRO Domain Observed (teredo.ipv6.microsoft.com in DNS Lookup); dns_query; content:"teredo.ipv6.microsoft.com"; isdataat:!1,relative; reference: md5,098adaa6fcebafefeb19774bbfb3e4e0; sid:98581784; rev:17; metadata: created_at 2018_3_28, updated_at 2018_3_28)

What's left to do?

- Website polish
- Any additional information put on dashboard
- Stretch Goals:
- Automation of Cuckoo Node Generation
- Distributed Cuckoo

Questions?

?

?

?

?

?

?

?

?

?

